| NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA | Narodowy Standard Cyberbezpieczeństwa | | |
|---|---|---|---|
| Nazwa standardu | Symbol | Wersja | Data wydania |
| **Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD)** | **NSC 800-46** | 1.0 | 01/09/2021 |

# Przewodnik po telepracy w podmiocie publicznym

## Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD)

**PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA**

**Warszawa 2021**

***Szanowni Państwo,***

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

## WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji 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, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania innych standardów.

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

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

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

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi obowiązkami ustawowymi. Informacje zawarte w tej publikacji, 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, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD),*** opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-46 rev. 2.

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 występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

Występujące w publikacji odwołania do standardów NSC oraz ogólnodostępnych dokumentów anglojęzycznych NIST SP, FIPS, OMB stanowią uzupełnienie i rozszerzenie wiedzy na temat szerokorozumianego cyberbezpieczeństwa.

**Streszczenie**

W wielu organizacjach pracownicy, kontrahenci, partnerzy biznesowi, sprzedawcy i/lub inne osoby korzystają z technologii telepracy lub zdalnego dostępu w celu wykonywania pracy z lokalizacji zewnętrznych. Wszystkie komponenty tych technologii, w tym urządzenia klienckie wydawane przez organizację oraz urządzenia prywatne używane do wykonywania pracy na rzecz pracodawcy (*ang. bring your own device -BYOD*), powinny być zabezpieczone przed spodziewanymi zagrożeniami zidentyfikowanymi za pomocą modeli zagrożeń. Niniejsza publikacja zawiera informacje o względach bezpieczeństwa dla kilku typów rozwiązań zdalnego dostępu oraz zalecenia dotyczące zabezpieczenia różnych technologii telepracy, zdalnego dostępu i BYOD. Zawiera również porady dotyczące tworzenia odpowiednich polityk bezpieczeństwa.

**Słowa kluczowe**

przynieś swoje własne urządzenie (BYOD); bezpieczeństwo hosta; bezpieczeństwo informacji; bezpieczeństwo sieci; zdalny dostęp; telepraca.

# SPIS TREŚCI

## Streszczenie

W wielu organizacjach pracownicy, kontrahenci, partnerzy biznesowi, sprzedawcy i/lub inni użytkownicy korzystają z technologii telepracy w celu wykonywania pracy z lokalizacji zewnętrznych. Większość z tych osób używa technologii zdalnego dostępu do niepublicznych zasobów obliczeniowych organizacji. Natura technologii telepracy i zdalnego dostępu - pozwalająca na dostęp do chronionych zasobów z sieci zewnętrznych i często również z zewnętrznie kontrolowanych hostów - generalnie stawia je w grupie podwyższonego ryzyka w porównaniu z podobnymi technologiami, do których dostęp uzyskuje się tylko z wewnątrz organizacji, jak również zwiększa ryzyko zagrożenia wewnętrznych zasobów udostępnianych użytkownikom poprzez zdalny dostęp.

Wszystkie komponenty rozwiązań telepracy i zdalnego dostępu, w tym urządzenia klienckie, serwery zdalnego dostępu oraz zasoby wewnętrzne dostępne poprzez zdalny dostęp, powinny być zabezpieczone przed spodziewanymi zagrożeniami, zidentyfikowanymi za pomocą modeli zagrożeń. Główne problemy związane z bezpieczeństwem to brak fizycznych zabezpieczeń, korzystanie z niezabezpieczonych sieci, podłączanie zainfekowanych urządzeń do sieci wewnętrznych oraz dostępność zasobów wewnętrznych dla hostów zewnętrznych.

Dodatkowe problemy związane z bezpieczeństwem dotyczą organizacji, które zezwalają na korzystanie z urządzeń klienckich znajdujących się poza kontrolą organizacji, określanych w niniejszej publikacji jako technologie kontrolowane przez strony trzecie. Należą do nich urządzenia kontrolowane przez kontrahentów, partnerów biznesowych i dostawców, a także laptopy, smartfony i tablety będące własnością osobistą (*ang. bring your own device - BYOD*) pracowników, kontrahentów, partnerów biznesowych i dostawców. Nawet jeśli organizacja posiada umowy z pracownikami i stronami trzecimi, które wymagają, aby ich urządzenia klienckie były odpowiednio zabezpieczone, umowy te zazwyczaj nie mogą być automatycznie egzekwowane, więc niezabezpieczone, zainfekowane złośliwym oprogramowaniem i/lub w inny sposób zagrożone urządzenia mogą być podłączane do wrażliwych zasobów organizacyjnych. Niniejsza publikacja zawiera informacje dotyczące bezpieczeństwa kilku

typów rozwiązań zdalnego dostępu oraz zalecenia dotyczące zabezpieczania różnych technologii telepracy, zdalnego dostępu i rozwiązań typu „przynieś własne urządzenie (*BYOD*). Zawiera również porady dotyczące tworzenia odpowiednich polityk bezpieczeństwa. W celu poprawy bezpieczeństwa technologii telepracy i zdalnego dostępu w organizacji, a także lepszego ograniczania ryzyka zagrożeń sieci i systemów organizacji stwarzanego przez BYOD i technologie kontrolowane przez strony trzecie, organizacje powinny wdrożyć następujące zalecenia:

**Planuj polityki i środki bezpieczeństwa związane z pracą w sieci teleinformatycznej w oparciu o założenie, że środowiska zewnętrzne zawierają wrogie zagrożenia.**

Organizacja powinna założyć, że zewnętrzne obiekty, sieci i urządzenia zawierają wrogie zagrożenia, które będą próbowały uzyskać dostęp do danych i zasobów organizacji. Organizacje powinny założyć, że urządzenia klienckie telepracy, które są używane w różnych lokalizacjach zewnętrznych i są szczególnie narażone na utratę lub kradzież, zostaną przejęte przez atakujących, które będą próbowały pozyskać z nich wrażliwe dane lub wykorzystać je do uzyskania dostępu do sieci organizacji. Opcje ograniczania zagrożeń związanych z utratą lub kradzieżą obejmują szyfrowanie pamięci masowej urządzenia, szyfrowanie wszystkich danych wrażliwych przechowywanych lub przetwarzanych na urządzeniach klienckich. W celu ograniczenia zagrożeń związanych z ponownym wykorzystaniem urządzeń, podstawową opcją jest stosowanie silnego uwierzytelniania - najlepiej wieloskładnikowego - w celu uzyskania dostępu do zasobów organizacji.

Organizacje powinny również założyć, że komunikacja w sieciach zewnętrznych, które są poza kontrolą organizacji, jest podatna na podsłuch, przechwycenie i modyfikację. Ten rodzaj zagrożenia można ograniczyć, ale nie wyeliminować, stosując technologie szyfrowania w celu ochrony poufności i integralności komunikacji, a także uwierzytelniając każdy z punktów końcowych w celu weryfikacji jego tożsamości.

Innym ważnym założeniem jest to, że urządzenia klienckie mogą zostać zainfekowane złośliwym oprogramowaniem; możliwe sposoby kontroli tego zjawiska obejmują użycie

technologii antymalware, użycie rozwiązań kontroli dostępu do sieci, które weryfikują stan bezpieczeństwa klienta przed przyznaniem dostępu, oraz użycie oddzielnej sieci w obiektach organizacji dla urządzeń klienckich telepracy przyniesionych do użytku wewnętrznego (zobacz ostatnią rekomendację w Streszczeniu, w celu uzyskania dodatkowych informacji).

**Opracuj politykę bezpieczeństwa telepracy, która określa wymagania dotyczące telepracy, zdalnego dostępu i BYOD.**

Polityka bezpieczeństwa telepracy powinna definiować, jakie formy zdalnego dostępu są dozwolone w organizacji, jakie typy urządzeń wykorzystywanych do telepracy mogą korzystać z każdej formy zdalnego dostępu, oraz jaki rodzaj dostępu jest przyznawany każdemu typowi „telepracownika". Powinna również obejmować zasady administrowania serwerami zdalnego dostępu oraz sposób aktualizacji polityk na tych serwerach.

W ramach tworzenia polityki bezpieczeństwa telepracy, organizacja powinna podjąć decyzję na podstawie ryzyka, jakie poziomy zdalnego dostępu powinny być dozwolone dla poszczególnych typów urządzeń klienckich. Na przykład, organizacja może zdecydować się na wielopoziomowy dostęp zdalny, zezwalając komputerom osobistym (PC) będącym własnością organizacji na dostęp do wielu zasobów, komputerom BYOD i urządzeniom klienckim kontrolowanym przez inne firmy na dostęp do ograniczonego zestawu zasobów, a smartfonom i tabletom BYOD na dostęp tylko do jednego lub dwóch zasobów o niższym ryzyku, takich jak webmail. Posiadanie wielopoziomowych poziomów zdalnego dostępu pozwala organizacji ograniczyć ponoszone ryzyko poprzez umożliwienie najbardziej kontrolowanym urządzeniom największego dostępu, a najmniej kontrolowanym urządzeniom minimalnego dostępu.

Istnieje wiele czynników, które organizacja powinna brać pod uwagę ustalając politykę w zakresie poziomu zdalnego dostępu; przykładowo: wrażliwość pracy zdalnej, poziom zaufania do zabezpieczeń urządzeń klienckich, koszty związane z urządzeniami wykorzystywanymi do telepracy, lokalizacje, z których wykonywana jest praca zdalna, zgodność z wymogami i innymi politykami. W sytuacjach, w których telepraca jest

szczególnie ryzykowna, organizacja może określić dodatkowe wymagania bezpieczeństwa. Na przykład, telepraca o wysokim poziomie ryzyka może być dozwolona tylko z zabezpieczonych urządzeń klienckich wydanych przez organizację, które wykorzystują uwierzytelnianie wieloskładnikowe i szyfrowanie pamięci. Organizacje mogą również podjąć decyzję o ograniczeniu ryzyka poprzez zakaz telepracy i zdalnego dostępu do określonych typów informacji, takich jak wrażliwe informacje umożliwiające identyfikację osób (*ang. Personally Identifiable Information - PII*).[1]

**Upewnij się, że serwery zdalnego dostępu są skutecznie zabezpieczone i skonfigurowane w celu egzekwowania zasad bezpieczeństwa telepracy.**

Bezpieczeństwo serwerów zdalnego dostępu jest szczególnie ważne, ponieważ zapewniają one zewnętrznym hostom dostęp do zasobów wewnętrznych, a także bezpieczne, odizolowane środowisko telepracy dla urządzeń klienckich wydanych przez organizację, kontrolowanych przez strony trzecie oraz BYOD. Oprócz umożliwienia nieautoryzowanego dostępu do zasobów przedsiębiorstwa i urządzeń klienckich telepracy, skompromitowany serwer może zostać wykorzystany do podsłuchiwania komunikacji i manipulowania nią, a także stanowić punkt startowy do ataku na inne hosty w organizacji. Szczególnie ważne dla organizacji jest zapewnienie, aby serwery zdalnego dostępu posiadały aktualne poprawki i aby mogły być zarządzane tylko z zaufanych hostów przez upoważnionych administratorów. W większości przypadków, serwer powinien być umieszczony na granicy sieci tak, aby pracował jako pojedynczy punkt wejścia do sieci i egzekwował politykę bezpieczeństwa telepracy zanim jakikolwiek ruch zdalnego dostępu lub inny ruch z urządzeń klienckich telepracy (takich jak urządzenia BYOD korzystające z bezprzewodowej sieci BYOD) zostanie wpuszczony do sieci wewnętrznej organizacji.

[1] Więcej informacji na temat ochrony PII można znaleźć w publikacji specjalnej NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (http://dx.doi.org/10.6028/NIST.SP.800-122).

**Zabezpiecz urządzenia klienckie telepracy kontrolowane przez organizację przed typowymi zagrożeniami i regularnie dbaj o ich bezpieczeństwo.**

Istnieje wiele zagrożeń odnoszących się do urządzeń klienckich telepracy, w tym złośliwe oprogramowanie oraz utrata lub kradzież urządzeń. Ogólnie rzecz biorąc, urządzenia klienckie do telepracy powinny posiadać wszystkie lokalne mechanizmy bezpieczeństwa, które są stosowane w organizacji do bezpiecznego konfigurowania urządzeń klienckich niebędących urządzeniami do telepracy. Przykładem może być stosowanie aktualizacji systemu operacyjnego i aplikacji, wyłączanie niepotrzebnych usług, stosowanie oprogramowania antymalware i osobistej zapory sieciowej. Ponieważ jednak urządzenia do telepracy są zwykle bardziej narażone na ryzyko w środowiskach zewnętrznych niż w środowiskach korporacyjnych, zaleca się stosowanie dodatkowych środków bezpieczeństwa, takich jak szyfrowanie wrażliwych danych przechowywanych na urządzeniach. Istniejące środki bezpieczeństwa mogą wymagać dostosowania. Na przykład, jeżeli osobista zapora sieciowa na urządzeniu klienckim telepracy ma jedną politykę dla wszystkich środowisk, to w niektórych sytuacjach może być zbyt restrykcyjna, a w innych niewystarczająco rygorystyczna. Jeśli to możliwe, organizacje powinny używać osobistych zapór sieciowych zdolnych do obsługi wielu polityk urządzeń klienckich do telepracy i odpowiednio skonfigurować zapory sieciowe dla środowiska korporacyjnego i zewnętrznego. Organizacje powinny zadbać o zabezpieczenie wszystkich typów urządzeń klienckich do telepracy, w tym komputerów, smartfonów i tabletów. W przypadku komputerów PC obejmuje to zabezpieczenia fizyczne. W przypadku urządzeń innych niż komputery PC, możliwości zabezpieczeń i odpowiednie działania różnią się w zależności od typu urządzenia i konkretnego produktu, więc organizacje powinny zapewnić wytyczne dla administratorów urządzeń i użytkowników, którzy są odpowiedzialni za zabezpieczenie urządzeń przenośnych do telepracy, w jaki sposób powinni je zabezpieczyć.

**Jeśli korzystanie z urządzeń zewnętrznych (np. BYOD, kontrolowanych przez strony trzecie) jest dozwolone w obrębie obiektów organizacji, należy zdecydowanie rozważyć utworzenie oddzielnej, zewnętrznej, dedykowanej sieci do tego użytku.**

Zezwolenie na bezpośrednie podłączenie urządzeń klienckich należących do osób prywatnych lub kontrolowanych przez osoby trzecie do sieci korporacyjnych zwiększa ryzyko, jeśli urządzenia te są umieszczone w sieciach wewnętrznych organizacji, ponieważ często nie są one zabezpieczone w takim samym stopniu, jak urządzenia własne organizacji. Ryzyko to można jednak w znacznym stopniu ograniczyć poprzez utworzenie w organizacji oddzielnej sieci przewodowej lub bezprzewodowej przeznaczonej dla tych urządzeń. Sieć ta powinna być zewnętrzna (np. poza strefą ograniczonego zaufania [*ang. demilitarized zone - DMZ*]) i nie powinna zapewniać dostępu do zasobów przedsiębiorstwa w stopniu większym niż ten, który mają użytkownicy poprzez dostęp zdalny. Sieć ta powinna być zabezpieczona i monitorowana w sposób spójny z tym, w jaki zabezpieczone i monitorowane są segmenty zdalnego dostępu.

# 1. WSTĘP

## 1.1. Cel i zakres

Celem tego dokumentu jest pomoc organizacjom w ograniczeniu ryzyka związanego z technologiami korporacyjnymi wykorzystywanymi do telepracy, takimi jak serwery zdalnego dostępu, urządzenia klienckie do telepracy (w tym urządzenia typu "przynieś własne urządzenie" [BYOD] oraz urządzenia klienckie kontrahentów, partnerów biznesowych i dostawców, znane również jako urządzenia kontrolowane przez strony trzecie) oraz komunikacja zdalnego dostępu. Dokument ten podkreśla znaczenie zabezpieczania wrażliwych informacji przechowywanych na urządzeniach do telepracy i przesyłanych poprzez zdalny dostęp w sieciach zewnętrznych. Zawiera zalecenia dotyczące tworzenia polityk związanych z telepracą oraz wyboru, wdrożenia i utrzymania niezbędnych zabezpieczeń serwerów i klientów zdalnego dostępu.

## 1.2. Odbiorcy

Dokument ten jest przeznaczony przede wszystkim dla inżynierów i administratorów bezpieczeństwa, systemów i sieci, a także dla menadżerów programów bezpieczeństwa komputerowego, którzy są odpowiedzialni za techniczne aspekty przygotowania, obsługi i zabezpieczenia rozwiązań zdalnego dostępu oraz urządzeń klienckich. Fragmenty dokumentu są również przeznaczone dla kadry zarządzającej wyższego szczebla, np. osób odpowiedzialnych za tworzenie polityki telepracy. Materiał zawarty w tym dokumencie jest zorientowany technicznie i zakłada się, że czytelnicy mają przynajmniej podstawowe pojęcie o zdalnym dostępie, sieci, bezpieczeństwie sieciowym i bezpieczeństwie systemu.

## 1.3. Struktura dokumentu

Pozostała część niniejszego dokumentu została podzielona na następujące sekcje:

Rozdział 2 zawiera przegląd zagadnień związanych z bezpieczeństwem telepracy i zdalnego dostępu w organizacji. Omówiono w nim ogólne podatności i zagrożenia dla rozwiązań

telepracy i zdalnego dostępu. Opisano również podstawowe architektury powszechnie stosowanych metod zdalnego dostępu oraz charakterystykę bezpieczeństwa każdej z nich. Omówiono problemy związane z wykorzystaniem sieci firmowych przez BYOD.

W rozdziale 3 przedstawiono zalecenia dotyczące zabezpieczania rozwiązań zdalnego dostępu, w tym bezpieczeństwa serwerów, rozmieszczenia serwerów i bezpieczeństwa oprogramowania klienckiego. Omówiono również uwierzytelnianie, autoryzację i kontrolę dostępu dla rozwiązań zdalnego dostępu.

W rozdziale 4 przedstawiono zalecenia dotyczące zabezpieczenia urządzeń klienckich do telepracy oraz ochrony znajdujących się na nich danych.

Rozdział 5 omawia bezpieczeństwo w całym cyklu życia telepracy i zdalnego dostępu. Przykłady tematów poruszonych w tej sekcji obejmują tworzenie polityki bezpieczeństwa telepracy, uwarunkowania projektowe i wdrożeniowe oraz procesy operacyjne, które są szczególnie pomocne w zapewnieniu bezpieczeństwa.

Dokument zawiera również załączniki z materiałami uzupełniającymi:

- Załączniki A i B zawierają odwzorowania odpowiednio zabezpieczeń zawartych w publikacji NSC 800-53 oraz podkategorii Ram Cyberbezpieczeństwa.
- Załączniki C i D zawierają odpowiednio słownik i wykaz akronimów.
- Załącznik E zawiera listę referencji, które mogą być przydatne w uzyskaniu lepszego zrozumienia zagadnień związanych z bezpieczeństwem telepracy i zdalnego dostępu.

# 2. PRZEGLĄD BEZPIECZEŃSTWA TELEPRACY I DOSTĘPU ZDALNEGO W ORGANIZACJI

Wiele osób wykonuje *telepracę* (znaną również jako *praca zdalna*), czyli możliwość wykonywania pracy przez pracowników organizacji, kontrahentów, partnerów biznesowych, sprzedawców i innych użytkowników z miejsc innych niż siedziba organizacji. Telepracownicy korzystają z różnych urządzeń klienckich, takich jak komputery stacjonarne i przenośne, smartfony i tablety, aby czytać i wysyłać wiadomości e-mail, odwiedzać strony internetowe, przeglądać i edytować dokumenty oraz wykonywać wiele innych zadań. Urządzenia te mogą być kontrolowane przez organizację, osoby trzecie (kontrahentów organizacji, partnerów biznesowych, dostawców) lub przez samych użytkowników (np. BYOD). Większość telepracowników korzysta ze *zdalnego dostępu,* czyli możliwości dostępu użytkowników organizacji do jej niepublicznych zasobów obliczeniowych z lokalizacji zewnętrznych, innych niż siedziba organizacji.

Ta część publikacji zawiera przegląd problemów bezpieczeństwa związanych z technologiami telepracy i zdalnego dostępu w przedsiębiorstwach. Wyjaśnia główne podatności i zagrożenia związane z bezpieczeństwem telepracy i zdalnego dostępu oraz zaleca strategie łagodzenia tych zagrożeń. Omówiono również najczęściej stosowane typy metod zdalnego dostępu, przeanalizowano ich główne podatności oraz zalecane środki bezpieczeństwa w celu ograniczenia zagrożeń. Krótko przedstawiono specjalne rozważania związane z wykorzystaniem BYOD i urządzeń klienckich kontrolowanych przez strony trzecie we własnych sieciach organizacji.

## 2.1. Podatności, zagrożenia i zabezpieczenia

Rozwiązania telepracy i zdalnego dostępu zazwyczaj muszą wspierać kilka celów związanych z bezpieczeństwem. Cele te mogą być osiągnięte poprzez kombinację zabezpieczeń wbudowanych w rozwiązania zdalnego dostępu oraz dodatkowych zabezpieczeń stosowanych na urządzeniach klienckich do telepracy i innych komponentach rozwiązania

zdalnego dostępu. Najczęściej spotykane cele bezpieczeństwa stawiane przed technologiami telepracy i zdalnego dostępu obejmują:

- Poufność - zapewnienie, że komunikacja zdalnego dostępu i przechowywane dane użytkownika nie mogą być odczytane przez osoby nieupoważnione;
- Integralność - wykrywanie wszelkich celowych lub niezamierzonych zmian w komunikacji zdalnej, które występują podczas przesyłania informacji; oraz
- Dostępność - zapewnienie użytkownikom zdalnego dostępu do zasobów zawsze, gdy jest to potrzebne.

W celu osiągnięcia tych celów, wszystkie komponenty rozwiązań telepracy i zdalnego dostępu, w tym urządzenia klienckie, serwery zdalnego dostępu oraz wewnętrzne serwery dostępne poprzez zdalny dostęp, powinny być zabezpieczone przed różnego rodzaju zagrożeniami. Ogólne zalecenia dotyczące bezpieczeństwa dla wszystkich urządzeń IT są zawarte w publikacji NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji*.[2] Szczegółowe zalecenia dotyczące zabezpieczenia technologii telepracy i zdalnego dostępu zostały przedstawione w niniejszej publikacji i mają na celu uzupełnienie środków bezpieczeństwa określonych w NSC 800-53.

Technologie telepracy i zdalnego dostępu często wymagają dodatkowej ochrony, ponieważ z istoty narażone są na zagrożenia zewnętrzne w większym stopniu, niż technologie, do których dostęp odbywa się tylko z wewnątrz organizacji. Przed zaprojektowaniem i wdrożeniem rozwiązań telepracy i zdalnego dostępu, organizacje powinny opracować modele zagrożeń systemowych[3] odnoszące się do serwerów zdalnego dostępu oraz zasobów, z którymi uzyskuje się połączenie poprzez dostęp zdalny. Modelowanie zagrożeń

[2] Zalecenia te są powiązane z trzema kategoriami bezpieczeństwa - niską, umiarkowaną i wysoką - w oparciu o potencjalny wpływ zagrożeń na atrybuty bezpieczeństwa danego systemu, zgodnie z definicją zawartą w dokumencie NSC 199, Standardy kategoryzacji bezpieczeństwa.

[3] Dodatkowe informacje na temat modelowania zagrożeń, a w szczególności modelowania zagrożeń dla systemów zorientowanych na dane, można znaleźć w publikacji specjalnej NIST SP 800-154 (Draft), *Guide to Data-Centric System Threat Modeling* (http://csrc.nist.gov/publications/drafts/800154/sp800_154_draft.pdf).

obejmuje identyfikację interesujących zasobów oraz możliwych zagrożeń, podatności i środków bezpieczeństwa związanych z tymi zasobami, następnie kwantyfikację prawdopodobieństwa udanych ataków i ich skutków, a na końcu analizę tych informacji w celu określenia, gdzie należy poprawić lub rozszerzyć środki bezpieczeństwa. Modelowanie zagrożeń pomaga organizacjom zidentyfikować wymagania dotyczące bezpieczeństwa i zaprojektować rozwiązanie zdalnego dostępu w taki sposób, aby zawierało zabezpieczenia niezbędne do spełnienia wymagań bezpieczeństwa. Główne problemy związane z bezpieczeństwem tych technologii, które zostałyby uwzględnione w większości modeli zagrożeń telepracy są następujące:

- **Brak fizycznych zabezpieczeń.** Urządzenia klienckie do telepracy są używane w różnych miejscach poza kontrolą organizacji, takich jak domy użytkowników, kawiarnie, hotele, konferencje. Mobilna natura tych urządzeń sprawia, że są one bardziej narażone na zgubienie lub kradzież, co powoduje zwiększone ryzyko utraty danych znajdujących się na tych urządzeniach. Planując politykę bezpieczeństwa i zabezpieczenia telepracy, organizacje powinny założyć, że urządzenia klienckie zostaną przejęte przez wrogie podmioty, które będą próbowały pozyskać z nich poufne dane lub wykorzystać je do uzyskania dostępu do sieci przedsiębiorstwa. Podstawowe strategie ograniczania ryzyka utraty lub kradzieży urządzenia to szyfrowanie pamięci masowej urządzenia klienckiego lub samych danych wrażliwych, tak aby nie mogły zostać odzyskane z urządzenia przez osoby nieupoważnione, lub nieprzechowywanie danych wrażliwych na urządzeniach klienckich. Nawet jeśli urządzenie klienckie jest zawsze w posiadaniu właściciela, istnieją inne fizyczne zagrożenia bezpieczeństwa, takie jak osoba atakująca zaglądająca użytkownikowi przez ramię w kawiarni i przeglądająca wrażliwe dane na ekranie urządzenia klienckiego. Organizacje mogą ograniczyć zagrożenia związane z ponownym użyciem urządzenia, takie jak uzyskanie przez atakującego zdalnej kontroli nad urządzeniem lub podszywanie się pod użytkownika, poprzez stosowanie silnego uwierzytelniania,

najlepiej uwierzytelnianie wieloskładnikowe, w celu uzyskania dostępu do przedsiębiorstwa.

