Materiały dydaktyczne do konkursu

CyberSkiller

Materiały dydaktyczne do konkursu

CyberSkiller

Spis treści

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Część I

Top 10 codziennych dobrych praktyk w cyberświecie

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 10 – Zwracaj uwagę na otoczenie

Wprowadzenie

Codziennie znajdujemy się w przeróżnych miejscach. Niezależnie od tego, czy to dom, szkoła czy praca - ważne jest, aby zwracać uwagę na ludzi przebywających w naszym otoczeniu. Może się zdarzyć, że w Twoim środowisku zaczną dziać się podejrzane rzeczy, które mogą mieć związek z hakerami i próbami oszukania Cię podczas Twojej **powszedniej rutyny**. Pamiętaj, że atak na Twoich współlokatorów i rówieśników może doprowadzić do wycieku także Twoich poufnych informacji. Wówczas sam staniesz się ofiarą, a Twoja sieć może zostać poważnie uszkodzona i podatna na dalsze hakerskie działania.

Cyber Fakt

Przykładowym zagrożeniem, które może zdarzyć się przez brak uważności na otaczającą nas rzeczywistość, jest atak znany jako ***tailgating***. W tego typu ataku osoba atakująca podąża za uwierzytelnionym pracownikiem do obszaru o ograniczonym dostępie. Agresor może na przykład **podszyć się** pod kierowcę samochodu dostawczego i cierpliwie czekać na zewnątrz budynku aż do rozpoczęcia ataku. Kiedy pracownik uzyskuje zgodę ochrony i otwiera drzwi, osoba atakująca zwyczajnie prosi pracownika o ich przytrzymanie, uzyskując w ten sposób dostęp do budynku.

Tailgating nie działa jednak we wszystkich środowiskach korporacyjnych. W dużych firmach często wymagane jest użycie specjalnych, indywidualnych kart dostępu. Za to w średnich przedsiębiorstwach napastnicy mogą bez problemu nawiązać rozmowę z pracownikami i wykorzystać ten krótki przejaw znajomości, aby sprawnie ominąć recepcję.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Konsultant ds. bezpieczeństwa w Siemens Enterprise Communications, Colin Greenless, wykorzystał tę taktykę, aby uzyskać dostęp do wielu pięter i pokojów z danymi w firmie finansowej notowanej na giełdzie. Był nawet w stanie pracować incognito przez kilka dni w sali konferencyjnej tej firmy – cały czas jako osoba nieznana przez nikogo w tej organizacji.

Dobre praktyki

- Zwracaj uwagę na dziwne i odbiegające od codzienności zdarzenia. Być może hakerzy próbują przekonać Cię do uwierzenia w ich szczerość i dobre zamiary. Musisz jednak pamiętać, że mają oni na celu wyłudzenie Twoich danych - czyli zwyczajne oszustwo.

- Zwracaj również szczególną uwagę na działania odbywające się w Twoim otoczeniu. Sprawdzaj, czy nowo pojawiające się osoby mają odpowiednie upoważnienia. Zawsze zastanów się dwa razy, czy nie próbują wykorzystać technologii oraz Twojej nieuwagi w złych celach.

- Rozmawiaj ze swoimi współpracownikami, rówieśnikami oraz współlokatorami. Zwracajcie uwagę na czynności odbiegające od normy. Informujcie się wzajemnie o podejrzanych sytuacjach. Dzięki temu unikniecie ataku prowadzącego do wycieku danych.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 9 – Zwiększaj świadomość zasad cyberbezpieczeństwa wśród osób z Twojego otoczenia

Wprowadzenie

Bezpieczeństwo w cyberprzestrzeni jest sprawą każdego z nas. Zwiększając swoją świadomość w tym zakresie, chronisz nie tylko siebie, ale także innych. Osoby z Twojego otoczenia widzą, jak zachowujesz się w stosunku do otrzymanych e-maili, łączności z sieciami Wi-Fi – czyli ogólnie w cyberprzestrzeni. **Twój przykład** może wpłynąć skutecznie na zachowania osób z Twojego środowiska. Warto poruszać tematy związane z bezpieczeństwem w Internecie podczas codziennych rozmów. Dzięki temu dbamy o bezpieczeństwo naszych najbliższych, a w dalszej kolejności wywieramy wpływ na globalną świadomość dotyczącą cyberbezpieczeństwa.

Cyber Fakt

Jeśli ataki cyberbezpieczeństwa polegają na manipulowaniu ludzkim zachowaniem, to zachowanie to musi się zmienić. W raporcie badawczym The Aberdeen Group odkryto, że stosując szkolenia **uświadamiające** w zakresie bezpieczeństwa, można zmniejszyć ryzyko cybernetycznych zagrożeń wykorzystujących inżynierię społeczną nawet o 70%. Jednak Aberdeen podkreśla znaczenie ciągłego szkolenia, aby przeciwdziałać wciąż zmieniającym się metodom wykorzystywanym przez cyberprzestępców. Ważne jest, żeby, oprócz dedykowanych szkoleń, przekazywać dobre praktyki i uczyć czujności w cyberświecie osobom z Twojego otoczenia. Badania wskazują również, że **zwiększenie świadomości w dziedzinie cyberbezpieczeństwa** daje ludziom większą pewność przy korzystaniu z technologii. Obec-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

nie zdarzają się sytuacje, w których boimy się otworzyć wiadomość e-mail na wypadek, gdyby zainfekowała naszą firmę oprogramowaniem ransomware. Jeśli będziemy posiadali wiedzę, jak wykryć oznaki fałszywej wiadomości, będziemy również odważniejsi w cyber-rzeczywistości – a więc często w miejscu naszej pracy i życia społecznego.

Dobre praktyki

- Rozmawiaj z najbliższymi oraz osobami z Twojego otoczenia o dobrych praktykach poruszania się w cyberprzestrzeni. Dzięki temu wzmocnisz znaczenie i rozwiniesz kulturę bezpieczeństwa.

