Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-209

4 sierpnia 2023

Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

Niniejszy publikacja NSC 800-209, ***Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych***, opracowana została za zgodą National Institute of Science and Technology na podstawie specjalnej publikacji NIST SP 800-209, *Security Guidelines for Storage Infrastructure*.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy oraz kluczowe pojęcia z zakresu cyberbezpieczeństwa występujące w publikacji zdefiniowane są w dokumencie **NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***.

W publikacji posłużono się pojęciami zdefiniowanymi w poradniku źródłowym, na podstawie którego powstały niniejsze zalecenia. W przypadku, gdy tożsame pojęcia zostały zdefiniowane również w powszechnie obowiązujących aktach prawnych lub normatywnych, a ich definicja różni się od tej zamieszczonej w niniejszej publikacji, wówczas należy stosować sformułowania zawarte w tych aktach / w obiegu prawnym.

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem ,prywatnością działalności i majątku organizacji. Dotyczy to również osób fizycznych i państwa.

Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i rekomendacjami, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST jako godne zaufania i rekomendują stosowanie ich przez polskie

[1] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, rekomendacje i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:


Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.


+48222455922


sekretariat.dc@cyfra.gov.pl

Sprawozdania dotyczące technologii systemów komputerowych

Laboratorium Technologii Informacyjnych (*ang. Information Technology Laboratory – ITL*) przy Narodowym Instytucie Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*) działa na rzecz gospodarki USA i dobra publicznego poprzez zapewnienie technicznego wsparcia krajowej infrastruktury pomiarowej i normalizacyjnej. ITL opracowuje testy, metody testowe, dane referencyjne, weryfikacje koncepcji (*ang. proof of concept*) oraz analizy techniczne mające na celu rozwój i produktywne wykorzystanie technologii informacyjnych. Zakres zadań ITL obejmuje opracowywanie norm i rekomendacji w zakresie zarządzania, administracji, a także aspektów technicznych i fizycznych w celu zapewnienia bezpieczeństwa i prywatności informacji innych niż związane z bezpieczeństwem narodowym w federalnych systemach informacyjnych przy zachowaniu efektywności kosztowej. Niniejsza publikacja specjalna oznaczona numerem 800 zawiera sprawozdanie dotyczące badań, rekomendacji oraz działań ITL w zakresie komunikacji, bezpieczeństwa systemów informacyjnych oraz o współpracy z przemysłem, jednostkami rządowymi oraz organizacjami akademickimi.

Streszczenie

Technologie magazynowania danych są nieustannie rozwijane, podobnie jak technologie obliczeniowe oraz sieciowe. Na przestrzeni lat byliśmy świadkami ich rozwoju z tradycyjnych technologii opartych na magazynach blokowych, plikach oraz obiektach. Rozwój ten przebiegał dwutorowo. Jeden z głównych obszarów rozwoju dotyczył zwiększania pojemności nośników pamięci masowej (takich jak taśmy, dyski twarde, dyski półprzewodnikowe (*ang. ang. solid-state drives - SSD*); drugi z kolei dotyczył architektur technologii magazynowania danych – począwszy od pamięci masowej podłączanej bezpośrednio (*ang. direct-attached storage, DAS*), poprzez podłączanie zasobów pamięci masowej do sieci dostępnych za pośrednictwem różnych interfejsów i protokołów, aż po dostęp do zasobów pamięci masowej w chmurze, która zapewnia warstwę abstrakcji ponad wszystkimi technologiami pamięci masowej.

Rozwojowi architektury towarzyszy wzrost złożoności zarządzania, co w konsekwencji zwiększa prawdopodobieństwo wystąpienia błędów w konfiguracji i związanych z tym zagrożeń bezpieczeństwa.

Niniejszy dokument omawia rozwój technologii pamięci masowej, obecnych zagrożeń dla bezpieczeństwa oraz wynikających z nich ryzyk. Głównym celem tego dokumentu jest dostarczenie kompleksowego zestawu zaleceń dotyczących bezpieczeństwa, które będą odpowiedzią na występujące zagrożenia. Zalecenia obejmują zarówno obszary zarządzania bezpieczeństwem dotyczące infrastruktur informatycznych, takie jak: bezpieczeństwo fizyczne, uwierzytelnianie i autoryzacja, zarządzanie zmianami, zabezpieczenia konfiguracyjne oraz reagowanie na incydenty i usuwanie skutków awarii, jak i obszary dotyczące wyłącznie infrastruktury pamięci masowych, takie jak: na przykład ochrona danych, izolacja, zapewnianie możliwości odtworzenia danych oraz szyfrowanie).

Słowa kluczowe

sieć pamięci masowej (*ang. storage area network - SAN*), sieciowa macierz dyskowa (*ang. network attached storage - NAS*); macierz dyskowa (*ang. storage array*); usługa przechowywania plików (*ang. file storage service*); usługa przechowywania bloków (*ang. block storage service*); usługa przechowywania obiektów (*ang. object storage service*); wirtualizacja pamięci masowej (*ang. storage virtualization*); pamięć masowa definiowana programowo (*ang. software-defined storage*); hiperkonwergentna macierz dyskowa (*ang. hyper-converged storage*); ochrona danych (*ang. data protection*); magazynowanie danych w chmurze/chmurowa przestrzeń składowania/macierz dyskowa w chmurze/ chmurowa macierz dyskowa (*ang. cloud storage*); kopia zapasowa (*ang. backup*); replikacja danych (*ang. replication*).

PODSUMOWANIE

Pamięć masowa, jednostki obliczeniowe oraz urządzenia sieciowe stanowią trzy podstawowe elementy infrastruktury informatycznej. Podobnie jak technologie obliczeniowe i sieciowe, również technologie pamięci masowej rozwijały się na przestrzeni lat. Rozwój ten przebiegał dwutorowo – z czasem zwiększeniu ulegała pojemność nośników danych, zmieniały się też architektury systemów pamięci masowej. Zmiany w tym drugim obszarze umożliwiły wykorzystanie usług pamięci masowej w wielu nowych kontekstach, jednak przyczyniły się także do wzrostu złożoności samego zarządzania pamięcią masową, co przekłada się na wiele wyzwań dotyczących bezpieczeństwa.

Podobnie jak w przypadku technologii obliczeniowych i sieci, także w przypadku infrastruktury pamięci masowej mamy do czynienia z mieszanką nowoczesnych oraz przestarzałych systemów i rozwiązań. Z tego powodu niniejszy dokument zawiera omówienie technologii pamięci masowej, w tym tradycyjnych usług pamięci masowej (np. blokowej, plikowej i obiektowej pamięci masowej), a także zagadnień takich jak wirtualizacja pamięci masowej, architektury pamięci masowej projektowane z myślą o zwirtualizowanych środowiskach serwerowych oraz zasoby pamięci masowej dostępne w chmurze. Obejmuje także opisy różnych zagrożeń dotyczących magazynów danych, a także analizę ryzyka dotyczącą infrastruktur magazynowania danych i ocenę wpływu tych zagrożeń.

Podstawowym celem tego dokumentu jest przedstawienie kompleksowego zestawu zaleceń dotyczących bezpieczeństwa z punktu widzenia obecnej sytuacji dotyczącej infrastruktury pamięci masowej. Obszary bezpieczeństwa obejmują aspekty wspólne dla całej infrastruktury informatycznej, w tym: bezpieczeństwo fizyczne, uwierzytelnianie i autoryzację, zarządzanie zmianami, zabezpieczenia konfiguracyjne, reagowanie na incydenty i przywracanie działania systemów po awarii. W ramach tych obszarów uwzględniono również mechanizmy bezpieczeństwa dotyczące w szczególności technologii pamięci masowej, takich jak sieciowe macierze dyskowe (NAS) czy sieciowe pamięci masowe (SAN).

Dokument zawiera ponadto zalecenia dotyczące bezpieczeństwa dotyczące technologii pamięci masowych w następujących obszarach działania infrastruktury pamięci masowej:

- ochrona danych,
- izolacja,
- zapewnienie możliwości odzyskania danych,
- szyfrowanie.

Spis treści

1. WPROWADZENIE

Pamięci masowe, technologie obliczeniowe oraz technologie sieciowe stanowią trzy podstawowe filary każdej infrastruktury informatycznej. Infrastruktury pamięci masowej rozwijały się na przestrzeni lat, co doprowadziło do opracowania nowych rozwiązań oraz funkcji w wielu obszarach, a także przełożyło się na wzrost wydajności oraz efektywności. Rozwój ten przebiegał dwutorowo. Jednym z obszarów rozwoju był obszar nośników pamięci, w którym pojawiły się dyski półprzewodnikowe (*SSD*) o dużej pojemności, wyposażone w funkcje zwiększające efektywność przechowywania danych takie jak na przykład deduplikacja, kompresja i inne, które dorównują i wyprzedzają tradycyjne dyski twarde (*ang. Hard Disk Drives - HDD*). Drugi z nich dotyczył architektury systemów pamięci masowej, który opiera się na koncepcjach takich jak wirtualizacja pamięci masowej. Rozwój na tym drugim froncie przyczynił się również do wzrostu złożoności zarządzania, przyczyniając się do utrudnienia możliwości zapewnienia bezpieczeństwa danych.

Nawet pobieżna analiza historii architektury systemów pamięci masowej pokazuje, że najwcześniejszą formą infrastruktury pamięci masowej jest pamięć masowa podłączona bezpośrednio, w której nośnik lub urządzenie pamięci masowej (np. taśma czy dysk twardy) są podłączane bezpośrednio do serwera bez pośrednictwa sieci. Technologie pamięci masowej ewoluowały następnie w kierunku inteligentnego łączenia wszystkich zasobów pamięci masowej oraz umieszczania ich w sieci, gdzie dostęp do nich ma wiele hostów oraz serwerów za pośrednictwem protokołów sieciowych. Ten rodzaj infrastruktury pamięci masowej jest jedynym sposobem zapewniającym dostęp do danych w systemach rozproszonych, w których komponenty aplikacji, które muszą korzystać z tych samych danych, mogą znajdować się w różnych węzłach sieci. Na tym etapie rozwoju infrastruktura pamięci masowej mogła przybrać dwie formy w zależności od rodzaju wykorzystywanego protokołu sieciowego.
W jednym z tych przypadków zasób pamięci masowej stanowi kolejny węzeł w sieci i wykorzystuje powszechnie stosowane technologie sieciowe, takie jak lokalne sieci komputerowe (*ang. local area network - LAN*) czy rozległe sieci informatyczne (*ang. - wide area network - WAN*). W drugim zaś istnieje sieć przeznaczona wyłącznie do komunikacji ze wszystkimi zasobami pamięci masowej. Za przykład tego pierwszego przypadku

może posłużyć sieciowa macierz dyskowa (NAS), które zapewnia dostęp do plików różnorodnym klientom działającym w sieci za pośrednictwem wysokopoziomowych protokołów, takich jak protokół zdalnego udostępniania systemu plików (*ang. Network File System - NFS*) czy protokół służący udostępnianiu zasobów komputerowych (*ang. Server Message Block - SMB*), znany również jako CIFS (*ang. Common Internet File System*). Za przykład drugiego przypadku może posłużyć sieć pamięć masowej (SAN) oparta na wyspecjalizowanych sieciach wysokich prędkości i rozwiązania takie jak na przykład Fibre-Channel[2], zapewniającą dostęp do pamięci masowej na poziomie bloku. Inna implementacja SAN wykorzystuje technikę umożliwiającą wykonywanie operacji wejścia-wyjścia na dysku twardym odległej maszyny (*ang. Internet Small Computer Systems Interface -iSCSI)* za pomocą protokołu TCP/IP (*ang. Transmission Control Protocol/Internet Protocol*) za pośrednictwem współdzielonej infrastruktury LAN/WAN.

Nowymi wariantami tradycyjnej infrastruktury pamięci masowych wykorzystywanych w organizacjach są infrastruktury konwergentne i hiperkonwergentne (*ang. Hyper-Converged Infrastructure - HCI*). Systemy konwergentne charakteryzują się wstępnie skonfigurowanym pakietem oprogramowania oraz rozwiązaniami sprzętowymi w jednej obudowie, co pozwala na uproszczenie procesu zarządzania. W przypadku infrastruktury konwergentnej komponenty obliczeniowe, pamięci masowe i sieciowe są odrębne i mogą być rozdzielone. Podobnie jak systemy konwergentne, także hiperkonwergentne macierze dyskowe łączą pamięć masową, elementy obliczeniowe oraz sieciowe w ramach jednego urządzenia lub obudowy, są także wyposażone w warstwę abstrakcji pozwalającą na zarządzanie każdym z tych trzech elementów. W przeciwieństwie do systemów konwergentnych, systemy hiperkonwergentne nie wymagają wydzielonej pamięci masowej. W większości przypadków zawierają konsolę programową lub narzędzie do zarządzania wszystkimi trzema elementami. Obejmują także hipernadzorcę, czyli oprogramowanie umożliwiające tworzenie i uruchamianie maszyn wirtualnych, pamięci masowych zdefiniowanych programowo, a także

[2] Standard magistrali szeregowej definiujący wielowarstwową architekturę, która służy do przesyłania danych przez sieć. Fibre Channel definiuje atrybuty warstwy fizycznej, transportowej, a także obsługę protokołów wyższych warstw takich jak TCP/IP, SCSI-3 i innych. Jest stosowany w sieciach SAN. Niezależnie od nazwy, Fibre Channel pracuje zarówno na połączeniach galwanicznych (prawie zawsze miedzianych), jak i światłowodach.

zwirtualizowanych urządzeń sieciowych, które mogą być uruchamiane na standardowych urządzeniach. Zintegrowane komponenty pamięci masowej, obliczeniowe i sieciowe zostały zaprojektowane w taki sposób, by mogły być sterowane jako pojedynczy system we wszystkich instancjach infrastruktury. Ponadto każda jednostka sprzętowa może być skonfigurowana jako węzeł klastra w celu utworzenia puli współdzielonych zasobów pamięci masowej, zapewniając w ten sposób korzyści wynikające ze scentralizowanej infrastruktury pamięci masowej.

Następna fala rozwoju pamięci masowych wiązała się z pojawieniem się na rynku usług magazynowania danych w chmurze, czyli wysoce skalowalnego oraz odpornego zestawu usług pamięci masowej, które są definiowane programowo. Usługi magazynowania danych w chmurze zazwyczaj obejmują:

- Usługi blokowej pamięci masowej, które eksponują zdefiniowane programowo urządzenia blokowe, które mogą być udostępniane wirtualnym hostom działającym w chmurze.
- Usługi przechowywania obiektów, które mogą być mapowane do hostów, aplikacji, a nawet innych usług w chmurze i umożliwiają adresowanie dyskretnych, nieuporządkowanych elementów danych według identyfikatorów lub metadanych.
- Skalowalne współdzielone systemy plików, które mogą pozwolić skalowalnemu zestawowi hostów na dostęp do tego samego systemu plików z dużą prędkością.
- Różnorodne usługi replikacji, buforowania, archiwizacji, tworzenia lustrzanych kopii danych oraz kopii danych z określonego momentu w czasie, dostępne dla wszystkich powyższych rozwiązań.

Oferowane są również dodatkowe usługi w chmurze, takie jak: zarządzane usługi bazodanowe, jeziora danych[3] (*ang. data lakes*), pamięci podręczne i kolejki komunikatów. Każda z tych technologii pozwala na przechowywanie danych stanowych i tymczasowych. Opinie ekspertów na temat tego, czy należy je klasyfikować jako usługi magazynowania danych, są jednak podzielone.

[3] Jezioro danych przechowuje ustrukturyzowane i nieustrukturyzowane dane w dowolnej skali.

Innym rodzajem infrastruktury pamięci masowej jest infrastruktura zawierająca interfejsy wspierające realizację potrzeb związanych z magazynowaniem danych aplikacji stanowych, które są projektowane z wykorzystaniem architektury opartej na mikrousługach i wdrażane z wykorzystaniem kontenerów danych zorganizowanych w klastry dzięki platformom orkiestracji kontenerów. Platformy te są wyposażone w standardowy mechanizm umożliwiający połączenie z pamięcią masową –interfejs kontenerowej pamięci masowej (*ang. Container Storage Interface - CSI*), który łączy skonfigurowane przez nie klastry z różnymi rodzajami pamięci trwałej.

1.1 Zakres

Niniejszy dokument zawiera zalecenia dotyczące bezpieczeństwa następujących technologii pamięci masowej:

- Tradycyjne technologie pamięci masowej wykorzystywane w organizacjach, sklasyfikowane na podstawie rodzaju interfejsu usług pamięci masowej (np. blokowe, plikowe i obiektowe).
- Sieć pamięci masowej (np. NFS, SAN).
- Systemy pamięci masowej, które zostały wyposażone w warstwę abstrakcji programowej (np. pamięć masowa definiowana programowo, wirtualizacja pamięci masowej).
- Systemy pamięci masowej opracowane wyłącznie z myślą o zwirtualizowanych środowiskach serwerowych (np. pamięć masowa dla maszyn wirtualnych i kontenerów, systemy konwergentnej i hiperkonwergentnej macierzy dyskowej).
- Systemy pamięci masowej obejmujące interfejsy programistyczne aplikacji (*ang. Application Programming Interfaces - API*) pozwalające na dostęp do usług chmurowych.

Zalecenia dotyczące bezpieczeństwa obejmują następujące obszary:

- Działania dotyczące wyłącznie infrastruktury pamięci masowej, takie jak ochrona danych i zapewnienie odtworzenia danych.
- Działania dotyczące innych rodzajów infrastruktur (np. obliczeniowych i sieciowych), w przypadku których konkretne zadania mają zastosowanie do

infrastruktury pamięci masowej, takie jak: bezpieczeństwo fizyczne, uwierzytelnianie i autoryzacja, prowadzenie dzienników, konfiguracja sieci, izolacja, zabezpieczenia konfiguracyjne, zarządzanie zmianami i szkolenia.

Infrastruktura pamięci masowej dla komputerów klasy mainframe nie została uwzględniona w zakresie niniejszego dokumentu.

1.2 Odbiorcy docelowi

Docelowa grupa odbiorców zaleceń dotyczących bezpieczeństwa omawianych w niniejszym dokumencie obejmuje:

- osoby zajmujące wyższe stanowiska kierownicze do spraw bezpieczeństwa (*ang. Chief Security Officer - CSO*) oraz do spraw technologii (*ang. Chief Technology Officer - CTO*) w działach IT podmiotów publicznych i prywatnych oraz dostawców usług chmurowych, którzy chcą opracować zasady obowiązujące w organizacji lub centrum danych dotyczące całej infrastruktury, w tym infrastruktury pamięci masowej.
- administratorów systemów lub pamięci masowej, którzy muszą opracować konfiguracje systemów pamięci masowej, systemów konwergentnych lub zwirtualizowanych.

1.3 Związek z innymi dokumentami zawierającymi rekomendacje NIST

Niniejsze rekomendacje koncentrują się na szczególnym rodzaju infrastruktury, która zapewnia dostęp do wszystkich zasobów danych i usług, podobnie jak infrastruktura obliczeniowa zapewnia dostęp do usług obliczeniowych, a infrastruktura sieciowa zapewnia dostęp do usług komunikacyjnych. Z tego powodu wybrane informacje oraz zalecenia dotyczące bezpieczeństwa związane z elementami obliczeniowymi oraz sieciowymi mają także zastosowanie w przypadku infrastruktury pamięci masowej omawianej w niniejszym dokumencie. Takie wspólne zalecenia zostały zaprezentowane w niniejszym dokumencie i opatrzone krótkim opisem lub uwzględnione poprzez umieszczenie stosownego odnośnika.

Odpowiednie dokumenty NIST[4] zawierające zalecenia obejmujące wszystkie infrastruktury (obliczeniową, sieciową i pamięci masowej) to:

- SP 800-52 Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (2019)[5].
- SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (2020)[6].
- SP 800-57 Part 1, *Recommendation for Key Management: Part 1* (2020).
- 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing* (2020).
- 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management* (2020).
- SP 800-88 Rev. 1, *Guidelines for Media Sanitization* (2014).
- SP 800-125A, Revision 1, *Security Recommendations for Server-based Hypervisor Platforms* (2018).
- SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM)* Protection (2016).

1.4 Organizacja niniejszego dokumentu

Treść niniejszego dokumentu została zorganizowana w następujący sposób:

- Rozdział 2 zawiera omówienie tradycyjnych technologii pamięci masowej dla organizacji, technologii dostępu do pamięci masowej zapewniających poziom abstrakcji, architektur pamięci masowej dostosowanych do zwirtualizowanych środowisk serwerowych oraz interfejsów programowych aplikacji (API) umożliwiających dostęp do zasobów macierzy dyskowej w chmurze. W tym rozdziale przedstawiono również przegląd pewnych ogólnych zasad administrowania pamięcią masową.

[4] Publikacje NIST zostały podane w celach uzupełniających dla osób zainteresowanych.

[5] Patrz: publikacja NSC 800-52, *Wskazówki dotyczące wyboru, konfigurowania i wykorzystania implementacji TLS (Transport Layer Security)*, wer. 1 – polskie opracowanie dokumentu NIST SP 800-52.

[6] Patrz: publikacja NSC 800-53 wer. 2 – polskie opracowanie dokumentu NIST SP 800-53 rev. 5.

- Rozdział 3 zawiera omówienie zagrożeń związanych z infrastrukturą pamięci masowej oraz powiązanych z nimi ryzyk. Oprócz zagrożeń ogólnych, takich jak na przykład eskalacja uprawnień dostępu, kradzież lub kompromitacja danych uwierzytelniających, złamanie kluczy szyfrujących, złośliwe oprogramowanie (*ang. malware*) czy ataki typu ransomware[7], w rozdziale omówione zostały także zagrożenia dotyczące wyłącznie pamięci masowej takie jak nieautoryzowane zmiany konfiguracji pamięci masowej, kradzież nośników i niezabezpieczone obrazy pamięci masowej. Wynikające z tego zagrożenia dla infrastruktury pamięci masowej, w tym wyciek danych lub zagrożenie bezpieczeństwa danych, wprowadzenie nieautoryzowanych zmian lub dodanie nowych danych, uszkodzenie danych, zaszyfrowanie danych, manipulacja plikami dziennika związanymi z pamięciami masowymi, a także kompromitacja kopii zapasowych i oprogramowania układowego / sprzętowego (*ang. firmware*), zostały przeanalizowane pod kątem możliwości wystąpienia tych zagrożeń oraz ich potencjalnych skutków.
- Rozdział 4 stanowi zasadniczy materiał publikacji. Zawiera on szczegółowe zalecenia dotyczące bezpieczeństwa związane ze wszystkimi aspektami zarządzania infrastrukturą pamięci masowej.
- Załącznik A zawiera listę referencyjnych publikacji.
- Załącznik B zawiera listę akronimów używanych w niniejszym dokumencie.

[7] Rodzaj szkodliwego oprogramowania, powodującego utratę dostępności informacji, za przywrócenie której atakujący żąda od zaatakowanego okupu.

2. TECHNOLOGIE MAGAZYNOWANIA DANYCH: INFORMACJE OGÓLNE

Technologia magazynowania danych to ogólne pojęcie obejmujące zarówno urządzenia, jak i poszczególne obiekty (np. elementy pamięci masowej, macierze pamięci masowej, przełączniki sieciowe pamięci masowej lub nośniki pamięci) oraz procesy (w tym na przykład protokoły i interfejsy) stosowane do przechowywania danych komputerowych w postaci nieulotnej w postaci nieulotnej (trwałej). Z tego powodu technologię tę można rozpatrywać z punktu widzenia dwóch następujących taksonomii:

- **Ze względu na lokalizację zasobu pamięci masowej:** Urządzenie pamięci masowej jest podłączone bezpośrednio do klienta pamięci masowej lub komputera hosta, nazywamy je wówczas pamięcią masową podłączoną bezpośrednio (*ang. direct-attached storage - DAS*), bądź host i urządzenie pamięci masowej są połączone za pośrednictwem sieci – mówimy wtedy o sieciowej pamięci masowej.
- **Ze względu na typ pamięci masowej (typ dostępu):** Klasyfikacja ta opiera się na interfejsie udostępnianym przez system pamięci masowej, który jest wykorzystywany przez oprogramowanie klienckie. Przykłady obejmują pamięć masową opartą na blokach (usługa przechowywania bloków), pamięć masową opartą na plikach (usługa przechowywania plików) i pamięć masową opartą na obiektach (usługa przechowywania obiektów).

W przypadku pamięci masowej podłączanej bezpośrednio (DAS), urządzenie pamięci masowej może być integralną częścią komputera (gdy jest podłączone do magistrali) lub być podłączone jako zewnętrzna pamięć masowa (gdy jest podłączone do portu komputera, na przykład portu USB).

Sieciowe przestrzenie magazynowe są szeroko klasyfikowane na podstawie rodzaju dostępu; są to między innymi sieciowe macierze dyskowe (NAS), które zapewniają możliwość uzyskiwania dostępu do plików za pośrednictwem sieci, a także sieciowe pamięci masowe (SAN), których protokoły zapewniają dostęp do bloków. Co więcej, w przypadku rozwiązań SAN cały stos sieciowy może składać się z protokołów

wykorzystywanych wyłącznie do celów związanych z usługami pamięci masowej, takich jak Fibre-Channel, może jednak także wykorzystywać protokoły opracowane z myślą o pamięciach masowych działających za pośrednictwem lub enkapsulowanych w ramach typowych protokołów sieciowych. Za przykład może posłużyć protokół iSCSI z założenia działający za pośrednictwem protokołu TCP/IP, a także Fibre-Channel over IP (*FCIP*), Fibre-Channel over Ethernet (*FCoE*) oraz magazynu blokowego w chmurze (*ang. Cloud Block Storage*). W sieciowych pamięciach masowych zdalne urządzenia pamięci masowej są prezentowane tak, jakby były lokalnie podłączone do systemu hosta, na którym działa oprogramowanie klienckie.

Taksonomia oparta na typach pamięci masowej, dostępu lub usług obejmuje typy lub usługi blokowe, plikowe i obiektowe. Z racji tego, że wybór usługi pamięci masowej jest podyktowany konkretnym przypadkiem użycia systemu informacyjnego oraz wymogami, takimi jak: objętość danych, wymagana kontrola nad danymi, wymagana wydajność czy rodzaj reprezentacji danych, niniejszy dokument zawiera omówienie technologii pamięci masowej z punktu widzenia usług, czyli rodzajów pamięci masowej oraz dostępu do niej.

Wśród nośników danych funkcjonuje obecnie wiele technologii, a ich zakres ulega nieustannym zmianom. Do powszechnie stosowanych technologii należą:

- nośniki magnetyczne (np. tradycyjne dyski twarde, taśmy),
- nośniki optyczne (np. napędy optyczne takie jak CD-R, DVD-R, Blu-ray) oraz magnetooptyczne,
- nośniki półprzewodnikowe (np. pamięci flash, urządzenia pamięci trwałej).

Eksperymentalne i mniej powszechne technologie obejmują pamięć molekularną (np. opartą na polimerach), holograficzną (np. opartą na kryształach), pamięć zbliżoną do DNA i inne rozwiązania.

2.1 Usługa przechowywania bloków

Usługi blokowej pamięci masowej obejmują interfejs, który pozwala na odczyt oraz zapis bloków danych o stałej wielkości, zwykle oferując wysoką przepustowość i niskie opóźnienia w dostępie do urządzeń pamięci masowej na poziomie bloku poprzez sieciową pamięć masową. Każde urządzenie pamięci masowej w systemie pamięci masowej opartym na blokach może być sterowane jako pojedynczy dysk twardy, a poszczególne bloki są sterowane przez system operacyjny hosta.

2.1.1 Sieć pamięci masowej (SAN)

Systemy oparte na sieciowej pamięci masowej (SAN) zwykle składają się z następujących elementów: (a) komputerów hostów (klientów); (b) topologii, która obejmuje rozmieszczenie przełączników; a także (c) urządzeń/macierzy pamięci masowej. Wszystkie trzy elementy są połączone za pomocą różnych stosów sieciowych. Ze względu na to, że sieć pamięci masowej stanowi wyspecjalizowaną, szybką sieć zapewniającą dostęp do pamięci masowych na poziomie bloków, konieczne jest bliższe przyjrzenie się jej wariantom [1][8]. Warianty te są wynikiem stosowania różnych rodzajów stosów sieciowych z różnymi protokołami w określonych warstwach stosu. Istnieje kilka protokołów SAN. Niektóre z powszechnie stosowanych to:

a. Fibre-Channel SAN (FC SAN) [2],

b. IP SAN,

c. Fibre-Channel over Ethernet (FCoE),

d. protokoły NVMe-oF (Non Volatile Memory Express over Fabrics).

FC SAN to stos sieciowy wykorzystujący protokół Fibre-Channel, który składa się z pięciu warstw (od FC0 do FC4, co odróżnia go od siedmiowarstwowego modelu odniesienia łączenia systemów otwartych (OSI)). Logiczny zasób pamięci masowej adresowany w ramach sieciowej pamięci masowej Fibre-Channel jest określany numerem jednostki logicznej (*ang. Logical Unit Number - LUN*).

[8] W nawiasie kwadratowym [ ] znajduje się numer publikacji anglojęzycznej wyszczególnionej w rozdziale Referencje

IP SAN jest stosem sieciowym, który wykorzystuje protokół IP w warstwie sieciowej. Przykładem wykorzystania IP SAN jest protokół iSCSI [3].

W przypadku Fibre-Channel over Ethernet (FCoE)ramka Fibre-Channel jest enkapsulowana w pakietach Ethernet.

Urządzenie blokowe w sieciowych pamięciach masowych FC SAN lub IP SAN są także często określane mianem LUN, choć z technicznego punktu widzenia takie użycie tego terminu jest nieprawidłowe. Historyczne korzenie terminu wywodzą się z numerów jednostek logicznych wykorzystywanych w protokole SCSI, które trafiły bezpośrednio do sieciowych pamięci masowych.

Zanim przyjrzymy się protokołom NVMe-oF, konieczne jest przypatrzenie się bliżej protokołowi NVMe. NVMe to standardowy interfejs sterownika hosta w systemach wykorzystujących dyski SSD podłączane do magistrali PCI Express (*ang. Peripheral Component Interconnect Express - PCIe*). Specyfikacja NVMe-oF określa interfejs protokołu i powiązane rozszerzenia, które umożliwiają przesyłanie poleceń NVMe przez sieć. Dzięki temu protokół NVMe oF umożliwia wykorzystywanie pamięci NVMe nie tylko na lokalnych urządzeniach, lecz także na zdalnych hostach, umożliwiając budowę skalowalnych systemów pamięci masowej opartej na dyskach NVMe.

Protokoły NVMe-oF obejmują rodzinę protokołów zdalnego bezpośredniego dostępu do pamięci (*ang. Remote Direct Memory Access - RDMA*), a także protokoły Fibre-Channel i TCP. Protokół RDMA [4] umożliwia bezpośredni przepływ danych zawartych w pamięci aplikacji między serwerami bez udziału procesora, dzięki czemu lokalna aplikacja może odczytywać lub zapisywać dane w pamięci zdalnego komputera przy minimalnym zapotrzebowaniu na przepustowość magistrali pamięci i czas procesora, zachowując semantykę ochrony pamięci. Infiniband [5] jest jednym ze standardowych interfejsów wykorzystywanych w branży, który pozwala na wykorzystanie protokołu RDMA w systemach obliczeniowych dużej skali.

Topologia węzłów wraz z różnymi elementami sprzętowymi w systemie SAN nazywana jest siecią szkieletową SAN. Dla przykładu, sieć szkieletowa Fibre-Channel SAN składa się z serwera nazw (*ang. Name Server - NS*), który rejestruje i utrzymuje komunikację z przełącznikami oraz urządzeniami końcowymi, w tym wypadku z kontrolerem

pamięci masowej (*ang. Host Bus Adapter - HBA*). W przypadku systemów FC SAN istnieją dwa rodzaje topologii – topologia punkt-punkt, w której dwa urządzenia są połączone bezpośrednio, a także topologia „switched fabric" – nazwa nie ma polskiego odpowiednika. W tej topologii wykorzystywany jest zestaw przełączników sieciowych pełniących funkcję jednego dużego przełącznika logicznego, który łączy hosta z zasobami pamięci masowej. Zalecenia dotyczące bezpieczeństwa zawarte w tym dokumencie dotyczą tylko tej topologii ze względu na jej powszechne zastosowanie w praktyce.

2.1.2 Inne formy sieciowej pamięci blokowej

Inne formy pamięci blokowej, które mogą być łączone do hostów przy pomocy sieci IP to między innymi:

- Usługi hiperkonwergentnej macierzy dyskowej. Więcej informacji na ich temat znajduje się w podrozdziale 2.9 „Konwergentne i hiperkonwergentne macierze dyskowe (sieciowe pamięci masowe SAN oparte na serwerach)" w dalszej części niniejszego dokumentu.
- Blokowe pamięci masowe w chmurze, oferowane we wszystkich środowiskach chmurowych (więcej informacji na ich temat znajduje się w podrozdziale 2.10. Przestrzeń składowania danych w chmurze w dalszej części niniejszego dokumentu).

2.2 Usługa przechowywania plików

Ten typ usługi prezentuje zasoby pamięci masowej w postaci modelu systemu plików z plikami zawartymi w katalogach w ramach woluminów. W tle pliki mogą być replikowane poprzez tworzenie nadmiarowych kopii, mogą także być szyfrowane. Różne rodzaje tego typu usług oraz powiązane z nimi protokoły to:

- Sieciowe macierze dyskowe (NAS) wykorzystujące protokół NFS [6] – moduł będący częścią systemu wdrożenia protokołu, zwany sterownikiem klienta NFS, montuje woluminy istotne dla klienta w jego środowisku. Wolumin może być współdzielony przez wielu klientów. Pliki lub foldery mogą być również udostępniane z odpowiedniego urządzenia (zwykle określanego mianem „urządzenia NAS" lub „macierzy NAS") bądź z dowolnego hosta, na którym działa usługa serwera NFS.