- **Niezabezpieczone sieci.** Ponieważ prawie cały zdalny dostęp odbywa się przez Internet, organizacje zazwyczaj nie mają kontroli nad bezpieczeństwem sieci zewnętrznych używanych przez telepracowników. Systemy telekomunikacyjne używane do zdalnego dostępu obejmują sieci szerokopasmowe, takie jak kablowe, oraz mechanizmy bezprzewodowe, takie jak IEEE 802.11 i sieci komórkowe.[4] Wykorzystane systemy telekomunikacyjne są podatne na podsłuch, co naraża wrażliwe informacje przesyłane podczas zdalnego dostępu na ryzyko kompromitacji. Ataki typu Man-in-the-middle (MITM) mogą być również przeprowadzane w celu przechwycenia i modyfikacji komunikacji.
  Organizacje powinny planować swoje zabezpieczenia zdalnego dostępu zakładając, że sieci pomiędzy urządzeniem klienckim, a organizacją mogą nie być zaufane. Ryzyko wynikające z korzystania z niezabezpieczonych sieci może być zmniejszone, ale niewyeliminowane, poprzez zastosowanie technologii szyfrowania w celu ochrony poufności i integralności komunikacji, jak również poprzez zastosowanie mechanizmów wzajemnego uwierzytelniania w celu weryfikacji tożsamości obu punktów końcowych.
- **Zainfekowane urządzenia w sieciach wewnętrznych.** Urządzenia klienckie do telepracy, w szczególności laptopy BYOD i kontrolowane przez osoby trzecie, są często używane w sieciach zewnętrznych, a następnie wnoszone do organizacji i podłączane bezpośrednio do jej sieci wewnętrznych. Napastnik mający fizyczny dostęp do urządzenia klienckiego może zainstalować na nim złośliwe oprogramowanie w celu gromadzenia danych z tego urządzenia oraz z sieci

[4] Ze względu na założenie braku bezpieczeństwa połączenia sieciowego, niniejsza publikacja nie odnosi się do linii dzierżawionych, modemów dialup i DSL oraz innych mechanizmów komunikacyjnych, które mogą być zabezpieczone w warstwie łącza danych. Jeżeli organizacja korzysta z mechanizmu łącza danych, który dodaje zabezpieczenia, typ zabezpieczeń opisany w niniejszym dokumencie byłby na najwyższym poziomie zabezpieczeń łącza danych, ale nie wchodziłby z nimi w interakcję.

i systemów, z którymi się ono łączy. Jeśli urządzenie klienckie zostanie zainfekowane złośliwym oprogramowaniem, może ono rozprzestrzenić się w całej organizacji, gdy tylko urządzenie klienckie zostanie podłączone do sieci wewnętrznej. Organizacje powinny założyć, że urządzenia klienckie mogą zostać zainfekowane i odpowiednio zaplanować środki bezpieczeństwa.

Oprócz wprowadzenia obowiązku stosowania odpowiednich technologii antymalware, takich jak oprogramowanie antywirusowe na komputerach, organizacje powinny rozważyć zastosowanie rozwiązań kontroli dostępu do sieci (*ang. network access control - NAC*), które weryfikują stan bezpieczeństwa urządzenia klienckiego przed zezwoleniem mu na korzystanie z sieci wewnętrznej. Organizacje powinny również rozważyć korzystanie z oddzielnej sieci dla wszystkich zewnętrznych urządzeń klienckich, w tym urządzeń BYOD i urządzeń kontrolowanych przez inne firmy, zamiast zezwalać im na bezpośrednie połączenie z siecią wewnętrzną. Rozdział 4 zawiera dodatkowe zalecenia i sugestie dotyczące poprawy bezpieczeństwa urządzeń klienckich.

- **Zewnętrzny dostęp do zasobów wewnętrznych.** Zdalny dostęp, w tym dostęp z urządzeń BYOD i kontrolowanych przez strony trzecie urządzeń klienckich podłączonych do bezprzewodowych sieci BYOD organizacji, zapewnia hostom zewnętrznym dostęp do zasobów wewnętrznych, takich jak serwery. Jeśli te wewnętrzne zasoby nie były wcześniej dostępne z sieci zewnętrznych, udostępnienie ich poprzez zdalny dostęp narazi je na nowe zagrożenia, w szczególności ze strony niezaufanych urządzeń i sieci klienckich, oraz znacząco zwiększy prawdopodobieństwo ich naruszenia. Każda forma zdalnego dostępu, która może być wykorzystana do uzyskania dostępu do zasobu wewnętrznego, zwiększa ryzyko kompromitacji tego zasobu.

  Organizacje powinny starannie rozważyć równowagę pomiędzy korzyściami płynącymi z zapewnienia zdalnego dostępu do dodatkowych zasobów, a potencjalnym wpływem narażenia tych zasobów na niebezpieczeństwo. Organizacje

powinny zapewnić, że wszelkie wewnętrzne zasoby, które zdecydują się udostępnić poprzez zdalny dostęp, są odpowiednio zabezpieczone przed zewnętrznymi zagrożeniami[5]oraz, że dostęp do zasobów jest ograniczony do niezbędnego minimum poprzez zapory sieciowe i inne mechanizmy kontroli dostępu.

Informacje na temat problemów z bezpieczeństwem specyficznym dla BYOD i urządzeń klienckich kontrolowanych przez osoby trzecie znajdują się w sekcji 2.3.

W sekcji 2.2 opisano technologie zdalnego dostępu i omówiono względy bezpieczeństwa odnoszące każdej z nich, koncentrując się na elementach opisanych powyżej.

## 2.2. Metody zdalnego dostępu

Organizacje mają wiele możliwości zapewnienia zdalnego dostępu do swoich zasobów obliczeniowych. Jak wspomniano wcześniej, metody zdalnego dostępu mogą być również wykorzystywane do umożliwienia dostępu do zasobów wewnętrznych dla urządzeń BYOD oraz urządzeń klienckich kontrolowanych przez inne firmy, podłączonych do bezprzewodowych sieci BYOD organizacji. Na potrzeby niniejszej publikacji, metody zdalnego dostępu najczęściej wykorzystywane przez telepracowników zostały podzielone na cztery kategorie w oparciu o ich wysokopoziomowe architektury: tunelowanie, portale, zdalny dostęp do pulpitu oraz bezpośredni dostęp do aplikacji. Metody zdalnego dostępu we wszystkich czterech kategoriach mają pewne cechy wspólne:

- Wszystkie zależą od fizycznego bezpieczeństwa urządzeń klienckich.
- Mogą wykorzystywać wiele typów mechanizmów uwierzytelniania serwera i użytkownika. Ta elastyczność pozwala niektórym metodom zdalnego dostępu współpracować z istniejącymi w organizacji mechanizmami uwierzytelniania, takimi jak hasła lub certyfikaty. Niektóre metody zdalnego dostępu posiadają standardowe

[5] Źródła informacji na temat podnoszenia odporności obejmują National Checklist Repository (http://checklists.nist.gov/) oraz NIST SP 800-123, *Guide to General Server Security* (http://dx.doi.org/10.6028/NIST.SP.800-123).

mechanizmy uwierzytelniania, podczas gdy inne wykorzystują mechanizmy specyficzne dla danej implementacji. Mogą one wykorzystywać kryptografię do ochrony przed podglądem przez inne osoby danych przepływających pomiędzy urządzeniem klienckim, a organizacją. Ochrona kryptograficzna jest nieodłącznym elementem sieci VPN i tunelowania kryptograficznego i stanowi opcję w większości systemów zdalnego dostępu do pulpitu i bezpośredniego dostępu do aplikacji.

- Umożliwiają telepracownikom przechowywanie danych na swoich urządzeniach klienckich. Na przykład, większość systemów tunelowych, portalowych i zdalnego dostępu do pulpitu oferuje funkcje kopiowania plików z komputerów wewnątrz organizacji na urządzenie klienckie telepracownika. Dzięki temu telepracownik może pracować z danymi lokalnie, np. w zainstalowanym lokalnie edytorze tekstu. Niektóre aplikacje, do których można uzyskać bezpośredni dostęp, umożliwiają również przesyłanie plików do telepracownika. Dane mogą być również przechowywane na urządzeniach klienckich w sposób niezamierzony, np. poprzez pliki stron systemu operacyjnego lub cache przeglądarki internetowej. Ważne jest, aby wszystkie dane przesyłane do telepracownika poprzez zdalny dostęp były objęte obowiązującymi w organizacji zasadami dystrybucji i przechowywania danych.

Rozdziały 3 i 4 zawierają więcej szczegółów na temat uwierzytelniania zdalnego dostępu, szyfrowania komunikacji i bezpieczeństwa danych klienta.

Dodatkowe informacje na temat czterech kategorii metod zdalnego dostępu znajdują się poniżej. Podczas planowania rozwiązania zdalnego dostępu, organizacje powinny dokładnie rozważyć implikacje metod zdalnego dostępu w każdej kategorii pod względem bezpieczeństwa, a także to, jak każda z metod może poprawnie spełniać wymagania operacyjne.

Na rysunkach w kolejnych sekcjach przedstawiono niektóre właściwości operacyjne i bezpieczeństwa omawianych czterech kategorii metod zdalnego dostępu.

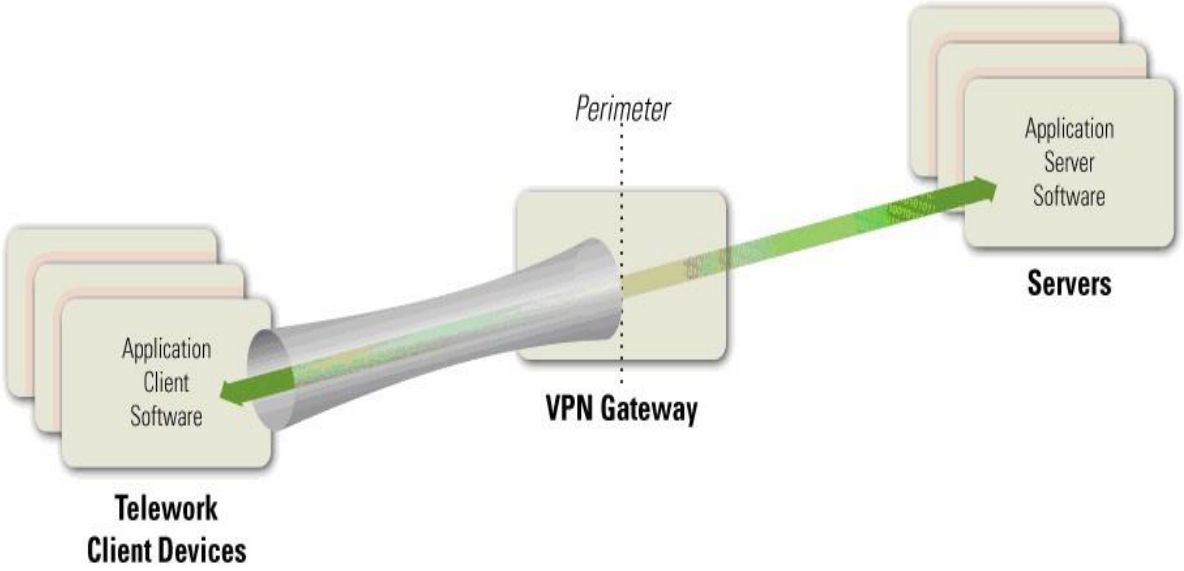
- Rozwinięty tunel jest kryptograficznie chronionym kanałem komunikacyjnym, który rozpoczyna się od urządzenia telepracownika.
- Strzałka i etykiety oprogramowania aplikacji wskazują przepływ komunikacji pomiędzy klientem aplikacji, a oprogramowaniem serwera.
- Pionowa linia przerywana pokazuje granicę obwodu (*ang. perimeter*) sieci organizacji. Wszystko na lewo od linii przerywanej reprezentuje Internet i/lub zewnętrzne bezprzewodowe sieci BYOD organizacji, natomiast na prawo od linii przerywanej znajduje się sieć wewnętrzna.

### 2.2.1. Tunelowanie

Wiele metod zdalnego dostępu oferuje bezpieczny tunel komunikacyjny, przez który można przesyłać informacje między sieciami, w tym sieciami publicznymi, takimi jak Internet. Tunele są zazwyczaj tworzone za pomocą technologii *wirtualnej sieci prywatnej* (*ang. virtual private network - VPN*). Po ustanowieniu tunelu VPN pomiędzy urządzeniem klienckim telepracownika, a bramą VPN organizacji, telepracownik może uzyskać za pośrednictwem tunelu dostęp do wielu zasobów obliczeniowych organizacji. W celu korzystania z VPN, użytkownicy muszą posiadać odpowiednie oprogramowanie VPN na swoich urządzeniach klienckich lub znajdować się w sieci, w której funkcjonuje system bramy VPN. Na rysunku 2-1[6] na każdym urządzeniu klienckim zainstalowany jest klient VPN (*ang. Application Client Software*), a na pojedynczej bramie VPN działa oprogramowanie serwera VPN (*ang. Application Server Software)*. „Rura" reprezentuje bezpieczne połączenie zdalnego dostępu (tunel) między urządzeniem klienckim (*ang. Telework Client Device*), a bramą VPN (*ang. VPN Gateway*). Poprzez ten tunel, oprogramowanie klienta aplikacji (np. klient poczty elektronicznej, edytor tekstu, przeglądarka internetowa, klient bazy danych) zainstalowane na urządzeniu klienckim komunikuje się z oprogramowaniem serwera aplikacji rezydującym

[6] Nazewnictwo polskie pojęć angielskich przedstawionych na rysunkach niniejszej publikacji, zostało odzwierciedlone w tekście powyżej / poniżej danego rysunku.

na serwerach w organizacji.[7] Brama VPN może zajmować się uwierzytelnianiem użytkowników, kontrolą dostępu (na poziomie hosta, usługi i aplikacji) oraz innymi funkcjami bezpieczeństwa skierowanych do telepracowników.




*Rysunek 2-1 Architektura tunelowania*

Tunele wykorzystują kryptografię do ochrony poufności i integralności informacji przesyłanych między urządzeniem klienckim, a bramą VPN. Tunele mogą również uwierzytelniać użytkowników, zapewniać kontrolę dostępu (np. ograniczając, które protokoły mogą być przesyłane lub do których hostów wewnętrznych można się dostać za pośrednictwem zdalnego dostępu) oraz wykonywać inne funkcje bezpieczeństwa. Chociaż metody zdalnego dostępu oparte na tunelowaniu chronią komunikację między urządzeniem klienckim, a bramą VPN, nie zapewniają one żadnej ochrony komunikacji między bramą VPN, a zasobami wewnętrznymi. Ponadto w rozwiązaniach tunelowania oprogramowanie klienta aplikacji i dane w stanie spoczynku rezydują na urządzeniu klienckim, więc nie są chronione przez rozwiązanie tunelowania i powinny być chronione w inny sposób.

[7] Ta architektura, w której brama VPN i serwery aplikacji znajdują się na oddzielnych hostach, jest najczęściej stosowanym rozwiązaniem tunelowania dla zdalnego dostępu. Jednak brama VPN i serwery aplikacji mogą także znajdować się na jednym hoście.

Najczęściej używane przez telepracowników rodzaje sieci VPN to tunele[8] Internet Protocol Security (IPsec) i Secure Sockets Layer (SSL)[9]. Tunelowanie można również osiągnąć za pomocą Secure Shell (SSH), chociaż jest to rzadziej stosowane i często uważa się, że jest trudniejsze do skonfigurowania i utrzymania niż tunele IPsec lub SSL VPN. Wszystkie trzy formy tunelowania wymienione w tym rozdziale mogą chronić wiele protokołów jednocześnie. Więcej informacji na temat protokołów tunelowania można znaleźć w publikacji NIST SP 800-77, Guide to IPsec VPNs[10], NIST SP 800-113, Guide to SSL VPNs[11], oraz NIST Internal Report (IR) 7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH)[12]. Wiele protokołów szyfrowania komunikacji może być rozszerzonych do protokołów tunelowania w ten sam sposób, w jaki TLS jest używany w SSL VPN. Na przykład, niektóre systemy używają protokołu SSH do tworzenia tuneli. Ogólnie rzecz biorąc, standardowe protokoły tunelowania mogą być skonfigurowane tak, aby miały tę samą moc kryptograficzną i używały tego samego (lub funkcjonalnie podobnego) mechanizmu uwierzytelniania dwóch stron. Różne systemy tunelowania mogą tunelować różne protokoły; na przykład IPsec ma standardowe rozszerzenia, które pozwalają mu na tunelowanie protokołów warstwy 2, takich jak Point-to-Point Protocol (PPP) i Multiprotocol Label Switching (MPLS). Ogólnie rzecz biorąc, prawie każdy protokół szyfrowania komunikacji może być wykorzystany do tunelowania praktycznie każdej warstwy.

[8] Inna, częściej stosowana forma SSL VPN wykorzystuje architekturę portalową. W punkcie 2.2.2 omówiono portalowe sieci SSL VPN. Tunelowa sieć SSL VPN zazwyczaj wykorzystuje wtyczkę (*ang. plug-in*) instalowaną w przeglądarce internetowej, która obsługuje tunelowanie w ramach połączenia TLS.

[9] Chociaż technologia ta jest powszechnie znana jako SSL VPN, zazwyczaj do szyfrowania komunikacji wykorzystuje Transport Layer Security (TLS) zamiast SSL, ponieważ TLS oferuje silniejsze zabezpieczenia niż SSL. Dodatkowe informacje na temat TLS i SSL można znaleźć w dokumencie NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (http://dx.doi.org/10.6028/NIST.SP.800-52r1).

[10] http://dx.doi.org/10.6028/NIST.SP.800-77

[11] http://dx.doi.org/10.6028/NIST.SP.800-113

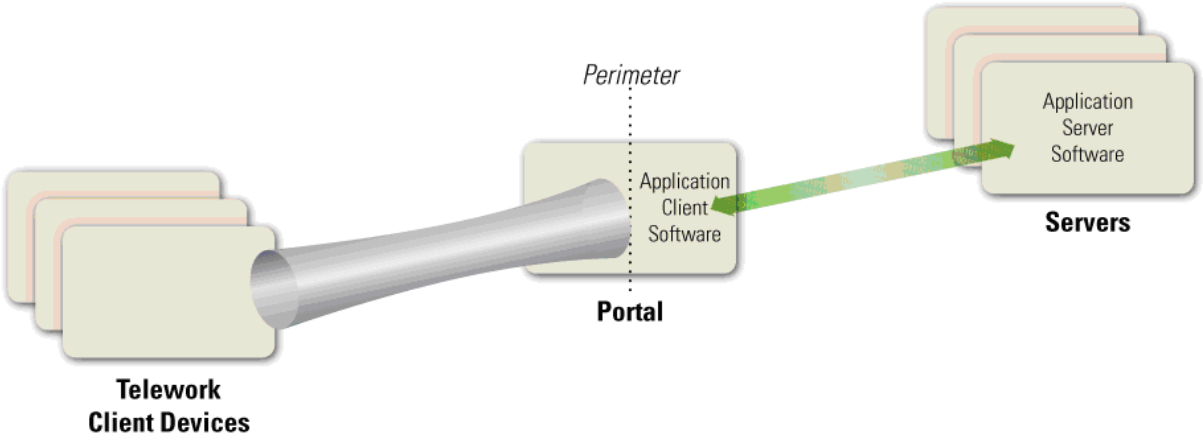
[12] http://dx.doi.org/10.6028/NIST.IR.7966

Brama VPN może kontrolować dostęp do poszczególnych części sieci oraz rodzaje dostępu, które telepracownik uzyskuje po uwierzytelnieniu. Na przykład, VPN może zezwalać użytkownikowi na dostęp tylko do jednej podsieci, lub na uruchamianie tylko określonych aplikacji na określonych serwerach w chronionej sieci. W ten sposób, mimo że tunel kryptograficzny kończy się na bramie VPN, brama może dodać dodatkowy routing do ruchu telepracownika, aby umożliwić dostęp tylko do niektórych części sieci wewnętrznej.

Sieci VPN są zwykle tworzone i zarządzane przez bramy VPN, których właścicielem i zarządcą jest chroniona organizacja. W niektórych przypadkach, organizacje zlecają zarządzanie sieciami VPN zaufanym stronom trzecim. Taka strona trzecia może zarządzać bramą VPN, która jest własnością organizacji. Inne strony trzecie oferują usługi, w których są właścicielami i kontrolują bramę VPN. W tym drugim przypadku, organizacja powinna ocenić bezpieczeństwo proponowanego rozwiązania i upewnić się, że będzie ono wspierać politykę bezpieczeństwa organizacji.

### 2.2.2. Portale aplikacyjne

Inną kategorią rozwiązań zdalnego dostępu są portale. Portal to serwer, który oferuje dostęp do jednej lub wielu aplikacji poprzez pojedynczy, scentralizowany interfejs. W celu uzyskania dostępu do portalu, telepracownik korzysta z klienta portalu na urządzeniu klienckim wykorzystywanym do telepracy. Większość portali jest oparta na przeglądarce internetowej - dla nich klientem portalu jest zwykła przeglądarka internetowa.
Rysunek 2-2 przedstawia podstawową architekturę rozwiązania portalowego. Oprogramowanie klienta aplikacji (*ang. Application Client Software*) jest zainstalowane na serwerze portalowym (*ang. Portal*) i komunikuje się z oprogramowaniem serwera aplikacji (*ang. Application Server Software*) na serwerach w organizacji. Serwer portalowy komunikuje się bezpiecznie z klientem portalowym w zależności od potrzeb; dokładny charakter tej komunikacji zależy od typu używanego rozwiązania portalowego, co zostało omówione poniżej.




*Rysunek 2-2 Architektura portalu*

Pod względem bezpieczeństwa portale mają większość tych samych cech, co tunele: portale chronią informacje pomiędzy urządzeniami klienckimi, a portalem i mogą zapewniać uwierzytelnianie, kontrolę dostępu i inne usługi bezpieczeństwa. Istnieje jednak istotna różnica między tunelami i portalami - lokalizacja oprogramowania klienckiego aplikacji i powiązanych z nim danych. W tunelu, oprogramowanie i dane znajdują się na urządzeniu klienckim, natomiast w portalu - na serwerze portalu. Serwer portalowy przekazuje dane do urządzenia klienckiego w postaci renderowanych[13] obrazów ekranu pulpitu lub stron internetowych, ale dane są zazwyczaj przechowywane na urządzeniu klienckim tymczasowo, znacznie dłużej niż w przypadku rozwiązania tunelowego. Portale mogą być jednak skonfigurowane tak, aby umożliwić klientom pobieranie zawartości z portalu i przechowywanie jej na urządzeniu klienckim lub w innych lokalizacjach poza środowiskiem bezpiecznego zdalnego dostępu. Scentralizowanie oprogramowania klienckiego daje organizacji większą kontrolę nad sposobem zabezpieczenia oprogramowania i danych, w przeciwieństwie do bardziej rozproszonych rozwiązań zdalnego dostępu. Portale ograniczają dostęp telepracownika do poszczególnych klientów aplikacji działających na

[13] Renderowanie (*ang*. *rendering*) – graficzne przedstawienie treści zapisanej cyfrowo w formie właściwej dla danego środowiska (np. wyświetlenie w oknie przeglądarki, strony WWW zapisanej w kodzie HTML). Część programu komputerowego odpowiedzialna za renderowanie nazywana jest mechanizmem renderującym, silnikiem renderującym lub rendererem.

samym portalu. Aplikacje te dodatkowo ograniczają dostęp telepracownika do serwerów wewnątrz sieci.

Istnieje kilka rodzajów rozwiązań portalowych powszechnie używanych do zdalnego dostępu. **Portal oparty na sieci Web** *(ang. web-based portal)* zapewnia użytkownikowi dostęp do wielu aplikacji internetowych z jednej witryny portalu. Popularną formą portalu internetowego jest portal SSL VPN. Innym rodzajem rozwiązania portalowego jest **dostęp do serwera terminali** (*ang. terminal server access)*, który zapewnia każdemu telepracownikowi dostęp do oddzielnego, standardowego pulpitu wirtualnego. Serwer terminali symuluje wygląd i działanie stacjonarnego systemu operacyjnego i zapewnia dostęp do aplikacji. Dostęp do serwera terminali wymaga od telepracownika albo zainstalowania na urządzeniu klienckim specjalnej aplikacji klienckiej serwera terminali, albo korzystania z interfejsu opartego na sieci WWW, często z wykorzystaniem wtyczki do przeglądarki lub innego dodatkowego oprogramowania dostarczonego przez organizację. Inna podobna metoda zdalnego dostępu, zwana **wirtualizacją pulpitów** *(ang. virtual desktop infrastructure - VDI)*, polega na podłączeniu użytkownika do systemu zawierającego wirtualne obrazy standardowych, niesymulowanych systemów operacyjnych i pulpitów. Jeżeli telepracownik kończy sesję zdalnego dostępu, wirtualny obraz jest usuwany, dzięki czemu kolejny użytkownik ma do dyspozycji czysty wirtualny pulpit. VDI jest szczególnie pomocne przy zabezpieczaniu telepracy na urządzeniach BYOD oraz kontrolowanych przez firmy trzecie, które częściej niż urządzenia firmowe nie spełniają wymogów bezpieczeństwa organizacji.

