Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-114 wer. 1.0

5 kwietnia 2023

Poradnik bezpieczeństwa w zakresie telepracy/pracy zdalnej i używania prywatnych urządzeń (BYOD)

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

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

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

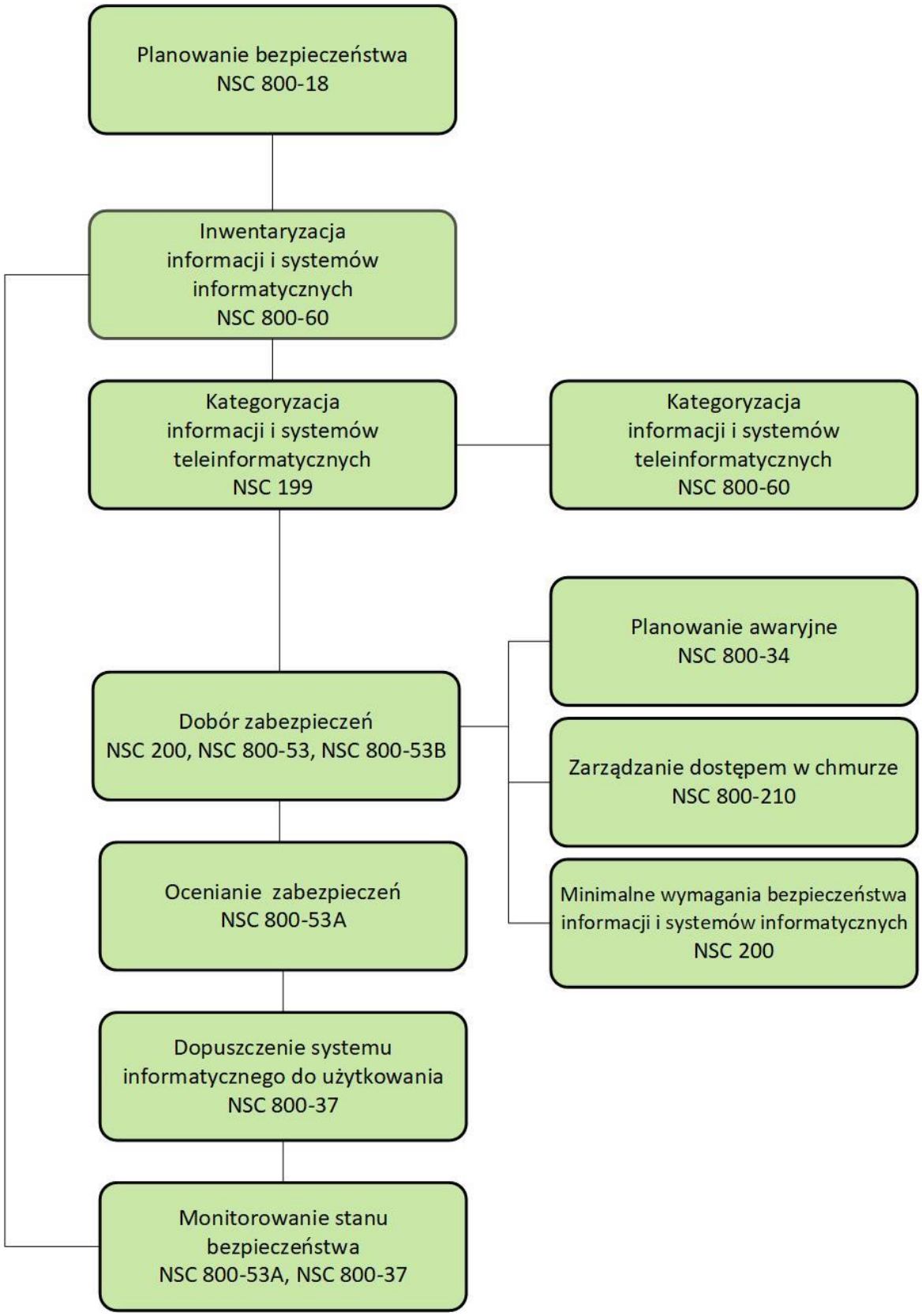
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.
- NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.
- NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych 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 800-34, Poradnik planowania awaryjnego – na podstawie NIST SP 800-34.
- NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.

- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.
- NSC 800-46, *Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD*).- na podstawie NIST SP 800-46.
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60.
- NSC 800-61, Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



Cykl zarządzania bezpieczeństwem informacji

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

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

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

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

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

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

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

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

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

Narodowe Standardy Cyberbezpieczeństwa

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

+48222455922

sekretariat.dc@kprm.gov.pl

Niniejsza publikacja NSC 800-114, ***Poradnik bezpieczeństwa w zakresie telepracy/pracy zdalnej i używania prywatnych urządzeń (BYOD)***, została opracowana za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-114 rev. 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*.

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***.

Raporty dotyczące technologii systemów komputerowych

Laboratorium informatyczne (ITL) w ramach Narodowego Instytutu Standaryzacji i Technologii (NIST) wspiera gospodarkę USA i promuje dobrobyt publiczny poprzez zapewnienie Stanom Zjednoczonym Ameryki wiodącej pozycji w zakresie infrastruktury pomiarowej i normalizacyjnej. ITL opracowuje testy, metody testowe, dane referencyjne, metody wdrożenia koncepcji oraz analizy techniczne w celu przyspieszenia rozwoju i produktywnego wykorzystania technologii informatycznych. Do zadań ITL należy opracowywanie standardów i wytycznych w zakresie zarządzania, administracji, techniki oraz cech fizycznych. Pozwala to zapewnić ekonomiczne rozwiązania w dziedzinie bezpieczeństwa i prywatności przechowywanych w federalnych systemach informacji niezwiązanych z bezpieczeństwem narodowym. Niniejsza publikacja specjalna z serii „800" informuje o badaniach, wytycznych i działaniach ITL w zakresie bezpieczeństwa systemów informacyjnych oraz o współpracy z przemysłem, rządem i organizacjami akademickimi.

Abstrakt

Z systemu telepracy/pracy zdalnej korzysta tysiące osób, wykorzystując do tego celu różne urządzenia, takie jak komputery stacjonarne, laptopy, smartfony czy tablety. Za ich pomocą osoby te odczytują i wysyłają wiadomości e-mail, odwiedzają witryny internetowe, przeglądają i edytują dokumenty oraz wykonują całą gamę innych zadań. Każde urządzenie przeznaczone do telepracy/pracy zdalnej znajduje się w posiadaniu organizacji, osoby trzeciej (np. kontrahentów organizacji, partnerów biznesowych lub sprzedawców) bądź telepracownika. W tym ostatnim przypadku mówimy o przynoszeniu do miejsca pracy własnego urządzenia (*ang. bring your own device — BYOD*). Niniejsza publikacja zawiera zalecenia dotyczące zabezpieczania osobistych urządzeń wykorzystywanych do telepracy i zdalnego dostępu, jak również tych, które są bezpośrednio podłączone do sieci organizacji.

Słowa kluczowe

„wykorzystuj własne urządzenie”[2] (*ang. bring your own device - BYOD*); bezpieczeństwo hosta (*ang. host security*); bezpieczeństwo informacji (*ang. information security*); bezpieczeństwo sieci (*ang. network security*); zdalny dostęp (*ang. remote access*); telepraca (*ang. telework*)

[2] „Przynieś własne urządzenie”.

Spis treści

Streszczenie

Obecnie tysiące osób wykonuje swoje zadania w ramach *telepracy/pracy zdalnej*, pozwalającej pracownikom organizacji, kontrahentom, partnerom biznesowym, sprzedawcom lub innym użytkownikom realizować obowiązki w miejscach innych niż siedziba organizacji. Telepracownicy[3] korzystają z różnych urządzeń, takich jak komputery stacjonarne, laptopy, smartfony czy tablety, w celu odczytywania i wysyłania poczty elektronicznej, odwiedzania stron internetowych, przeglądania i edytowania dokumentów oraz wykonywania wielu innych zadań. Większość telepracowników korzysta ze *zdalnego dostępu*, który umożliwia pracownikom organizacji dostęp do jej niepublicznych zasobów komputerowych z miejsca innego niż jej siedziba. Organizacje mają wiele możliwości zapewnienia zdalnego dostępu, w tym poprzez wirtualne sieci prywatne (*ang. virtual private network - VPN*), systemy zdalnego dostępu (*ang. remote system control*) oraz indywidualny dostęp do aplikacji (np. poczta internetowa - webmail).

Urządzenia do telepracy/pracy zdalnej można podzielić na dwie kategorie: komputery (stacjonarne, laptopy) i urządzenia mobilne (np. smartfony, tablety). Każde urządzenie do telepracy/pracy zdalnej znajduje się w posiadaniu organizacji, telepracownika lub osoby trzeciej, z którą telepracownik ma powiązania (zleceniobiorca, partner biznesowy lub dostawca organizacji). Urządzenia do telepracy/pracy zdalnej należące do użytkownika nazywane są również urządzeniami typu *„bring your own device" (BYOD)*. Niniejsza publikacja zawiera zalecenia dotyczące zabezpieczenia własnych urządzeń wykorzystywanych do telepracy i zdalnego dostępu, jak również podłączanych bezpośrednio do sieci organizacji. Wiele organizacji stosuje ograniczenia w zakresie rodzajów własnych urządzeń, jakich mogą używać pracownicy, a także zasobów, z których mogą one korzystać. Przykładem może być ograniczenie dostępu prywatnych laptopów pracowników jedynie do wąskiego zestawu zasobów lub zezwolenie innym osobistym urządzeniom jedynie na dostęp do poczty internetowej. Dzięki temu organizacje mogą ograniczyć ryzyko, jakie ponoszą

[3] Telepracownik - termin używany zarówno do osoby świadczącej usługę telepracy jak i pracy zdalnej.

w związku z wykorzystywaniem własnych urządzeń przez pracowników. Podczas korzystania ze zdalnego dostępu, urządzenie do telepracy/pracy zdalnej zasadniczo stanowi logiczne przedłużenie sieci organizacji. Tym samym, jeśli takie urządzenie nie jest odpowiednio zabezpieczone, to stwarza dodatkowe ryzyko nie tylko dla informacji, do których telepracownik ma dostęp, ale również dla innych systemów i sieci organizacji. Przykładowo nawiązanie zdalnego dostępu przez urządzenie do telepracy/pracy zdalnej, które jest zainfekowane „robakiem", może spowodować przedostanie się takiego zagrożenia do wewnętrznych komputerów organizacji. Dlatego też urządzenia do telepracy/pracy zdalnej należy odpowiednio zabezpieczać, a także regularnie aktualizować ich systemy bezpieczeństwa.

Przed zastosowaniem jakichkolwiek zaleceń lub sugestii zawartych w niniejszym poradniku użytkownikom zaleca się wykonanie kopii zapasowej wszystkich danych oraz zweryfikowanie jej prawidłowości. Czytelnicy nieposiadający doświadczenia w konfiguracji komputerów, urządzeń mobilnych lub sieci domowych, bądź tacy posiadający w tym zakresie jedynie niewielkie doświadczenie, powinni zasięgnąć porady eksperta przy wdrażaniu zaleceń. Każda konfiguracja urządzenia do telepracy/pracy zdalnej oraz jego środowisko pracy są unikalne. Tym samym zmiana konfiguracji może mieć nieprzewidziane konsekwencje, takie jak utrata danych lub funkcjonalności urządzenia bądź aplikacji.

Wdrożenie poniższych zaleceń powinno pomóc telepracownikom zwiększyć bezpieczeństwo urządzeń wykorzystywanych do telepracy/pracy zdalnej. Warto zaznaczyć, że wdrożenie niektórych proponowanych tu zaleceń może stanowić istotne wyzwanie dla wielu użytkowników. W przypadku braku pewności co do tego, jak wdrożyć takie zalecenia, należy skorzystać z pomocy eksperta.

Przed podjęciem telepracy/pracy zdalnej użytkownicy powinni poznać nie tylko politykę i wymagania organizacji, ale również odpowiednie sposoby ochrony należących do organizacji informacji, do których mogą mieć dostęp.

Informacje wrażliwe przechowywane na urządzeniach do telepracy/pracy zdalnej lub wysyłane z nich muszą być chronione tak, aby nieuprawnione osoby nie mogły uzyskać dostępu do informacji ani ich zmienić. Nieautoryzowane ujawnienie informacji

wrażliwych może naruszyć zaufanie społeczeństwa do organizacji, zagrozić jej misji, a nawet zaszkodzić osobom fizycznym, jeśli doszło do ujawnienia ich danych osobowych. Świadomość tego, jak chronić informacje, do których uzyskujemy dostęp podczas telepracy/pracy zdalnej, nie jest rzeczą oczywistą — sposobów na ochronę informacji jest bowiem naprawdę wiele. Przykłady obejmują zagwarantowanie fizycznego bezpieczeństwa urządzeń do telepracy/pracy zdalnej, szyfrowanie przechowywanych w nich plików oraz zapewnienie, że wykonano kopię zapasową zapisanych w nich informacji.

Telepracownicy wykorzystujący do pracy własne urządzenia powinni upewnić się, że ich sieci domowe oraz wszelkie podłączone do nich urządzenia — korzystające zarówno z łączności przewodowej, jak i bezprzewodowej — są należycie zabezpieczone.

Jednym z ważnych elementów bezpieczeństwa telepracy oraz zdalnego dostępu jest stosowanie zabezpieczeń w komputerach (*ang. personal computer - PC*) i urządzeniach mobilnych korzystających z tych samych przewodowych i bezprzewodowych sieci domowych, z którymi łączy się urządzenie do telepracy/pracy zdalnej. W przypadku zainfekowania takich urządzeń złośliwym oprogramowaniem lub innego naruszenia ich zabezpieczeń może dojść do ataku na urządzenie wykorzystywane do telepracy/pracy zdalnej lub „podsłuchiwania" jego komunikacji z poziomu rzeczonych urządzeń.

Telepracownicy powinni również zachować ostrożność w kwestii zezwalania innym osobom na podłączanie urządzeń do swojej sieci domowej — mogą one stanowić źródło zagrożenia, jeśli doszło do naruszenia ich zabezpieczeń. Telepracownicy powinni stosować środki bezpieczeństwa w sieciach domowych, z którymi łączą się ich urządzenia używane do telepracy/pracy zdalnej. Przykładem takich zabezpieczeń jest zastosowanie routera szerokopasmowego lub sprzętowej zapory sieciowej, które uniemożliwiają komputerom spoza sieci domowej nawiązanie komunikacji z pracującymi w sieci domowej urządzeniami do telepracy/pracy zdalnej. Inną opcją jest zapewnienie, że wrażliwe informacje przesyłane przez bezprzewodową sieć domową są odpowiednio chronione poprzez silne szyfrowanie.

Telepracownicy, którzy używają własnego komputera stacjonarnego lub laptopa do wykonywania telepracy/pracy zdalnej, powinni zabezpieczyć jego system operacyjny i podstawowe aplikacje.

Zabezpieczenie osobistego komputera obejmuje:

- Stosowanie kombinacji oprogramowania zabezpieczającego, takiego jak oprogramowanie antywirusowe, osobiste zapory sieciowe, filtry spamu i treści internetowych oraz blokowanie wyskakujących okienek (*ang. popup*), aby powstrzymać większość ataków, zwłaszcza za pomocą złośliwego oprogramowania.
- Ograniczenie możliwości korzystania z komputera poprzez założenie oddzielnego konta standardowego użytkownika dla każdej osoby, zabezpieczenie każdego konta użytkownika hasłem, używanie kont standardowego użytkownika do codziennego użytku oraz zabezpieczanie sesji użytkowników przed nieuprawnionym dostępem fizycznym.
- Regularne aktualizowanie systemu operacyjnego i podstawowych aplikacji, takich jak przeglądarki internetowe, programy pocztowe, komunikatory internetowe i oprogramowanie zabezpieczające.
- Wyłączenie zbędnych funkcji sieciowych na komputerze i bezpieczna konfiguracja sieci bezprzewodowej.
- Konfiguracja podstawowych aplikacji tak, aby filtrować treści i powstrzymywać inne działania, które mogą mieć złośliwy charakter.
- Instalowanie i używanie tylko znanego i zaufanego oprogramowania.
- Konfiguracja oprogramowania do zdalnego dostępu w oparciu o wymagania i zalecenia organizacji oraz
- Stałe utrzymywanie bezpieczeństwa komputera, np. regularna zmiana haseł i okresowe sprawdzanie stanu oprogramowania zabezpieczającego.

Telepracownicy wykorzystujący własne urządzenia mobilne do wykonywania telepracy/pracy zdalnej powinni zabezpieczyć taki sprzęt zgodnie z zaleceniami producenta urządzenia dotyczącymi bezpieczeństwa.

Istnieje wiele różnych urządzeń mobilnych, a dostępne dla nich funkcje bezpieczeństwa także są mocno zróżnicowane. Niektóre rodzaje sprzętu posiadają jedynie kilka podstawowych funkcji, z kolei inne oferują zaawansowane funkcje podobne do tych dostępnych na komputerach. W tym przypadku, więcej, nie zawsze jednak oznacza lepiej. W rzeczywistości wiele urządzeń oferuje więcej funkcji bezpieczeństwa dlatego, że zapewniane przez nie możliwości (np. sieć bezprzewodowa, komunikatory internetowe) czynią je bardziej podatnymi na ataki w porównaniu do urządzeń pozbawionych takich funkcjonalności. Ogólne zalecenia dotyczące zabezpieczania własnych urządzeń mobilnych są następujące:

- Ograniczenie dostępu do urządzenia, np. ustawienie unikalnego osobistego numeru identyfikacyjnego (*ang. personal identification number - PIN*) lub hasła, które nie jest używane w innych miejscach, oraz automatyczne blokowanie urządzenia po okresie bezczynności.
- Wyłączanie funkcji sieciowych, np. Bluetooth i komunikacji zbliżeniowej (*ang. Near Field Communication - NFC*), ilekroć nie są one niezbędne.
- Pobieranie i instalowanie aktualizacji zabezpieczeń, kiedy są dostępne.
- Konfiguracja aplikacji w celu wspierania bezpieczeństwa (np. blokowanie aktywności, która może mieć złośliwy charakter).
- Pobieranie i uruchamianie programów pochodzących wyłącznie z autoryzowanych sklepów posiadających pozytywne recenzje i dużą liczbę pobrań danej aplikacji.

- Unikanie ingerencji w oprogramowanie urządzenia, takich jak „jailbreak”[4] czy „rootowanie”[5].
- Unikanie podłączania urządzenia do nieznanych stacji ładowania oraz
- W celu uzyskania dostępu do danych i usług organizacji należy korzystać z odizolowanego, chronionego i chronionego kryptograficznie środowiska, które jest wspierane i zarządzane przez organizację.

Telepracownicy powinni unikać telepracy/pracy zdalnej z wykorzystaniem urządzeń klienckich, które nie są kontrolowane przez organizację, samego telepracownika lub organizację z nim powiązaną (kontrahenta, partnera biznesowego, sprzedawcy itp.).

Nierzadko zdarza się, że pracownik próbuje uzyskać zdalny dostęp z nieznanego urządzenia, np. sprawdzić pocztę za pomocą kiosku multimedialnego w hotelu lub telefonu komórkowego znajomego. Niemniej telepracownicy zazwyczaj nie wiedzą, czy takie urządzenia zostały odpowiednio zabezpieczone lub czy nie zostały zaatakowane. Tym samym telepracownik może nieopatrznie skorzystać z urządzenia zainfekowanego złośliwym oprogramowaniem, które wykradnie jego informacje (np. hasła, wiadomości e-mail i inne wrażliwe dane). Wiele organizacji zakazuje używania nieznanych urządzeń do zdalnego dostępu lub zezwala na korzystanie z nich tylko wtedy, gdy pracownik najpierw zrestartuje komputer wraz z podłączeniem do niego specjalnego nośnika wymiennego, który pozwoli na ponowne uruchomienie urządzenia w bezpiecznym środowisku do celów telepracy/pracy zdalnej.

[4] “Jailbreaking” to proces usuwania ograniczeń wprowadzonych przez producenta urządzenia

[5] “Rootowanie” to proces uzyskiwania "dostępu root" do urządzenia.