- Jeżeli ktoś z Twojego otoczenia nie będzie umiał wykonywać w bezpieczny sposób operacji w sieci, poświęć mu czas i pokaż, jak powinien wykonywać te działania.

- Warto dyskutować z najbliższymi, co zrobić w przypadku spotkania się z zagrożeniami lub groźnymi incydentami w cyberświecie. Podczas takiej rozmowy możesz pomóc im opracować sposób postępowania w razie ataku.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 8 - Uważaj na szkodliwe wyskakujące okienka

Wprowadzenie

Podczas przeglądania Internetu, często spotykamy się z natrętnymi okienkami, które informują nas o aktualizacjach oprogramowania lub zachęcają do ściągnięcia przeróżnych programów. Klikanie w takie reklamy często prowadzi do **instalacji niechcianego oprogramowania**. Ponadto okienka te nierzadko zaprojektowane są w taki sposób, że instalacja może odbywać się na komputerze pomimo odrzucenia przez nas niechcianego komunikatu.

Cyber Fakt

Bardzo popularne jest wykorzystywanie przez hakerów wyskakującego okienka z informacją o wygranym konkursie lub unikatowej szansie na zakup produktu. Często zdarza się, że niezależnie od miejsca, w które klikniesz, reklama/okno wciąż próbuje przekierować Cię na inną stronę. Wchodząc na nią, automatycznie stajesz się ofiarą cyberataku. Strony takie mają na celu wprowadzenie złośliwego kodu do Twojej przeglądarki lub systemu. Znany atak tego typu miał miejsce w 2019 roku. Hakerzy informowali wówczas na wyskakującym okienku, że wygrałeś iPhona, ponieważ wziąłeś udział w ankiecie. Klikając w link, zostawałeś przekierowany na stronę, gdzie należało podać numer karty płatniczej wraz z kodem bezpieczeństwa CVV (znajdującym z tyłu karty). Po wprowadzeniu powyższych danych, hakerzy „czyścili" konto bankowe z pieniędzy, a telefon oczywiście nigdy nie docierał do oszukanych osób.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

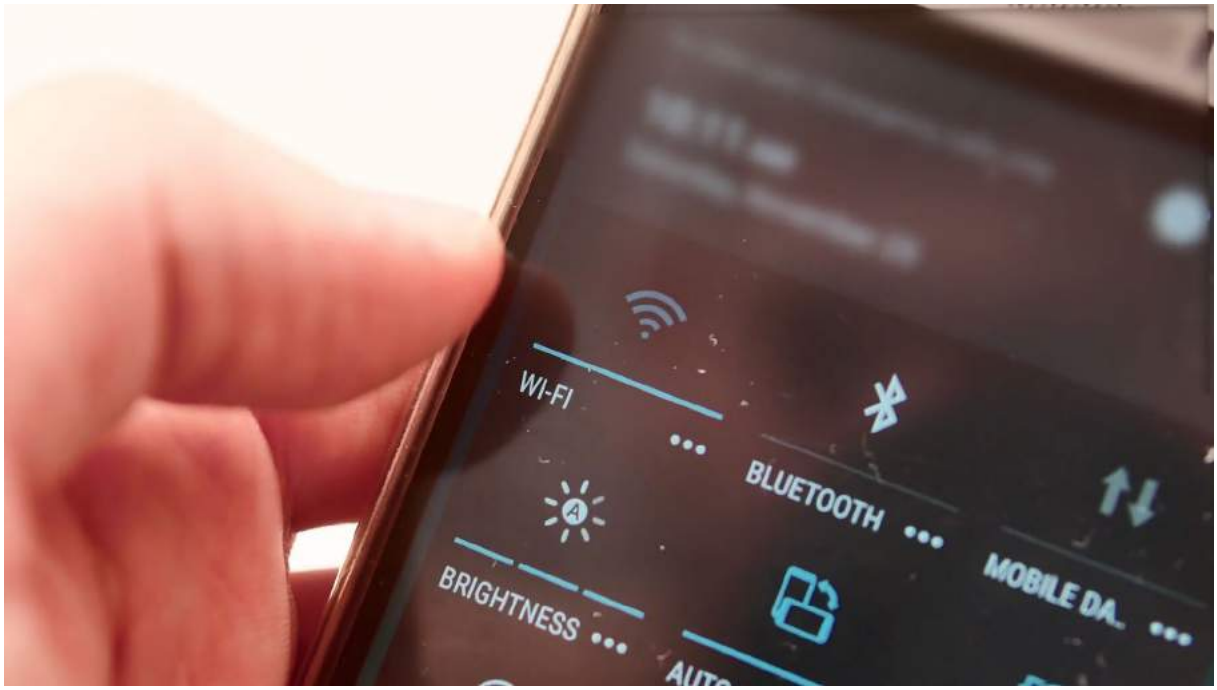
- Korzystaj z oprogramowania blokującego wyskakujące okienka.
- Unikaj klikania w podejrzane reklamy z zachęcającymi ofertami. Mogą one kierować na strony ze złośliwym oprogramowaniem, a w konsekwencji doprowadzić do przejęcia kontroli nad Twoim komputerem.
- Jeżeli omyłkowo kliknąłeś na taką reklamę, zalecane jest wyłączenie przeglądarki oraz zresetowanie systemu. Istotne jest także uruchomienie skanowania w programie antywirusowym w celu upewnienia się, że na Twoim urządzeniu nie zostały już zainstalowane złośliwe programy.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 7 - Unikaj korzystania z otwartych sieci WiFi

Wprowadzenie

Podczas codziennych czynności - podróżowania lub po prostu wizyt w miejscach publicznych - możemy natrafić na darmowe i otwarte sieci Wi-Fi. Bardzo ważne jest, aby uważać na swoją aktywność podczas korzystania z nich. Tego typu punkty dostępu są narażone na podsłuchiwanie i przekierowywanie ruchu sieciowego. Hakerzy stosujący te techniki są w stanie wychwycić Twoje konwersacje, zdjęcia, a także inne wrażliwe dane. W szczególnych przypadkach mogą nawet przejąć kontrolę nad Twoim urządzeniem bez Twojej wiedzy. Dlatego podczas korzystania z otwartych sieci, unikaj wykonywania ważnych czynności, takich jak logowanie się do witryny banku czy wymiany poufnych informacji.