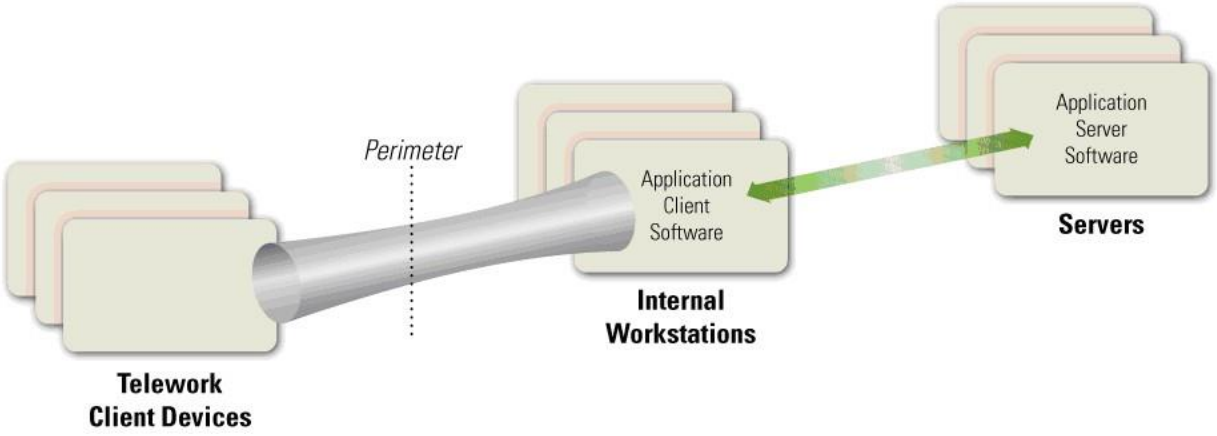
Mechanizm dostarczania interfejsu do telepracownika różni się w zależności od portalu. Na przykład, dostęp do serwera terminali oraz VDI prezentują telepracownikowi standardowy wirtualny pulpit, podczas gdy portale SSL VPN prezentują każdą aplikację poprzez stronę WWW. Charakter tego interfejsu jest ważny, ponieważ odnosi się do tymczasowego lub stałego przechowywania danych. W przypadku wielu portali, interfejs użytkownika jest wirtualny, a po zakończeniu sesji użytkownika ta instancja interfejsu jest zasadniczo niszczona, a czysta wersja jest używana do następnej sesji. Niektóre portale, takie jak portal

SSL VPN, mogą być skonfigurowane tak, aby utworzyć bezpieczną maszynę wirtualną na urządzeniu klienckim poprzez rozwiązanie VDI, ograniczyć wszystkie dane zdalnego dostępu do rezydowania w tej maszynie wirtualnej, a następnie bezpiecznie zniszczyć instancję maszyny wirtualnej i wszystkie dane, które istniały w niej po zakończeniu sesji. Pozwala to zapewnić, że wrażliwe informacje nie będą przypadkowo przechowywane na urządzeniu klienckim telepracy, gdzie mogłyby zostać odzyskane w przyszłości.

Mimo, że technologie dostępu do serwerów terminali oraz VDI są przeznaczone głównie dla komputerów PC do telepracy, pojawia się technologia, która zapewnia podobne możliwości dla urządzeń mobilnych: wirtualna infrastruktura mobilna (*ang. virtual mobile infrastructure - VMI*). Tak jak rozwiązanie VDI dostarcza bezpieczny wirtualny pulpit na komputer telepracownika, tak VMI dostarcza bezpieczne środowisko wirtualnego urządzenia mobilnego na urządzenie mobilne używane w telepracy. Organizacje, które rozważają wykorzystanie urządzeń mobilnych do telepracy, szczególnie BYOD lub urządzeń mobilnych kontrolowanych przez inne firmy, powinny zbadać technologie VMI, aby sprawdzić czy mogą być pomocne w poprawie bezpieczeństwa.

### 2.2.3. Zdalny dostęp do pulpitu

Rozwiązanie *zdalnego dostępu do pulpitu* daje telepracownikowi możliwość zdalnego sterowania określonym komputerem w organizacji, najczęściej własnym komputerem użytkownika w biurze organizacji, z urządzenia klienckiego telepracy. Telepracownik ma kontrolę nad klawiaturą i myszką zdalnego komputera i widzi jego ekran na ekranie lokalnego urządzenia klienckiego. Zdalny dostęp do pulpitu pozwala użytkownikowi na dostęp do wszystkich aplikacji, danych i innych zasobów, które są normalnie dostępne z komputera w biurze. Rysunek 2-3 przedstawia podstawową architekturę zdalnego dostępu do pulpitu. Na każdym urządzeniu klienckim zainstalowany jest program kliencki zdalnego dostępu do pulpitu lub wtyczka do przeglądarki internetowej, która łączy się bezpośrednio z odpowiednią stacją roboczą telepracownika (*ang. Telework Client Device*) w sieci wewnętrznej organizacji.




*Rysunek 2-3 Architektura zdalnego dostępu do pulpitu*

Istnieją dwa główne rodzaje zdalnego dostępu do pulpitu: bezpośredni pomiędzy klientem telepracy, a wewnętrzną stacją roboczą oraz pośredni poprzez zaufany system pośredni. Jednak dostęp bezpośredni często nie jest możliwy, ponieważ uniemożliwia go wiele zapór sieciowych. Na przykład, jeżeli wewnętrzna stacja robocza znajduje się za zaporą sieciową wykonującą translację adresów (*ang. network address translation - NAT*), urządzenie klienckie telepracy nie może nawiązać kontaktu z wewnętrzną stacją roboczą, chyba, że NAT zezwoli na taki kontakt[14] lub wewnętrzna stacja robocza zainicjuje komunikację z zewnętrznym urządzeniem klienckim telepracy (np. okresowo sprawdzając, czy urządzenie klienckie chce się połączyć).

Pośredni zdalny dostęp do pulpitu jest realizowany za pośrednictwem serwera pośredniego. Serwer ten jest czasem częścią zapory sieciowej organizacji, ale częściej jest obsługiwany przez zaufaną komercyjną lub bezpłatną usługę zewnętrzną, znajdującą się poza obrębem sieci organizacji. Zazwyczaj istnieją oddzielne połączenia pomiędzy urządzeniem klienckim, a usługodawcą oraz pomiędzy usługodawcą, a wewnętrzną stacją roboczą, przy czym serwer pośredniczący obsługuje nieszyfrowaną komunikację pomiędzy tymi połączeniami. Bezpieczeństwo serwera pośredniczącego jest bardzo ważną kwestią, ponieważ jest on

[14] Można to osiągnąć za pomocą schematu "pinhole", który wymaga przypisania poszczególnych portów do każdej stacji roboczej.

odpowiedzialny za prawidłowe uwierzytelnianie telepracowników i uniemożliwienie dostępu do niezaszyfrowanego ruchu osobom nieupoważnionym. Ponadto, jeżeli polityka bezpieczeństwa organizacji wymaga określonego rodzaju uwierzytelniania (np. uwierzytelniania dwuskładnikowego), serwer pośredniczący powinien obsługiwać to uwierzytelnianie w obu kierunkach. Przed wdrożeniem rozwiązania pośredniego zdalnego dostępu do pulpitu, organizacja powinna ocenić zabezpieczenia zapewniane przez dostawcę usług, a w szczególności możliwe zagrożenia dotyczące serwera pośredniego i potencjalny wpływ tych zagrożeń. Następnie organizacja może zidentyfikować zabezpieczenia kompensacyjne w celu zmniejszenia zagrożeń, takie jak zastosowanie drugiego poziomu szyfrowania komunikacji w warstwie aplikacji, oraz określić, w jakich okolicznościach system pośredni może być używany, np. do działań o niskim ryzyku. Oprogramowanie zdalnego dostępu do pulpitu chroni poufność i integralność komunikacji zdalnego dostępu, a także uwierzytelnia użytkownika, aby zapewnić, że nikt inny nie połączy się z wewnętrzną stacją roboczą. Ponieważ jednak wiąże się to z szyfrowaniem end-to-end komunikacji przez granicę organizacji, treść komunikacji jest ukryta przed zabezpieczeniami sieciowymi na granicy, takimi jak zapory i systemy wykrywania włamań. Dla wielu organizacji zwiększone ryzyko wynikające z takiego rozwiązania jest większe niż korzyści, dlatego bezpośrednie połączenia z zewnętrznych urządzeń klienckich do wewnętrznych stacji roboczych są zabronione.

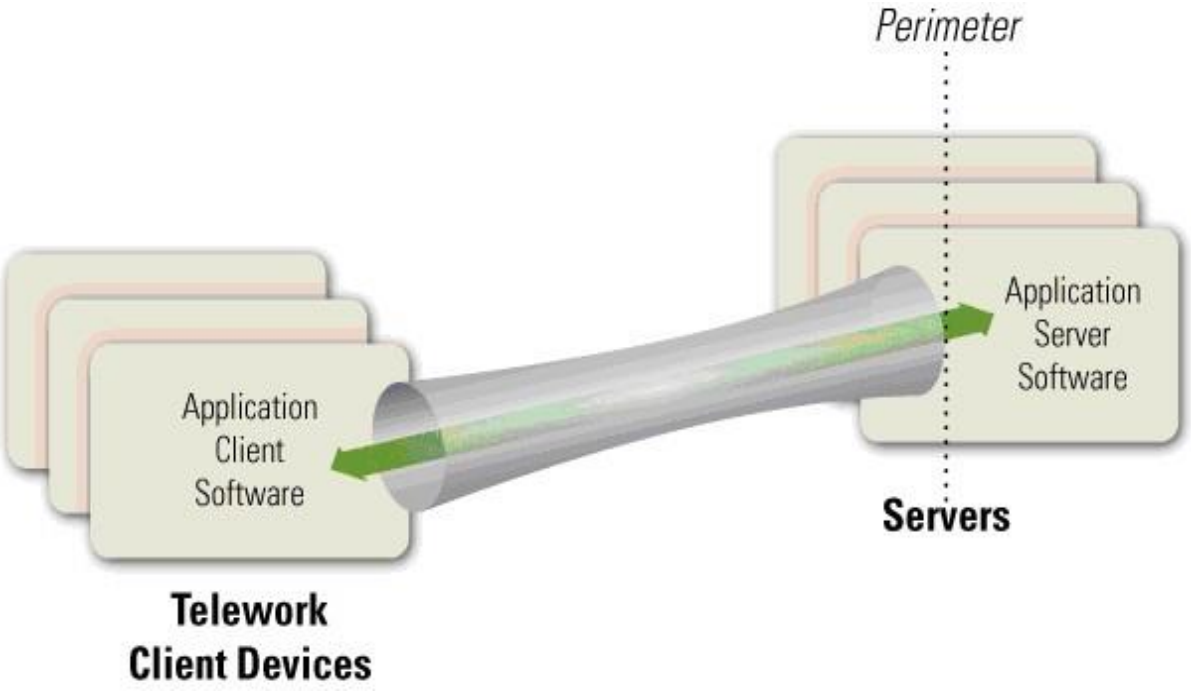
Innym poważnym problemem związanym z bezpieczeństwem oprogramowania zdalnego dostępu do pulpitu jest fakt, że jest ono zdecentralizowane; zamiast zabezpieczać pojedynczy serwer bramy VPN lub serwer portalu, organizacja musi zabezpieczyć każdą wewnętrzną stację roboczą, która może być dostępna poprzez zdalny dostęp do pulpitu. Ponieważ te wewnętrzne stacje robocze mogą być dostępne z Internetu, bezpośrednio lub pośrednio, muszą być zabezpieczone prawie tak rygorystycznie, jak pełnoprawne serwery zdalnego dostępu. Jednakże takie stacje robocze zazwyczaj nie były projektowane z myślą o takim stopniu bezpieczeństwa. Zastosowanie zabezpieczeń kompensacyjnych dla każdej stacji roboczej w celu podniesienia jej bezpieczeństwa do akceptowalnego poziomu, często wiąże się ze znacznym nakładem czasu i środków, a także z zakupem dodatkowych środków

bezpieczeństwa. Ponadto na każdej wewnętrznej stacji roboczej korzystającej ze zdalnego dostępu do pulpitu może być konieczne wdrożenie rozwiązań uwierzytelniających, takich jak funkcje uwierzytelniania dwuskładnikowego.

Generalnie, rozwiązania zdalnego dostępu do pulpitu, takie jak te wykorzystujące Microsoft Remote Desktop Protocol (RDP) lub Virtual Network Computing (VNC), powinny być stosowane tylko w wyjątkowych przypadkach, po dokładnej analizie zagrożeń bezpieczeństwa. Inne typy rozwiązań zdalnego dostępu opisane w tej sekcji oferują lepsze możliwości bezpieczeństwa.

### 2.2.4. Bezpośredni dostęp do aplikacji

Zdalny dostęp może być realizowany bez użycia oprogramowania zdalnego dostępu. Telepracownik może uzyskać bezpośredni dostęp do poszczególnych aplikacji, przy czym aplikacja zapewnia własne zabezpieczenia (szyfrowanie komunikacji, uwierzytelnianie użytkownika, itp.) Rysunek 2-4 przedstawia architekturę wysokiego poziomu dla bezpośredniego dostępu do aplikacji. Oprogramowanie klienckie aplikacji (*ang. Application Client Software*) zainstalowane na urządzeniu klienckim telepracownika (*ang. Telework Client Device*) inicjuje połączenie z serwerem, który zazwyczaj znajduje się na granicach sieci organizacji (np. w strefie DMZ) lub w architekturze chmury internetowej.




*Rysunek 2-4 Architektura bezpośredniego dostępu do aplikacji*

Jednym z najczęstszych przykładów bezpośredniego dostępu do aplikacji jest webmail. Telepracownik uruchamia przeglądarkę internetową i łączy się z serwerem WWW, który zapewnia dostęp do poczty elektronicznej. Serwer internetowy wykorzystuje protokół HTTP over TLS (HTTPS) w celu ochrony komunikacji, a aplikacja webmail na serwerze uwierzytelnia telepracownika przed przyznaniem dostępu do jego poczty elektronicznej. W przypadkach takich jak webmail, w których wykorzystuje się wspólnego klienta aplikacji (np. przeglądarkę internetową), bezpośredni dostęp do aplikacji zapewnia bardzo elastyczne rozwiązanie zdalnego dostępu, które może być używane z niemal każdego urządzenia klienckiego. Innym powszechnym przykładem bezpośredniego dostępu do aplikacji jest aplikacja na smartfona (oprogramowanie klienckie), która łączy się z usługą świadczoną przez jeden z serwerów organizacji poprzez HTTPS.

Z tych samych powodów, które zostały omówione w punkcie 2.2.3, architektura bezpośredniego dostępu do aplikacji jest generalnie akceptowalna tylko wtedy, gdy serwery, do których mają dostęp telepracownicy, znajdują się na obrzeżach sieci organizacji lub

w publicznej chmurze, a nie w sieciach wewnętrznych. Serwery, które są bezpośrednio dostępne z Internetu powinny być już dobrze zabezpieczone, aby zmniejszyć prawdopodobieństwo kompromitacji. Wiele organizacji decyduje się na zapewnienie bezpośredniego dostępu do aplikacji tylko do kilku aplikacji o niższym ryzyku, które są powszechnie używane, takich jak poczta elektroniczna, i używa metod tunelowych lub portalowych, aby zapewnić dostęp do innych aplikacji, szczególnie tych, które byłyby zbyt zagrożone, gdyby były dostępne bezpośrednio z Internetu.

## 2.3. Uwagi dotyczące BYOD i urządzeń klienckich kontrolowanych przez osoby trzecie

Od wielu lat powszechną praktyką w organizacjach jest zezwalanie na zdalny dostęp i telepracę z osobistych urządzeń komputerowych pracowników, kontrahentów, partnerów biznesowych i sprzedawców. Najnowszy trend, BYOD, rozszerza koncepcję telepracy, pozwalając na bezpośrednie podłączenie tych urządzeń do sieci przedsiębiorstwa. Wiąże się to ze znacznym ryzykiem dla organizacji, jeśli urządzenia te zostaną umieszczone w jej sieciach wewnętrznych, ponieważ urządzenia BYOD, którymi zarządzają sami użytkownicy, zazwyczaj nie są zabezpieczone w takim samym stopniu jak urządzenia własne organizacji. Ryzyko to można jednak w znacznym stopniu ograniczyć poprzez utworzenie w organizacji osobnej sieci przewodowej lub bezprzewodowej przeznaczonej dla urządzeń BYOD. Taka sieć BYOD powinna być zewnętrzna (np. poza strefą DMZ organizacji) i nie powinna zapewniać dostępu do zasobów przedsiębiorstwa w stopniu większym niż ten, który użytkownicy mają już zapewniony dzięki dostępowi zdalnemu. Organizacje, które rozważają dopuszczenie do używania w organizacji urządzeń BYOD, powinny zdecydowanie rozważyć utworzenie oddzielnej, zewnętrznej, dedykowanej sieci do użytku BYOD w obiektach przedsiębiorstwa. Sieć ta powinna być zabezpieczona i monitorowana w sposób spójny z tym, w jaki zabezpieczone i monitorowane są segmenty dostępu zdalnego.

Zagrożenia związane z BYOD i urządzeniami klienckimi kontrolowanymi przez strony trzecie są dość podobne do zagrożeń związanych z telepracą i zdalnym dostępem. Istnieje jednak kilka istotnych różnic:

- Złośliwy ruch generowany przez urządzenie BYOD lub urządzenie klienckie kontrolowane przez stronę trzecią w sieci przedsiębiorstwa, może wydawać się stronom zewnętrznym, że został wygenerowany przez samą organizację. Może to wpłynąć na reputację organizacji.
- Urządzenia BYOD i/lub kontrolowane przez osoby trzecie mogą atakować się nawzajem poprzez dedykowaną sieć.

## 2.4. Podsumowanie kluczowych zaleceń

Poniższa lista przedstawia niektóre z kluczowych rekomendacji zawartych w tej części dokumentu.

- W celu zapewnienia właściwego poziomu poufności, integralności i dostępności, wszystkie elementy rozwiązań telepracy i zdalnego dostępu, w tym urządzenia klienckie, serwery zdalnego dostępu oraz wewnętrzne serwery dostępne poprzez zdalny dostęp, powinny być zabezpieczone przed różnymi zagrożeniami. (Sekcja 2.1)
- Przed zaprojektowaniem i wdrożeniem rozwiązań telepracy i zdalnego dostępu, organizacje powinny opracować modele zagrożeń systemowych dla serwerów zdalnego dostępu oraz zasobów, do których uzyskuje się dostęp poprzez połączenie zdalne. (Sekcja 2.1)
- Planując politykę bezpieczeństwa i środki bezpieczeństwa telepracy, organizacje powinny założyć, że urządzenia klienckie zostaną przejęte przez wrogie podmioty, które będą próbowały pozyskać z nich wrażliwe dane lub wykorzystać je do uzyskania dostępu do sieci przedsiębiorstwa. (Sekcja 2.1)

- Organizacje powinny planować swoje zabezpieczenia dostępu zdalnego zakładając, że sieci pomiędzy urządzeniem klienckim, a organizacją nie mogą być zaufane. (Sekcja 2.1)
- Organizacje powinny założyć, że urządzenia klienckie mogą zostać zainfekowane złośliwym oprogramowaniem i w tym celu zaplanować odpowiednie środki bezpieczeństwa. (Sekcja 2.1)
- Organizacje powinny starannie rozważyć równowagę pomiędzy korzyściami płynącymi z zapewnienia zdalnego dostępu do dodatkowych zasobów, a potencjalnym wpływem narażenia tych zasobów na niebezpieczeństwo. Organizacje powinny zapewnić, że wszelkie wewnętrzne zasoby, które zostaną udostępnione poprzez zdalny dostęp są odpowiednio zabezpieczone przed zagrożeniami zewnętrznymi oraz, że dostęp do zasobów jest ograniczony do niezbędnego minimum poprzez zapory sieciowe i inne mechanizmy kontroli dostępu. (Sekcja 2.1)
- Planując rozwiązanie zdalnego dostępu, organizacje powinny dokładnie rozważyć implikacje metod zdalnego dostępu w każdej z czterech kategorii opisanych w sekcji 2.2, a także to, jak poszczególne metody mogą spełniać wymagania operacyjne organizacji. (Sekcja 2.2)
- Organizacje rozważające dopuszczenie w organizacji urządzeń BYOD, powinny zdecydowanie rozważyć utworzenie oddzielnej, zewnętrznej, dedykowanej sieci do korzystania z urządzeń BYOD na terenie przedsiębiorstwa. Taka sieć może być również wykorzystywana do obsługi urządzeń klienckich kontrolowanych przez strony trzecie, jeśli jest to pożądane. (Punkt 2.3)

# 3. ROZWIĄZANIA BEZPIECZEŃSTWA ZDALNEGO DOSTĘPU

W tym rozdziale przedstawiono zalecenia dotyczące zabezpieczania rozwiązań zdalnego dostępu. Skupiono się na bezpieczeństwie serwerów zdalnego dostępu i ich rozmieszczeniu. Omówiono również uwierzytelnianie, autoryzację i kontrolę dostępu. Zalecenia dotyczące zabezpieczania oprogramowania klienckiego zdalnego dostępu są przedstawione w tym rozdziale, natomiast zalecenia w zakresie zabezpieczania urządzeń klienckich do telepracy są przedstawione w rozdziale 4.

## 3.1. Bezpieczeństwo serwera zdalnego dostępu

Bezpieczeństwo serwerów zdalnego dostępu, takich jak bramy VPN i serwery portalowe, jest szczególnie ważne, ponieważ zapewniają one zewnętrznym hostom dostęp do zasobów wewnętrznych, a także bezpieczne, odizolowane środowisko telepracy dla urządzeń klienckich wydanych przez organizację, kontrolowanych przez strony trzecie oraz BYOD. Oprócz umożliwienia nieautoryzowanego dostępu do zasobów przedsiębiorstwa i urządzeń klienckich telepracy, zagrożony serwer może być wykorzystany do podsłuchiwania komunikacji i manipulowania nią, a także jako punkt startowy do ataku na inne hosty w organizacji. Zalecenia dotyczące ogólnego bezpieczeństwa serwerów są dostępne w dokumencie NIST SP 800-123, *Guide to General Server Security*. Serwery zdalnego dostępu powinny być w pełni załatane, obsługiwane przy użyciu zdefiniowanych przez organizację zabezpieczeń bazowych i zarządzane tylko z zaufanych hostów przez upoważnionych administratorów.

Na bramach i portalach VPN można uruchamiać wiele usług i aplikacji, takich jak zapory, oprogramowanie antymalware i oprogramowanie do wykrywania włamań. Organizacje powinny starannie rozważyć bezpieczeństwo wszelkich rozwiązań, które wymagają uruchomienia serwera zdalnego dostępu na tym samym hoście, na którym działają inne usługi i aplikacje. Takie rozwiązania mogą oferować korzyści, takie jak oszczędność kosztów sprzętu, ale kompromitacja jednej z usług lub aplikacji może pozwolić atakującemu na naruszenie zasad ochrony całego serwera zdalnego dostępu. Umieszczenie serwera zdalnego

dostępu na oddzielnym, dedykowanym hoście zmniejsza prawdopodobieństwo kompromitacji serwera zdalnego dostępu i ogranicza potencjalne skutki naruszenia zasad bezpieczeństwa. Użycie oddzielnego hosta może być również wskazane, jeśli serwer zdalnego dostępu może narazić inne usługi i aplikacje na znacznie zwiększone ryzyko. Organizacja powinna również rozważyć zastosowanie wielu rozwiązań zdalnego dostępu, jeżeli jej użytkownicy korzystający ze zdalnego dostępu mają bardzo różne potrzeby w zakresie bezpieczeństwa, np. jedna grupa ma dostęp do typowych zasobów niskiego ryzyka, a inna do wrażliwych danych o znaczeniu krytycznym. Bezpieczeństwo przechowywanych danych to kolejny ważny aspekt bezpieczeństwa serwerów zdalnego dostępu. W przypadku serwerów portalowych, które mogą tymczasowo przechowywać wrażliwe dane użytkowników, usuwanie takich danych z serwera, gdy tylko przestają być potrzebne, może zmniejszyć potencjalne skutki naruszenia serwera. Potrzeba usuwania wrażliwych danych z serwerów zdalnego dostępu powinna być określona na podstawie przeprowadzonej oceny ryzyka.