1. WPROWADZENIE

1.1. Cel i zakres

Niniejsza publikacja ma na celu pomóc telepracownikom zabezpieczyć osobiste sieci i urządzenia wykorzystywane w ramach telepracy/pracy zdalnej, np. należące do nich komputery stacjonarne, laptopy i urządzenia mobilne (np. smartfony, tablety). Dokument koncentruje się w szczególności na bezpieczeństwie telepracy/pracy zdalnej zakładającej zdalny dostęp do niepublicznych zasobów komputerowych organizacji. Przedstawia praktyczne zalecenia dotyczące zabezpieczania systemów operacyjnych (*ang. operating systems - OS*) i aplikacji zainstalowanych na komputerach do telepracy/pracy zdalnej, a także sieci domowych wykorzystywanych przez wspomniane urządzenia. Ponadto w treści poradnika przedstawiono podstawowe zalecenia dotyczące zabezpieczania urządzeń mobilnych wykorzystywanych w telepracy/pracy zdalnej, a także porady dotyczące ochrony informacji przechowywanych na komputerach i nośnikach wymiennych wykorzystywanych do telepracy/pracy zdalnej.

1.2. Odbiorcy docelowi

Niniejszy dokument został stworzony przede wszystkim z myślą o telepracownikach odpowiedzialnych za zapewnianie bezpieczeństwa sieci i urządzeń własnych, z których korzystają w ramach telepracy/pracy zdalnej. Poradnik może być również pomocny dla personelu odpowiedzialnego za bezpieczeństwo informacji oraz innych osób, które mogą wspierać telepracowników przy korzystaniu z ich urządzeń i zdalnego dostępu.

1.3. Struktura dokumentu

Niniejszy dokument przeznaczony jest dla czytelników o różnym poziomie doświadczenia i wiedzy na temat bezpieczeństwa, którzy doświadczają różnych problemów związanych z zabezpieczeniem swoich urządzeń. Jeden czytelnik może przykładowo chcieć zabezpieczyć sieć domową i laptopa, inny zaś — smartfona. Tym samym nie wszystkie rozdziały poradnika mają zastosowanie w każdej sytuacji.

Pozostała część dokumentu podzielona jest na pięć głównych rozdziałów:

- Rozdział 2 zawiera przegląd zagadnień związanych z telepracą i zdalnym dostępem oraz wprowadzenie do kwestii bezpieczeństwa urządzeń do telepracy/pracy zdalnej.
- Rozdział 3 zawiera wytyczne dotyczące zabezpieczania informacji przetwarzanej[6] na urządzeniach stosowanych w telepracy/pracy zdalnej.
- W rozdziale 4 przedstawiono zalecenia dotyczące zabezpieczania przewodowych i bezprzewodowych sieci domowych wykorzystywanych do telepracy/pracy zdalnej.
- W rozdziale 5 omówiono zabezpieczanie osobistych komputerów stacjonarnych (PC) wykorzystywanych do telepracy/pracy zdalnej za pomocą metod takich jak aktualizacje oprogramowania oraz instalacja i konfiguracja oprogramowania antywirusowego i osobistych zapór ogniowych.
- Rozdział 6 zawiera przegląd zabezpieczeń osobistych urządzeń mobilnych używanych w telepracy/pracy zdalnej.
- W rozdziale 7 opisane są względy bezpieczeństwa dotyczące urządzeń osób trzecich.

[6] Przetwarzanie informacji–wszelkie operacje wykonywane w odniesieniu do informacji i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Dokument zawiera również załączniki z materiałami pomocniczymi:

- Załącznik A przedstawia dodatkowe kwestie związane z bezpieczeństwem telepracy/pracy zdalnej, np. w zakresie korzystania z usług telefonicznych (np. telefony komórkowe, usługi telefonii internetowej (*ang. Voice over internet Protocol -VoIP*), korzystanie z technologii bezprzewodowych sieci osobistych (*ang. wireless personal area network - WPAN*), takich jak Bluetooth, czy też korzystanie z bezprzewodowych, szerokopasmowych kart sieciowych, a także bezpieczne niszczenie nośników wymiennych i materiałów drukowanych, które mogą zawierać informacje wrażliwe.
- Załącznik B zawiera słownik wybranych pojęć użytych w publikacji.
- Załącznik C zawiera listę akronimów i skrótów zastosowanych w poradniku.
- Załącznik D zawiera listę źródeł drukowanych publikacji oraz narzędzi i zasobów internetowych, które mogą być pomocne w zabezpieczaniu osobistych urządzeń do telepracy/pracy zdalnej.

2. PRZEGLĄD TECHNOLOGII TELEPRACY/PRACY ZDALNEJ

Obecnie cała rzesza osób wykonuje swoje obowiązki w ramach *telepracy/pracy zdalnej*. Dzięki niej pracownicy, kontrahenci, partnerzy biznesowi, sprzedawcy lub inni użytkownicy mogą wykonywać zadania w miejscu innym niż siedziba organizacji, dla której pracują. Telepracownicy korzystają z różnych urządzeń, np. komputerów stacjonarnych, laptopów, smartfonów i tabletów, do odczytywania i wysyłania poczty elektronicznej, odwiedzania stron internetowych, przeglądania i edytowania dokumentów oraz wykonywania wielu innych zadań. W ramach swojej pracy większość telepracowników korzysta ze *zdalnego dostępu*, który umożliwia użytkownikom organizacji dostęp do jej niepublicznych zasobów komputerowych z miejsc innych niż jej siedziba.

Niniejszy rozdział zawiera przegląd technologii wykorzystywanych w telepracy/pracy zdalnej. Omawia on powszechnie stosowane metody zdalnego dostępu, a także konieczność zabezpieczania urządzeń do telepracy/pracy zdalnej, np. laptopów i smartfonów.

2.1. Metody zdalnego dostępu

Organizacje mają do dyspozycji wiele możliwości zapewnienia zdalnego dostępu do swoich zasobów komputerowych. W odniesieniu do telepracowników najczęściej stosuje się następujące opcje:

- **Wirtualna sieć prywatna (VPN).** VPN to bezpieczny „tunel", który łączy urządzenie telepracownika z siecią organizacji. Po ustanowieniu połączenia poprzez wspomniany tunel, telepracownik może za jego pośrednictwem uzyskać dostęp do zasobów obliczeniowych organizacji. Do telepracy/pracy zdalnej najczęściej wykorzystuje się następujące rodzaje sieci VPN:

- **Internet Protocol Security (IPsec) VPN.** IPsec VPN może zapewnić telepracownikom dostęp do wielu różnych rodzajów zasobów, takich jak aplikacje, serwery plików i drukarki. Korzystanie z IPsec VPN wymaga zainstalowania i skonfigurowania oprogramowania klienta IPsec na każdym urządzeniu telepracownika. Konieczne może być również zainstalowanie odpowiednich aplikacji, np. edytora tekstów do przeglądania i edycji dokumentów. Ze względu na konieczność instalacji i konfiguracji oprogramowania, dostęp do sieci IPsec VPN jest najczęściej możliwy tylko za pośrednictwem komputerów należących do organizacji i wydanych przez nią pracownikowi. Niektóre organizacje zezwalają telepracownikom na instalowanie klientów IPsec VPN na ich własnych komputerach i urządzeniach przenośnych. Oprogramowanie klienckie jest często wstępnie konfigurowane przez organizację i dostarczane personelowi. W innym przypadku telepracownik może skonfigurować klienta IPsec VPN zainstalowanego na swoim urządzeniu lub nabyć, zainstalować i skonfigurować klienta innej firmy.
- **Secure Sockets Layer (SSL) VPN.** Rolą niektórych SSL VPN jest głównie zapewnianie dostępu do aplikacji internetowych za pośrednictwem standardowych przeglądarek internetowych. Inne są z kolei bardzo podobne do IPsec VPN i mogą zapewniać dostęp do wielu typów aplikacji — tego typu rozwiązania VPN zazwyczaj wymagają jednak od użytkowników zainstalowania dodatkowego oprogramowania.

- **System zdalnego dostępu. P**ozwala telepracownikowi na zdalne korzystanie z komputera znajdującego się w siedzibie organizacji za pomocą urządzenia do telepracy/pracy zdalnej. Na zdalnym komputerze zainstalowane jest oprogramowanie, które telepracownik musi uruchomić, np. oprogramowanie biurowe (edytory tekstu, arkusze kalkulacyjne itp.) oraz aplikacje unikatowe dla danej organizacji. Najczęściej wykorzystywaną metodą systemu zdalnego dostępu w telepracy/pracy zdalnej jest dostęp do serwera terminali, który umożliwia każdemu telepracownikowi korzystanie z odrębnego, standardowego wirtualnego pulpitu.[7] Dostęp do serwera terminali wymaga od telepracownika zainstalowania specjalnej aplikacji klienckiej na urządzeniu do telepracy/pracy zdalnej lub użycia interfejsu internetowego, często z wykorzystaniem wtyczki (*ang. plug-in*) do przeglądarki lub innego dodatkowego oprogramowania dostarczanego przez organizację. Do podobnych metod należy infrastruktura pulpitu wirtualnego (*ang. virtual desktop infrastructure - VDI*), która dostarcza użytkownikom wirtualne obrazy systemów operacyjnych. Inną metodą, będącą zasadniczo rozwiązaniem VDI dla smartfonów i tabletów, jest wirtualna infrastruktura mobilna (*ang. virtual mobile infrastructure - VMI*).
- **Dostęp do indywidualnych aplikacji.** Telepracownik może uzyskać zdalny dostęp do pojedynczej aplikacji. Zazwyczaj jest to aplikacja internetowa, np. poczta elektroniczna. Taki rodzaj dostępu zwykle wymaga jedynie zainstalowania przeglądarki internetowej na urządzeniu telepracownika, toteż w większości przypadków nie ma potrzeby ponownego konfigurowania urządzenia lub instalowania na nim oprogramowania przed uzyskaniem dostępu do aplikacji.

[7] Rzadziej stosowaną metodą jest zdalny dostęp do pulpitu. Funkcja ta umożliwia telepracownikowi dostęp do konkretnego pulpitu w organizacji, najczęściej do komputera danego pracownika w jej biurze. Rozwiązania polegające na zdalnym dostępie do pulpitu mogą być trudniejsze do zabezpieczenia i utrzymania niż takie oparte na dostępie do serwera terminali (np. narażenie komputerów wewnętrznych na złośliwe oprogramowanie z urządzeń zewnętrznych). Dlatego też wiele organizacji nie zezwala na zdalny dostęp do pulpitu z urządzeń niebędących pod kontrolą organizacji.

Telepracownicy mogą uzyskać dostęp do internetu na wiele sposobów, w tym za pomocą sieci szerokopasmowych (np. modem kablowy, bezprzewodowa sieć szerokopasmowa), sieci komórkowych, bezprzewodowych hotspotów i sieci innych organizacji. Do celów niniejszej publikacji metoda dostępu wykorzystywana przez telepracownika nie ma znaczenia — uwaga skupia się tutaj na wszelkich specjalnych względach związanych z konkretnym sposobem dostępu.

Większość zasobów obliczeniowych udostępnianych zdalnie jest dostępna tylko dla użytkowników organizacji. Przed uzyskaniem dostępu do nich użytkownicy muszą potwierdzić swoją tożsamość, np. za pomocą nazwy użytkownika i hasła lub za pomocą poświadczeń z inteligentnej karty weryfikacji tożsamości osobistej (*ang. Personal Identity Verification - PIV*) lub pochodnych poświadczeń PIV (ang. derived PIV credentials). Wiele rozwiązań w zakresie zdalnego dostępu wymaga od telepracowników wielokrotnego uwierzytelnienia. Przykładowo od telepracownika może być wymagane uwierzytelnienie w celu skorzystania z sieci VPN, a następnie kolejne, by zalogować się do poszczególnych aplikacji dostępnych przez sieć VPN. Organizacje nierzadko posiadają odrębne systemy uwierzytelniania dla zdalnego dostępu. Tym samym często zdarza się, że telepracownik otrzymuje token sprzętowy i w celu uwierzytelnienia musi wprowadzić wygenerowany przez niego kod w komputerze. Wiele organizacji wymaga również od telepracowników okresowego ponownego uwierzytelnienia podczas długich sesji zdalnego dostępu, np. po każdych ośmiu godzinach sesji lub po 30 minutach bezczynności. Takie opcje uwierzytelniania pomagają organizacjom potwierdzić, że osoba korzystająca ze zdalnego dostępu rzeczywiście jest do tego upoważniona.

Większość technologii zdalnego dostępu, a także spora część aplikacji, umożliwia automatyczne szyfrowanie prowadzonej komunikacji. Uniemożliwia to osobom atakującym za pośrednictwem internetu i innych sieci podsłuchiwanie komunikacji lub manipulowanie nią. Szczegółowy opis kwestii ochrony komunikacji leży poza zakresem niniejszej publikacji.

Telepracownikom zaleca się skonsultowanie ze swoją organizacją w zakresie wykorzystywanego sposobu ochrony komunikacji. Pozwoli to uniknąć nieumyślnego przekazania wrażliwych informacji przez sieci bez odpowiedniej ochrony.

2.2. Urządzenia do telepracy/pracy zdalnej

Urządzenia do telepracy/pracy zdalnej można podzielić na dwie ogólne kategorie:

- **Komputery osobiste (PC), czyli komputery stacjonarne i laptopy**. Komputery osobiste działają w oparciu o systemy takie jak Windows, Apple OS X i Linux. W przypadku tego rodzaju urządzeń można wykorzystywać każdą z metod zdalnego dostępu opisanych w punkcie 2.1.
- **Urządzenia mobilne**, czyli małe komputery przenośne — np. smartfony i tablety. Urządzenia mobilne najczęściej wykorzystują metody zdalnego dostępu oparte na przeglądarkach internetowych, przede wszystkim SSL VPN oraz dostęp do indywidualnych aplikacji internetowych.

Różnica między „pecetami" a urządzeniami mobilnymi stale się zmniejsza. Te drugie oferują coraz więcej funkcji, które dotychczas dostępne były tylko na komputerach osobistych. Niemniej na dzień opracowania niniejszej publikacji mechanizmy zarządzania bezpieczeństwem, które dostępne są na komputerach PC, znacząco różnią się od tych stosowanych w rozwiązaniach mobilnych. Dlatego też w treści poradnika przedstawiono odrębne zalecenia dla komputerów osobistych i urządzeń mobilnych, ilekroć ma to zastosowanie.

Kolejny zestaw kategorii użytych w zaleceniach dotyczy podmiotu odpowiedzialnego za bezpieczeństwo urządzenia do telepracy/pracy zdalnej. Wspomniane kategorie to:

- **Urządzenia organizacji (***ang. Corporate-owned Personally-Enabled – COPE)*. Urządzenia do telepracy/pracy zdalnej w tej kategorii są zazwyczaj nabywane, konfigurowane i kontrolowane przez organizację. Na takich urządzeniach można wykorzystywać każdą z metod zdalnego dostępu stosowanych przez organizację.

- **Urządzenia należące do osób trzecich.** Takie urządzenia do telepracy/pracy zdalnej są kontrolowane przez osobę trzecią, zwykle taką, która zatrudnia telepracownika w imieniu organizacji (np. jeden z kontrahentów, partnerów biznesowych lub sprzedawców). Ostateczną odpowiedzialność za zabezpieczenie urządzeń do telepracy/pracy zdalnej i utrzymanie ich bezpieczeństwa ponosi osoba trzecia. Na tego rodzaju urządzeniach zazwyczaj można wykorzystywać wiele metod zdalnego dostępu stosowanych przez organizację lub nawet wszystkie z nich.
- **Urządzenia prywatne używane do wykonywania pracy (BYOD).** Wszystkie urządzenia nienależące do organizacji i zarządzane przez samych telepracowników nazywane są urządzeniami typu *BYOD (ang. Bring Your Own Device)*[8]. Na tego rodzaju urządzeniach zazwyczaj można wykorzystywać wiele metod zdalnego dostępu stosowanych przez organizację lub nawet wszystkie z nich.
- **Urządzenia nieznane.** Pozostałe urządzenia określa się jako „nieznane", gdyż nie ma pewności co do ich bezpieczeństwa — znajdują się bowiem pod kontrolą innych osób i stanowią ich własność. Mogą to być np. kioski multimedialne w hotelach, komputery PC lub urządzenia przenośne należące do przyjaciół lub członków rodziny. Opcje zdalnego dostępu z poziomu takich urządzeń są zazwyczaj dość ograniczone, ponieważ użytkownicy nie mogą lub nie powinni instalować na nich oprogramowania organizacji, np. oprogramowania VPN, oprogramowania serwera terminali lub wtyczek do przeglądarki internetowej. Korzystanie z nich jest niezwykle ryzykowne ze względu na brak pewności co do ich bezpieczeństwa. Z tego względu wiele organizacji zakazuje korzystania z nieznanych urządzeń do telepracy/pracy zdalnej, albo też zezwala

[8] Ściśle rzecz ujmując, urządzenia BYOD można wykorzystywać wewnątrz organizacji bez używania ich do telepracy lub zdalnego dostępu. Niemniej zdecydowana większość takich urządzeń jest używana na zewnątrz, toteż do celów niniejszej publikacji wszystkie urządzenia BYOD uważa się za urządzenia do telepracy/pracy zdalnej. Obawy związane z bezpieczeństwem prywatnych urządzeń używanych wyłącznie wewnątrz organizacji zasadniczo nie różnią się od tych występujących w odniesieniu do własnych urządzeń stosowanych przez pracowników do telepracy/pracy zdalnej.

na korzystanie z nich tylko pod warunkiem, że użytkownik najpierw zrestartuje komputer z podłączonym do niego specjalnym nośnikiem wymiennym, który uruchamia urządzenie w bezpiecznym środowisku do celów telepracy/pracy zdalnej.

Z wielu względów, w tym z uwagi na politykę bezpieczeństwa i ograniczenia technologiczne, organizacje często ograniczają rodzaje urządzeń, jakich pracownik może używać do zdalnego dostępu. Przykładowo organizacja może zezwolić na wykorzystanie wyłącznie jej własnych komputerów PC i urządzeń mobilnych. Niektóre organizacje stosują podział na poziomy dostępu, np. komputer firmowy może mieć dostęp do wielu zasobów, prywatny komputer pracownika — do nieco bardziej ograniczonego zestawu zasobów, a prywatne urządzenie mobilne pracownika — tylko do jednego lub dwóch zasobów, takich jak poczta internetowa. W ten sposób organizacja może ograniczyć ponoszone ryzyko, zezwalając na najszerszy dostęp urządzeniom, nad którymi ma największą kontrolę, jednocześnie ograniczając do minimum lub całkowicie blokując dostęp z poziomu niekontrolowanych przez nią urządzeń.

Przed użyciem prywatnego urządzenia telepracownik powinien skonsultować się ze swoją organizacją w celu potwierdzenia, że jest to dopuszczalne.
Telepracownicy powinni również mieć świadomość, że wiele organizacji okresowo dokonuje ponownej oceny swojej polityki dotyczącej narzędzi do telepracy/pracy zdalnej i może zmienić rodzaje urządzeń, w przypadku których jest ona dopuszczalna. Dlatego też telepracownicy powinni upewnić się, że zapoznali się z aktualnymi informacjami dotyczącymi urządzeń do zdalnego dostępu.

2.3. Przegląd zabezpieczeń urządzeń do telepracy/pracy zdalnej

W dzisiejszym środowisku obliczeniowym istnieje wiele zagrożeń dla urządzeń telepracy. Ich źródłem są osoby motywowane przez różne powody, w tym chęć wywołania zamieszania i zakłóceń w pracy bądź dokonania kradzieży tożsamości lub innych oszustw. Telepracownicy mogą zwiększyć bezpieczeństwo swoich urządzeń, aby zapewnić lepszą ochronę przed takimi niebezpieczeństwami.

Podstawowym zagrożeniem dla większości urządzeń do telepracy/pracy zdalnej jest złośliwe oprogramowanie (*ang. malware*). *Złośliwe oprogramowanie*, znane również jako *złośliwy kod (ang. malicious code)*, to program komputerowy potajemnie umieszczany na urządzeniu z zamiarem naruszenia poufności, integralności lub dostępności danych urządzenia, aplikacji lub systemu operacyjnego. Typowe rodzaje złośliwego oprogramowania to wirusy, „robaki", złośliwy kod mobilny, konie trojańskie, rootkity, oprogramowanie szpiegujące i boty.[9] Złośliwe oprogramowanie może infekować urządzenia na wiele sposobów, w tym za pośrednictwem poczty elektronicznej, stron internetowych, pobieranych i udostępnianych plików, oprogramowania peer to peer, komunikatorów internetowych i mediów społecznościowych. Innym częstym zagrożeniem dla urządzeń do telepracy/pracy zdalnej jest utrata lub kradzież urządzenia. Osoba posiadająca fizyczny dostęp do urządzenia może spróbować przejrzeć lub skopiować przechowywane na nim informacje na wiele różnych sposobów.