- Sieciowa macierz dyskowa połączona przy pomocy protokołu SMB – serwer plików podłączony do lokalnej sieci komputerowej, podobnie jak w przypadku serwerów wykorzystujących protokół NFS; wykorzystuje standardowy protokół SMB, który znajduje się w stosie sieciowym systemów operacyjnych instalowanych na komputerach osobistych oraz stacjach roboczych. Na protokole SMB opiera się usługa udostępniania plików CIFS.
- Sieciowa macierz dyskowa z obsługą wielu protokołów – na rynku istnieją produkty obsługujące wiele protokołów obsługi folderów oraz systemów plików. Takie urządzenia pozwalają na jednoczesne wykorzystanie na przykład protokołów NFS i CIFS. Każdy z tych protokołów może wykorzystywać nieco inne struktury kontroli dostępu, na przykład listy kontroli dostępu (*ang. Access Control List - ACL*) oraz specyfikacje uprawnień, a niektóre konflikty praw kontroli dostępu mogą wymagać rozwiązania w czasie żądań dostępu.
- Sieciowa macierz dyskowa wykorzystująca równoległy protokół NFS (pNFS) – klaster serwerów pamięci masowej (wykorzystywany zamiast pojedynczego serwera NFS), który rozdziela dane i metadane, zapewniając jednocześnie dynamiczne, rozproszone połączenia dla klientów w całym zbiorze hostów klastra. Protokół pNFS jest realizowany poprzez (a) partycjonowanie przestrzeni nazw systemu plików i przypisywanie zasobów pamięci masowej (tj. plików) należących do różnych przestrzeni nazw do różnych serwerów (zwane klastrowaniem symetrycznym) lub (b) rozdzielanie funkcjonalności pomiędzy serwery (zwane klastrowaniem asymetrycznym) poprzez przekazywanie przez główny serwer plików informacji dotyczących lokalizacji drugorzędnych serwerów pamięci masowej, zawartych w nich danych oraz metod dostępu do nich. Usługa ta jest wykorzystywana w celu realizacji wielkoskalowych repozytoriów treści (ze względu na skalowalność), magazynów mediów oraz środowisk deweloperskich [7].

2.3 Usługa przechowywania obiektów

Usługa przechowywania obiektów prezentuje dane w postaci wydzielonych pojemników lub kontenerów o elastycznej wielkości przechowujących obiekty. W przeciwieństwie do bloków o stałej wielkości oferowanych przez usługi blokowej pamięci masowej lub katalogów i podkatalogów występujących w tradycyjnych systemach plików oraz

sieciowych macierzach dyskowych, każdy obiekt może mieć dowolny rozmiar i ma przypisany wyjątkowy identyfikator (identyfikator obiektu ID, nazywany także ID obiektu - OID), który jest gromadzony wraz z innymi identyfikatorami w ramach indeksu wykorzystywanego w celu uzyskania dostępu do danych w każdym obiekcie. Ponadto do obiektu można dołączyć dynamiczne metadane, które ułatwiają elastyczne wyszukiwanie i adresowanie.

Technicznie rzecz biorąc, obiekt może mieć prawie dowolny rozmiar i może zawierać wiele plików lub ich fragmenty. Powszechnym zastosowaniem magazynowania obiektów jest archiwizacja nieuporządkowanych danych, zwłaszcza dużych plików danych takich jak treści cyfrowe. Może być jednak stosowana także do przechowywania dynamicznych danych, takich jak te przechowywane przez dostawców aplikacji internetowych.

Podstawową zaletą usługi przechowywania obiektów jest jej skalowalność – przeszukiwanie indeksu jest szybsze i wydajniejsze niż przeszukiwanie tradycyjnych systemów plików. Ze względu na to, że do wyszukiwania danych wymagany jest wyłącznie identyfikator obiektu oraz informacja dotycząca lokalizacji samego obiektu, wyszukiwania są w zasadzie procesem dwuetapowym, w przeciwieństwie do wielu kroków wymaganych do przejścia drzewa katalogów, którym charakteryzują się tradycyjne systemy plików. Zastosowanie takiego rozwiązania bezpośrednio przekłada się na ograniczenie konieczności obsługi metadanych przez system pamięci masowej, co oznacza szybszy dostęp do plików, zwłaszcza gdy system rozrasta się do bardzo dużych rozmiarów.

2.4 Usługa CAS (*Content-Addressable Storage*)

Pamięć masowa adresowana treścią (*ang. Content-Addressable Storage – CAS*) jest wyspecjalizowaną formą magazynowania obiektów, przeznaczoną do przechowywania skrótów treści dokumentów. Umożliwia użytkownikom dostęp do magazynowanych obiektów bez konieczności znajomości lokalizacji rzeczywistych danych lub liczby kopii.

Udostępnia użytkownikom skrót wygenerowany przez kryptograficzną funkcję skrótu (np. SHA-256), który jest identyfikatorem dokumentu, do którego się odwołuje i jest wykorzystywany do pobierania tego dokumentu.

Usługa CAS jest wykorzystywana do magazynowania i wyszukiwania dokumentów charakteryzujących się wymogami retencji w krótkiej i średniej perspektywie czasowej, w związku z czym nie jest stosowana powszechnie.

2.5 Usługi dostępu do danych wyższego rzędu

Istnieją usługi dostępu do danych, które dostarczają dane na wyższym poziomie abstrakcji niż podstawowe typy pamięci masowej (tj. pliki, bloki lub obiekty). Dostęp do tych usług jest możliwy tylko za pośrednictwem klientów opracowanych z myślą o dostępie do danych na tym samym poziomie abstrakcji (np. klientów baz danych SQL). Usługi te są dostępne zarówno w centrach danych, jak i w chmurach obliczeniowych. Poniżej przedstawiono niektóre z tych usług:

- usługi bazodanowe NoSQL,
- usługi bazodanowe SQL,
- usługi przechowywania kolejek komunikatów.

Usługi bazodanowe NoSQL umożliwiają przechowywanie i pobieranie danych niestandardowych dla baz opartych o SQL, takich jak: obrazy, filmy, dokumenty i duże obiekty binarne. Nieuporządkowane dane charakteryzują się wyższymi strukturami logicznymi i reprezentacjami niż podstawowe typy pamięci masowej w celu ułatwienia szybszego przechowywania i wyszukiwania. Należą do nich bazy danych klucz-wartość, bazy danych multimodalnych, bazy danych oparte na grafach oraz inne podtypy.

Usługi bazodanowe SQL umożliwiają przechowywanie i pobieranie uporządkowanych danych, zwykle w postaci tabel (zwanych również tabelami relacyjnymi). Dostęp ten jest możliwy dzięki znormalizowanemu interaktywnemu językowi programowania SQL, który opisuje norma ISO/IEC 9075:2016, *Database languages – SQL*. Współczesne bazy danych SQL mogą przechowywać dane nie tylko dzięki relacyjnym tabelom i widokom, lecz także innym strukturom takim jak: języki XML (eXtensible Markup Language), JavaScript Object Notation (JSON), a nawet dużym obiektom binarnym (BLOB).

Usługi przechowywania kolejek komunikatów stanowią wyspecjalizowane usługi pozwalające na przechowywanie i pobieranie danych z infrastruktury kolejek komunikatów. Infrastruktury te są wykorzystywane przez aplikacje rozproszone, których komponenty komunikują się asynchronicznie poprzez subskrypcję systemu

kolejkowania komunikatów. Oprócz zapewnienia dostępu do trwałych danych, usługa ta ułatwia również specjalistyczne operacje, takie jak integracja z przetwarzaniem strumieniowym, gdzie zdarzenia związane z przechowywaniem i pobieraniem wielu wiadomości przez komponenty systemu rozproszonego mogą być analizowane w celu wykrywania wzorców.

2.6 Pamięć masowa definiowana programowo

Pamięć masowa definiowana programowo (*ang. Software-defined storage - SDS*) obejmuje pamięci masowe wzbogacone o obsługę danych[9], które mogą być wykorzystywane w celu spełnienia wymagań określonych poprzez interfejs zarządzania usługami [8].

Różne rodzaje SDS można znaleźć w prywatnych i publicznych środowiskach chmurowych, infrastrukturach hiperkonwergentnych i różnych rozwiązaniach programowych. To architektura pamięci masowej, która oddziela sprzęt komputerowy wykorzystywany w celu przechowywania danych od oprogramowania, które zarządza infrastrukturą pamięci masowej i automatyzuje jej konfigurację. Innymi słowy, możliwości i usługi pamięci masowej są oddzielone od urządzeń realizujących usługi pamięci masowej. Do zalet takiej separacji należą:

- Elastyczność wykorzystania różnorodnego sprzętu do magazynowania danych bez problemów związanych z interoperacyjnością.
- Umożliwienie korzystania z funkcji takich jak deduplikacja, replikacja, migawki i alokowanie elastyczne (*ang. thin provisioning – TP*)[10] przy użyciu standardowych serwerów; choć należy pamiętać, że takie funkcje nie są wyjątkowe dla SDS.
- Automatyczne i wydajne przydzielanie połączonych zasobów pamięci masowej (*ang. pooled storage*) w celu dopasowania do indywidualnych potrzeb i zastosowań.
- Szybkość wdrożenia rozwiązania.

[9] Funkcjonalności typu replikacja, thin provisioning, snapshot czy backup.

[10] Polega na alokacji przestrzeni na żądanie, co oznacza, że volumen zajmuje małą ilość miejsca i rozrasta się, kiedy na dysku zapisywane jest więcej danych. Często nazywane jest przydzielaniem pojemności w locie lub alokacją nadmiarową.

Od oprogramowania zarządzającego sprzętowymi zasobami pamięci masowej w systemie pamięci masowej definiowanej programowo oczekuje się następujących możliwości oraz usług:

- Oddzielenie polityki zarządzania pamięcią masową od rozwiązań sprzętowych.
- Obsługa zróżnicowanych środowisk pamięci masowej.
- Umożliwienie dodawania nowych zasobów pamięci masowej we wszystkich platformach, nie tylko w poszczególnych macierzach.
- Zapewnianie, że oprogramowanie zna i wykorzystuje możliwości urządzeń magazynujących dane.

2.7 Wirtualizacja pamięci masowej

Wirtualizacja pamięci masowej to działanie polegające na abstrakcji, ukryciu lub izolacji wbudowanej funkcji (pod)systemu pamięci masowej lub usługi w celu oddzielenia ich od aplikacji, serwerów obliczeniowych lub ogólnych zasobów sieciowych, aby umożliwić zarządzanie pamięcią masową lub danymi niezależnie od aplikacji i sieci [9]. Wirtualizacja pamięci masowej umożliwia łączenie pojemności wielu urządzeń lub macierzy pamięci masowej, dzięki czemu można nimi zarządzać jako jedną całością. Wirtualizacja pozwala na agregowanie i zarządzanie zasobami pamięci masowej zawartymi w wielu fizycznych urządzeniach pamięci masowej w dużych sieciach (np. SAN) lub centrach danych. Wirtualizacja pozwala również na rozdzielenie zasobu pamięci masowej lub puli zasobów, na wiele wirtualnych reprezentacji tych zasobów. Zastosowanie tej techniki zapewnia możliwość elastycznej zmiany relacji fizycznych i logicznych w czasie oraz maskowanie szczegółów dotyczących fizycznych zasobów pamięci masowej [10].

Poniżej przedstawiono kilka scenariuszy, w których wykorzystywana jest wirtualizacja pamięci masowej:

- Fragmenty wielu fizycznych dysków mogą być prezentowane jako oddzielnego lustrzanego woluminu logicznego dzięki zastosowaniu menedżera woluminów logicznych zainstalowanego na hoście lub macierzy pamięci masowej. Co więcej, zastosowanie takiego rozwiązania umożliwia wymianę fizycznych dysków w woluminie lustrzanym, a zapis może przebiegać równolegle na obu woluminach.

- W przypadku wykrycia zmian we wzorcach dostępu możliwa jest wymiana dysków, na których przechowywane są dane, na przykład w celu przechowywania często używanych informacji na najwydajniejszych dyskach, co pozwala na zapewnienie funkcji automatycznego tworzenia warstw i kategorii danych.
- Migracje danych na dużą skalę, które muszą być wykonywane w sposób niewpływający na działanie hostów i aplikacji.

Korzyści z wirtualizacji pamięci masowej to: skalowalność, wydajność, redundancja i zwiększone wykorzystanie zasobów pamięci masowej.

2.8 Pamięć masowa dla zwirtualizowanych serwerów i kontenerów

Serwer zwirtualizowany to taki, w którym na pojedynczym serwerze fizycznym działa wiele stosów obliczeniowych (każdy składający się z systemu operacyjnego, pamięci masowej, sieci i aplikacji) nazywanych maszynami wirtualnymi (*ang. virtual machine - VM*) obsługiwanych dzięki oprogramowaniu nazywanym hipernadzorcą lub hiperwizorem (*ang. hypervisor*). Infrastruktura pamięci masowej zaprojektowana z myślą o współpracy z serwerami zwirtualizowanymi jest często określana skrótem VAS od angielskiej nazwy „virtualization-aware storage" lub „VM-aware storage" [11]. W większości środowisk infrastruktura ta jest zarządzana razem z maszynami wirtualnymi przez hipernadzorcę, nie zaś jako oddzielnie zarządzane urządzenia blokowe.

Kluczowym czynnikiem przemawiającym za budową takiej pamięci masowej jest umożliwienie opartego na określonych zasadach przydziału zasobów pamięci masowej na poziomie maszyny wirtualnej za pośrednictwem hipernadzorcy kontrolującego przydzielanie wszystkich zasobów maszynom wirtualnym, aby spełnić wymagania dotyczące jakości usług (*ang. quality of service - QoS*) dostępu do danych dla aplikacji hostowanych na maszynach wirtualnych. Ze względu na to, że system VAS mapuje pamięć masową do maszyn wirtualnych, zadania związane z zarządzaniem takie jak monitorowanie wydajności pozwalają na określanie kwestii takich jak opóźnienie komunikacji między pamięcią masową i maszyną wirtualną. Wdrożenie rozwiązania VAS wymaga wykorzystania interfejsów programowych aplikacji (API) w wywoływanych z poziomu hipernadzorcy w systemie zarządzania pamięcią masową.

Innymi słowy, warstwa oprogramowania integrującego na poziomie hipernadzorcy jest umieszczona ponad konwencjonalną macierzą pamięci masowej, z kolei sama macierz może opierać się na dowolnych nośnikach pamięci, na przykład na dyskach magnetycznych lub półprzewodnikowych [12].

Z racji tego, że funkcje zarządzania w infrastrukturze pamięci masowej VAS są realizowane za pośrednictwem oprogramowania, systemy takie można postrzegać jako przykłady SDS dostosowane do zwirtualizowanych środowisk serwerowych. Kluczowym czynnikiem w środowisku VAS jest fakt, że komponenty pamięci masowej są zarządzane wspólnie z maszynami wirtualnymi, a nie jako oddzielnie zarządzane wolumeny lub numer jednostki logicznej (*ang. Logical Unit Number – LUN*) [13].

Kontenery stanowią pakiety rozwiązań obliczeniowych, sieciowych i pamięci masowej, które charakteryzują się mniejszym zapotrzebowaniem na zasoby niż maszyny wirtualne. Na pojedynczym serwerze w jednej maszynie wirtualnej lub w wyspecjalizowanych klastrach zapewniających usługi orkiestracji może działać wiele kontenerów.

Magazyny danych dla kontenerów [14] są zapewniane poprzez tworzenie woluminów w nowo utworzonym katalogu plików na hoście, na którym uruchomiony jest kontener, bądź też poprzez mapowanie do zewnętrznego urządzenia SAN lub NAS za pomocą wtyczek (*ang. plugins*). Woluminy te mogą być tworzone z wyprzedzeniem lub w momencie uruchomienia kontenera, mogą także być współdzielone przez wiele kontenerów. Wtyczki są dostarczane przez dostawców systemów pamięci masowych, aby ułatwić proces tworzenia wolumenów przy zachowaniu zgodności ze specyfikacją rozwiązania do obsługi lub orkiestracji kontenerów. Wtyczki automatyzują proces tworzenia i mapowania LUN bądź wolumenu do hosta oraz do kontenera.

2.9 Konwergentne i hiperkonwergentne macierze dyskowe (sieciowe pamięci masowe SAN oparte na serwerach)

W architekturze konwergentnej pamięć masowa, pamięć operacyjna, sieć oraz oprogramowanie do wirtualizacji są wstępnie skonfigurowane i preinstalowane w celu szybkiego wdrożenia w pojedynczej obudowie (np. szafie serwerowej zawierającej jeden lub więcej fizycznych hostów, zasoby pamięci masowej {DAS lub macierze pamięci masowej} i komponenty sieciowe). Architektura hiperkonwergentna zwiększa poziom abstrakcji – poszczególne komponenty pamięci masowej związane z fizycznymi hostami

są wirtualizowane w celu stworzenia wspólnej puli pamięci masowej, która jest współdzielona pomiędzy wszystkie maszyny wirtualne lub kontenery dzięki wykorzystaniu oprogramowania zarządzającego pamięcią masową definiowaną programowo [15]. Dlatego maszyna wirtualna lub kontener zlokalizowane na jednym fizycznym hoście – na przykład H(i) – mogą korzystać z pamięci masowej związanej z innym fizycznym hostem, na przykład H(j). Takie rozwiązanie umożliwia abstrakcję pamięci masowej i pozwala na zdalny dostęp do dysków.

W przypadku infrastruktury hiperkonwergentnej urządzenia wymagane do realizacji obliczeń, a także urządzenia sieciowe i pamięć masowa są ściśle powiązane. Wszystkie podstawowe funkcje zarządzania pamięcią masową, a także inne możliwości, takie jak: tworzenie kopii zapasowych, odzyskiwanie, replikacja, deduplikacja i kompresja, są realizowane za pośrednictwem warstwy oprogramowania zarządzającego dostawcy infrastruktury bądź sprzętu, a także przez przydział mocy obliczeniowych. Za przykłady takich rozwiązań mogą posłużyć rozwiązania firm takich jak Nutanix, Scale Computing, Dell (VxRail i PowerFlex Rack), Cisco (HyperFlex) i SimpliVity [16]. Ścisła integracja sprzętu wynika z tego, że dostawcy infrastruktur hiperkonwergentnych współpracują z producentami urządzeń pamięci masowej, aby wspólnie budować rozwiązania pamięci masowej dostosowane do ich stosu oprogramowania. Takie produkty stanowią oryginalne wyposażenie lub część standardowej architektury referencyjnej powszechnie akceptowanej w branży.

W takich systemach może zaistnieć potrzeba współdzielenia części czasu obliczeniowego procesora w celu realizacji funkcji dostępu do pamięci masowej i zarządzania nią. Szeroko pojęty stos oprogramowania zarządzającego może obejmować węzeł obliczeniowy, hipernadzorcę i oprogramowanie SDS, w zależności od środowiska, w którym wdrażane jest dane rozwiązanie – na przykład zwirtualizowanych infrastruktur, wirtualnych pulpitów, magazynów nieuporządkowanych danych czy superkomputerów [17]. Częstym scenariuszem wdrożenia jest sytuacja, w której środowisko aplikacji składa się z aplikacji opartych na mikrousługach realizowanych przy pomocy maszyn wirtualnych bądź kontenerów. Do oczekiwanych funkcji infrastruktur hiperkonwergentnych należą [18]:

- Opcjonalne funkcje redukcji danych, takie jak deduplikacja i kompresja w obrębie podstawowej pamięci masowej i kopii zapasowych.

- Zarządzanie poprzez pojedynczy panel kontrolny lub centralne rozwiązanie.
- Zdolność do realizacji wymagań w zakresie jakości usług dotyczących magazynowania danych w oparciu o potrzeby aplikacji.

Możliwości przetwarzania aplikacji w sterowniku urządzenia pamięci masowej (np. dyskach SSD obsługujących technologię NVMe) przy użyciu systemu na chipie (*ang. system on chip - SoC*) jest jednym z podejść do realizacji architektury hiperkonwergentnej macierzy dyskowe. Innym podejściem jest dostarczenie dodatkowej karty zawierającej pamięć masową w postaci dysku SSD lub układy pamięci flash z wbudowanym procesorem pozwalającym na uruchamianie aplikacji, przy czym są one podłączone bezpośrednio do magistrali PCIe serwera i działają w oparciu o protokół NVMe [19]. Nie są obecnie dostępne żadne komercyjne realizacje oparte na tej architekturze.

2.10 Przestrzeń składowania danych w chmurze

Przestrzenie składowania danych w chmurze mogą być oparte na ogólnodostępnych standardach lub własnościowych rozwiązaniach. Mogą obejmować usługi oparte na obiektach, blokach lub plikach. Techniczne przyczyny stosowania przez organizacje przestrzeni składowania danych w chmurze to [20]:

- Zaspokajanie zapotrzebowania na zasoby pamięci masowej bez konieczności budowy dodatkowego centrum danych.
- Reagowanie na zmiany w zapotrzebowaniu na pamięć masową do przechowywania danych, na przykład w przypadku występowania większych i mniejszych obciążeń.
- Zaspokojenie potrzeby szybkiego poszerzenia pamięci masowej na dane.
- Rosnąca złożoność zarządzania infrastrukturą pamięci masowej zainstalowanej w centrum danych.

Przestrzenie składowania danych w chmurze oferują szereg zaawansowanych usług związanych z danymi [21]:

- Współpraca – obejmuje funkcje takie jak na przykład (a) powiadomienia, gdy pliki są zmieniane przez innych użytkowników; (b) udostępnianie plików z możliwością

ustawienia uprawnień do odczytu i zapisu; (c) jednoczesna edycja plików; a także (d) śledzenie zmian i kontrola wersji.

- Możliwości integracji i analizy danych – możliwości łączenia danych znajdujących się w kilku źródłach w chmurze, wykonywania złożonych analiz oraz natychmiastowego przekazywania uzyskanych informacji lub przechowywania ich w magazynie danych w celu późniejszego dostępu przez klientów.
- Zaawansowane usługi ochrony danych, w tym replikacja, wykonywanie kopii lustrzanych, archiwizacja, audyt i szyfrowanie.

Przestrzenie składowania danych w chmurze często obejmują:

- Usługi przechowywania bloków, które eksponują zdefiniowane programowo urządzenia blokowe, które mogą być udostępniane wirtualnym hostom działającym w chmurze.
- Usługi przechowywania obiektów, które można mapować do hostów, aplikacji, a nawet innych usług w chmurze.
- Skalowalne współdzielone systemy plików, które mogą pozwolić skalowalnemu zestawowi hostów na dostęp do tego samego systemu plików z dużą prędkością.
- Różnorodne usługi replikacji, buforowania, archiwizacji, tworzenia lustrzanych kopii danych oraz kopii danych z określonego momentu w czasie, dostępne dla wszystkich powyższych rozwiązań.

Oferowane są również dodatkowe usługi w chmurze, takie jak zarządzane usługi bazodanowe, jeziora danych, pamięci podręczne i kolejki komunikatów. Technologia pozwala na przechowywanie danych stanowych i tymczasowych. Opinie ekspertów na temat tego, czy należy je klasyfikować jako usługi magazynowania danych, są jednak podzielone.

2.11 Zarządzanie danymi oraz pamięcią masową

Pojęcie zarządzania pamięcią masową odnosi się do wszystkich działań mających na celu zapewnienie niezawodności, odporności, wydajności i bezpieczeństwa zasobów pamięci masowej poprzez wykorzystanie narzędzi i procesów zarządzania. Ze względu na fakt, że bezpieczeństwo pamięci masowej stanowi główny przedmiot

zainteresowania niniejszego dokumentu, podrozdział ten skupia się na wszystkich działaniach niezwiązanych z mechanizmami bezpieczeństwa i związanymi z nimi zaleceniami znajdującymi się w rozdziale 4. Działania niezwiązane z mechanizmami bezpieczeństwa, które stanowią podstawy wykorzystywanych obecnie praktyk to:

- konfiguracja zasobów pamięci masowej i zarządzanie zasobami,
- klasyfikacja danych,
- sanityzacja danych,
- przechowywanie danych,
- ochrona danych,
- redukcja danych.

2.11.1 Konfiguracja zasobów pamięci masowej i zarządzanie zasobami

Konfiguracja zasobów pamięci masowej i zarządzanie zasobami obejmują pełne zarządzanie cyklem życia infrastruktury pamięci masowej. Proces ten zawiera w sobie między innymi:

- Orkiestrację zmian dotyczących wielu zasobów.
- Zarządzanie fizycznymi urządzeniami pamięci masowej oraz kontrolowanie ich działania. Dotyczy to urządzeń takich jak macierze pamięci masowej, przełączniki SAN, a także czynności takich jak aktualizacje oprogramowania, konfiguracja urządzeń, w tym ich zabezpieczeń, a także wprowadzanie do użytku i usuwanie urządzeń.
- Zarządzanie zasobami pamięci masowej (np. urządzeniami blokowymi, systemami plików, pulami pamięci), które obejmuje ich przypisywanie do hostów, replikację, zarządzanie migawkami, migrację danych oraz ich kategoryzację.
- Zarządzanie wydajnością i jej optymalizację.
- Zarządzanie przepustowością i jej optymalizację.
- Zarządzanie urządzeniami.
- Zarządzanie zdarzeniami.

2.11.2 Klasyfikacja danych

Dane organizacji mogą być klasyfikowane na podstawie szeregu aspektów, takich jak:

- wrażliwość (na przykład dane wrażliwe oraz dane niewrażliwe),
- częstotliwość (na przykład dane wymagające częstego dostępu oraz dane, które nie wymagają częstego dostępu),
- środowisko (na przykład produkcyjne, rozwojowe, testowe, wdrożeniowe).

Klasyfikacja danych pod kątem wrażliwości jest wymagana, aby umożliwić zapewnienie odpowiednich zabezpieczeń takich jak: uwierzytelnianie, autoryzacja, szyfrowanie, zarządzanie kluczami, czy sanityzacja. Ponadto kategoria wrażliwości może wymagać podkategorii opartych na przepisach dotyczących danych, na przykład danych osobowych, danych e z dokumentacją medyczną, a także danych związanych z normą bezpieczeństwa cyfrowego w branży kart płatniczych (*ang. Payment Card Industry Digital Security Standard - PCI-DSS*).

Klasyfikacja danych pod kątem częstotliwości jest wymagana w celu doboru odpowiednich nośników pamięci, na przykład dysków półprzewodnikowych oraz tradycyjnych dysków twardych. Klasyfikacja danych pod kątem środowiska może być wymagana zarówno w przypadku wyboru nośnika, jak i środków bezpieczeństwa. Można wykorzystać także inne modele klasyfikacji oparte na projekcie, aplikacji i innych aspektach, jednak nie zostały one wymienione powyżej, ponieważ nie muszą mieć wpływu na środki bezpieczeństwa.

2.11.3 Sanityzacja danych

Sanityzacja jest procesem, w wyniku którego zapisane wcześniej dane stają się niemożliwe do odzyskania. Służy uzyskaniu pewności, że uzyskanie dostępu do danych lub ich odtworzenie jest niemożliwe [10]. Istnieją trzy metody sanityzacji nośników:

- Czyszczenie (*ang. clearing*) – na przykład poprzez nadpisanie istniejących danych.
- Kasowanie (*ang. purge*) – na przykład usuwanie danych przy pomocy silnego pola magnetycznego do rozmagnesowania nośników magnetycznych, wymazywanie kryptograficzne zaszyfrowanych danych.
- Zniszczenie – na przykład fizyczne zniszczenie nośnika poprzez spalenie, zmiażdżenie itp.

Czynniki wpływające na wybór odpowiedniego rodzaju sanityzacji obejmują kategorię danych przechowywanych na nośniku, charakter nośnika (półprzewodnikowy, magnetyczny lub optyczny) oraz plany ponownego wykorzystania nośnika.

Sanityzacja może dotyczyć pojedynczych nośników danych lub danych logicznych, w tym danych przechowywanych w chmurze. W celu zapewnienia skuteczności, w procesie sanityzacji należy uwzględnić charakter oraz rodzaje nośników i danych. Na przykład nadpisywanie danych jest skuteczne na dyskach magnetycznych, ale nie na dyskach półprzewodnikowych wykorzystujących moduły pamięci flash – nadpisywanie danych na tych urządzeniach nie następuje w tych samych komórkach.

2.11.4 Retencja danych

Mogą zaistnieć sytuacje, w których dostęp do konkretnych danych jest wymagany w perspektywie krótko- i średnioterminowej (tj. mniej niż 10 lat) lub w perspektywie długoterminowej. Retencja danych jest zwykle realizowane poprzez przechowywanie kopii danych na jakimś nośniku zapasowym. Wymogi dotyczące retencji danych mogą wynikać z wymogów prawnych, regulacyjnych, operacyjnych lub statutowych.

2.11.5 Ochrona danych

Ochrona danych jest terminem zbiorczym obejmującym wszystkie działania, które prowadzą do zapewnienia, że dane są osiągalne, możliwe do wykorzystania, nieuszkodzone i dostępne dla wszystkich dopuszczonych celów, a dostęp odbywa się z akceptowalnym poziomem wydajności i zgodnie z wymogami dotyczącymi zgodności z przepisami, w tym prywatności i wszystkich fizycznych, administracyjnych i technicznych zabezpieczeń przed przypadkowym lub nieautoryzowanym ujawnieniem, modyfikacją lub zniszczeniem danych.

Pojęcie ochrony danych obejmuje działania i mechanizmy dotyczące całego cyklu życia pamięci masowej. Należą do nich [22]:

- Dane w spoczynku/na urządzeniu końcowym – dane znajdują się na serwerze lub urządzeniu klienckim.
- Dane w tranzycie – dane są przekazywane między urządzeniami pamięci masowej, klientem a serwerem lub różnymi serwerami.

- Dane w użyciu – dane są przeglądane, zmieniane lub synchronizowane między urządzeniami.
- Dane przekazywane poza obwód zabezpieczeń – dane są pobierane, wysyłane wraz z nośnikami fizycznymi itp.

Zakres celów i związanych z nimi działań stanowi taksonomię klasyfikacji działań związanych z ochroną danych w trzech aspektach – przechowywania, prywatności i zapewnienia bezpieczeństwa i integralności informacji [22]. Działania związane z prywatnością wykraczają poza zakres niniejszego dokumentu, ponieważ przepisy oraz regulacje dotyczące prywatności różnią się w zależności od krajów i społeczności, których dotyczą. Wśród działań związanych z zapewnieniem bezpieczeństwa i integralności informacji najważniejsze dotyczą zabezpieczeń technicznych. Każde z nich wymaga osobnego rozdziału, w którym zostanie omówione bardziej szczegółowo. Z tego powodu w niniejszej sekcji omówiono jedynie działania i zabezpieczenia dotyczące ochrony danych związane z ich przechowywaniem. Do tej kategorii zalicza się:

- tworzenie kopii zapasowych i odzyskiwanie danych,
- archiwizację,
- technologie replikacji,
- niezmienność,
- ciągłą ochronę danych,
- kopie punktowe w czasie i migawki danych.

Tworzenie kopii zapasowych to działania, w którym dane przechowywane w urządzeniach pamięci masowej są przeglądane przez systemy produkcyjne[11] i okresowo kopiowane na inny zestaw urządzeń pamięci masowej, z których część może pozostawać odłączona. Ze względu na zmienny charakter danych kopie zapasowe wykonane wcześniej są w wielu przypadkach dezaktualizowane przez kopię zapasową wykonaną w późniejszym okresie. Kopie zapasowe mogą przyjmować postać kopii

[11] System produkcyjny to zbiór elementów, ludzi, maszyn i procesów odpowiedzialnych za wytworzenie produktu lub usługi.

zapasowych plików, złożonych z kopii zapasowych wybranych zasobów danych przechowywanych w urządzeniu pamięci masowej (często opartych na logicznych strukturach danych, takich: jak pliki, katalogi, dane zawarte w schemacie bazy danych itp.), lub kopii zapasowych opartych na obrazach, które zawierają całą zawartość określonego urządzenia (np. pojedynczego LUN).

Archiwizacja polega na magazynowaniu danych w celu ich długotrwałego przechowywania. Choć do tworzenia kopii zapasowych i archiwizacji mogą być stosowane odrębne techniki i rozwiązania, często występuje między nimi ścisła zależność, ponieważ w przypadku archiwizacji często mamy do czynienia z tworzeniem kopii danych w celu ich długotrwałego przechowywania, a także z dodatkową klasyfikacją. Archiwizacja pozwala na:

- Zarządzanie cyklem życia informacji – umożliwia zapisywanie, przechowywanie oraz usuwanie różnych rodzajów danych i dokumentów na podstawie wymagań organizacji.
- Przeszukiwanie rekordów i dokumentów oraz wyszukiwanie danych – umożliwia na przykład wyszukiwanie rekordów na podstawie możliwych do zidentyfikowania atrybutów, takich jak identyfikator osoby.
- Zaspokojenie wymagań w zakresie ochrony danych, ich przechowywania i ochrony wynikających z obowiązujących przepisów.

Replikacja danych to proces zapisywania tych samych danych w co najmniej dwóch oddzielnych miejscach [20]. Replikacja jest często stosowana jako część procesu odzyskiwania danych i polega na kopiowaniu danych z jednej lokalizacji do drugiej. Ogólnie rzecz ujmując, istnieją dwa rodzaje replikacji – synchroniczna i asynchroniczna. Replikacja synchroniczna polega na kopiowaniu w czasie rzeczywistym danych z lokalizacji A (np. platformy produkcyjnej) do lokalizacji B (np. specjalnie wyznaczonej lokalizacji, z której dane zostaną odtworzone w przypadku awarii). Replikacja asynchroniczna między dwiema lokalizacjami wiąże się z opóźnieniem czasowym i może być wykonywana w sposób ciągły lub z określoną częstotliwością. Opóźnienie czasowe i częstotliwość replikacji są podyktowane planami odtworzenia danych po awarii i opisane w kategoriach określonych celów w zakresie czasu odzyskiwania

(*ang. Recovery Time Objective - RTO*) i punktu odtworzenia danych (*ang. Recovery Point Objective - RPO*).

Niezmienność polega na możliwości zablokowania danych po ich utworzeniu, co uniemożliwia ich zmianę lub usunięcie.

Ciągła ochrona danych (*ang. Continuous data protection - CDP*) jest formą kopii zapasowej, która umożliwia szczegółowe odzyskiwanie danych i wpływa pozytywnie na punkt odtworzenia danych. W przeciwieństwie do tradycyjnych kopii zapasowych, w przypadku których kopie danych wykonywane są okresowo, w przypadku CDP zmienione bloki danych są nieustannie przesyłane do docelowego środowiska, które kataloguje i zapisuje zmiany w czasie. Pod tym względem CDP przypomina replikację danych. Jednak w odróżnieniu od replikacji danych, CDP umożliwia zwykle odtwarzanie skopiowanych danych do poprzednich stanów przy użyciu różnych technik (np. bajt po bajcie, według wcześniej ustalonych zakładek, przywracania do poprzednich wersji itp.). Dodatkowe technologie, takie jak wersjonowanie lub dziennik plików i obiektów (z replikacją wersjonowanych kopii danych lub bez niej), przesyłanie logów transakcyjnych baz danych oraz inne rozwiązania, również można rozważać w kategoriach ciągłej ochrony danych.