## 3.2. Lokalizacja serwera zdalnego dostępu

Główne czynniki, które organizacje powinny wziąć pod uwagę przy określaniu miejsca, w którym należy umieścić serwer zdalnego dostępu, są następujące:

- **Wydajność urządzenia**. Usługi zdalnego dostępu mogą wymagać dużych mocy obliczeniowych, głównie z powodu szyfrowania i deszyfrowania. Świadczenie usług zdalnego dostępu z urządzenia, które świadczy również inne usługi, może spowodować zbyt duże obciążenie serwera w godzinach szczytu użytkowania, powodując zakłócenia w świadczeniu usług. Wpływ szyfrowania i wymiany kluczy na wydajność można zmniejszyć poprzez wykonywanie ich na sprzętowych układach akceleratorów kryptograficznych. Tego rodzaju mikroprocesory mogą być umieszczone na płytach głównych komputerów lub kartach dodatkowych.
- **Analiza ruchu sieciowego.** Ponieważ treść zaszyfrowanej komunikacji zdalnego dostępu nie może być zbadana przez zapory sieciowe, systemy wykrywania włamań

i inne urządzenia zabezpieczające sieć, ogólnie zaleca się, żeby architektura zdalnego dostępu była zaprojektowana w taki sposób, aby niezaszyfrowana forma komunikacji mogła być zbadana przez odpowiednie sieciowe i/lub oparte na hostach środki bezpieczeństwa.

- **Ruch sieciowy niezabezpieczony przez rozwiązanie zdalnego dostępu**. Organizacje powinny dokładnie rozważyć zagrożenia dla ruchu sieciowego niechronionego przez rozwiązanie zdalnego dostępu, takiego jak ruch przekazywany pomiędzy serwerem zdalnego dostępu, a zasobami wewnętrznymi.
- **Translacja adresów sieciowych (NAT)**. Zastosowanie NAT może powodować problemy operacyjne w przypadku niektórych rozwiązań zdalnego dostępu. Na przykład, każdy system zdalnego dostępu, który wymaga od telepracownika bezpośredniego połączenia z hostem wewnątrz sieci, taki jak system zdalnego pulpitu lub VPN z publicznym punktem końcowym wewnątrz sieci, nie może współpracować z NAT bez specjalnej konfiguracji, która nie zawsze funkcjonuje. NAT uniemożliwia również korzystanie z aplikacji, które wymagają, aby adresy nie ulegały zmianie (np. osadzają adresy w treści aplikacji). Protokoły i mechanizmy, które przełamują NAT w celu rozwiązania konkretnych problemów z dostępem, często wprowadzają własne zagrożenia bezpieczeństwa, takie jak możliwość zezwolenia na dostęp do różnych hostów wewnątrz NAT w różnym czasie. Niektóre nowsze technologie NAT, w szczególności te wykorzystujące IPv6, nie są jeszcze dobrze poznane, a ich właściwości bezpieczeństwa nie zostały jeszcze w pełni przeanalizowane.

Organizacje powinny dokładnie rozważyć umiejscowienie swoich serwerów zdalnego dostępu. Niektóre serwery zdalnego dostępu, takie jak bramy VPN, generalnie działają, jako elementy pośredniczące pomiędzy urządzeniami do telepracy, a wewnętrznymi zasobami obliczeniowymi organizacji. Inne hosty świadczące usługi zdalnego dostępu, takie jak bezpośredni dostęp do aplikacji i rozwiązania zdalnego dostępu do pulpitu, są rzeczywistymi punktami końcowymi umożliwiającymi komunikację zdalnego dostępu. Obie kategorie serwerów zdalnego dostępu zostały omówione poniżej.

Serwery zdalnego dostępu są zazwyczaj umieszczane na granicach sieci organizacji. Takie umiejscowienie jest powszechne, ponieważ polityki bezpieczeństwa organizacji najczęściej dotyczą całej sieci organizacji. Nawet jeśli określona polityka bezpieczeństwa dotyczy jednej podsieci organizacji, większość serwerów zdalnego dostępu może ograniczać dostęp do podsieci i dlatego może być umieszczona na jej obrzeżach. W niektórych układach sieci, lepiej jest umieścić serwer zdalnego dostępu wewnątrz obwodu, na granicy podsieci. W dalszej części tego rozdziału opisano, kiedy zastosowanie takiego układu sieci może być odpowiednie.

### 3.2.1. Pośrednie serwery zdalnego dostępu

Pośrednie serwery zdalnego dostępu łączą zewnętrzne hosty z wewnętrznymi zasobami, dlatego powinny być zazwyczaj umieszczane na obrzeżach sieci. Serwer działa jako pojedynczy punkt wejścia do sieci z obwodu i egzekwuje politykę bezpieczeństwa telepracy. Jeżeli konieczny jest zdalny dostęp do konkretnej podsieci wewnątrz organizacji, istnieją na ogół dwie możliwości: 1) umieszczenie serwera zdalnego dostępu na brzegu podsieci, gdzie podsieć łączy się z siecią ogólną; lub 2) umieszczenie go na obwodzie macierzystej sieci i zastosowanie dodatkowych mechanizmów ograniczających telepracownikom możliwość dostępu tylko do określonej podsieci. Korzyści z umieszczenia serwera zdalnego dostępu na obwodzie sieci w porównaniu z posadowieniem go na obwodzie podsieci są różne dla poszczególnych czterech typów metod zdalnego dostępu:

- Serwery tunelowe zazwyczaj dają administratorom wystarczającą kontrolę nad wewnętrznymi zasobami, do których telepracownik ma dostęp, tak więc nie ma większych korzyści z umieszczenia serwera tunelowego na obrzeżu podsieci, zamiast na obwodzie sieci.
- Serwery portalowe uruchamiają oprogramowanie klienta aplikacji bezpośrednio na swoich dyskach. Umieszczenie tych serwerów na obwodzie sieci ma podobny efekt, jak umieszczenie ich na brzegu podsieci, ponieważ użytkownik zdalnego dostępu

uruchamia aplikacje tylko na serwerze portalowym, a nie na serwerach wewnątrz sieci.

- Zdalny dostęp do pulpitu nie angażuje serwerów zdalnego dostępu, więc nie ma znaczenia umiejscowienie serwera zdalnego dostępu.
- Serwery bezpośredniego dostępu do aplikacji uruchamiają oprogramowanie serwera aplikacji na samych serwerach. Umieszczenie ich na obwodzie sieci daje podobny efekt, jak umieszczenie ich na brzegu podsieci, ponieważ użytkownik zdalnego dostępu uruchamia aplikacje tylko na serwerze bezpośredniego dostępu do aplikacji, a nie na serwerach wewnątrz sieci.

Tak więc, jedynymi typami serwerów zdalnego dostępu, które mogą być odpowiednie do umieszczenia na obwodzie podsieci są serwery portalowe i serwery bezpośredniego dostępu do aplikacji, ale nawet w tych dwóch przypadkach, często lepiej jest uruchomić je na obwodzie organizacji, tak aby firewall organizacji mógł kontrolować dostęp do tych serwerów udzielany wszystkim pracownikom, a nie tylko telepracownikom. Ponadto, w celu uproszczenia zarządzania siecią i jej polityką bezpieczeństwa, zaleca się również uruchomienie wszystkich serwerów zdalnego dostępu na obwodzie tej sieci. Dlatego organizacje powinny umieszczać serwery zdalnego dostępu na obwodzie sieci zamiast na obwodzie podsieci, chyba, że istnieją istotne powody, aby postąpić inaczej.

Jeśli sieć ma na obwodzie zaporę sieciową, serwery zdalnego dostępu w tej sieci powinny być bezpośrednio podłączone do zapory sieciowej lub znajdować się w tym samym fizycznym urządzeniu, co zapora sieciowa, aby nie omijać jej polityki bezpieczeństwa. W przypadku, gdy te dwa urządzenia są takie same, nie ma oczywiście wątpliwości co do umiejscowienia serwera zdalnego dostępu. Jeśli jednak serwer zdalnego dostępu jest innym urządzeniem niż firewall, projektant sieci musi zdecydować, gdzie umieścić serwer zdalnego dostępu. Jeśli zapora sieciowa ma powiązaną strefę DMZ, to taka strefa DMZ jest prawdopodobnie najlepszym miejscem dla serwera zdalnego dostępu, w przeciwnym razie serwer powinien znajdować się poza zaporą sieciową, jeśli topologia sieci na to pozwala. Oba te miejsca

zapewniają logiczną separację między serwerem zdalnego dostępu, a sieciami wewnętrznymi. W celu zmniejszenia potencjalnych skutków kompromitacji serwera zdalnego dostępu, organizacje powinny ograniczyć komunikację między serwerem, a sieciami wewnętrznymi. Serwer powinien mieć możliwość inicjowania komunikacji tylko z wewnętrznymi hostami i usługami specjalnie autoryzowanymi do korzystania ze zdalnego dostępu, a tylko odpowiednie hosty wewnętrzne (np. zaufane hosty używane do administrowania serwerem zdalnego dostępu) powinny mieć możliwość inicjowania komunikacji z serwerem zdalnego dostępu.

Jeśli serwer zdalnego dostępu musi być umieszczony wewnątrz zapory sieciowej, polityka bezpieczeństwa firewalla powinna być tak dostosowana, aby do serwera zdalnego dostępu docierał tylko niezbędny ruch pochodzący tylko i wyłącznie od telepracowników. Może to polegać między innymi na ograniczeniu ruchu przychodzącego tylko do adresów IP lub zakresów adresów używanych przez sieci kontrahentów, partnerów biznesowych i dostawców oraz używanych przez sieci domowe pracowników, jeśli te sieci mają stałe (niezmienne) adresy. Ustanowienie tak precyzyjnej polityki telepracy odnoszącej się do mobilnych urządzeń klienckich może być trudne do utrzymania i podatne na błędy Z uwagi na to, że cała komunikacja zdalnego dostępu powinna być szyfrowana, jak to zostało omówione w rozdziale 4, środki bezpieczeństwa sieci nie będą w stanie monitorować zawartości komunikacji. Dlatego też należy unikać tego rozwiązania.

### 3.2.2. Serwery zdalnego dostępu punktów końcowych

Serwery zdalnego dostępu punktów końcowych powinny być umieszczone w DMZ organizacji, kiedy tylko jest to możliwe. Pozwala to zaporze sieciowej ograniczyć dostęp do serwerów zarówno z hostów zewnętrznych, jak i wewnętrznych, a także uniknąć problemów bezpieczeństwa omówionych w punkcie 2.2.3, związanych z dopuszczeniem ruchu zewnętrznego bezpośrednio do sieci wewnętrznej. Implementacje rozwiązań zdalnego dostępu do pulpitu zazwyczaj opierają się na wewnętrznych stacjach roboczych

zapewnianiających usługi zdalnego dostępu, więc korzystanie z takich rozwiązań nie jest ogólnie zalecane.

## 3.3. Uwierzytelnianie, autoryzacja i kontrola dostępu do zdalnego dostępu

Większość zasobów obliczeniowych wykorzystywanych poprzez zdalny dostęp jest dostępna tylko dla użytkowników organizacji, a często tylko dla podzbioru tych użytkowników. Aby zapewnić, że dostęp jest odpowiednio ograniczony, serwery zdalnego dostępu powinny uwierzytelniać każdego telepracownika przed przyznaniem mu dostępu do zasobów organizacji, a następnie używać technologii autoryzacji, aby zagwarantować, że tylko niezbędne zasoby mogą być wykorzystane. Uwierzytelnienie może być również użyte do potwierdzenia legalności urządzeń klienckich telepracy i serwerów zdalnego dostępu. Technologie kontroli dostępu są również potrzebne do ograniczenia dostępu do komunikacji sieciowej i aplikacji. Ten rozdział zawiera dodatkowe szczegóły na temat uwierzytelniania, autoryzacji i kontroli dostępu do zdalnego dostępu.

### 3.3.1. Uwierzytelnianie

Istnieje wiele sposobów uwierzytelniania użytkowników zdalnego dostępu, takich jak hasła[15], certyfikaty cyfrowe lub sprzętowe tokeny uwierzytelniające. Jeśli hasła są jedyną formą uwierzytelniania stosowaną w rozwiązaniach zdalnego dostępu, to generalnie mechanizm uwierzytelniania zdalnego dostępu powinien być inny, niż pozostałe mechanizmy uwierzytelniania organizacji, takie jak hasła poczty elektronicznej lub usług katalogowych, chyba, że używany jest bezpośredni dostęp do aplikacji. Posiadanie różnych haseł zmniejsza wpływ, jaki kompromitacja danych uwierzytelniających zdalnego dostępu miałaby na inne zasoby informacyjne i vice versa, i jest szczególnie ważne, jeżeli użytkownicy wprowadzają hasła do urządzeń telepracy, które nie są kontrolowane przez organizację. Jednakże, posiadanie różnych haseł do zdalnego dostępu i innych systemów często nie jest

[15] Więcej informacji i zaleceń dotyczących haseł można znaleźć w projekcie NIST SP 800-118, *Guide to Enterprise Password Management* (http://csrc.nist.gov/publications/PubsSPs.html#800-118).

egzekwowalne[16] i należy założyć, że niektórzy użytkownicy będą używać tych samych haseł w obu systemach. Organizacje o wyższych wymaganiach bezpieczeństwa lub mające obawy co do bezpieczeństwa haseł, powinny rozważyć zastosowanie uwierzytelniania, które nie opiera się wyłącznie na hasłach, np. stosując uwierzytelnianie wieloskładnikowe.

Podmioty publiczne powinny wydawać zezwolenia na zdalny dostęp tylko z użyciem uwierzytelniania dwuskładnikowego, gdzie jeden z czynników jest zapewniany przez urządzenie oddzielne od komputera uzyskującego dostęp. Takie dwuskładnikowe uwierzytelnianie jest obecnie zazwyczaj realizowane poprzez użycie tokena kryptograficznego i hasła, ponieważ inne metody uwierzytelniania są często niedostępne na urządzeniach klienckich telepracy. Na przykład, większość urządzeń mobilnych nie posiada funkcji biometrycznych, czytników kart inteligentnych lub innych dodatkowych funkcji uwierzytelniania.[17] Jest to szczególnie istotne w przypadku urządzeń klienckich nienależących do organizacji.

Wiele organizacji wymaga od telepracowników okresowego ponownego uwierzytelniania się podczas długich sesji zdalnego dostępu, np. po każdych ośmiu godzinach sesji lub po 30 minutach bezczynności. Pomaga to organizacjom potwierdzić, że osoba korzystająca ze zdalnego dostępu jest do tego upoważniona. Wskazane jest stosowanie funkcji 'time-out' dla zdalnego dostępu i urządzeń mobilnych, wymagającej ponownego uwierzytelnienia użytkownika po trzydziestu minutach bezczynności.[18] Serwery zdalnego dostępu różnią się pod względem obsługi metod uwierzytelniania i limitów czasu sesji, dlatego do wdrożenia i egzekwowania tych zasad mogą być potrzebne dodatkowe mechanizmy. Dodatkowe informacje na temat rodzajów metod uwierzytelniania użytkownika odpowiednich dla

[16] W niektórych przypadkach można to wymusić za pomocą scentralizowanego systemu zarządzania hasłami, zarówno hasłami zdalnego dostępu, jak i hasłami innych systemów. Wiele scentralizowanych systemów zarządzania hasłami może zapewnić, że to samo hasło nie jest używane dla dwóch różnych systemów.

[17] Jedną z możliwości dla organizacji jest wykorzystanie pochodnych danych uwierzytelniających Personal Identity Verification (PIV). Więcej informacji można znaleźć w dokumencie NIST SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials (http://dx.doi.org/10.6028/NIST.SP.800-157).

[18] Patrz: NSC 800-53, zabezpieczenie AC-11.

zdalnego dostępu można znaleźć w publikacji NIST SP 800-63, Electronic Authentication Guideline[19].

Jeśli to możliwe, organizacje powinny zaimplementować wzajemne uwierzytelnianie, tak, aby użytkownik zdalnego dostępu mógł zweryfikować legalność serwera zdalnego dostępu przed przekazaniem mu danych uwierzytelniających. Przykładem może być weryfikacja cyfrowego certyfikatu przedstawionego przez serwer zdalnego dostępu, aby upewnić się, że serwer jest kontrolowany przez organizację. Certyfikaty cyfrowe użytkownika mogą być stosowane w wielu systemach zdalnego dostępu, choć systemy te mogą się różnić sposobem obsługi certyfikatów. Większość certyfikatów cyfrowych użytkownika ma klucz prywatny związany z certyfikatem chronionym hasłem. Niektóre metody zdalnego dostępu, takie jak technologie IPsec i SSL VPN, obejmują obowiązkowe uwierzytelnianie serwera podczas konfigurowania bezpiecznego kanału komunikacyjnego. Uwierzytelnianie serwera jest najistotniejsze w przypadku metod zdalnego dostępu, w których użytkownik ręcznie nawiązuje połączenie zdalnego dostępu, np. wpisując adres URL w przeglądarce internetowej. Dodatkowe informacje na ten temat przedstawiono w sekcji 3.4.

### 3.3.2. Autoryzacja

Po zweryfikowaniu tożsamości użytkownika zdalnego dostępu, organizacja może zdecydować się na przeprowadzenie kontroli urządzenia klienckiego w celu określenia zasobów wewnętrznych, do których użytkownik powinien mieć dostęp. Kontrole te są czasami nazywane badaniami *kondycji*, *przydatności*, *kwalifikacyjnymi* lub *oceniającymi*. Najczęstszym sposobem realizacji tego zadania jest wykonanie przez serwer zdalnego dostępu kontroli stanu urządzenia klienckiego telepracownika. Sprawdzenia te wymagają zazwyczaj, aby oprogramowanie na urządzeniu użytkownika, które jest kontrolowane przez serwer zdalnego dostępu, weryfikowało zgodność z określonymi wymaganiami bazowej bezpiecznej konfiguracji organizacji, takimi jak aktualność oprogramowania antymalware,

[19] http://dx.doi.org/10.6028/NIST.SP.800-63-2

poprawność systemu operacyjnego oraz fakt, że urządzenie użytkownika jest własnością i jest kontrolowane przez organizację. Urządzenia przenośne są zazwyczaj poddawane rzadszym kontrolom, jednakże ważną czynnością jest sprawdzenie, czy na urządzeniu przenośnym nie zdjęto zabezpieczenia systemu (*ang. jailbroken*) lub uzyskano dostęp do konta administratora (*ang. rooted*), co może mieć poważne negatywne skutki dla bezpieczeństwa.[20]

Niektóre rozwiązania zdalnego dostępu mogą również określić, czy urządzenie zostało zabezpieczone przez organizację i jakiego typu jest to urządzenie (np. komputer stacjonarny/laptop, smartfon, tablet). Na podstawie wyników tych kontroli organizacja może określić, czy urządzenie powinno być dopuszczone do korzystania ze zdalnego dostępu i jaki poziom dostępu powinien być przyznany. Jeśli użytkownik posiada akceptowalne poświadczenia autoryzacji, ale urządzenie klienckie nie przechodzi pomyślnie kontroli kwalifikacyjnej, użytkownik i urządzenie mogą otrzymać ograniczony dostęp do sieci wewnętrznej, całkowity brak dostępu do sieci lub dostęp do sieci kwarantanny, aby można było naprawić braki w zabezpieczeniach. Decyzja ta może również dotyczyć tej części sieci, do której urządzenie próbuje uzyskać dostęp; natomiast organizacja może mieć bardziej rygorystyczne zasady w przypadku bardziej wrażliwych danych. Niektóre organizacje wydają również certyfikaty cyfrowe urządzeniom klienckim, aby w ramach zabezpieczenia umożliwić uwierzytelnienie samego urządzenia.

Autoryzacja na podstawie typu używanego urządzenia i jego właściwości jest określana mianem kontroli dostępu do sieci (*ang. network access control - NAC*). NAC jest mechanizmem egzekwowania polityki bezpieczeństwa, a nie rzeczywistym mechanizmem ochrony bezpieczeństwa. Przykłady kontroli NAC obejmują sprawdzenie obecności poprawek bezpieczeństwa, potwierdzenie, że oprogramowanie antymalware jest włączone i aktualne, upewnienie się, że osobista zapora sieciowa jest włączona i blokuje ruch przychodzący, oraz

[20] Nowe metody rootowania i jailbreakingu urządzeń mobilnych są często tworzone, więc jest mało prawdopodobne, aby kontrole kondycji urządzenia mogły wykryć każdy przypadek użycia takich metod.

przeprowadzenie uwierzytelnienia urządzenia. Jednakże, wiele kontroli stanu jest wykonywanych w sposób, który może być łatwo ominięty przez złośliwe oprogramowanie, więc organizacje nie powinny polegać na NAC w celu uniemożliwienia uzyskania dostępu do sieci przez zdeterminowanych napastników. Organizacje powinny używać NAC zawsze wtedy, gdy jest to możliwe, aby wykryć poważne naruszenia polityki bezpieczeństwa na urządzeniach klienckich do telepracy oraz, aby zapobiec przypadkowemu użyciu przez telepracowników niewłaściwego urządzenia do telepracy. Niektóre rozwiązania NAC mogą być również wykorzystywane do kontrolowania, zasobów wewnętrznych, do których dostęp może mieć każde urządzenie klienckie, oraz czy działania naprawcze mogą być wykonane na urządzeniu klienckim zanim uzyska ono dostęp.

### 3.3.3. Kontrola dostępu do systemów komunikacji sieciowej

Głównym sposobem kontrolowania dostępu do komunikacji sieciowej i ochrony jej zawartości jest stosowanie kryptografii. Wszystkie wrażliwe informacje przekazywane za pośrednictwem Internetu, sieci bezprzewodowych i innych niezaufanych sieci powinny co najmniej zachować poufność i integralność dzięki zastosowaniu kryptografii.

Przykładowo, w USA agencje federalne są zobowiązane do stosowania algorytmów kryptograficznych zatwierdzonych przez instytut NIST i zawartych w modułach zatwierdzonych przez FIPS. Specyfikacja FIPS 140, Wymagania bezpieczeństwa dla modułów kryptograficznych, definiuje sposób walidacji modułów kryptograficznych.[21] Należy zauważyć, że aby system zdalnego dostępu został uznany za zgodny ze standardem FIPS 140, obie strony interakcji muszą przejść walidację zgodną ze standardem FIPS 140.

Wiele systemów zdalnego dostępu, takich jak sieci SSL VPN, obsługuje oprogramowanie klienckie innych producentów, dlatego w przypadku danego systemu zdalnego dostępu mogą istnieć dwa lub więcej odrębnych certyfikatów walidacji.

[21] Aktualną wersja standardu FIPS 140 jest standard FIPS 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

Niektóre metody zdalnego dostępu, takie jak IPsec i SSL VPN, często zawierają zatwierdzone przez NIST mechanizmy szyfrowania komunikacji i sprawdzania jej integralności. Niektóre metody zdalnego dostępu mogą wykorzystywać inne, zatwierdzone przez NIST mechanizmy kryptograficzne w celu zapewnienia ochrony. W przypadku metod zdalnego dostępu, które nie oferują zatwierdzonych przez NIST mechanizmów ochrony poufności i integralności komunikacji, należy zastosować dodatkowe zatwierdzone przez NIST zabezpieczenia, takie jak tunelowanie komunikacji w ramach metody zdalnego dostępu w sieci VPN lub prowadzenie komunikacji za pośrednictwem protokołu TLS. Metody zdalnego dostępu, które oferują zarówno mechanizmy kryptograficzne zatwierdzone przez NIST, jak i niezatwierdzone przez NIST, powinny w miarę możliwości wyłączać stosowanie wszystkich niezatwierdzonych mechanizmów kryptograficznych. Zwykle osiąga się to poprzez konfigurację serwera zdalnego dostępu.

Kontrola dostępu do komunikacji sieciowej może również obejmować określenie, który ruch powinien być chroniony. Niektóre rozwiązania zdalnego dostępu oferują odpowiednie opcje umożliwiające dostęp; na przykład wielu klientów VPN posiada funkcję zwaną tunelowaniem dzielonym (*ang. split tunneling*), która, jeśli zostanie włączona, będzie tunelować całą komunikację dotyczącą wewnętrznych zasobów organizacji przez VPN, chroniąc je w ten sposób, ale wykluczy wszelką inną komunikację przechodzącą przez tunel. Tunelowanie dzielone zwiększa wydajność komunikacji i zmniejsza obciążenie rozwiązania zdalnego dostępu, ale jednocześnie uniemożliwia organizacji zbadanie dużej części ruchu sieciowego telepracowników oraz ochronę poufności i integralności tego ruchu. Ponadto, zastosowanie tunelowania dzielonego może spowodować, że urządzenie telepracownika, które posiada dwa aktywne interfejsy internetowe - np. komputer PC podłączony jednocześnie do sieci Ethernet i sieci bezprzewodowej - nieumyślnie stanie się mostem pomiędzy siecią zaufaną i niezaufaną. Stanowi to poważne zagrożenie bezpieczeństwa i jest naruszeniem zasad bezpieczeństwa większości organizacji. W przypadku telepracowników korzystających z VPN w niezaufanych sieciach, szczególnie tych o podwyższonym ryzyku, takich jak hotspoty

bezprzewodowe, organizacje powinny rozważyć wyłączenie możliwości dzielenia tuneli, aby osoby atakujące nie mogły podsłuchiwać komunikacji sieciowej telepracowników.