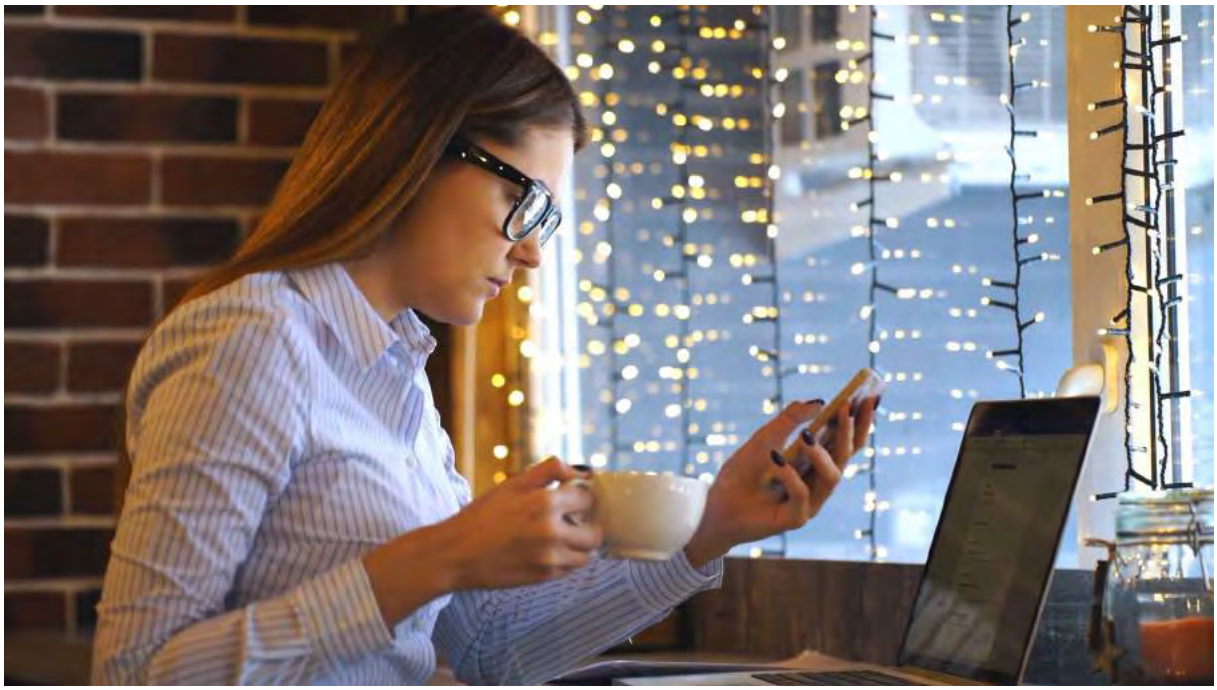


Cyber Fakt

Korzystając z otwartej sieci Wi-Fi, należy mieć świadomość, że absolutnie każdy może się do niej podłączyć. W tego typu połączeniu łatwo jest podejrzeć nieszyfrowany ruch sieciowy wszystkich urządzeń. Ponadto hakerzy potrafią przekonać Twój komputer, że to ich urządzenie jest Twoją bramą domyślną (routerem). Powoduje to przekazanie całego Twojego ruchu sieciowego do hakera, który decyduje o tym, jakie informacje zwrotne dostaniesz oraz co zostanie faktycznie wysłane do sieci. **Taki atak nazywamy MITM (Man In The Middle)**. W praktyce wygląda on tak: haker uruchamia bezprzewodowy punkt dostępowy, który wydaje się być legalny i dzięki niemu może swobodnie przechwytywać Twoje dane. Przykładowo: będąc w ulubionej kawiarni, widzisz na swoim smartfonie sieć Wi-Fi o znanej Ci nazwie. Telefon łączy się z nią automatycznie, ponieważ byłeś już w tym miejcu kilka razy. Ten atak jest bardzo niebezpieczny, ponieważ nie wymaga indywidualnego łączenia się z bezpłatną siecią -smartfon robi to automatycznie i bez naszego udziału. Jeden z bar-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

dziej znanych incydentów tego typu miał miejsce podczas Narodowej Konwencji Republikanów w 2016 r. Wówczas 1200 uczestników połączyło się z fałszywą siecią Wi-Fi „I VOTE TRUMP", która znajdowała się poza centrum kongresowym.