Zabezpieczenia, zwane również *środkami bezpieczeństwa*, to środki przeciwko zagrożeniom, które mają na celu zniwelowanie luk w zabezpieczeniach urządzenia, zwanych również *podatnościami*. Czyhające na urządzenie cyberzagrożenia będą próbowały wykorzystać takie luki. Niektóre podatności można wyeliminować za pomocą odpowiednich zabezpieczeń, np. funkcji automatycznego pobierania i instalowania nowych wersji aplikacji, zawierających poprawki usuwające wcześniejsze błędy. W przypadku istnienia luk niemożliwych do wyeliminowania, zabezpieczenia mogą uniemożliwić ich wykorzystanie, np. oprogramowanie antywirusowe może powstrzymać użytkownika przed otwarciem zainfekowanej wiadomości e-mail, a szyfrowanie dysku twardego pozwoli zapewnić, że plików nie może odczytać inna osoba. Jednocześnie jednak, bez względu na ilość zastosowanych zabezpieczeń, zapewnienie stuprocentowej ochrony przed atakami jest zwyczajnie niemożliwe ze względu na złożoną naturę informatyki. Bardziej realistycznym celem jest tutaj zastosowanie takich zabezpieczeń, które dadzą atakującemu jak najmniej okazji

[9] Więcej informacji na temat złośliwego oprogramowania znajduje się w punkcie 5.4.1.

do uzyskania dostępu do urządzenia lub uszkodzenia jego oprogramowania czy zapisanych na nim informacji.

Umożliwienie telepracownikom zdalnego dostępu do zasobów komputerowych przez organizację daje atakującym dodatkowe możliwości naruszenia jej bezpieczeństwa. Urządzenie do telepracy/pracy zdalnej korzystające ze zdalnego dostępu zasadniczo stanowi przedłużenie własnej sieci organizacji. Dotyczy to także sytuacji, gdy urządzenie BYOD jest bezpośrednio podłączone do sieci lokalnej organizacji. Dlatego też, jeśli urządzenie do telepracy/pracy zdalnej nie jest odpowiednio zabezpieczone, to wówczas stwarza dodatkowe ryzyko nie tylko dla informacji, do których telepracownik ma dostęp, ale również dla innych systemów i sieci organizacji. Przykładowo zainfekowane „robakiem" urządzenie do telepracy/pracy zdalnej może rozprzestrzenić takie złośliwe oprogramowanie do wewnętrznych komputerów organizacji za pośrednictwem zdalnego dostępu. Urządzenia do telepracy/pracy zdalnej powinny być zatem odpowiednio zabezpieczone, a ich zabezpieczenia należy regularnie aktualizować.

Wiele organizacji stosuje mechanizmy automatycznej kontroli zabezpieczeń każdego urządzenia do telepracy/pracy zdalnej próbującego uzyskać zdalny dostęp, aby upewnić się, że jest ono zgodne z ich polityką. Taka kontrola może obejmować np. sprawdzenie, czy zainstalowano wszystkie poprawki do systemu operacyjnego komputera, weryfikację, czy oprogramowanie antywirusowe jest zainstalowane i aktualne, potwierdzenie uruchomienia osobistej zapory sieciowej bądź sprawdzenie, czy oprogramowanie smartfona nie zostało naruszone poprzez „rooting" lub „jailbreak". Niektóre rozwiązania zdalnego dostępu mogą również określić, czy urządzenie zostało zabezpieczone przez organizację, a także zidentyfikować jego typ (np. komputer stacjonarny/laptop, smartfon, tablet). Na podstawie wyników takiej kontroli organizacja może określić, czy dane urządzenie powinno być dopuszczone do korzystania ze zdalnego dostępu.

Pozostała część niniejszej publikacji zawiera zalecenia w zakresie zabezpieczania urządzeń do telepracy/pracy zdalnej. Dotyczą one zapewnienia bezpieczeństwa komputerów i urządzeń mobilnych oraz sieci wykorzystywanych przez urządzenia

do telepracy/pracy zdalnej, jak również ochrony informacji przechowywanych na urządzeniach do telepracy/pracy zdalnej i wysyłanych z nich. Poradnik określa również wskazówki dotyczące oceny bezpieczeństwa nieznanych urządzeń, tak aby telepracownicy mogli zdecydować, czy powinni wykorzystywać je do celów zdalnego dostępu.

3. ZABEZPIECZANIE INFORMACJI

Informacje wrażliwe, takie jak dane identyfikacyjne (np. akta osobowe, medyczne, finansowe),[10] które są przechowywane na urządzeniach do telepracy/pracy zdalnej lub wysyłane z nich, muszą być chronione w taki sposób, aby nieupoważnione osoby nie mogły uzyskać do nich dostępu lub dokonać ich zmiany. Nieuprawnione ujawnienie informacji wrażliwych może naruszyć zaufanie społeczeństwa do organizacji, zagrozić jej misji, a nawet zaszkodzić osobom fizycznym, jeśli doszło do ujawnienia ich danych.

Przed podjęciem telepracy/pracy zdalnej użytkownicy powinni zapoznać się z polityką i wymaganiami swojej organizacji oraz odpowiednimi sposobami ochrony informacji będących w jej posiadaniu. Świadomość tego, jak chronić takie informacje nie jest rzeczą oczywistą — sposobów na ich ochronę jest bowiem naprawdę wiele. Z tego względu organizacje mogą oczekiwać lub wymagać od telepracowników stosowania metod takich jak:

- **Fizyczne zabezpieczenie** urządzeń do telepracy/pracy zdalnej i nośników wymiennych. Przykładowo organizacja może wymagać, aby nie pozostawiać laptopów bez nadzoru, gdy są zabierane do hoteli, na konferencje lub w inne miejsca, gdzie osoby trzecie mogą łatwo uzyskać fizyczny dostęp do nich. Organizacja może również wprowadzić wymagania dotyczące fizycznych zabezpieczeń w zakresie dokumentów papierowych i innych nośników niekomputerowych, które zawierają wrażliwe informacje i są zabierane poza teren organizacji.

[10] Dla zainteresowanych - dokument „OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*", definiuje dane identyfikacyjne (*ang. personally identifiable information, PII*) jako "wszelkie informacje o osobie przechowywane przez agencję, w tym m.in. informacje o wykształceniu, transakcjach finansowych, historii medycznej, informacje o karalności lub historii zatrudnienia oraz informacje, które mogą być wykorzystane do określenia lub śledzenia tożsamości osoby, takie jak jej imię i nazwisko, numer ubezpieczenia społecznego, data i miejsce urodzenia, nazwisko panieńskie matki, dane biometryczne itp., łącznie z wszelkimi innymi danymi osobowymi, które są powiązane lub możliwe do powiązania z daną osobą". Pełna treść ww. dokumentu dostępna jest pod adresem: http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf.

- **Szyfrowanie plików przechowywanych na urządzeniach do telepracy/pracy zdalnej i nośnikach wymiennych,** takich jak płyty CD i pendrive'y. Zapobiega to łatwemu uzyskaniu przez atakujących dostępu do informacji zawartych w plikach. Istnieje wiele możliwości ochrony plików tą metodą, w tym szyfrowanie pojedynczych plików lub folderów, a także całych woluminów i dysków twardych. Zastosowanie metody szyfrowania do ochrony plików wymaga również zastosowania mechanizmu uwierzytelniania (np. hasła) w celu odszyfrowania plików w razie potrzeby.
- **Tworzenie kopii zapasowych informacji przechowywanych na urządzeniach do telepracy/pracy zdalnej.** Jeżeli z urządzeniem stanie się coś złego, np. na skutek awarii sprzętu, oprogramowania lub zasilania bądź nastania klęski żywiołowej, przechowywane na nim informacje zostaną utracone, chyba że skopiowano je na inne urządzenie lub nośnik wymienny. Niektóre organizacje zezwalają telepracownikom na tworzenie kopii zapasowych plików lokalnych w scentralizowanym systemie (np. poprzez zdalny dostęp VPN). Inne zaś zalecają telepracownikom wykonywanie lokalnych kopii zapasowych (np. nagrywanie płyt CD, kopiowanie plików na nośniki wymienne). Telepracownicy powinni wykonywać kopie zapasowe zgodnie z wytycznymi organizacji i weryfikować czy sporządzono je prawidłowo i czy są kompletne.[11] Ważne jest, aby kopie zapasowe na nośnikach wymiennych były zabezpieczone co najmniej tak dobrze, jak urządzenie, na którym są przechowywane. Jeżeli komputer trzymamy w zamkniętym pomieszczeniu, to nośnik również powinien znajdować się w zabezpieczonym miejscu. Jeżeli zaś na komputerze przechowujemy dane w sposób zaszyfrowany, to ich kopie zapasowe również należy zaszyfrować.

[11] Sprawdzanie poprawności i kompletności kopii zapasowych jest niezwykle ważne — jeżeli kopia jest niekompletna lub wykonano ją nieprawidłowo, może dojść do utraty informacji. Niektóre programy do tworzenia kopii zapasowych oferują funkcje pozwalające sprawdzić kopię zapasową pod kątem jej prawidłowości. W przypadku wykonywania prostych kopii zapasowych, np. kopiowania plików na nośnik wymienny, telepracownik może dokonać sprawdzenia kopii poprzez próbę otwarcia wybranych plików z nośnika. Telepracownicy mogą również przetestować proces przywracania kopii zapasowej,

- **Niszczenie informacji, gdy nie są już potrzebne.** Przykładem może być usuwanie plików należących do organizacji z komputerów wycofywanych z eksploatacji. Niektóre metody zdalnego dostępu umożliwiają usuwanie podstawowych informacji, np. czyszczenie pamięci podręcznej przeglądarki internetowej, która może zawierać wrażliwe informacje. Jednakże bardziej kompleksowe oczyszczanie wymaga zwykle użycia szczególnych narzędzi, takich jak specjalnie zaprojektowany program do oczyszczania dysku, wymazujący z urządzenia wszystkie pozostałości informacji. Wiele organizacji oferuje swoim telepracownikom pomoc w usuwaniu informacji z prywatnych urządzeń. Innym przykładem niszczenia informacji może być niszczenie papierowych dokumentów zawierających wrażliwe informacje dotyczące telepracy/pracy zdalnej, gdy nie są już potrzebne.
- **Zdalne wymazywanie informacji z zaginionych urządzeń.** W przypadku zgubienia lub kradzieży smartfona lub tabletu, jego zawartość może zostać zdalnie wymazana przez organizację lub jej dostawcę usług, szczególnie jeżeli urządzenie jest podłączone do sieci komórkowej. Wymazanie zawartości uniemożliwia osobie niepożądanej uzyskanie jakichkolwiek informacji z urządzenia. Dostępność tej funkcji zależy od możliwości produktu i dostawcy jego usług sieciowych.

Wymagana kombinacja mechanizmów ochrony może różnić się w zależności od przypadku: organizacja może wymagać jednej kombinacji w przypadku dostępu za pomocą SSL VPN z prywatnego komputera, a innej w przypadku dostępu do indywidualnych aplikacji z prywatnego urządzenia mobilnego. Telepracownicy powinni stosować się do wymagań i zaleceń swojej organizacji w zakresie ochrony informacji wrażliwych, do których mają dostęp za pomocą urządzeń do telepracy/pracy zdalnej. Niektóre organizacje stosują te same wymagania i zalecenia w odniesieniu

np. przywracając ją na inny komputer lub dokonując przywrócenia plików z kopii zapasowej do osobnego folderu testowego. Telepracownicy powinni zachować ostrożność podczas testowania takich funkcji, aby uniknąć niezamierzonego nadpisania aktualnych informacji na urządzeniu. Powinni oni także zapoznać się z dokumentacją procesu tworzenia kopii zapasowych, aby określić, jak należy weryfikować prawidłowość utworzonych kopii.

do wszystkich rodzajów informacji ze względu na trudności w rozróżnieniu informacji wrażliwych i niewrażliwych. Telepracownicy muszą również zadbać o odpowiednią ochronę swoich środków uwierzytelniających wykorzystywanych do zdalnego dostępu, takich jak hasła, osobiste numery identyfikacyjne (PIN) i tokeny sprzętowe. Takich środków uwierzytelniających nie należy przechowywać wraz z urządzeniem do telepracy/pracy zdalnej. Nie należy również przechowywać wielu tego rodzaju środków w jednym miejscu (np. hasła lub kodu PIN nie należy zapisywać na odwrocie tokena sprzętowego).

Telepracownicy powinni również wiedzieć, jak postępować w przypadku zagrożeń związanych z *socjotechniką*. Tym stosunkowo ogólnym terminem określa się działania nieuprawnionych osób mające na celu podstępem nakłonić nieświadome ofiary do ujawnienia wrażliwych informacji lub wykonania pewnych czynności, np. pobrania i wykonania pliku, który wydaje się nieszkodliwy, ale w rzeczywistości zawiera złośliwe oprogramowanie. Przykładowo atakujący może podejść do telepracownika w kawiarni i poprosić o chwilowe skorzystanie z komputera lub zaoferować pomoc w jego obsłudze. Telepracownicy powinni zachować ostrożność wobec wszelkich próśb o dostęp do urządzenia do telepracy/pracy zdalnej, które mogą prowadzić do naruszenia jego bezpieczeństwa lub kradzieży. Telepracownicy powinni zwrócić się do przełożonego o przeprowadzenie szkolenia dotyczącego rozpoznawania i radzenia sobie z atakami z użyciem socjotechniki, jeśli w nim jeszcze nie uczestniczyli.

Jeżeli telepracownik podejrzewa, że doszło do naruszenia bezpieczeństwa (w tym utraty lub kradzieży materiałów) w odniesieniu do urządzenia do telepracy/pracy zdalnej, środków zdalnego dostępu, nośników wymiennych lub innych elementów środowiska telepracy/pracy zdalnej, powinien niezwłocznie zastosować się do polityki i procedur organizacji dotyczących zgłaszania możliwego naruszenia. Jest to szczególnie ważne, jeżeli którykolwiek z elementów telepracy/pracy zdalnej zawiera informacje wrażliwe, takie jak dane identyfikacyjne, aby zminimalizować potencjalne skutki naruszenia bezpieczeństwa. W przypadku pytań lub wątpliwości dotyczących bezpieczeństwa telepracy/pracy zdalnej telepracownicy powinni również kontaktować się z odpowiednimi osobami w organizacji.

4. ZABEZPIECZANIE SIECI DOMOWYCH I KORZYSTANIE Z INNYCH SIECI

Ważnym elementem bezpieczeństwa telepracy i zdalnego dostępu jest stosowanie środków bezpieczeństwa w sieciach domowych, z którymi zwykle łączy się urządzenie do telepracy/pracy zdalnej.[12] Istotną kwestią w zakresie bezpieczeństwa sieci domowej jest zabezpieczenie innych podłączonych do niej komputerów i urządzeń mobilnych. Jeżeli dowolne z tych urządzeń zostanie zainfekowane złośliwym oprogramowaniem lub w inny sposób narażone na niebezpieczeństwo, to wówczas może ono zostać wykorzystane do zaatakowania urządzenia do telepracy/pracy zdalnej lub „podsłuchiwania" jego komunikacji. Telepracownicy powinni upewnić się, że wszystkie urządzenia pracujące w ich sieci domowej są odpowiednio zabezpieczone. Ponadto telepracownicy powinni również zachować ostrożność w kwestii zezwalania osobom trzecim na podłączanie urządzeń do swoich domowych sieci przewodowych lub bezprzewodowych — takie urządzenia mogą stanowić źródło zagrożenia, jeśli doszło do naruszenia ich zabezpieczeń. Telepracownicy muszą być również świadomi ryzyka związanego z korzystaniem z sieci zewnętrznych oraz procedur podłączania urządzeń do telepracy/pracy zdalnej, w tym urządzeń prywatnych, do sieci należących do organizacji.

W punktach 4.1 i 4.2 przedstawiono zalecenia dotyczące zabezpieczania przewodowych i bezprzewodowych sieci domowych. Punkt 4.3 zawiera krótkie omówienie implikacji dla bezpieczeństwa związanych z wykonywaniem telepracy/pracy zdalnej za pośrednictwem sieci zewnętrznych. Wdrożenie niektórych zaleceń proponowanych w punktach 4.1–4.3 może stanowić istotne wyzwanie dla wielu użytkowników. W przypadku braku pewności co do tego, jak wdrożyć takie zalecenia, należy skorzystać z pomocy eksperta. Wreszcie w punkcie 4.4 omówiono kwestie dotyczące podłączania urządzeń prywatnych do sieci należących do organizacji.

[12] Niektóre urządzenia do telepracy/pracy zdalnej, np. smartfony i laptopy z bezprzewodowymi kartami sieciowymi, mogą pracować bez połączenia z siecią domową.

4.1. Domowe sieci przewodowe

Telepracownicy powinni zabezpieczyć swoje przewodowe sieci domowe w celu ochrony urządzeń wykorzystywanych do telepracy/pracy zdalnej. Podstawą zabezpieczenia większości przewodowych sieci domowych jest maksymalne odseparowanie sieci domowej od dostawcy usługi dostępu do internetu. Jeżeli urządzenie do telepracy/pracy zdalnej łączy się bezpośrednio z infrastrukturą dostawcy świadczącego usługi dostępu do internetu telepracownikowi, np. poprzez podłączenie urządzenia bezpośrednio do modemu kablowego, wówczas urządzenie staje się bezpośrednio dostępne z sieci internet i jest bardzo narażone na atak. Aby temu zapobiec, sieć domowa powinna posiadać urządzenie zabezpieczające umieszczone pomiędzy infrastrukturą dostawcy a urządzeniem do telepracy/pracy zdalnej. Takie zabezpieczenie najczęściej stanowi router szerokopasmowy (np. modem kablowy z routerem) lub sprzętowa zapora sieciowa.[13] Tego typu urządzenie zabezpieczające powinno być skonfigurowane tak, aby uniemożliwiać komputerom spoza sieci domowej nawiązanie komunikacji z jakimkolwiek podłączonym do niej urządzeniem, włącznie z tym wykorzystywanym do telepracy/pracy zdalnej.[14] W celu zapewnienia dodatkowego zabezpieczenia sprzętową zaporę sieciową, router szerokopasmowy lub inne podobne rozwiązanie należy zastosować nawet wówczas, gdy każde urządzenie posiada osobistą zaporę

[13] Sprzętowych zapór sieciowych (*ang. firewall appliance*) nie należy mylić z opartą na oprogramowaniu osobistą zaporą sieciową (*ang. personal firewall*) — te pierwsze są odrębnymi, fizycznymi urządzeniami. Sprzętowe zapory sieciowe używane na potrzeby sieci domowych nie stanowią tak solidnej bariery, jak te stosowane przez organizacje (np. dzięki funkcji *stateful inspection* — analizie stanu połączeń). Mają one za zadanie zapewnić dodatkowe zabezpieczenie poprzez zmniejszenie liczby ataków, jakie są w stanie przedostać się do komputerów w sieci domowej.

[14] Niektóre zapory sieciowe zapewniają taką ochronę dzięki funkcji znanej jako translacja adresów sieciowych (*ang. Network Address Translation — NAT*). Funkcja NAT „przekłada" zewnętrzny, publiczny adres IP sieci domowej przydzielony przez dostawcę usługi dostępu do internetu na wiele wewnętrznych, prywatnych adresów IP. W ten sposób nie tylko zapobiega się nawiązywaniu połączeń z komputerami sieci domowej przez komputery zewnętrzne, ale także umożliwia się sieci domowej korzystanie z jednego publicznego adresu IP, mimo że w sieci domowej może znajdować się wiele urządzeń. Takie rozwiązanie przynosi oszczędności konsumentom (wielu dostawców usługi dostępu do internetu pobiera opłaty za korzystanie z wielu adresów IP). NAT może jednak utrudniać korzystanie z rozwiązań zdalnego dostępu w organizacji, w szczególności z VPN, z protokołu IPv6. Telepracownicy powinni skonsultować się ze swoją organizacją, jeżeli podczas korzystania z NAT występują problemy z jej usługami VPN lub IPv6.

sieciową. Jeżeli na przykład osobista zapora sieciowa na komputerze ulegnie awarii, urządzenie lub router nadal będzie chronił komputer przed niepożądaną komunikacją sieciową z komputerów zewnętrznych. W niektórych przypadkach urządzenie lub router może również chronić urządzenia w sieci domowej przed sobą nawzajem — jeżeli urządzenia są logicznie oddzielone przez urządzenie lub router. Przykładowo router wyposażony zarówno w interfejs przewodowy, jak i bezprzewodowy może być w stanie zapobiec rozprzestrzenianiu się pewnych rodzajów złośliwego oprogramowania z urządzenia w sieci bezprzewodowej na urządzenie w sieci przewodowej, w zależności od swoich możliwości i konfiguracji. Niemniej tego rodzaju konfiguracje sieci domowych są stosunkowo skomplikowane we wdrożeniu i utrzymaniu, toteż taką opcję powinni rozważyć jedynie użytkownicy posiadający doświadczenie w zakresie konfiguracji sieci i mechanizmów bezpieczeństwa.