Niektóre organizacje dostarczają, do sieci domowych telepracowników lub sieci ich kontrahentów, partnerów biznesowych i dostawców, bramy VPN, urządzenia firewall lub inne urządzenia zabezpieczające, które są skonfigurowane tak, aby egzekwować politykę bezpieczeństwa organizacji. Daje to organizacjom większą kontrolę nad bezpieczeństwem telepracy, ale może również wiązać się ze znacznymi kosztami związanymi z zakupem, wdrożeniem, zarządzaniem i konserwacją urządzeń zabezpieczających. Ponadto, ponieważ większość sieci wykorzystywanych do telepracy jest używana również do innych celów, polityka bezpieczeństwa może kolidować z innymi zastosowaniami sieci, jeżeli nie zostanie odpowiednio zaprojektowana. Inną wadą jest to, że urządzenia zabezpieczające, jeśli zostaną skradzione lub w inny sposób przejęte przez atakującego, mogą zapewnić atakującemu łatwy dostęp do systemów organizacji, jeśli stosowane przez organizację rozwiązanie zdalnego dostępu uwierzytelnia tylko urządzenie zabezpieczające, a nie uwierzytelnia użytkownika zdalnego dostępu. Dlatego też, gdy takie urządzenia zabezpieczające są używane, zarówno urządzenie jak i użytkownik powinny być uwierzytelniane przez organizację.

### 3.3.4. Kontrola dostępu do aplikacji

Różne typy architektur zdalnego dostępu oferują różne poziomy szczegółowości kontroli dostępu do aplikacji. Tunele często posiadają mechanizm pozwalający administratorowi na określenie, do których portów, na których hostach, telepracownik ma dostęp; może to ograniczyć dostęp tak, że tylko określone aplikacje mogą być używane. Portale ze swej natury ograniczają telepracownika do aplikacji działających na serwerze portalu. Podobnie, bezpośredni dostęp do aplikacji ogranicza telepracownika do konkretnej aplikacji na jednym serwerze. Zdalny dostęp do pulpitu może zapewnić kontrolę dostępu do aplikacji jedynie poprzez połączenie jego zasad z ograniczeniami kontroli dostępu obowiązującymi na wewnętrznych stacjach roboczych.

Ograniczenie dostępu do aplikacji niekoniecznie zapobiega wpływowi telepracowników na inne zasoby, ponieważ uruchamiane aplikacje mogą mieć dostęp do innych zasobów sieciowych. Na przykład, serwer WWW, do którego telepracownik ma dostęp, może powodować odszukiwanie danych na serwerach baz danych, pobieranie danych z serwerów plików i inne działania angażujące dodatkowe serwery. Dlatego też polityka ograniczająca telepracownika do określonych aplikacji powinna być rozpatrywana w świetle tego, z jakimi innymi aplikacjami i hostami te aplikacje mogą wchodzić w interakcję.

## 3.4. Bezpieczeństwo oprogramowania klienckiego zdalnego dostępu

Innym ważnym elementem bezpieczeństwa rozwiązań zdalnego dostępu jest konfiguracja zabezpieczeń oprogramowania klienckiego zdalnego dostępu. Wielu klientów zdalnego dostępu posiada funkcje i ustawienia zabezpieczeń, którymi może zdalnie zarządzać administrator systemu. Takie zarządzanie jest szczególnie ważne w przypadku oprogramowania klienckiego, które ma złożone ustawienia zabezpieczeń. Na przykład, wielu użytkowników ma trudności z ręcznym ustawieniem konfiguracji IPsec lub opcji uwierzytelniania zdalnego dostępu do pulpitu. Jeśli klient ma możliwość zdalnego zarządzania, administrator może przejrzeć jego konfigurację, zmienić ją i ewentualnie zablokować. Blokowanie zapewnia, że ustawienia zabezpieczeń nie zostaną przypadkowo lub celowo zmienione, co mogłoby zmniejszyć bezpieczeństwo zdalnego dostępu. Nie ma jednak standaryzacji funkcjonalności i interfejsów zdalnego zarządzania, a wiele systemów zdalnego dostępu nie posiada funkcji zdalnego zarządzania w swoim oprogramowaniu klienckim.

Przed wyborem i wdrożeniem rozwiązania zdalnego dostępu, organizacje powinny dokładnie zaplanować, w jaki sposób będzie utrzymywane i zarządzane bezpieczeństwo oprogramowania klienckiego zdalnego dostępu. W szerszym ujęciu, organizacje powinny również zaplanować, w jaki sposób urządzenia klienckie udostępniane telepracownikom do telepracy, będą zarządzane i wspierane, np. pracownik działu pomocy technicznej będzie miał zdalny dostęp do urządzenia w celu rozwiązywania problemów operacyjnych zgłoszonych przez telepracownika. W przypadku braku odpowiedniego zabezpieczenia,

funkcje zdalnego zarządzania mogą zostać wykorzystane przez atakujących do przejęcia kontroli nad urządzeniami klienckimi telepracy i użycia ich do uzyskania dostępu do wewnętrznych zasobów organizacji. Dlatego też, organizacje powinny zapewnić, że zdalne zarządzanie jest odpowiednio zabezpieczone, w szczególności poprzez szyfrowanie komunikacji sieciowej i wzajemne uwierzytelnianie punktów końcowych.

Organizacje powinny również rozważyć "grubość" (*ang. thickness*) oprogramowania klienckiego zdalnego dostępu. Klient zdalnego dostępu jest uważany za *grubego klienta,* jeśli jest skonfigurowany w taki sposób, że organizacja ma prawie całkowitą kontrolę nad środowiskiem zdalnego dostępu. Na przykład, wielu klientów VPN może być skonfigurowanych tak, aby było bardzo grubych, np. tunelowanie całej komunikacji sieciowej z urządzenia klienckiego do sieci organizacji, używanie usług systemu nazw domen (*ang. Domain Name System - DNS*) organizacji zamiast usług DNS sieci lokalnej oraz twarde kodowanie adresu IP bramy VPN, zamiast polegania na lokalnym rozwiązywaniu nazwy serwera DNS.

Jednak wielu klientów VPN może być również skonfigurowanych jako *cienki klient*, co oznacza, że klient używa wspólnej aplikacji już obecnej na urządzeniu telepracy, takiej jak przeglądarka internetowa. W przypadku cienkiego klienta VPN, organizacja ma znacznie mniejszą kontrolę nad środowiskiem zdalnego dostępu w porównaniu do grubego klienta. Cienki klient VPN może polegać na usługach sieci lokalnej i zezwalać na komunikację, która nie dotyczy wewnętrznych zasobów organizacji i jest przesyłana bez ochrony przez sieci publiczne. Niektóre typy rozwiązań zdalnego dostępu, takie jak portale, zdalny dostęp do pulpitu i bezpośredni dostęp do aplikacji, to z natury ciency klienci zdalnego dostępu.

Cienki klient zdalnego dostępu jest ogólnie bardziej elastyczny i wydajny niż gruby klient, ale powoduje również większe ryzyko błędu i kompromitacji - na przykład, użytkownik może błędnie wpisać adres URL serwera portalowego w przeglądarce internetowej i dotrzeć do fałszywej witryny. Gruby klient pomaga zapewnić, że klient komunikuje się z legalnymi serwerami zdalnego dostępu i innymi zasobami. Organizacje o wyższych potrzebach

w zakresie bezpieczeństwa lub o szczególnie wysokim ryzyku związanym z komunikacją zdalnego dostępu powinny używać grubych klientów zdalnego dostępu, gdy tylko jest to możliwe, aby zmniejszyć ryzyko kompromitacji.

## 3.5. Podsumowanie kluczowych zaleceń

Poniższa lista przedstawia niektóre z kluczowych rekomendacji zawartych w tej części dokumentu.

- Bezpieczeństwo serwerów zdalnego dostępu jest szczególnie ważne. Zalecenia dotyczące ogólnego bezpieczeństwa serwerów są dostępne w dokumencie NIST SP 800-123, *Guide to General Server Security*. Serwery zdalnego dostępu powinny być w pełni załatane, obsługiwane z wykorzystaniem zdefiniowanej przez organizację konfiguracji zabezpieczeń bazowych i zarządzane z zaufanych hostów tylko przez upoważnionych administratorów. (Sekcja 3.1)
- Organizacje powinny dokładnie rozważyć bezpieczeństwo wszelkich rozwiązań zdalnego dostępu, które wymagają uruchomienia serwera zdalnego dostępu na tym samym hoście co inne usługi i aplikacje. (Sekcja 3.1)
- Organizacje powinny wziąć pod uwagę kilka głównych czynników przy określaniu miejsca umieszczenia serwera zdalnego dostępu, w tym wydajność urządzenia, badanie ruchu, występowanie ruchu niezabezpieczonego i stosowanie NAT. Organizacje powinny umieszczać serwery zdalnego dostępu na granicach sieci, chyba, że istnieją istotne powody, aby postąpić inaczej. (Sekcja 3.2)
- W celu odpowiedniego ograniczenia dostępu, serwery zdalnego dostępu powinny uwierzytelniać każdego telepracownika przed przyznaniem mu jakiegokolwiek dostępu do zasobów organizacji, a następnie dokonywać autoryzacji, w celu zapewnienia, że tylko niezbędne zasoby mogą być używane. Jeśli jest to możliwe, organizacje powinny wdrożyć wzajemne uwierzytelnianie, tak aby użytkownik zdalnego dostępu mógł zweryfikować legalność serwera zdalnego dostępu przed przekazaniem mu danych uwierzytelniających. (Sekcja 3.3)

- Wszelkie poufne informacje pochodzące z komunikacji zdalnego dostępu przechodzącej przez Internet, sieci bezprzewodowe i inne niezaufane sieci, powinny być chronione pod względem poufności i integralności za pomocą kryptografii. Może to być osiągane, np. poprzez stosowanie algorytmów kryptograficznych zatwierdzonych przez instytut NIST i zawartych w modułach zatwierdzonych przez FIPS. (Sekcja 3.3)
- Przed wyborem i wdrożeniem rozwiązania zdalnego dostępu organizacje powinny dokładnie zaplanować, w jaki sposób będzie utrzymywane i zarządzane bezpieczeństwo oprogramowania klienckiego zdalnego dostępu. Organizacje powinny również zaplanować, w jaki sposób będą zarządzane i wspierane urządzenia klienckie do telepracy, które są udostępniane telepracownikom. Organizacje powinny zapewnić, że zdalne zarządzanie jest odpowiednio zabezpieczone, w szczególności poprzez szyfrowanie komunikacji sieciowej i wzajemne uwierzytelnianie punktów końcowych. (Punkt 3.4)
- Organizacje o wyższych potrzebach w zakresie bezpieczeństwa lub o szczególnie wysokim ryzyku związanym z komunikacją zdalnego dostępu, powinny w miarę możliwości korzystać z grubych klientów zdalnego dostępu, aby zmniejszyć ryzyko kompromitacji. (Sekcja 3.4)

# 4. BEZPIECZEŃSTWO URZĄDZEŃ KLIENCKICH DO TELEPRACY

Urządzenia klienckie do telepracy można podzielić na dwie ogólne kategorie:

- **Komputery osobiste (PC), czyli komputery** stacjonarne i laptopy. Na komputerach PC działają stacjonarne/laptopowe systemy operacyjne, takie jak Windows, Apple OS X i Linux. Komputery PC mogą być używane do każdej z metod zdalnego dostępu opisanych w tej sekcji.
- **Urządzenia mobilne,** czyli małe komputery przenośne, takie jak smartfony i tablety, na których często działa system operacyjny dedykowany dla urządzeń mobilnych, taki jak Apple iOS czy Google Android. Urządzenia mobilne są najczęściej wykorzystywane do metod zdalnego dostępu wykorzystujących przeglądarki internetowe, głównie SSL VPN i indywidualny dostęp do aplikacji internetowych.

Różnica między komputerami PC, a urządzeniami mobilnymi zmniejsza się. Urządzenia mobilne oferują coraz więcej funkcji, które wcześniej były dostępne tylko na komputerach PC. Mimo to, zabezpieczenia dostępne dla komputerów PC i urządzeń mobilnych różnią się znacząco od siebie, dlatego w dalszej części niniejszej publikacji znajdują się osobne zalecenia dla komputerów PC i urządzeń mobilnych, tam gdzie ma to zastosowanie.

Kolejnym zestawem kategorii użytych w rekomendacjach jest strona, która jest odpowiedzialna za bezpieczeństwo urządzenia klienckiego. Kategorie te są następujące:

- **Organizacja.** Urządzenia klienckie w tej kategorii są zazwyczaj nabywane, konfigurowane i zarządzane przez organizację. Urządzenia te mogą być wykorzystywane do każdej z metod zdalnego dostępu stosowanych przez organizację.
- **Kontrolowane przez stronę trzecią.** Te urządzenia klienckie są kontrolowane przez pracodawcę telepracownika, np. zleceniobiorcę, partnera biznesowego lub dostawcę. Osoba trzecia jest ostatecznie odpowiedzialna za zabezpieczenie urządzeń klienckich i utrzymanie ich bezpieczeństwa, co jest udokumentowane w umowach pomiędzy

organizacją a osobą trzecią. Urządzenia te mogą być zazwyczaj wykorzystywane do wielu lub wszystkich metod zdalnego dostępu stosowanych przez organizację.

- **BYOD.** Te urządzenia klienckie są kontrolowane przez telepracownika, który jest w pełni odpowiedzialny za ich zabezpieczenie i utrzymanie bezpieczeństwa. Urządzenia te mogą być zazwyczaj wykorzystywane do wielu lub wszystkich metod zdalnego dostępu stosowanych w organizacji.
- **Nieznane.** Te urządzenia klienckie, określane jako "nieznane", ponieważ nie ma pewności co do ich bezpieczeństwa, są własnością i są kontrolowane przez inne podmioty, np. komputery w kioskach hotelowych, komputery PC lub urządzenia mobilne należące do przyjaciół i rodziny. Opcje zdalnego dostępu do tych urządzeń są zazwyczaj dość ograniczone, ponieważ użytkownicy nie mogą lub nie powinni instalować na nich oprogramowania, a ich używanie jest bardzo ryzykowne ze względu na nieznany charakter ich zabezpieczeń.

W dzisiejszym środowisku komputerowym istnieje wiele zagrożeń dla urządzeń klienckich telepracy. Zagrożenia te są stwarzane przez osoby o różnych motywacjach, w tym powodujące zakłócenia w pracy, kradnące własność intelektualną, dokonujące kradzieży tożsamości i innych form oszustwa. Podstawowym zagrożeniem dla większości urządzeń klienckich do telepracy jest złośliwe oprogramowanie, w tym wirusy, robaki, złośliwy kod mobilny, konie trojańskie, rootkity, oprogramowanie szpiegujące i boty.[22] Złośliwe oprogramowanie może zainfekować urządzenia klienckie na wiele sposobów, w tym za pośrednictwem poczty elektronicznej, stron internetowych, pobierania i udostępniania plików, oprogramowania peer-to-peer, komunikatorów internetowych i mediów społecznościowych. Użycie nieautoryzowanych nośników lub urządzeń wymiennych, takich jak dyski flash, jest częstym mechanizmem przenoszenia złośliwego oprogramowania. Innym powszechnym zagrożeniem dla urządzeń klienckich telepracy jest ich utrata lub kradzież.

[22] Więcej informacji na temat złośliwego oprogramowania można znaleźć w dokumencie NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (http://dx.doi.org/10.6028/NIST.SP.800-83r1).

Osoba mająca fizyczny dostęp do urządzenia ma wiele możliwości, aby spróbować przejrzeć lub skopiować przechowywane na nim informacje. Atakujący może również dodać do urządzenia złośliwe oprogramowanie, które umożliwi mu dostęp do danych wprowadzonych do urządzenia, takich jak hasła użytkowników wpisywane na klawiaturze laptopa.

Zezwolenie telepracownikom na zdalny dostęp do zasobów obliczeniowych organizacji lub na lokalny dostęp do jej sieci daje napastnikom dodatkowe możliwości naruszenia bezpieczeństwa organizacji. Gdy urządzenie klienckie korzysta ze zdalnego dostępu lub ma dostęp do sieci lokalnej, jest ono w istocie rozszerzeniem sieci własnej organizacji. Jeżeli urządzenie nie jest odpowiednio zabezpieczone, stwarza dodatkowe ryzyko nie tylko dla informacji, do których telepracownik ma dostęp, ale również dla innych systemów i sieci organizacji. Dlatego też, urządzenia klienckie powinny być odpowiednio zabezpieczone i regularnie konserwowane.

Ogólnie rzecz biorąc, urządzenia klienckie do telepracy powinny posiadać te same lokalne mechanizmy zabezpieczeń, co inne urządzenia klienckie w organizacji - system operacyjny i aktualizacje bezpieczeństwa aplikacji, wyłączenie niepotrzebnych usług itp. Jednakże, ze względu na zagrożenia, na jakie narażone są urządzenia klienckie w środowiskach zewnętrznych, zalecane są dodatkowe zabezpieczenia, a niektóre z nich mogą wymagać dostosowania do efektywnego działania w środowiskach telepracy. Na przykład, przechowywanie wrażliwych danych na komputerze stacjonarnym w siedzibie organizacji ma inne konsekwencje niż przechowywanie tych samych danych na laptopie używanym w kilku lokalizacjach zewnętrznych. W rozdziale omówiono zalecenia dotyczące zabezpieczania urządzeń klienckich do telepracy oraz danych, które się na nich znajdują.

Jeśli zastosowanie dodatkowych zabezpieczeń na urządzeniach do telepracy jest niemożliwe do wykonania lub wyegzekwowania, lepszym rozwiązaniem może być zastosowanie innych metod, takich jak zapewnienie bezpiecznego środowiska lokalnego do telepracy z wykorzystaniem technologii VDI lub VMI, udostępnienie pracownikom nośników wymiennych, za pomocą których mogą oni uruchamiać komputer do telepracy

w bezpiecznym środowisku zdalnego dostępu i telepracy, lub zastosowanie rozwiązań do zarządzania urządzeniami mobilnymi (MDM) i aplikacjami mobilnymi (MAM) w celu poprawy i egzekwowania bezpieczeństwa urządzeń mobilnych.

Organizacje powinny być odpowiedzialne za zabezpieczenie własnych urządzeń klienckich do telepracy, a także powinny wymagać od swoich użytkowników lub organizacji użytkowników niebędących pracownikami wdrożenia i utrzymania odpowiedniego, często podobnego, poziomu bezpieczeństwa dla urządzeń klienckich niebędących własnością organizacji, z których korzystają w telepracy. Mechanizmy zabezpieczenia urządzeń należących do organizacji i innych urządzeń klienckich telepracy są podobne, ale niektóre z zabezpieczeń mogą być niewykonalne do wdrożenia przez telepracowników we własnym zakresie. Aby zapoznać się z zaleceniami dla użytkowników zabezpieczających urządzenia klienckie telepracy BYOD patrz NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [23]. Rozdział 5 zawiera dodatkowe omówienie w zakresie ustanawiania i utrzymywania bezpieczeństwa.

## 4.1. Zabezpieczanie komputerów do telepracy

Jednym z najważniejszych zabezpieczeń komputera do telepracy jest prawidłowo skonfigurowana i włączona zapora sieciowa. Osobiste zapory sieciowe są niezbędne do ochrony przed zagrożeniami sieciowymi w wielu środowiskach. Jeśli osobista zapora sieciowa ma jedną politykę dla wszystkich środowisk, to może być zbyt restrykcyjna w niektórych sytuacjach, np. w sieci wewnętrznej organizacji, a niewystarczająco restrykcyjna w innych, np. w zewnętrznej sieci bezprzewodowej innej firmy. Dlatego osobiste zapory sieciowe obsługujące wiele polityk powinny być używane zawsze, gdy jest to możliwe i odpowiednio skonfigurowane co najmniej dla środowiska korporacyjnego i zewnętrznego.[24]

[23] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

[24] Więcej informacji na temat osobistych zapór sieciowych można znaleźć w dokumencie NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* (http://dx.doi.org/10.6028/NIST.SP.800-41r1).

Wiele zapór sieciowych wymaga od użytkownika ręcznego wybrania z listy odpowiedniej polityki lub środowiska, ale niektóre zapory osobiste można skonfigurować tak, aby automatycznie wykrywały sieć, w której się znajdują i na podstawie tych informacji wybierały politykę bezpieczeństwa. Chociaż automatyczne wykrywanie pomaga zautomatyzować proces zabezpieczeń, nie zawsze działa poprawnie i może czasami zastosować niewłaściwą politykę, czyniąc komputer niezabezpieczonym lub blokując potrzebne funkcje. Dlatego organizacje, które chcą korzystać z funkcji automatycznego wykrywania, powinny je dokładnie przetestować, zanim zaczną na nich polegać, a także poinformować użytkowników o sposobie ich działania oraz o tym, jak użytkownicy mogą je zmienić w przypadku wybrania niewłaściwej polityki. Funkcje autodetekcji powinny być stosowane tylko wtedy, gdy informują telepracownika, w jakim środowisku według nich się znajduje, tak aby użytkownik mógł je zmienić, jeżeli funkcja autodetekcji błędnie zidentyfikowała środowisko.

Kolejnym ważnym aspektem w przypadku komputerów do telepracy jest stosowanie aktualizacji zabezpieczeń systemu operacyjnego i aplikacji.[25] W przypadku komputerów do telepracy, które są zabezpieczone przez użytkowników, polega to na skonfigurowaniu systemu operacyjnego i aplikacji w taki sposób, aby automatycznie kontaktowały się z serwisami internetowymi dostawców w celu sprawdzenia dostępności aktualizacji, pobrania i zainstalowania ich. Określenie sposobu konfigurowania innych komputerów do telepracy (kontrolowanych przez organizację lub jej kontrahentów, partnerów biznesowych, dostawców, itp.) do pobierania aktualizacji może być znacznie bardziej skomplikowane. Organizacja może chcieć korzystać ze scentralizowanego systemu zarządzania poprawkami dla wszystkich swoich komputerów, ale jeśli komputery telepracy polegają na takim systemie, mogą nie otrzymywać szybko aktualizacji, jeśli są skonfigurowane do pobierania

[25] Ogólnie rzecz biorąc, najważniejsze aplikacje, które należy aktualizować, to te, które są wykorzystywane do zapewnienia bezpieczeństwa (np. oprogramowanie antymalware, osobiste zapory sieciowe) lub zdalnego dostępu, oraz te, które są przystosowane do pracy w sieci i stanowią częsty wektor exploitów, takie jak przeglądarki internetowe, klienci poczty elektronicznej i klienci komunikatorów internetowych.

aktualizacji tylko ze scentralizowanego systemu zarządzania poprawkami organizacji.[26] Na przykład, użytkownik może podłączyć komputer telepracy do sieci zewnętrznej, ale nie ustanowić połączenia zdalnego dostępu do własnej organizacji. Komputer może być narażony na zagrożenia, które mogą wykorzystać jego niezałatane luki, a poprawki będą dostępne dopiero po nawiązaniu sesji zdalnego dostępu do własnej organizacji. Innym potencjalnym problemem związanym z aktualizacją oprogramowania jest fakt, że sesje zdalnego dostępu mogą być krótkie, szczególnie jeśli telepracownik jest w podróży. Może to uniemożliwić pobranie większych aktualizacji, jeżeli oprogramowanie przeprowadzające aktualizacje nie pozwala na pobieranie aktualizacji w częściach.

Organizacje powinny dokładnie rozważyć te kwestie podczas planowania sposobu, w jaki komputery do telepracy będą na bieżąco aktualizowane w zakresie systemu operacyjnego i aplikacji. Organizacje powinny również zachęcać użytkowników do pełnego aktualizowania komputerów do telepracy przed wyjazdem w podróż lub do innych niekontrolowanych środowisk, w których prawdopodobieństwo pojawienia się nowych zagrożeń jest większe niż w sieciach domowych.

Inne środki bezpieczeństwa, które są szczególnie ważne w przypadku telepracy, obejmują następujące elementy:

- Dla każdej osoby, która będzie korzystała z komputera do telepracy, należy założyć osobne konto użytkownika z ograniczonymi uprawnieniami. Telepracownicy powinni używać kont z ograniczonymi uprawnieniami do zwykłej pracy, a oddzielne konto administracyjne tylko do zadań wymagających dostępu na poziomie administratora, takich jak aktualizacje oprogramowania. Zmniejsza to prawdopodobieństwo uzyskania przez napastnika dostępu do komputera na poziomie administratora.

[26] Więcej informacji na temat zarządzania poprawkami można znaleźć w dokumencie NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies (http://dx.doi.org/10.6028/NIST.SP.800-40r3).

- Wymuszenie *blokady sesji*, która uniemożliwia dostęp do komputera po pewnym czasie bezczynności (np. 15 minut) lub pozwala użytkownikowi na zablokowanie sesji na żądanie. Po zablokowaniu sesji dostęp do komputera można przywrócić tylko poprzez uwierzytelnienie. Blokada sesji jest często częścią oprogramowania wygaszacza ekranu. Zapobiega to łatwemu uzyskaniu dostępu do bieżącej sesji przez napastnika znajdującego się w fizycznej bliskości komputera. Nie udaremnia to jednak atakującemu, który kradnie komputer lub ma do niego dostęp przez dłuższy czas, albowiem blokadę sesji można obejść za pomocą różnych technik.
- Zabezpieczenie fizycznie komputery do telepracy, stosując linki zabezpieczające (np. kensington lock) lub inne środki zapobiegające kradzieży. Jest to szczególnie ważne w przypadku komputerów do telepracy w niezaufanych środowiskach zewnętrznych. W takich środowiskach należy również wyłączać komputer, jeżeli ma on pozostać bez nadzoru (więcej informacji na ten temat znajduje się w rozdziale 4.3.1).