Dobre praktyki

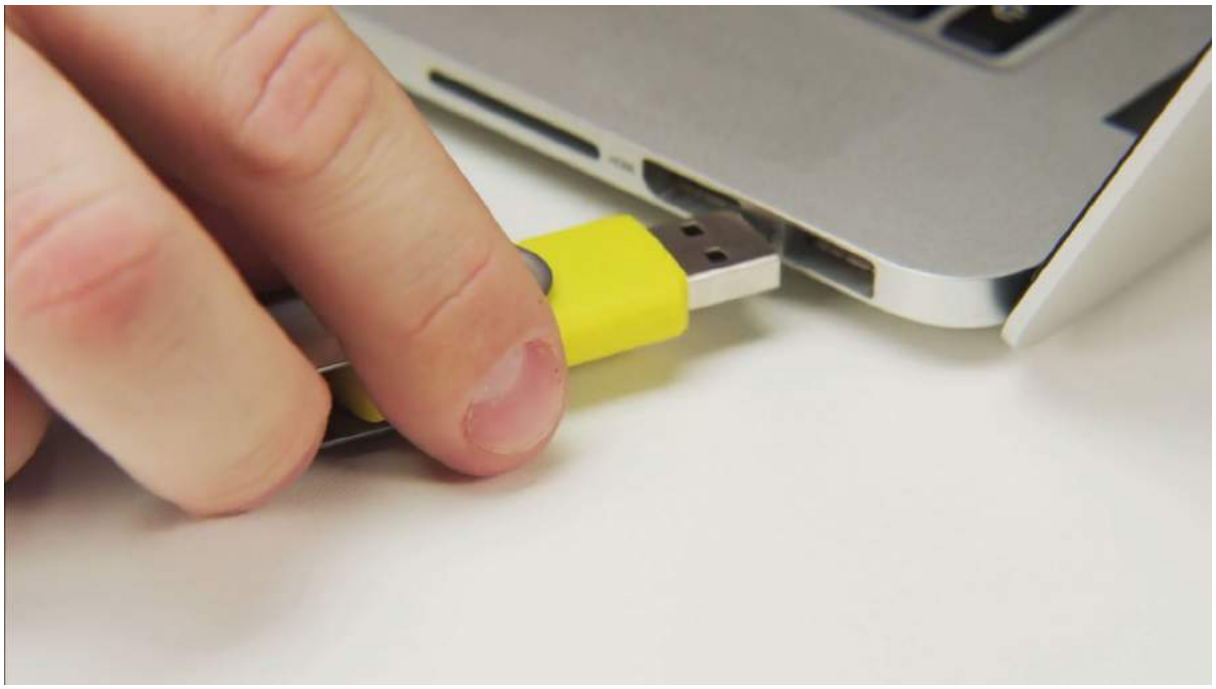
- Wybieraj zaufane i bezpieczne punkty dostępowe do sieci.
- Jeżeli nie masz dostępu do zaufanego Wi-Fi, korzystaj z transferu danych oferowanego przez Twojego operatora. Jeżeli potrzebujesz Internetu na laptopie, możesz udostępnić go przez swój telefon, tworząc na nim punkt dostępu.
- Sprawdzaj, czy strony, na które wchodzisz w otwartych sieciach, są zabezpieczone szyfrowanym protokołem HTTPS.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 6 - Nie podłączaj niezaufanych urządzeń pamięci masowej i innego sprzętu do swojego komputera, urządzenia mobilnego lub sieci

Wprowadzenie

Należy ograniczać udostępnianie dysków USB oraz zewnętrznych dysków twardych pomiędzy komputerami lub innymi urządzeniami. Trzeba także uważać, komu pożycza się dyski i w jakim celu. Główna zasada jest taka, że nie wolno podłączać żadnego nieznanego lub niezaufanego sprzętu do swojego komputera czy sieci. Dotyczy to także dysków CD, DVD oraz urządzeń USB. Przestępcy, umieszczając dyski USB w miejscach publicznych, zakładają, że zaciekawieni użytkownicy będą je odbierać i podłączać. Znajduje się na nich zazwyczaj złośliwe oprogramowanie, które może szpiegować komputer lub przejmować nad nim kontrolę.



Cyber Fakt

Bardzo sławny atak związany z zainfekowanymi urządzeniami USB miał miejsce w 2010 roku. Wykorzystane zostało wtedy oprogramowanie Stuxnet worm. Nie wiadomo jednak przez ile lat wcześniej wirus wyrządzał szkody. Atak ten jest nazywany pierwszą bronią cybernetyczną. Hakerzy uderzyli w irański zakład nuklearny. Wirus spowodował wiele szkód w systemie, a także wykradał dane z komputerów placówki oraz przejmował nad nimi pełną kontrolę. Przykładowo, wykorzystywał sprzęt do kontroli wirówek, którym następnie zmieniał ciśnienie i doprowadzał do awarii. Ponadto był pierwszym w tamtych czasach oprogramowaniem, które zaprojektowano w celu uszkodzenia sprzętu nuklearnego. Program spowodował problemy ze sprzętem w placówce i, pomimo licznych wymian oraz

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

analiz, inżynierowie wciąż nie potrafili znaleźć przyczyn awarii.

Pięć miesięcy później pojawiła się pierwsza przesłanka, że komputery zakładu zostały zainfekowane nieznanym i groźnym oprogramowaniem. Urządzenia stale restartowały się i odmawiały posłuszeństwa, wyświetlając różne błędy systemowe. Doprowadziło to do odnalezienia złośliwych plików na komputerach. Hakerzy nie byli w stanie zaatakować placówki bezpośrednio, ponieważ ta nie miała połączenia z siecią Internet. Zainfekowanie placówki nuklearnej odbyło się więc poprzez urządzenie USB zawierające złośliwe oprogramowanie.

Dobre praktyki

- Uważaj, komu pożyczasz pamięci zewnętrzne oraz od kogo je odbierasz. Przed przekazaniem lub użyciem sprzętu zastanów się, czy na pewno możesz zaufać danej osobie.
- Wyłącz funkcję AutoRun dla portów USB i napędów optycznych, takich jak CD i DVD, aby zapobiec instalowaniu złośliwych programów.
- Jeśli wiesz o zainfekowanym urządzeniu znajdującym się w Twoim domu, szkole, miejscu pracy - informuj o takich przypadkach ludzi w swoim otoczeniu.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 5 - Bezpieczne korzystanie z przeglądarki internetowej

Wprowadzenie

Podczas korzystania z Internetu, na pewno zdarza Ci się kupować coś w e-sklepach, robić przelewy lub wymieniać się wrażliwymi informacjami. Ważne jest, aby takie czynności wykonywać w ramach szyfrowanego połączenia. Zazwyczaj możemy się o tym przekonać sprawdzając, czy przeglądarka nawiązała połączenie HTTPS z serwisem WWW. Możemy to zauważyć poprzez oznaczenie małą kłódką widoczną w prawym dolnym lub w lewym górnym rogu okna przeglądarki internetowej, a także odnajdując słowo „https" na początku adresu serwisu. Oprócz szyfrowanego połączenia, w przypadku komputerów współdzielonych z innymi osobami, zalecane jest regularne usuwanie pamięci podręcznej w przeglądarkach - w tym czasowych plików cookie oraz historii przeglądanych stron.