Kopie punktowe w czasie są zwykle tworzone bezpośrednio na urządzeniu magazynującym dane źródłowe (np. macierz dyskową, system plików, bazę danych) i są przeznaczone do szybkiego odzyskiwania danych oraz wielu innych zastosowań, takich jak klonowanie danych produkcyjnych do celów testowych. Punkty przywracania mogą być również wykonywane ze zdalnych replik danych – wtedy określamy je mianem zdalnych migawek.

Migawka to zajmująca niewiele miejsca forma kopii punktowej, która przechowuje tylko poszczególne fragmenty danych zmienione od danego punktu w czasie w odniesieniu do danych źródłowych. Często oznacza to, że jeśli dane źródłowe są niedostępne, migawki również nie mogą zostać wykorzystane.

2.11.6 Redukcja danych

Redukcja danych to proces zmniejszania ilości przechowywanych bądź przesyłanych danych w celu zmniejszenia kosztów i poprawy efektywności. Dwa popularne podejścia

do redukcji danych to deduplikacja i kompresja danych. W niektórych przypadkach mogą być stosowane równolegle.

Kompresja danych, która czasem jest wykonywana sprzętowo, pozwala na zmniejszenie ilości danych poprzez zakodowanie ich za pomocą znanego algorytmu w celu uzyskania reprezentacji danych, która wykorzystuje mniej miejsca niż w postaci niezakodowanej [10]. Kompresja danych może być stosowana w wielu scenariuszach, jednak najczęściej jest wykorzystywana w procesie wykonywania kopii zapasowych na taśmach oraz podczas zdalnej replikacji danych w bramach sieciowych w celu zmniejszenia wymagań dotyczących przepustowości na potrzeby odtwarzania danych w przypadku awarii oraz zapewnienia ciągłości działania. Interoperacyjność jest kluczowym wymogiem dla kompresji danych, jeśli kompresja i późniejsza dekompresja mogą być wykonywane przez różne podmioty.

Celem **deduplikacji danych** jest zastąpienie wielu kopii identycznych danych odwołaniami do jednej kopii. Podstawę jej działania stanowi eliminacja identycznych bloków pamięci masowej. Przykładowo, jeśli w systemie pamięci masowej znajduje się 500 identycznych bloków, to macierz pamięci masowej będzie przechowywała tylko jedną kopię, eliminując tym samym konieczność przechowywania pozostałych 499 kopii [20]. Może się to odbywać na poziomie urządzenia pamięci masowej, na etapie transmisji lub na poziomie systemu plików.

3. ZAGROŻENIA, RYZYKA I WEKTORY ATAKU

W tym rozdziale zawarte są podstawowe informacje dotyczące zagrożeń bezpieczeństwa systemów pamięci masowej, ryzyka i wektorów ataku. Na potrzeby tego rozdziału pojęcie ryzyka określa możliwe skutki lub cele zagrożeń, a wektory ataku to możliwe środki, za pomocą których zagrożenia mogą zostać zrealizowane.

3.1 Zagrożenia

Zagrożenie to potencjalna przyczyna niepożądanego zdarzenia, które może spowodować szkody w systemie lub organizacji. Poniższe podrozdziały zawierają krótki przegląd zagrożeń związanych z infrastrukturą pamięci masowej.

3.1.1 Kradzież lub kompromitacja poświadczeń

Poświadczenia służą do weryfikacji tożsamości użytkowników, ich uwierzytelniania oraz przyznawania dostępu do systemów i narzędzi pamięci masowej. Istnieją różne formy poświadczeń, w tym klucze fizyczne, tokeny i karty, hasła, cyfrowe klucze prywatne, pliki cookie sesji, certyfikaty cyfrowe na stronach internetowych i inne rozwiązania. Wszystkie one są jednak podatne na ataki hakerów wykorzystujących odpowiednie narzędzia lub techniki. Najczęściej używanymi i najłatwiejszymi do skompromitowania są dane uwierzytelniające typu login/hasło, a ich stosowanie naraża organizacje na duże ryzyko. Kradzież danych uwierzytelniających stanowi coraz ważniejszy obszar działania cyberprzestępców. Sama długość i złożoność hasła w wielu przypadkach nie zapewnia wystarczającego stopnia ochrony przed atakiem. Niemal wszystkie skuteczne metody kradzieży poświadczeń (poza atakami typu „password spraying" oraz łamania haseł metodą „brute force") polegają na uzyskaniu dokładnego hasła użytkownika, a nie na jego losowym odgadywaniu. Współczesne oprogramowanie ransomware często pozyskuje hasła użytkowników z przechwyconych zbiorów danych. Poza wyłudzaniem informacji oraz sprawdzaniem danych pozyskanych przy pomocy oprogramowania ransomware, cyberprzestępcy wykorzystują także logowanie klawiszy przy pomocy złośliwego oprogramowania, które monitoruje proces wprowadzania hasła przed użytkownika. To kolejna metoda kradzieży poświadczeń, która działa niezależnie od złożoności hasła [23]. W wielu przypadkach poświadczenia logowania są przechowywane w ramach infrastruktury pamięci masowej. Jeśli dane te nie są odpowiednio zaszyfrowane w stanie spoczynku,

a infrastruktura pamięci masowej zostanie skompromitowana, haker może uzyskać dostęp do wielu poświadczeń użytkowników.

3.1.2 Złamanie szyfrowania

Szyfrowanie jest stosowane do zabezpieczania danych w stanie spoczynku i w czasie ich przesyłania, a także do ochrony sesji, w których dane w stanie spoczynku oraz przesyłane dane są zarządzane i nadzorowane. Algorytmy generowania kluczy szyfrujących wykorzystują losowość do tworzenia kluczy lub ich elementów składowych. Zastosowane metody szyfrowania mogą charakteryzować różne słabości, od słabych algorytmów szyfrowania i słabych generatorów kluczy, po podatności występujące po stronie serwera, wyciek kluczy, fundamentalne wady projektowe lub błędy i tylne furtki[12] (*ang. backdoor*) [24]. Z tego powodu niezwykle ważne jest, by nie tylko stosować silne algorytmy szyfrujące, lecz także dbać o odpowiednie zabezpieczenie kluczy szyfrujących. Proaktywna zmiana kluczy szyfrujących może być częścią strategii ochrony przed skompromitowanymi lub słabymi kluczami. Z punktu widzenia generowania kluczy niezwykle ważną rolę odgrywają zarówno siła klucza, jak i jego jakość oraz entropia. Kluczy szyfrujących nie należy wykorzystywać wielokrotnie. Niektóre ataki opierają się na wykorzystaniu słabości generatora liczb losowych, w tym przewidywalności lub ograniczonej entropii oraz możliwości zakłócenia jego działania, tak aby dwukrotnie zastosował tę samą liczbę losową do generacji klucza [25].

3.1.3 Infekcja złośliwym oprogramowaniem i oprogramowaniem typu ransomware

Złośliwe oprogramowanie (*ang. malware*) to ogólny termin określający każdy program, który został zaprojektowany w celu uszkodzenia, zakłócenia działania lub umożliwienia naruszenia zasad ochrony urządzenia. Złośliwe oprogramowanie narusza zasady ochrony systemu, spowalnia jego działanie i obniża jego bezpieczeństwo. Może być wykorzystane w celu kradzieży danych, przejęcia kontroli nad urządzeniem lub systemem, a także wykorzystania zasobów systemu do nielegalnych działań. Złośliwe oprogramowanie może dostać się do systemu na wiele sposobów. Może na przykład zostać przeniesione w czasie wymiany plików, pobrane wraz z darmowym oprogramowaniem, przesłane w postaci załącznika do wiadomości e-mail,

[12] Inna nazwa: *tylne wejście*. Potoczna nazwa: *backdor*.

zainstalowane ze skompromitowanej przenośnej pamięci masowej lub pobrane w czasie odwiedzin na zainfekowanej stronie internetowej [26]. Złośliwe oprogramowanie może zostać omyłkowo zainstalowane na hoście zarządzającym pamięcią masową i w konsekwencji spowodować wiele szkód, takich jak na przykład kradzież danych uwierzytelniających, eskalacja uprawnień, uszkodzenie, utrata lub zmiana danych, kompromitacja przyszłych kopii zapasowych i innych. Złośliwe oprogramowanie wykorzystuje luki w systemie operacyjnym i podatności w zainstalowanym oprogramowaniu w celu umożliwienia instalacji oraz wykonywania różnych działań. Im bardziej popularny jest dany pakiet oprogramowania, narzędzie lub dystrybucja systemu operacyjnego, tym większe prawdopodobieństwo, że zestawy złośliwego oprogramowania zostały już opublikowane. Z tego powodu łatwiej jest przeprowadzić atak na system zarządzania pamięcią masową niż samo urządzenie pamięci masowej. Nie oznacza to, że urządzenia pamięci masowej nie padają celem ataków – zagrożenia związane z wykorzystaniem skompromitowanych obrazów, oprogramowania układowego lub mikrokodu budzą coraz większe obawy ekspertów.

Oprogramowanie ransomware to forma złośliwego oprogramowania, które szyfruje przechowywane dane, czyniąc je bezużytecznymi. Następnie napastnik żąda okupu, a po jego zapłaceniu przywraca dostęp do danych. W niektórych przypadkach atakujący publikują poufne dane uzyskane z systemu pamięci masowej, aby wzbudzić w ofierze poczucie pilności sytuacji.

3.1.4 Niezałatane podatności oraz tylne furtki (tylne wejścia)

Niezałatane podatności oraz tylne furtki (tylne wejścia) mogą być wykorzystane bezpośrednio lub pośrednio do obejścia innych mechanizmów bezpieczeństwa.

Tylne furtki to mechanizmy zaszyte w oprogramowaniu, które zostały umieszczone w nim ***celowo*** przez dostawców lub indywidualnych twórców, a w rzadkich przypadkach także przez społeczeństwa lub złośliwe podmioty, z powodów uznawanych przez autora za uzasadnione – na przykład w celu usprawnienia wsparcia, rozwiązywania problemów, zapewnienia bezpieczeństwa narodowego i innych. Ze względu na możliwość ich wykorzystania w celu wyrządzenia szkód, informacje o tylnych furtkach nie znajdują się w oficjalnej dokumentacji i są udostępniane wyłącznie ograniczonej grupie osób.

Z czasem jednak informacje o ich istnieniu mogą zostać celowo lub nieumyślnie opublikowane lub odkryte przez społeczność.

Niezałatane podatności to ***niezamierzone*** efekty uboczne oprogramowania lub zależności, które nie zostały wychwycone przez testerów w procesie zapewniania jakości (*ang. quality assurance - QA*) lub testowania funkcjonalnego, których wykorzystanie może stanowić zagrożenie dla bezpieczeństwa.

Gdy podatności są ujawniane, w szczególności, gdy dotyczą wersji oprogramowania, które nadal są wspierane przez dostawców, zwykle wydają oni poprawkę w postaci łatki lub nowej wersji, która pozwala na rozwiązanie problemu. Z tego powodu niezwykle ważne jest instalowanie poprawek w krótkim czasie po ich publikacji. Duża część skutecznych ataków opiera się na lukach, dla których istnieją już odpowiednie poprawki.

3.1.5 Eskalacja uprawnień

Eskalacja uprawnień to działanie polegające na wykorzystaniu luki w oprogramowaniu, błędu projektowego lub wdrożeniowego albo błędu w konfiguracji oprogramowania w celu uzyskania dostępu do zasobów, które w normalnych warunkach są chronione przed daną aplikacją lub niedostępne dla danego użytkownika [27]. Działanie to jest często związane z wykorzystaniem tylnych wejść i podatności, a niektórzy eksperci uznają eskalację uprawnień za podtyp powyższych zagrożeń. Eskalacja uprawnień występuje w dwóch formach: 1) pionowa eskalacja uprawnień (znana również jako podnoszenie uprawnień) – sytuacja, w której użytkownik lub aplikacja o niższym poziomie uprawnień uzyskuje dostęp do funkcji lub treści dostępnych wyłącznie dla użytkowników lub aplikacji o wyższym poziomie uprawnień; 2) pozioma eskalacja uprawnień – sytuacja, w której zwykły użytkownik uzyskuje dostęp do funkcji lub treści dostępnych wyłącznie dla innych zwykłych użytkowników. W systemach pamięci masowej ten rodzaj zagrożenia może przekładać się na występowanie zróżnicowanych ryzyk, w tym uszkodzenia, zmiany i utraty danych. Napastnik może na przykład użyć podwyższonych uprawnień, aby uzyskać dostęp do systemu pamięci masowej, usunąć woluminy i zmodyfikować konfigurację dostępu. Atak może również doprowadzić do naruszenia zabezpieczeń kopii zapasowych danych, w tym na przykład kopii synchronicznych i asynchronicznych oraz migawek, a także wpłynąć na proces tworzenia nowych kopii zapasowych. Do samej eskalacji uprawnień może dojść na wielu poziomach, począwszy od elementów systemu

pamięci masowej (np. macierzy pamięci masowej, hosta lub klienta), przez urządzenia sieciowe, aż po systemy zarządzania.

3.1.6 Błąd ludzki i celowe wprowadzenie błędnej konfiguracji

Nawet pomimo wdrożenia odpowiednich mechanizmów zabezpieczeń użytkownicy mogą wprowadzić technicznie wykonalne i możliwe zmiany konfiguracji pamięci masowej, które mogą stanowić zagrożenie dla bezpieczeństwa danych (na przykład mapowanie zastrzeżonego zasobu pamięci obiektowej do sieci publicznej, zatrzymanie replikacji lub tworzenia kopii zapasowych w celu przeprowadzenia konserwacji bez ponownego włączenia ich po zakończeniu). Takie zaniechania mogą być niezamierzone - w takich wypadkach mamy do czynienia z błędem; mogą być także celowe, wówczas stanowią sabotaż.

Błędy ludzkie przybierają różne formy, a niektóre z nich są znacznie trudniejsze do dostrzeżenia niż inne, co utrudnia skutecznemu przeciwdziałaniu. Wśród nich znajdują się między innymi:

- literówki,
- brak wiedzy lub nieznajomość wewnętrznych zabezpieczeń bazowych oraz najlepszych praktyk dostawców,
- problemy z komunikacją między jednostkami lub zespołami,
- błędy związane z orkiestracją lub automatyzacją infrastruktury pamięci masowej:
  - ✓ bezpośrednie, na przykład błędy w skryptach i manifestach,
  - ✓ pośrednie, takie jak niezrealizowane zależności między oprogramowaniem.

3.1.7 Fizyczna kradzież nośników danych

Niezależnie od rodzaju, wszystkie dane są magazynowane w jednej lub kilku kopiach na nośnikach fizycznych, które są podatne na kradzież. Nośniki, zarówno podłączone do urządzeń, jak i odłączone, mogą zostać usunięte z wyznaczonego miejsca lub podczas fizycznego transportu między lokalizacjami (na przykład nośniki kopii zapasowych transportowane w celu archiwizacji lub urządzenia magazynujące dane transportowane w ramach projektu przeniesienia centrum danych). Kradzież może mieć charakter oportunistyczny, gdy złodziej nie zna zawartości skradzionych nośników z wyprzedzeniem,

może też mieć charakter celowy, gdy to konkretne dane są przedmiotem zainteresowania sprawców, którzy dysponują środkami pozwalającymi określić, które nośniki muszą przejąć.

3.1.8 Podsłuch sieciowy

Dane mogą zostać przechwycone także w trakcie ich przesyłania. Przesyłanie danych wykorzystuje wiele elementów infrastruktury – karty sieciowe (przewodowe lub bezprzewodowe), kable (przewodzące prąd lub światło), repeatery, przełączniki, routery itp. Każdy z tych elementów może zostać skompromitowany, a wiele form naruszenia zabezpieczeń jest trudne lub niemożliwe do wykrycia za pomocą najnowocześniejszych narzędzi i metodologii.

Chociaż szyfrowanie danych na ścieżce transmisji odgrywa ważną rolę w ograniczaniu możliwości ich wykorzystania w sytuacji podsłuchania transmisji, jednak nadal może dojść do naruszenia zasad ochrony, na przykład poprzez przechwycenie danych przed ich zaszyfrowaniem lub po ich odszyfrowaniu, lub poprzez zgromadzenie wystarczającej ilości danych do złamania szyfrowania.

Niektóre naruszenia zasad ochrony transmisji mogą wykraczać poza przechwytywanie danych (określane także mianem pasywnego podsłuchu) i obejmować wprowadzanie, usuwanie lub zmienianie przesyłanych danych, metadanych lub ruchu sterującego.

3.1.9 Niezabezpieczone obrazy, aplikacje i oprogramowanie układowe

Atakujący mogą podjąć próbę wpływania na proces dystrybucji, aktualizacji lub instalacji oprogramowania urządzenia pamięci masowej w celu wprowadzenia nieprawidłowego, nieaktualnego lub złośliwie zmodyfikowanego kodu (na przykład w postaci plików binarnych, obrazów, oprogramowania układowego, sterowników itp.) Takie zagrożenia mogą dotyczyć dysków twardych, napędów i bibliotek taśmowych, kart sieciowych i kontrolerów (takich jak HBA, NIC, adaptery FCoE itp.), przełączników i innych urządzeń sieciowych, obudów, macierzy pamięci masowej, systemu operacyjnego urządzenia pamięci masowej, systemu operacyjnego urządzenia klienta oraz innych elementów. Procesy aktualizacji oprogramowania mogą opierać się na złożonych łańcuchach dostaw, w których skład wchodzi wystawca (np. sprzedawca, podmiot zewnętrzny, społeczność open source), metody dostarczania (np. transmisja lub pobieranie, wysyłka nośnika instalacyjnego, wykonanie kopii pliku przez

pracownika sprzedawcy), lokalne kopie przechowywane przez poszczególne organizacje (np. proxy, wewnętrzne serwery plików) i inne elementy. Każde ogniwo łańcucha może zostać obrane za cel przez przestępców w celu wprowadzenia zmanipulowanego oprogramowania. W związku z tym może dojść na przykład do infiltracji systemów wystawców w celu wprowadzenia zmian do kodu źródłowego, uzyskania dostępu do oprogramowania lub urządzeń pozwalających na podpisywanie oprogramowania, publikacji zmienionych podpisanych plików binarnych na stronach pobierania lub serwerach aktualizacji itp. Podobne strategie można opracować dla innych ogniw łańcucha dostaw oprogramowania.

3.2 Ryzyka dotyczące infrastruktury pamięci masowej

Ryzyko związane z bezpieczeństwem określa się jako:

> „…stopień, w jakim dany podmiot jest zagrożony przez potencjalne wystąpienie danej okoliczności lub danego zdarzenia. Ryzyko stanowi zwykle wypadkową: (I) niekorzystnych skutków, które zaistniałyby w przypadku wystąpienia danej okoliczności lub danego zdarzenia; oraz (II) prawdopodobieństwa jego wystąpienia.
>
> Ryzyka bezpieczeństwa związane z systemem informacyjnym wynikają z utraty poufności, integralności lub dostępności informacji bądź systemów informacyjnych. Ryzyka te odzwierciedlają potencjalny niekorzystny wpływ na działania danej organizacji, w tym misję, wizerunek lub reputację, jej majątek, a także jednostki, organizacje oraz państwo”. [28]

3.2.1 Wyciek oraz naruszenie danych

Wyciek danych to zdarzenie, w wyniku którego wrażliwe, chronione informacje są kopiowane, przekazywane, przeglądane, celowo wystawiane na widok publiczny lub wykorzystywane przez osoby lub podmioty do tego nieuprawnione. Informacje te mogą obejmować numery kart bankowych i kredytowych, dane osobowe (w tym dane dotyczące zdrowia, adres domowy, numery telefonów, daty urodzenia), tokeny sesji, hasła, dane klientów, tajemnice handlowe, kwestie bezpieczeństwa narodowego lub inne zastrzeżone lub wrażliwe informacje.

Wyciek danych może być wynikiem działania zewnętrznego podmiotu, takiego jak na przykład haker lub cyberprzestępca, a także podmiotu wewnętrznego, takiego jak

złośliwy lub niezadowolony pracownik. Wycieki danych mogą być dokonywane w sposób ukryty – w takich przypadkach ich ślady są zacierane lub całkowicie usuwane, a także w sposób umożliwiający łatwe określenie sposobu oraz sprawcy, niezależnie od tego, czy był wynikiem działania zamierzonego, czy wynikał z braku odpowiedniej wiedzy. Wycieki danych mogą nieść za sobą różne skutki, od niedogodności dla użytkowników, aż po naruszenie wrażliwych lub poufnych danych, co może spowodować nieodwracalne naruszenie reputacji oraz zakłócić działalność organizacji.

Choć niektóre wycieki danych wiążą się zastosowaniem zaawansowanych technik, wiele z nich jest skutkiem prostych błędów w konfiguracji zabezpieczeń magazynów danych. Możliwe przyczyny obejmują między innymi słabe szyfrowanie (lub jego brak) danych w stanie spoczynku lub podczas przesyłania, błędy oprogramowania, utrata kontroli nad nośnikami wymiennymi, kradzież nośników, niewłaściwie skonfigurowane lub zbyt luźne ograniczenia dostępu, nieprawidłowe lub niepełne przeprowadzenie sanityzacji danych (na przykład w przypadku usuniętych obiektów, wycofanych z użytku nośników, a także nośników wykorzystywanych ponownie), przesłanie lub przekazanie informacji do niewłaściwego odbiorcy, przesyłanie danych do nieprawidłowej lokalizacji lub w nieprawidłowy sposób (na przykład przesyłanie chronionych danych do publicznego magazynu danych).

3.2.2 Nieuprawniona zmiana i dodanie danych

Zmiana danych odnosi się do procesu modyfikacji danych przed lub po ich wprowadzeniu do systemu. W tym przypadku atakujący uzyskuje dostęp do infrastruktury pamięci masowej i modyfikuje dane w sposób, który wpłynie na przyszłe operacje aplikacji lub inne zastosowania danych.

Zmiana i dodawanie danych mogą być prowadzone przez podmioty zewnętrzne lub wewnętrzne w sposób ukryty lub łatwy do wykrycia. W niektórych przypadkach ten rodzaj ryzyka występuje w wyniku tak zwanego „ataku salami”, w którym atakujący kradnie niewielkie fragmenty danych lub pieniędzy przez długi czas, wykorzystując w tym celu dużą liczbę transakcji. Skutki zmiany i dodawania danych mogą być różne – od utraty środków finansowych po trwałe naruszenie reputacji i zaufania.

3.2.3 Uszkodzenie danych

Uszkodzenie danych oznacza wystąpienie błędów lub zniekształceń w danych pojawiające się podczas zapisu, odczytu, przechowywania, przesyłania lub przetwarzania danych. Ich efektem jest wprowadzenie niezamierzonych zmian do oryginalnych danych. Gdy dochodzi do uszkodzenia danych, obiekt zawierający te dane będzie zwracał nieoczekiwane wyniki w czasie uzyskiwania dostępu do danych przez system lub powiązane aplikacje. Skutki uszkodzenia danych mogą być różne, od utraty niewielkiej ilości danych aż po awarię systemu. Na przykład w przypadku uszkodzenia pliku dokumentu użytkownik może nie być w stanie go otworzyć, a po otwarciu część lub wszystkie dane mogą być nieczytelne. Niektóre rodzaje złośliwego oprogramowania mogą celowo uszkadzać lub niszczyć pliki, zazwyczaj poprzez nadpisanie ich niedziałającym lub śmieciowym kodem, a także wymuszenie bezpiecznego wymazania ich zawartości. Choć niektóre formy uszkodzenia danych powodują występowanie błędów urządzenia pamięci masowej, systemu operacyjnego lub oprogramowania przy próbie dostępu do danych, niektóre metody mogą być zaprojektowane w taki sposób, aby zmiany nie powodowały błędów.

3.2.4 Naruszenie zasad ochrony kopii zapasowych

Tworzenie kopii zapasowych, czyli przechowywanie i archiwizowanie kopii (w tym replik i migawek) zasobów danych jest ważne, aby umożliwić odzyskanie tych zasobów w przypadku ich uszkodzenia lub utraty. Zadowalające odzyskanie danych jest możliwe tylko wtedy, gdy kopie zapasowe są generowane prawidłowo, z zachowaniem odpowiedniego okresu przechowywania i aktualności, przechowywane w bezpieczny sposób i dostępne w sposób umożliwiający ich szybkie przywrócenie. Ze względu na fakt, że te warunki są ze sobą ściśle powiązane, proces tworzenia kopii zapasowych jest narażony na ryzyko występowania licznych problemów. Problemy te mogą obejmować nieprawidłową konfigurację, która może polegać na wykonaniu kopii zapasowej bazy danych bez zastosowania technik zapewniających spójność lub wierność kolejności zapisu. Brak zapewnienia odpowiedniej aktualności lub okresu przechowywania kopii może spowodować, że część danych, starych lub nowych, będzie niemożliwa do odzyskania. Napastnik ma zatem dużą motywację, aby obrać za cel nie tylko główny zasób danych, lecz także jego kopie zapasowe. W sytuacji, w której niemożliwe jest

przeprowadzenie ataku na istniejące kopie, występuje możliwość zastosowania strategii polegającej na ingerencji w sam proces tworzenia kopii zapasowych, a tym samym stopniowe „zatruwanie" przyszłych kopii. Gdy minie wystarczająco dużo czasu, atakujący może powrócić do pierwotnego celu, czyli skompromitowania podstawowych zasobów danych z pełną świadomością, że jedyne dostępne kopie zapasowe są zbyt stare.

Innym rodzajem strategii „zatruwania" jest celowe infekowanie kopii zapasowych elementów obliczeniowych lub aplikacji, w tym między innymi obrazów systemów operacyjnych, pakietów oprogramowania, oprogramowania układowego, a nawet repozytoriów kodu źródłowego. W ten sposób, gdy pojedynczy element lub całe środowisko zostaną odbudowane w celu zwalczenia infekcji, część złośliwego oprogramowania znajdzie się w odbudowanym środowisku, co pozwoli atakującemu na szybkie odzyskanie kontroli lub wyrządzenie większych szkód.

3.2.5 Złośliwa obfuskacja oraz szyfrowanie danych

Odwracalna obfuskacja[13] bądź szyfrowanie danych powodują, że dane stają się niedostępne dla użytkownika lub organizacji, chyba że zostaną odzyskane przy użyciu klucza posiadanego wyłącznie przez napastnika. Ten rodzaj ryzyka jest powszechnie wykorzystywany w atakach przy pomocy oprogramowania ransomware – złośliwego oprogramowania, które szyfruje dane ofiary i żąda okupu za przywrócenie dostępu. Choć pierwotnie jego celem padały dane lub pliki na komputerach użytkowników lub serwerach organizacji, z czasem oprogramowanie ransomware zmieniało się i obecnie atakuje także inne elementy systemów pamięci masowej, takie jak urządzenia NAS i urządzenia do tworzenia kopii zapasowych [30].

Obfuskacja oraz szyfrowanie danych zwykle odbywają się w wyniku ataku z zewnątrz, lecz mogą być potencjalnie spowodowane także przez podmioty wewnętrzne. Napastnicy często dążą do tego, by ich atak został odkryty, a samym atakom zwykle towarzyszą instrukcje dotyczące zagrożenia oraz wpłaty okupu.

[13] Zaciemnianie kodu (także obfuskacja, z *ang. obfuscation*) to technika przekształcania programów, która zmienia składnię, ale zachowuje ich semantykę, co znacząco utrudnia ich zrozumienie.

Skutki obfuskacji i szyfrowania danych mogą obejmować zarówno utratę środków finansowych po trwałe naruszenie reputacji i zaufania organizacji.

3.2.6 Niedostępność danych i odmowa świadczenia usługi

W przypadku wystąpienia incydentu dostępności danych lub ataku typu odmowa świadczenia usługi (*ang. denial-of-service - DoS*) klient nie może uzyskać dostępu do niektórych lub wszystkich swoich danych. Ryzyko zakłócenia dostępności danych może wystąpić w wyniku celowego lub niezamierzonego uszkodzenia trasy komunikacyjnej lub zmiany konfiguracji dostępu. Uszkodzenie może mieć charakter fizyczny, na przykład przerwanie trasy komunikacyjnej w wyniku rozłączenia, a także logiczny – przykładem może być na przykład błędna konfiguracja punktu końcowego lub elementów sieci. Napastnik może zmodyfikować lub usunąć ustawienia maskowania SAN w pamięci blokowej lub zawiesić ustawienia eksportu protokołu NFS, przez co klienci nie będą mogli uzyskać dostępu do swoich danych. Chociaż uszkodzenia mogą być odwracalne (na przykład poprzez przywrócenie ustawień, które zostały zmienione lub usunięte), mogą powodować długotrwałe zakłócenia i przestoje w pracy systemu lub usługi. Atak typu odmowa świadczenia usługi (DoS)również powoduje zakłócenie dostępu do danych poprzez zalanie docelowych urządzeń pamięci masowej, interfejsów zarządzania, klientów lub sieci zbędnymi żądaniami w celu przeciążenia systemów i uniemożliwienia realizacji niektórych lub wszystkich rzeczywistych żądań. Ataki DoS mogą potencjalnie wpłynąć nie tylko na poszczególne zasoby danych i klientów, lecz także na całą strukturę.

3.2.7 Manipulowanie logami i danymi dziennika audytu dotyczącymi pamięci masowej

Manipulowanie logami[14] i danymi dziennika audytu[15] odnoszącymi się do pamięci masowej polega na tym, że w celu ukrycia ataku napastnik usuwa lub modyfikuje logi, aby uniemożliwić skuteczne prześledzenie ścieżki audytu (w czasie rzeczywistym lub po zakończeniu ataku), a także w celu wprowadzenia w błąd osób badających atak poprzez umieszczenie w dzienniku fałszywych informacji. Pliki dziennika mogą być

[14] Zapis zdarzeń zachodzących w systemach i sieciach organizacji.

[15] Chronologiczny zapis działań systemowych. Obejmuje zapisy dostępów do systemu i operacji wykonywanych w danym okresie. Stanowi dokumentację dowodową określonych zdarzeń.

zmodyfikowane częściowo, na przykład poprzez modyfikację znacznika czasu. Skutkiem tego ryzyka jest to, że zarówno obecność napastnika, jak i sam fakt ataku mogą nie zostać wykryte przez systemy bezpieczeństwa, które opierają się na danych dziennika. W tym czasie atakujący może przeprowadzić dodatkowe działania i zaatakować inne systemy, co może doprowadzić do zagrożenia danych bądź usług. Przykładowo, atak typu „brute force" mający na celu zalogowanie się do wrażliwego systemu może zostać ukryty poprzez usunięcie z plików dziennika nieudanych prób logowania. Inna forma tego zagrożenia polega na manipulowaniu samym mechanizmem logowania poprzez na przykład wyłączanie go, zapełnianie całej wolnej przestrzeni sfabrykowanymi komunikatami, zmuszenie klientów do wysyłania danych z plików dziennika na przejęte serwery itp.

3.2.8 Kompromitacja systemu operacyjnego pamięci masowej lub plików binarnych, oprogramowania układowego i obrazów

Kompromitacja oprogramowania pamięci masowej, w tym systemu operacyjnego urządzenia pamięci masowej, oprogramowania układowego, obrazów i innych zasobów może wiązać się z wieloma problemami – może umożliwić napastnikom zdalny dostęp do danych, a także ich odczyt, kopiowanie, zmianę lub zniszczenie, naruszenie kopii danych, zmianę ustawień zabezpieczeń, ujawnienie danych, zmianę zachowania infrastruktury pamięci masowej i szereg innych działań. Zmiana konfiguracji pamięci masowej może budzić szczególne obawy ze względu na fakt, że może zostać wykorzystana do wprowadzenia różnych niewidocznych i trudnych do wykrycia wektorów ataku, w tym prezentowania nieprawidłowych danych klientom pamięci masowej (nawet jeśli przechowywane dane są nienaruszone), podawania nieprawidłowego stanu (np. fałszywych informacji o istnieniu lub stanie migawek i ustawień zabezpieczeń), obchodzenia zabezpieczeń zastosowanych w środowisku (np. ograniczeń maksymalnej temperatury, zużycia energii, prędkości), a także usuwania szyfrowania lub zmiany jego konfiguracji i wielu innych.

3.2.9 Mapowanie zagrożeń i ryzyk

Poniższa tabela mapuje zagrożenia omówione w podrozdziale 3.1 ze skutkami ryzyk omówionych w podrozdziale 3.2.

Zagrożenie – możliwość wystąpienia niepożądanych zdarzeń	**Ryzyko – Skutki wystąpienia zdarzenia**
Kradzież lub kompromitacja poświadczeń	*System aplikacji* – wyciek danych, narażenie danych, nieautoryzowana zmiana danych, uszkodzenie danych *System administracyjny* – kompromitacja istniejących i przyszłych kopii zapasowych, atak przy pomocy oprogramowania ransomware, atak DoS, manipulowanie plikami dziennika i danymi audytowymi związanymi z pamięcią masową, zmiana parametrów konfiguracji pamięci masowej na niebezpieczne
Złamanie szyfrowania	Wyciek danych i narażenie a) danych w stanie spoczynku, b) danych w czasie przesyłania oraz c) danych dotyczących sesji użytkownika/administratora
Infekcja złośliwym oprogramowaniem i oprogramowaniem typu ransomware	Złośliwe oprogramowanie może doprowadzić do powstania innych zagrożeń, w tym eskalacji uprawnień oraz kradzieży poświadczeń Złośliwe oprogramowanie, w zależności od miejsca występowania (w systemach aplikacji lub systemach administracyjnych) może doprowadzić do wystąpienia wszystkich skutków ryzyk wymienionych w podrozdziale 3.2.