W przypadkach, gdy organizacje obawiają się ryzyka związanego z nieodpowiednim zabezpieczeniem komputerów do telepracy, szczególnie tych, które nie są kontrolowane przez organizację lub są w inny sposób narażone na większe ryzyko kompromitacji, organizacje mogą rozważyć zastosowanie innych zabezpieczeń oprócz lub zamiast tych opisanych powyżej.

Na przykład, niektórzy producenci oferują rozwiązania, które zapewniają rozruchowy system operacyjny na nośniku wymiennym tylko do odczytu z prekonfigurowanym oprogramowaniem klienta zdalnego dostępu. Użytkownik może włożyć taki nośnik do komputera i uruchomić go. W ten sposób omija system operacyjny komputera, który może być zagrożony i ładuje zaufany system operacyjny oraz oprogramowanie klienta zdalnego dostępu z nośnika wymiennego. Umożliwienie rozruchu komputera z nośnika zewnętrznego rodzi jednak ryzyko, że sprawca kradzieży może uruchomić własny system operacyjny i uzyskać dostęp do danych na dysku twardym komputera. Zatem system należy

skonfigurować w taki sposób, aby uniemożliwić użytkownikom przechowywanie plików na lokalnym dysku twardym, zapisywanie plików na nośnikach wymiennych oraz przenoszenie w inny sposób informacji ze znanego systemu operacyjnego do innej lokalizacji. Rozwiązania z systemem operacyjnym uruchamianym z nośnika wymiennego sprawiają, że bezpieczeństwo logiczne komputera do telepracy jest znacznie mniej istotne dla bezpieczeństwa informacji organizacji, chociaż nie zapobiegają one wszystkim zagrożeniom (np. luki w systemie operacyjnym nośnika wymiennego mogą zostać wykorzystane lub złośliwy kod może być obecny w BIOS-ie, firmware lub sprzęcie komputera). Innym problemem związanym z tymi rozwiązaniami jest fakt, że wymagają one, aby komputer obsługiwał uruchamianie z nośnika wymiennego przed dyskiem twardym, co może wymagać zmiany konfiguracji ustawień systemu BIOS komputera.

Inną opcją jest dostarczenie telepracownikom pamięci flash, które są specjalnie skonfigurowane do pracy w systemie telepracy. Na takich dyskach przechowywane są zatwierdzone przez organizację aplikacje, które są uruchamiane w części dysków przeznaczonej tylko do odczytu, co chroni je przed nieautoryzowaną modyfikacją. Pliki tymczasowe z tych aplikacji są przechowywane w innej części pamięci flash, co zmniejsza prawdopodobieństwo wycieku danych na komputer.

## 4.2. Zabezpieczanie urządzeń mobilnych do telepracy

Wiele urządzeń mobilnych do telepracy może mieć centralnie zarządzane zabezpieczenia poprzez oprogramowanie do zarządzania urządzeniami mobilnymi w organizacji. Organizacje powinny korzystać z takich możliwości zarządzania bezpieczeństwem, szczególnie w przypadku urządzeń kontrolowanych przez organizację - na przykład ograniczając instalację i korzystanie z aplikacji firm trzecich lub udostępniając sklep z autoryzowanymi, zweryfikowanymi aplikacjami i zezwalając na pobieranie i instalowanie aplikacji tylko z tego

sklepu.[27] Wiele urządzeń będzie jednak wymagało ręcznego zabezpieczenia. Możliwości zabezpieczeń i odpowiednie działania różnią się w zależności od typu urządzenia i konkretnego produktu, dlatego organizacje powinny zapewnić wytyczne dla administratorów urządzeń i użytkowników, którzy są odpowiedzialni za zabezpieczenie urządzeń mobilnych do telepracy, w jaki sposób powinni je zabezpieczyć.

NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, [28]zaleca zabezpieczenia dla najczęściej spotykanych typów urządzeń mobilnych wykorzystywanych w telepracy. Poniżej przedstawiono przykłady tych zabezpieczeń:

- Ograniczaj możliwości sieciowe urządzeń mobilnych. Jest to szczególnie ważne w przypadku urządzeń, które posiadają wiele funkcji bezprzewodowych. Telepracownik może nawet nie wiedzieć, że niektóre protokoły bezprzewodowe, takie jak Bluetooth i współdzielona sieć bezprzewodowa, narażają urządzenie na dostęp osób atakujących. Czasami konieczne jest jednoczesne zezwolenie na korzystanie z wielu funkcji sieciowych, np. zezwolenie na dostęp funkcji głosowej urządzenia mobilnego w tym samym czasie co dostęp do Wi-Fi.
- W przypadku urządzeń, które są narażone na poważne zagrożenia ze strony złośliwego oprogramowania, należy uruchomić programy antymalware. Urządzenia, które łączą się z Internetem mogą mieć nawet osobiste zapory sieciowe. Należy je włączyć, aby zapobiec atakom i nieautoryzowanemu dostępowi. Niezbędne jest ustalenie, czy producent urządzenia dostarcza aktualizacje i poprawki. Jeśli tak, należy się upewnić, że są one niezwłocznie stosowane w celu ochrony urządzenia przed atakami wykorzystującymi znane luki w zabezpieczeniach.
- Wskazane jest silne szyfrowanie przechowywanych danych zarówno na wbudowanej pamięci masowej, jak i na nośnikach wymiennych.

[27] Więcej informacji na temat sprawdzania aplikacji mobilnych można znaleźć w dokumencie NIST SP 800-163, Vetting the Security of Mobile Applications (http://dx.doi.org/10.6028/NIST.SP.800-163).
[28] http://dx.doi.org/10.6028/NIST.SP.800-124r1

- Należy wymagać podania hasła/kodu dostępu i/lub innego sposobu uwierzytelniania przed uzyskaniem dostępu do zasobów organizacji.
- Należy stosować możliwość instalacji aplikacji poprzez ich białą lub czarną listę.[29]

Biorąc pod uwagę podobieństwo funkcji urządzeń mobilnych, szczególnie w miarę jak stają się one coraz bardziej zaawansowane i komputerów PC, organizacje powinny zdecydowanie rozważyć traktowanie ich podobnie lub tak samo jak komputery PC. Oznacza to, że polityki organizacyjne dotyczące komputerów PC mogą być po prostu rozszerzone na urządzenia mobilne. Jeśli te dwie polityki są utrzymywane oddzielnie, dokumenty ich dotyczące powinny w dużym stopniu odnosić się do siebie nawzajem.

Organizacje powinny rozważyć skorzystanie z rozwiązań do zarządzania urządzeniami mobilnymi (MDM), rozwiązań do zarządzania aplikacjami mobilnymi (MAM) oraz innych technologii do kontroli korzystania z urządzeń mobilnych. Rozwiązania MDM są w stanie egzekwować różne polityki bezpieczeństwa w imieniu organizacji, nawet do pewnego stopnia na urządzeniach mobilnych, które nie są kontrolowane przez organizację. Na przykład, oprogramowanie MDM jest często używane do wymagania użycia kodu PIN w celu odblokowania urządzenia mobilnego, do włączenia technologii szyfrowania w celu ochrony wrażliwych danych przechowywanych na urządzeniu mobilnym oraz do określenia, czy urządzenie mobilne zostało poddane jailbroken lub rootowaniu. Oprogramowanie MDM może być również wykorzystywane do zdalnego wymazywania danych w przypadku zgubienia lub kradzieży urządzenia mobilnego, aby zapobiec nieautoryzowanemu dostępowi do zawartych na nim danych wrażliwych. Organizacja może ustawić różne polityki MDM dla każdej kategorii urządzeń mobilnych, takich jak urządzenia wydawane przez organizację, kontrolowane przez strony trzecie i BYOD, aby uwzględnić różne poziomy dostępu. Oprogramowanie MAM zapewnia środowisko, które izoluje aplikacje i dane organizacji od reszty urządzenia. Może być wymagane silne uwierzytelnienie do uzyskania dostępu do

[29] Więcej informacji na temat whitelistingu aplikacji można znaleźć w dokumencie NIST SP 800-167, *Guide to Application Whitelisting* (http://dx.doi.org/10.6028/NIST.SP.800-167).

środowiska korporacyjnego, które jest również szyfrowane w celu ochrony wrażliwych danych i aplikacji organizacji oraz w celu zminimalizowania wycieku danych z tych aplikacji do innych aplikacji i usług działających na urządzeniu. W przypadku utraty urządzenia lub odejścia pracownika z organizacji, chronione środowisko może zostać zdalnie wymazane w celu usunięcia danych organizacji.

Oprócz lub zamiast rozwiązań MDM/MAM, organizacje mogą polegać na rozwiązaniach NAC, które zostały omówione w sekcjach 2 i 3 niniejszego dokumentu. Rozwiązania NAC mogą zidentyfikować urządzenia mobilne typu jailbroken lub rooted oraz inne poważne naruszenia zasad bezpieczeństwa na urządzeniach mobilnych próbujących połączyć się z sieciami organizacji.

## 4.3. Ochrona danych na urządzeniach klienckich telepracy

Telepraca często wiąże się z tworzeniem i edytowaniem informacji związanych z pracą, takich jak poczta elektroniczna, dokumenty w edytorze tekstu i arkusze kalkulacyjne. Ponieważ dane te są ważne, powinny być traktowane jak inne ważne aktywa organizacji. Dwie rzeczy, które organizacja może zrobić w celu ochrony danych na urządzeniach do telepracy to zabezpieczenie ich na urządzeniu do telepracy oraz okresowe tworzenie kopii zapasowych w miejscu kontrolowanym przez organizację. Więcej informacji na ten temat znajduje się w punktach 4.3.1 do 4.3.3. Organizacje mogą również zrezygnować z przechowywania informacji na urządzeniach do telepracy i zamiast tego przechowywać je centralnie w organizacji.

Informacje wrażliwe, takie jak niektóre rodzaje danych osobowych (PII) (np. dane osobowe, medyczne, finansowe), które są przechowywane lub przesyłane do lub z urządzeń telepracy, powinny być chronione tak, aby złośliwe strony nie mogły uzyskać do nich dostępu lub ich zmienić. Na przykład, telepracownicy często zapominają, o tym, że przechowywane są poufne informacje na płycie CD, która jest przenoszona wraz z urządzeniem, lub drukują informacje na publicznej drukarce, co powoduje, że może również ujawnić informacje, do którego nie doszłoby w środowisku korporacyjnym. Nieautoryzowane ujawnienie poufnych

informacji może naruszyć zaufanie opinii publicznej do organizacji, zagrozić jej misji lub zaszkodzić osobom, których dane osobowe zostały ujawnione.

### 4.3.1. Szyfrowanie danych w stanie spoczynku

Wszystkie urządzenia do telepracy, niezależnie od ich wielkości i lokalizacji, mogą zostać skradzione. Niektórzy złodzieje mogą chcieć odczytać zawartość danych znajdujących się na urządzeniu, a nawet wykorzystać je do celów przestępczych. Aby temu zapobiec, organizacja powinna posiadać politykę szyfrowania wszystkich wrażliwych danych, gdy znajdują się one w stanie spoczynku na urządzeniu oraz na nośnikach wymiennych używanych przez to urządzenie. Tworzenie i stosowanie kluczy kryptograficznych do szyfrowania zdalnych danych w stanie spoczynku powinno odbywać się zgodnie z tymi samymi zasadami, które organizacja stosuje w odniesieniu do innych kluczy chroniących dane w stanie spoczynku.[30]

Istnieje wiele metod ochrony danych w stanie spoczynku i zależą one głównie od typu urządzenia lub nośnika wymiennego, który ma być chroniony. Większość systemów operacyjnych ma własne mechanizmy szyfrowania danych, a ponadto istnieje wiele aplikacji innych firm niż producent systemu operacyjnego, które zapewniają podobne możliwości.[31] Generalnie, gdy do ochrony danych na komputerach PC stosowane są technologie takie jak pełne szyfrowanie dysków Telepracownicy powinni wyłączać swoje urządzenia do telepracy zamiast przełączać je w tryb uśpienia, gdy nie będą one używane przez dłuższy czas lub gdy telepracownik nie będzie przebywał z urządzeniem. Pomaga to zapewnić, że dane w stanie spoczynku i klucz deszyfrujący są chronione przez technologię szyfrowania pamięci masowej.

[30] Więcej informacji na temat stosowania kluczy kryptograficznych można znaleźć w dokumencie NIST SP 800-57 (Części 1-3), *Zalecenia dotyczące zarządzania kluczami* (http://csrc.nist.gov/publications/PubsSPs.html#800-57pt1).

[31] Więcej informacji na temat szyfrowania pamięci masowej na urządzeniach klienckich i nośnikach wymiennych można znaleźć w dokumencie NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices. (http://dx.doi.org/10.6028/NIST.SP.800-111).

### 4.3.2. Korzystanie z maszyn wirtualnych

Jeżeli organizacja ma bezpośrednią kontrolę nad urządzeniem do telepracy, może egzekwować swoje polityki dotyczące zdalnego dostępu, aktualizacji itp. W przypadku innych urządzeń do telepracy, takich jak komputery BYOD, organizacja ma ograniczone możliwości egzekwowania polityk bezpieczeństwa. Metodą kontrolowania środowiska, w którym pracuje telepracownik jest uruchomienie maszyny wirtualnej (VM) na komputerze telepracownika. Zazwyczaj odbywa się to poprzez uruchomienie programu *hypervisor VM* w systemie operacyjnym telepracownika, ale niektóre nowsze rozwiązania pozwalają na instalację hiperwizora, który działa zamiast systemu operacyjnego komputera. Jest to tzw. *hypervisor bare-metal*. Hiperwizory typu bare-metal są generalnie uważane za bezpieczniejsze od innych hiperwizorów, ponieważ jest o jeden element oprogramowania mniej, który może zostać zaatakowany.[32]

Użytkownik uruchamia *obraz maszyny wirtualnej* w środowisku maszyny wirtualnej; obraz ten zachowuje się jak pełnowartościowy komputer z systemem operacyjnym i oprogramowaniem aplikacyjnym. Wykorzystanie maszyn wirtualnych jako urządzeń do telepracy jest rozszerzeniem koncepcji cienkich klientów. Aby wykorzystać obrazy maszyn wirtualnych do egzekwowania polityki telepracy, organizacja dystrybuuje obraz maszyny wirtualnej, który jest skonfigurowany tak, aby był w pełni zgodny ze wszystkimi odpowiednimi politykami bezpieczeństwa. Telepracownik uruchamia obraz maszyny wirtualnej na swoim komputerze. Gdy obraz wymaga aktualizacji, organizacja dystrybuuje nowy obraz do swoich telepracowników. Użycie maszyny wirtualnej do zabezpieczenia telepracy działa dobrze tak długo, jak długo sam komputer telepracownika nie posiada złośliwego oprogramowania, które mogłoby zaatakować maszynę wirtualną. W przypadku hypervisorów, które działają wewnątrz systemu operacyjnego hosta (nie są to hypervisory

[32] Więcej informacji na temat hypervisorów można znaleźć w dokumencie NIST SP 800-125, *Guide to Security for Full Virtualization Technologies.* (http://dx.doi.org/10.6028/NIST.SP.800-125).

bare-metal), jakikolwiek kompromitacja w systemie operacyjnym hosta może wpłynąć na bezpieczeństwo maszyny wirtualnej i jej obrazu.

Dyski maszyn wirtualnych zachowują się tak samo jak dyski w zwykłych komputerach, więc organizacje powinny posiadać polityki dla danych przechowywanych w obrazach maszyn wirtualnych. Obrazy maszyn wirtualnych mogą być zaszyfrowane na komputerze telepracy, gdy nie są używane i odszyfrowane dopiero po podaniu przez użytkownika odpowiedniego uwierzytelnienia przed uruchomieniem obrazu. Jeżeli obrazy maszyn wirtualnych są zaszyfrowane, osoba nieupoważniona, która uzyska dostęp do urządzenia telepracy, nie będzie w stanie odczytać danych przechowywanych w obrazie maszyny wirtualnej. Podobnie, obraz maszyny wirtualnej może zawierać wiele dysków, a niektóre z nich mogą być zaszyfrowane. Jeżeli telepracownik przechowuje swoje dane na zaszyfrowanym dysku w maszynie wirtualnej, będzie to wyglądało tak samo, jakby dane były przechowywane na zaszyfrowanym dysku bezpośrednio na komputerze telepracownika.

Aby zmniejszyć ryzyko kompromitacji organizacje powinny rozważyć zaszyfrowanie wszystkich obrazów maszyn wirtualnych używanych do telepracy,. Może to być osiągnięte poprzez zastosowanie pełnego szyfrowania dysku, szyfrowania plików lub innych środków.[33] W sytuacjach wysokiego ryzyka, szczególnie w przypadku dostępu do bardzo wrażliwych informacji, organizacje powinny szyfrować każdy pojedynczy obraz maszyny wirtualnej wykorzystywany do telepracy, a także mogą zapewnić drugą warstwę ochrony poprzez pełne szyfrowanie dysku.

### 4.3.3. Tworzenie kopii zapasowych danych na urządzeniach telepracy

Większość organizacji posiada politykę regularnego tworzenia kopii zapasowych danych. Taka polityka powinna obejmować dane na komputerach i urządzeniach mobilnych telepracowników. Polityka taka może jednak wymagać odmiennych zapisów dla kopii

[33] Opcje te wyjaśnia dokument NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, (http://dx.doi.org/10.6028/NIST.SP.800-111).

zapasowych wykonywanych w siedzibie organizacji w porównaniu z lokalizacjami zewnętrznymi. Jeżeli dane, które mają być backupowane, zawierają informacje wrażliwe lub z innych powodów wymagają ochrony ich poufności, istnieją dodatkowe aspekty bezpieczeństwa, jeżeli kopia zapasowa jest wykonywana w lokalizacji zewnętrznej.

Jeżeli kopia zapasowa danych jest tworzona zdalnie - z urządzenia telepracowniczego do systemu w organizacji - to komunikacja przenosząca te dane powinna być zaszyfrowana i mieć zweryfikowaną integralność. Powyższy zakres szczegółowo omówiono w punkcie 3.3.3. Jeżeli kopia zapasowa danych jest tworzona lokalnie na nośnikach wymiennych, takich jak płyty CD lub pendrive'y, kopia ta powinna być chroniona co najmniej tak dobrze, jak dane oryginalne. Na przykład, jeżeli oryginalne dane są zaszyfrowane, dane w kopii zapasowej również powinny być zaszyfrowane. Jeśli oryginalne dane są zaszyfrowane w formie przenośnej, np. poprzez szyfrowanie dysku wirtualnego lub zaszyfrowany obraz maszyny wirtualnej, wystarczające może być skopiowanie zaszyfrowanej jednostki na nośnik kopii zapasowej. Jednak w przypadku nieprzenośnych form szyfrowania pamięci masowej, takich jak pełne szyfrowanie dysku, dane musiałyby zostać odszyfrowane na urządzeniu telepracy, a następnie zaszyfrowane w celu zapisania na nośniku zapasowym.

## 4.4. Podsumowanie kluczowych zaleceń

Poniższa lista przedstawia niektóre z kluczowych rekomendacji zawartych w tej części dokumentu.

- Urządzenia klienckie do telepracy powinny być odpowiednio zabezpieczone i regularnie konserwowane. Ogólnie rzecz biorąc, urządzenia klienckie do telepracy powinny posiadać takie same lokalne mechanizmy zabezpieczeń jak inne urządzenia klienckie w organizacji. Jednak ze względu na zagrożenia, na jakie narażone są urządzenia klienckie w środowiskach zewnętrznych, zalecane jest stosowanie dodatkowych zabezpieczeń, a niektóre zabezpieczenia mogą wymagać dostosowania do efektywnego działania w środowisku telepracy. Jeżeli zastosowanie dodatkowych środków bezpieczeństwa nie jest wykonalne lub możliwe do wyegzekwowania,

lepszym rozwiązaniem może być zastosowanie innych metod, takich jak wykorzystanie technologii VDI, VMI lub wymiennych nośników startowych w celu stworzenia bezpiecznego środowiska lub przyjęcie rozwiązań MDM w celu zwiększenia i egzekwowania bezpieczeństwa urządzeń mobilnych. (Patrz wprowadzenie do sekcji 4)

- W przypadku komputerów osobistych do telepracy należy w miarę możliwości stosować osobiste zapory sieciowe zdolne do obsługi wielu polityk, skonfigurowane prawidłowo przynajmniej dla środowiska przedsiębiorstwa i środowiska zewnętrznego. (Sekcja 4.1)
- W przypadku urządzeń mobilnych przeznaczonych do telepracy, organizacje powinny korzystać z możliwości scentralizowanego zarządzania bezpieczeństwem, jeśli tylko są one dostępne. Jednakże, wiele urządzeń będzie musiało być zabezpieczonych ręcznie. Organizacje powinny zapewnić wytyczne dla administratorów urządzeń i użytkowników, którzy są odpowiedzialni za zabezpieczenie urządzeń mobilnych do telepracy, w jaki sposób powinni je zabezpieczyć. (Sekcja 4.2)
- Informacje wrażliwe, takie jak niektóre rodzaje PII (np. dokumentacja personalna, medyczna, finansowa), które są przechowywane lub wysyłane do lub z urządzeń do telepracy, powinny być chronione tak, aby złośliwe strony nie miały do nich dostępu lub nie mogły ich zmienić. Organizacja powinna posiadać politykę szyfrowania wszystkich wrażliwych danych, gdy znajdują się one w stanie spoczynku na urządzeniu oraz na nośnikach wymiennych używanych przez to urządzenie. Tworzenie i używanie kluczy kryptograficznych do szyfrowania zdalnych danych w stanie spoczynku powinno odbywać się zgodnie z tymi samymi zasadami, które organizacja stosuje dla innych kluczy chroniących dane w stanie spoczynku. (Sekcja 4.3)

# 5. UWAGI DOTYCZĄCE BEZPIECZEŃSTWA W CYKLU ŻYCIA TELEPRACY I DOSTĘPU ZDALNEGO

W tym rozdziale zebrano koncepcje przedstawione w poprzednich częściach przewodnika i wyjaśniono, w jaki sposób powinny być one uwzględniane w całym cyklu życia rozwiązań telepracy i zdalnego dostępu, od polityki po działania operacyjne. W rozdziale tym przedstawiono pięciofazowy model cyklu życia, który ma pomóc organizacjom w określeniu, w którym momencie rekomendacja wdrożenia rozwiązań telepracy i zdalnego dostępu może być istotna. Model ten jest oparty na modelu wprowadzonym w NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*.[34] Organizacje mogą stosować metodykę zarządzania projektami lub model cyklu życia, który nie odwzorowuje bezpośrednio faz w przedstawionym tu modelu, ale rodzaje zadań w metodyce i ich sekwencjonowanie są prawdopodobnie podobne. Fazy cyklu życia są następujące:

- **Faza 1: Inicjacja.** Faza ta obejmuje zadania, które organizacja powinna wykonać przed przystąpieniem do projektowania rozwiązania telepracy lub zdalnego dostępu. Obejmują one identyfikację potrzeb w zakresie telepracy i zdalnego dostępu (w tym ewentualne wsparcie dla urządzeń BYOD i/lub urządzeń kontrolowanych przez strony trzecie), przedstawienie ogólnej wizji tego, w jaki sposób rozwiązania telepracy i zdalnego dostępu będą wspierać misję organizacji, stworzenie wysokopoziomowej strategii wdrażania rozwiązań telepracy i zdalnego dostępu, opracowanie polityki bezpieczeństwa telepracy oraz określenie wymagań biznesowych i funkcjonalnych dla tego rozwiązania.
- **Faza 2: Rozwój.** W tej fazie personel określa charakterystykę techniczną rozwiązania telepracy lub zdalnego dostępu oraz powiązanych komponentów. Obejmuje to metody uwierzytelniania, mechanizmy kryptograficzne wykorzystywane do ochrony komunikacji oraz zapory sieciowe i inne mechanizmy wykorzystywane do kontroli

[34] http://dx.doi.org/10.6028/NIST.SP.800-64r2

dostępu do sieci i zasobów w tych sieciach. Należy również rozważyć typy klientów telepracy, które mogą mieć wpływ na pożądane polityki. Należy zadbać o to, aby polityka bezpieczeństwa telepracy mogła być stosowana i egzekwowana przez wszystkich klientów. Na końcu tej fazy następuje zakup komponentów rozwiązania.

- **Faza 3: Wdrożenie.** W tej fazie konfigurowany jest sprzęt w celu spełnienia wymagań operacyjnych i bezpieczeństwa, w tym polityki bezpieczeństwa telepracy udokumentowanej w planie bezpieczeństwa systemu, instalowany i testowany jako prototyp, a następnie aktywowany w sieci produkcyjnej. Wdrożenie obejmuje zmianę konfiguracji innych zabezpieczeń i technologii, takich jak rejestrowanie zdarzeń bezpieczeństwa, zarządzanie siecią i integracja z serwerami uwierzytelniającymi.
- **Faza 4: Eksploatacja i utrzymanie.** Ta faza obejmuje zadania związane z bezpieczeństwem, które organizacja powinna wykonywać na bieżąco po uruchomieniu rozwiązania telepracy lub zdalnego dostępu, w tym przegląd logów, wykrywanie ataków, reagowanie na incydenty i odzyskiwanie danych. Zadania te powinny być udokumentowane w polityce zarządzania konfiguracją.
- **Faza 5: Utylizacja.** Ta faza obejmuje zadania, które pojawiają się, gdy rozwiązanie zdalnego dostępu lub jego komponenty są wycofywane, w tym zachowanie informacji w celu spełnienia wymagań prawnych, sanityzację nośników i prawidłową utylizację sprzętu.[35]

Ta sekcja przedstawia aspekty bezpieczeństwa, które są szczególnie istotne dla rozwiązań telepracy i zdalnego dostępu. Rozważania te nie mają charakteru wyczerpującego, ani nie sugerują, że elementy bezpieczeństwa niewymienione tutaj są nieważne lub niepotrzebne.