Cyber Fakt

Korzystając z serwisu, na którym podaje się swoje dane logowania, można spotkać się z tzw. *zieloną kłódką*. Wówczas wiemy, że taka strona korzysta z protokołu https i przesyłane dane są zaszyfrowane. Możliwe jest jednak, że haker zmusi Twoją przeglądarkę do skorzystania z protokołu http (nie będzie już zielonej kłódki). W takim przypadku wpisane przez Ciebie hasło zostanie wysłane do sieci Internet w formie niezaszyfrowanej, którą będzie mógł swobodnie odczytać atakujący. Zawsze warto sprawdzać, z jakich protokołów korzysta nasza przeglądarka na danym serwisie. Nie należy nigdy podawać wrażliwych danych oraz haseł, jeśli przy adresie nie będzie *zielonej kłódki* i rozpocznie się on od czego innego niż „https".
Trzeba jednak pamiętać, że hakerzy mogą przekierować Cię na swój serwis z łudząco podobnym adresem WWW do adresu banku lub innej atakowanej strony. Wtedy również po-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

jawi się *zielona kłódka* – ale za to adres strony nie będzie identyczny jak ten strony podrabianej.

Dobre praktyki

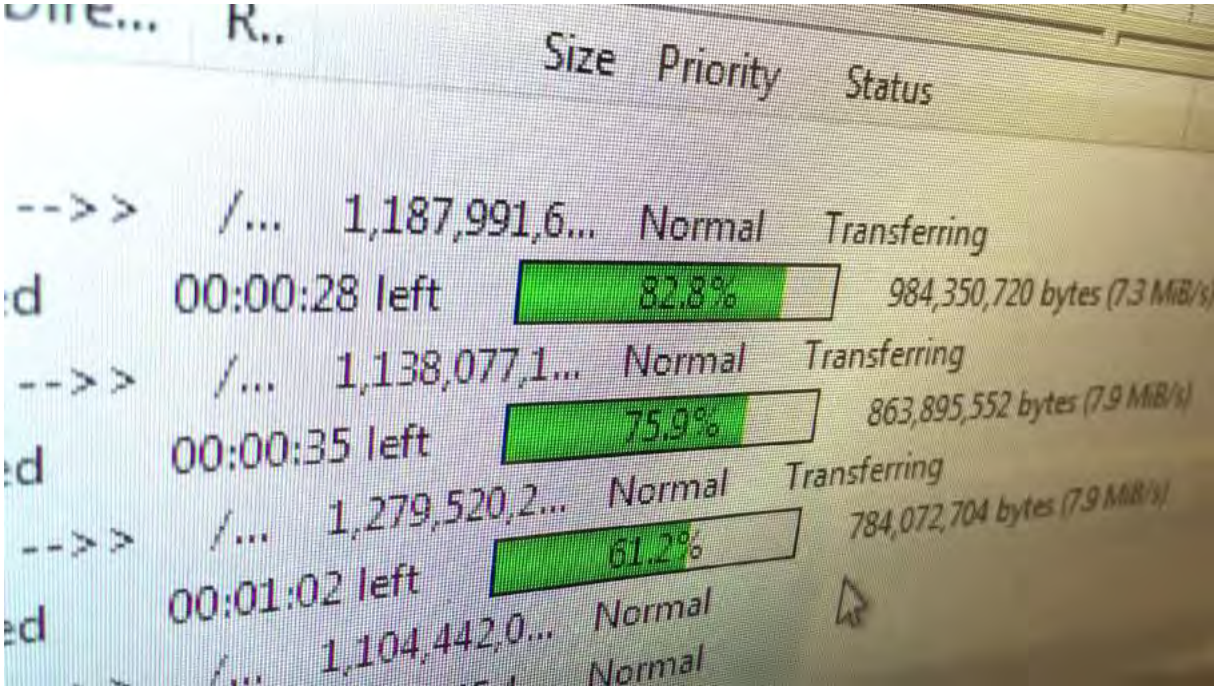
- Korzystaj z zabezpieczonych sieci, które znasz i którym możesz zaufać.
- Staraj się regularnie usuwać tymczasowe pliki, pliki podręczne, historię i pliki cookie Twojej przeglądarki.
- Korzystając z innych komputerów pamiętaj, aby wylogować się i usunąć wszelkie dane, które mogły pozostawić ślad po Twojej aktywności.
- Sprawdzaj dokładnie adres strony oraz czy połączenie jest szyfrowane (adres rozpoczyna się od https i jest *zielona kłódka*).

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 4 - Zachowaj ostrożność podczas pobierania oprogramowania

Wprowadzenie

Zwracaj uwagę, skąd i jakie oprogramowanie pobierasz - czy strona udostępniająca taki program jest zaufana, czy ma dobre opinie oraz czy jest stroną zaprojektowaną w sposób profesjonalny. Sprawdź również, czy jest zabezpieczona szyfrowanym połączeniem, a także czy certyfikat strony jest ważny oraz poprawny (jest *zielona kłódka*). Zachowaj szczególną ostrożność podczas pobierania bezpłatnego oprogramowania (ang. *freeware*). Niektóre z darmowych programów nie posiadają pełnej funkcjonalności, której potrzebujesz, oraz nie oferują przydatnego wsparcia technicznego. Podczas instalacji takiego oprogramowania, zdarza się, że aplikacja sama doinstaluje dodatkowe elementy, które mogą zawierać wirusy.