Zagrożenie – możliwość wystąpienia niepożądanych zdarzeń	**Ryzyko – Skutki wystąpienia zdarzenia**
Niezałatane podatności oraz tylne furtki	Zależnie od charakteru podatności, jednak w wielu przypadkach do tego zagrożenia odnoszą się wszystkie skutki ryzyka kradzieży lub kompromitacji poświadczeń
Eskalacja uprawnień	W zależności od tego, czy skompromitowane zostały poświadczenia użytkownika, czy administratora, do tego zagrożenia odnoszą się wszystkie skutki ryzyka kradzieży poświadczeń.
Błąd ludzki i celowe wprowadzenie błędnej konfiguracji	W zależności od rodzaju i zakresu błędu niewłaściwa konfiguracja może prowadzić do występowania wszystkich skutków ryzyk wymienionych w podrozdziale 3.2
Fizyczna kradzież nośników danych	W zależności od skali kradzieży może dojść do wycieku danych oraz naruszenia danych, uszkodzenia danych, uszkodzenia istniejących kopii zapasowych, uniemożliwienia dostępu do danych oraz ataków typu „odmowa świadczenia usługi.
Niebezpieczne obrazy, aplikacje i oprogramowanie układowe	W zależności od rodzaju i zakresu błędu, niewłaściwa konfiguracja może prowadzić do występowania wszystkich skutków ryzyk wymienionych w podrozdziale 3.2

3.3 Powierzchnie ataku

Mianem powierzchni ataku (*ang. attack aurfaces*) określa się sumę różnych punktów („wektorów ataku" - *ang. „attack vectors")*, w których nieautoryzowany użytkownik („napastnik") może próbować wprowadzić dane do lub wydobyć dane ze środowiska [31]. W tym podrozdziale znajdują się opisy typowych cyfrowych i fizycznych powierzchni ataku związanych z infrastrukturą pamięci masowej.

3.3.1 Dostęp fizyczny

Uzyskanie fizycznego dostępu do infrastruktury pamięci masowej polega na fizycznym wtargnięciu do centrum danych, na jego teren, do obiektów infrastruktury komunikacyjnej (w tym okablowania) lub do pojazdów przewożących obiekty fizyczne (np. hosty, macierze pamięci masowej, dyski twarde, taśmy). Wtargnięcie takie jest dokonywane w celu uzyskania dostępu, kradzieży lub uszkodzenia danych, a także ograniczenia ich dostępności.

Wtargnięcie może polegać na uzyskaniu dostępu przez napastnika udającego osobę, która powinna znajdować się w danym miejscu (na przykład pracownika sprzątającego, technika czy konserwatora budynku).

Kolejnym sposobem na uzyskanie dostępu do obszarów chronionych w centrach danych jest wejście za drugą osobą. Intruz może dostać się do centrum operacyjnego sieci, na przykład niosąc tacę z jedzeniem. Mimo że dostęp do centrum danych jest chroniony przy pomocy czujników biometrycznych, pracownicy mogą otworzyć drzwi intruzowi z jedzeniem. W innych przypadkach intruz może po prostu wejść za pracownikiem wchodzącym do środka. Ochrona dostępu fizycznego stanowi ostatnią linię obrony.

Intruz, który uzyska dostęp do infrastruktury pamięci masowej, może ukraść, powielić, uszkodzić lub zniszczyć nośniki i dane. Mając fizyczny dostęp do urządzeń, intruz może także zmodyfikować system operacyjny pamięci masowej i konfigurację dostępu, a także zainstalować fizyczne urządzenia podsłuchowe lub transmisyjne, aby umożliwić późniejszy zdalny dostęp do urządzeń. Intruz może także podłączać lub usuwać nośniki, podłączać urządzenia do portów systemu pamięci masowej, podłączyć się do portu zarządzania, a także portu używanego do aktualizacji oprogramowania układowego bądź do terminala zarządzania. Nawet jeśli centralne systemy pamięci masowej są dobrze

chronione przy pomocy zabezpieczeń fizycznych, napastnik może obrać za cel dodatkowe elementy infrastruktury pamięci masowej, które mogą być słabiej chronione, takie jak: przełączniki brzegowe, odsłonięte porty sieciowe i stacje robocze wykorzystywane do zarządzania systemem. Podatne na atak są również kable wykorzystywane do komunikacji. Wyrafinowany napastnik może na przykład podsłuchać komunikację z pamięcią masową dzięki uzyskaniu fizycznego dostępu do kabli. Inna metoda dostępu fizycznego polega na zastąpieniu urządzeń peryferyjnych takich jak klawiatura i mysz zainfekowanymi urządzeniami – na przykład klawiaturą z zainstalowanym urządzeniem typu „keylogger" zapisującym wprowadzane dane takie jak nazwy użytkownika i hasła bądź na przykład z wbudowanym modułem, który jest w stanie zainfekować system złośliwym oprogramowaniem.

3.3.2 Dostęp do systemu operacyjnego pamięci masowej

Ta powierzchnia ataku obejmuje włamanie do urządzenia pamięci masowej poprzez wykorzystanie luk w systemie operacyjnym, pod którego kontrolą działa. Termin „system operacyjny pamięci masowej" odnosi się do wszystkich systemów operacyjnych związanych z infrastrukturą pamięci masowej, w tym systemów macierzy dyskowych, przełączników, urządzeń realizujących funkcje ochrony danych oraz urządzeń do wirtualizacji pamięci masowej. W wielu przypadkach systemy operacyjne sterujące pracą tych urządzeń są oparte na dostosowanych do potrzeb danego rozwiązania wariantach systemów operacyjnych z rodziny Linux/Unix, które charakteryzują się zwykle większymi ograniczeniami oraz wyższym poziomem bezpieczeństwa niż dystrybucje ogólnego przeznaczenia. Wszystkie systemy operacyjne zawierają jednak luki w zabezpieczeniach, dlatego należy regularnie instalować aktualizacje oraz poprawki bezpieczeństwa. Co więcej, każdy system operacyjny może być skonfigurowany w sposób, który może mieć wpływ na jego bezpieczeństwo. Napastnik może uzyskać dostęp do systemu operacyjnego pamięci masowej różnymi metodami, począwszy od lokalnego procesu logowania (przy użyciu standardowego protokołu, na przykład Secure Shell (SSH), rshell, telnet i podobnych), poprzez zdalne logowanie przy użyciu protokołu TCP/IP lub poprzez wykorzystanie podatności w systemie operacyjnym. W przypadku infrastruktury hiperkonwergentnej powierzchnia ataku może być znacznie większa, ponieważ obejmuje ona wiele instancji

systemu operacyjnego hosta, z których część może uruchamiać dowolne zadania obliczeniowe.

3.3.3 Dostęp do hostów odpowiedzialnych za zarządzanie

Większość elementów systemów pamięci masowej jest zarządzana lub konfigurowana za pośrednictwem hostów zarządzających, które zwykle działają pod kontrolą komercyjnych systemów operacyjnych. Dzięki skutecznemu atakowi na hosta odpowiedzialnego za zarządzanie z wykorzystaniem złośliwego oprogramowania lub podatności w systemie operacyjnym, napastnik może na przykład zmodyfikować plik wykonywalny, odczytać dane z pamięci podręcznej, zainstalować aplikację pozwalającą na podgląd zawartości pamięci w celu odczytania jej zawartości, zainstalować złośliwe oprogramowanie lub uzyskać dostęp do powiązanej macierzy pamięci masowej bądź jej konfiguracji. W wyniku tego działania dzięki atakowi na hosta odpowiedzialnego za zarządzanie, napastnik może doprowadzić do realizacji większości ryzyk, które obejmują między innymi uszkodzenie danych, ich usunięcie lub zmianę, kompromitację przyszłych kopii zapasowych, manipulację plikami dziennika i audytu i im podobne. Dostęp do hostów zarządzających zapewnia atakującemu możliwość wyrządzenia niemal nieograniczonych szkód w całej domenie zarządzanej przez danego hosta.

3.3.4 Interfejsy API, oprogramowanie zarządzające oraz zarządzanie wewnętrzne

Komponenty infrastruktury pamięci masowej udostępniają interfejsy użytkownika oprogramowania zarządzającego, API oraz inne protokoły zarządzania wewnątrz pasma oraz poza pasmem (*ang. in-band management* oraz *out-of-band management*) służące do administrowania urządzeniami i zarządzania pamięcią masową.
W niektórych przypadkach urządzenie jest wyposażone w interfejs zarządzania oparty na protokole Simple Object Access Protocol (SOAP) lub API REST, a także oprogramowanie zarządzające zainstalowane na hoście odpowiedzialnym za zarządzanie. Co więcej, systemy pamięci masowej często współdziałają z zewnętrznymi usługami sieciowymi w zakresie zarządzania kluczami, uwierzytelniania i autoryzacji i innych zadań. Każdy z tych interfejsów może stanowić powierzchnię ataku. Napastnik może na przykład uzyskać dostęp do urządzenia pamięci masowej za pośrednictwem interfejsu zarządzania API, podszywając się pod hosta zarządzającego lub oprogramowanie zarządzające. W tym przypadku napastnik nie musi przełamywać

zabezpieczeń oprogramowania zarządzającego, aby uzyskać dostęp do opcji zarządzania. Niektóre systemy zezwalają na wykorzystanie protokołów zarządzania wewnątrz pasma przy użyciu łącza danych (na przykład ścieżki Fibre-Channel) wykorzystywanego także do realizacji zadań związanych z pamięcią masową (dodatkowe omówienie płaszczyzn danych znajduje się w podrozdziale 4.2 „Ochrona danych" w dalszej części niniejszego dokumentu). Taka konfiguracja powoduje powstanie kolejnej powierzchni ataku, którą napastnik może wykorzystać podszywając się pod klienta pamięci masowej podczas wysyłania poleceń zarządzania.

3.3.5 Klienci pamięci masowej

Klienci pamięci masowej to urządzenia obliczeniowe lub aplikacje zainstalowane na urządzeniach obliczeniowych, które używają protokołu pamięci masowej do odczytu/zapisu danych z obiektu pamięci masowej lub sieci. Jeśli klient pamięci masowej zostanie skompromitowany, napastnik może uzyskać dostęp do danych używanych przez klienta, zapisać dane na urządzeniu pamięci masowej lub w obiekcie bądź na przykład zaszyfrować dane. Co więcej, jeśli dostępna jest opcja dostępu wewnątrz pasma do systemu pamięci masowej, napastnik podszywający się pod klienta pamięci masowej może wysyłać polecenia zarządzania. Systemy archiwizacji mogą czasami wykorzystywać klientów pamięci masowej w celu uzyskania dostępu do danych, by tworzyć kopie zapasowe. W przypadku kompromitacji klienta pamięci masowej, napastnik może także wpłynąć na przyszłe kopie zapasowe. W takiej sytuacji napastnik może następnie wstrzymać się z dalszymi działaniami przez pewien czas, w czasie którego zaatakowana organizacja będzie stopniowo traciła możliwość obrony przed atakiem ze względu na brak możliwości wykorzystania skompromitowanych kopii zapasowych.

3.3.6 Sieć pamięci masowej (podsłuch i zmiana w celu uzyskania dostępu)

Gdy klienci pamięci masowej pobierają dane z systemów pamięci masowej, są one przesyłane przez różne elementy sieci pamięci masowej, takie jak kontrolery pamięci masowej, karty sieciowe, przełączniki, kable i extendery. Mówimy wtedy o danych w tranzycie lub danych w trakcie przesyłu. Atak na te elementy i skuteczne naruszenie ich zasad ochrony mogą sprawić, że napastnik będzie w stanie uzyskać dostęp do strumienia danych oraz kopiować, przeglądać, przekierować lub ukraść przesyłane

dane. Ponadto atakujący może odczytać dane konfiguracyjne, polecenia zarządzania lub inne metadane, na przykład w sytuacji, w której przesyłane dane zawierają poświadczenia użytkowników, klucze szyfrowania i inne kluczowe dane. Kompromitując komponent sieciowy, napastnik może także mieć możliwość uszkodzenia, zmiany lub dodania danych poprzez modyfikację treści użytkowej. Kolejną formą ataku jest atak typu MITM (*ang. man-in-the-middle*), który może dotyczyć szerokiego zakresu protokołów transportowych i rodzajów nośników, w tym systemów opartych na protokołach Fibre-Channel, iSCSI, NVMeoF, systemów zarządzania i im podobnych. Celem ataku MITM jest podsłuchiwanie strumienia danych, zmiana danych lub obejście mechanizmów szyfrowania i uwierzytelniania.

3.3.7 Urządzenia kontrolowane przez kluczowych użytkowników

Wybrani użytkownicy otrzymują uprawnienia oraz narzędzia pozwalające na realizację zadań związanych ze zdalnym zarządzaniem infrastrukturą pamięci masowej. Administrator pamięci masowej może na przykład korzystać z jednej lub wielu stacji roboczych do zdalnego łączenia się z hostem odpowiedzialnym za zarządzanie pamięcią masową. Urządzenia, z których korzystają kluczowi użytkownicy (np. laptopy, komputery stacjonarne, sieci domowe, komputery domowe) mogą zostać wykorzystane w celu uzyskania dostępu do infrastruktury pamięci masowej i naruszenia jej zasad ochrony. Napastnik może na przykład zainstalować w takim środowisku złośliwe oprogramowanie, które pozwoli na instalację modułu „keyloggera" zapisującego wciśnięte klawisze, co umożliwi przechwycenie poświadczeń logowania. W związku z tym takie urządzenie może stanowić potencjalną powierzchnię ataku.

3.3.8 Sieć elektroenergetyczna i inne media

Ze względu na fakt, że infrastruktura pamięci masowej jest podłączona do sieci elektroenergetycznej, także ona może potencjalnie stać się powierzchnią ataku. Duży skok napięcia, który możne zostać wywołany na przykład przez wyładowanie atmosferyczne, może doprowadzić do uszkodzenia, a nawet usunięcia danych zapisanych na nośnikach elektromagnetycznych. Co więcej, fluktuacje napięcia odpowiadające naciśnięciom klawiszy powodują powstawanie szumu na przewodzie masowym. Szumy te mogą zostać przechwycone przez hakera podłączonego do pobliskiego gniazdka elektrycznego. Inna metoda ataku może opierać się na złośliwym

oprogramowaniu o nazwie *PowerHammer*, które jest w stanie przechwytywać w sposób niezauważony dane z odizolowanych od sieci telekomunikacyjnych urządzeń, wykorzystując do tego sieć energetyczną do której te urządzenia są podłączone. To złośliwe oprogramowanie przechwytuje dane ze skompromitowanego urządzenia poprzez pomiar zmian poboru prądu wynikającego z obciążania procesora. Wrażliwe dane, w tym hasła i klucze szyfrowania, mogą być wykradane bit po bicie poprzez modulowanie zmian w przepływie prądu. Wariant tego rodzaju ataku na poziomie linii elektroenergetycznej umożliwia napastnikowi przechwytywanie bitów danych uzyskiwanych przez złośliwe oprogramowanie przez kabel zasilający skompromitowanego komputera. Z kolei w wariancie ataku na poziomie przewodu fazowego atakujący zbiera dane z głównej rozdzielni elektroenergetycznej. Dane mogą być gromadzone przy pomocy bezinwazyjnego urządzenia mierzącego emisje kabli elektrycznych, a następnie przetwarzającego wynik pomiarów do postaci binarnej poprzez demodulację i dekodowanie [33].

Inne instalacje, systemy zabezpieczające oraz systemy sterujące warunkami środowiskowymi, w tym ogrzewanie, wentylacja, klimatyzacja, systemy przeciwpożarowe i gaśnicze, systemy zasilania bezprzerwowego, czujniki czy systemy nadzoru mogą wpłynąć na działanie systemów magazynowania danych, począwszy od zagrożeń dla samych systemów takich jak na przykład: przegrzanie, zalanie, wybuch, poprzez ryzyko wycieku danych w wyniku przejęcia kontroli nad systemem monitoringu wizyjnego w celu przechwycenia haseł lub zawartości ekranów, paneli, lampek sygnalizacyjnych lub rejestrowania sygnałów dźwiękowych, aż po ataki wykorzystujące moduły komunikacyjne systemów środowiskowych (np. Wi-Fi, Bluetooth) w próbach obejścia zabezpieczeń systemów odizolowanych od sieci oraz zabezpieczeń samych sieci.

4. REKOMENDACJE DOTYCZĄCE BEZPIECZEŃSTWA SYSTEMÓW PAMIĘCI MASOWEJ

W kolejnych podrozdziałach od 4.1 do 4.12 przedstawiono szereg zaleceń i wskazówek dotyczących bezpieczeństwa infrastruktury pamięci masowej. Każdy z podrozdziałów został poświęcony wybranemu aspektowi bezpieczeństwa pamięci masowych i zawiera zestaw zaleceń i wskazówek, których konwencja nazewnicza i schemat numeracji zostały zaprojektowane w sposób umożliwiający jednoznaczną identyfikację każdego z nich. Niepowtarzalne identyfikatory zostały opracowane według schematu xx-SS-Ry, gdzie „xx" stanowi połączenie dwóch liter odnoszących się do tytułu oryginalnego podrozdziału w języku angielskim, SS oznacza „bezpieczeństwo pamięci masowych" (*ang. Storage Security - SS*), z kolei „y" jest kolejną cyfrą rekomendacji (*ang. recomendation*). Na przykład w podrozdziale 4.1 zatytułowanym „Bezpieczeństwo fizyczne pamięci masowych" (*ang. „Physical Storage Security"*), kolejne identyfikatory przyjmują postać PS-SS-R1, PS-SS-R2 itd. W ramach poszczególnych rekomendacji mogą być stosowane dodatkowe identyfikatory alfabetyczne – na przykład (a) lub (b), itd. Takie rozwiązanie umożliwia umieszczanie odniesień do dodatkowych wskazówek dzięki wykorzystaniu głównego identyfikatora, na przykład „PS-SS-R1" (dotyczącego bezpieczeństwa nośników), a jednocześnie odniesienia do ich wybranych części. Przykładowo w sekcji 4.1 niniejszych zaleceń: „PS-SS-R1.a" - stosowanie zaleceń zawartych w rozdziale 3.10 publikacji specjalnej NIST SP 800-53[16]; „PS-SS-R1.b" - przestrzeganie zasad ochrony łańcucha dostaw, itd.

W wybranych przypadkach w ramach rekomendacji wykorzystywane są wypunktowane listy, gdy nie występuje potrzeba odnoszenia się do każdej pozycji listy z osobna.

4.1 Bezpieczeństwo fizyczne pamięci masowych

Bezpieczeństwo fizyczne ma fundamentalne znaczenie dla bezpieczeństwa dowolnego składnika infrastruktury IT. Większość zabezpieczeń opartych na oprogramowaniu może zostać naruszona, jeśli napastnik uzyska dostęp fizyczny do obiektu i zainstalowanych w nim urządzeń.

[16] Patrz: publikacja NSC 800-53 wer. 2, rozdział 3

Pod wieloma względami wymagania dotyczące bezpieczeństwa fizycznego infrastruktury pamięci masowej są takie same jak w przypadku innych elementów infrastruktury, takich jak komputery i urządzenia sieciowe, tj. ochrona obiektu, nadzór, transport itp. Wymagania te zostały szczegółowo opisane w wielu publikacjach, w tym NIST SP 800-53 [28], Rev5, NIST SP 800-171 [34]. Dodatkowe ważne informacje dotyczące utylizacji i niszczenia nośników zostały zawarte w normie ISO 27040 [10] oraz w publikacji NIST SP 800-88 Rev. 1 [29].

W niniejszym podrozdziale zawarte są szczegółowe rekomendacje dotyczące różnych zagadnień związanych z bezpieczeństwem fizycznym, unikalnych dla infrastruktury pamięci masowej, a także obszary, którym inne publikacje poświęcają ograniczoną ilość miejsca.

PS-SS-R1 – Działania związane z bezpieczeństwem nośników:

a. Należy przestrzegać ogólnych zaleceń zawartych w rozdziale 3.10 dokumentu NIST SP 800-53, Rev5 (dotyczących zasad, dostępu, znakowania, przechowywania, transportu, sanityzacji, szyfrowania, nośników wymiennych, poufności i utylizacji).

b. Zarządzanie cyklem życia nośników powinno obejmować zakup nośników z zapewnieniem bezpieczeństwa łańcucha dostaw.

c. W przypadku danych wrażliwych, fizyczne nośniki zawierające kopie zapasowe powinny być przechowywane w miejscu wystarczająco oddalonym od lokalizacji, w której przechowywane są dane pierwotne.

d. W przypadku danych wrażliwych należy utrzymywać kompleksowy katalog nośników pozwalający na ustalenie ich lokalizacji, własności, pojemności oraz innych istotnych danych na temat ich właściwości i konfiguracji. Szczególną uwagę należy zwrócić na katalogowanie zawartości nośników, w tym:

   - ✓ poziomu wrażliwości danych;
   - ✓ klasyfikacji (jakiego typu dane znajdują się na nośniku, do jakich aplikacji oraz usług biznesowych się odnoszą);
   - ✓ poziomu szyfrowania danych;

- ✓ potencjalnego wpływu w przypadku kompromitacji lub kradzieży (na przykład kompromitacja informacji finansowych lub medycznych; wyciek haseł, certyfikatów lub kluczy szyfrujących);
- ✓ działania lub procedury, które należy zastosować w celu ograniczenia ryzyka (na przykład zmiana haseł, zmiana kluczy szyfrujących, ponowne zaszyfrowanie danych i powiadomienie odpowiednich interesariuszy);
- ✓ zależności między danymi a inną aplikacją.

e. Należy rozważyć zastosowanie zaawansowanych metod śledzenia w przypadku nośników wymiennych zawierających wrażliwe dane, na przykład etykiety RFID (*ang. Radio-Frequency Identification*), urządzenia śledzące oparte na systemie GPS oraz zabezpieczenia antysabotażowe.

f. W przypadku danych wyjątkowo wrażliwych należy rozważyć zastosowanie samoczynnego bądź zdalnie sterowanego mechanizmu samozniszczenia nośnika. W przypadku wdrożenia takiego rozwiązania należy rozważyć szczegółowo sposób ochrony takich nośników, gdyż mogą wówczas stanowić one wektor ataku, który może zostać wykorzystany przez napastnika do zniszczenia urządzeń lub uszkodzenia pobliskiego sprzętu, zniszczenia danych lub spowodowania obrażeń personelu.

PS-SS-R2 – Ochrona wszystkich wrażliwych urządzeń administracyjnych: Wrażliwe stacje robocze, które mogą być wykorzystywane do uzyskania dostępu administracyjnego do infrastruktury pamięci masowej, powinny być zabezpieczone przy użyciu dopuszczonych i zatwierdzonych przez organizację środków bezpieczeństwa dotyczących dostępu, nadzoru i audytu, w tym zabezpieczeń fizycznych. Środki bezpieczeństwa wdrożone w celu ochrony stacji roboczych wykorzystywanych do zarządzania systemami pamięci masowej powinny być co najmniej tak samo rygorystyczne, jak zabezpieczenia wdrożone w celu ochrony danych przechowywanych przez systemy, a także systemów wykorzystujących te dane. Obejmuje to stacje robocze znajdujące się poza obiektem, w którym znajduje się system pamięci masowej, a także środowiska wykorzystywane w czasie pracy z domu, jeśli dana organizacja oferuje tę możliwość.

PS-SS-R3 – Procedury sanityzacji danych muszą obejmować kompleksowo infrastrukturę pamięci masowej, w tym jej nieewidencjonowane komponenty. Niektóre elementy, które mogą zawierać informacje wrażliwe, a które nie są nośnikami, są czasami pomijane przy utylizacji elementów infrastruktury pamięci masowej; dotyczy to między innymi pamięci nieulotnej oraz pamięci podręcznej wykorzystywanej w macierzach pamięci masowej, przełącznikach SAN, routerach i innych urządzeniach; ustawień oprogramowania układowego/BIOS i ustawień kontrolerów pamięci masowej (mogą zawierać adresy umożliwiające identyfikację organizacji, takie jak adresy IP i nazwy WWN[17] sieci SAN, konfiguracje maskowania, hasła). Należy upewnić się, że wszystkie te elementy zostały uwzględnione w procedurach sanityzacji danych organizacji i obejmują zasady, konkretne działania oraz audyt.

4.2 Ochrona danych

W podrozdziale 2.11.5 omówiono cele i związane z nimi działania w zakresie ochrony danych (*ang. Data Protection – DP*), trzy obszary oparte na zakresie celów oraz podstawowe zabezpieczenia dotyczące pamięci masowych. Zabezpieczenia te obejmują:

- tworzenie kopii zapasowych i odzyskiwanie danych,
- archiwizację,
- technologie replikacji,
- ciągłą ochronę danych,
- kopie i migawki danych.

Zalecenia dotyczące bezpieczeństwa zawarte w tym rozdziale określają kwestie związane z należytą starannością, dotyczące wdrożenia każdego z powyższych zabezpieczeń. Dodatkowe wymagania zostały zawarte w podrozdziałach 4.7 Izolacja oraz 4.8 Zapewnienie odtworzenia danych.

[17] World Wide Name (WWN) to unikalny identyfikator przypisany przez Institute of Electrical and Electronics Engineers (IEEE) producentom produktów sieciowej pamięci masowej.

Przy omawianiu różnych aspektów zarządzania pamięcią masową, dostępu, użytkowania i ochrony warto określić i rozróżnić różne **płaszczyzny danych**. Mianem płaszczyzny danych określa się zbiór metod dostępu, protokołów, komunikacji, metod kontroli dostępu oraz autoryzacji, a także działań dotyczących obiektu danych lub zbioru powiązanych obiektów danych. Należy pamiętać, że przedstawiona lista nie jest wiążąca ani wyczerpująca; niektóre z zawartych w niej działań mogą zostać pominięte, z kolei inne – na przykład zasady filtrowania, a także role i mechanizmy autoryzacji urządzeń wejścia/wyjścia mogą zostać wdrożone w zależności od potrzeb. Przykładowo, urządzenie blokowe może być związane z jedną lub wieloma z następujących płaszczyzn:

- Płaszczyzna wykorzystania danych – na potrzeby przykładu zdefiniowana jako zestaw protokołów dostępu używanych do wykonywania operacji wejścia/wyjścia, same operacje wejścia/wyjścia oraz fizyczne i logiczne połączenia sieciowe używane do wykonywania takich operacji.
- Płaszczyzna zarządzania danymi – obejmuje protokoły, operacje i dostęp do sieci używane do tworzenia i niszczenia urządzenia, konfigurowania jego atrybutów, mapowania go do hostów itp.
- Płaszczyzna ochrony danych – obejmuje protokoły, operacje i dostęp do sieci używane do replikacji, tworzenia migawek i kopii zapasowych, a także archiwizacji zawartości urządzenia.

Wybrany projekt i implementacja mogą w znacznym stopniu wpłynąć na stopień separacji pomiędzy poszczególnymi płaszczyznami. Separacja stanowi w tym wypadku sumę wielu zmiennych, w tym między innymi:

- Separacji w warstwie 2 sieci – na przykład użycie różnych wirtualnych sieci lokalnych (VLAN) zwiększy separację między płaszczyznami, podczas gdy użycie tych samych sieci VLAN spowoduje jej zmniejszenie.
- Separacja logiczna sieci – na przykład użycie oddzielnych podsieci IP zwiększy separację, natomiast użycie tej samej podsieci doprowadzi do jej zmniejszenia.

- Filtrowanie i listy kontroli dostępu (*ACL*) – dodanie ACL uniemożliwiających wykonywanie operacji zarządzania na płaszczyźnie konsumpcji danych zwiększy jej separację od płaszczyzny zarządzania danymi.
- Autoryzacja – używanie różnych kont użytkowników i ról dla każdej płaszczyzny i ograniczanie uprawnień każdej roli wyłącznie do uprawnień związanych z daną płaszczyzną.

Zasadniczo zwiększenie liczby oraz poziomu separacji płaszczyzn danych może pozytywnie wpłynąć na bezpieczeństwo zasobów danych, niosąc jednak za sobą potencjalne konsekwencje w postaci zwiększonych wymagań w zakresie zarządzania i administracji oraz sieci (dodatkowe porty przełączników, kontrolery wejścia/wyjścia itp.). W powyższym przykładzie niedostateczna separacja pomiędzy płaszczyznami konsumpcji i ochrony danych może pozwolić napastnikowi, który przejmie kontrolę nad hostem połączonym z urządzeniem blokowym, nie tylko na uszkodzenie zawartych w nim danych, ale także na uszkodzenie kopii danych oraz kopii zapasowych. Niedostateczna separacja pomiędzy płaszczyznami konsumpcji danych i zarządzania nimi może pozwolić napastnikowi na atak na inne urządzenia pamięci masowej.

4.2.1 Tworzenie kopii zapasowych i odzyskiwanie danych oraz ich archiwizacja

DP-SS-R1: Ustanowienie planu lub zasad ochrony danych przed wdrożeniem rozwiązania, obejmujących co najmniej:

a. Określenie specyfikacji poziomów, częstotliwości i liczby kopii, aby realizować cele odzyskiwania danych. Specyfikacja może obejmować więcej niż jeden poziom (np. kopie ciągłe, godzinne, dzienne, tygodniowe itd.) i w przypadku każdego poziomu powinna zawierać:
   - ✓ Częstotliwość wykonywania kopii oraz okres retencji – na przykład 48 godzinnych migawek, 30 dziennych kopii zapasowych.
   - ✓ Rodzaj kopii – na przykład pełne, przyrostowe, ciągłe (wersjonowanie plików, wysyłka i archiwizacja dzienników lub logów), replikacja, migawki itp.

b. Rodzaje nośników, które zostaną wykorzystane do tworzenia kopii.

c. Wymagania dotyczące szyfrowania dotyczące danych w stanie spoczynku (metody szyfrowania kopii zapasowych powinny być co najmniej tak bezpieczne jak szyfrowanie danych chronionych) oraz danych w czasie przesyłania. Należy również uwzględnić problem retencji oraz rotacji kluczy szyfrowania.

d. Inne wymogi dotyczące ochrony, takie jak: podpis cyfrowy, archiwizacja, lokalizacja, bezpieczeństwo obiektu (w tym ochrona przed pożarem, wybuchem i zakłóceniami magnetycznymi), niezmienność oraz zabezpieczenia fizyczne, minimalna liczba kopii na zestaw kopii zapasowych oraz rozmieszczenie geograficzne kopii zapasowych.

e. Należy uwzględnić obowiązujące przepisy i ramy regulacyjne oraz wdrożyć stosowne zabezpieczenia.

f. Należy wdrożyć kompleksowe zarządzanie cyklem życia, które obejmuje analizę istniejących kopii danych i kopii zapasowych pod kątem zasad ochrony i retencji, w tym usuwanie kopii danych, które nie są już potrzebne.

g. Procedury przywracania danych.

DP-SS-R2: Wdrożone plany lub zasady ochrony danych powinny:

a. Obejmować wszystkie zasoby danych organizacji niezależnie od tego, gdzie się znajdują (tj. w lokalnym centrum danych lub w chmurze). Dopuszczalne jest zaniechanie ochrony danych, które nie mają znaczenia dla organizacji lub takich, które mogą być odtworzone z innych chronionych źródeł danych przy zachowaniu wymaganego czasu odzyskiwania, jednak każdy taki przypadek powinien zostać udokumentowany.

b. Zostać zorganizowane według rodzaju danych, których dotyczą (np. poziom 1, poziom 2 itd.).

c. Uwzględniać kwestię integralności danych na poziomie aplikacji i procesu biznesowego (np. jeśli dwa elementy powinny zostać odtworzone do tego samego punktu w czasie, aby funkcjonować prawidłowo, należy zaplanować i wdrożyć stosowne mechanizmy spójności lub inne działania mające na celu zapewnienie takiej możliwości).

d. Uwzględnić wymaganą szybkość przywracania danych w celu zaspokojenia wymagań biznesowych lub wynikających ze stosownych przepisów, by zapewnić wdrożenie działań opartych na technologii o odpowiedniej charakterystyce (np. kopie dyskowe, migawki lub klony, taśmy magnetyczne lub odzyskiwanie danych przez sieć WAN).

DP-SS-R3: Oprócz planu lub zasad tworzenia kopii zapasowych, standardowe procedury operacyjne związane z tworzeniem kopii zapasowych powinny obejmować:

a. Monitorowanie wykonywania kopii zapasowych w oparciu o zasady i powiązane mechanizmy powiadamiania.

b. Okresowe testy kopii zapasowych (co najmniej raz w miesiącu w przypadku danych krytycznych) w celu sprawdzenia ich integralności oraz możliwości przywrócenia danych. W przypadku obszarów, w których występują rygorystyczne wymagania dotyczące szybkości przywracania danych, należy przeprowadzić testowe przywracanie całościowe (np. całkowite odzyskanie zbioru danych do środowiska odzyskiwania symulujące rzeczywiste scenariusze przywracania danych).

c. Prowadzenie aktualnego katalogu odzyskiwania obejmującego wszystkie kopie (w tym kopie zapasowe, replikacje, migawki itd.), zawierającego informacje na temat tego, jakimi narzędziami antywirusowymi zostały przeskanowane kopie i jakie były wyniki skanowania. W przypadku danych wrażliwych zaleca się ponadto okresowe skanowanie co najmniej części istniejących kopii za pomocą aktualnych narzędzi antywirusowych w celu zidentyfikowania zainfekowanych kopii. Więcej informacji znajduje się w dodatkowych wymogach dotyczących katalogowania w zaleceniu **CM-SS-R2**.

d. Okresowy przegląd (co najmniej raz w roku) planu awaryjnego i procedur operacyjnych.

e. Utrzymywanie ścieżki audytu w celu zapewnienia dostępu do informacji niezbędnych w celu zapewnienia zgodności operacji tworzenia kopii zapasowych z zasadami.

f. Stosowanie specjalnych zabezpieczeń, jeśli pojawi się taka potrzeba (np. odświeżanie kopii zawartych na starych, zagrożonych lub wycofanych nośników poprzez wykonywanie nowych kopii itd.).

DP-SS-R4: Zarządzanie konfiguracją ochrony danych (w tym kopiami zapasowymi, migawkami oraz replikacją) powinno odbywać się na szczeblu centralnym i powinno być oddzielone od płaszczyzny konsumpcji danych. Serwery i urządzenia klienckie nie powinny mieć możliwości dokonywania zmian dotyczących konfiguracji ochrony danych. Powyższej zasady nie należy interpretować jako wykluczenia mechanizmów redundancji, które chronią przed ryzykiem wystąpienia pojedynczych punktów podatności na awarię.

4.2.2 Replikacja i kopie lustrzane

DP-SS-R5: Zarówno w przypadku zastosowania replikacji synchronicznej, jak i asynchronicznej należy stosować ten sam poziom ochrony danych (np. szyfrowanie danych w spoczynku, ograniczenia dostępu) w podstawowym systemie pamięci masowej oraz w systemie zapasowym.