[35] Informacje o cyklu życia przedstawione w niniejszym wprowadzeniu pochodzą z Sekcji 8 publikacji NIST SP 800-97, *Establishing Wireless Robust Security Networks: a Guide to IEEE 802.11i* (http://dx.doi.org/10.6028/NIST.SP.800-97).

## 5.1. Inicjacja

Faza inicjacji obejmuje wiele działań przygotowawczych, takich jak identyfikacja obecnych i przyszłych potrzeb oraz określenie wymagań dotyczących wydajności, funkcjonalności i bezpieczeństwa. Krytyczną częścią fazy inicjacji jest opracowanie polityki bezpieczeństwa telepracy dla organizacji. W rozdziale tym wymieniono elementy, które powinna zawierać polityka bezpieczeństwa telepracy oraz, tam gdzie jest to istotne, opisano czynniki, które powinny być brane pod uwagę przy podejmowaniu decyzji dotyczących każdego z elementów. Polityka bezpieczeństwa telepracy powinna definiować, jakie formy zdalnego dostępu są dozwolone w organizacji, jakie typy urządzeń do telepracy (np. komputery i urządzenia mobilne kontrolowane przez organizację, urządzenia mobilne BYOD, komputery kontrolowane przez podwykonawców) są dozwolone do korzystania z jakiej formy zdalnego dostępu, jaki typ dostępu jest przyznawany każdemu typowi telepracownika oraz jak powinno być prowadzone zakładanie kont użytkowników. Powinna ona również obejmować sposób administrowania serwerami zdalnego dostępu oraz sposób aktualizacji polityk na tych serwerach. Polityka bezpieczeństwa telepracy powinna być udokumentowana w planie bezpieczeństwa systemu.

Oprócz opisanych w tej części rozważań dotyczących polityk bezpieczeństwa telepracy, organizacje powinny również rozważyć, w jaki sposób telepraca może wpłynąć na inne polityki bezpieczeństwa. Na przykład, organizacja może wymagać, aby niektóre rodzaje zablokowanych kont użytkowników były odblokowywane tylko osobiście, ale może to być niewykonalne dla telepracowników, którzy są w podróży lub wykonują długoterminowe zadania w lokalizacjach zewnętrznych. Inne zasady bezpieczeństwa powinny być dostosowane do potrzeb telepracy.

### 5.1.1. Dozwolone formy zdalnego dostępu

Jedną z pierwszych decyzji, jaką należy podjąć tworząc politykę bezpieczeństwa telepracy jest to, jakie typy rozwiązań zdalnego dostępu będą dozwolone. Każdy typ rozwiązania ma

swoje mocne i słabe strony, a użyteczność każdego z nich zależy od wielu czynników wewnątrz organizacji. Niektóre z tych czynników obejmują:

- Istniejący zdalny dostęp używany przez organizację, taki jak systemy zdalnego sterowania używane przez personel IT;
- oprogramowanie już zainstalowane na urządzeniach do telepracy, które może być używane do zdalnego dostępu; oraz
- Możliwości dostępne w zaporach sieciowych, które są już zainstalowane na brzegu sieci organizacji.

Polityka dotycząca rodzajów zdalnego dostępu dozwolonych do telepracy powinna być ściśle powiązana z ogólną polityką bezpieczeństwa organizacji. Jeżeli jedna z rozważanych form zdalnego dostępu nie może być zabezpieczona w sposób wymagany przez politykę bezpieczeństwa organizacji, np. przy użyciu zatwierdzonych algorytmów kryptograficznych do ochrony wrażliwych danych, wówczas ta forma zdalnego dostępu nie powinna być stosowana przez organizację. Przy tworzeniu polityki bezpieczeństwa telepracy priorytetem powinna być ogólna polityka bezpieczeństwa.

### 5.1.2. Ograniczenia dotyczące urządzeń klienckich do telepracy oraz poziomów zdalnego dostępu

Polityka bezpieczeństwa telepracy może ograniczać typy urządzeń klienckich, z których mogą korzystać telepracownicy. Z wielu powodów, w tym z powodu polityki bezpieczeństwa i ograniczeń technologicznych, organizacje często ograniczają typy urządzeń, które mogą być używane do zdalnego dostępu. Na przykład, organizacja może zezwalać na korzystanie wyłącznie z komputerów osobistych kontrolowanych przez organizację. Niektóre organizacje stosują poziomy dostępu, na przykład zezwalając komputerom PC kontrolowanym przez organizację na dostęp do wielu zasobów, komputerom PC BYOD i komputerom PC kontrolowanym przez inne firmy na dostęp do ograniczonego zestawu zasobów, a urządzeniom mobilnym BYOD na dostęp tylko do jednego lub dwóch zasobów, takich jak poczta elektroniczna. Dzięki temu organizacja może ograniczyć ponoszone ryzyko, zezwalając

najbardziej kontrolowanym urządzeniom na największy dostęp, a najmniej kontrolowanym urządzeniom na minimalny dostęp lub całkowity brak dostępu.

Każda organizacja powinna podejmować własne decyzje oparte na szacowaniu ryzyka, dotyczące tego, jakie poziomy zdalnego dostępu powinny być dozwolone z jakich typów urządzeń. Czynniki, które organizacje powinny rozważyć przy ustalaniu polityki bezpieczeństwa telepracy to m.in:

- **Sensowność telepracy.** Niektóre rodzaje telepracy wiążą się z dostępem do poufnych informacji lub zasobów, podczas gdy inne nie. Organizacje mogą wprowadzić bardziej restrykcyjne wymagania dotyczące telepracy związanej z dostępem do poufnych informacji, np. zezwolić na korzystanie tylko z urządzeń kontrolowanych przez organizację.
- **Poziom pewności co do zgodności z polityką bezpieczeństwa.** Spełnienie wielu wymagań bezpieczeństwa organizacji może być zapewnione tylko wtedy, gdy organizacja kontroluje konfigurację urządzeń do telepracy. W przypadku urządzeń niekontrolowanych przez organizację, niektóre wymagania mogą być zweryfikowane przez automatyczne sprawdzanie stanu bezpieczeństwa przeprowadzane przez serwer zdalnego dostępu na urządzeniach próbujących się połączyć, ale inne wymagania nie mogą być zweryfikowane przez organizację w sposób zautomatyzowany. Uświadomienie użytkownikom ich odpowiedzialności może przyczynić się do poprawy bezpieczeństwa na urządzeniach BYOD do telepracy, ale nie spowoduje takiego samego stopnia zgodności z polityką bezpieczeństwa jak obowiązkowe kontrole bezpieczeństwa na urządzeniach kontrolowanych przez organizację. Nawet najbardziej sumienni użytkownicy mogą nie być w stanie utrzymać bezpieczeństwa swoich urządzeń BYOD przez cały czas ze względu na złożoność techniczną, wysiłek związany z ich obsługą lub brak świadomości nowych zagrożeń. W przypadku urządzeń kontrolowanych przez strony trzecie, organizacja

może być w stanie egzekwować zgodność z polityką bezpieczeństwa poprzez zapisy umowne.

- **Koszt.** Koszty związane z urządzeniami do telepracy będą się różnić w zależności od podjętych decyzji. Podstawowym kosztem bezpośrednim jest wydanie telepracownikom urządzeń do telepracy oraz oprogramowania klienckiego. Istnieją również koszty pośrednie związane z utrzymaniem urządzeń do telepracy oraz zapewnieniem wsparcia technicznego dla telepracowników. Organizacja może uzasadnić zakup urządzeń do telepracy dla osób, które pracują regularnie (np. jeden dzień w tygodniu z domu, częste podróże służbowe), ale nie kupuje urządzeń do telepracy dla osób, które pracują sporadycznie i przez krótki czas, np. szybko sprawdzają pocztę elektroniczną z domu kilka razy w miesiącu.
- **Miejsce wykonywania telepracy.** Ryzyko będzie na ogół niższe w przypadku urządzeń używanych tylko w środowisku domowym lub tylko w środowisku przedsiębiorstwa (np. sieć kontrahenta, partnera biznesowego lub dostawcy) niż w przypadku urządzeń używanych w różnych miejscach.
- **Ograniczenia techniczne.** Niektóre typy urządzeń mogą być niezbędne do wykonywania telepracy, np. do lokalnego uruchamiania specjalistycznych programów. Ponadto, jeżeli organizacja posiada jeden typ serwera zdalnego dostępu, a serwer ten umożliwia połączenia tylko poprzez klienta zainstalowanego na urządzeniu telepracy, wówczas dozwolone są tylko te typy urządzeń, które mogą obsługiwać tego klienta.
- **Zgodność z wymogami i innymi politykami.** Organizacje mogą być zobowiązane do przestrzegania wymagań związanych z telepracą, wynikających z i innych powodów. Przykładem takiego wymogu mogą być ograniczenia dotyczące wykonywania telepracy w rejonach, w których występują znane wysokie zagrożenia dla systemów informatycznych.

Chociaż decyzja o tym, jakie typy urządzeń klienckich powinny być dopuszczone do zdalnego dostępu leży w gestii każdej organizacji, zaleca się, aby nie zezwalać na korzystanie

z nieznanych urządzeń, chyba, że istnieje możliwość zapewnienia telepracownikom bezpiecznego sposobu korzystania z tych urządzeń. Przykładem może być wydanie nośnika wymiennego zawierającego bezpieczne środowisko startowe, poinstruowanie użytkowników jak używać tego nośnika z komputerami PC oraz skonfigurowanie rozwiązania zdalnego dostępu w taki sposób, aby blokowało użycie każdego nieznanego urządzenia, które nie korzysta z tego bezpiecznego środowiska. Ryzyko związane z używaniem nieznanych urządzeń do zdalnego dostępu bez bezpiecznego środowiska jest niezwykle wysokie, dlatego organizacje powinny unikać takich sytuacji, jeśli jest to w ogóle możliwe.

Organizacje mogą zdecydować się na określenie dodatkowych wymagań bezpieczeństwa, które są związane z takimi czynnikami jak wrażliwość telepracy. Wiele organizacji wymaga bardziej rygorystycznych środków bezpieczeństwa w sytuacjach telepracy o szczególnie wysokim ryzyku. Wymagania bezpieczeństwa, które mogą być szczególnie przydatne w takich sytuacjach, obejmują następujące elementy:

- Zezwolenie na telepracę wysokiego ryzyka tylko z urządzeń do telepracy wydanych przez organizację i zabezpieczonych.
- Wymóg stosowania wieloskładnikowego uwierzytelniania przy dostępie do urządzenia do telepracy oraz do rozwiązań zdalnego dostępu.
- Stosowanie szyfrowania pamięci masowej na urządzeniu do telepracy, przynajmniej w celu ochrony wszystkich poufnych informacji. Konieczne może być zastosowanie wielu poziomów szyfrowania. Na przykład, pełne szyfrowanie dysku może być potrzebne do ochrony przed napastnikiem, który uzyskał fizyczny dostęp do urządzenia; jednocześnie szyfrowanie dysku wirtualnego lub szyfrowanie plików/folderów może być potrzebne do ochrony przed napastnikiem, który uzyskał logiczny dostęp do urządzenia (tj. dostęp po uwierzytelnieniu pełnego szyfrowania dysku, gdy dane na dysku twardym są automatycznie odszyfrowywane w razie potrzeby). Nośniki wymienne zawierające dane dotyczące telepracy również powinny być zaszyfrowane.

- Migrowanie zasobów wysokiego ryzyka na serwery, które przejmują odpowiedzialność za ich ochronę. Na przykład, telepracownik może połączyć się z serwerem terminalowym, który przechowuje poufne dane, do których telepracownik musi mieć dostęp.
- Przechowywanie i uzyskiwanie dostępu tylko do niezbędnego minimum danych. Niektóre organizacje wydają urządzenia "pożyczkowe", które są całkowicie wymazywane przed i po wykonaniu telepracy wysokiego ryzyka (np. niektóre podróże zagraniczne). Na urządzeniach użyczanych są ładowane tylko dane i autoryzowane aplikacje niezbędne do wykonania telepracy. Urządzenia użyczane są tylko do telepracy i nie mogą być podłączone do wewnętrznych sieci organizacji. Wymazywanie danych przed użyciem urządzenia zapewnia, że urządzenie jest czyste przed wykonaniem telepracy, a wymazywanie danych po użyciu zapewnia, że nie pozostały żadne dane, do których można by uzyskać dostęp w przyszłości.

W sytuacjach wysokiego ryzyka organizacje mogą również zdecydować się na ograniczenie ryzyka poprzez zakaz telepracy i zdalnego dostępu do określonych rodzajów informacji, takich jak wrażliwe informacje osobiste.

Tabela 1 przedstawia przykładowy sposób definiowania poziomów dostępu. Istnieje siedem kategorii urządzeń klienckich: urządzenia rządowe (GFE) w biurze, GFE w telepracy, BYOD w biurze, BYOD w telepracy, kontrahent/partner biznesowy/dostawca w biurze, kontrahent/partner biznesowy/dostawca w telepracy oraz urządzenia innych firm (np. kafejka internetowa, kiosk hotelowy). W tabeli podano kilka przykładów aplikacji lub systemów oraz sposobów ograniczania dostępu do nich w zależności od typu urządzenia i lokalizacji. Na przykład, dostęp do systemu kadrowego może być dozwolony tylko z urządzeń GFE w biurze, a zabroniony dla urządzeń GFE w telepracy i wszystkich innych typów urządzeń, ze względu na wrażliwość zawartych w nim PII. Dostęp do poczty elektronicznej, kalendarza i innych ogólnych zasobów może być dozwolony ze wszystkich typów urządzeń i lokalizacji innych niż urządzenia osób trzecich. Należy zauważyć, że w wielu

przypadkach organizacja może połączyć kolumny BYOD w biurze i BYOD w telepracy, ponieważ istnieją zalecenia, aby zabezpieczyć BYOD w biurze tak, jakby była to telepraca/dostęp zdalny.

***Tabela 5-1 Przykład poziomów dostępu***

| Aplikacja lub system | GFE w biurze | GFE telepraca | BYOD w biurze | BYOD telepraca | Wykonawca, partner, sprzedawca w biurze | Telepraca zleceniobiorców, partnerów, sprzedawców | Strona trzecia (kafejka internetowa, itp.) |
|---|---|---|---|---|---|---|---|
| System kadrowy | Tak | Nie | Nie | Nie | Nie | Nie | Nie |
| System finansowy | Tak | Tak | Nie | Nie | Nie | Nie | Nie |
| E-mail | Tak | Tak | Tak | Tak | Tak | Tak | Nie |
| Kalendarze | Tak | Tak | Tak | Tak | Tak | Tak | Nie |
| Własność intelektualna | Tak | Nie | Nie | Nie | Nie | Nie | Nie |
| …….. | | | | | | | |

Każdego roku następuje wiele zmian w możliwościach urządzeń do telepracy, dostępnych dla organizacji mechanizmach zabezpieczeń, rodzajach zagrożeń dla różnych typów urządzeń itd. Dlatego też, organizacje powinny okresowo oceniać swoje polityki dotyczące urządzeń do telepracy i rozważać zmianę typów urządzeń klienckich, które są dozwolone oraz poziomów dostępu do nich. Organizacje powinny być również świadome pojawiania się nowych typów rozwiązań zdalnego dostępu oraz istotnych zmian w istniejących technologiach zdalnego dostępu i zapewnić, że polityki organizacji są odpowiednio aktualizowane w miarę potrzeb.

### 5.1.3. Dodatkowe wymagania użytkowników

Organizacje często stosują dodatkowe środki bezpieczeństwa w odniesieniu do telepracy, które, choć są pomocne w ograniczaniu zagrożeń, nie mogą być bezpośrednio egzekwowane przez organizację. Organizacje powinny edukować użytkowników o znaczeniu tych dodatkowych środków bezpieczeństwa i zdefiniować odpowiedzialność telepracowników za wdrożenie tych środków w polityce i umowach o telepracę.

Jednym z najważniejszych aspektów bezpieczeństwa telepracy jest szkolenie użytkowników w zakresie wykrywania i radzenia sobie z atakami phishingowymi oraz innymi formami socjotechniki z wykorzystaniem urządzeń do telepracy i zdalnego dostępu. Ponadto, organizacje powinny zapewnić użytkownikom dostęp do pomocy w przypadku pytań lub wątpliwości dotyczących bezpieczeństwa telepracy, a także upewnić się, że użytkownicy są świadomi istnienia takiej pomocy i sposobu, w jaki mogą się o nią zwrócić.

Innym możliwym zagadnieniem związanym z bezpieczeństwem są usługi telefoniczne. W zależności od wrażliwości komunikacji w ramach telepracy, powinno być brane pod uwagę bezpieczeństwo połączeń telefonicznych. Telefony przewodowe korzystające z tradycyjnych przewodowych sieci telefonicznych nie mogą być przechwycone bez fizycznego połączenia, więc są wystarczająco bezpieczne dla typowej telepracy. Telefony bezprzewodowe korzystające z tradycyjnych przewodowych sieci telefonicznych powinny wykorzystywać technologię spread spectrum do kodowania transmisji, zmniejszając w ten sposób ryzyko podsłuchu w fizycznej bliskości (zazwyczaj maksymalnie kilkaset metrów). Dla typowej telepracy [36] powinny być akceptowalne cyfrowe telefony komórkowe. Komunikacja za pośrednictwem usług VoIP (Voice over IP) nie powinna być uważana za bezpieczną, o ile nie jest stosowana jakaś forma szyfrowania; jednakże wiele usług VoIP zapewnia obecnie silne

[36] Komunikacja w cyfrowej telefonii komórkowej, mimo stosowania szyfrowania systemowego, może zostać przechwycona przez osoby posiadające sprzęt skanujący i deszyfrowana. Dlatego należy unikać korzystania z niej podczas omawiania informacji stanowiących tajemnicę. Jednak analogowe sieci telefonii komórkowej zostały wycofane z użytku.

szyfrowanie, które powinno być stosowane w celu ochrony poufnych informacji. Każde stosowane szyfrowanie musi posiadać certyfikat zgodności z wymogami instytutu NIST. Specyfikacja FIPS 140, *Wymagania bezpieczeństwa dla modułów* kryptograficznych, określa sposób walidacji modułów kryptograficznych.

Organizacje mogą również rozważyć bezpieczeństwo bezprzewodowych sieci osobistych (WPAN), które są niewielkimi sieciami bezprzewodowymi niewymagającymi infrastruktury do działania. Przykłady technologii WPAN to używanie bezprzewodowej klawiatury lub myszy z komputerem, bezprzewodowe drukowanie, synchronizacja smartfona z komputerem oraz umożliwienie używania bezprzewodowego zestawu słuchawkowego lub słuchawki ze smartfonem. Najpowszechniej stosowaną technologią WPAN jest Bluetooth. W przypadku urządzeń znajdujących się w pobliżu zagrożeń telepracownicy powinni wyłączać technologie WPAN, gdy nie są one używane, aby zapobiec nadużyciom przez osoby nieupoważnione.

Dodatkowe informacje na temat tych aspektów bezpieczeństwa są dostępne w NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [37]oraz NIST SP 800-121 Revision 1, *Guide to Bluetooth Security*.[38]

## 5.2. Rozwój

Po ustaleniu polityki bezpieczeństwa telepracy, określeniu potrzeb w zakresie telepracy i zdalnego dostępu oraz wykonaniu innych czynności przygotowawczych, kolejnym krokiem jest określenie rodzaju technologii telepracy lub zdalnego dostępu oraz zaprojektowanie rozwiązania do wdrożenia. Przy projektowaniu rozwiązania należy wziąć pod uwagę wiele czynników, z których większość ma ogólne zastosowanie do każdej technologii IT; niektóre z nich zostały omówione w rozdziale 2.1 niniejszego dokumentu oraz w NIST SP 800-53. W tym rozdziale skupiono się na technicznych aspektach bezpieczeństwa, które są

[37] http://dx.doi.org/10.6028/NIST.SP.800-114r1
[38] http://dx.doi.org/10.6028/NIST.SP.800-121r1

najważniejsze przy projektowaniu rozwiązań telepracy i zdalnego dostępu. Najważniejsze z nich obejmują następujące kwestie:[39]

- **Architektura.** Projektowanie architektury obejmuje umieszczenie serwera zdalnego dostępu, wybór oprogramowania klienckiego zdalnego dostępu (jeśli jest potrzebne) oraz zaprojektowanie jednego lub więcej segmentów sieci organizacji dla urządzeń klienckich niekontrolowanych przez organizację.
- **Uwierzytelnianie.** Uwierzytelnianie polega na wyborze metody uwierzytelniania zdalnego dostępu, opisanej w sekcji 3, oraz określeniu sposobu implementacji jej komponentów klient/użytkownik i serwer, w tym procedur wydawania i resetowania identyfikatorów oraz wyposażania użytkowników i urządzeń klienckich w identyfikatory.
- **Kryptografia.** Decyzje związane z kryptografią obejmują wybór algorytmów szyfrowania i ochrony integralności komunikacji zdalnego dostępu oraz ustawienie siły klucza dla algorytmów obsługujących wiele długości klucza.
- **Kontrola dostępu.** Obejmuje ona określenie, które rodzaje komunikacji zdalnego dostępu powinny być dozwolone, a które odrzucane. Sekcja 3 zawiera dodatkowe informacje na temat możliwości kontroli dostępu.
- **Bezpieczeństwo punktów końcowych.** Decyzje dotyczące bezpieczeństwa punktów końcowych dotyczą określenia sposobu zabezpieczenia serwerów zdalnego dostępu oraz urządzeń klienckich telepracy, co zostało opisane odpowiednio w sekcjach 3 i 4.

Aspekty bezpieczeństwa związane z projektowaniem rozwiązań telepracy i zdalnego dostępu powinny być udokumentowane w planie bezpieczeństwa systemu. Organizacja powinna

[39] Rozważania te są oparte na materiale z sekcji 4 NIST SP 800-77, *Guide to IPsec VPNs* (http://dx.doi.org/10.6028/NIST.SP.800-77).

również rozważyć, jak należy postępować w przypadku incydentów związanych z rozwiązaniami telepracy i zdalnego dostępu i również udokumentować te plany.[40]

## 5.3. Wdrożenie

Po zaprojektowaniu rozwiązania zdalnego dostępu, kolejnym krokiem jest wdrożenie i przetestowanie prototypu projektu przed wprowadzeniem rozwiązania do produkcji. Aspekty rozwiązania, które powinny zostać ocenione, obejmują następujące elementy:[41]

- **Łączność.** Użytkownicy mogą nawiązywać i utrzymywać połączenia zdalnego dostępu. Użytkownicy mogą łączyć się ze wszystkimi zasobami, na które mają pozwolenie i nie mogą łączyć się z żadnymi innymi zasobami.
- **Ochrona.** Każdy strumień ruchu jest chroniony zgodnie z ustalonymi wymaganiami. Dotyczy to zarówno przepływów pomiędzy urządzeniem klienckim telepracy, a serwerem zdalnego dostępu, jak i pomiędzy serwerem zdalnego dostępu, a zasobami wewnętrznymi. Ochrona powinna być weryfikowana za pomocą takich środków, jak monitorowanie ruchu sieciowego lub sprawdzanie logów ruchu.
- **Uwierzytelnianie.** Uwierzytelnianie jest wymagane i nie może być łatwo naruszone lub ominięte. Wszystkie polityki uwierzytelniania są egzekwowane. Przeprowadzanie solidnych testów uwierzytelniania jest ważne, aby zmniejszyć ryzyko dostępu napastników do chronionych zasobów wewnętrznych.
- **Aplikacje.** Rozwiązanie zdalnego dostępu nie zakłóca korzystania z aplikacji, które są dopuszczone do użytku poprzez zdalny dostęp, ani nie zakłóca działania urządzeń klienckich telepracy (np. klient VPN wchodzący w konflikt z firewallem hosta).
- **Zarządzanie.** Administratorzy mogą skutecznie i bezpiecznie konfigurować rozwiązanie i zarządzać nim. Dotyczy to wszystkich komponentów, w tym serwerów

[40] Więcej informacji na temat obsługi *incydentów można znaleźć w dokumencie* NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (http://dx.doi.org/10.6028/NIST.SP.800-61r2).
[41] Rozważania te są oparte na materiale z sekcji 4 NIST SP 800-77, *Guide to IPsec VPNs* (http://dx.doi.org/10.6028/NIST.SP.800-77).

zdalnego dostępu, usług uwierzytelniania i oprogramowania klienckiego. Szczególnie ważna jest łatwość wdrażania i konfiguracji, np. w pełni zautomatyzowana konfiguracja klienta w porównaniu z ręcznym konfigurowaniem każdego klienta przez administratorów. Innym problemem jest możliwość zmiany ustawień klienta zdalnego dostępu przez użytkowników, co może osłabić bezpieczeństwo zdalnego dostępu. Automatyzacja konfiguracji urządzeń może w znacznym stopniu ograniczyć niezamierzone błędy wynikające z nieprawidłowego skonfigurowania ustawień przez użytkowników.