Podczas instalacji i konfiguracji sprzętowych zapór sieciowych, routerów szerokopasmowych i podobnych urządzeń, telepracownicy powinni stosować środki ostrożności opisane w dokumentacji producenta.

Poniżej podano kilka przykładów takich środków:[15]

- Zmiana domyślnych haseł dostępowych do urządzenia, aby atakujący nie mogli użyć ich do uzyskania dostępu (listy domyślnych haseł są powszechnie dostępne w Internecie).
- Skonfigurowanie urządzenia w taki sposób, aby nie można było nim zarządzać spoza sieci domowej, uniemożliwiając atakującym przejęcie kontroli nad urządzeniem z zewnątrz.
- Skonfigurowanie urządzenia w taki sposób, aby ignorowało wszelkie wysyłane do niego niechciane żądania, co zasadniczo pozwala ukryć je przed nieupoważnionymi osobami. Przed skonfigurowaniem urządzenia w ten sposób telepracownicy powinni skonsultować się z dostawcą usługi dostępu

[15] Jeśli dokumentacja producenta nie zaleca wyraźnie żadnych środków bezpieczeństwa, telepracownicy powinni rozważyć wdrożenie przedstawionych zaleceń, zakładając, że urządzenie lub router obsługuje opcje konfiguracji wymienione w tych przykładach.

do internetu, gdyż może to skutkować zakłóceniem niezbędnej komunikacji z infrastrukturą dostawcy usługi.

- Sprawdzanie dostępności aktualizacji i okresowe instalowanie ich zgodnie z dokumentacją producenta — automatycznie (zazwyczaj codziennie lub co tydzień) lub ręcznie (co najmniej raz w miesiącu, zainicjowane przez telepracownika) oraz
- W przypadku routerów szerokopasmowych — wyłączenie lub dezaktywacja wbudowanych punktów dostępu do sieci bezprzewodowej (*ang. Access Point — AP*), które nie są używane.

Wymagane środki ostrożności dla sprzętowych zapór sieciowych, routerów szerokopasmowych itp. znacząco różnią się od siebie w zależności od urządzenia. Tym samym niektóre lub nawet wszystkie z powyższych zaleceń mogą nie mieć zastosowania do wielu urządzeń.

4.2. Domowe sieci bezprzewodowe

Sieć bezprzewodowa przesyła informacje pomiędzy urządzeniem do telepracy/pracy zdalnej a punktem dostępu do sieci bezprzewodowej.[16] W przypadku niewłaściwej konfiguracji bezprzewodowa sieć domowa będzie przesyłać wrażliwe informacje bez odpowiedniej ochrony, narażając je na nieuprawniony dostęp z innych urządzeń bezprzewodowych znajdujących się w pobliżu. Dlatego też telepracownicy powinni zabezpieczyć swoje bezprzewodowe sieci domowe, aby ich komunikacja zdalna była chroniona. Powinni stosować się do zaleceń dotyczących bezpieczeństwa zawartych w dokumentacji bezprzewodowego punktu dostępu do sieci domowej.

Zakładając, że sieć korzysta z protokołu Institute of Electrical and Electronics Engineers (IEEE) 802.11, zaleca się stosowanie następujących środków bezpieczeństwa:

[16] Urządzenie może również połączyć się bezprzewodowo bezpośrednio z innym urządzeniem za pomocą tak zwanej sieci bezprzewodowej „ad hoc". Z sieciami „ad hoc" wiążą się jednak znane zagrożenia bezpieczeństwa, dlatego niniejszy poradnik nie zaleca stosowania tych sieci.

- **Stosowanie silnego szyfrowania do ochrony komunikacji.** Grupa branżowa działająca pod nazwą Wi-Fi Alliance stworzyła serię certyfikatów bezpieczeństwa produktów o nazwie Wi-Fi Protected Access (WPA), która obejmuje certyfikaty WPA i WPA2. Wspomniane certyfikaty określają wymogi bezpieczeństwa dla bezprzewodowych urządzeń sieciowych. Urządzenia z bezprzewodowymi kartami sieciowymi, które obsługują WPA, mogą wykorzystywać zapewniane przez ten standard zabezpieczenia, np. szyfrowanie komunikacji sieciowej za pomocą AES[17] lub TKIP[18]. W tym przypadku zaleca się wybór następującej ochrony[19], w kolejności od najbardziej preferowanej opcji: 1). WPA3[20], 2). WPA2 z AES. Starszą formą zabezpieczenia komunikacji bezprzewodowej jest szyfrowanie WEP (*ang. Wired Equivalent Privacy*), które jest niestety obciążone znacznymi wadami i **nie jest zalecane**. Atakujący mogą łatwo obejść zabezpieczenia WEP i uzyskać dostęp do informacji przesyłanych przez sieć bezprzewodową. Jeżeli standard WEP jest jedynym dostępnym mechanizmem ochronnym sieci domowej, użytkownicy powinni skonfigurować go tak, aby używał 128-bitowego szyfrowania (co w pewnym stopniu ograniczy skutki ataków), a także korzystać z zapewnianego przez organizację rozwiązania bezpiecznego dostępu zdalnego (np. VPN) w celu ochrony komunikacji zdalnej. Powinni także unikać wysyłania wrażliwych informacji bez zabezpieczeń.

[17] AES (*ang. Advanced Encryption Security*) - algorytm szyfrujący zatwierdzony zgodnie z federalnymi standardami przetwarzania informacji (*ang. Federal Information Processing Standards — FIPS*). Oznacza to, że został sprawdzony i zatwierdzony przez rząd federalny Stanów Zjednoczonych jako rozwiązanie wystarczająco silne, by stosować je do ochrony informacji w systemach federalnych.

[18] TKIP (*ang. Temporal Key Integrity Protocol*) – protokół używany w celu zabezpieczenia warstwy łącza danych w sieciach bezprzewodowych zgodnych ze standardem IEEE 802.11.

[19] Ze względów bezpieczeństwa stosowanie **WPA z AES oraz WPA z TKIP nie jest zalecane**.

[20] W styczniu 2018 roku Wi-Fi Alliance ogłosiło WPA3 jako zamiennik WPA2. Nowy standard wykorzystuje 128-bitowe szyfrowanie w trybie WPA3-Personal (192-bitowe w WPA3-Enterprise) oraz mechanizm przekazywania sekretu (*ang. forward secrecy*). Standard WPA3 zastępuje również wymianę klucza wstępnie współdzielonego (PSK) metodą SAE (*ang. Simultaneous Authentication of Equals*) zdefiniowaną w IEEE 802.11-2016 (SAE to metoda uwierzytelniania i uzgadniania kluczy oparta na haśle, co skutkuje bezpieczniejszą wymianą klucza pierwotnego w trybie osobistym). Wi-Fi Alliance twierdzi również, że WPA3 zmniejszy problemy bezpieczeństwa stwarzane przez słabe hasła i uprości proces konfigurowania urządzeń nieposiadających interfejsu wyświetlacza.

- **Stosowanie klucza WPA3, WPA2, WPA lub WEP** (w zależności od opcji wybranej powyżej). Taki klucz jest ciągiem znaków (lub hasłem składającym się z liter, cyfr i znaków interpunkcyjnych, albo liczbą szesnastkową), który służy do ograniczenia dostępu do sieci bezprzewodowej. Bezprzewodowy punkt dostępu do sieci można skonfigurować tak, aby każde łączące się urządzenie musiało podać taki sam klucz, jak ten zapisany w samym punkcie dostępu. Urządzenia, które nie podadzą tego klucza, nie mogą korzystać z sieci bezprzewodowej. Klucz powinien być długi i złożony, co utrudni innym osobom jego odgadnięcie. Powinno to zapobiec uzyskaniu nieautoryzowanego dostępu do sieci przez osoby znajdujące się w pobliżu punktu dostępu do sieci.
- **Zezwalanie na dostęp tylko określonym bezprzewodowym kartom sieciowym.** Niektóre punkty dostępu można skonfigurować tak, aby zezwalały na korzystanie z sieci bezprzewodowej tylko określonym urządzeniom. W tym celu należy zidentyfikować adres MAC (*ang. Media Access Control*) bezprzewodowej karty sieciowej każdego urządzenia i wpisać go na odpowiednią listę na stronie konfiguracji punktu dostępu. Z racji, że każdy interfejs sieciowy powinien posiadać unikatowy adres MAC, wpisanie takiego adresu do konfiguracji punktu dostępu może uniemożliwić nieupoważnionym osobom uzyskanie dostępu do sieci bezprzewodowej.[21] Aby dowiedzieć się, jak ustalić adres MAC danego urządzenia, należy zapoznać się z jego dokumentacją.
- **Zmiana domyślnego identyfikatora sieci (*ang. service set identifier - SSID*).** SSID to nazwa przypisana do punktu dostępu do sieci bezprzewodowej. Pozwala on użytkownikom i urządzeniom odróżnić jedną sieć od drugiej. Większość punktów dostępu wykorzystuje domyślny identyfikator SSID — często jest to

[21] Doświadczony atakujący może obejść filtrowanie adresów MAC, konfigurując swój komputer tak, aby ów „udawał", że używa autoryzowanego adresu MAC. Listy filtrowania adresów MAC są pomocne głównie w zapobieganiu korzystania z sieci bezprzewodowej przez osoby nieposiadające złych zamiarów, np. takie, które przypadkowo podłączyły się do sieci, lub szukające sposobu na uzyskanie dostępu do internetu. Korzystanie z list filtrowania adresów MAC stanowi dodatkową warstwę zabezpieczeń, która może odstraszyć napastników (np. skłonić ich do poszukania łatwiejszego celu), ale sama w sobie nie zdoła ich powstrzymać.

nazwa producenta lub urządzenia. Jeżeli taki domyślny identyfikator SSID nie zostanie zmieniony, a inna pobliska sieć bezprzewodowa posiada taki sam, to urządzenie telepracownika może przypadkowo próbować połączyć się z niewłaściwą siecią bezprzewodową.[22] Wybór nietypowego identyfikatora SSID — tj. innego niż identyfikator domyślny lub oczywisty, np. „SSID" lub „sieć bezprzewodowa" — znacznie zmniejsza prawdopodobieństwo, że urządzenie wybierze niewłaściwą sieć.

- **Wyłączenie rozgłaszania SSID przez punkt dostępu do sieci bezprzewodowej.** Wiele punktów dostępu do sieci bezprzewodowej ma włączoną funkcję rozgłaszania SSID, co zasadniczo informuje wszystkie komputery w pobliżu o istnieniu takiego punktu dostępu. Skonfigurowanie punktu dostępu tak, aby nie rozgłaszał swojego identyfikatora SSID, zmniejsza prawdopodobieństwo wystąpienia przypadkowych prób połączenia z siecią bezprzewodową, jednakże nie uniemożliwi dokonywania takich prób atakującym.
- **Wyłączenie zarządzania punktem dostępu poprzez komunikację bezprzewodową.** W narzędziach administracyjnych punktów dostępu do sieci bezprzewodowej często wykrywane są luki. Jeżeli punkt dostępu posiada taką lukę, atakujący znajdujący się w pobliżu może skonfigurować go tak, aby wyłączyć jego zabezpieczenia lub wykorzystać go do uzyskania dostępu do sieci domowej telepracownika lub do internetu.
  Aby temu zapobiec, telepracownicy powinni w miarę możliwości skonfigurować swoje punkty dostępu tak, aby można było nimi zarządzać tylko lokalnie — np. podłączając komputer do punktu dostępu za pomocą kabla — oraz aby wykluczyć możliwość zarządzania nimi bezprzewodowo lub w inny sposób zdalnie.

[22] Jeżeli punkt dostępowy telepracownika i urządzenie telepracownicze są skonfigurowane do korzystania z szyfrowania, urządzenie telepracownicze nie będzie w stanie połączyć się z inną siecią bezprzewodową, ponieważ obie sieci używają różnych kluczy szyfrowania. Jest to kolejna korzyść z zastosowania szyfrowania w komunikacji bezprzewodowej.

4.3. Sieci zewnętrzne

Telepracownicy powinni mieć świadomość, że sieci inne niż ich sieci domowe nie zapewnią dużej ochrony dla ich urządzeń i komunikacji w ramach telepracy/pracy zdalnej. Dotyczy to np. korzystania z laptopa podłączonego do bezprzewodowego hotspotu w kawiarni. Sieci zewnętrzne mogą nie szyfrować komunikacji sieciowej, czyniąc ją podatną na podsłuch, szczególnie w przypadku sieci bezprzewodowych. Urządzenia do telepracy/pracy zdalnej podłączone do sieci zewnętrznych są również często bezpośrednio dostępne z internetu. Niektóre sieci zapewniają częściową ochronę, np. blokują określone rodzaje komunikacji, które zwykle kojarzone są ze złośliwą działalnością, oraz sprawdzają komunikację pod kątem najbardziej powszechnych znanych zagrożeń, takich jak rozpowszechnione „robaki" lub spam.

Z racji, że telepracownicy zazwyczaj nie mogą łatwo określić, jaką ochronę zapewnia ich urządzeniom sieć zewnętrzna, powinni z góry zakładać, że nie gwarantuje ona żadnej ochrony. Urządzenia do telepracy/pracy zdalnej pracujące w sieciach zewnętrznych są z reguły bardziej podatne na niebezpieczeństwo niż te w sieciach domowych, a ich komunikacja jest bardziej narażona na podsłuchiwanie. Przed skorzystaniem z sieci osoby trzeciej telepracownicy powinni upewnić się, że ich urządzenia są w pełni zaktualizowane (patrz Rozdział 5.1 i Rozdział 6). Aktualizacje należy pobierać przez zaufaną sieć, np. sieć domową użytkownika. Jeżeli telepracownicy korzystają z sieci osób trzecich w celu uzyskania dostępu do zasobów komputerowych organizacji, powinni korzystać z VPN lub innego bezpiecznego rozwiązania zdalnego dostępu dostarczonego przez organizację i powinni aktywować bezpieczne rozwiązanie zdalnego dostępu (np. ustanawiając sesję VPN) natychmiast po połączeniu się z siecią osób trzecich, jeżeli ma to zastosowanie.

4.4. Sieci organizacji

Organizacje mogą zezwolić na bezpośrednie podłączanie prywatnych urządzeń do sieci dostępnych na ich terenie, np. za pomocą sieci bezprzewodowej w budynku biurowym, w którym przebywa telepracownik. Telepracownicy, którzy chcą przynieść własne urządzenia do biura w celu korzystania z sieci firmowych, powinni najpierw ustalić, czy organizacja zezwala na dostęp do sieci z takich urządzeń, a jeśli tak, to z jakich sieci mogą one korzystać. Wiele organizacji tworzy specjalną sieć dla urządzeń BYOD. Zwykle jest to sieć bezprzewodowa, a prywatne urządzenia pracowników mogą się bezpośrednio łączyć tylko z nią. Telepracownicy nie powinni podłączać własnych urządzeń do sieci wewnętrznych organizacji bez uzyskania wyraźnej zgody.

5. ZABEZPIECZANIE KOMPUTERÓW BYOD UŻYWANYCH DO TELEPRACY/PRACY ZDALNEJ

Telepracownicy używający prywatnych komputerów stacjonarnych lub laptopów do wykonywania telepracy/pracy zdalnej powinni wdrożyć zalecenia przedstawione w tym rozdziale. Wspomniane zalecenia będą pomocne w zabezpieczeniu systemu operacyjnego i podstawowych aplikacji komputera.

Wdrożenie niektórych zaleceń zawartych w tym rozdziale może stanowić wyzwanie dla wielu użytkowników. W przypadku braku pewności co do tego, jak wdrożyć te zalecenia, należy skorzystać z pomocy eksperta.

5.1. Aktualizacje oprogramowania

Wiele zagrożeń wykorzystuje luki w oprogramowaniu komputerów PC, dlatego też producenci oprogramowania regularnie wydają aktualizacje, aby wyeliminować takie podatności. Telepracownicy powinni regularnie aktualizować podstawowe oprogramowanie swoich komputerów BYOD. Oprócz systemu operacyjnego należy także aktualizować:

- Przeglądarki internetowe.
- Klientów poczty elektronicznej.
- Klientów komunikatorów internetowych.
- Oprogramowanie biurowe (przeglądarki dokumentów, edytory tekstu, arkusze kalkulacyjne itp.).
- Oprogramowanie antywirusowe oraz
- Osobiste zapory sieciowe.

Telepracownikom zaleca się zapoznanie z dokumentacją wydaną przez producenta każdego zainstalowanego programu na komputerze, aby określić możliwości jego aktualizacji. Większość popularnych programów posiada wbudowane mechanizmy automatycznej aktualizacji. Telepracownicy powinni aktywować te funkcje, aby umożliwić programom automatyczne sprawdzanie aktualizacji (szczególnie w przypadku oprogramowania antywirusowego i innych programów

zabezpieczających). W przypadku programów, które nie oferują automatycznej aktualizacji, telepracownik powinien ustalić inne dostępne opcje na podstawie stosownej dokumentacji, np. cotygodniowo uruchamiać funkcję aktualizacji z menu aplikacji lub odwiedzać stronę internetową producenta, by sprawdzić dostępność aktualizacji i zainstalować te nowo udostępnione.

W przypadku korzystania z sieci z limitem transferu danych, np. modemu GSM, telepracownicy powinni zachować ostrożność przy konfigurowaniu funkcji automatycznej aktualizacji oprogramowania. Pliki z aktualizacjami często mają bardzo duże rozmiary, toteż pobieranie ich przez sieci z limitem transferu może okazać się kosztowne. W miarę możliwości warto pobierać duże aktualizacje przez sieci nieposiadające limitu transferu.

Niektórzy producenci oprogramowania oferują bezpłatne aktualizacje, inni zaś wymagają uiszczenia rocznej opłaty lub innej płatności, aby otrzymywać aktualizacje — np. opłacenia subskrypcji za dostęp do najnowszych sygnatur programu antywirusowego. Większość producentów oprogramowania z płatną subskrypcją umożliwia użytkownikom uiszczenie opłaty za pośrednictwem strony internetowej producenta i otrzymanie aktualizacji w ciągu kilku minut od dokonania płatności.

5.2. Konta użytkowników i sesje

Na komputerze PC można skonfigurować konta użytkowników i hasła w taki sposób, aby ograniczyć innym osobom możliwości korzystania z urządzenia. W niniejszym punkcie wyjaśniono, jak telepracownik może zapobiec nieautoryzowanemu dostępowi do aplikacji i danych poprzez odpowiednie skonfigurowanie swojego komputera BYOD.

5.2.1. Używanie kont z ograniczonymi uprawnieniami

W większości systemów operacyjnych konta użytkowników mogą mieć pełne lub ograniczone uprawnienia. Konta z pełnymi uprawnieniami, zwane również *kontami administratora*, powinny być używane wyłącznie do wykonywania zadań związanych z zarządzaniem komputerem, np. instalowania aktualizacji i oprogramowania, zarządzania kontami użytkowników oraz modyfikowania ustawień systemu operacyjnego i aplikacji. Jeśli komputer zostanie zaatakowany podczas korzystania

z konta administratora, atak będzie mógł wyrządzić większe szkody. Dlatego też konta użytkowników należy skonfigurować tak, aby miały ograniczone uprawnienia. Takie konto nazywane jest *kontem codziennego użytku*, *kontem z ograniczeniami lub kontem użytkownika standardowego*. Telepracownicy nie powinni używać kont administratora podczas wykonywania podstawowych czynności, takich jak odczytywanie poczty elektronicznej, przeglądanie stron internetowych czy korzystanie z serwisów społecznościowych — podczas takich działań często dochodzi do zainfekowania komputera złośliwym oprogramowaniem.