DP-SS-R6 – Eliminacja powiązań związanych z replikacją pomiędzy urządzeniami pamięci masowej: Gdy macierze nie mają współdzielonych woluminów replikowanych, należy wyłączyć uprawnienia pozwalające na replikację pomiędzy tymi macierzami. Jeśli macierze mają współdzielone woluminy replikowane, ich uprawnienia względem siebie powinny być ograniczone do współdzielonych woluminów.

DP-SS-R7: Poufność i integralność przesyłanych danych podczas replikacji i tworzenia kopii lustrzanych powinny być chronione za pomocą szyfrowania. Zalecenie to można złagodzić, jeżeli zostały wdrożone stosowne zabezpieczenia (np. tworzenie kopii lustrzanych w ramach tej samej „obudowy" lub serwerowni itp.). Dodatkowe informacje znajdują się w zaleceniu **EN-SS-R8**.

DP-SS-R8: Należy włączyć automatyczne zawieszenie operacji wejścia/wyjścia w przypadku replikacji synchronicznej we wszystkich sytuacjach, w których nie można pozwolić, aby replikowane dane były starsze niż ich pierwotna kopia. Włączenie tej funkcji oznacza, że podstawowe urządzenie pamięci masowej nie zezwoli na żadne operacje zapisu na magazynowanych danych w przypadku utraty synchronizacji

z zapasowym serwerem danych, a przetwarzanie zostanie wznowione dopiero po przywróceniu synchronizacji. Włączenie tej funkcji wiąże się z wprowadzeniem dodatkowego wektora ataku – napastnik, który wie o jej włączeniu lub podejrzewa, że może być używana, może przypuścić atak odmowy świadczenia usługi na podstawową pamięć masową poprzez zaatakowanie sieci realizującej replikację. Z tego powodu należy rozważyć za i przeciw włączeniu tej funkcji.

DP-SS-R9: Przestarzałe repliki danych powinny zostać usunięte, aby ograniczyć powierzchnię ataku.

4.2.3 Punkty przywracania

Pojęcie „punkty przywracania" obejmuje szereg mechanizmów kopiowania danych wykorzystywanych przez rozwiązania pamięci masowej, które mogą być stosowane do tworzenia kopii oryginalnych danych w postaci, w jakiej występowały one w danym czasie. Obejmuje także wbudowane narzędzia do tworzenia kopii (często określane przez producentów mianem migawek, klonów itp.), kopie na poziomie systemu plików, kopie na poziomie bazy danych, kopie pamięci masowej w chmurze itp.

DP-SS-R10: Jeśli punkty przywracania lub na przykład migawki są wykorzystywane w harmonogramie tworzenia kopii zapasowych, należy je odpowiednio skonfigurować:

a. Konfiguracja powinna umożliwić spełnianie wymagań dotyczących punktu odtworzenia danych (RPO) docelowych zbiorów danych w migawce. Na przykład, jeśli standardy biznesowe lub wymogi przepisów określają, by w wyniku odzyskania nie doszło do utraty więcej niż pięciu minut danych, wówczas przedział czasowy pomiędzy wykonywaniem kolejnych migawek powinien wynosić pięć minut lub mniej.

b. Konfiguracja powinna gwarantować spełnienie wymagań dotyczących retencji danych. Na przykład, jeśli wymogi dotyczące retencji określają konieczność utrzymywania kopii godzinnych sięgających co najmniej 48 godzin wstecz, należy zapewnić przechowywanie wystarczającej liczby migawek godzinnych.

DP-SS-R11: Przestarzałe migawki i klony powinny zostać usunięte, aby ograniczyć powierzchnię ataku.

4.2.4 Ciągła ochrona danych

DP-SS-R12 – Względy bezpieczeństwa w przypadku zastosowania ciągłej ochrony danych (CDP): Poza korzyściami funkcjonalnymi (takimi jak na przykład poprawa RPO czy lepsza retencja), zastosowanie technik ciągłej ochrony danych takich jak CDP, kontrola wersji danych źródłowych lub replik w przypadku przechowywania plików i obiektów w chmurze, a także przesyłanie dzienników transakcji, może również pomóc w analizie ataków na dane wrażliwe. Choć takie działania mogą pochłaniać wiele czasu, odtwarzanie poprzednich wersji danych pozwala na uzyskanie dodatkowych informacji na temat profilu ataku, czasu jego wystąpienia i innych czynnikach.

4.3 Uwierzytelnianie i kontrola dostępu do danych

Systemy infrastruktury pamięci masowej są administrowane przez wyznaczonych użytkowników, którzy korzystają z różnych kont w celu uzyskiwania dostępu do tych systemów. Administratorzy oraz wykorzystywane przez nich urządzenia stanowią ważną powierzchnię ataku, która może być wykorzystana przez napastników. Z racji tego, że osoby zarządzające systemami pamięci masowej i infrastrukturą są zazwyczaj użytkownikami uprzywilejowanymi, przyznawanie dostępu do uprzywilejowanych kont użytkowników oraz korzystanie z tych uprawnień powinny być ograniczone i kontrolowane. Niewłaściwe wykorzystanie uprawnień administracyjnych może być głównym czynnikiem wpływającym na wystąpienie awarii lub ataku na system pamięci masowej.

Należy wdrożyć model oparty na ograniczonych uprawnieniach i wyznaczonych rolach użytkowników. Zgodnie z normą ISO/IEC 27040 [10] w ramach technologii pamięci masowych należy wdrożyć i stosować następujące role:

- **Administrator bezpieczeństwa –** użytkownik w tej roli ma uprawnienia do przeglądania oraz zmiany ustawień związanych z tworzeniem oraz zarządzaniem kontami użytkowników, przypisywaniem ról oraz uprawnień użytkownikom oraz administratorom, a także tworzeniem zasad dotyczących poświadczeń (np. wspólnych kluczy tajnych – *ang. shared secret*), zarządzaniem certyfikatami oraz kluczami, zarządzaniem szyfrowaniem oraz kluczami szyfrowania, zarządzania ścieżką audytu oraz dziennikami, a także ustawień związanych z kontrolą dostępu.

- **Administrator pamięci masowej –**użytkownik w tej roli ma uprawnienia do przeglądania oraz zmiany ustawień dotyczących wszystkich aspektów działania systemu pamięci masowej. Użytkownik nie ma dostępu do elementów lub danych związanych z bezpieczeństwem systemu.
- **Audytor bezpieczeństwa –**użytkownik w tej roli ma uprawnienia do przeglądania informacji oraz danych pozwalających na weryfikację uprawnień, parametrów i konfiguracji zabezpieczeń oraz przegląd dzienników audytu. Użytkownik nie ma dostępu do pamięci masowej, konfiguracji ani danych.
- **Audytor pamięci masowej –**użytkownik w tej roli ma uprawnienia do przeglądania informacji oraz danych pozwalających na weryfikację parametrów i konfiguracji pamięci masowej, a także inspekcję dzienników stanu pamięci masowej lub awarii. Użytkownik nie ma dostępu do elementów lub danych związanych z bezpieczeństwem systemu.

4.3.1 Zalecenia dotyczące uwierzytelniania

AC-SS-R1 – Unikatowe identyfikatory dla wszystkich użytkowników: Wszyscy użytkownicy (w tym administratorzy) powinni posiadać unikatowe identyfikatory przeznaczone wyłącznie do ich osobistego użytku. Identyfikatory przypisane administratorom powinny spełniać wymagania trzeciego poziomu wiarygodności tożsamości (*ang. identity assurance level - IAL 3*) określone w podrozdziałach 4.2 i 4.5 dokumentu NIST SP 800-63A[18] [35]. Jedynym wyjątkiem jest konto do użytku awaryjnego; zasady jego bezpiecznego użytkowania zostały omówione w zaleceniu AC-SS-R16. Zasada ta jest niezwykle ważna z punku widzenia rozliczalności i audytu, a także ze względu na możliwość wprowadzenia zasad kontroli dostępu na poziomie pojedynczego użytkownika.

AC-SS-R2 – Scentralizowane rozwiązanie uwierzytelniające: W środowiskach charakteryzujących się większą skalą należy wdrożyć scentralizowane rozwiązanie uwierzytelniające (takie jak Active Directory, Lightweight Directory Access Protocol [LDAP], pojedyncze logowanie [SSO], zatwierdzone przez organizację usługi

[18] Lub innym standardzie określającym wymagania stawiane przed identyfikatorem przypisanym administratorowi.

uwierzytelniania oparte na chmurze), aby umożliwić ścisłe monitorowanie i kontrolę dostępu użytkowników do zasobów pamięci masowej oraz zapewnić jednolite egzekwowanie zasad uwierzytelniania obowiązujących w organizacji. Należy unikać korzystania z wbudowanych funkcji uwierzytelniania i zarządzania uprawnieniami, a najlepiej je wyłączyć.

AC-SS-R3 – Konfiguracja serwerów uwierzytelniania:

a. Proces wyznaczania serwerów odpowiedzialnych za realizację usług uwierzytelniania powinien być ściśle kontrolowany, a ich działanie powinno być okresowo weryfikowane i sprawdzane w celu wykrycia i uniemożliwienia wprowadzenia jakichkolwiek nieautoryzowanych serwerów uwierzytelniania do sieci.

b. Należy wdrożyć wiele serwerów uwierzytelniania, aby zapewnić pełną dostępność i uniknąć pojedynczych punktów awarii.

AC-SS-R4 – Bezpieczne połączenie z centralnym serwerem uwierzytelniania: Cała komunikacja pomiędzy scentralizowanym serwerem uwierzytelniania a klientami powinna być zabezpieczona poprzez najnowocześniejsze protokoły takie jak Transport Layer Security (TLS) 1.2 lub nowsze.

AC-SS-R5 – Stosowanie uwierzytelniania wieloskładnikowego: Konfiguracja dostępu do elementów infrastruktury pamięci masowej, w których przechowywane są dane krytyczne, powinna być chroniona z wykorzystaniem uwierzytelniania dwuskładnikowego obejmującego dodatkowy czynnik uwierzytelniający spełniający wymagania określone w rozdziale 5.1.9 dokumentu NIST SP800-63B[19] [36]. Wymóg ten powinien być obowiązkowy dla użytkowników przypisanych do ról Administrator Bezpieczeństwa oraz Administrator Pamięci Masowej.

4.3.2 Zalecenia dotyczące haseł

AC-SS-R6 – Zasady dotyczące bezpiecznych haseł powinny obejmować konta serwisowe: Zasady dotyczące bezpiecznych haseł powinny być stosowane nie tylko w przypadku kont użytkowników, ale także kont serwisowych odpowiedzialnych za usługi takie jak Simple Network Management Protocol (SNMP), Network Data

[19] Lub innym standardzie określającym wymagania stawiane przed uwierzytelnianiem wieloskładnikowym.

Management Protocol (NDMP), a także kont wykorzystywanych przez narzędzia automatyzacji. Hasła powinny spełniać co najmniej wymagania dla zapamiętywanych sekretów[20] przedstawione w podrozdziale 5.1.1 dokumentu NIST SP800-63B [36]. Ponadto hasła powinny spełniać następujące wymagania.

AC-SS-R7 – Długość hasła: Dobre hasło powinno składać się z co najmniej 15, a najlepiej 20 znaków.

AC-SS-R8 – Złożoność hasła: Dobre hasło powinno zawierać duże i małe litery, cyfry oraz znaki specjalne. Nie powinno być podobne do nazwy użytkownika i nie powinno zawierać powtarzających się sekwencji znaków.

AC-SS-R9 – Wygaśnięcie hasła: Dla wszystkich haseł należy ustawić czasy wygaśnięcia. W przypadku kont administratorów czas wygaśnięcia hasła powinien być krótszy niż w przypadku kont użytkowników.

AC-SS-R10 – Ponowne użycie hasła: Użytkownikom należy uniemożliwić ponowne użycie co najmniej czterech poprzednich haseł, w zależności od czynników ryzyka występujących w danej organizacji.

AC-SS-R11 – Przechowywanie haseł w pamięci podręcznej:

a. Hasła nie powinny być przechowywane w pamięci podręcznej serwerów, komputerów ani innych systemów.

b. Należy skonfigurować mechanizmy i zabezpieczenia gwarantujące szybką propagację zmian w całej sieci, na przykład odpowiednio krótki „czas życia" (*ang. Time to Live – TTL*).

AC-SS-R12 – Zapisywanie haseł: Hasła nie powinny być nigdzie zapisywane otwartym tekstem (np. w plikach) ani umieszczane w skryptach. Nie należy także włączać opcji pozwalających aplikacjom do zarządzania pamięcią masową zapamiętywania użytkowników i haseł w celu automatycznego logowania, nawet jeśli hasła są przechowywane w formie zaszyfrowanej; chyba że są zarządzane za pośrednictwem autoryzowanej centralnej usługi uwierzytelniania, takiej jak LDAP SSO.

[20] Ciąg znaków (liter, cyfr i innych symboli), który jest używany do uwierzytelniania tożsamości, weryfikacji uprawnień dostępu lub do uzyskiwania kluczy kryptograficznych.

AC-SS-R13 – Wyłączenie lub zmiana domyślnych haseł: Domyślne hasła, które są konfigurowane w czasie instalacji systemu lub jego wdrożenia, powinny zostać niezwłocznie zmienione.

4.3.3 Zalecenia dotyczące zarządzania kontami

AC-SS-R14 – Korzystanie z kont, które nie są przypisane do użytkowników systemu: Wszelkie konta, które nie są przypisane do konkretnych użytkowników systemu, w tym konta, które nie znajdują się w Active Directory, takie jak: „guest", „anonymous" czy „nobody", powinny zostać wyłączone. W sytuacjach, w których tego rodzaju konta muszą być używane, nie powinny być przypisane do żadnego użytkownika systemu, a wszystkie domyślne konfiguracje (np. hasło, uprawnienia) powinny być zmienione zgodnie z zasadami obowiązującymi w organizacji.

AC-SS-R15 – Blokada konta: Konta użytkowników powinny być blokowane po określonej liczbie nieudanych prób logowania. Niektóre implementacje blokad kont obejmują automatyczne resetowanie hasła (odblokowanie konta) po określonym czasie lub po wyłączeniu i przywróceniu zasilania. Automatyczne resetowanie nie powinno być dozwolone w przypadku wrażliwych systemów pamięci masowej.

AC-SS-R16 – Lokalne konto użytkownika do celów awaryjnych: W celu zapewnienia dostępu do zasobów pamięci masowej należy utrzymywać jedno lokalne konto użytkownika, aby w razie awarii scentralizowanego systemu uwierzytelniania zapewnić dostęp w sytuacjach awaryjnych. Konfiguracja konta powinna być zgodna ze wszystkimi zasadami obowiązującymi w organizacji, dotyczącymi między innymi długości hasła. Co więcej, korzystanie z tego konta powinno być dozwolone wyłącznie w odpowiednio zabezpieczonym miejscu i zgodnie z udokumentowanymi procedurami obejmującymi zezwolenie na użycie konta przez odpowiednie osoby oraz udokumentowanie informacji o jego użyciu.

AC-SS-R17 – Usunięcie lub wyłączenie domyślnych kont użytkowników: Domyślne konta użytkowników konfigurowane w czasie instalacji systemów pamięci masowej powinny zostać niezwłocznie usunięte lub wyłączone, jeśli istnieje taka możliwość.

Gdy funkcja wyłączenia lub usunięcia konta nie istnieje lub istnieje uzasadniony powód utrzymania któregoś z tych kont, uprawnienia przypisane do tego konta powinny być ograniczone do niezbędnego minimum.

AC-SS-R18 – Ograniczenie lokalnych i domyślnych kont użytkowników: W miarę możliwości należy uniemożliwić korzystanie z kont lokalnych i domyślnych.
W sytuacjach, w których nie jest to możliwe:

a. Należy ograniczyć korzystanie z takich kont oraz przypisane do nich uprawnienia.

b. Zasady dotyczące haseł powinny obejmować wszystkie konta użytkowników, w tym konta lokalne i domyślne, w szczególności konta z przypisanymi uprawnieniami administracyjnymi.

4.3.4 Zalecenia dotyczące zarządzania uprawnieniami i sesjami

AC-SS-R19 – Konfiguracja ról i obowiązków: Należy wdrożyć co najmniej cztery role opisane w normie ISO ISO/IEC 27040 [10] obejmujące dostęp do zasobów pamięci masowej (tj. Administrator Bezpieczeństwa, Administrator Pamięci Masowej, Audytor Bezpieczeństwa, Audytor Pamięci Masowej) – dodatkowe informacje znajdują się w podrozdziale 4.2. Systemy pamięci masowej, które oferują tylko jeden lub dwa poziomy dostępu lub uprawnień, nie powinny być wykorzystywane do przechowywania danych wrażliwych, chyba że dostępne są dodatkowe zabezpieczenia zapewniające równoważną funkcjonalność. Cały ruch związany z zarządzaniem systemem może być przekierowywany przez hosta proxy lub bramę zarządzania z zainstalowanymi narzędziami zarządzania uprawnieniami, aby ograniczyć możliwości użytkowników w zależności od przypisanej roli.

AC-SS-R20 – Przestrzeganie zasady podziału obowiązków podczas nadawania uprawnień rolom oraz przypisywania ról użytkownikom: Krytycznym aspektem bezpieczeństwa pamięci masowej jest oddzielenie płaszczyzn administracji (więcej informacji znajduje się w podrozdziale 4.2, Ochrona danych). Jeśli napastnicy przejmą kontrolę nad hostem lub uzyskają uprawnienia administratora hosta, nie powinni być w stanie w prosty sposób uzyskać dostępu do zasobów danych, kopii zapasowych i replik. Stosowne rozwiązania obejmują co najmniej następujące zasady:

a. Uprawnienia wymagane do *zarządzania danymi* (np. tworzenie i mapowanie wolumenu lub współdzielenia) oraz *ochrony danych* (np. konfigurowanie, zatrzymywanie i usuwanie kopii zapasowych) powinny być przypisane do różnych ról, które nie powinny być przypisane temu samemu użytkownikowi.

b. Uprawnienia wymagane do *zarządzania danymi* i *administrowania hostem* (np. zadania takie jak tworzenie/usuwanie obiektów w kontrolerze pamięci masowej) powinny być przypisane do różnych ról, które nie powinny być przypisane temu samemu użytkownikowi.

AC-SS-R21 – Przywileje przypisane do każdej roli powinny być zgodne z zasadą minimalnych uprawnień: Uprawnienia przypisane danej roli nie powinny być większe niż uprawnienia wymagane do realizacji zadań związanych z daną rolą. W kontekście pamięci masowej uprawnienia te dotyczą dostępu do zasobów związanych z pamięcią masową, takich jak urządzenia blokowe, pliki, obiekty itp.

AC-SS-R22 – Zarządzanie bezpieczną sesją: Wszystkie sesje pomiędzy klientem a systemem infrastruktury pamięci masowej powinny być zarządzane w oparciu o wymagany poziom pewności uwierzytelnienia zgodny z wymaganiami zawartymi w rozdziale 7 dokumentu [63B], w tym z wymogami dotyczącymi zakończenia sesji oraz automatycznego wylogowania użytkowników.

AC-SS-R23 – Wdrożenie powiadomienia typu „wiadomość dnia" oraz informacji dotyczącej logowania: Powiadomienie typu „wiadomość dnia" oraz informacja dotycząca logowania (baner logowania) powinny być wyświetlane przed każdym logowaniem do dowolnego elementu infrastruktury pamięci masowej lub systemu za pośrednictwem interfejsu użytkownika (*ang. User Interface - UI*), wiersza poleceń (*ang. Command Line Interface - CLI*) lub API (jeśli dotyczy). Komunikat powinien zawierać informację prawną oraz ostrzeżenie, że użytkownik uzyskuje dostęp do zabezpieczonego systemu zawierającego wrażliwe dane, a także wszelkie dodatkowe ostrzeżenia i informacje zgodnie z zasadami bezpieczeństwa i prywatności organizacji.

4.3.5 Zalecenia dotyczące rozwiązań SAN

Zagadnienie kontroli dostępu do rozwiązań SAN obejmuje wiele aspektów. Niektóre z nich pokrywają się z zagadnieniami takimi jak konfiguracja sieci (*ang. Network*

Configuration) i dostęp administracyjny *(ang. Administrative Access*), które są omówione w innych podrozdziałach.

W celu uniknięcia zbędnych powtórzeń:

- Zalecenia dotyczące kontroli dostępu ściśle związane z *infrastrukturą sieciową* (np. konfiguracja przełączników, portów, kontrolerów pamięci masowej i kart sieciowych; dodatkowe rekomendacje dotyczące podziału na strefy) oraz *protokołami* zostały omówione w podrozdziale 4.6. Szyfrowanie przesyłanych danych (jeden z mechanizmów kontroli dostępu) zostało umówione w podrozdziale 4.9.
- Dostęp administracyjny został omówiony w podrozdziale 4.10.
- Kontrola dostępu związana z danymi jest omówiona w niniejszym podrozdziale i obejmuje kontrolę dostępu do urządzeń blokowych, wdrożenie podziału na strefy i specyfikację kontroli dostępu w związku z podłączeniem do sieci szkieletowej.

Aby w pełni zrozumieć wszystkie zagadnienia związane z kontrolą dostępu, należy zapoznać się z treścią wszystkich trzech wymienionych podrozdziałów.

AC-SS-R24 – Kontrola dostępu do urządzeń blokowych: Zbiór hostów, które mogą uzyskać dostęp do urządzeń pamięci masowej SAN, powinien być ograniczony poprzez podział na strefy (programowy lub sprzętowy) i maskowanie zgodnie z zasadą minimalnych uprawnień.

AC-SS-R25 – Kontrola dostępu do kopii i replik urządzeń blokowych: Zbiór hostów, które mogą uzyskać dostęp do zbioru replikowanych urządzeń blokowych, migawek i innych rodzajów kopii urządzeń blokowych, powinien być ograniczony poprzez podział na strefy i maskowanie zgodnie z zasadą minimalnych uprawnień. W wielu przypadkach host, który ma dostęp do urządzenia, nie powinien mieć dostępu do jego kopii.

AC-SS-R26: Uprawnienia w przypadku domyślnej strefy, której konfiguracja może różnić się w zależności od urządzenia, powinny zawsze zostać skonfigurowane w trybie „odrzuć wszystkie" (*ang. „deny all"*).

AC-SS-R27: Podział na strefy w topologii „switched fabric" powinien być realizowany w oparciu o zasady logiki, w szczególności w kwestii separacji środowisk i rodzaju

ruchu, które powinny być rozdzielone w największym możliwym stopniu, na podstawie:

a. rodzaju środowiska – np. *rozwojowe*, *testowe*, *produkcyjne* itd.;

b. rodzaju ruchu – np. dostęp do danych, zarządzanie, replikacja, tworzenie kopii zapasowych itp.;

c. rodzaju hostów – np. *zwirtualizowane*, *fizyczne*;

d. rodzaju urządzenia pamięci masowej – np. *Taśma*, *dysk*.

AC-SS-R28: W przypadku wdrożenia podziału na strefy przy użyciu oprogramowania, poszczególne hosty powinny mieć możliwość łączenia się wyłącznie z urządzeniami pamięci masowej udostępnianymi przez prosty serwer nazw (*ang. simple name server – SNS*) poprzez wyszukanie ich w tabeli stref, nie zaś bezpośrednio przy użyciu funkcji wykrywania urządzeń.

AC-SS-R29 – Kontrolowanie urządzeń, które mogą dołączyć do sieci szkieletowej: W stosownych przypadkach należy wykorzystać funkcję tworzenia zasad, która umożliwia tworzenie dozwolonej listy przełączników, macierzy i hostów, które mogą dołączyć do sieci szkieletowej SAN.

4.3.6 Zalecenia dotyczące dostępu do plików i obiektów

AC-SS-R30 - Ograniczenie dostępu do danych dotyczących przechowywania wszystkich rodzajów obiektów (na przykład plików oraz obiektów) do niezbędnego minimum.

Należy przestrzegać zasady minimalnych uprawnień:

a. Dostęp do danych dotyczących przechowywania obiektów przy użyciu dowolnego protokołu (np. CIFS, SMB, NFS, a także protokołów wykorzystywanych w chmurach publicznych) powinien być ograniczony na podstawie adresu IP klienta oraz podsieci, z kolei porty/protokoły powinny być wymagane.

b. Jeśli taka opcja jest dostępna, należy również wdrożyć bardziej szczegółowe mechanizmy kontroli dostępu (np. według roli, identyfikatora, etykiet, kont, wirtualnej chmury prywatnej, urządzeń końcowych wirtualnej chmury prywatnej i innych aspektów).

c. Dostęp powinien być przyznawany wyłącznie użytkownikom i rolom centralnie zarządzanym, na przykład rolom znajdującym się w katalogach głównych lub autoryzowanym usługom komercyjnym, nie zaś lokalnym użytkownikom konkretnego systemu.

d. Domyślną zasadą dostępu do dowolnego udziału powinna być odmowa dostępu („deny all") lub równoważna opcja.

e. Domyślnie skonfigurowane współdzielenia powinny zostać wyłączone lub usunięte. Jeśli istnieje określony powód, który wymaga ich wykorzystania, uprawnienia dostępu powinny być ograniczone do wymaganego minimum.

f. Prawa dostępu (np. odczyt, zapis, wykonanie, modyfikacja, usunięcie, przeglądanie ACL, zmiana ACL), powinny być przydzielane indywidualnie zgodnie z zasadą wiedzy koniecznej.

g. Jeżeli dostępna jest funkcja określania ACL dla pamięci masowej obiektów, należy ją wykorzystać wraz z ustawieniami uprawnień użytkownika, grupy lub administratora dostępnymi w systemie operacyjnym.

h. Jeśli dostępna jest funkcja określania zasad dostępu do poszczególnych plików, należy ją wykorzystać, a także zaimplementować funkcję wykrywania naruszeń, która pozwoli na przesyłanie powiadomień w wypadku naruszeń.

AC-SS-R31 – Konta użytkowników, które nie wymagają uwierzytelnienia, powinny zostać wyłączone – dotyczy to kont takich jak Anonymous, null, guest oraz kont publicznych. Wyjątkiem może być zezwolenie na działanie funkcji krytycznych dla organizacji, takich jak wykrywanie urządzeń w sieci; w takich przypadkach tego rodzaju konta użytkowników powinny zostać przydzielone do grupy „nobody", nie zaś do grupy „ID 0".

AC-SS-R32 – Przeprowadzanie regularnych kontroli wszystkich wymienionych powyżej ustawień zabezpieczeń dla przechowywanych danych wszystkich rodzajów (np. plików, obiektów), aby upewnić się, że nie występują żadne odstępstwa. Wyniki kontroli powinny być udokumentowane.

AC-SS-R33 – Skanowanie w czasie dostępu do plików zawierających wrażliwe dane przy pomocy narzędzi antywirusowych: Za każdym razem, gdy uzyskuje się dostęp do pliku zawierającego dane wrażliwe należy w pierwszej kolejności przeskanować plik za pomocą zatwierdzonych przez organizację narzędzi antywirusowych, aby upewnić się, że nie został on skompromitowany.

AC-SS-R34 – Szczegółowe przydzielanie uprawnień: W przypadku systemów udostępniających pliki i obiekty (na przykład za pośrednictwem protokołów NFS, CIFS lub pamięci masowej w chmurze) uprawnienia powinny być przyznawane szczegółowo (np. do poszczególnych plików lub obiektów, nie zaś do folderów; do etykiet, nie zaś do udziałów lub pojemników).

AC-SS-R35 – Zabezpieczenie protokołu NFS poprzez ograniczenie dostępu użytkownika poziomu root: Zabezpieczenie obejmuje użycie opcji „nosuid”[21] i unikanie użycia opcji „no_root_squash”, aby zapobiec wykonywaniu programów jako użytkownik poziomu root na kliencie i modyfikowaniu współdzielonych plików przez zdalnych użytkowników poziomu root. Klienci NFS nie powinni mieć możliwości uruchamiania programów „suid” i „sgid” na eksportowanych systemach plików.

AC-SS-R36: W przypadku protokołu NFS, dla plików, które mają być używane w trybie „tylko do odczytu”, konfiguracja montowania dla stosownych udziałów NFS powinna zawsze obejmować opcję „noexec”.

AC-SS-R37 – Eksport administracyjnych systemów plików nie powinien być dozwolony: Obejmuje to systemy plików „/” oraz zastrzeżone foldery systemowe systemu operacyjnego lub macierzy pamięci masowej.

AC-SS-R38 – Gdy używany jest protokół CIFS, nie należy przyznawać uprawnień pełnej kontroli („Full Control”) żadnemu użytkownikowi, ponieważ osoba posiadająca takie uprawnienia może wykorzystać je do modyfikacji uprawnień, co skutkuje ich wyciekiem.

AC-SS-R39 – Należy stosować ochronę obiektów przed nieautoryzowanym usunięciem: W przypadku danych wrażliwych, należy w miarę możliwości stosować zaawansowane zabezpieczenia, aby zapobiec nieautoryzowanemu usunięciu obiektów.

[21] „nosuid” oznacza zablokowanie działania bitów „suid” oraz „sgid”.

Takie zabezpieczenia mogą stanowić na przykład wymuszanie uwierzytelniania wieloskładnikowego do usuwania obiektów lub blokada obiektów przed usunięciem.

4.4 Dzienniki audytu

Składniki infrastruktury pamięci masowej generują wpisy do dziennika zdarzeń dla wielu transakcji lub zdarzeń. Wpisy w dzienniku zdarzeń muszą być w jakiś sposób rejestrowane w celu zapisywania informacji na temat zdarzeń. Z punktu widzenia bezpieczeństwa oraz zgodności z przepisami ważne jest, aby gromadzić informacje z dzienników zdarzeń, które są niezbędne do udowodnienia przeprowadzenia wybranych operacji (np. szyfrowania i retencji danych), egzekwowania odpowiedzialności i identyfikowalności, spełnienia wymogów dowodowych oraz odpowiedniego monitorowania systemów. Taki podzbiór zdarzeń rejestrowanych w dziennikach zdarzeń określa się mianem dziennika audytu.

Następujące zdarzenia są istotne dla celów bezpieczeństwa:

- **Zdarzenia związane z zarządzaniem –** na przykład resetowanie haseł użytkowników, tworzenie oraz usuwanie kont, modyfikacja uprawnień, zmiany ról, zmiany przynależności do grup, działania wykorzystujące uprawnienia, tworzenie bądź zmiany konfiguracji. Takie zdarzenia należy rejestrować w każdym przypadku.
- **Zdarzenia związane z bezpieczeństwem** – na przykład zmiany w profilach użytkowników i konfiguracji zabezpieczeń, nieudane bądź zablokowane próby połączenia, zablokowane logowania. Te zdarzenia są najczęściej przedmiotem zainteresowania, choć niektóre z nich mogą pokrywać się ze zdarzeniami związanymi z zarządzaniem.
- **Zdarzenia związane z dostępem do danych –** takie dane mogą okazać się istotne w przypadku reagowania na incydenty oraz monitorowania danych wrażliwych, na przykład w celu określenia jakie dane zmodyfikował napastnik.

Gromadzenie niedostatecznych danych o zdarzeniach oraz niedostateczna analiza informacji związanych z bezpieczeństwem pozwalają napastnikom ukryć swoje działania, wykorzystywane złośliwe oprogramowanie i operacje realizowane na maszynach ofiar. Nawet jeśli ofiary wiedzą, że ich systemy zostały skompromitowane,

bez odpowiednio zabezpieczonych oraz kompletnych dzienników nie jest możliwe ustalenie szczegółów ataku, a także obserwowanie kolejnych działań napastników. Brak kompleksowych dzienników audytu może sprawić, że atak może pozostać niezauważony przez dowolny czas, a wyrządzone szkody mogą być nieodwracalne. W niektórych przypadkach informacje w plikach dziennika są jedynym dowodem na udany atak. Wiele organizacji prowadzi dzienniki audytu w celu zapewnienia zgodności z przepisami, ale atakujący wykorzystują fakt, że ich pracownicy rzadko sprawdzają pliki dziennika, w związku z czym nie wiedzą, że ich systemy zostały skompromitowane. Z powodu niedostatecznych lub nieistniejących procesów analizy plików dziennika, napastnicy czasami kontrolują maszyny ofiar przez miesiące lub lata bez wiedzy jakichkolwiek przedstawicieli organizacji, nawet jeśli dowody ataku znajdują się w plikach dziennika.

Ze względu na to, jak kluczowe są dane zawarte w dziennikach zdarzeń dla wykrywalności ataków oraz ich analizy, poniżej przedstawiono zalecenia dotyczące bezpieczeństwa w zakresie wdrażania możliwości tworzenia dzienników audytu (*ang. audit logging - AL*).

AL-SS-R1 – Opcja tworzenia dzienników audytu powinna być włączona w przypadku wszystkich elementów infrastruktury pamięci masowej, wraz z odpowiednimi zabezpieczeniami i bezpiecznymi protokołami.

AL-SS-R2 – Niezawodna synchronizacja czasu z serwerem zewnętrznym: Usługa protokołu synchronizacji czasu (*ang. Network Time Protocol - NTP*) jest krytyczna dla synchronizacji czasu. W przypadku wyłączenia usługi NTP w systemach mogą wystąpić rozbieżności znaczników czasowych opisujących poszczególne komunikaty, zdarzenia oraz alarmy, a także rozbieżności czasu w różnych urządzeniach, co może uniemożliwić przeprowadzenie analiz plików dziennika, powiązanie faktów, wykrywanie anomalii oraz analizę ataku. Wybór i wykorzystanie jednego dokładnego źródła czasu w całym środowisku umożliwia zapewnienie, że zapisy zdarzeń z różnych źródeł mogą być ze sobą skorelowane. Poniżej przedstawiono zalecenia dotyczące wdrażania i integracji protokołu NTP z urządzeniami pamięci masowej:

a. Usługa NTP powinna być włączona na wszystkich urządzeniach (w tym na serwerach gromadzących pliki dziennika oraz elementach infrastruktury pamięci masowej).

b. Wszystkie urządzenia powinny być skonfigurowane w taki sposób, by synchronizowały czas lokalny z serwerem źródła czasu, na przykład z serwerem NTP.

c. Należy monitorować synchronizację czasu na wszystkich urządzeniach; kontrola powinna obejmować sprawdzanie czy usługa jest aktywna, czy w każdym urządzeniu skonfigurowane są zatwierdzone przez organizację serwery czasu, a alerty dotyczące wykrytych anomalii powinny być sprawdzane możliwie niezwłocznie i z najwyższym priorytetem.

d. Należy zapewnić redundancję serwerów czasu poprzez wdrożenie co najmniej trzech zsynchronizowanych serwerów czasu w różnych lokalizacjach geograficznych.

e. Uwierzytelnienie serwera czasu powinno opierać się na certyfikatach.

f. Opcje kontroli dostępu, takie jak ograniczenia dostępu do usługi NTPdaemon[22] (ntpd), powinny być wykorzystane do ograniczenia dostępu do serwerów czasu.