Cyber Fakt

Bardzo głośnymi atakami były przejęcia kont na Twitterze znanych osobistości, takich jak Elon Musk czy Bill Gates w roku 2020. Wszystkie przejęcia były wynikiem oszustwa przygotowanego przez 17-latka z Florydy. Chłopak spreparował wiadomości i przekierował je do pracowników Twittera, którzy pobrali oprogramowanie pozwalające hakerowi na dostanie się do danych logowania całej bazy użytkowników Twittera. Następnie wykorzystał zgromadzone dane , aby zalogować się na konta ofiar i nakłonił ich obserwujących do przelewania pieniędzy na portfel Bitcoin. Mężczyzna posiada aktualnie ponad 30 zarzutów nielegalnego dostępu do informacji.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

- Czytaj uważnie, co zamierzasz zainstalować i czy zgadzasz się na instalację różnych dodatków niekoniecznie potrzebnych do uruchomienia programu.
- Sprawdzaj opinię strony, z której pobierasz oprogramowanie, a także samego oprogramowania.
- Jeżeli jest taka możliwość, sprawdzaj poprawność pobranych danych i zobacz, czy program nie został podczas pobierania podmieniony przez hakera. Możesz to sprawdzić analizując sumę kontrolną pobieranego pliku i porównać ją z sumą podaną na stronie ściąganego oprogramowania.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 3 - Używaj silnych haseł

Wprowadzenie

Większość serwisów w Internecie wykorzystuje mechanizm logowania, dzięki któremu może określić, jaki użytkownik korzysta z portalu. W celu dostępu do danych należy podać nasz identyfikator i hasło. Bardzo ważne jest korzystanie z silnych i długich haseł, które będą trudne do złamania. Powinny one składać się z losowej sekwencji liter (wielkich i małych), cyfr i znaków specjalnych. Ich długość to co najmniej 12 znaków. Innym sposobem wymyślania haseł, które łatwiej zapamiętać, jest tworzenie ich w formie ciągu wielu wyrazów. Ten sposób jest wykorzystywany między innymi do ochrony portfeli kryptowalut. W celu odzyskania dostępu np. do portfela Bitcoin, należy podać 12 tajnych słów.

W przypadku systemów lub aplikacji, które zawierają ważne informacje, używaj wielu form identyfikacji (tzw. uwierzytelnianie wieloskładnikowe), takich jak kod jednorazowy czy ten wysłany SMSem. Unikaj korzystania z domyślnych haseł w konfiguracjach urządzeń, np. w routerach. W Internecie jest mnóstwo informacji na temat tego typu haseł i każdy użytkownik sieci jest w stanie znaleźć domyślne hasła dla danego urządzenia.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Cyber Fakt

Poprzez podanie swojej nazwy użytkownika oraz hasła uzyskujemy dostęp do wielu usług w sieci. Jest to najprostsza i najbardziej popularna metoda na świecie, dlatego tak istotne jest, aby zadbać o trudne do odgadnięcia hasło. Według Narodowego Centrum Bezpieczeństwa Cybernetycznego (NCSC) rządu Wielkiej Brytanii imiona, piłkarze, muzycy i postacie fikcyjne to jedne z najgorszych haseł. Jednak to hasło „123456" zasługuje na miano najsłabszego ze wszystkich. NCSC stwierdziło, że ponad 30 milionów ofiar korzysta z hasła „123456" lub jego dłuższej wersji „123456789". Jest to zgodne z najnowszą analizą włamań opartą na danych pobranych z serwisu Pwned Passwords (https://haveibeenpwned.com) - strony internetowej prowadzonej przez badacza bezpieczeństwa Troya Hunta.

Dobre praktyki

- Używaj silnych haseł składających się z losowych, małych i dużych liter, cyfr, znaków specjalnych i mających długość co najmniej 12 znaków. Możesz też korzystać z haseł składających się z wielu wyrazów.

- Jeżeli masz problem z zapamiętaniem swoich haseł, skorzystaj z oprogramowania, które je szyfruje i przechowuje (tzw. menadżery haseł). Pozwoli Ci to na zgromadzenie ich wszystkich w bezpiecznym miejscu. Ważne jest, aby utworzyć kopię zapasową oraz zapisać hasło do takiego programu w miejscu, do którego będziesz miał dostęp w razie uszkodzenia pamięci.

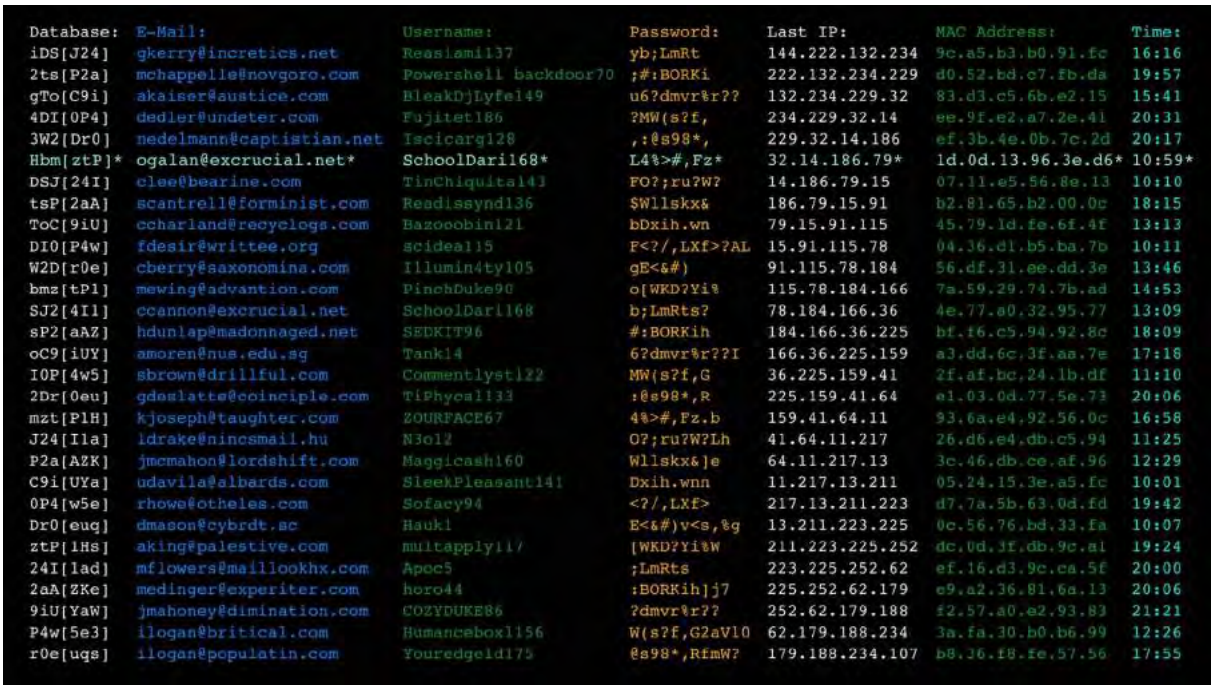
- Korzystaj z wieloskładnikowej weryfikacji np. kodu jednorazowego lub sprzętowych kluczy bezpieczeństwa (np. Yubikey).