Podstawową wadą posiadania oddzielnego konta administratora oraz konta użytkownika standardowego jest fakt, że to drugie może nie dawać możliwości uruchamiania niektórych aplikacji, szczególnie tych przeznaczonych dla starszych systemów operacyjnych, a także instalowania aplikacji i aktualizacji systemu bądź aplikacji. To z kolei może powodować znaczne opóźnienia w pobieraniu i instalowaniu aktualizacji, a także utrudniać użytkownikowi wykonywanie innych zadań. Niektóre systemy operacyjne posiadają funkcję, która umożliwia osobie zalogowanej na koncie użytkownika standardowego wykonywanie poszczególnych zadań administracyjnych poprzez wybranie specjalnej opcji.

Każda osoba korzystająca z komputera do telepracy/pracy zdalnej powinna posiadać odrębne konto użytkownika standardowego. W większości systemów operacyjnych pozwala to zachować prywatność danych i ustawień każdej osoby (np. plików, zapisanych wiadomości e-mail, zakładek przeglądarki internetowej i ustawień bezpieczeństwa) względem tych należących do innych osób korzystających z urządzenia. Pozwala to również ograniczyć szkody, jakie mogą wyrządzić niektóre ataki, np. uszkodzić tylko pliki jednego użytkownika, a nie wszystkich.

5.2.2. Ochrona kont za pomocą haseł

Każde konto użytkownika komputera powinno być zabezpieczone hasłem, aby uniemożliwić korzystanie z komputera osobom nieupoważnionym — nie tylko tym mającym fizyczny dostęp do komputera, ale również atakującym próbującym połączyć się z nim z innych komputerów. Użytkownicy powinni wybierać silne hasła, których atakujący nie będzie w stanie odgadnąć.

Poniżej przedstawiono zalecane praktyki dotyczące wyboru hasła:[23]

- **Wybierz odpowiednio długie hasło**. Dłuższe hasła są trudniejsze do odgadnięcia niż krótsze hasła o podobnej złożoności (patrz poniżej). Wadą jest jednak to, że dłuższe hasło często jest trudniejsze do zapamiętania przez użytkownika. Zaleca się, ażeby użytkownicy wybierali hasła o długości co najmniej 15, a najlepiej 20 znaków. Tzw. „frazy kodujące" (*ang. passphrase*)[24], czyli dłuższe hasła złożone z wielu słów, mogą okazać się łatwiejsze do zapamiętania niż standardowe hasła.
- **Utwórz złożone hasło**. Hasło powinno składać się z różnych znaków. Przykładowo hasło składające się jedynie z małych liter jest stosunkowo proste. Jednakże hasło o tej samej długości, które jednocześnie zawiera wielkie i małe litery, cyfry i symbole (np. znaki interpunkcyjne), jest już hasłem złożonym. Im bardziej złożone jest hasło, tym trudniej będzie je odgadnąć. Użytkownikom zaleca się wybieranie haseł zawierających nie tylko litery, ale także cyfry i/lub symbole. Jednocześnie tworząc nowe hasła użytkownicy powinni unikać wybierania takich, które są podobne do starych. Jeśli nasze poprzednie hasło brzmiało „dalia*1", to jako nowego nie powinniśmy wybierać sformułowania „dalia*2".
- **Nie korzystaj z podpowiedzi do tworzenia haseł**. Podpowiedzi do haseł mogą być bardzo pomocne w odgadywaniu haseł innych osób i wykorzystywaniu ich do uzyskania nieautoryzowanego dostępu do komputera. Użytkownicy nie powinni korzystać z podpowiedzi haseł, chyba że ich komputery nie wymagają ochrony przed osobami mającymi do nich fizyczny dostęp.

[23] Organizacje mogą ustanowić dodatkowe wymagania dotyczące wyboru i zarządzania hasłami na prywatnych komputerach używanych do telepracy/pracy zdalnej. Telepracownicy powinni upewnić się, że oprócz zapewnienia zgodności z wymienionymi tu zaleceniami spełniają także wszelkie takie wymagania.

[24] Fraza kodująca to zapamiętany sekret składający się z sekwencji słów lub innego tekstu, który użytkownik wykorzystuje do uwierzytelnienia swojej tożsamości. Fraza kodująca jest podobna w użyciu do hasła, ale jest zazwyczaj dłuższa dla zwiększenia bezpieczeństwa.

- **Nie używaj tego samego hasła do innych kont.** Telepracownicy nie powinni używać tego samego hasła do wielu kont, np. do służbowych i osobistych kont e mail, kont w komunikatorach internetowych czy też kont na stronach sklepów internetowych. Jeśli do zabezpieczenia swoich innych kont użytkownik zastosuje takie samo hasło jak to chroniące jego komputer do telepracy/pracy zdalnej, atakujący, który przechwyci hasło do jednego konta, będzie także w stanie uzyskać dostęp do innych kont.

Telepracownicy powinni regularnie zmieniać swoje hasła, w odstępach czasu określonych w polityce dotyczącej haseł ich organizacji. Jest to konieczne, gdyż w przypadku nieświadomego ujawnienia hasła osobie nieuprawnionej lub odkrycia go przez złośliwe oprogramowanie bądź inne ataki automatyczne, może ono być używane bez upoważnienia aż do chwili jego zmiany przez telepracownika.

Jeżeli zdarzy się nam zapomnieć hasło do systemu operacyjnego, zwłaszcza do konta administratora, odzyskanie dostępu do komputera może być trudne. Użytkownicy powinni rozważyć spisanie swoich haseł do systemu operacyjnego i przechowywanie ich w bezpiecznym miejscu, np. w zamkniętym sejfie. Użytkownikom zaleca się również zabezpieczenie pozostałych haseł, np. do aplikacji i stron internetowych. Niektóre organizacje udostępniają telepracownikom kryptograficzne tokeny, które mogą być wykorzystywane do przechowywania haseł. W przypadku konieczności odzyskania hasła telepracownik uwierzytelnia się na tokenie (np. wprowadzając kod PIN), a ów udostępnia mu przechowywaną informację. Token pomaga zapobiec zgubieniu hasła przez użytkownika, jednocześnie chroniąc je przed nieuprawnionymi osobami. Inną możliwością ochrony haseł do aplikacji i stron internetowych jest narzędzie do zarządzania hasłami, czyli program, który może być używany do bezpiecznego generowania, przechowywania i dostępu do haseł. Korzystając z takiego programu telepracownik zazwyczaj musi wpisać jedno hasło, aby uzyskać dostęp do wszystkich haseł przechowywanych przez narzędzie.

5.2.3. Ochrona sesji użytkowników przed nieuprawnionym dostępem fizycznym

Sesje użytkowników należy chronić przed nieuprawnionym dostępem fizycznym. Przykładowo, jeśli komputer jest pozostawiony bez nadzoru w miejscu, do którego

mają dostęp inne osoby, to wówczas każda z nich może podejść do urządzenia i podszyć się pod użytkownika, np. wysyłając e-mail z jego konta. Takie działanie może pozwolić jej na uzyskanie dostępu do zasobów zdalnego dostępu organizacji, dokonania zakupów na stronach internetowych lub uzyskania dostępu do wrażliwych informacji przechowywanych na komputerze. Aby temu zapobiec, większość systemów operacyjnych umożliwia użytkownikowi zablokowanie bieżącej sesji poprzez opcje menu lub kombinację klawiszy. Ponadto wiele systemów operacyjnych oferuje wygaszacze ekranu aktywowane automatycznie po określonym czasie bezczynności urządzenia lub ręcznie przez użytkownika. Niektóre wygaszacze można skonfigurować tak, aby blokowały komputer i wymagały podania hasła w celu jego odblokowania. Pozostawiając komputer bez nadzoru w miejscu dostępnym dla osób postronnych, użytkownik powinien posiadać aktywny wygaszacz ekranu wymagający podania hasła w celu ponownego dostępu lub też ręcznie zablokować urządzenie. Jednocześnie użytkownik powinien mieć świadomość, że takie zabezpieczenia zapewniają jedynie krótkotrwałą ochronę. Osoba mająca dostęp do komputera przez dłuższy czas może je obejść i uzyskać dostęp do sesji użytkownika oraz jego danych.

5.3. Konfiguracja sieci

Większość komputerów PC można skonfigurować tak, aby ograniczyć dostęp do sieci, zmniejszając liczbę dostępnych dla atakujących sposobów na uzyskanie dostępu do komputera. Poniższe punkty zawierają zalecenia dotyczące konfiguracji funkcji sieciowych w celu lepszej ochrony urządzenia.

5.3.1. Wyłączanie niepotrzebnych funkcji sieciowych

Domyślnie większość komputerów PC oferuje szereg funkcji sieciowych, które umożliwiają komunikację i współdzielenie danych między urządzeniami. Większość telepracowników potrzebuje dostępu jedynie do kilku z nich. Z racji, iż wiele ataków odbywa się z wykorzystaniem sieci, na komputerze PC powinny być aktywne jedynie niezbędne funkcje sieciowe. Przykładowo usługi współdzielenia plików i drukarek, które umożliwiają innym komputerom dostęp do plików i drukarek komputera telepracownika, powinny być wyłączone, chyba że komputer rzeczywiście współdzieli swoje pliki lub drukarki z innymi komputerami lub określona aplikacja wymaga

aktywowania tych usług.[25] Inne przykłady usług, które mogą nie być potrzebne, to protokoły IPv6 i protokoły sieci bezprzewodowych (np. Bluetooth, IEEE 802.11, NFC). Aby określić, które funkcje sieciowe powinny być wyłączone, należy zapoznać się z dokumentacją sprzętu komputerowego i systemu operacyjnego. W razie wątpliwości należy zasięgnąć porady eksperta.

5.3.2. Ograniczenie korzystania z narzędzi do zdalnego dostępu

Niektóre systemy operacyjne oferują funkcje umożliwiające telepracownikowi uzyskanie zdalnej pomocy technicznej od współpracownika, przyjaciela, producenta produktu lub innych osób w przypadku problemów z komputerem. Dostępnych jest również wiele aplikacji, które umożliwiają zdalny dostęp do komputera z innych urządzeń. Mimo iż funkcje te są wygodne, to jednocześnie zwiększają również ryzyko uzyskania dostępu do komputera przez atakujących. Z tego względu takie narzędzia powinny być wyłączone przez cały czas, z wyjątkiem sytuacji, gdy rzeczywiście są potrzebne. Ponadto narzędzia te powinny być skonfigurowane w taki sposób, aby przed uzyskaniem dostępu do komputera osoba łącząca się zdalnie musiała zostać uwierzytelniona, zazwyczaj za pomocą nazwy użytkownika i hasła (patrz zalecenia dotyczące wyboru silnych haseł w punkcie 5.2.2). Osobie łączącej się zdalnie należy przekazać nazwę użytkownika i hasło osobiście, telefonicznie lub w inny sposób uniemożliwiający odkrycie tych informacji przez atakujących. Nie należy wysyłać haseł za pośrednictwem wiadomości e-mail, komunikatorów internetowych lub innych metod, które mogą nie zapewniać ochrony komunikacji.

5.3.3. Konfiguracja sieci bezprzewodowej

Nieprawidłowo skonfigurowana sieć bezprzewodowa może przesyłać informacje wrażliwe bez odpowiedniego zabezpieczenia, umożliwiając ich „podsłuchiwanie" osobom znajdującym się w pobliżu. W punkcie 4.2 wyjaśniono, jak zabezpieczyć

[25] Wyłączenie takich usług jest szczególnie ważne, jeżeli komputer będzie używany w niezabezpieczonych sieciach bezprzewodowych, takich jak większość bezprzewodowych hotspotów.

domową sieć bezprzewodową. Oprócz tego komputery PC powinny być skonfigurowane tak, aby nie próbowały automatycznie łączyć się z wykrytymi sieciami bezprzewodowymi. W innym razie komputer telepracownika mógłby na przykład połączyć się z bezprzewodową siecią domową sąsiada zamiast tej należącej do samego pracownika. Gdyby sieć sąsiada była niewłaściwie zabezpieczona, prowadzona komunikacja i urządzenie telepracownika mogłyby zostać narażone na zwiększone ryzyko. Telepracownicy powinni zatem skonfigurować swoje komputery tak, aby nie łączyły się automatycznie z wykrytymi sieciami bezprzewodowymi, z wyjątkiem własnych sieci bezprzewodowych organizacji, o ile organizacja to dopuszcza. Telepracownicy powinni również wyłączyć możliwość korzystania z sieci ad hoc na swoich urządzeniach — ta stanowi bowiem łatwy sposób na zaatakowanie komputera.

5.4. Zapobieganie atakom

Jak wyjaśniono w rozdziale 2, nie istnieje rozwiązanie zapewniające stuprocentowe bezpieczeństwo komputera — udaremnienie każdego możliwego ataku jest zwyczajnie niemożliwe. Komputery PC powinny wykorzystywać kombinację oprogramowania i funkcji, które pozwolą powstrzymać większość ataków, zwłaszcza ze strony złośliwego oprogramowania. Rodzaje oprogramowania opisane w poniższych punktach obejmują programy antywirusowe, osobiste zapory sieciowe, filtrowanie spamu i treści internetowych oraz blokowanie wyskakujących okienek (*ang. popup*). Niektóre ataki można również powstrzymać poprzez zmianę części ustawień w popularnych aplikacjach, takich jak klienci poczty elektronicznej i przeglądarki internetowe.

Pomimo iż narzędzia zabezpieczające pozwalają powstrzymać wiele ataków, telepracownicy muszą również wyrobić w sobie pewne bezpieczne nawyki dotyczące pracy z komputerem. Jednym z najczęstszych sposobów na zaatakowanie komputera jest otwarcie lub uruchomienie przez użytkownika pliku z nieznanego, niezaufanego źródła. Telepracownicy mogą pobrać takie pliki ze stron internetowych, serwisów wymiany plików bądź z innych źródeł, a także otrzymać je za pośrednictwem poczty elektronicznej, komunikatorów, mediów społecznościowych i innych usług komunikacyjnych. Z racji, że takie pliki często zawierają złośliwe oprogramowanie,

próba ich otwarcia może skutkować nieświadomym zainfekowaniem komputera przez telepracownika. Telepracownicy powinni unikać korzystania z wszelkich plików pochodzących z nieznanych, niezaufanych źródeł. Inne osoby korzystające z komputera BYOD również powinny zostać poinformowane o zasadach jego bezpiecznej eksploatacji.

5.4.1. Instalacja i konfiguracja oprogramowania antywirusowego

Oprogramowanie antywirusowe jest narzędziem specjalnie zaprojektowanym do wykrywania wielu form złośliwego oprogramowania i zapobiegania infekowaniu przez nie komputerów, a także do oczyszczania komputerów, które zostały już zainfekowane. Ponieważ złośliwe oprogramowanie jest najczęstszym zagrożeniem dla komputerów PC, National Institute of Science and Technology (NIST) zaleca, aby komputery PC w każdym przypadku korzystały z oprogramowania antywirusowego.[26] Oprogramowanie antywirusowe powinno być na bieżąco aktualizowane, jak opisano w punkcie 5.1.

Oprogramowanie antywirusowe sprzedawane jest pod wieloma markami, z których większość oferuje podobną funkcjonalność. **Zaleca się skonfigurowanie oprogramowania antywirusowego tak, aby korzystało z następujących funkcji:**

- Automatyczne sprawdzanie i pobieranie aktualizacji sygnatur lub definicji co najmniej raz dziennie.
- Skanowanie krytycznych komponentów systemu operacyjnego, takich jak pliki startowe, podstawowy system wejścia/wyjścia (BIOS) i rekordy rozruchowe.

[26] W przypadku niektórych systemów operacyjnych, np. większości systemów opartych na Uniksie, alternatywne rodzaje oprogramowania chroniącego przed złośliwym kodem (*ang. antimalware*), takie jak wykrywacze rootkitów, mogą być bardziej skuteczne w ochronie komputera przed złośliwym oprogramowaniem niż oprogramowanie antywirusowe. Wówczas zaleca się stosowanie takich rozwiązań zamiast oprogramowania antywirusowego. Czytelnicy korzystający z ww. systemów operacyjnych powinni stosować zalecenia przedstawione w niniejszej publikacji z uwzględnieniem tego, jakie typy oprogramowania chroniącego przed złośliwym kodem są najbardziej odpowiednie dla ich systemu.

- Monitorowanie zachowania popularnych aplikacji, takich jak klienci poczty elektronicznej, przeglądarki internetowe, programy do przesyłania i udostępniania plików oraz komunikatory internetowe.
- Skanowanie w czasie rzeczywistym każdego pliku podczas jego pobierania, otwierania lub wykonywania.
- Regularne skanowanie wszystkich dysków twardych w celu wykrycia możliwej infekcji systemu plików, opcjonalnie również skanowanie nośników wymiennych.
- Odpowiednie postępowanie z zainfekowanymi plikami — próba ich dezynfekcji, czyli usunięcia złośliwego oprogramowania z plików, a także poddanie ich kwarantannie, czyli odizolowanie plików ze złośliwym oprogramowaniem w celu późniejszej dezynfekcji lub zbadania oraz
- Rejestrowanie wszystkich istotnych zdarzeń, takich jak wyniki skanowania, uruchamianie i wyłączanie oprogramowania antywirusowego, instalowanie aktualizacji oraz przypadki wykrycia i sposób postępowania ze złośliwym oprogramowaniem.

5.4.2. Używanie osobistych zapór sieciowych

Osobista zapora sieciowa (*ang. personal firewall*) to oprogramowanie, które monitoruje komunikację między komputerem PC a innymi urządzeniami, blokując przy tym tę niepożądaną. Prawidłowo skonfigurowana zapora sieciowa ogranicza możliwość inicjowania przez inne urządzenia komunikacji z komputerem telepracownika, co może znacznie zmniejszyć jego narażenie na ataki sieciowe, np. z użyciem „robaków" i „botnetów". Osobistą zaporę sieciową można również wykorzystać do ochrony współdzielonych zasobów na komputerze, takich jak udostępnianie plików i wydruków (*ang. file and print shares*).

Dlatego też osobista zapora sieciowa powinna być włączona na każdym komputerze do telepracy/pracy zdalnej. Należy ją skonfigurować tak, aby rejestrowała istotne zdarzenia, takie jak zablokowana i dozwolona aktywność, uruchamianie i zamykanie oprogramowania zapory sieciowej czy zmiany jej konfiguracji, co pomoże

w rozwiązywaniu problemów. Wszystkie osobiste zapory sieciowe mogą monitorować komunikację przychodzącą, a niektóre umożliwiają również monitorowanie komunikacji wychodzącej — to drugie rozwiązanie zapewnia zwiększone bezpieczeństwo, ale może powodować problemy w korzystaniu z niektórych aplikacji.

Osobiste zapory sieciowe stanowią ważny środek bezpieczeństwa dla komputerów PC. Ich prawidłowe skonfigurowanie może być jednak stosunkowo trudne. Jeżeli zapora zostanie skonfigurowana z zastosowaniem zbyt restrykcyjnych reguł, to wówczas może uniemożliwiać prawidłowe działanie niektórych aplikacji lub funkcji systemu operacyjnego, np. korzystanie z usług związanych z plikami i drukowaniem. Z drugiej strony, jeżeli zastosowane w jej konfiguracji reguły będą zbyt luźne, komputer może być narażony na ataki. Telepracownicy powinni uważnie zapoznać się z dokumentacją swojej zapory sieciowej, aby zrozumieć, jak należy ją skonfigurować. Jeżeli nie jest to jasne, w zakresie konfiguracji osobistej zapory sieciowej telepracownik powinien zasięgnąć porady eksperta.[27]

W idealnej sytuacji osobista zapora sieciowa powinna odrzucać wszelkie rodzaje komunikacji, które nie zostały wyraźnie dopuszczone przez telepracownika. Jest to tzw. domyślne odrzucanie (*ang. deny by default*), w ramach którego wszystkie połączenia, które nie znajdują się na liście wyjątków, są automatycznie odrzucane (blokowane). Większość zapór sieciowych można skonfigurować tak, aby zezwalały na komunikację na podstawie list autoryzowanych aplikacji, takich jak przeglądarki internetowe kontaktujące się z serwerami internetowymi oraz klienci poczty elektronicznej do wysyłania i odbierania wiadomości e-mail. Wówczas komunikacja z każdą inną aplikacją będzie automatycznie odrzucana lub też dopuszczana bądź odrzucana na podstawie decyzji telepracownika w odpowiedzi na wyświetlony monit dotyczący danej czynności. Przykładowo, jeśli telepracownik instaluje nową aplikację i uruchamia ją po raz pierwszy, zapora sieciowa może wyświetlić komunikat

[27] Konfiguracja osobistej zapory sieciowej może być skomplikowanym zadaniem. Niektóre zapory umożliwiają ustalenie reguł dla określonych protokołów, usług lub numerów portów (np. File Transfer Protocol [FTP], Hypertext Transfer Protocol [HTTP], Simple Mail Transfer Protocol [SMTP]). Prawidłowa konfiguracja takiej zapory może wymagać wiedzy w zakresie konfiguracji sieci i ich bezpieczeństwa.

z zapytaniem, czy pozwolić takiej aplikacji na dostęp do internetu.