AL-SS-R3 – Centralizacja gromadzenia plików dziennika: Gromadzenie plików dziennika na centralnych serwerach (takich jak na przykład serwer syslog bądź usługi logowania w chmurze) ogranicza ryzyko utraty lub zmiany tych plików, ponieważ są one bardziej bezpieczne w sieci wewnętrznej. Poniżej przedstawiono zalecenia dotyczące wdrażania centralnego gromadzenia plików dziennika oraz integracji takich rozwiązań z urządzeniami związanymi z pamięcią masową:

a. Należy zdefiniować organizacyjne standardy tworzenia plików dziennika dla urządzeń pamięci masowej, aby określić wymagany poziom logowania. *Zdarzenia związane z zarządzaniem* oraz *zdarzenia związane z bezpieczeństwem* (zgodnie z definicjami podanymi powyżej) powinny być rejestrowane dla wszystkich rodzajów danych. W przypadku wyjątkowo wrażliwych danych należy również rejestrować *zdarzenia dostępu do danych* (zgodnie z definicją podaną powyżej). Szczegółowe informacje znajdują się w zaleceniu AL-SS-R4.

b. Wszystkie urządzenia powinny być skonfigurowane w taki sposób, by przekazywały dane z dzienników zdarzeń na centralne serwery zatwierdzone

[22] Demon (*ang. daemon*) – program lub proces, wykonywany wewnątrz środowiska wielozadaniowego systemu operacyjnego, bez konieczności interakcji z użytkownikiem (jako proces drugoplanowy).

przez organizację, zgodnie z obowiązującymi w organizacji wytycznymi dotyczącymi gromadzenia plików dziennika.

c. Na wszystkich urządzeniach należy monitorować poprawność konfiguracji dzienników oraz ich przesyłania (np. czy usługa tworzenia plików dziennika jest aktywna, czy konfiguracja poziomu rejestracji zdarzeń odpowiada normom obowiązującym w organizacji, czy w każdym urządzeniu skonfigurowane są zatwierdzone przez organizację serwery plików dziennika), a alerty dotyczące wykrytych nieprawidłowości powinny być obsługiwane z wysokim priorytetem.

d. Należy wdrożyć wiele serwerów syslog, aby umożliwić ciągłe rejestrowanie i uniknąć sytuacji, w których w infrastrukturze występuje pojedynczy punkt podatności na awarię.

e. Należy przechowywać co najmniej jedną kopię każdego pliku dziennika poza siedzibą organizacji.

f. Aby zapobiec utracie wpisów w przypadku zatrzymania i ponownego uruchomienia procesu rejestrowania przed zapisaniem wszystkich wpisów, należy skonfigurować rejestrowanie w taki sposób, by plik dziennika był zapisywany na dysku w czasie rzeczywistym bez buforowania i przesyłany za pomocą niezawodnych protokołów.

AL-SS-R4 - Poziom gromadzonych informacji o zdarzeniach: W dziennikach audytu związanych z infrastrukturą pamięci masowej należy gromadzić informacje o następujących zdarzeniach związanych z wszystkimi obiektami, miejscami i kontami:

a. Wywołania API tylko do odczytu w środowiskach wrażliwych.

b. Wszystkie odrzucone próby dostępu do usług, portów, plików, obiektów lub urządzeń.

c. Operacje zarządzania kluczami kryptograficznymi obejmujące cały cykl życia kluczy (szczególnie w przypadku kluczy szyfrujących), takie jak generowanie kluczy, usuwanie kluczy, zarządzanie certyfikatami itp.

AL-SS-R5 – Należy wdrożyć następujące działania dotyczące przechowywania i ochrony dzienników audytu:

a. Przechowywanie danych z dzienników przez odpowiednio długi okres, ze względu na fakt, że dostrzeżenie trwającego lub zakończonego ataku może zająć dłuższy czas.

b. Przydzielenie wystarczającej ilości miejsca w pamięci masowej oraz proaktywne monitorowanie wolnego miejsca i nietypowych przyrostów rozmiarów dzienników zdarzeń, by zapobiec brakowi miejsca na gromadzenie nowych dzienników. Jeden z typowych mechanizmów ataku wiąże się z zapełnieniem plików dziennika, by uniemożliwić analizę ataku. Odpowiedni monitoring może pomóc w identyfikacji takich ataków w czasie rzeczywistym.

c. Zarchiwizowane dane dziennika powinny być chronione przed manipulacją (np. poprzez stosowanie zasady jednorazowego zapisu i wielokrotnego odczytu lub metod przechowywania uniemożliwiających modyfikację, blokowanie obiektów, potwierdzanie usunięcia przy pomocy uwierzytelniania wieloskładnikowego). Jeśli istnieje taka możliwość, centralne serwery dzienników powinny również korzystać z takich opcji.

d. Należy ograniczyć dostęp do danych zawartych w dziennikach oraz serwerów stosując odpowiednie role i konta.

e. Należy włączyć szyfrowanie, gdyż dostęp do danych w plikach dzienników może zapewnić napastnikom dostęp do cennych informacji na temat zasobów oraz możliwych wektorów ataku.

AL-SS-R6 – Integracja z systemem SIEM: Jeśli jest to możliwe, pliki dzienników dotyczące infrastruktury pamięci masowej powinny być zintegrowane z oprogramowaniem bezpieczeństwa informacji i zarządzanie zdarzeniami (*ang. Security Information and Event Management - SIEM*) w celu wykrywania potencjalnych zagrożeń.

4.5 Przygotowanie do reagowania na incydenty dotyczące danych i odzyskiwania danych

Planowanie procesu reagowania na incydenty (*ang. incident response – IR*) jest ważną częścią szeroko pojętego zagadnienia cyberbezpieczeństwa. Kompleksowe omówienie znaczenia reagowania na incydenty w zarządzaniu programem cyberbezpieczeństwa

oraz rekomendacje dotyczące budowy ram poprawy cyberbezpieczeństwa można znaleźć w dokumencie *NIST Framework for Improving Critical Infrastructure Cybersecurity*[23] [40]. Incydenty związane z pamięcią masową powinny być obsługiwane w ramach procesu reagowania na incydenty w organizacji, obejmującego takie aspekty jak: izolacja, analiza przyczyn źródłowych, określenie planu reagowania i zarządzanie nim, testowanie oraz okresowy przegląd i odświeżanie procesu.

Poniższe zalecenia obejmują konkretne obszary, które należy wziąć pod uwagę w odniesieniu do infrastruktury pamięci masowej i zasobów związanych z danymi.

IR-SS-R1 – Opracowanie planu reagowania na kompromitację elementu systemu pamięci masowej: W procesach analizy ryzyka, procedurach izolacji, korygowania, przywracania działania oraz testowania należy uwzględnić następujące zdarzenia:

a. Naruszenie zasad ochrony całej macierzy dyskowej lub całego zasobu pamięci masowej w chmurze (np. SAN, NAS, magazyn obiektów, elastyczny system plików).

b. Naruszenie zasad ochrony systemu kopii zapasowej.

c. Naruszenie zasad ochrony pojedynczego elementu systemu pamięci masowej (np. udziału, urządzenia blokowego).

d. Naruszenie zasad ochrony sieci FC SAN (w tym poszczególnych przełączników i usług SAN).

IR-SS-R2 – Niezmienność zasobów służących do odzyskiwania w procesie usuwania skutków incydentu: W połączeniu z zaleceniami przedstawionymi w podrozdziale 4.7 dotyczącymi ochrony kopii pozwalających na odzyskanie danych, kopie te powinny pozostać odizolowane w procesie usuwania skutków zdarzenia.

IR-SS-R3 – Weryfikacja bezpieczeństwa odzyskanych urządzeń obliczeniowych: Należy upewnić się, że odzyskane pliki wykonywalne, aplikacje, kontenery i obrazy systemu operacyjnego nie zostały zainfekowane przed wprowadzeniem ich do środowiska produkcyjnego.

[23] Link do polskiej wersji dokumentu.

4.6 Rekomendacje dotyczące konfiguracji sieci

Jak wspomniano we wcześniejszej części dokumentu, zagadnienie sieci związanych z systemami pamięci masowej obejmuje wiele aspektów, z których część pokrywa się z zagadnieniami *kontroli dostępu do danych*, *dostępu administracyjnego* oraz *szyfrowania*, które zostały omówione w innych rozdziałach. Aby ograniczyć powtórzenia, w niniejszym dokumencie omówiono:

- Niektóre zalecenia dotyczące sieci ściśle związane z kontrolą dostępu do danych w podrozdziale 4.3.
- Zalecenia dotyczące szyfrowania związane z siecią i protokołami w podrozdziale 4.9.
- Niektóre zalecenia dotyczące sieci ściśle związane z dostępem administracyjnym w podrozdziale 4.10.
- Zalecenia dotyczące *infrastruktury sieciowej* (w tym konfiguracji przełączników, portów, kontrolerów pamięci masowej, kart sieciowych, stref itp.) oraz *protokołów* w niniejszym podrozdziale.

Aby w pełni zrozumieć wszystkie zagadnienia związane z konfiguracją sieci (*ang. network configuration – NC*), należy zapoznać się z treścią wszystkich wymienionych podrozdziałów.

4.6.1 FC SAN i NVMEoF

NC-SS-R1 – Uwierzytelnianie hostów i przełączników: Każdy host i przełącznik związany z systemem pamięci masowej powinien mieć przypisaną unikalną tożsamość i powinien być uwierzytelniony przed dołączeniem do sieci (np. FC-SP-2 AUTH-A).

NC-SS-R2 – Wdrożenie zatwierdzonego mechanizmu infrastruktury klucza publicznego (*ang. Public Key Infrastructure –PKI*): Do zarządzania certyfikatami przełączników należy używać zatwierdzonego i certyfikowanego przez organizację scentralizowanego systemu PKI (np. Fibre-Channel Certificate Authentication Protocol lub FCAP), nie zaś certyfikatów urządzeń podpisanych przez ich producentów.

NC-SS-R3 – Podejście mieszane do podziału na strefy: Należy wdrożyć podział na strefy oparty na podejściu łączącym różne rodzaje mechanizmów. Takie rozwiązanie jest preferowane względem standardowego podziału na strefy przy użyciu jednego typu (tj. hosta, przełącznika i urządzenia pamięci masowej):

a. Mechanizmy podziału na strefy oparte na hostach pozwalają na kontrolowanie, jakie zasoby lub urządzenia pamięci masowej są widoczne dla aplikacji działających na danym hoście, a także do jakich urządzeń mogą uzyskać dostęp. Na najniższym poziomie możliwości maskowania w oprogramowaniu sprzętowym lub sterowniku kontrolera pamięci masowej mogą być wykorzystywane do kontrolowania, czy host może wchodzić w interakcje z dowolnym urządzeniem pamięci masowej. Na kolejnym poziomie można wykorzystać możliwości systemu operacyjnego do konfiguracji, które urządzenia może zamontować dany host jako wolumeny pamięci masowej. Dodatkowo oprogramowanie pozwalające na scentralizowane zarządzanie woluminami na poziomie hosta (np. *Logical Volume Manager – LVM*), narzędzia umożliwiające budowę klastrów i system plików mogą być wykorzystywane do kontrolowania dostępu do urządzeń przez aplikacje.

b. W wyznaczaniu stref opartym na przełącznikach, przełączniki (zwłaszcza przełączniki FC) mają możliwość określenia, które urządzenia podłączone do których portów mogą uzyskać dostęp do innych urządzeń lub portów. Wyznaczanie stref oparte na portach wykorzystuje urządzenia do egzekwowania podziału na strefy, z tego powodu często określa się je mianem sztywnego lub twardego (*ang. hard zoning*). Innymi słowy, przełączniki powinny obsługiwać kontrolę stref na poziomie WWN portu, a nie na poziomie WWN przełącznika (węzła).

c. W przypadku wyznaczania stref opartego na urządzeniach pamięci masowej, konfiguracja macierzy pamięci masowej obejmuje listę zawierającą hosty oraz konkretne porty kontrolerów pamięci masowej, które mogą uzyskać dostęp do urządzeń blokowych podłączonych do konkretnych portów. Żądania dostępu pochodzące z innych hostów lub portów są ignorowane lub odrzucane.

d. Jeśli funkcja konfiguracji stref jest dostępna, należy ją wykorzystać. Dzięki temu można utworzyć wiele stref z myślą o konkretnych celach, takich jak testowanie, dynamiczna rekonfiguracja, tworzenie kopii zapasowych i konserwacja.

NC-SS-R4 – Zalecenie dotyczące maskowania: Maskowanie oznacza ukrycie lub ujawnienie urządzenia blokowego przed hostami. W **miarę możliwości należy wybierać maskowanie jak najbliżej danych** i jak najdalej od konsumenta danych lub klienta (np. maskowanie na poziomie macierzy jest lepsze niż maskowanie na poziomie

przełącznika; maskowanie na podstawie przełącznika sieci szkieletowej jest lepsze niż maskowanie na poziomie przełącznika brzegowego, z kolei maskowanie na poziomie przełącznika brzegowego jest lepsze niż na poziomie kontrolera pamięci masowej).

NC-SS-R5 - Tworzenie kopii zapasowych konfiguracji przełączników: Należy utworzyć kopie zapasowe konfiguracji przełączników, w tym pliku konfiguracyjnego stref. Kopia zapasowa powinna być przechowywana poza przełącznikami SAN, aby umożliwić odtworzenie konfiguracji w przypadku błędu, złośliwego uszkodzenia lub usunięcia konfiguracji.

NC-SS-R6 – Ograniczenie możliwości zarządzania przełącznikiem do niezbędnego minimum:

a. Podczas wdrażania sieci szkieletowej SAN należy wdrożyć szczegółowe zasady określające zestaw przełączników, które są upoważnione do dystrybucji danych konfiguracyjnych i minimalizujących ich liczbę przy zapewnieniu akceptowalnej redundancji.

b. Nie należy włączać zbędnych uprawnień i usług zarządzania konfiguracją, takich jak dystrybucja haseł.

NC-SS-R7 – Stosowanie różnych rodzajów podziału na strefy:

- **Elastyczny podział na strefy** (*ang. soft zoning*) opiera się na filtrowaniu na poziomie przełączników Fibre-Channel, aby uniemożliwić widoczność portów poza przypisanymi strefami. Rozwiązanie charakteryzuje się pewną podatnością – porty mogą być nadal dostępne, jeśli użytkownik przypisany do innej strefy odgadnie adres Fibre-Channel. W tym przypadku przełącznik FC umieści WWN hosta w danej strefie bez sprawdzania numerów portów przełącznika, które zostały użyte do nawiązania połączenia. Identyfikacja PWWN (*ang. Port World-Wide Name*) jest uważana za bardziej bezpieczną niż identyfikacja numeru portu (stosowana w strefach twardych), ponieważ każde urządzenie fizycznie podłączone do portu może udzielić dostępu do pamięci masowej nieautoryzowanemu hostowi. Jeśli sieć SAN obejmuje obiekty charakteryzujące się różnym poziomem zabezpieczeń fizycznych i jeśli istnieje ryzyko, że dostęp do portów fizycznych mogą uzyskać osoby nieupoważnione, preferowany może być elastyczny podział na strefy.

- **Sztywny podział na strefy** (*ang. hard zoning*) opiera się na numerach fizycznych portów przełączników SAN, tym samym fizycznie blokując dostęp do strefy z każdego urządzenia spoza strefy. Ten rodzaj podziału na strefy chroni przed atakami opierającymi się na spoofingu nazw WWN, ponieważ nie wykorzystuje tożsamości hosta. Jeśli organizacja zapewnia solidną ochronę bezpieczeństwa wszystkich obiektów, dzięki czemu prawdopodobieństwo, że napastnik uzyska dostęp do fizycznego portu jest znikome, stosowanie tej metody może być preferowane.

NC-SS-R8 – Ograniczenie fizycznych i logicznych portów SAN Fibre-Channel wykorzystywanych do zarządzania we wszystkich przełącznikach SAN i macierzach pamięci masowej.

NC-SS-R9 – Ograniczenie komunikacji między przełącznikami: Należy ograniczyć komunikację między przełącznikami SAN na podstawie zasad bezpieczeństwa, zapewniając jednocześnie, że przełączniki mogą komunikować się tylko z tymi przełącznikami, z którymi komunikacja jest niezbędna.

NC-SS-R10 – Trwałe wyłączanie nieużywanych portów SAN, aby zapobiec przypadkowemu lub celowemu podłączeniu nieautoryzowanych urządzeń.

4.6.2 Komunikacja z systemami pamięci masowej w sieciach IP

NC-SS-R11 – Separacja pamięci masowej w sieci IP: W przypadku komunikacji związanej z pamięcią masową za pośrednictwem sieci IP należy zastosować podstawowe zasady separacji środowisk i rodzaju ruchu zarówno w warstwie 2, jak i 3 stosu sieciowego. Środowiska wrażliwe powinny być odseparowane w maksymalnym możliwym stopniu na podstawie następujących przesłanek:

a. Rodzaj ruchu – protokoły dostępu do danych, zarządzanie, replikacja, tworzenie kopii zapasowych, sieci hostów i aplikacji

b. W środowiskach wrażliwych należy dodatkowo odseparować ruch związany z zarządzaniem powiązany z różnymi rozwiązaniami, dostawcami i technologiami. Na przykład, jeśli używane są dwa lub więcej rozwiązań pamięci masowej (np. różne rodzaje macierzy, produkty SAN oparte na serwerach, technologie przełączników, wirtualizacja pamięci masowej lub dowolna kombinacja takich

rozwiązań), a każde z nich jest wyposażone w oddzielny zestaw narzędzi do zarządzania, ruch związany z zarządzaniem dotyczący każdego środowiska powinien być odseparowany od pozostałych.

c. Protokoły dostępu do danych (np. iSCSI, NFS, protokoły własnościowe producentów rozwiązań, np. SAN oparty na serwerach).

d. Rodzaj serwerów lub hostów uzyskujących dostęp do danych – hosty zwirtualizowane, hosty fizyczne

NC-SS-R12 – Porty IP lub Ethernet przełączników SAN przeznaczone do zarządzania powinny być połączone z odizolowaną podsiecią, która powinna być odseparowana od podsieci używanych w celu uzyskiwania dostępu do danych przez hosty i system pamięci masowej oraz do komunikacji między hostami.

NC-SS-R13 – Włączenie kontroli dostępu do urządzeń przez sieć IP: Należy włączyć i skonfigurować funkcje bezpieczeństwa urządzeń pamięci masowej, które odpowiadają za kontrolę adresów IP, portów oraz protokołów na wszystkich urządzeniach pamięci masowej, jeśli jest to możliwe. Dotyczy to między innymi wbudowanych reguł zapory sieciowej, filtrowania adresów IP oraz list dostępu, w celu:

a. Kontrolowania oraz ograniczania dostępu do danych do wybranych hostów oraz aplikacji a także używanych przez nie obiektów w pamięci masowej;

b. Kontrolowanie ruchu zarządzania w sieci IP pomiędzy hostami odpowiedzialnymi za zarządzanie i aplikacjami zarządzania oraz odpowiednimi interfejsami zarządzania pamięcią masową, z których korzystają.

NC-SS-R14 – Włączenie kontroli dostępu do sieci IP: Ograniczenia należy stosować na poziomie sieci (np. odpowiedni routing, zapora, listy dostępu, grupy zabezpieczeń VPC, klienci SAN), aby ograniczyć wszystkie rodzaje ruchu (np. ruch związany z dostępem do danych i zarządzaniem) wyłącznie do dozwolonych adresów IP oraz portów i protokołów TCP/UDP:

a. Pomiędzy hostami lub aplikacjami a wykorzystywanymi przez nie obiektami w pamięci masowej; a także

b. Między hostami i aplikacjami zarządzającymi a odpowiednimi interfejsami

zarządzania obiektami pamięci masowej, którymi zarządzają.

NC-SS-R15 – Blokada publicznego dostępu do niepublicznych obiektów pamięci masowej, zwłaszcza dostępu z poziomu Internetu.

NC-SS-R16 – Dostęp publiczny: W przypadku obiektów, które wymagają publicznego dostępu, należy wdrożyć stosowne środki bezpieczeństwa, w tym:

a. Minimalizację możliwości dostępu.

b. Używanie fizycznie i logicznie oddzielonych podsieci pamięci masowej, a najlepiej oddzielnych urządzeń i puli pamięci masowej od tych używanych do magazynowania obiektów niepublicznych.

c. Wdrożenie ochrony przed atakami typu odmowa świadczenia usługi.

d. Zabezpieczenie podręcznych kopii danych (na przykład udostępnianych w sieciach dostarczania treści (*ang. content delivery network - CDN*)), a także replik i serwerów proxy co najmniej na takim samym poziomie jak danych źródłowych.

e. Uwzględnienie wymogów regulacyjnych (dotyczących między innymi poufności oraz ograniczeń dotyczących miejsc przechowywania danych).

f. Wszelkie dodatkowe środki bezpieczeństwa (np. szyfrowanie, uwierzytelnianie).

NC-SS-R17 – Kontrola adresów IP używanych w związku z protokołem SNMP: W ramach konfiguracji protokołu SNMP cały ruch związany z tym protokołem powinien być przekierowywany do stosownych wewnętrznych adresów IP organizacji. Prawidłowość konfiguracji powinna być okresowo weryfikowana.

NC-SS-R18 – Możliwość użycia odizolowanych nieroutowalnych sieci VLAN dla rozwiązań SAN opartych na serwerach: Więcej informacji na temat rozwiązań SAN opartych na serwerach znajduje się w podrozdziale 2.9 niniejszej publikacji. W celu ochrony środowiska przechowywania danych i ograniczenia obaw związanych z bezpieczeństwem należy stosować nieroutowalne sieci VLAN w przypadku rozwiązań SAN opartych na serwerach.

4.6.3 Protokoły

NC-SS-R19 – Wyłączenie niebezpiecznych wersji protokołów dostępu do plików: Należy zablokować przestarzałe, niezalecane lub niebezpieczne wersje protokołów,

takie jak SMB v1 lub NFS 1 i 2. Jeśli to możliwe, protokoły te powinny być wyłączone zarówno po stronie klienta, jak i po stronie serwera.

NC-SS-R20 – Bezpieczeństwo protokołu SNMP:

a. Jeśli protokół SNMP nie jest używany, powinien być wyłączony.

b. Należy zmienić domyślne i znane hasła, nawet jeśli protokół SNMP jest wyłączony. Skonfigurowane hasła powinny być zgodne z zasadami organizacji dotyczącymi haseł.

c. Należy używać różnych haseł dla urządzeń różniących się poziomem poufności.

d. Należy korzystać z protokołu SNMP co najmniej w wersji 3.

e. Należy włączyć funkcje uwierzytelniania i szyfrowania (prywatności) protokołu SNMP.

f. Nie należy konfigurować komunikacji opartej na protokole SNMP z uprawnieniami odczytu i zapisu, chyba że jest to absolutnie niezbędne. W takim przypadku należy ograniczyć wykorzystanie protokołu SNMP w trybie odczytu i zapisu oraz kontrolować jego użycie.

g. Należy użyć listy kontroli dostępu, aby kontrolować dostęp do urządzeń poprzez protokół SNMP.

h. Należy okresowo weryfikować, czy „SNMP traps" są wysyłane do autoryzowanych i właściwych menadżerów.

i. Dodatkowe zalecenia dotyczące tego zagadnienia można znaleźć w dokumencie Department of Homeland Security Cybersecurity & Infrastructure Security (DHS CISA) TA17-156A [39].

NC-SS-R21 – Autentyczność usług katalogowych, domenowych i podobnych (np. Active Directory, DNS, LDAP): Konfiguracje usług związanych ze wszystkimi elementami pamięci masowej (w tym urządzeniami, przełącznikami, stacjami roboczymi wykorzystywanymi do zarządzania, oprogramowaniem do zarządzania) powinny być aktywnie i okresowo przeglądane w celu upewnienia się, że stosowane są zatwierdzone warianty konfiguracji oraz w celu usunięcia wszelkich rozbieżności.

NC-SS-R22 – Uwagi dotyczące korzystania ze standardowych i niestandardowych portów TCP/IP lub UDP: Konfiguracja większości aplikacji i usług obejmuje domyślny port TCP/IP lub UDP, który jest używany do komunikacji z aplikacją lub usługą. Ze względu na to, że w większości przypadków istnieje możliwość konfiguracji portów logicznych wykorzystywanych przez różne aplikacje i usługi, należy rozważyć wady i zalety stosowania niestandardowych portów.

- **Zalety –** Stosowanie niestandardowych portów pomaga ukryć aplikację lub usługę, ponieważ potencjalni napastnicy nie wiedzą, którego portu użyć.
- **Wady –** Stosowanie niestandardowych portów może utrudnić narzędziom zapewniającym bezpieczeństwo wykrycie podejrzanych działań, ponieważ są one zaprojektowane tak, aby oczekiwać określonych zachowań na standardowych portach.

NC-SS-R23 – Należy włączyć filtry snoopingowe protokołu FCoE Initialization Protocol (FIP) w sieciach FCoE VLAN, aby zapobiec nieautoryzowanemu dostępowi do danych: Snooping protokołu FCoE Initialization Protocol (FIP) to mechanizm bezpieczeństwa, który ma na celu uniemożliwienie nieautoryzowanego dostępu i transmisji danych do sieci FC. Jego działanie polega na filtrowaniu ruchu w taki sposób, by zezwolić na dostęp do sieci FC tylko serwerom, które są do niej zalogowane. Przełączniki FCoE łączą inicjatory FC (serwery) w sieci Ethernet z forwarderami FCoE (FCF) na brzegu sieci FC SAN, umożliwiając spoofing FIP w odpowiednich sieciach VLAN.

NC-SS-R24 – Ograniczenie liczby portów iSCSI: Hosty w sieci iSCSI powinny mieć zablokowany dostęp do portów TCP innych niż te przeznaczone dla iSCSI w danej sieci.

NC-SS-R25 – Użycie uwierzytelniania iSCSI: Do uwierzytelniania inicjatorów iSCSI przy otwieraniu sesji należy użyć jednej z obsługiwanych metod uwierzytelniania, takich jak na przykład protokół CHAP (Challenge-Handshake Authentication Protocol), protokół SRP (Server Routing Protocol), Kerberos, bądź mechanizm Simple Public-Key GSS-API Mechanism (SPKM)1/2). W przypadku korzystania z protokołu CHAP należy preferować uwierzytelnianie dwukierunkowe nad jednokierunkowym.

Należy pamiętać, że zastosowanie uwierzytelniania nie gwarantuje szyfrowania ani ochrony integralności kanału.

NC-SS-R26 – Stosowanie zabezpieczeń protokołu NDMP (*Network Data Management Protocol*): Protokół NDMP zapewnia mechanizmy bezpośredniego transportu między macierzami dyskowymi a urządzeniami do tworzenia kopii zapasowych. W przypadku stosowania tego protokołu należy skonfigurować następujące zabezpieczenia:

a. Kontrola dostępu hostów, które mogą inicjować sesje NDMP.

b. Uwierzytelnianie typu wezwanie-odpowiedź – nie należy używać opcji uwierzytelniania otwartym tekstem (*ang. plaintext authentication*).

c. Rejestrowanie prób połączeń NDMP.

d. Hasło NMDP spełniające wymogi organizacji w zakresie długości, złożoności i innych cech.

e. Ograniczone uprawnienia użytkownika związane z protokołem NDMP.

f. Szyfrowane połączenia związane z zarządzaniem protokołem NDMP.

g. Ograniczanie prędkości protokołu NDMP dla danej sesji lub serwera.

NC-SS-R27 – Włączenie protokołu TLS w LDAP: Należy użyć protokołu TLS do zabezpieczenia połączeń LDAP podczas konfigurowania opcji Active Directory dla systemów pamięci masowej.

NC-SS-R28 – Protokoły dodatkowe: W przypadku stosowania dodatkowych protokołów, takich jak SymAPI, Storage Management Initiative Specification (SMI-S), Global Name Server (GNS) i innych, należy rozważyć dostosowanie do ich użycia zaleceń zawartych w podrozdziałach 4.6.2 i 4.6.3 . Przede wszystkim należy stosować:

a. izolację ruchu związanego z dostępem do danych i zarządzaniem od innych środowisk,

b. ograniczenie wykorzystywanych portów TCP i UDP,

c. włączenie szyfrowania.

4.7 Izolacja

W przypadku uszkodzenia lub utraty danych produkcyjnych organizacje powinny mieć możliwość ich odzyskania z wykorzystaniem repliki danych lub utworzonej uprzednio kopii zapasowej. Jeśli uszkodzenie lub utrata danych są wynikiem złośliwego ataku, a napastnicy byli również w stanie skompromitować kopie zapasowe, atak na środowisko produkcyjne może mieć katastrofalne skutki, ponieważ organizacja może nie mieć możliwości ich odzyskania. Aby zwiększyć odporność kopii zapasowych na zniszczenie i ataki, należy zagwarantować dostateczny poziom izolacji (*ang. isolation – IS*) między zasobami danych a ich kopiami zapasowymi.

Biorąc pod uwagę tę kwestię organizacje powinny brać pod uwagę co najmniej dwa odrębne scenariusze ochrony danych:

- **Odzyskanie danych w przypadku utraty niezwiązanej z atakiem** – ten scenariusz wymaga uprzedniego utworzenia kopii danych, które mogą być wykorzystane w przypadku katastrofy naturalnej, awarii sprzętu, błędu ludzkiego itp. Mogą one obejmować kopie lokalne (np. migawki wykonywane przed przeprowadzeniem konserwacji), kopie pozwalające na odzyskanie danych w razie katastrofy, kopie zapasowe i zarchiwizowane dane. Im bardziej kopia jest zbliżona do środowiska produkcyjnego, tym większe prawdopodobieństwo, że odpowiada systemom obliczeniowym i może być wykorzystana na potrzeby testów oraz odzyskiwania w przypadku katastrofy.
- **Odzyskiwanie danych w przypadku cyberataku –** ten scenariusz wymaga uprzedniego utworzenia zabezpieczonych, zablokowanych i odizolowanych kopii danych. Celem planowania takich kopii zapasowych jest osiągnięcie stanu, w którym żadne czynniki nie będą w stanie wpłynąć na zawartość tych kopii zapasowych, nawet w sytuacji, w których woluminy produkcyjne lub inne rodzaje kopii, z którymi są powiązane, zostaną skompromitowane.

Przechowywanie kopii do odzyskiwania danych w przypadku cyberataku w formie całkowicie odizolowanej od kopii używanych do odzyskiwania danych po przypadkowej utracie danych nie jest obowiązkowe, choć takie rozwiązanie jest zalecane w przypadku systemów wrażliwych i systemów o kluczowym znaczeniu. Ważne jest

jednak upewnienie się, że stosowany system ochrony danych może zostać wykorzystany w obu scenariuszach. Jeżeli istniejące mechanizmy przechowywania kopii (np. kopie zapasowe przeznaczone do odzyskiwania danych w przypadku katastrofy, archiwa zewnętrzne) mają posłużyć także do odzyskiwania danych w przypadku cyberataku, należy przeanalizować ich konfigurację i w razie potrzeby dostosować ją w celu umożliwienia izolacji danych. Przegląd ten powinien objąć sprawdzenie, czy przynajmniej część zbioru tych kopii i systemów odzyskiwania jest niedostępna i niezależna od środowiska produkcyjnego oraz czy kompromitacja tego środowiska nie pozwoli napastnikom na dokonanie zmian lub zniszczenie tych kopii.

Poniższe zalecenia dotyczące bezpieczeństwa dotyczą przygotowywania kopii danych, zarządzania oraz związanego z nimi systemu zarządzania.

IS-SS-R1 – Rozdzielenie systemów pamięci masowej:

a. Kopie zapasowe danych przeznaczone do odzyskiwania danych w przypadku cyberataku powinny być tworzone na specjalnych, wydzielonych systemach pamięci masowej. W przypadku chmur prywatnych oznacza to fizycznie oddzielone systemy pamięci masowej. W przypadku chmur publicznych oznacza to oddzielne konta lub równoważne rozwiązanie.

b. Systemy długoterminowej archiwizacji danych oraz kopii zapasowych powinny być odseparowane od systemów magazynujących dane produkcyjne.

IS-SS-R2 – Rozdzielenie systemów zarządzania: Systemy pamięci masowej, w których przechowywane są kopie przeznaczone do odzyskiwania danych w przypadku cyberataku powinny być zarządzane z wyznaczonych systemów zarządzania odseparowanych od środowiska produkcyjnego oraz wszelkich innych systemów połączonych ze środowiskiem produkcyjnym (w tym mechanizmów ochrony danych). Nie powinno być możliwe uzyskanie dostępu do takich systemów zarządzania przy pomocy standardowych poświadczeń, w tym poświadczeń do systemów produkcyjnych oraz systemów kopii zapasowych. System powinien opierać się na dedykowanym środowisku, które jest podłączone wyłącznie do odizolowanej sieci.

IS-SS-R3 – Ograniczenie dostępu do systemu odzyskiwania danych w przypadku cyberataku oraz długoterminowych archiwów i kopii zapasowych:

a. W przypadku informacji wrażliwych, kopie przeznaczone do odzyskiwania danych w przypadku cyberataku oraz systemy, w których są przechowywane, nie powinny być dostępne dla zwykłych pracowników IT; dostęp do nich powinna mieć wyłącznie wybrana osoba (np. CISO), lub bardzo wąska grupa przedstawicieli kadry kierowniczej ds. bezpieczeństwa, którzy używają poświadczeń odrębnych od tych używanych w trakcie realizacji innych codziennych obowiązków. Takie rozwiązanie gwarantuje, że w przypadku skompromitowania poświadczeń administratora IT napastnik nie będzie w stanie użyć ich w celu uzyskania dostępu do kopii danych, która może posłużyć do ich odzyskania w przypadku cyberataku. Taki zespół złożony z ograniczonej liczby pracowników może mieć dostęp do kopii przeznaczonej do odzyskiwania danych w przypadku cyberataku, jednak uprawnienia administratora pozwalające na nadawanie uprawnień innym użytkownikom powinny zostać przydzielone jeszcze mniejszej liczbie pracowników.

b. Uprawnienia do dostępu do kopii zapasowych oraz archiwów długoterminowych powinny być oddzielone od poświadczeń używanych do wykonywania innych zadań związanych z administrowaniem pamięcią masową (np. zarządzanie rozwiązaniami SAN czy alokacją pamięci masowej) i powinny obejmować stosowanie oddzielnych identyfikatorów użytkowników, kont i poświadczeń.