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 2 - Nie podawaj osobom niezaufanym informacji osobistych oraz wrażliwych

Wprowadzenie

Hakerzy bardzo często wyłudzają informacje osobiste i wrażliwe od użytkowników, którzy są przekonani, że rozmawiają z osobą upoważnioną do uzyskania takich danych. Ta technika stanowi część inżynierii społecznej. Jest to próba uzyskania fizycznego lub elektronicznego dostępu do informacji poprzez podszywanie się pod inną osobę. Haker zazwyczaj korzysta ze zwykłego połączenia telefonicznego lub wiadomości e-mail z wiarygodną, ale zmyśloną historią, mającą na celu przekonanie Cię do podania istotnych danych – hasła, numeru konta, zdjęć dokumentów itp.



Database:	E-Mail:	Username:	Password:	Last IP:	MAC Address:	Time:
iDS[J24]	gkerry@incretics.net	Reasiami137	yb;LmRt	144.222.132.234	9c.a5.b3.b0.91.fc	16:16
2ts[P2a]	mchappelle@novgoro.com	Powershell backdoor70	;#:BORKi	222.132.234.229	d0.52.bd.c7.fb.da	19:57
gTo[C9i]	akaiser@austice.com	BleakDjLyfe149	u6?dmvr%r??	132.234.229.32	83.d3.c5.6b.e2.15	15:41
4DI[OP4]	dedler@undeter.com	Fujitet186	?MW(s?f,	234.229.32.14	ee.9f.e2.a7.2e.41	20:31
3W2[Dr0]	nedelmann@captistian.net	Iscicarg128	,:@s98*,	229.32.14.186	ef.3b.4e.0b.7c.2d	20:17
Hbm[ztP]*	ogalan@excrucial.net*	SchoolDari168*	L4%>#,Fz*	32.14.186.79*	1d.0d.13.96.3e.d6*	10:59*
DSJ[24I]	clee@bearine.com	TinChiquita143	FO?;ru?W?	14.186.79.15	07.11.e5.56.8e.13	10:10
tsP[2aA]	scantrell@forminist.com	Readissynd136	$Wllskx&	186.79.15.91	b2.81.65.b2.00.0c	18:15
ToC[9iU]	ccharland@recyclogs.com	Bazooobin121	bDxih.wn	79.15.91.115	45.79.1d.fe.6f.4f	13:13
DI0[P4W]	fdesir@writtee.org	scidea115	F<?/,LXf>?AL	15.91.115.78	04.36.d1.b5.ba.7b	10:11
W2D[r0e]	cberry@saxonomina.com	Illumin4ty105	gE<&#)	91.115.78.184	56.df.31.ee.dd.3e	13:46
bmz[tP1]	mewing@advantion.com	PinchDuke90	o[WKD?Yi%	115.78.184.166	7a.59.29.74.7b.ad	14:53
SJ2[4I1]	ccannon@excrucial.net	SchoolDari168	b;LmRts?	78.184.166.36	4e.77.a0.32.95.77	13:09
sP2[aAZ]	hdunlap@madonnaged.net	SEDKIT96	#:BORKih	184.166.36.225	bf.f6.c5.94.92.8c	18:09
oC9[iUY]	amoren@nus.edu.sg	Tank14	6?dmvr%r??I	166.36.225.159	a3.dd.6c.3f.aa.7e	17:18
I0P[4W5]	sbrown@drillful.com	Commentlyst122	MW(s?f,G	36.225.159.41	2f.af.bc.24.1b.df	11:10
2Dr[0eu]	gdeslatte@coinciple.com	TiPhycal133	:@s98*,R	225.159.41.64	e1.03.0d.77.5e.73	20:06
mzt[PlH]	kjoseph@taughter.com	ZOURFACE67	4%>#,Fz.b	159.41.64.11	93.6a.e4.92.56.0c	16:58
J24[Ila]	ldrake@nincsmail.hu	N3o12	O?;ru?W?Lh	41.64.11.217	26.d6.e4.db.c5.94	11:25
P2a[AZK]	jmcmahon@lordshift.com	Maggicash160	Wllskx&]e	64.11.217.13	3c.46.db.ce.af.96	12:29
C9i[UYa]	udavila@albards.com	SleekPleasant141	Dxih.wnn	11.217.13.211	05.24.15.3e.a5.fc	10:01
0P4[w5e]	rhowe@otheles.com	Sofacy94	<?/,LXf>	217.13.211.223	d7.7a.5b.63.0d.fd	19:42
Dr0[euq]	dmason@cybrdt.sc	Hauk1	E<&#)v<s,%g	13.211.223.225	0c.56.76.bd.33.fa	10:07
ztP[1Hs]	aking@palestive.com	multapply117	[WKD?Yi%W	211.223.225.252	dc.0d.3f.db.9c.a1	19:24
24I[1ad]	mflowers@maillookhx.com	Apoc5	;LmRts	223.225.252.62	ef.16.d3.9c.ca.5f	20:00
2aA[ZKe]	medinger@experiter.com	horo44	:BORKih]j7	225.252.62.179	e9.a2.36.81.6a.13	20:06
9iU[YaW]	jmahoney@dimination.com	COZYDUKE86	?dmvr%r??	252.62.179.188	f2.57.a0.e2.93.83	21:21
P4w[5e3]	ilogan@britical.com	Humancebox1156	W(s?f,G2aVl0	62.179.188.234	3a.fa.30.b0.b6.99	12:26
r0e[uqs]	ilogan@populatin.com	Youredgeld175	@s98*,RfmW?	179.188.234.107	b8.36.f8.fe.57.56	17:55