Ta funkcja może niestety okazać się problematyczna. Osobiste zapory sieciowe często nie dostarczają jasnych informacji o tym, jaka aplikacja próbuje korzystać z sieci, utrudniając telepracownikom określenie, czy mają do czynienia z normalną, czy też złośliwą aktywnością. Jeżeli charakter aktywności jest niejasny, ostrożni telepracownicy często decydują się na jej zablokowanie, co może jednak skutkować blokowaniem potrzebnych funkcji. Aby uniknąć tego problemu, wielu telepracowników udziela dostępu na każde żądanie, tym samym narażając się na złośliwe działania. W przypadku braku pewności, telepracownikom zaleca się wyszukanie dodatkowych informacji o danej usłudze lub oprogramowaniu lub zasięgnięcie porady osoby z większym doświadczeniem w zakresie bezpieczeństwa.

Na komputerze powinna być włączona tylko jedna osobista zapora sieciowa.[28] Jeżeli włączonych jest kilka zapór, mogą one wzajemnie zakłócać swoje działanie. Przykładowo jedna zapora może zezwalać na działania, które inna blokuje ze względu na swoją konfigurację. Może to spowolnić działanie komputera, spowodować nieprawidłowe funkcjonowanie aplikacji, a także osłabić bezpieczeństwo urządzenia. Przy uruchamianiu zapory sieciowej telepracownik powinien sprawdzić, czy jej funkcje włączone są dla każdego interfejsu sieciowego na komputerze, w tym dla VPN oraz przewodowych, bezprzewodowych i wirtualnych kart sieciowych.

Wiele osobistych zapór sieciowych oferuje dodatkowe zabezpieczenia. Obejmują one np. możliwość ustanowienia hasła, które telepracownik będzie musiał podać przed uzyskaniem dostępu do ustawień konfiguracyjnych zapory. Pozwala to chronić konfigurację programu przed przypadkową lub celową zmianą przez użytkownika.

[28] Posiadanie wielu osobistych zapór sieciowych zainstalowanych na jednym komputerze nie jest szkodliwe, o ile w danym momencie aktywna jest tylko jedna z nich. Niektóre systemy operacyjne posiadają wbudowane osobiste zapory sieciowe, jednakże użytkownik może zainstalować na komputerze zaporę sieciową innej firmy, będącą częścią pakietu oprogramowania składającego się z oprogramowania antywirusowego i innych aplikacji zabezpieczających.

Telepracownicy powinni mieć świadomość, że zapory sieciowe często powstrzymują niepożądane działania. „Robaki" i inne złośliwe oprogramowanie nieustannie próbują zainfekować kolejne komputery. Wyświetlane przez zaporę komunikaty wskazujące, że zablokowano połączenia przychodzące lub próbowano przeprowadzić konkretny atak, nie powinny stanowić dla telepracownika powodu do niepokoju. Jeżeli zapora informuje, że komputer został właśnie przeskanowany pod kątem obecności konkretnego „robaka", w żaden sposób nie oznacza to, że urządzenie rzeczywiście zostało nim zainfekowane.

5.4.3. Uruchomienie i konfiguracja oprogramowania do filtrowania treści

Filtrowanie treści (*ang. content filtering*)to proces monitorowania komunikacji, takiej jak poczta elektroniczna i strony internetowe, a także analizowania jej pod kątem podejrzanej zawartości i zapobiegania dostarczaniu takiej zawartości użytkownikom. Popularne rodzaje filtrów treści to np. oprogramowanie do filtrowania spamu i oprogramowanie do filtrowania treści internetowych.

Spam jest często wykorzystywany do przesyłania użytkownikom oprogramowania szpiegującego i innych form złośliwego oprogramowania. Nierzadko jest także wykorzystywany do przeprowadzania prób wyłudzenia informacji (*ang. phishing*), czyli ataków komputerowych, których celem jest podstępne nakłonienie ofiary do ujawnienia wrażliwych danych osobowych. Oprogramowanie filtrujące spam analizuje wiadomości e-mail w poszukiwaniu cech spamu i zazwyczaj umieszcza wiadomości, które wydają się być spamem, w osobnym folderze. Większość organizacji stosuje filtrowanie spamu, by chronić swoich użytkowników. Niestety z racji, że filtrowanie to ma charakter subiektywny, część spamu nadal dociera do użytkowników, a ponadto niektóre pożądane wiadomości e-mail są przypadkowo klasyfikowane jako spam. Mimo to oprogramowanie do filtrowania spamu może znacznie zmniejszyć ilość spamu otrzymywanego przez użytkowników. Wiele klientów poczty elektronicznej również oferuje możliwość filtrowania spamu.

Użytkownicy mogą udoskonalić możliwości filtrowania spamu, korzystając z następujących opcji:

- **Czarne listy.** Czarna lista to lista nadawców poczty elektronicznej, którzy wcześniej wysyłali spam do użytkownika. Po otrzymaniu wiadomości ze spamem użytkownik może dodać adres e-mail nadawcy do czarnej listy. Dzięki temu przyszłe wiadomości od tego samego nadawcy będą automatycznie klasyfikowane jako spam.
- **Białe listy**. Biała lista to lista zaufanych nadawców poczty elektronicznej, takich jak współpracownicy, przyjaciele, rodzina. Użytkownik może dodać ich adresy e mail do białej listy, dzięki czemu kolejne wysłane przez nich wiadomości nie zostaną zaklasyfikowane jako spam. Zdarza się, że filtrowanie spamu przypadkowo oznacza jako spam niektóre wiadomości, które nim nie są. Biała lista zastępuje tę klasyfikację i zapewnia, że użytkownik będzie otrzymywał wiadomości od zaufanych nadawców.
- **Bayesowskie filtry spamu**. Bayesowski filtr spamu określa prawdopodobieństwo, że dana wiadomość e-mail jest spamem na podstawie porównania cech wiadomości e-mail z cechami wcześniej otrzymanych wiadomości o charakterze spamu. Po otrzymaniu wiadomości e-mail użytkownik koryguje ewentualne błędy popełnione przez oprogramowanie filtrujące. Następnie filtr Bayesa analizuje nieszkodliwe wiadomości oraz spam, aby zarejestrować ich cechy. Przykładowo filtr może ustalić, że użytkownik otrzymał 35 wiadomości o charakterze spamu, z których każda zawierała frazę „DARMOWE DARMOWE DARMOWE”, ale nie otrzymał żadnych nieszkodliwych wiadomości z takim wyrażeniem. Gdy użytkownik otrzymuje nową wiadomość e-mail, filtr sprawdza ją pod kątem występowania takiej frazy, jak również innych cech kojarzonych z wiadomościami nieszkodliwymi oraz spamem, a następnie określa prawdopodobieństwo, że dana wiadomość jest spamem. Skuteczność filtrów Bayesa zależy od tego, czy użytkownik przejrzy wszystkie swoje wiadomości e-mail i upewni się, że każda z nich została prawidłowo oznaczona jako spam lub treść niestanowiąca spamu.

Działanie oprogramowania do filtrowania treści internetowych zazwyczaj polega na porównaniu adresu strony internetowej, którą próbuje odwiedzić użytkownik, z listą znanych, szkodliwych witryn internetowych. Mimo iż głównym celem programów do filtrowania treści jest uniemożliwianie dostępu do niestosownych materiałów, wiele z nich zawiera również listy znanych, szkodliwych witryn internetowych, które np. próbują infekować urządzenia odwiedzających złośliwym oprogramowaniem lub hostują strony służące do wyłudzania informacji. Oprogramowanie do filtrowania treści internetowych może nieumyślnie klasyfikować nieszkodliwe treści jako niestosowne lub odwrotnie.

Z punktu widzenia bezpieczeństwa komputerów do telepracy/pracy zdalnej zdecydowanie zaleca się stosowanie filtrów spamu oraz treści internetowych. Wszystkie stosowane produkty do filtrowania treści należy regularnie aktualizować, aby zapewnić jak najdokładniejsze wykrywanie szkodliwej zawartości.

5.5. Konfiguracja podstawowych aplikacji

W ramach wielu ataków, w szczególności tych przeprowadzanych złośliwym oprogramowaniem, wykorzystuje się funkcje oferowane przez popularne aplikacje, np. klientów poczty elektronicznej, przeglądarki internetowe, klientów komunikatorów internetowych i pakiety biurowe. Nierzadko aplikacje są bowiem domyślnie skonfigurowane tak, aby przedkładać funkcjonalność nad bezpieczeństwo. Dlatego też telepracownicy powinni rozważyć wyłączenie niepotrzebnych funkcji i uprawnień aplikacji, szczególnie tych, które są powszechnie wykorzystywane przez złośliwe oprogramowanie. Zaleca się im również odpowiednie skonfigurowanie aplikacji w celu filtrowania treści i zatrzymywania innych potencjalnie złośliwych działań.

Poniżej wymieniono przykłady ustawień aplikacji, których zmianę należy rozważyć. Telepracownik powinien wiedzieć, że na jednym komputerze może być zainstalowanych wiele przeglądarek internetowych, programów do poczty elektronicznej, komunikatorów i pakietów biurowych, z których każdy może mieć inne

funkcje i ustawienia konfiguracyjne.[29]

Telepracownicy powinni również uwzględnić politykę swojej organizacji dotyczącą korzystania z aplikacji. Organizacje często zabraniają na przykład korzystania z oprogramowania typu peer-to-peer (*ang. peer-to-peer software*) i programów do wymiany plików na komputerach firmowych ze względu na zwiększone ryzyko związane z ich użytkowaniem. Telepracownik powinien usunąć z komputera wykorzystywanego do telepracy/pracy zdalnej wszelkie oprogramowanie, którego zabrania polityka firmy, aby lepiej chronić informacje organizacji. Ogólnie rzecz biorąc, telepracownicy powinni instalować i używać na swoich komputerach BYOD wyłącznie znane i zaufane oprogramowanie.

5.5.1. Przeglądarki internetowe

Telepracownikom zaleca się wdrożenie następujących zasad dotyczących przeglądarek internetowych używanych na komputerach BYOD:

- **Do telepracy/pracy zdalnej stosuj przeglądarkę internetową innego producenta.** Na jednym komputerze może być zainstalowanych wiele przeglądarek internetowych (np. Microsoft internet Explorer lub Edge, Mozilla Firefox, Apple Safari, Google Chrome, Opera itp.). Odwiedzanie stron internetowych zawierających złośliwe treści jest jednym z najczęstszych sposobów atakowania komputerów, np. poprzez instalowanie w przeglądarce wtyczek programów szpiegujących (ang. spyware plug-ins). Aby zmniejszyć prawdopodobieństwo oddziaływania takich ataków na telepracę/pracę zdalną, telepracownicy mogą zdecydować się na używanie przeglądarki jednej marki tylko do telepracy/pracy zdalnej oraz przeglądarki innej marki do odwiedzania wszystkich pozostałych stron internetowych. W ten sposób związane z telepracą/pracą zdalną dane przechowywane w jednej przeglądarce będą

[29] Wielu producentów podaje w dokumentacji produktu lub na swojej stronie internetowej własne zalecenia dotyczące bezpieczeństwa. Niektórzy udostępniają również listy kontrolne dotyczące bezpieczeństwa systemów operacyjnych, aplikacji i urządzeń. Wiele spośród tych list zamieszczonych jest na specjalnej stronie NIST dotyczącej list kontrolnych dla produktów IT, dostępnej pod adresem http://checklists.nist.gov/.

oddzielone od danych w drugiej przeglądarce, co zapewni lepszą ochronę informacji związanych z telepracą/pracą zdalną (choć samo to nie zabezpieczy w wystarczającym stopniu danych w przeglądarce). Telepraca z wykorzystaniem przeglądarki innej marki pozwala również telepracownikowi na lepsze zabezpieczenie takiego programu.

- **Blokuj wyskakujące okienka.** Przeglądarki internetowe umożliwiają obsługę tzw. wyskakujących okienek (*ang. popup*), czyli odrębnych okienek przeglądarki internetowej, otwierających się automatycznie po załadowaniu strony internetowej lub wykonaniu przez użytkownika konkretnej czynności. Wyskakujące okienka często zawierają jedynie reklamy, ale niektóre są wykorzystywane do atakowania komputerów. Niektóre okna *popup* są spreparowane tak, aby wyglądem przypominały prawdziwe okna komunikatów systemowych lub strony internetowe. Mogą one m.in. podstępem przenieść nieświadomych użytkowników na fałszywe strony internetowe, w tym takie używane do wyłudzania informacji lub nakłonić ich do zatwierdzenia zmian w komputerze. Wyskakujące okienko może na przykład „informować" użytkownika, że jego komputer jest zainfekowany oprogramowaniem szpiegującym i że należy kliknąć przycisk „OK", aby go zdezynfekować. Klikając ów przycisk użytkownik nieświadomie zezwala na zainstalowanie na urządzeniu oprogramowania szpiegującego lub innych rodzajów złośliwego oprogramowania. Telepracownicy powinni skonfigurować swoje przeglądarki internetowe tak, aby blokowały wyskakujące okienka albo skorzystać z zewnętrznych programów służących do ich blokowania. Obie opcje zapobiegają pojawianiu się okienek *popup*, a w razie próby ich otwarcia informują telepracownika, że wyskakujące okienko zostało zablokowane. Jeżeli telepracownik nie chce, by dane okienko było blokowane, to wówczas może zezwolić na otwarcie tego konkretnego okienka lub też na otwieranie wszystkich okien *popup* wyświetlanych przez zaufaną stronę internetową, np. stronę zdalnego dostępu organizacji.

- **Włącz filtr witryn wyłudzających informacje.** Większość przeglądarek potrafi wykryć ewentualne próby wyłudzenia informacji i ostrzec użytkownika, zanim pozwoli mu odwiedzić podejrzaną stronę. Telepracownicy powinni sprawdzić w dokumentacji swojej przeglądarki, czy oferuje ona filtr witryn wyłudzających informacje, a jeśli tak — włączyć go.
- **Usuń niepotrzebne wtyczki do przeglądarki.** *Wtyczka* to narzędzie współpracujące z przeglądarką internetową w celu zwiększenia jej możliwości. Mimo iż większość wtyczek jest przydatna, niektóre z nich mają złośliwy charakter. Telepracownikom zaleca się okresowe sprawdzanie wtyczek zainstalowanych w przeglądarkach i odinstalowywanie tych, które nie są im potrzebne lub są dla nich nieznane. Jeśli nawet telepracownik przypadkiem usunie potrzebną wtyczkę, to zazwyczaj zostanie proszony o jej pobranie i zainstalowanie przy następnym dostępie do treści wymagających jej stosowania.
- **Chroń wrażliwe informacje przechowywane w przeglądarce.** Przeglądarka może zapisywać dla użytkownika wrażliwe informacje, np. hasła do stron internetowych, certyfikaty cyfrowe i klucze szyfrujące. Niektóre przeglądarki posiadają opcje silnej ochrony tych informacji. Zazwyczaj przeglądarka wymaga od użytkownika wprowadzenia hasła głównego, służącego wyłącznie do ochrony wrażliwych informacji. Telepracownicy powinni sprawdzić w dokumentacji przeglądarki, czy oferuje ona opcję takiej ochrony, a jeśli tak — włączyć ją i ustawić hasło główne.
- **Wyłącz automatyczne uzupełnianie haseł na stronach internetowych.** Większość przeglądarek umożliwia zapisywanie haseł wprowadzanych na stronach internetowych. Jednakże wiele z nich oferuje również opcje automatycznego wypełniania lub autouzupełniania, które automatycznie wprowadzają zapisane hasła do pól tekstowych podczas logowania. W ten sposób osoba mająca dostęp do urządzenia telepracownika może uzyskać dostęp do różnych stron internetowych, podając się za telepracownika. Aby temu zapobiec, telepracownicy powinni wyłączyć funkcje autouzupełniania

lub automatycznego wypełniania nazw użytkownika i haseł w swoich przeglądarkach internetowych.

- **Uruchamiaj przeglądarki internetowe z jak najniższymi uprawnieniami.** Niektóre przeglądarki internetowe mogą funkcjonować z niskimi uprawnieniami, dzięki czemu wykonywane w nich działania wpływają na komputer w bardzo ograniczony sposób. Pomaga to w zapobieganiu niektórym atakom przez przeglądarki internetowe, a także ogranicza szkody w przypadku udanego ataku. Telepracownicy powinni uruchamiać swoje przeglądarki internetowe z jak najniższymi uprawnieniami.
- **Używaj oferowane przez niezależnych dostawców wtyczki zwiększające bezpieczeństwo i prywatność**. Tego rodzaju wtyczki mogą poprawić bezpieczeństwo i prywatność telepracy/pracy zdalnej na wiele sposobów, przy czym niektóre z nich są specyficzne dla danego typu przeglądarki. Przykładem może być uniemożliwianie automatycznego uruchamiania aktywnych treści w przeglądarce, powstrzymanie śledzenia na różnych stronach internetowych oraz blokowanie pobierania treści reklamowych do przeglądarki.

5.5.2. Klienci poczty elektronicznej

Telepracownikom zaleca się wdrożenie następujących zasad w zakresie programów do poczty elektronicznej, które wykorzystują w swoich komputerach BYOD:

- **Ogranicz wykonywanie kodu mobilnego.** Kod mobilny (*ang. mobile code*) umożliwia łączącemu się zdalnie komputerowi, np. stronie internetowej, uruchomienie programu na urządzeniu telepracownika. Wiadomości e-mail mogą zawierać złośliwy kod mobilny, który może próbować zainfekować odczytujące je urządzenia. Aby zapobiec infekcjom, większość klientów poczty elektronicznej można skonfigurować tak, aby zezwalać tylko na wymagane formy kodu mobilnego (np. JavaScript, ActiveX, Java itp.). Telepracownicy powinni rozważyć wyłączenie obsługi kodu mobilnego w swoich klientach poczty elektronicznej. Należy jednak mieć na uwadze, że wówczas pełna treść niektórych nieszkodliwych wiadomości e-mail może być niedostępna.

- **Wybierz „zwykły tekst" jako domyślny format odczytu i wysyłania wiadomości.** Wiele klientów poczty elektronicznej umożliwia użytkownikom określenie domyślnego formatu odczytu i wysyłania wiadomości e-mail. Najczęściej stosowane formaty to zwykły tekst (*ang. plain text*) i Hypertext Markup Language (HTML). Z racji, że złośliwe oprogramowanie (malware), phishing i inne rodzaje ataków często wykorzystują funkcje oferowane przez HTML, jako domyślny format wiadomości najlepiej wybrać zwykły tekst. Wówczas e-maile będą wyświetlane wyłącznie w formie tekstowej — wszelkie obrazki, hiperłącza i inne treści udostępniane przez HTML będą pomijane lub wyświetlane tylko za pomocą tekstu alternatywnego. Ponadto wysyłanie wiadomości e-mail w formie zwykłego tekstu jest pomocne dla innych dbających o bezpieczeństwo użytkowników, preferujących odczytywanie poczty w formie zwykłego tekstu.
- **Wyłącz automatyczny podgląd i otwieranie wiadomości e-mail.** Niektóre złośliwe programy oparte na wiadomościach e-mail mogą zostać aktywowane i zainfekować komputer w momencie podglądu lub otwarcia otrzymanej korespondencji. Wiele klientów poczty elektronicznej można skonfigurować tak, aby automatycznie wyświetlały podgląd lub otwierały wiadomość e-mail. Może to umożliwić łatwiejsze zainfekowanie komputera przez złośliwe oprogramowanie. Dlatego też klienta poczty elektronicznej należy skonfigurować w taki sposób, by wyłączyć funkcje automatycznego podglądu i otwierania wiadomości. Pozwoli to telepracownikowi zidentyfikować i usunąć wiadomość wyglądającą na podejrzaną ze względu na nadawcę, odbiorcę, temat lub inne informacje identyfikacyjne, które można sprawdzić bez przeglądania jej treści.
- **Włącz filtrowanie spamu.** Dodatkowe informacje dotyczące tego zagadnienia przedstawiono w punkcie 5.4.3.