IS-SS-R4 – Przechowywanie danych poza siedzibą organizacji: Kopie przeznaczone do odzyskiwania danych w przypadku cyberataku powinny być przechowywane poza siedzibą organizacji i poza miejscem, w którym przechowywane są dane produkcyjne. Dzięki takiemu rozwiązaniu nawet jeśli napastnicy uzyskają fizyczny dostęp do miejsca przechowywania danych lub uda im się naruszyć zasady ochrony, nie będą w stanie uzyskać dostępu do kopii przeznaczonej do odzyskiwania danych w przypadku cyberataku ani jej skompromitować.

IS-SS-R5 – Przygotowanie niezależnej, kompletnej kopii podstawowej: Systemy kopii zapasowych często wykorzystują kopie przyrostowe, które pozwalają na kopiowanie wyłącznie danych zmienionych względem poprzedniej kopii podstawowej. Przyrostowe kopie zapasowe nie pozwalają na odzyskanie danych bez kopii podstawowej zawierającej stan wyjściowy. W przypadku niektórych technik tworzenia kopii zapasowych, na przykład w przypadku migawek, stosowane są wyłącznie kopie przyrostowe – kopią podstawową są same dane produkcyjne.

Aby prawidłowo zrealizować scenariusz odzyskiwania danych, należy uwzględnić zależności między kopiami oraz zachować wystarczającą izolację między różnymi rodzajami kopii. Przede wszystkim:

a. Replikowane kopie danych stworzone z myślą o odtwarzaniu danych po katastrofie nie powinny być zależne od danych w systemach produkcyjnych.

b. Kopie przeznaczone do odzyskiwania danych w przypadku cyberataku nie powinny być zależne od danych w systemach produkcyjnych. Zależność od kopii danych stworzonej z myślą o odtwarzaniu danych po katastrofie jest dopuszczalna wyłącznie w sytuacji, gdy kopie te są odpowiednio odizolowane od danych produkcyjnych i spełniają wymogi zaleceń zawartych w punktach IS-SS-R1, IS-SS-R2 oraz IS-SS-R3.

c. Długoterminowo archiwizowane dane nie powinny być zależne od danych produkcyjnych ani kopii danych stworzonej z myślą o odtwarzaniu po katastrofie.

IS-SS-R6 – Wyłączenie wszystkich zbędnych usług i protokołów: Zbędne usługi i protokoły powinny być wyłączone w systemach pamięci masowej wykorzystywanych do odzyskiwania danych w przypadku cyberataku. W środowiskach, w których do zarządzania wystarcza interfejs programowy aplikacji (API) lub interfejs wiersza poleceń (CLI) zaleca się również wyłączenie wszelkich interaktywnych interfejsów sieciowych.

IS-SS-R7 – Niezależność od hostów i aplikacji:

a. Kopie przeznaczone do odzyskiwania danych w przypadku cyberataku nie powinny być instalowane, eksportowane ani mapowane do hostów ani aplikacji; powinny być także przywracane na odizolowane lub odłączone fizycznie od sieci środowisko

odzyskiwania, nie zaś bezpośrednio na docelowe hosty lub aplikacje. Mniej bezpieczną opcją jest zezwolenie docelowym hostom lub aplikacjom na ograniczony dostęp tylko do odczytu (np. mapowanie lub instalowanie) na czas przywracania danych, a następnie odebranie dostępu do danych po zakończeniu procesu.

b. Długoterminowe kopie archiwalne lub zapasowe nie powinny być instalowane, eksportowane ani mapowane bezpośrednio do hosta lub aplikacji.

IS-SS-R8 – Fizyczne odłączenie urządzeń od sieci: Organizacje powinny rozważyć odłączenie systemów przechowujących kopie pozwalające na odzyskanie danych w przypadku cyberataku od sieci. Systemy magazynujące kopie danych powinny być odizolowane fizycznie oraz odłączone od sieci. Niektóre technologie pamięci masowych pozwalają na korzystanie z mniej ścisłych metod izolacji, które umożliwiają na przykład wyłączanie portów wykorzystywanych do przesyłu danych oraz otwieranie ich przez ograniczony czas w celu przeprowadzenia okresowej synchronizacji z systemem produkcyjnym. Niezwykle ważne jest, by przeanalizować skuteczność każdej z tych technik względem wagi danych oraz możliwości potencjalnego napastnika. W przypadku podjęcia decyzji o całkowitej izolacji i pełnym odłączeniu systemów, należy uwzględnić metody ochrony przed wykorzystaniem znanych podatności dotyczących takich systemów, które obejmują:

a. Zapobieganie możliwości przechwycenia sygnałów wizualnych, dźwiękowych i termicznych z odizolowanych systemów przez inne urządzenia – na przykład poprzez zachowanie odpowiedniej odległości, zastosowanie tłumienia lub izolacji fizycznej.

b. Zapobieganie wszelkim możliwościom bezprzewodowego przesyłu danych z odizolowanych urządzeń.

c. Wyłączenie dostępnych portów danych takich jak gniazdo USB lub gniazdo sieciowe.

d. Zastosowanie kondycjonera zasilania lub wydzielonego obwodu zasilania.

IS-SS-R9 – Wykonywanie okresowych przeglądów izolacji kopii zapasowych: Przestrzeganie powyższych zaleceń dotyczących izolacji kopii zapasowych powinno być weryfikowane co najmniej raz w roku, w ramach okresowej kontroli, aby upewnić

się, że nie doszło do zmian konfiguracji lub braków, które mogą naruszyć zasadę izolacji kopii przeznaczonych do odzyskiwania danych w przypadku cyberataku. Wrażliwe i najważniejsze systemy pamięci masowych mogą wymagać kontroli raz na kwartał oraz po każdej znaczącej zmianie, w zależności od tego, co nastąpi wcześniej.

Wyniki kontroli powinny być udokumentowane.

IS-SS-R10 – Rozważenie zastosowania niezmiennej pamięci masowej, która mogłaby pomóc w skuteczniejszej izolacji i ochronie danych wymaganych do odzyskiwania; może to obejmować na przykład blokady retencji, blokady magazynów oraz wprowadzenie zasad niezmienności.

4.8 Zapewnienie odtworzenia danych

Aby zapewnić skuteczne odzyskiwanie danych w wypadku ich katastrofalnej utraty lub cyberataku, wdrożenie procesu odzyskiwania danych nie jest wystarczające. Organizacje powinny także sprawdzić, czy wszystkie składniki krytycznych zasobów danych są chronione i czy mogą być przywrócone w sposób wierny, spójny i kompletny, a także czy szybkość przywrócenia oraz aktualność przywracanych danych są dostosowane do wymagań biznesowych i regulacyjnych. W wielu przypadkach organizacje posiadają kopie zapasowe swoich krytycznych systemów, lecz nie sprawdzają regularnie, czy mogą one być rzeczywiście wykorzystane do przywrócenia systemu w razie wystąpienia takiej konieczności. Często z powodów zmian konfiguracji, zmian w środowiskach, a nawet złośliwego ataku prowadzącego do skompromitowania kopii zapasowych dochodzi do sytuacji, w której organizacje nie są w stanie wykorzystać zarchiwizowanych danych do przywrócenia swoich systemów. Poniższe zalecenia dotyczące bezpieczeństwa dotyczą zapewnienia możliwości odzyskania danych (*ang. Restoration Assurance* - RA).

RA-SS-R1 – Zapewnienie kompletności kopii danych przeznaczonych do ich odzyskiwania: Wszystkie komponenty infrastruktury pamięci masowej, które zawierają kluczowe elementy zasobów danych, powinny być chronione, w tym przez tworzenie kopii zapasowych danych w celu umożliwienia ich odtworzenia w przypadku katastrofy lub cyberataku. Obejmuje to woluminy pamięci masowej, najważniejsze systemy plików, bazy danych, obrazy oprogramowania, certyfikaty, klucze szyfrowania,

pliki startowe, informacje o katalogach, ACL, ustawienia wirtualizacji i pliki konfiguracyjne.

RA-SS-R2 – Zabezpieczenie wszystkich zależnych elementów: Zależne komponenty, takie jak usługi Active Directory i DNS, a także zewnętrzne systemy zarządzania kluczami powinny być chronione, aby zagwarantować pełne odtworzenie danych. Jeśli do konfiguracji pamięci masowej używane są zautomatyzowane procesy, repozytoria kodu źródłowego, środowiska oraz stosowne procedury powinny zostać również objęte stosownymi zabezpieczeniami.

RA-SS-R3 – Zapewnienie dostępności wszystkich istotnych składników oprogramowania i sprzętu: Wszystkie istotne składniki oprogramowania i sprzętu (np. sterowniki, oprogramowanie sprzętowe) używane do uruchomienia systemu powinny zostać zabezpieczone przez wykonanie kopii zapasowej, odpowiednio chronione i dostępne na wypadek konieczności przeprowadzenia odtwarzania danych.

RA-SS-R4 – Wybrane przez organizację technologie i nośniki kopii zapasowych i danych powinny odpowiadać wymogom w zakresie czasu odzyskiwania: Czas odzyskiwania (RTO) to kluczowy wskaźnik efektywności (*ang. Key Performance Indicator - KPI*) używany do określenia oczekiwanego czasu odtworzenia danych. Zdolność do odtworzenia danych zgodnie z parametrem RTO powinna być analizowana całościowo, z uwzględnieniem wszystkich zależnych i powiązanych elementów – w tym na przykład przywrócenia danych, plików konfiguracyjnych, kluczy szyfrujących; jednocześnie należy równoważyć rzeczywistą szybkość odtwarzania danych wymaganą przez organizację, z kosztem jaki należy ponieść w celu dostosowania wszystkich zależnych elementów systemu, by osiągnąć zakładany czas RTO.

RA-SS-R5 — Testowanie odtwarzania danych w celu zapewnienia odpowiedniego czasu odzyskiwania: Okresowo organizacja powinna przeprowadzać testowe odtworzenia danych, aby upewnić się, że może zostać przeprowadzone pomyślnie i jego realizacja jest możliwa w oczekiwanych ramach czasowych.

RA-SS-R6 — Realizacja wymogów związanych z punktem odtworzenia danych: Dla każdego zasobu danych należy określić punkt odtworzenia danych (RPO), czyli ilość danych, które mogą zostać utracone w wyniku awarii, wyrażoną w czasie. Projekt

i wdrożenie systemów tworzenia kopii zapasowych i replikacji danych powinny umożliwiać odzyskanie danych zgodnie z założonym celem dotyczącym punktu ich odtworzenia.

RA-SS-R7 — Spełnienie organizacyjnych wymogów dotyczących częstotliwości tworzenia kopii zapasowych oraz przechowywania danych: Wymagania dotyczące przechowywania danych i częstotliwości wykonywania kopii dla każdego zasobu danych (por. **DP-SS-R1**) powinny być określone w stosownych zasadach. Projekt i wdrożenie systemów tworzenia kopii zapasowych i replikacji danych powinny umożliwiać spełnienie tych wymogów.

RA-SS-R8 – Zapewnienie dobrego stanu kondycji kopii zapasowych oraz zdalnych replik danych: Należy okresowo weryfikować, czy kopie zapasowe danych są w dobrym stanie. Obejmuje to sprawdzenie, czy w plikach dzienników nie występują żadne istotne błędy oraz czy nośniki, na których znajdują się kopie zapasowe danych, są w dobrym stanie technicznym. Częstotliwość tej kontroli powinna odpowiadać poziomowi wrażliwości i wagi chronionych danych, lecz nie powinna być przeprowadzana rzadziej niż raz w roku. Utrzymywanie współczynnika próbkowania na poziomie około 1 – 1,5 rzędu wielkości niższym niż częstotliwość tworzenia kopii zapasowych danych może stanowić dobrą rekomendację – oznacza to, że kopie godzinowe powinny być weryfikowane raz dziennie, kopie dzienne powinny być odtwarzane co dwa tygodnie lub raz w miesiącu itd.

RA-SS-R9 – Umożliwienie oddzielnego odtwarzania danych i aplikacji: Dane powinny być oddzielone od aplikacji, aby umożliwić odtworzenie danych bez konieczności przywracania zainfekowanego kodu lub oprogramowania.

RA-SS-R10 – Dokumentacja planu odtwarzania w wypadku katastrofy, zasobów, połączeń z systemami produkcyjnymi, procesów oraz procedur testowych: Należy opracować plan odtwarzania danych po katastrofie dotyczący infrastruktury pamięci masowej, obejmujący wszystkie zasoby, ich powiązania z systemami produkcyjnymi, procesy oraz procedury testowe. Każdy z tych dokumentów również powinien mieć kopię zapasową.

RA-SS-R11 – Cyberhigiena kopii danych: W przypadku najważniejszych danych, kopie wykorzystywane do odzyskiwania danych w przypadku cyberataku powinny być

skanowane za pomocą różnych narzędzi antywirusowych pod kątem znanych podatności i anomalii. Zalecanym rozwiązaniem jest skanowanie wszystkich kopii. Jeśli nie jest to możliwe, należy zeskanować wybraną część kopii i udokumentować, że wybrane kopie zostały przeskanowane i są bezpieczne. Stosowne narzędzia obejmują między innymi programy antywirusowe i wykrywające złośliwe oprogramowanie, programy wykrywające znane podatności oraz programy analizujące bezpieczeństwo.

RA-SS-R12 – Przeprowadzanie okresowych kontroli: Sposób realizacji powyższych zaleceń należy weryfikować w ramach okresowych kontroli, które mają na celu weryfikację kompletności kopii zapasowych, ponowną analizę zależności, określenie wymagań dotyczących sprzętu i oprogramowania, możliwości odzyskania danych w określonym czasie oraz do ustalonego punktu odtworzenia danych, retencji, weryfikację stanu nośników, analizę planu odtworzenia po katastrofie oraz cyberhigieny kopii. Wszelkie luki i niedociągnięcia należy wykryć, udokumentować oraz skorygować. Częstotliwość tej kontroli powinna odpowiadać poziomowi wrażliwości i wagi chronionych danych, lecz nie powinna być przeprowadzana rzadziej niż raz w roku. Wrażliwe i najważniejsze systemy pamięci masowych mogą wymagać kontroli raz na kwartał oraz po każdej znaczącej zmianie, w zależności od tego, co nastąpi wcześniej. Wyniki kontroli powinny być udokumentowane.

4.9 Szyfrowanie

Szyfrowanie to przetworzenie danych z postaci czytelnej (otwartego tekstu) w postać nieczytelną (zaszyfrowaną), która nie może zostać w prosty sposób odczytana przez osoby do tego nieuprawnione. W systemach pamięci masowej szyfrowanie informacji wrażliwych powinno być realizowane w sposób kompleksowy i obejmować:

- **Dane w spoczynku –** dane, które są w sposób fizyczny lub logiczny przechowywane w infrastrukturze pamięci masowej (np. na taśmach, dyskach i nośnikach optycznych). Należy przyjąć kompleksowe podejście, które obejmuje nie tylko same dane, lecz także metadane, które mogą zawierać informacje na temat uprawień dostępu, etykiet, ścieżek oraz dzienników.
- **Dane w czasie przesyłania –** gdy dane są przenoszone między elementami systemu pamięci masowej (na przykład odczytywane lub zapisywane przez

klienta, replikowane między urządzeniami pamięci masowej lub pulami, przesyłane w sieciach SAN bazujących na serwerach czy przy pomocy rozwiązania vMotion) lub przesyłane przez sieć, powinny pozostawać zaszyfrowane, chyba że cała komunikacja odbywa się w chronionym środowisku, takim jak centrum danych.

- **Dostęp administracyjny –**obejmuje połączenia za pośrednictwem standardowych i własnościowych protokołów i interfejsów API w celu konfiguracji elementów pamięci masowej, sieci pamięci masowej i danych oraz sterowania ich działaniem.

Szyfrowanie danych opiera się na dostępności i zarządzaniu kluczami kryptograficznymi. Wszystkie podmioty biorące udział w procesie komunikacji powinny mieć dostęp do wymaganych kluczy, które muszą być generowane, rozpowszechniane oraz utylizowane w odpowiedni sposób. Taką funkcjonalność zapewniają narzędzia do zarządzania kluczami, które stanowią podstawowe wymaganie w przypadku większości środowisk. Szczegółowe zalecenia dotyczące zarządzania kluczami zawiera dokument NIST SP 800-57 Part 1 [41].

Poniższe rekomendacje dotyczące szyfrowania (*ang. encryption – EN*) mają zastosowanie do infrastruktury pamięci masowej:

EN-SS-R1 – Protokół TLS, skróty kryptograficzne i szyfrowanie: Do obsługi szyfrowanej komunikacji między klientami i serwerami pamięci masowej należy stosować protokół Transport Layer Security (TLS). Aby zapobiec użyciu niebezpiecznej lub przestarzałej konfiguracji, wybór i konfiguracja implementacji protokołu TLS, w tym wybór wersji protokołu TLS oraz wybór algorytmów wykorzystywanych do tworzenia skrótów kryptograficznych i szyfrowania, powinny być oparte na następujących zaleceniach (lub ich aktualizacjach, gdy zostaną opublikowane):

- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (NIST SP 800-52 Rev2) [37]
- SNIA TLS Specification for Storage Systems Version 1.1 [38]

EN-SS-R2 – Nie należy używać protokołów opartych na otwartej nieszyfrowanej komunikacji, takich jak na przykład HyperText Transfer Protocol (HTTP), Telnet, File

Transfer Protocol (FTP), a także Remote Shell (RSH): Protokoły nieszyfrowane są podatne na podsłuchiwanie, przechwytywanie strumieni danych oraz inne rodzaje ataków, ponieważ przesyłane przy ich pomocy treści nie są szyfrowane, podobnie jak poświadczenia logowania, co ułatwia napastnikowi ich przechwycenie. W przypadku niektórych rozwiązań protokół HTTP jest wykorzystywany w celu przekierowania do protokołu HTTPS w celu zapobiegania przypadkom wprowadzenia błędnego adresu URL. W przypadku systemów pamięci masowej wykorzystywanych do przechowywania danych wrażliwych stosowanie takich rozwiązań jest niedopuszczalne.

EN-SS-R3 – Szyfrowanie sesji API wykorzystywanych do zarządzania pamięcią masową: Interfejsy API oraz wiersze poleceń pozwalające na zarządzanie pamięcią masową pozwalają użytkownikom na dostęp do systemów pamięci masowej z poziomu administratora. Wszystkie sesje API oraz wiersza poleceń powinny być szyfrowane przy pomocy funkcji oferowanych przez producenta oprogramowania do zarządzania lub na poziomie API bądź wiersza poleceń.

EN-SS-R4 – Szyfrowanie sesji dostępu administracyjnego: Sesje administracyjne realizowane za pośrednictwem protokołu HTTP powinny być szyfrowane za pomocą protokołu TLS (HTTPS). Dostęp do systemów za pośrednictwem wiersza poleceń powinien odbywać się za pośrednictwem szyfrowanego rozwiązania SSH zamiast niezabezpieczonego protokołu Telnet. Uwierzytelnianie w przypadku dostępu przez API nie powinno odbywać się przy pomocy otwartego tekstu, a sama sesja powinna być zaszyfrowana.

EN-SS-R5 — Włączenie trybu FIPS dla środowisk opartych na FIPS: Norma FIPS 1403 określa, że moduł kryptograficzny powinien stanowić połączenie urządzenia sprzętowego, oprogramowania, oprogramowania układowego lub wybranych elementów, które realizują funkcje lub procesy kryptograficzne, w tym algorytmy kryptograficzne; mogą także odpowiadać za generowanie kluczy kryptograficznych. Tego rodzaju moduł powinien obsługiwać wybrane algorytmy kryptograficzne. FIPS określa pewne algorytmy kryptograficzne jako bezpieczne i wskazuje, jakie algorytmy powinny być stosowane, jeśli dany moduł kryptograficzny ma być określony jako zgodny z FIPS. Organizacje, których systemy są zgodne z normą FIPS, powinny upewnić

się, że tryb FIPS jest włączony w urządzeniach wchodzących w skład infrastruktury pamięci masowej zgodnych z tą normą.

EN-SS-R6 – Szyfrowanie wrażliwych danych w stanie spoczynku: Szyfrowanie w stanie spoczynku chroni przed różnymi zagrożeniami dotyczącymi danych, w tym przed nieautoryzowanym dostępem, kompromitacją w przypadku utraty lub kradzieży nośnika i innymi ryzykami. Powinno zostać włączone w przypadku danych wrażliwych. Należy przy tym wziąć pod uwagę następujące kwestie:

- **Stosowanie szyfrowania zapewnianego przez elementy infrastruktury:** Korzystanie z funkcji szyfrowania zapewnianych przez dysk, macierz dyskową lub macierz dyskową w chmurze, niezależnie od wykorzystania kluczy dostawcy bądź kluczy organizacji, może chronić przed utratą, zgubieniem lub kradzieżą urządzenia, jednak nie jest uważane za skuteczne zabezpieczenie przed:
  - ✓ **Atakami wewnątrz pasma –** z taką sytuacją mamy do czynienia, gdy napastnik naruszy zasady ochrony hosta podłączonego do pamięci masowej lub gdy dojdzie do podłączenia pamięci masowej do nieautoryzowanego hosta przy pomocy standardowych metod.
  - ✓ **Atakami polegającymi na eskalacji uprawnień –** administratorzy lub napastnicy uzyskujący podwyższone uprawnienia mogą wyłączyć szyfrowanie lub odszyfrować dane.
- **Używanie szyfrowania typu „end-to-end”:** Dane są szyfrowane u źródła – na przykład w aplikacji, w bazie danych, na woluminie; infrastruktura pamięci masowej oraz administratorzy mają dostęp jedynie do postaci zaszyfrowanej. Choć takie rozwiązanie znacząco zwiększa bezpieczeństwo, szyfrowanie na poziomie aplikacji wiąże się z pewnymi wadami, które w wybranych przypadkach mogą okazać się znaczące:
  - ✓ **Negatywny wpływ na mechanizmy redukcji danych –** Szyfrowanie może spowodować, że mechanizmy kompresji i deduplikacji staną się znacznie mniej skuteczne i wydajne.
  - ✓ **Powoduje to także zwiększenie złożoności zarządzania.**

- **Stosowanie podwójnych, niezależnych warstw szyfrowania:** W miarę możliwości należy rozważyć stosowanie takiego rozwiązania w przypadku danych wrażliwych. Taka konfiguracja zwiększa bezpieczeństwo danych w przypadku kompromitacji klucza szyfrującego, zwłaszcza jeśli używane są różne algorytmy kryptograficzne.
- **Należy wziąć pod uwagę wymogi dotyczące przechowywania danych:** Jeśli zaszyfrowane dane stanowią część kopii zapasowej lub są archiwizowane, powiązane z nimi klucze należy chronić przez cały czas przechowywania tych kopii. Alternatywnym rozwiązaniem jest ponowne zaszyfrowanie zarchiwizowanych danych przy pomocy nowego klucza. Niezależnie od zastosowanego rozwiązania, dane i klucze szyfrowania nie powinny być przechowywane w jednym miejscu.

EN-SS-R7 – Szyfrowanie przesyłanych danych:

a. **Przesyłanie bloków w protokole Fibre-Channel**: Szyfrowanie połączeń opartych na protokole FC nie jest obecnie obsługiwane przez większość producentów kontrolerów pamięci masowych oraz systemów pamięci masowych, choć stosowne zalecenia zostały opisane w dokumencie ANSI/ INCITS 545-2019, Information Technology - Fibre-Channel - Framing and Signaling - 5 (FC-FS-5). W przypadku informacji wrażliwych należy stosować szyfrowanie typu end-to-end na całej trasie, od hosta do systemu pamięci masowej.

b. **Przesyłanie bloków w sieciach IP:** Przesyłanie danych do systemu pamięci masowej w sieci IP wiąże się z takimi samymi zagrożeniami bezpieczeństwa jak przesyłanie innego ruchu w standardowych sieciach IP. W domyślnej konfiguracji protokoły przesyłu bloków w sieciach IP nie zapewniają poufności, integralności ani uwierzytelniania danych w każdym pakiecie. Podobnie jak w przypadku szyfrowania połączeń w protokole FC, choć istnieją stosowne specyfikacje dotyczące szyfrowania ruchu związanego z pamięciami masowymi w sieciach IP, dostępne na rynku rozwiązania nie obsługują ich natywnie. W przypadku korzystania z protokołów opartych na sieciach IP, takich jak iSCSI, FCIP czy własnościowe protokoły wybranych producentów, należy rozważyć możliwość wykorzystania tunelowania IPsec w celu ochrony

niezabezpieczonych segmentów sieci. Co więcej, w przypadku informacji wrażliwych należy stosować szyfrowanie typu end-to-end na całej trasie, od hosta do systemu pamięci masowej.

c. **Dostęp do plików i obiektów w pamięci masowej:** Należy włączyć opcje szyfrowania danych „w locie" w systemach kopii zapasowych i systemach wykorzystywanych do replikacji danych, jeśli takie rozwiązania są obsługiwane. W przypadku dostępu do plików, dane wrażliwe powinny być przesyłane i szyfrowane przy użyciu mechanizmów takich jak szyfrowanie SMB oraz dostępne opcje szyfrowania NFS, w tym rozwiązania oferowane przez dostawców chmur, a także protokół NFS z szyfrowaniem opartym na protokole TLS z wykorzystaniem tunelowania – na przykład „stunnel". Należy upewnić się, że wszelki dostęp do obiektów odbywa się przy pomocy protokołu HTTPS z szyfrowaniem TLS.

d. **Komunikacja sieciowa poza granicami fizycznej ochrony:** Szczególną uwagę należy zwrócić na kwestię włączenia szyfrowania na każdym etapie łączności, który rozszerza komunikację sieciową poza granice fizycznej ochrony, na przykład łącze wykorzystujące protokół ISL (*ang. Inter Switch Link*) między dwoma fizycznie oddzielonymi centrami danych, ruch IP przez sieć WAN lub Internet.

EN-SS-R8 — Komunikacja między elementami systemu pamięci masowej powinna być szyfrowana: Należy przeanalizować interakcje elementów systemu pamięci masowej i włączyć dostępne opcje szyfrowania. Szyfrowanie powinno być stosowane do ochrony komunikacji pomiędzy węzłami pamięci masowej i hostami odpowiedzialnymi za zarządzanie, pomiędzy aktywnymi węzłami pamięci masowej i innymi urządzeniami, pomiędzy węzłami i serwerami zasad oraz serwerami odpowiedzialnymi za ochronę antywirusową.

EN-SS-R9 – Wymagania dotyczące zarządzania kluczami szyfrowania: Należy przestrzegać ogólnych zaleceń zawartych w dokumencie NIST SP 800-57 Parts 1-3 dotyczących zarządzania kluczami kryptograficznymi, w szczególności czasu użytkowania, maksymalnej ilości danych, które mogą być zabezpieczone przy pomocy pojedynczego klucza, infrastruktury zarządzania kluczami, wymiany kluczy, kontroli kluczy oraz tworzenia kopii zapasowych i odtwarzania kluczy.

4.10 Dostęp administracyjny

Dostęp administracyjny jest wymagany do kontroli i zarządzania niemal wszystkimi rodzajami infrastruktur IT. W tej części dokumentu zawarto zalecenia dotyczące dostępu administracyjnego do elementów pamięci masowej, w tym macierzy, sieci oraz sieci szkieletowych, narzędzi do zarządzania, kopii zapasowych, systemów do replikacji danych oraz systemów pamięci masowej w chmurze. Dostęp administracyjny może opierać się na bezpośrednim połączeniu z komponentem pamięci masowej oraz poprzez oprogramowanie zarządzające. Niezależnie od rodzaju połączeń, mogą wiązać się one z użytkowaniem różnych interfejsów, w tym interfejsu zarządzania, wiersza poleceń bądź API.

Zabezpieczenie dostępu administracyjnego ma niezwykle ważne znaczenie ze względu na fakt, że większość zagrożeń związanych z systemami pamięci masowej omówione w podrozdziale 3.2 niniejszego dokumentu, w tym zagrożenia niosące za sobą ryzyko największych strat, mogą być związane z niedostatecznym zabezpieczeniem dostępu administracyjnego.

Niektóre podrozdziały zawarte w tym rozdziale omawiają pewne zagadnienia, które są związane z dostępem administracyjnym. W celu uniknięcia zbędnych powtórzeń, istotne zalecenia związane z tym zagadnieniem znajdują się także w:

- podrozdziale 4.9 dotyczącym szyfrowania,
- podrozdziale 4.3 dotyczącym kontroli dostępu do danych, w którym część zaleceń może dotyczyć także zagadnienia administracji.

W przypadku konfiguracji dostępu administracyjnego (*ang. administrative access – AA*) zaleca się stosowanie następujących zaleceń dotyczących bezpieczeństwa.

AA-SS-R1 – Ograniczenie dostępu sieciowego do portów zarządzania przełączników SAN: Dostęp sieciowy do portów zarządzania przełączników SAN powinien być ograniczony do urządzeń i administratorów wyznaczonych do zarządzania przełącznikami poprzez mechanizm taki jak lista kontroli dostępu (ACL).

AA-SS-R2 – Kontrolowanie i ograniczenie liczby urządzeń i składników infrastruktury posiadających przywileje administracyjne do wymaganego minimum: Obejmuje to wiersze poleceń, konsole zarządzania, bramy API, hosty oraz urządzenia pamięci masowej z uprawnieniami kontrolnymi. Przede wszystkim należy:

a. Aktywnie wykrywać urządzenia posiadające możliwość zarządzania pamięcią masową, aby ograniczyć uprawnienia wyłącznie do autoryzowanych urządzeń. W przypadku wykrycia urządzeń, które nie powinny posiadać uprawnień, należy je usunąć i udokumentować ten fakt.

b. Wyłączyć nadmiarowe uprawnienia.

AA-SS-R3 – Wdrożenie zasady przydzielania minimalnych uprawnień: Należy ograniczyć uprawnienia użytkowników z uprawnieniami administracyjnymi do wymaganego minimum. Dotyczy to zarówno czynności, które może wykonać użytkownik, jak i ograniczeń zakresu uprawnień do stosownych systemów lub regionów. Pełne prawa administracyjne powinny być przyznawane tylko użytkownikom, którzy potrzebują ich do wykonywania swoich obowiązków.

AA-SS-R4 – Ograniczenie praw dostępu dla kont serwisowych: Konta serwisowe, w tym konta wykorzystywane przez narzędzia monitorujące, powinny dysponować uprawnieniami pozwalającymi wyłącznie na odczyt danych i metadanych.

AA-SS-R5 – Uwierzytelnianie i autoryzacja wszystkich przypadków dostępu przy pomocy wiersza poleceń bądź API: Korzystanie z wiersza poleceń bądź API powinno wiązać się z koniecznością przeprowadzenia uwierzytelniania i autoryzacji. W przypadkach, gdy nie jest możliwe przeprowadzenie uwierzytelnienia lub autoryzacji, należy zabezpieczyć nieautoryzowany dostęp za pomocą dodatkowych mechanizmów bezpieczeństwa, takich jak narzędzia do zarządzania uprawnieniami w celu ograniczenia do wymaganego minimum uprawnień i dostępu użytkownika.

AA-SS-R6 – Dostęp przez API zamiast dostępu przez wiersz poleceń (CLI) lub powłokę (Shell access): Jeśli istnieje taka możliwość, dostęp do systemów przez interfejs programowy aplikacji API powinien być wybierany zamiast dostępu przez wiersz poleceń lub powłokę systemową ze względu na możliwość dostępu do systemu operacyjnego i systemu plików, w tym plików konfiguracyjnych, przy użyciu tych rozwiązań. Jeśli

dostęp przy pomocy wiersza poleceń jest jedyną dostępną opcją, należy używać go za pośrednictwem bezpiecznych protokołów, takich jak SSH, zgodnie z zaleceniem **EN-SS-R4**.

AA-SS-R7 – Ograniczenie uprawnień konsoli zarządzania w systemach operacyjnych: Dostęp do konsoli zarządzania powinien być realizowany wyłącznie za pośrednictwem wyznaczonych kont, nie zaś przy pomocy konta administracyjnego systemu operacyjnego (por. **AC-SS-R20)**.

AA-SS-R8 – Zabezpieczenie dostępu administracyjnego z poziomu interfejsu webowego: Dostęp do konsoli zarządzania przez interfejs webowy powinien zostać zabezpieczony w taki sposób, by spełniać lub przewyższać normy bezpieczeństwa dotyczące innych serwerów aplikacji internetowych w organizacji.

AA-SS-R9 – Ograniczenie uprawnień hosta do zmiany konfiguracji pamięci masowej: W wybranych konfiguracjach klastrów obliczeniowych połączonych z magazynami danych, takich jak na przykład: klastry, geoklastry lub infrastruktury wirtualizacji pamięci masowej, poszczególne hosty otrzymują dostęp administracyjny do pamięci masowej w celu sterowania alokacją i zachowaniem zasobów danych klastra. Gdy przydzielenie w tym celu dostępu administracyjnego jest konieczne, należy ograniczyć zakres uprawnień przyznawanych hostów do:

a. wybranych elementów takich jak: LUN, udostępnienia, pliki, obiekty, którymi zarządzają hosty,

b. wybranych zadań, które muszą realizować hosty.

AA-SS-R10 – Konfiguracja urządzeń kontrolnych (*ang. gatekeeper; command device*): Niektóre macierze dyskowe pozwalają na dostęp administracyjny z poziomu hostów, które mają dostęp do specjalnych urządzeń blokowych określanych mianem urządzeń kontrolnych. Polecenia są przekazywane za pomocą operacji wejścia/wyjścia przy pomocy tych specjalnych urządzeń. W przypadku stosowania takich rozwiązań zaleca się wdrożenie następujących rekomendacji dotyczących bezpieczeństwa:

a. **Ograniczenie stosowania urządzeń kontrolnych do niezbędnego minimum:** Jeśli to możliwe, należy całkowicie wykluczyć korzystanie z takich urządzeń, zastępując korzystanie z nich na przykład dostępem przez API. Jeśli nie jest to

możliwe, należy upewnić się, że zostały połączone wyłącznie z wybranymi hostami, na przykład hostami odpowiedzialnymi za zarządzanie.

b. **Należy przeskanować sieć w poszukiwaniu urządzeń kontrolnych –**Należy przeprowadzić skanowanie sieci w celu wykrycia urządzeń kontrolnych i upewnić się, że zostały połączone wyłącznie z autoryzowanymi hostami.