- **Rejestrowanie.** Rozwiązanie zdalnego dostępu rejestruje zdarzenia związane z bezpieczeństwem zgodnie z zasadami obowiązującymi w danej organizacji. Niektóre rozwiązania zdalnego dostępu zapewniają bardziej szczegółowe możliwości rejestrowania niż inne - na przykład rejestrowanie użycia poszczególnych aplikacji, a nie tylko połączeń z określonymi hostami - dlatego w niektórych przypadkach może być konieczne poleganie na zasobach używanych przez zdalny dostęp w celu wykonania części rejestrowania, których nie może wykonać serwer zdalnego dostępu.
- **Wydajność.** Rozwiązanie zapewnia odpowiednią wydajność podczas normalnego i szczytowego wykorzystania. Ważne jest, aby wziąć pod uwagę nie tylko wydajność głównych komponentów zdalnego dostępu, ale także urządzeń pośrednich, takich jak routery i zapory sieciowe. Wydajność jest szczególnie ważna, gdy duże aktualizacje oprogramowania są dostarczane przez rozwiązanie zdalnego dostępu do urządzeń klienckich telepracy. W wielu przypadkach najlepszym sposobem na przetestowanie wydajności prototypu pod obciążeniem jest użycie symulowanych generatorów ruchu w sieci testowej na żywo, aby jak najwierniej naśladować rzeczywistą charakterystykę spodziewanego ruchu. Testy powinny obejmować różnorodne aplikacje, które będą wykorzystywane przy zdalnym dostępie.
- **Bezpieczeństwo implementacji.** Sama implementacja zdalnego dostępu może zawierać luki i słabości, które napastnicy mogliby wykorzystać. Organizacje o wysokich wymaganiach w zakresie bezpieczeństwa mogą zdecydować się na

przeprowadzenie szeroko zakrojonej oceny podatności komponentów zdalnego dostępu. Przynajmniej, wszystkie komponenty powinny być aktualizowane najnowszymi łatami i konfigurowane zgodnie z solidnymi praktykami bezpieczeństwa.

- **Ustawienia domyślne.** Wdrożeniowcy powinni dokładnie przejrzeć wartości domyślne dla każdego ustawienia zdalnego dostępu i zmienić ustawienia, jeśli jest to konieczne do wspierania wymagań bezpieczeństwa. Wdrożeniowcy powinni również upewnić się, że rozwiązanie zdalnego dostępu nie powoduje nieoczekiwanego "powrotu" do ustawień domyślnych z powodu interoperacyjności lub innych powodów.

## 5.4. Eksploatacja i konserwacja

Procesy operacyjne, które są szczególnie pomocne w utrzymaniu bezpieczeństwa telepracy i zdalnego dostępu, a więc powinny być wykonywane regularnie, to m.in:[42]

- Sprawdzanie dostępności aktualizacji i poprawek do komponentów oprogramowania zdalnego dostępu oraz pozyskiwanie, testowanie i wdrażanie aktualizacji.
- Zapewnienie, że każdy komponent infrastruktury zdalnego dostępu (serwery, bramy, serwery uwierzytelniania itp.) ma zsynchronizowany zegar ze wspólnym źródłem czasu, tak aby jego znaczniki czasu były zgodne z tymi generowanymi przez inne systemy.
- Rekonfigurowanie funkcji kontroli dostępu, w razie potrzeby, w oparciu o czynniki takie jak zmiany polityki, zmiany technologiczne, wyniki audytów i nowe potrzeby w zakresie bezpieczeństwa.
- Wykrywanie i dokumentowanie anomalii wykrytych w infrastrukturze zdalnego dostępu. Takie anomalie mogą wskazywać na złośliwe działanie lub odstępstwa od

[42] Część informacji dotyczących operacji i konserwacji zaczerpnięto z sekcji 5.4 i 5.5 NIST SP 800-92, *Guide to Computer Security Log Management* (http://dx.doi.org/10.6028/NIST.SP.800-92).

polityki i procedur. Anomalie powinny być zgłaszane administratorom innych systemów, jeśli jest to właściwe.

Organizacje powinny również okresowo przeprowadzać oceny w celu potwierdzenia, że polityki, procesy i procedury zdalnego dostępu są właściwie stosowane. Działania oceniające mogą być pasywne, takie jak przeglądanie logów, lub aktywne, takie jak wykonywanie skanowania podatności i testów penetracyjnych.

Więcej informacji na temat oceny technicznej telepracy i zdalnego dostępu można znaleźć w dokumencie NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*.[43]

## 5.5. Utylizacja

Zanim urządzenie klienckie do telepracy lub serwer zdalnego dostępu na stałe opuści organizację (np. gdy wygaśnie umowa dzierżawy serwera lub gdy przestarzały komputer zostanie poddany recyklingowi), organizacja powinna usunąć wszelkie poufne dane z hosta. Usuwanie danych może być również konieczne w przypadku, gdy organizacja udostępnia telepracownikom urządzenia "pożyczkowe", szczególnie na czas podróży. Zadanie wyczyszczenia wszystkich wrażliwych danych z urządzeń pamięci masowej takich jak dyski twarde czy karty pamięci jest często zaskakująco trudne ze względu na ilość miejsc, w których takie dane się znajdują. Patrz NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, [44]aby uzyskać dodatkowe informacje i zalecenia dotyczące usuwania danych z urządzeń do telepracy i zdalnego dostępu. Należy pamiętać, że dane wrażliwe często znajdują się w miejscach innych niż obszar danych użytkownika; na przykład, oprogramowanie działające pod kontrolą systemu Microsoft Windows często przechowuje potencjalnie wrażliwe dane w rejestrze Windows. Organizacja powinna zdecydowanie rozważyć całkowite usunięcie wszystkich urządzeń pamięci masowej.

[43] http://dx.doi.org/10.6028/NIST.SP.800-115
[44] http://dx.doi.org/10.6028/NIST.SP.800-88r1

Szczególnym wyzwaniem dla organizacji może być rozwiązanie problemu wymazywania danych z urządzeń BYOD. Ponieważ urządzenia te są wykorzystywane zarówno do celów osobistych, jak i służbowych, konieczne może być usunięcie danych dotyczących telepracy bez wpływu na dane osobiste. Selektywne usuwanie danych można przeprowadzić za pomocą oprogramowania do zarządzania urządzeniami mobilnymi w organizacji (dla urządzeń mobilnych) oraz specjalistycznych narzędzi. Organizacje powinny dokładnie przeanalizować kwestie związane z usuwaniem danych z urządzeń BYOD przed wydaniem zgody na ich wykorzystanie.

Organizacje mogą mieć również obawy dotyczące wymazywania danych na urządzeniach klienckich kontrolowanych przez inne podmioty. Podobnie jak w przypadku urządzeń BYOD, organizacja może chcieć wymazywać swoje dane z tych urządzeń bez naruszania danych organizacji kontrolującej. Opcją może być selektywne usuwanie danych przez organizację lub bardziej praktyczne może być zlecenie organizacji kontrolującej wykonanie własnego usuwania danych dla danych, o których mowa.

## 5.6. Podsumowanie kluczowych zaleceń

Poniższa lista przedstawia niektóre z kluczowych rekomendacji zawartych w tej części dokumentu.

- Polityka bezpieczeństwa telepracy powinna definiować, jakie formy zdalnego dostępu są dozwolone w organizacji, jakie typy urządzeń telepracowników mogą korzystać z każdej formy zdalnego dostępu, jaki rodzaj dostępu jest przyznawany każdemu typowi telepracownika oraz w jaki sposób powinno być prowadzone zakładanie kont użytkowników. Powinna ona również obejmować sposób administrowania serwerami zdalnego dostępu oraz sposób aktualizacji polityk na tych serwerach. Polityka bezpieczeństwa telepracy powinna być udokumentowana w planie bezpieczeństwa systemu. (Sekcja 5.1)

- Każda organizacja powinna podejmować własne, oparte na analizie ryzyka decyzje dotyczące tego, jakie poziomy zdalnego dostępu powinny być dozwolone dla poszczególnych typów urządzeń klienckich do telepracy. (Sekcja 5.1)
- Organizacje powinny okresowo oceniać swoje zasady dotyczące urządzeń do telepracy i rozważać zmianę typów urządzeń klienckich, które są dozwolone, oraz poziomów dostępu, jakie mogą zostać im przyznane. (Sekcja 5.1)
- Organizacje powinny udokumentować aspekty bezpieczeństwa projektu rozwiązania telepracy i zdalnego dostępu w planie bezpieczeństwa systemu. (Sekcja 5.2)
- Przed wdrożeniem rozwiązania zdalnego dostępu do produkcji, organizacja powinna wdrożyć i przetestować prototyp projektu i ocenić go, w tym jego łączność, ochronę ruchu, uwierzytelnianie, zarządzanie, logowanie, wydajność, bezpieczeństwo wdrożenia i interferencję z aplikacjami. (Sekcja 5.3)
- Organizacje powinny regularnie przeprowadzać procesy operacyjne w celu utrzymania bezpieczeństwa telepracy i zdalnego dostępu, takie jak wdrażanie aktualizacji, weryfikacja synchronizacji zegara, rekonfiguracja funkcji kontroli dostępu w razie potrzeby oraz wykrywanie i dokumentowanie anomalii w infrastrukturze zdalnego dostępu. (Sekcja 5.4)
- Organizacje powinny również okresowo przeprowadzać oceny w celu potwierdzenia, że zasady, procesy i procedury zdalnego dostępu są właściwie stosowane. (Sekcja 5.4)
- Przed utylizacją urządzenia klienckiego do telepracy lub serwera zdalnego dostępu, organizacja powinna usunąć z nich wszelkie dane wrażliwe. (Punkt 5.5)

# ZAŁĄCZNIK A MAPOWANIE Z ZABEZPIECZENIAMI NSC 800-53

Niniejszy załącznik zawiera listę zabezpieczeń z publikacji NSC 800-53, które są najbardziej istotne dla bezpieczeństwa telepracy, zdalnego dostępu i technologii BYOD w organizacji. Obok każdego zabezpieczenia znajduje się wyjaśnienie jej implikacji dla bezpieczeństwa telepracy, zdalnego dostępu i BYOD w organizacji.

| **Zabezpieczenie**<br><br>**NIST SP 800-53** | **Implikacje dla bezpieczeństwa telepracy / dostępu zdalnego / BYOD** |
|---|---|
| AC-2<br><br>Zarządzanie kontami | Zabezpieczenie to obejmuje zarządzanie jedno- lub wieloskładnikowym uwierzytelnianiem użytkowników zdalnego dostępu, takim jak hasła, certyfikaty cyfrowe i/lub sprzętowe tokeny uwierzytelniające. |
| AC-17<br><br>Dostęp zdalny | Całe to zabezpieczenie jest poświęcona dokumentowaniu wymagań dotyczących zdalnego dostępu, autoryzacji zdalnego dostępu przed zezwoleniem na połączenia, monitorowaniu i kontroli zdalnego dostępu, szyfrowaniu połączeń zdalnego dostępu itp. |
| AC-19<br><br>Kontrola dostępu dla urządzeń przenośnych | Zabezpieczenie to obejmuje wymagania dotyczące kontrolowanych przez organizację urządzeń przenośnych oraz upoważnienia do podłączania urządzeń przenośnych do systemów organizacyjnych, np. poprzez zdalny dostęp. |

| **Zabezpieczenie**<br><br>**NIST SP 800-53** | **Implikacje dla bezpieczeństwa telepracy / dostępu zdalnego / BYOD** |
|---|---|
| AC-20<br><br>Wykorzystanie systemów zewnętrznych | Zabezpieczenie to obejmuje korzystanie z zewnętrznych systemów informatycznych, takich jak urządzenia klienckie będące własnością osobistą (BYOD) oraz urządzenia klienckie kontrolowane przez strony trzecie, które mogą przetwarzać, przechowywać lub przesyłać dane kontrolowane przez organizację w imieniu organizacji. |
| CA-9<br><br>Połączenia wewnątrzsystemowe | Zabezpieczenie to dotyczy połączeń między systemem, a jego elementami. |
| CP-9<br><br>Kopia zapasowa | Urządzenia do telepracy muszą posiadać lokalną lub zdalną kopię zapasową danych. |
| IA-2<br><br>Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Zabezpieczenie to polega na stosowaniu jedno- lub wieloskładnikowego uwierzytelniania użytkowników zdalnego dostępu, takiego jak hasła, certyfikaty cyfrowe i/lub sprzętowe tokeny uwierzytelniające. |
| IA-3<br><br>Identyfikacja i uwierzytelnianie urządzenia | Wzajemne uwierzytelnianie jest zalecane zawsze, gdy jest to możliwe, aby zweryfikować legalność serwera dostępu zdalnego przed przekazaniem mu danych uwierzytelniających. |

| **Zabezpieczenie**<br><br>**NIST SP 800-53** | **Implikacje dla bezpieczeństwa telepracy / dostępu zdalnego / BYOD** |
|---|---|
| IA-11<br><br>Ponowne uwierzytelnienie | Wiele organizacji wymaga od telepracowników okresowego uwierzytelniania się podczas długich sesji zdalnego dostępu, np. po każdych ośmiu godzinach sesji lub po 30 minutach bezczynności. Pomaga to organizacjom potwierdzić, że osoba korzystająca ze zdalnego dostępu jest do tego upoważniona. |
| RA-3<br><br>Szacowanie ryzyka | W ramach wyboru metody zdalnego dostępu (tunelowanie, portale aplikacyjne, zdalny dostęp do pulpitu, bezpośredni dostęp do aplikacji) należy przeprowadzić szacowanie ryzyka. |
| SC-7<br><br>Ochrona połączeń brzegowych | Zabezpieczenie to obejmuje segmentację sieci (np. przy użyciu podsieci) w celu utrzymania publicznie dostępnych komponentów poza sieciami wewnętrznymi oraz monitorowanie i kontrolowanie komunikacji w kluczowych punktach granicznych. |
| SC-8<br><br>Poufność i integralność transmisji | Różne metody zdalnego dostępu omówione w niniejszej publikacji chronią poufność i integralność transmisji poprzez wykorzystanie kryptografii. |

# ZAŁĄCZNIK B MAPOWANIE Z PODKATEGORIĄ RAM CYBERBEZPIECZEŃSTWA

Niniejszy załącznik zawiera listę podkategorii Ram Cyberbezpieczeństwa (*ang. Cybersecurity Framework*), które są najistotniejsze z punktu widzenia zabezpieczenia technologii telepracy, zdalnego dostępu i BYOD w organizacji. Obok każdej podkategorii znajduje się wyjaśnienie jej implikacji dla bezpieczeństwo telepracy, zdalnego dostępu i BYOD w organizacji.

| **Podkategoria Ram Cyberbezpieczeństwa** | **Implikacje dla bezpieczeństwa telepracy / dostępu zdalnego / BYOD** |
|---|---|
| ID.GV-1: Ustanowiona jest organizacyjna polityka bezpieczeństwa informacji | Organizacja powinna posiadać politykę bezpieczeństwa telepracy. |
| ID.RA-5: Zagrożenia, podatności, prawdopodobieństwa i wpływ wykorzystywane są do określania ryzyka | W ramach wyboru metody zdalnego dostępu (tunelowanie, portale aplikacyjne, zdalny dostęp do pulpitu, bezpośredni dostęp do aplikacji) należy przeprowadzić szacowanie ryzyka. |
| PR.AC-1: Tożsamości i dane uwierzytelniające są kontrolowane w przypadku uprawnionych urządzeń i użytkowników | Zabezpieczenie to polega na zastosowaniu jedno- lub wieloskładnikowego uwierzytelniania użytkowników zdalnego dostępu, takie jak hasła, certyfikaty cyfrowe i/lub sprzętowe tokeny uwierzytelniające. Zaleca się również wzajemne uwierzytelnianie, gdy tylko jest to możliwe, aby zweryfikować legalność serwera zdalnego dostępu przed przekazaniem mu danych uwierzytelniających użytkownika. |

| Podkategoria Ram Cyberbezpieczeństwa | Implikacje dla bezpieczeństwa telepracy / dostępu zdalnego / BYOD |
|---|---|
| PR.AC-3: Dostęp zdalny jest kontrolowany | Organizacja powinna formalnie zarządzać wszystkimi procesami i technologiami zdalnego dostępu. |
| PR.AC-5: Integralność sieci jest chroniona, łącznie z segregacją sieci, w miarę możliwości | Obejmuje to segmentację sieci (np. przy użyciu podsieci) w celu utrzymania publicznie dostępnych komponentów poza sieciami wewnętrznymi oraz monitorowanie i kontrolowanie komunikacji w kluczowych punktach granicznych. |
| PR.DS-2: Przesyłane dane są chronione | Różne metody zdalnego dostępu omówione w niniejszej publikacji chronią poufność i integralność transmisji poprzez wykorzystanie kryptografii. |
| PR.IP-4: Okresowo tworzone, utrzymywane i testowane są kopie zapasowe informacji | Urządzenia do telepracy muszą posiadać lokalną lub zdalną kopię zapasową danych. |

# ZAŁĄCZNIK C SŁOWNIK

***PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA***

Poniżej zdefiniowano wybrane pojęcia użyte w publikacji.

**Bezpośredni dostęp do aplikacji:** Architektura zdalnego dostępu wysokiego poziomu, która pozwala telepracownikom na bezpośredni dostęp do poszczególnych aplikacji, bez użycia oprogramowania zdalnego dostępu.

**Blokowanie sesji:** Funkcja umożliwiająca użytkownikowi zablokowanie sesji na żądanie lub zablokowanie sesji po upływie zadanego czasu bezczynności.

**Bring Your Own Device (BYOD):** Urządzenie będące własnością telepracownika, niekontrolowane przez organizację.

**Komputer osobisty:** Komputer stacjonarny lub przenośny.

**Portal:** Architektura zdalnego dostępu wysokiego poziomu, oparta na serwerze, która oferuje telepracownikom dostęp do jednej lub wielu aplikacji poprzez pojedynczy, scentralizowany interfejs.

**Telepraca:** Możliwość wykonywania pracy przez pracowników organizacji, kontrahentów, partnerów biznesowych, sprzedawców i innych użytkowników z miejsc innych niż siedziba organizacji.

**Tunelowanie:** Architektura zdalnego dostępu wysokiego poziomu, która zapewnia bezpieczne połączenie pomiędzy urządzeniem klienckim telepracy a serwerem poprzez sieć niezaufaną.

**Tunelowanie dzielone:** Funkcja klienta VPN, która tuneluje całą komunikację dotyczącą wewnętrznych zasobów organizacji przez VPN, chroniąc je w ten sposób, i wyklucza wszelką inną komunikację z przechodzenia przez tunel.

**Urządzenie klienckie:** System używany przez pracownika zdalnego w celu uzyskania dostępu do sieci organizacji i systemów w tej sieci.

**Urządzenie klienckie do telepracy:** Komputer PC lub urządzenie mobilne używane przez telepracownika do wykonywania telepracy.

**Urządzenie mobilne:** przenośne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią. Urządzenie mobilne może być użytkowane przez użytkownika bez konieczności angażowania dodatkowych środków.

**Wirtualna sieć prywatna (VPN):** Sieć wirtualna, zbudowana na bazie istniejących sieci fizycznych, która zapewnia bezpieczny tunel komunikacyjny dla danych i innych informacji przesyłanych między sieciami.

**Zdalny dostęp:** Zdolność użytkowników organizacji do uzyskania dostępu do jej niepublicznych zasobów obliczeniowych z lokalizacji zewnętrznych, innych niż obiekty organizacji.

**Zdalny dostęp do pulpitu:** Architektura zdalnego dostępu wysokiego poziomu, która daje telepracownikowi możliwość zdalnego sterowania określonym komputerem stacjonarnym w organizacji, najczęściej własnym komputerem użytkownika w biurze organizacji, z urządzenia klienckiego telepracy.

# ZAŁĄCZNIK D AKRONIMY

***PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA***

Poniżej zdefiniowano wybrane akronimy i skróty stosowane w niniejszej publikacji.

| | |
|---|---|
| **DSL** | **Cyfrowa linia abonencka** |
| **HTTPS** | Protokół przesyłania hipertekstu przez TLS |
| **IP** | Protokół internetowy |
| **IT** | Technologia informacyjna |
| **MDM** | Zarządzanie urządzeniami mobilnymi |
| **MPLS** | Multiprotocol Label Switching |
| **NAC** | Kontrola dostępu do sieci |
| **NAT** | Translacja adresów sieciowych |
| **NIST** | National Institute of Standards and Technology |
| **OMB** | Office of Management and Budget (Urząd Federalny USA) |
| **OS** | System operacyjny |
| **PC** | Komputer osobisty |
| **PII** | Dane osobowe |
| **PPP** | Protokół transmisji punkt-punkt |

| | |
|---|---|
| **RDP** | Protokół pulpitu zdalnego |
| **SP** | Publikacja specjalna |
| **SSH** | Bezpieczny Shell |
| **TLS** | Bezpieczeństwo warstwy transportowej |
| **VDI** | Infrastruktura wirtualnych pulpitów |
| **VM** | Maszyna wirtualna |
| **VMI** | Wirtualna infrastruktura mobilna |
| **VNC** | Obliczenia w sieci wirtualnej |
| **VoIP** | Komutacja pakietów |
| **WPAN** | Bezprzewodowa sieć osobista |

# ZAŁĄCZNIK E REFERENCJE

Poniższe referencje zawierają przykłady zasobów, które mogą być pomocne w lepszym zrozumieniu bezpieczeństwa telepracy i zdalnego dostępu. Specjalne publikacje NIST wymienione poniżej, jak również wiele innych, są również dostępne poprzez stronę http://csrc.nist.gov/publications/PubsSPs.html.

**Strony www z zasobami dotyczącymi bezpieczeństwa telepracy**

| Nazwa strony www | URL |
|---|---|
| Home Network Security | https://www.us-cert.gov/security-publications/home-network-security |
| Safety & Security Center | http://www.microsoft.com/security/default.aspx |
| StaySafeOnline.org | http://www.staysafeonline.org/ |
| telework.gov | http://www.telework.gov/ |

**Publikacje związane z bezpieczeństwem telepracy**

| Tytuł dokumentu | URL |
|---|---|
| *Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs* | https://www.whitehouse.gov/digitalgov/bring-your-own-device |
| *Guide to Telework in the Federal Government* | http://www.telework.gov/guidance_and_legislation/telework_guide/telework_guide.pdf |

| Tytuł dokumentu | URL |
|---|---|
| NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks* | http://dx.doi.org/10.6028/NIST.SP.800-48r1 |
| NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* | http://dx.doi.org/10.6028/NIST.SP.800-52r1 |
| NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* | http://dx.doi.org/10.6028/NIST.SP.800-53r4 |
| NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security* | http://dx.doi.org/10.6028/NIST.SP.800-55r1 |
| NIST SP 800-63-2, *Electronic Authentication Guideline* | http://dx.doi.org/10.6028/NIST.SP.800-63-2 |
| NIST SP 800-77, *Guide to IPsec VPNs* | http://dx.doi.org/10.6028/NIST.SP.800-77 |
| NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* | http://dx.doi.org/10.6028/NIST.SP.800-83r1 |
| NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization* | http://dx.doi.org/10.6028/NIST.SP.800-88r1 |
| NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* | http://dx.doi.org/10.6028/NIST.SP.800-97 |
| NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* | http://dx.doi.org/10.6028/NIST.SP.800-111 |
| NIST SP 800-113, *Guide to SSL VPNs* | http://dx.doi.org/10.6028/NIST.SP.800-113 |

| Tytuł dokumentu | URL |
|---|---|
| NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* | http://dx.doi.org/10.6028/NIST.SP.800-114r1 |
| NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* | http://dx.doi.org/10.6028/NIST.SP.800-115 |
| NIST SP 800-118 (Draft), *Guide to Enterprise Password Management* | http://csrc.nist.gov/publications/PubsSPs.html#800-118 |
| NIST SP 800-121 Revision 1, *Guide to Bluetooth Security* | http://dx.doi.org/10.6028/NIST.SP.800-121r1 |
| NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* | http://dx.doi.org/10.6028/NIST.SP.800-122 |
| NIST SP 800-123, *Guide to General Server Security* | http://dx.doi.org/10.6028/NIST.SP.800-123 |
| NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* | http://dx.doi.org/10.6028/NIST.SP.800-124r1 |
| NIST SP 800-125, *Guide to Security for Full Virtualization Technologies* | http://dx.doi.org/10.6028/NIST.SP.800-125 |
| NIST SP 800-147, *BIOS Protection Guidelines* | http://dx.doi.org/10.6028/NIST.SP.800-147 |
| NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)* | http://dx.doi.org/10.6028/NIST.SP.800-153 |
| NIST SP 800-163, *Vetting the Security of Mobile Applications* | http://dx.doi.org/10.6028/NIST.SP.800-163 |

| Tytuł dokumentu | URL |
|---|---|
| NIST SP 800-167, *Guide to Application Whitelisting* | http://dx.doi.org/10.6028/NIST.SP.800-167 |
| OMB Memorandum M-11-27, *Implementing the Telework Enhancement Act of 2010: Security Guidelines* | http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-27.pdf |

| NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA | |
|---|---|
| NSC 199 | Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199 |
| NSC 200 | Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200 |
| NSC 800-18 | Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18 |
| NSC 800-30 | Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30 |
| NSC 800-53 | Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53 |
| NSC 800-53A | Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A |
| NSC 800-53B | Zabezpieczenia bazowe systemów informatycznych 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<br>Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations \| CSRC (nist.gov) |
| NSC 800-60 | Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60 |