5.5.3. Komunikatory internetowe

Telepracownikom zaleca się wdrożenie poniższych zaleceń w zakresie komunikatorów, które stosują na swoich komputerach BYOD:

- **Wyłącz wyświetlanie adresów e-mail.** Jeżeli wyświetlana nazwa konta telepracownika lub informacje pomocnicze zawierają adres e-mail, może on zostać zarejestrowany przez złośliwe oprogramowanie lub nieuprawnionych użytkowników, a następnie wykorzystany w przyszłych atakach.
- **Ogranicz przesyłanie plików.** Jeżeli komunikator umożliwia przesyłanie plików z innymi użytkownikami, funkcję tę należy skonfigurować tak, aby przed rozpoczęciem przesyłania plików telepracownik otrzymywał odpowiedni monit. Przesyłanie plików to częsty sposób na rozsyłanie złośliwego oprogramowania na inne komputery i infekowania ich.

5.5.4. Pakiety oprogramowania biurowego

Telepracownikom zaleca się wdrożenie następujących zasad w zakresie pakietów biurowych zainstalowanych na ich komputerach BYOD:

- **Ogranicz uruchamianie makr.** Aplikacje takie jak edytory tekstu i arkusze kalkulacyjne często zawierają języki makr, z których korzystają niektóre rodzaje złośliwego oprogramowania. Większość popularnych aplikacji z możliwością korzystania z makr oferuje zabezpieczenia, które zezwalają na korzystanie z makr tylko z zaufanych lokalizacji lub monitują użytkownika o zatwierdzenie lub odrzucenie każdej próby uruchomienia makra. Funkcja monitowania może być skuteczna w powstrzymywaniu zagrożeń związanych ze złośliwym oprogramowaniem opartym na makrach.
- **Ogranicz podawanie danych osobowych.** Wiele pakietów biurowych umożliwia przechowywanie informacji osobistych, takich jak nazwisko, inicjały, adres pocztowy i numer telefonu, w każdym tworzonym dokumencie. Mimo iż te najbardziej podstawowe informacje (zazwyczaj imię i inicjały) są często potrzebne do celów współpracy i śledzenia zmian, to już informacje takie jak adresy pocztowe i numery telefonów nie są do tego wymagane. Informacje

osobiste osadzone w plikach z dokumentami mogą zostać nieumyślnie przekazane innym osobom wraz z tymi plikami. Telepracownicy nie powinni wprowadzać w ustawieniach pakietów biurowych więcej danych osobowych niż jest to konieczne. Niektóre edytory tekstu umożliwiają telepracownikom korzystanie z narzędzi oczyszczania, które usuwają osadzone w dokumentach dane osobowe, komentarze, śledzone zmiany i inne informacje, które nie powinny być częścią dokumentu końcowego.

- **Przechowuj pliki aplikacji w zabezpieczonych folderach.** Większość aplikacji biurowych pozwala użytkownikom na zdefiniowanie domyślnych miejsc zapisywania dokumentów i przechowywania plików tymczasowych, w tym automatycznie zapisanych dokumentów oraz ich kopii zapasowych. Może to być niezwykle pomocne w ochronie plików aplikacji przed nieuprawnionym dostępem ze strony osób trzecich. Telepracownicy powinni również przechowywać swoje własne hasła słownikowe we własnym, odrębnym pliku zapisanym w jednym z chronionych folderów.

5.6. Konfiguracja oprogramowania do zdalnego dostępu

Jak wspomniano w rozdziale 2, telepracownicy mogą być zobowiązani do zainstalowania oprogramowania do zdalnego dostępu na swoich komputerach BYOD lub skonfigurowania tego typu oprogramowania dostarczonego z systemem operacyjnym komputera. Oprogramowanie to należy skonfigurować w oparciu o wymagania i zalecenia organizacji. W wielu przypadkach oprogramowanie do zdalnego dostępu jest wstępnie skonfigurowane przez organizację, dzięki czemu telepracownik nie musi osobiście zmieniać jego ustawień. Ogólnie rzecz ujmując, w tego rodzaju oprogramowaniu powinny być włączone tylko niezbędne funkcje. Telepracownicy powinni również pamiętać o pobieraniu i instalowaniu aktualizacji oprogramowania do zdalnego dostępu, ilekroć są one dostępne. Jeżeli aktualizacje zapewnia organizacja, telepracownik musi upewnić się, że będzie powiadamiany o ich dostępności.

5.7. Utrzymanie i monitorowanie bezpieczeństwa

Telepracownicy powinni stale dbać o bezpieczeństwo swoich komputerów BYOD. Typowe obowiązki telepracowników w tym zakresie są następujące:

- **Regularne sprawdzanie aktualności systemu operacyjnego i podstawowych aplikacji**. Wiele programów posiada opcję menu lub inny mechanizm, który wyświetla status aktualizacji, np. liczbę aktualizacji, które nie zostały jeszcze zastosowane lub ostatnią datę aktualizacji oprogramowania.
- **Regularne sprawdzanie stanu oprogramowania zabezpieczającego** w celu upewnienia się, że jest ono nadal włączone, prawidłowo skonfigurowane i aktualne. Niektóre systemy operacyjne oferują pulpity bezpieczeństwa, przedstawiające informacje o aktualnym stanie oprogramowania zabezpieczającego. Weryfikacja stanu takiego oprogramowania powinna obejmować również sprawdzenie, czy regularne skanowanie wykonywane przez oprogramowanie antywirusowe nie wykryło na komputerze żadnych infekcji. Jeśli urządzenie nadal jest zainfekowane, telepracownik powinien postępować zgodnie z instrukcjami oprogramowania antywirusowego dotyczącymi usuwania (dezynfekcji) złośliwego oprogramowania z komputera.
- **Tworzenie nowego konta użytkownika** za każdym razem, gdy inna osoba ma zacząć korzystać z komputera, jak również wyłączanie lub usuwanie takiego konta, gdy dana osoba nie ma już potrzeby korzystania z urządzenia. Wszystkie konta użytkowników należy okresowo przeglądać, aby upewnić się, że włączone są tylko te niezbędne.
- **Regularna zmiana hasła do komputera** telepracownika zgodnie z polityką haseł organizacji.
- **Regularne sprawdzanie komputera pod kątem problemów bezpieczeństwa**. Niektóre systemy operacyjne oferują narzędzia, które można uruchomić, aby sprawdzić komputer pod kątem potencjalnych problemów. Narzędzia te mogą zidentyfikować brakujące aktualizacje oprogramowania i nieprawidłowe ustawienia zabezpieczeń, a także dostarczyć zalecenia dotyczące rozwiązania

problemów. Niemniej zrozumienie raportów generowanych przez takie programy i prawidłowe wdrożenie zalecanych rozwiązań mogą wymagać posiadania dużej wiedzy na temat bezpieczeństwa. Telepracownicy nieposiadający wystarczającego doświadczenia w tym zakresie powinni zasięgnąć porady eksperta przed wdrożeniem jakichkolwiek zaleceń, które są dla nich niejasne.

Telepracownicy muszą również badać każdy przypadek nietypowego zachowania komputera. Zwykle najlepiej jest rozpocząć ten proces od upewnienia się, że oprogramowanie komputera (zwłaszcza oprogramowanie antywirusowe) jest w pełni aktualne. Następnie należy przeskanować cały komputer za pomocą programu antywirusowego. Jeżeli zostanie wykryte złośliwe oprogramowanie, należy je usunąć za pomocą oprogramowania antywirusowego. W przypadku braku wykrycia złośliwych narzędzi następnym krokiem powinno być ponowne uruchomienie komputera, które pozwala naprawić wiele błędów. Jeżeli ww. czynności nie przyniosą pożądanych skutków, należy podjąć dodatkowe działania związane z rozwiązywaniem problemów. Przykłady obejmują:

- **Sprawdzenie stron internetowych producentów programów antywirusowych** pod kątem występowania złośliwego oprogramowania, które powoduje zaobserwowane nietypowe zachowania,
- Odinstalowanie i ponowne zainstalowanie aplikacji, która nie działa prawidłowo,
- Przeszukanie strony internetowej producenta systemu operacyjnego w poszukiwaniu informacji o podobnych problemach; oraz
- **Zastosowanie narzędzi do rozwiązywania problemów**, które mogą pomóc ustalić przyczynę problemów z komputerem.

Jeżeli po wykonaniu takich czynności problem nadal nie ustępuje lub jeśli telepracownik nie posiada wystarczającej wiedzy, aby je wykonać, to wówczas powinien zwrócić się o pomoc do eksperta, np. do działu pomocy technicznej organizacji — jeśli organizacja zapewnia wsparcie dla komputerów BYOD. Telepracownicy mogą pomóc w rozwiązywaniu problemów poprzez zbieranie

i dokumentowanie dotyczących ich informacji. Niektóre systemy operacyjne posiadają funkcje, które automatyzują ten proces. Ponadto część producentów komputerów PC instaluje na swoich urządzeniach narzędzia przeznaczone specjalnie do tego celu. Telepracownikom zaleca się zapoznanie z instrukcją obsługi sprzętu komputerowego i systemu operacyjnego w celu uzyskania informacji na temat takich funkcji. Telepracownicy powinni również zapisywać komunikaty o błędach, wykonując zrzut ekranu, kopiując i wklejając komunikat o błędzie do pliku lub wiadomości e-mail, lub zapisując komunikat o błędzie w jego dosłownym brzmieniu na papierze. Odpowiednią technikę w tym zakresie należy wybrać w zależności od złożoności komunikatu o błędzie i ewentualnej możliwości wykonania zrzutu ekranu przez komputer.

6. ZABEZPIECZANIE URZĄDZEŃ MOBILNYCH BYOD UŻYWANYCH DO TELEPRACY/PRACY ZDALNEJ

Telepracownikom korzystającym z mobilnych urządzeń BYOD do wykonywania telepracy/pracy zdalnej, w szczególności smartfonów i tabletów, zaleca się wdrożenie zasad przedstawionych w tym rozdziale. Istnieje wiele różnych urządzeń mobilnych, a dostępne dla nich funkcje bezpieczeństwa także są niezwykle zróżnicowane. Niektóre urządzenia posiadają tylko kilka podstawowych zabezpieczeń, zaś inne dają użytkownikom dostęp do zaawansowanych funkcji podobnych do tych oferowanych przez komputery. Jednak w tym przypadku więcej nie zawsze znaczy lepiej: w rzeczywistości wiele urządzeń oferuje więcej zabezpieczeń dlatego, że oferowane przez nie funkcje czynią je bardziej podatnymi na ataki w porównaniu do takich, które tych funkcji nie posiadają. Ogólnie rzecz biorąc, urządzenia mobilne są obecnie mniej narażone na niebezpieczeństwo niż komputery PC, jednakże skala zagrożeń dla tych pierwszych stale rośnie. Różnorodność dostępnych zabezpieczeń sprawia, że opracowanie szczegółowych zaleceń dotyczących wszystkich urządzeń mobilnych jest niemożliwe. Telepracownik powinien zatem zapoznać się z dokumentacją dostarczoną przez producenta swojego urządzenia oraz dostawcę usług (np. usług telefonii komórkowej) i przestrzegać ich zaleceń dotyczących bezpieczeństwa. Ogólne zalecenia są następujące:

- **Ogranicz dostęp do urządzenia.** Większość urządzeń mobilnych umożliwia właścicielowi ograniczenie dostępu poprzez ustawienie kodu PIN lub hasła. Niektóre urządzenia obsługują również bardziej zaawansowane mechanizmy uwierzytelniania, takie jak biometria (np. odcisk kciuka właściciela, skan twarzy). Zastosowanie mechanizmu uwierzytelniania uniemożliwia dostęp do informacji i usług telepracownika nieuprawnionej osobie, która uzyskała fizyczny dostęp do urządzenia, bądź też zniechęca ją do podjęcia próby uzyskania do nich dostępu. Niektóre urządzenia można również skonfigurować tak, aby blokowały się automatycznie po pewnym okresie bezczynności — wówczas osoba próbująca skorzystać z urządzenia musi się ponownie uwierzytelnić, by je

odblokować.[30] Kody PIN oraz hasła należy zmieniać okresowo, a także każdorazowo w sytuacji, gdy telepracownik podejrzewa, że mogła je poznać inna osoba. Każdy kod PIN i każde hasło powinny być unikatowe i różne od tych używanych do logowania do innych urządzeń lub aplikacji — tak obecnie, jak i w przeszłości. Pozwoli to uniknąć ich przechwycenia przez osoby trzecie i wykorzystania do uzyskania dostępu do innych urządzeń, aplikacji, stron internetowych itp.

- **Wyłącz funkcje sieciowe, jeśli nie są potrzebne.** Urządzenia mobilne oferują wiele rodzajów funkcji sieciowych, np. IEEE 802.11, Bluetooth i NFC.[31] Atakujący mogą próbować wykorzystać te możliwości, aby uzyskać dostęp do informacji zapisanych na urządzeniu lub skorzystać z jego usług. Aby temu zapobiec, należy wyłączyć wszelkie nieużywane funkcje sieciowe i uruchamiać je tylko wtedy, gdy będą używane. Przykładowo, jeśli od czasu do czasu korzystamy ze słuchawki Bluetooth łączącej się ze smartfonem, to powinniśmy włączać funkcję Bluetooth w smartfonie tylko wtedy, gdy chcemy skorzystać ze słuchawki. Po zakończeniu korzystania z niej, funkcję Bluetooth należy wyłączyć. Każda włączona funkcja sieciowa przynosi zwiększone ryzyko udanego ataku, dlatego też telepracownicy powinni wziąć pod uwagę ryzyko stwarzane przez taką funkcję przed jej włączeniem (np. aktywacja Bluetooth w zatłoczonym miejscu publicznym zasadniczo jest bardziej ryzykowna niż uruchomienie tej funkcji w przestrzeni prywatnej).

[30] Niektóre urządzenia można skonfigurować tak, aby ich zawartość ulegała automatycznemu wymazaniu po określonej liczbie nieudanych prób uwierzytelnienia. Jeżeli ta funkcja jest włączona, telepracownicy powinni regularnie wykonywać kopie zapasowe informacji znajdujących się na urządzeniu, aby można było je odtworzyć w przypadku wymazania danych na skutek zbyt wielu prób uwierzytelnienia.

[31] Niektóre urządzenia są także kompatybilne z kartami sieciowymi innych firm, które zapewniają im dodatkowe funkcje sieciowe. Należy zapoznać się z dokumentacją takich kart i usunąć lub wyłączyć je, jeżeli nie są potrzebne.

- **Regularnie aktualizuj swoje urządzenia.** W większości urządzeń mobilnych można instalować aktualizacje lub łatki w celu eliminowania znanych błędów w zakresie bezpieczeństwa. Urządzenia mogą umożliwiać dokonywanie aktualizacji bezpośrednio (np. telepracownik wybiera na urządzeniu odpowiednią opcję, aby pobrać aktualizację) lub pośrednio (np. telepracownik pobiera łatkę na komputer, a następnie instaluje ją na urządzeniu mobilnym poprzez kabel do transmisji danych). Jeżeli urządzenie umożliwia instalowanie aktualizacji, telepracownicy powinni postępować zgodnie z dostarczonymi instrukcjami, aby zapewnić sprawdzanie dostępności, pobieranie i instalowanie aktualizacji w momencie jej wydania. Informacje na temat pobierania aktualizacji poprzez sieci z limitem transferu danych znajdują się w rozdziale 5.1.
- **Skonfiguruj aplikacje tak, aby zapewniały bezpieczeństwo.** Domyślna konfiguracja wielu aplikacji na urządzeniach mobilnych, np. przeglądarek internetowych, często przedkłada funkcjonalność nad bezpieczeństwo. W związku z tym telepracownicy powinni rozważyć wyłączenie niepotrzebnych funkcji aplikacji i skonfigurowanie tego typu programów tak, aby zatrzymywały lub blokowały potencjalnie złośliwe działania. W punkcie 5.5 przedstawiono zalecenia dotyczące konfiguracji przeglądarek internetowych, klientów poczty elektronicznej i komunikatorów internetowych na komputerach osobistych. W miarę możliwości zalecenia te należy również stosować w odniesieniu do urządzeń mobilnych.
- **Pobieraj i uruchamiaj aplikacje tylko z autoryzowanych sklepów z aplikacjami.** Telepracownicy powinni zachować ostrożność przy pobieraniu i instalowaniu oprogramowania, które nie jest dostarczane przez organizację lub producenta urządzenia. Przykładem może być pobieranie gier z nieznanej strony internetowej. Takie programy mogą zmniejszyć bezpieczeństwo urządzenia, jeżeli nie zostaną odpowiednio skonfigurowane, a dodatkowo same w sobie mogą zawierać złośliwe oprogramowanie zdolne do zainfekowania go. Mogą również nieumyślnie zakłócać działanie innych aplikacji, w tym oprogramowania zabezpieczającego.

- **Unikaj zabiegów takich jak jailbreak czy rootowanie.** Takie działania skutkują wyłączeniem wbudowanych przez producenta zabezpieczeń urządzenia. Korzystanie z urządzenia staje się tym samym na tyle ryzykowne, że obecnie wiele organizacji automatycznie sprawdza urządzenia mobilne próbujące uzyskać dostęp do ich sieci i usług pod kątem oznak jailbreak'u lub rootowania i uniemożliwia im taki dostęp. **Unikaj podłączania urządzenia do nieznanych stacji ładowania.** Wiele stacji ładowania umożliwia ładowanie urządzeń mobilnych poprzez bezpośrednie połączenie przewodowe między interfejsem USB urządzenia a stacją ładowania. Istnieje jednak ryzyko, że jakaś osoba zmodyfikowała stację ładowania, np. dostępną w miejscu publicznym, sprawiając, że próbuje ona automatycznie uzyskać nieuprawniony dostęp do danych, aplikacji, usług i innych zasobów podłączonych do niej urządzeń mobilnych.
- W celu uzyskania dostępu do danych i usług organizacji korzystaj z odizolowanego, chronionego i zaszyfrowanego środowiska wspieranego i zarządzanego przez organizację. Jeżeli takie środowisko jest dostępne, jest ono zazwyczaj automatycznie generowane i utrzymywane na urządzeniach mobilnych, dzięki czemu telepracownicy nie muszą podejmować żadnych działań. Środowisko to izoluje dane, aplikacje i inne pliki przechowywane przez organizację na urządzeniu mobilnym, pozwalając jej zachować nad nimi kontrolę. Jednocześnie nie posiada ona dostępu do informacji osobistych, plików itp. przechowywanych przez telepracownika na tym samym urządzeniu.

Telepracownicy powinni zachować ostrożność przy podłączaniu urządzeń mobilnych do komputerów, np. przy synchronizacji danych między smartfonem a komputerem. Podczas synchronizacji może dojść do przeniesienia złośliwego oprogramowania z jednego urządzenia na drugie. Synchronizacja może również spowodować nieumyślne przeniesienie informacji wrażliwych z jednego urządzenia na inne, a takie urządzenie może nie być skonfigurowane w sposób zapewniający ich odpowiednią ochronę, stwarzając większe ryzyko ich ujawnienia. Przed podłączeniem urządzenia mobilnego do komputera **należy upewnić się**, że urządzenia są odpowiednio zabezpieczone.

7. UWZGLĘDNIENIE BEZPIECZEŃSTWA URZĄDZEŃ OSÓB TRZECICH

Zdarza się, że telepracownicy chcą uzyskać zdalny dostęp do zasobów firmowych z urządzeń należących do osób trzecich, np. sprawdzić pocztę, korzystając z kiosku multimedialnego na konferencji. Jeśli jednak za zabezpieczenie urządzenia odpowiada strona trzecia, telepracownicy zazwyczaj nie wiedzą, czy dokonano tego odpowiednio. Wówczas telepracownik może zainicjować zdalny dostęp z urządzenia stwarzającego zagrożenie, na przykład zainfekowanego złośliwym oprogramowaniem przeznaczonym do kradzieży informacji użytkowników, takich jak hasła czy wiadomości e-mail.