AA-SS-R11– Wyłączanie lub ograniczanie komunikacji z serwerami producenta oraz dostępu zdalnego: Systemy infrastruktury pamięci masowej mogą mieć możliwość przesyłania producentom pewnych danych telemetrycznych i diagnostycznych, w tym plików dziennika. W wybranych przypadkach możliwe jest zdalne połączenie z systemem przez producenta, który dysponuje uprawnieniami administracyjnymi. Mechanizmy te zostały wprowadzone, aby umożliwić producentom weryfikację, diagnostykę oraz rozwiązywanie problemów technicznych, a także instalowanie automatycznych aktualizacji oprogramowania. Takie możliwości mogą być także wykorzystane przez hakerów i powinny być wyłączone, jeśli ich stosowanie nie jest bezwzględnie konieczne. W sytuacji, gdy ich stosowanie jest wymagane, powinny być w miarę możliwości ograniczone i zabezpieczone poprzez wdrożenie następujących ustawień:

a. **Zmiana domyślnych poświadczeń –** Należy zmienić domyślne poświadczenia wykorzystywane w celu nawiązania zdalnego połączenia.

b. **Ograniczenie uprawnień** – Należy ograniczyć uprawnienia dostępu do minimalnego wymaganego poziomu.

c. **Wymuszenie szyfrowania** – Należy wymusić stosowanie bezpiecznych protokołów takich jak TLS/SSH/IPSec wykorzystujących dopuszczone algorytmy szyfrowania.

d. **Ograniczenie dostępu za pomocą listy dostępu** – Należy wykorzystać listę dostępu, która ogranicza możliwość połączenia wyłącznie do określonych adresów IP oraz wybranych użytkowników.

e. **Zapewnienie kompleksowego dokumentowania przypadków dostępu zdalnego** – Każdy przypadek zdalnego dostępu do systemu powinien być udokumentowany w plikach dziennika na potrzeby kontroli.

f. **Włączenie wbudowanych funkcji obfuskacji danych –** Niniejszy punkt dotyczy urządzeń pamięci masowej, które umożliwiają obfuskację danych wrażliwych, takich jak: adresy IP, nazwy WWN, nazwy urządzeń i nazwy użytkowników.

g. **Ograniczenie zakresu przesyłanych danych** – Zakres przesyłanych danych należy ograniczyć do niezbędnego minimum.

h. **Przegląd i zatwierdzanie –** Okresowo należy przeglądać dane przesyłane do producenta urządzenia, aby upewnić się, że nie zawierają one wrażliwych informacji, takich jak adresy IP, nazwy użytkowników lub informacje na temat danych przechowywanych w urządzeniach pamięci masowej. Należy sprawdzić, czy połączenie jest nawiązywane z adresami IP należącymi do producenta urządzeń.

i. **Potwierdzanie połączeń –** Jeśli istnieje techniczna możliwość, należy wdrożyć mechanizm, który zapyta o pozwolenie przed nawiązaniem połączenia.

j. **Ograniczenie dostępu do bramy (*ang. gateway*) –** Jeśli zdalny dostęp producenta jest realizowany za pośrednictwem urządzenia, serwera lub bramy, należy zwrócić szczególną uwagę na zabezpieczenie i ograniczenie dostępu do bramy.

k. **Wyłączenie aktualizacji oprogramowania przy pomocy zdalnego dostępu –** W środowiskach wrażliwych nie należy zezwalać na pobieranie i instalowanie składników oprogramowania oraz aktualizacji (ręcznych lub automatycznych) poprzez zdalny dostęp.

AA-SS-R12– Ograniczenie dostępu do sieci zarządzania: Oprócz oddzielenia ruchu związanego z zarządzaniem od pozostałego ruchu w sieci (por. rozdziały 4.6 i 4.7) w środowiskach wrażliwych zaleca się dodatkowe ograniczenie dostępu do sieci zarządzania poprzez zastosowanie takich mechanizmów jak:

a. **Korzystanie z wirtualnych sieci prywatnych (VPN), protokołu szyfrowania danych IPsec lub serwera pośredniczącego –** Korzystanie z rozwiązań takich jak VPN, protokół szyfrowania danych IPsec, a także jednego lub kilku serwerów pośredniczących lub proxy uwierzytelniających będących jedynymi serwerami w sieci zarządzania dostępnymi z zewnątrz, które mogą posłużyć do nawiązania połączeń z innymi serwerami po odpowiednim uwierzytelnieniu i autoryzacji.

b. **Wdrożenie ulepszonych mechanizmów rejestracji i śledzenia –** Takie mechanizmy mogą obejmować na przykład zapis sesji.

AA-SS-R13 – Zabezpieczanie i ochrona kluczowych plików oraz plików binarnych związanych z zarządzaniem pamięcią masową: Oprogramowanie do zarządzania pamięcią masową często obejmuje pliki konfiguracyjne zawierające różne opcje wpływające na sposób działania systemu pamięci masowej, w tym opcje nieudokumentowane. Takie wrażliwe katalogi i pliki powinny być przechowywane w sposób gwarantujący dostęp wyłącznie uprawnionym użytkownikom, przypisanym do stosownych grup. Zakres takich danych obejmuje:

- **Pliki konfiguracyjne –** Zawierające informacje na temat kont użytkowników i ich ról, ustawień sieciowych, grup urządzeń oraz ustawień systemu pamięci masowej. Pliki konfiguracyjne zawierające informacje na temat grup i urządzeń są w wielu przypadkach przesyłane automatycznie przez hosty centralnego zarządzania do innych hostów podłączonych do systemu pamięci masowej. Skompromitowanie tego pliku może mieć znaczący negatywny wpływ na wiele systemów.
- **Skrypty –** Skrypty wykorzystywane do sterowania uruchamianiem, monitorowaniem i zatrzymywaniem usług i procesów odpowiedzialnych za zarządzanie pamięcią masową, a także pliki binarne powinny być odpowiednio zabezpieczone.

Do plików konfiguracyjnych, skryptów i wszelkich innych ważnych plików związanych z zarządzaniem systemami pamięci masowych należy zastosować następujące mechanizmy zabezpieczające:

a. Ograniczenie dostępu i uprawnień, kontrolowanie przypisania kluczowych folderów i plików.

b. W przypadku środowisk wrażliwych należy rozważyć monitorowanie zmian zawartości takich plików, aby zapobiec przypadkom wprowadzania nieautoryzowanych zmian.

AA-SS-R14 – Zastosowanie zatwierdzonego mechanizmu PKI w celu ograniczenia dostępu do opcji zarządzania: W celu uzyskiwania dostępu do interfejsów zarządzania urządzeniami pamięci masowej oraz konsoli zarządzania pamięcią masową należy

używać zatwierdzonego i certyfikowanego przez organizację scentralizowanego systemu PKI, nie zaś certyfikatów dostarczanych z urządzeniem lub oprogramowaniem.

4.11 Zarządzanie konfiguracją

Celem zarządzania konfiguracją jest zapewnienie wglądu i kontroli nad ustawieniami, zachowaniem oraz fizycznymi i logicznymi atrybutami zasobów pamięci masowej w całym ich cyklu życia.

W kontekście bezpieczeństwa magazynowania danych obejmuje to:

- prowadzenie kompleksowego przeglądu konfiguracji,
- zarządzanie zmianami, a także
- zapewnianie, że konfiguracja stale spełnia podstawowe założenia w zakresie bezpieczeństwa przyjęte przez organizację oraz jest zgodna z najlepszymi praktykami branżowymi, a także że nie prowadzi do występowania znanych zagrożeń.

W tym celu konieczne jest przeprowadzanie stosownych kontroli, wdrażanie zasad, wprowadzanie procesów oraz wykorzystywanie odpowiednich narzędzi. Kompleksowe rekomendacje dotyczące zarządzania konfiguracją w IT zawiera dokument NIST Special Publication (SP) 800-53 [28]. Poniższe punkty zawierają zalecenia dotyczące zarządzania konfiguracją (*ang. Configuration Management – CM*) infrastruktury pamięci masowej.

CM-SS-R1 – Kompleksowe katalogowanie wszystkich urządzeń pamięci masowej: Proces ten powinien obejmować ustalenie nazw, adresu, lokalizacji oraz wersji oprogramowania, oprogramowania układowego oraz wersji sterowników wszystkich elementów infrastruktury pamięci masowej, w tym:

- macierzy pamięci masowej,
- systemów wirtualizacji pamięci masowej,
- konsoli zarządzania,

- hostów wykorzystywanych do monitorowania stanu połączenia pamięci masowej z siecią,
- hostów z zainstalowanym oprogramowaniem do zarządzania pamięcią masową lub wtyczkami,
- urządzeń wykorzystywanych do ochrony danych,
- klientów i serwerów wykorzystywanych do tworzenia kopii zapasowych,
- przełączników sieciowych wykorzystywanych przez system pamięci masowej,
- kontrolerów pamięci masowej (HBA),
- oprogramowania do obsługi wielościeżkowości wejścia/wyjścia,
- powiązań podstawowych i docelowych systemów pamięci masowej wykorzystywanych w celu replikacji,
- wyznaczonych serwerów kopii zapasowych dla hostów lub kopii zapasowych przechowywanych poza siedzibą organizacji,
- bibliotek i napędów taśmowych; a także
- dysków i nośników wymiennych.

CM-SS-R2 – Opracowanie kompleksowego katalogu wszystkich zbiorów danych i konfiguracji: Proces ten powinien obejmować ustalenie logicznych zbiorów danych oraz konfiguracji dostępu do danych związanych z następującymi elementami:

- pule pamięci masowej, LUN, maskowanie, strefy,
- inicjatorzy i grupy inicjowania,
- udziały w plikach i listy kontroli dostępu,
- magazyny obiektów, pojemniki, itp.,
- repliki danych oraz migawki,
- katalog kopii zapasowych i uprawnień dostępu,
- zestawy kopii zapasowych znajdujące się w siedzibie organizacji zarchiwizowane, zwirtualizowane w chmurze, na taśmach, na urządzeniach archiwizujących itp.,

- użytkownicy, grupy, role i uprawnienia,
- konfiguracja dostępu hostów do zasobów pamięci masowej takich jak LUN, udziały, globalne systemy plików, magazyny obiektów,
- obrazy oprogramowania związane z systemami pamięci masowej, maszynami wirtualnymi itp.

CM-SS-R3 – Opracowanie kompleksowych zasad bezpieczeństwa dotyczących pamięci masowych, w formie oddzielnego zbioru zasad lub jako części zasad bezpieczeństwa obowiązujących w organizacji. Zasady te powinny zawierać podstawowe konfiguracje systemów pamięci masowej i mogą być oparte na:

- zaleceniach zawartych w niniejszej publikacji i cytowanych źródłach,
- wewnętrznych normach bezpieczeństwa dotyczących pamięci masowych w organizacji,
- najlepszych praktykach związanych z bezpieczeństwem promowanych przez dostawców rozwiązań.

CM-SS-R4 – Aktualizowanie zasad bezpieczeństwa dotyczących pamięci masowych: Zasady bezpieczeństwa dotyczące pamięci masowych powinny być poddawane przeglądowi oraz aktualizowane okresowo, jednak nie rzadziej niż raz w roku. Zabezpieczenia bazowe powinny być aktualizowane zgodnie z najnowszymi zaleceniami producentów i ekspertów branżowych dotyczącymi systemów pamięci masowej oraz wybranych urządzeń pamięci masowej; przeglądu najlepiej dokonywać co najmniej raz na kwartał.

CM-SS-R5 – Okresowa i proaktywna ocena zgodności konfiguracji z zasadami bezpieczeństwa dotyczącymi pamięci masowych:

a. Należy upewnić się, że rzeczywista konfiguracja jest zgodna z wymogami dotyczącymi zabezpieczeń bazowych dla pamięci masowych oraz zidentyfikować wszelkie rozbieżności.

b. Należy zadbać o niezwłoczne usunięcie nieprawidłowości i upewnić się, że problemy zostały rozwiązane.

c. Należy rozważyć możliwość opracowania wskaźników KPI do monitorowania zgodności z wymogami dotyczącymi zabezpieczeń bazowych dla pamięci masowych opartych na rodzajach danych, ich znaczeniu dla organizacji oraz stopnia ich wrażliwości.

CM-SS-R6 – Opracowanie procesu zarządzania zmianami związanymi z systemami pamięci masowej w formie osobnego procesu bądź elementu szerszego procesu zarządzania zmianami w organizacji. Proces ten powinien obejmować:

a. planowanie, przegląd i zatwierdzanie zmian w konfiguracji systemów pamięci masowej,

b. aktualizację dokumentacji oraz katalogów związanych ze środowiskiem, w tym informacji na temat elementów infrastruktury, danych, konfiguracji,

c. ocenę zgodności z wymogami dotyczącymi zabezpieczeń bazowych w przypadku dokonania jakichkolwiek zmian dotyczących środowisk, w których przechowywane są dane wrażliwe.

CM-SS-R7 – Wykrywanie nieautoryzowanych zmian dotyczących mechanizmów bezpieczeństwa pamięci masowej: Należy wdrożyć proces umożliwiający wykrywanie nieautoryzowanych zmian konfiguracji systemów pamięci masowej oparty na analizie plików dziennika, porównywaniu konfiguracji pamięci masowej z poprzednimi stanami, a także porównania z zatwierdzonymi przez organizację wymogami dotyczącymi zabezpieczeń bazowych.

CM-SS-R8 – Instalowanie aktualizacji oprogramowania i poprawek bezpieczeństwa:

a. **Należy upewnić się, że oprogramowanie systemów pamięci masowej jest na bieżąco aktualizowane.** W tym celu należy wdrożyć proces okresowej aktualizacji oprogramowania systemów pamięci masowej do najnowszej dostępnej stabilnej i bezpiecznej wersji. Działanie to powinno obejmować oprogramowanie wykorzystywane do zarządzania systemem, pakiety API oraz CLI, oprogramowanie układowe macierzy i kontrolerów pamięci masowej, a także sterowniki wykorzystywane przez systemy operacyjne.

b. **Należy upewnić się, że wszystkie ważne aktualizacje zabezpieczeń oraz poprawki bezpieczeństwa są zainstalowane.** W tym celu należy wdrożyć proces zapewniający proaktywne i częste instalowanie ważnych i krytycznych poprawek bezpieczeństwa systemów pamięci masowej.

c. **Należy wprowadzić plan ograniczający skutki braku stosownych poprawek bezpieczeństwa.** Jeśli element infrastruktury pamięci masowej zawiera podatność o znaczeniu krytycznym, dla której producent nie wydał jeszcze aktualizacji lub poprawki, takie urządzenie powinno zostać wycofane z eksploatacji, chyba że możliwe jest opracowanie stosownego planu łagodzenia skutków danej podatności.

CM-SS-R9 – Dokumentacja topologii sieci: Należy prowadzić dokumentację sieci związanej z systemami pamięci masowej oraz dbać o regularną aktualizację dokumentacji, także grafów, zarówno w przypadku sieci FC, jak i IP.

CM-SS-R10 – Kontrola konfiguracji zabezpieczeń FC SAN: Z upływem czasu niektóre zmiany w zabezpieczeniach mogą nie być propagowane we wszystkich przełącznikach sieci szkieletowej. Rozwiązania FC SAN należy poddawać okresowym przeglądom (podobnie jak w przypadku sieci IP i Ethernet), aby ocenić ich bezpieczeństwo, zidentyfikować i sklasyfikować podatności oraz opracować plan korekcji wszelkich problemów. Kontrola bezpieczeństwa powinna być przeprowadzana co najmniej raz w roku, a w środowiskach wrażliwych co najmniej raz na kwartał lub po każdej znaczącej zmianie, w zależności od tego, co nastąpi wcześniej. Wyniki kontroli powinny być udokumentowane.

4.12 Szkolenia w zakresie bezpieczeństwa systemów pamięci masowych

ST-SS-R1 – Przeprowadzenie szkolenia dotyczącego bezpieczeństwa systemów pamięci masowych: Należy opracować program szkoleń dotyczących bezpieczeństwa *(ang. security training – ST)* systemów pamięci masowych i włączyć go do istniejących w organizacji programów i harmonogramów szkoleń, by przeszkolić następujące grupy:

- **Specjaliści ds. bezpieczeństwa informacji –** Odbywają szkolenie w celu zdobycia podstawowej wiedzy na temat bezpieczeństwa systemów pamięci masowych.

- **Administratorzy systemów pamięci masowych –** Odbywają szkolenie w celu zapoznania się z zasadami bezpieczeństwa systemów pamięci masowych oraz zatwierdzonymi przez organizację wymogami dotyczącymi zabezpieczeń bazowych.
- **Przełożeni –** Odbywają szkolenie w celu zapoznania się z podstawowymi zagadnieniami dotyczącymi ochrony danych.

5. PODSUMOWANIE I WNIOSKI

Wychodząc od przeglądu technologii pamięci masowej, niniejszy dokument omawia zagrożenia i wynikające z nich ryzyka związane z bezpiecznym korzystaniem z zasobów pamięci masowej. Dokument obejmuje również szczegółowe zalecenia związane z zapewnianiem bezpieczeństwa w różnych obszarach, które pozwalają na bezpieczne wdrożenie, konfigurację oraz korzystanie z rozwiązań pamięci masowej. Obszary te obejmują następujące zagadnienia:

- Obszary wspólne dla wszystkich infrastruktur IT, takie jak bezpieczeństwo fizyczne, uwierzytelnianie i autoryzacja, dzienniki audytu, konfiguracja sieci, zarządzanie zmianami, reagowanie na incydenty i odzyskiwanie danych, dostęp administracyjny i zarządzanie konfiguracją.
- Obszary dotyczące infrastruktur pamięci masowej, takie jak ochrona danych i poufności z wykorzystaniem szyfrowania, izolacja oraz zapewnienie możliwości odzyskania danych.

Obok infrastruktury obliczeniowej (obejmującej system operacyjny i osprzęt hosta) oraz sieciowej, infrastruktura pamięci masowej jest jednym z trzech podstawowych filarów IT. W porównaniu do innych obszarów poświęca się jej jednak stosunkowo mało uwagi, zwłaszcza z punktu widzenia bezpieczeństwa, mimo że naruszenie danych może mieć tak samo negatywny wpływ na organizację p, jak naruszenie bezpieczeństwa infrastruktury obliczeniowej i sieciowej. Zawarte w tym dokumencie zalecenia dotyczące bezpieczeństwa infrastruktur pamięci masowych stanowią podstawę do zabezpieczenia jednego z kluczowych elementów infrastruktury IT.

Zbudowanie skutecznego programu zarządzania ryzykiem dotyczącego infrastruktury pamięci masowej w oparciu o środki bezpieczeństwa opisane w niniejszym dokumencie i ścisłe zintegrowanie go z istniejącymi ramami cyberbezpieczeństwa [40] może znacząco poprawić odporność organizacji na różnego rodzaju ataki na zbiory danych.

ZAŁĄCZNIK A - REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[24]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

[24] Narodowe Standardy Cyberbezpieczeństwa

PUBLIKACJE ANGLOJĘZYCZNE[25]

[1] Storage Networking Industry Association (2020) *Storage Area Network (SAN)*. Available at https://www.snia.org/education/online-dictionary/term/storage-area-network

[2] Storage Networking Industry AssociationRDMA (2020) *Fibre Channel (FC)*. Available at https://www.snia.org/education/online-dictionary/term/fibre-channel

[3] Storage Networking Industry Association (2020) *What is iSCSI?* Available at https://www.snia.org/education/what-is-iscsi

[4] Authors (2014) Remote Direct Memory Access Protocol. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 7146. https://tools.ietf.org/html/rfc7146

[5] Infinibandta.org (2020) *InfiniBand Architecture Specification*. Available at https://www.infinibandta.org/ibta-specification/

[6] Haynes T (2016) Network File System (NFS) Version 4 Minor Version 2 Protocol. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 7862. https://tools.ietf.org/html/rfc7862

[7] Black D, Glasgow J, Faibish S (2012) Parallel NFS (pNFS) Block Disk Protection. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 6688. https://tools.ietf.org/html/rfc6688

[8] Storage Networking Industry Association (2020) *software-defined storage (SDS)*. Available at https://www.snia.org/education/online-dictionary/term/software-defined- storage

[9] Storage Networking Industry Association (2020) *storage virtualization*. Available at https://www.snia.org/education/online-dictionary/term/storage-virtualization

[25] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

[10] International Organization for Standardization/International Electrotechnical Commission (2020) ISO/IEC 27040:2015 – *Information technology – Security Techniques – Storage Security* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44404.html

[11] Matsuzawa K, Shinagawa T (2017) VM-aware Adaptive Storage Cache Prefetching, IEEE 9th International Conference on Cloud Computing Technology and Science, pp 65-73.

[12] Techtarget.com (2018) *Understanding VM-aware Storage*.Available at https://searchservervirtualization.techtarget.com/feature/Understanding-VM-aware- storage-options?_ga=2.152423088.840316297.1600174454-797189360.1599574299

[13] Webopedia (2020) *VM-aware storage*. Available at https://www.webopedia.com/TERM/V/vm-aware_storage.html

[14] ComputerWeekly.com (2020) *Storage for Containers and Virtual Environments*. Available at https://media.bitpipe.com/io_10x/io_102267/item_1306461/Storage_for_containers_and_virtual_environments.pdf

[15] Azeem SA, Sharma S (2019) Study of Converged Infrastructure & Hyper Converged Infrastructure As Future of Data Centre. *International Journal of Advanced Computer Research* 8(5):900. https://doi.org/10.26483/ijarcs.v8i5.3476

[16] Gartner (2016) *Magic Quadrant for Integrated Systems*. Available at https://www.gartner.com/document/3471517?ref=ddisp&refval=3500917

[17] Gartner (2019) *Magic Quadrant for Hyperconverged Infrastructure*. Available at https://www.gartner.com/document/3975501?ref=ddisp&refval=3975577

[18] Gartner (2016) *Critical Capabilities for Integrated Systems*. Available at https://www.gartner.com/document/3500917?ref=ddisp&refval=3471517

[19] Gartner (2018) *Cool Vendors in Storage Technologies*. Available at https://www.gartner.com/document/3893182?ref=solrAll&refval=240504932

[20] Trust Radius (2020) *Cloud Storage Systems*. Available at https://www.trustradius.com/cloud-storage

[21] Galibus T, Krasnoproshin VV, De Oliveira Albuquerque R, Pignaton de Freitas E (2016) Elements of Cloud Storage Security (Springer Nature, Switzerland AG)

[22] Storage Networking Industry Association (2018) *Storage Security: Data Protection* Available at https://www.snia.org/sites/default/files/security/SNIA-Data-Protection- TechWhitepaper.pdf

[23] Blueliv (2018) *Credential theft: the business impact of stolen credentials*. https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/credential-theft/credential-theft-blog-news-and-articles-blueliv/

[24] MalwarebytesLABS (2018) *Encryption 101: How to break encryption*. Available at https://blog.malwarebytes.com/threat-analysis/2018/03/encryption-101-how-to-break- encryption/

[25] TechNadu (2018) *How is Encryption cracked?*. https://www.technadu.com/how-is- encryption-cracked/36616/

[26] vpnmentor.com (2020) *Virus vs Malware vs Ransomware: What is the Difference in 2020*. Available at https://www.vpnmentor.com/blog/difference-between-malware-ransomware/

[27] Wikipedia (2020) *Privilege escalation*. Available at https://en.wikipedia.org/wiki/Privilege_escalation

[28] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[29] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[30] MSSPAlert (2019) *Ransom Attacks Target Backups, NAS (Network Attached Storage)*. Available at (https://www.msspalert.com/cybersecurity-news/attacks-target-nas- backups/)

[31] Wikipedia (2020) *Attack Surface*. Available at https://en.wikipedia.org/wiki/Attack_surface

[32] TechTarget-SearchITChannel (2007) *Fibre Channel man-in-the-middle attacks*. Available at https://searchitchannel.techtarget.com/feature/Fibre-Channel-man-in-the- middle-attacks

[33] Security Week (2018) *Hackers Can Stealthily Exfiltrate Data vis Power Lines*. Available at https://www.securityweek.com/hackers-can-stealthily-exfiltrate-data-power-lines

[34] Ross RS, Pillitteri V, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[35] Grassi P.A, Fenton J.L, Lefkovitz N.B, Danker J.M, Choong Y.Y, Greene K.K, Theofanos M.F (2020) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63a

[36] Grassi P.A, Fenton J.L, Newton E.M, Perlner R.A, Regenscheid A.R, Burr W, Richer J.P (2020) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63b

[37] McKay K.A, Cooper D.A (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (NIST SP800-52 Rev2). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52 Rev 2. https://doi.org/10.6028/NIST.SP.800-52r2

[38] SNIA (2020) *TLS Specification for Storage Systems Version 1.1*. Available at https://www.snia.org/educational-library/tls-specification-storage-systems-version-1-1-2020

[39] Department of Homeland Security (2017) *Reducing the Risk of SNMP Abuse*. Available at https://us-cert.cisa.gov/ncas/alerts/TA17-156A

[40] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[41] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

ZAŁĄCZNIK B - AKRONIMY

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Wybrane akronimy użyte w treści niniejszego dokumentu zostały rozwinięte i zdefiniowane poniżej.

Akronim	Terminologia angielska	Terminologia polska
ACL	Access Control List	Lista kontroli dostępu
API	Application Programming Interface	Interfejs programistyczny aplikacji
BC	Business Continuity	Ciągłość działania
BIOS	Basic Input/Output System	Podstawowy system wejścia/wyjścia[26]
BLOB	Binary Large Object	Duży obiekt binarny
CAS	Content Addressable Storage	Pamięć masowa adresowana treścią
CDN	Content Delivery Networks	Sieć dostarczania treści
CDP	Continuous Data Protection	Ciągła ochrona danych
CHAP	Challenge-Handshake Authentication Protocol	Protokół uwierzytelniania
CIFS	Common Internet File System	Protokół CIFS lub sieciowy system plików (w środowisku Windows)
CISO	Chief Information Security Officer	Kluczowa osoba odpowiedzialna za. bezpieczeństwo informacji
CLI	Command Line Interface	Wiersz poleceń
CPU	Central Processing Unit	Procesor
CSI	Container Storage Interface	Interfejs kontenerowej pamięci masowej

[26] W niniejszej publikacji termin ten odnosi się do oprogramowania rozruchowego opartego na konwencjonalnym BIOS-ie, Extensible Firmware Interface (EFI) oraz Unified Extensible Firmware Interface (UEFI).

Akronim	Terminologia angielska	Terminologia polska
CSO	Chief Security Officer	Kluczowa osoba odpowiedzialna za bezpieczeństwa (pojęcie stosowane wymiennie z CISO)
CTO	Chief Technology Officer	Kluczowa osoba odpowiedzialna za technologię
DAS	Directly Attached Storage	Pamięć masowa podłączona bezpośrednio
DDoS	Distributed Denial of Service	Atak typu rozproszona odmowa usługi
DMA	Direct Memory Access	Bezpośredni dostęp do pamięci
DoS	Denial of Service	Atak typu odmowa świadczenia usługi
DR	Disaster Recovery	Odtwarzanie po katastrofie
FC	Fibre-Channel	Standard magistrali szeregowej
FCF	FCoE Forwarder	Typ przełącznika sieciowego
FCIP	Fibre-Channel over IP	Nazwa protokołu
FCoE	Fibre-Channel over Ethernet	Nazwa protokołu
FIP	FCoE Initialization Protocol	Nazwa protokołu
FIPS	Federal Information Processing Standards	Federalne standardy przetwarzania informacji
FTP	File Transfer Protocol	Protokół transferu plików
GNS	Global Name Server	Globalny serwer nazw
GPS	Global Positioning System	Globalny system pozycjonowania
HBA	Host Bus Adapter –	Kontroler pamięci masowej
HCI	Hyper-Converged Infrastructure	Infrastruktura hiperkonwergentna
HDD	Hard Disk Drive	Dysk twardy

Akronim	Terminologia angielska	Terminologia polska
HPC	High Performance Computing	Systemy obliczeniowe dużej skali (dużej wydajności)
HTTP	HyperText Transfer Protocol	Nazwa protokołu
HTTPS	HyperText Transfer Protocol Secure	Nazwa protokołu
iFCP	Internet Fibre-Channel Protocol	Nazwa protokołu
IP	Internet Protocol	Nazwa protokołu
IS	Information Security	Bezpieczeństwo informacji
iSCSI	Internet Small Computer Systems Interface	Nazwa protokołu
ISL	Inter Switch Link	Nazwa protokołu
iSNS	Internet Storage Name Service	Nazwa protokołu
IT	Information Technology	Technologia informatyczna; Technologia informacyjna
JSON	JavaScript Object Notation	Nazwa formatu danych
KPI	Key Performance Indicator	Wskaźnik efektywności; Kluczowy wskaźnik efektywności
LAN	Local Area Network	Lokalna sieć komputerowa
LDAP	Lightweight Directory Access Protocol	Nazwa protokołu
LUN	Logical Unit Number	Identyfikator jednostki logicznej; Numer jednostki logicznej
LVM	Logical Volume Manager	Menadżer woluminów logicznych
MAC	Message Authentication Codes	Kody uwierzytelniania wiadomości

Akronim	Terminologia angielska	Terminologia polska
MD5	Message-Digest algorithm 5	Algorytm kryptograficzny MD5
MFA	Multi Factor Authentication	Uwierzytelnianie wieloskładnikowe
MITM	Man In The Middle	Rodzaj ataku
NAS	Network-attached Storage – Sieciowa macierz dyskowa NDMP Network Data Management Protocol	Nazwa protokołu wykorzystywanego w procesie tworzenia kopii zapasowych
NFS	Network File System	Protokół NFS lub sieciowy system plików (w środowisku Linux/Unix)
NIC	Network Interface Card	Karta sieciowa
NS	Name Server	Serwer nazw
NTP	Network Time Protocol	Nazwa protokołu
NVM	Non Volatile Memory	Pamięć nieulotna; pamięć trwała
NVMe	Non Volatile Memory express (nazwa protokołu	Specyfikacja urządzeń logicznych dotycząca urządzeń pamięci nieulotnej podłączanych za pomocą magistrali PCI Express
NVMe-oF	NVMe over Fibre	Nazwa protokołu
OS	Operating System	System operacyjny
OSI	Open Systems Interconnection	Model komunikacji pomiędzy systemami komputerowymi wykorzystywany w sieciach oraz telekomunikacji; model odniesienia łączenia systemów otwartych, wykorzystywany w sieciach oraz telekomunikacji
PBKDF2	Password-Based Key Derivation Function 2	Nazwa funkcji kryptograficznej

Akronim	Terminologia angielska	Terminologia polska
PCI	„Payment Card Industry” (w kontekście prawnym) oraz „Peripheral Component Interconnect”	Termin techniczny dotyczący magistrali komunikacyjnej w systemach komputerowych
PCI-DSS	Payment Card Industry Digital Security Standard	Norma bezpieczeństwa dotycząca płatności przy pomocy kart płatniczych
PCIe	PCI express	Nowoczesny wariant magistrali PCI
PII	Personally Identifiable Information	Dane osobowe
PKI	Public Key Infrastructure	Infrastruktura klucza publicznego
pNFS	Parallel NFS	Równoległy protokół NFS
PWWN	Port World-Wide Name	Globalna nazwa portu, pojęcie używane w systemach FC
QA	Quality Assurance	Zapewnianie jakości
QoS	Quality of Service	Jakość usługi
RDMA	Remote Direct Memory Access	Zdalny bezpośredni dostęp do pamięci
REST	Representational State Transfer	Zmiana stanu poprzez reprezentacje (nazwa architektury)
RFID	Radio-Frequency Identification	System zdalnej identyfikacji radiowej
RPO	Recovery Point Objective	Punkt odtworzenia danych; maksymalny (akceptowalny) punkt odtworzenia danych
RSH	Remote Shell	Zdalnie uruchamiana powłoka systemowa
RTO	Recovery Time Objective	Czas odzyskiwania
SAN	Storage Area Network	Sieć pamięci masowej
SATA	Serial Advanced Technology Attachment	Interfejs SATA

Akronim	Terminologia angielska	Terminologia polska
SCSI	Small Computer System Interface	Interfejs SCSI
SDS	Software-Defined Storage	Pamięć masowa definiowana programowo
SHA	Secure Hash Algorithm	Nazwa rodziny kryptograficznych funkcji skrótu
SIEM	Security Information and Event Management	Bezpieczeństwo informacji i zarządzanie zdarzeniami (nazwa rodziny oprogramowania
SMB	Server Message Block	Nazwa protokołu dostępu sieciowego do plików wykorzystywanego w systemach z rodziny Windows
SMI-S	Storage Management Initiative Specification	Nazwa specyfikacji
SNMP	Simple Network Management Protocol	Nazwa protokołu
SNS	Simple Name Server	Prosty serwer nazw
SOAP	Simple Object Access Protocol	Nazwa protokołu
SoC	System on Chip	System na układzie scalonym (czipie)
SPKM	Simple Public-Key GSS-API Mechanism	Nazwa technologii
SQL	Structured Query Language	Nazwa języka zapytań
SRP	Server Routing Protocol	Nazwa protokołu
SSD	Solid-State Drive	Dysk typu flash; dysk półprzewodnikowy
SSH	Secure Shell	Nazwa protokołu oraz standardu komunikacji
SSO	Single Sign On	Pojedyncze logowanie

Akronim	Terminologia angielska	Terminologia polska
TCP	Transmission Control Protocol	Nazwa protokołu
TLS	Transport Layer Security	Nazwa protokołu
TTL	Time To Live	Czas życia pakietu danych
UDP	User Datagram Protocol	Protokół UDP; protokół pakietów użytkownika
UI	User Interface	Interfejs użytkownika
USB	Universal Serial Bus	Uniwersalna magistrala szeregowa
VLAN	Virtual LAN	Wirtualna sieć lokalna
VM	Virtual Machine	Maszyna wirtualna
VPC	Virtual Private Cloud	Wirtualna chmura prywatna
VPN	Virtual Private Network	Wirtualna sieć prywatna
WAN	Wide Area Network	Sieć typu WAN; rozległa sieć informatyczna
WORM	Write Once Read Many	Jednokrotny zapis, wielokrotny odczyt (mechanizm)
WWN	World-Wide Name	Pojęcie wykorzystywane w protokole FC SAN
XML	eXtensible Markup Language	Nazwa języka