Wiele organizacji zabrania używania urządzeń osób trzecich do celów zdalnego dostępu lub zezwala na to tylko w ograniczonym zakresie, np. do obsługi poczty internetowej. Jeśli organizacja zezwala na korzystanie z urządzeń osób trzecich do telepracy/pracy zdalnej, telepracownicy powinni wziąć pod uwagę środowisko pracy takiego urządzenia przed podjęciem decyzji o jego użyciu. Korzystanie przez telepracownika z urządzenia BYOD należącego do osoby trzeciej wiąże się z większym ryzykiem niż korzystanie z własnego urządzenia BYOD. W tym pierwszym przypadku nie ma bowiem pewności, w jaki sposób zabezpieczono urządzenie. Telepracownikom zaleca się uwzględnienie tego, kto jest odpowiedzialny za zabezpieczenie urządzenia osoby trzeciej i kto ma do niego dostęp. Przykładowo kiosk multimedialny dostępny wyłącznie dla uczestników konferencji będzie prawdopodobnie lepiej zabezpieczony niż taki ustawiony w ogólnodostępnym lobby w hotelu. W miarę możliwości telepracownicy nie powinni wykorzystywać publicznie dostępnych urządzeń do telepracy/pracy zdalnej, w tym do zdalnego dostępu do poczty elektronicznej i innych aplikacji.

Telepracownicy powinni unikać używania urządzeń osób trzecich do wykonywania wrażliwych działań lub uzyskiwania dostępu do wrażliwych informacji. Jeżeli telepracownik nie ma wystarczającej pewności co do bezpieczeństwa urządzenia osoby trzeciej, powinien unikać korzystania z niego. Ze względu na obawy związane z bezpieczeństwem wielu telepracowników decyduje się nie wykorzystywać do zdalnego dostępu żadnych urządzeń zabezpieczonych przez osoby trzecie.

ZAŁĄCZNIK A — DODATKOWE KWESTIE ZWIĄZANE Z BEZPIECZEŃSTWEM TELEPRACY/PRACY ZDALNEJ

Oprócz zabezpieczenia urządzeń do telepracy/pracy zdalnej i sieci domowych istnieją także inne kwestie związane z bezpieczeństwem telepracy/pracy zdalnej. Telepracownicy powinni na przykład wziąć pod uwagę bezpieczeństwo usług telefonicznych, takich jak bezprzewodowe telefony stacjonarne, telefony komórkowe i usługi Voice over internet Protocol (VoIP). Inne możliwe kwestie związane z bezpieczeństwem obejmują wykorzystanie technologii bezprzewodowych sieci osobistych (WPAN), takich jak Bluetooth, korzystanie z bezprzewodowych sieci szerokopasmowych, a także bezpieczne niszczenie nośników wymiennych, materiałów drukowanych oraz innych nośników mogących zawierać informacje wrażliwe. W niniejszym załączniku zawarto zalecenia dotyczące każdego z powyższych.

A.1 Usługi telefoniczne

W zależności od wrażliwości komunikacji w ramach telepracy/pracy zdalnej może być konieczne uwzględnienie bezpieczeństwa telefonu. Ogromna dostępność urządzeń i usług telefonicznych daje dziś szerokie spektrum możliwości w zakresie ochrony prywatności. Stosunkowo najniższy poziom bezpieczeństwa zapewniają starsze modele bezprzewodowych telefonów stacjonarnych, których rozmowy można podsłuchiwać przez krótkofalówki, elektroniczne nianie czy skanery radiowe; z kolei najwyższy — telefony przewodowe. Poniżej przedstawiono najczęściej stosowane opcje.

- **Telefony przewodowe wykorzystujące tradycyjne przewodowe sieci telefoniczne.** Do przechwycenia komunikacji prowadzonej za pomocą tradycyjnego telefonu korzystającego z sieci przewodowej wymagane jest fizyczne połączenie z taką siecią. To sprawia, że tego typu rozwiązanie zapewnia wystarczające bezpieczeństwo w przypadku typowej telepracy/pracy zdalnej. Kwestie dotyczące bezpieczeństwa telefonów przewodowych korzystających z sieci VoIP opisano poniżej.

- **Telefony bezprzewodowe wykorzystujące tradycyjne przewodowe sieci telefoniczne.** Komunikacja prowadzona przez telefon bezprzewodowy może zostać podsłuchana przez osoby znajdujące się w pobliżu urządzenia — zwykle nie dalej niż kilkaset metrów. Bezprzewodowe aparaty telefoniczne używane do telepracy/pracy zdalnej powinny wykorzystywać technologię szerokopasmowe lub systemy z rozproszonym widmem (*ang. spread spectrum*), która wykorzystuje szybko zmieniający się zestaw częstotliwości do zakodowania (*ang. scramble*) transmisji, zmniejszając w ten sposób ryzyko podsłuchu. Kwestie dotyczące bezpieczeństwa telefonów bezprzewodowych korzystających z sieci VoIP opisano poniżej.
- **Telefony komórkowe.** Transmisje sieci komórkowej są zakodowane, aby uniemożliwić podsłuchiwanie, a zatem ich użycie w przypadku typowej telepracy/pracy zdalnej należy uznać za dopuszczalne.
- **Voice over IP.** Istnieje wiele rozwiązań oferujących usługi telefonii przez Internet. Działanie takich usług, zwanych VoIP, polega na przetwarzaniu mowy na komunikację internetową i przesyłaniu jej do urządzenia połączonego z siecią telefoniczną. Rozmówca po drugiej stronie może korzystać z dowolnego rodzaju usług telefonicznych, nie tylko VoIP. Z punktu widzenia bezpieczeństwa należy mieć na uwadze, że taki rodzaj połączenia może być podatny na podsłuch, gdyż komunikacja może odbywać się poprzez sieć lokalną i internet. Ze względu na możliwość wystąpienia słabych punktów (podatności) w jednej lub kilku z tych sieci, komunikacja za pośrednictwem VoIP nie powinna być uważana za bezpieczną, chyba że zastosowane zostanie szyfrowanie. Wiele usług VoIP zapewnia silne szyfrowanie. Telepracownicy zainteresowani wykorzystaniem w ramach telepracy/pracy zdalnej technologii VoIP do rozmów dotyczących informacji wrażliwych lub zastrzeżonych handlowo, powinni najpierw sprawdzić u dostawcy VoIP, czy komunikacja jest szyfrowana i czy takie szyfrowanie spełnia wymagania odpowiedniego organu.

A.2 Technologie WPAN

WPAN to sieci bezprzewodowe o niewielkim zasięgu, których działanie nie wymaga dostępności infrastruktury. Sieci WPAN zazwyczaj wykorzystuje się do komunikacji pomiędzy kilkoma urządzeniami w jednym pomieszczeniu bez konieczności fizycznego łączenia ich przewodami. Przykładem może być używanie bezprzewodowej klawiatury lub myszy z komputerem, drukarki bezprzewodowe, synchronizacja smartfona z laptopem czy też możliwość używania bezprzewodowego zestawu słuchawkowego lub słuchawki z telefonem komórkowym. Najczęściej stosowaną technologią sieci WPAN jest Bluetooth. Z racji, że rozwiązanie to nie wymaga, aby na linii wzroku pomiędzy korzystającymi z niego urządzeniami nie znajdowały się żadne przeszkody, urządzenia Bluetooth mogą być umieszczone w odległości do 100 metrów od siebie, w zależności od mocy wyjściowej.

Jak wspomniano w rozdziałach 5 i 6, telepracownicy powinni wyłączyć funkcję Bluetooth, gdy nie jest ona używana. Użytkownicy Bluetooth powinni ponadto stosować kod PIN o długości co najmniej ośmiu znaków — najlepiej złożony z liter i cyfr. Utrudni to atakującemu odgadnięcie kodu PIN i uzyskanie dostępu do urządzeń Bluetooth. Jeśli urządzenie Bluetooth nie obsługuje długich kodów PIN (niektóre dopuszczają jedynie zastosowanie kodu czterocyfrowego), telepracownicy powinni wybrać PIN, który będzie trudny do odgadnięcia. Telepracownicy powinni również skonfigurować swoje urządzenia Bluetooth tak, aby szyfrowały komunikację, jeśli posiadają taką opcję. Dokumentacja urządzeń powinna zawierać wszelkie niezbędne informacje na temat konfiguracji funkcji szyfrowania.

A.3 Technologie bezprzewodowych sieci szerokopasmowych

Bezprzewodowe sieci szerokopasmowe to mobilne sieci dla komputerów PC. Technologia ta umożliwia urządzeniom bezprzewodowy dostęp do internetu praktycznie z dowolnego miejsca. Ze względu na charakter komunikacji przez sieć komórkową, podsłuchanie bezprzewodowej sieci szerokopasmowej jest dla atakującego znacznie trudniejsze niż w przypadku sieci WLAN, lecz nadal jest możliwe. Telepracownicy powinni zatem zakładać, że bezprzewodowa komunikacja szerokopasmowa nie jest wystarczająco bezpieczna do przesyłania informacji

wrażliwych. Przed użyciem bezprzewodowego łącza szerokopasmowego do przesyłania lub odbierania informacji wrażliwych, telepracownik powinien skonsultować się ze swoją organizacją, aby ustalić, jakie zabezpieczenia zapewnia stosowane przez nią rozwiązanie zdalnego dostępu.

A.4 Niszczenie informacji

Jeśli komputer należący do telepracownika nie będzie już używany, należy go odpowiednio przygotować do wycofania z eksploatacji. Zamontowane w komputerze urządzenia pamięci masowej, np. dyski twarde, często zawierają informacje nieprzeznaczone dla osób innych niż telepracownik, w tym pliki organizacji, dane osobowe czy też pliki oprogramowania do rozliczeń podatkowych. Nawet jeżeli telepracownik usunie z komputera wszystkie pliki, to osoby postronne, które uzyskają dostęp do urządzenia, mogą być w stanie odzyskać je za pomocą darmowego lub stosunkowo taniego oprogramowania do odzyskiwania usuniętej zawartości. Dlatego też przed przekazaniem komputera innej osobie lub jego sprzedażą bądź utylizacją, telepracownik powinien upewnić się, że wszystkie dane zapisane w urządzeniach pamięci masowej takiego komputera zostały usunięte. Usunięcia danych dokonuje się następującymi metodami:

- **Użycie oferowanego przez niezależnego dostawcę programu do czyszczenia dysku**. Na rynku dostępnych jest kilka programów komercyjnych i open source, które są specjalnie zaprojektowane do usuwania śladów danych z komputerów. Usuwając dane z dysku twardego z użyciem takiego rozwiązania należy przestrzegać wskazówek producenta.
- **Zachowanie dysku twardego**. Telepracownik może wymontować dysk twardy z komputera, postępując zgodnie z instrukcjami zawartymi w dokumentacji producenta urządzenia. Jeżeli w przyszłości z komputera będą chciały korzystać inne osoby, to wówczas mogą zakupić nowy dysk twardy i zainstalować na nim system operacyjny. Jest to najlepsze rozwiązanie w sytuacji, gdy komputer nie działa już prawidłowo, uniemożliwiając zastosowanie narzędzi do oczyszczania dysku.

- **Zniszczenie dysku twardego**. Dysk twardy można rozmagnesować, umieszczając go w polu magnetycznym. Takie działanie czyni nośnik niezdatnym do użytku. Dyski twarde można również rozdrobnić lub w inny sposób fizycznie zniszczyć za pomocą specjalistycznego sprzętu i usług.

Telepracownicy muszą również zadbać o zniszczenie nośników wymiennych, materiałów drukowanych oraz innych nośników, które mogą zawierać wrażliwe informacje. Wiele organizacji zapewnia swoim telepracownikom usługi niszczenia informacji, obejmujące np. wymazywanie lub niszczenie dysków twardych, a także niszczenie nośników wymiennych i materiałów drukowanych.

W przypadku urządzeń BYOD usuwanie danych może okazać się problematyczne. Takie urządzenia są bowiem używane zarówno do celów osobistych, jak i zawodowych, a zatem może być konieczne usunięcie danych dotyczących telepracy/pracy zdalnej bez wpływu na prywatne dane użytkownika.

Selektywne wymazywanie danych można przeprowadzić za pomocą oprogramowania do zarządzania urządzeniami mobilnymi organizacji (w przypadku urządzeń mobilnych) oraz specjalistycznych narzędzi. Telepracownicy powinni skonsultować się ze swoją organizacją w sprawie możliwości usuwania danych z urządzeń BYOD.

ZAŁĄCZNIK B — SŁOWNIK

Poniżej zdefiniowano wybrane pojęcia użyte w publikacji.

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

Biała lista (*ang. whitelist*): Lista zaufanych nadawców wiadomości e-mail, np. współpracownicy, przyjaciele i rodzina użytkownika.

Czarna lista (*ang. blacklist*): Lista nadawców poczty elektronicznej, którzy wcześniej wysyłali spam do użytkownika.

Dezynfekcja (*ang. disinfect*): Usuwanie złośliwego oprogramowania z pliku.

Filtrowanie treści (*ang. content filtering*): Proces monitorowania komunikacji, takiej jak poczta elektroniczna i strony internetowe, analizowania ich pod kątem podejrzanych treści i zapobiegania dostarczaniu podejrzanych treści użytkownikom.

Identyfikator SSID (*ang. service set identifier - SSID*): Nazwa nadawana punktowi dostępu do sieci bezprzewodowej.

Komputer osobisty/Komputer PC (*ang. personal computer - PC*): : Komputer stacjonarny lub laptop.

Konto administratora (*ang. administrative account*): Konto użytkownika posiadające pełne uprawnienia do zarządzania komputerem. Takie konto jest przeznaczone wyłącznie do wykonywania zadań związanych z zarządzaniem komputerem osobistym (PC), takich jak instalowanie aktualizacji i oprogramowania, zarządzanie kontami użytkowników oraz modyfikowanie ustawień systemu operacyjnego (OS) i aplikacji.

Konto do użytku codziennego (*ang. daily use account*): Patrz *Konto użytkownika standardowego*.

Konto użytkownika standardowego (*ang. standard user account*): Konto użytkownika z ograniczonymi uprawnieniami, które wykorzystuje się do ogólnych zadań, takich jak odczytywanie poczty elektronicznej i odwiedzanie stron internetowych.

Kwarantanna (*ang. quarantine*): Odizolowanie plików zawierających złośliwe oprogramowanie w celu przyszłej dezynfekcji lub zbadania.

Osobista zapora sieciowa (*ang. personal firewall*): Program monitorujący komunikację między komputerem a innymi komputerami i blokujący niechcianą komunikację.

Podatność (*ang. vulnerability*): Luka w zabezpieczeniach komputera.

Socjotechnika (*ang. social engineering*): Ogólny termin określający ataki, w ramach których atakujący usiłuje podstępem zmusić ofiarę do ujawnienia wrażliwych informacji lub wykonania pewnych czynności, np. pobrania i wykonania pliku, który wydaję się być nieszkodliwy, ale w rzeczywistości zawiera złośliwe oprogramowanie.

Środki bezpieczeństwa (*ang. security controls*): Patrz: *Zabezpieczenia*.

Telepraca (*ang. telework*; *telecommuting*): Wykonywanie pracy przez pracowników organizacji, kontrahentów, partnerów biznesowych, sprzedawców i innych użytkowników z miejsc innych niż siedziba organizacji.

Urządzenie do telepracy/pracy zdalnej (*ang. telework device*): Komputer lub urządzenie mobilne używane przez telepracownika do wykonywania telepracy/pracy zdalnej.

Urządzenie mobilne (*ang. mobile device*): Niewielki, przenośny komputer, taki jak smartfon lub tablet.

Wirtualna sieć prywatna (*ang. Virtual Private Network - VPN*): „Tunel", przez który komputer telepracownika łączy się z siecią organizacji.

Wyłudzanie informacji (*ang. phishing*): Komputerowe działania, których celem jest podstępem nakłonić ofiarę do ujawnienia wrażliwych danych osobowych.

Wyskakujące okienko (*ang. popup window*): Osobne okno przeglądarki internetowej, które otwiera się automatycznie po załadowaniu strony internetowej lub wykonaniu przez użytkownika konkretnej czynności.

Zabezpieczenia (*ang. security protections*): Środki przeciwdziałania zagrożeniom, które mają na celu zrekompensowanie słabości w zakresie bezpieczeństwa komputera.

System zdalnego dostępu (*ang. : remote system control*): Zdalne korzystanie z komputera znajdującego się na terenie obiektu organizacji za pośrednictwem komputera do telepracy/pracy zdalnej.

Zdalny dostęp (*ang. remote access*) : Możliwość uzyskania przez użytkowników organizacji dostępu do jej niepublicznych zasobów komputerowych z lokalizacji innych niż obiekty organizacji.

Złośliwe oprogramowanie (ang. malware): Program komputerowy, który jest potajemnie umieszczany na komputerze z zamiarem naruszenia prywatności, rzetelności lub niezawodności danych, aplikacji bądź systemu operacyjnego komputera.

Złośliwy kod (*ang. malicious code*): Patrz: *Złośliwe oprogramowanie.*

ZAŁĄCZNIK C — AKRONIMY I SKRÓTY

Akronimy i skróty użyte w niniejszym poradniku zdefiniowano poniżej.

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

AES	*Advanced Encryption Standard* — Zaawansowany standard szyfrowania
AP	*Access Point* — Punkt dostępu do sieci bezprzewodowej
BIOS	*Basic Input/Output System* — Podstawowy system wejścia/wyjścia[32]
FIPS	*Federal Information Processing Standards* — Federalne standardy przetwarzania informacji
FISMA	*Federal Information Security Management Act* — Ustawa federalna o zarządzaniu bezpieczeństwem informacji
FTP	*File Transfer Protocol* — Protokół transferu plików
HTML	*Hypertext Markup Language* — Hipertekstowy język znaczników
HTTP	*Hypertext Transfer Protocol* — Protokół przesyłania dokumentów hipertekstowych
IEEE	*Institute of Electrical and Electronics Engineers, Inc.*

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

IP	*Internet Protocol* — Protokół internetowy
IPsec	*Internet Protocol Security* — Protokół IPsec
ISP	*Internet Service Provider* — Dostawca usługi dostępu do internetu
IT	*Information Technology* — Informatyka
ITL	*Information Technology Laboratory* — Laboratorium informatyczne
MAC	*Media Access Control* — Sprzętowy adres karty sieciowej/Adres MAC
NAT	*Network Address Translation* — Translacja adresów sieciowych
NFC	*Near Field Communication* — Komunikacja bliskiego zasięgu
NIST	*National Institute of Standards and Technology* — Narodowy Instytut Standaryzacji i Technologii
OMB	*Office of Management and Budget* — Biuro Zarządzania i Budżetu
OS	*Operating System* — System operacyjny
PC	*Personal Computer* — Komputer osobisty/Komputer PC
PII	*Personally Identifiable Information* — Dane identyfikacyjne
PIN	*Personal Identification Number* — Osobisty numer identyfikacyjny/kod PIN

PIV	*Personal Identity Verification* — Inteligentna karta PIV/poświadczenie PIV
SMTP	*Simple Mail Transfer Protocol* — Prosty protokół przesyłania poczty
SSID	*Service Set Identifier* — Identyfikator SSID
SSL	*Secure Sockets Layer* — Protokół SSL
TKIP	*Temporal Key Integrity Protocol* — Protokół TKIP
VDI	*Virutal Desktop Infrastructure* — Infrastruktura pulpitu wirtualnego
VMI	*Virtual Mobile Infrastructure* — Wirtualna infrastruktura mobilna
VoIP	*Voice over internet Protocol* — Usługi VoIP
VPN	*Virtual Private Network* — Wirtualna sieć prywatna/VPN
WEP	*Wired Equivalent Privacy* — Szyfrowanie WEP
WPA	*Wi-Fi Protected Access* — Szyfrowanie WPA
WPAN	*Wireless Personal Area Network* — Bezprzewodowa sieć osobista

ZAŁĄCZNIK D — REFERENCJE

Poniższe zestawienia zawierają przykłady zasobów, które mogą być pomocne w zabezpieczaniu urządzeń wykorzystywanych do telepracy/pracy zdalnej.

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[33]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-46	*Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD)*.- na podstawie NIST SP 800-46.
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53

[33] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[33]	
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[34]

Strony internetowe z zasobami

Nazwa strony	URL
National Checklist Program Repository	http://checklists.nist.gov/
Safety & Security Center	http://www.microsoft.com/security/default.aspx
StaySafeOnline.org	http://www.staysafeonline.org/
telework.gov	http://www.telework.gov/

Dokumenty

Nazwa dokumentu	URL
Best Practices for Keeping Your Home Network Secure	https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure.pdf
NIST Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*	http://dx.doi.org/10.6028/NIST.SP.800-46r2
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 800-121 Revision 1, *Guide to Bluetooth Security*	http://dx.doi.org/10.6028/NIST.SP.800-121r1

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

Nazwa dokumentu	URL
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 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*	http://dx.doi.org/10.6028/NIST.SP.800-153