Cyber Fakt

W 2017 roku ponad milion użytkowników dostało tego samego maila phishingowego. Wiadomość informowała o próbie udostępnienia dokumentu przez osobę znajdującą się w naszych kontaktach. Klikając na link, zostawaliśmy przekierowywani na fałszywą stronę Google Docs. Wielu użytkowników podało swoje loginy i hasła będąc przekonanymi, że logują się na oficjalnej stronie Google. Dało to hakerom dostęp do ponad miliona kont Google, a więc do poczty e-mail, kontaktów, dokumentów online i kopii zapasowych urządzeń mobilnych.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

- Rozmawiając przez telefon o ważnych sprawach z rzekomymi współpracownikami lub znajomymi, zawsze postaraj się zweryfikować, czy Twój rozmówca jest tym, za kogo się podaje. Możesz na przykład powiedzieć, że zaraz oddzwonisz albo zapytać o coś, o czym wie tylko ta osoba.

- Nigdy nie odpowiadaj na niezamówione rozmowy od nieznanych osób czy firm. Powiadom o tym ludzi w swoim otoczeniu, aby przestrzec ich przed takimi próbami manipulacji.

- Nie podawaj rozmówcom ważnych danych - takich jak Twoje hasło, login itd. Nie ma racjonalnego powodu, dla którego inne osoby mogłyby pytać o kody dostępu do twoich kont.

- Nie zdradzaj także informacji z jakiego oprogramowania korzystasz, a zwłaszcza z jakich wersji. Może to być pomocne dla hakerów, którzy po uzyskaniu takich informacji, postarają się znaleźć luki bezpieczeństwa w Twoim systemie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 1 - Uważaj na załączniki do wiadomości e-mail i łącza internetowe

Wprowadzenie

Podczas codziennego surfowania po sieci, masowo korzystamy z poczty elektronicznej. Jest to bardzo powszechna w dzisiejszych czasach metoda komunikacji, a przez to szczególnie narażona na hakerskie ataki. Atakujący bardzo często podszywają się pod inne osoby i firmy. Wysyłają wiadomości e-mail z załącznikami lub fałszywymi linkami, które doprowadzają do zainstalowania złośliwego oprogramowania na Twoim komputerze lub przekierowania na stronę podszywającą się pod legalny serwis. W rzeczywistości mają na celu wyłudzenie Twoich danych - takich jak loginy lub hasła. Wśród najbardziej popularnych zagrożeń dotyczących wiadomości e-mail, można wymienić wirusy komputerowe, ataki typu phishing oraz ataki ransomware.

Wirus - złośliwe oprogramowanie mające na celu przyznanie dostępu do Twojego komputera osobie, która go rozpowszechnia. Wystarczy kliknąć w odpowiedni link, a wirus „wstrzyknie" swój kod w Twój system. Dzięki temu zabiegowi, haker otrzymuje pełny dostęp do Twoich danych.

Phishing - jest to atak socjotechniczny, polegający na wysłanie ofierze linku, który przypomina znany serwis (np. sieci społecznościowe). W rzeczywistości jest to strona mająca na celu wyłudzenie Twojego loginu i hasła. Po podaniu swoich danych logowania, jesteśmy przekierowywani na oryginalną stronę serwisu. Jeżeli nie zauważymy nieprawidłowości w linku, na który weszliśmy, możemy łatwo sprowadzić na siebie dalsze ataki hakerskie korzystające z podobnych technik. Finalnie phishing doprowadza do utraty danych i dostępu do kont.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Ransomware - złośliwe oprogramowanie, które ma na celu szyfrowanie Twoich danych na komputerze. Blokuje ono dostęp do wielu plików.. Celem takiego ataku jest często wyłudzenie okupu w zamian za Twoje dane. Oprogramowanie informuje nas o zaszyfrowaniu naszych plików, następnie podaje metodę płatności i informacje potrzebne do wpłacenia pieniędzy w zamian za odszyfrowanie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Cyber Fakt

W 2016 roku w aplikacji Facebook rozpowszechniał się wirus oznaczający znajomych w komentarzach. Klikając na powiadomienie, byliśmy przekierowywani na stronę Google Docs. Następnie uruchamiany był plik javascript, mający na celu ściągnięcie programu na nasz komputer. Gdy złośliwe oprogramowanie zostało pobrane , rozpoczynało wysyłanie powiadomień do osób znajdujących się w gronie znajomych. Oprócz wysyłania powiadomień (oczywiście z kopią samego siebie - czyli wirusa), szyfrowane były dane na dysku. W kolejnym kroku wysłane były żądania okupu za klucz, który pozwalał je odzyskać. Wirus ten był bardzo groźny i szybko się replikował. Na szczęście w porę udało się go zlikwidować.

Dobre praktyki

- Zawsze sprawdzaj, kto jest nadawcą wiadomości e-mail. Zadaj sobie pytanie, czy spodziewałeś się takiej wiadomości i czy jesteś w stanie skontaktować się z nadawcą w celu jej weryfikacji. Jeżeli nie jesteś w stanie tego sprawdzić, pod żadnym pozorem nie klikaj w załączniki i linki od nieznanych nadawców.

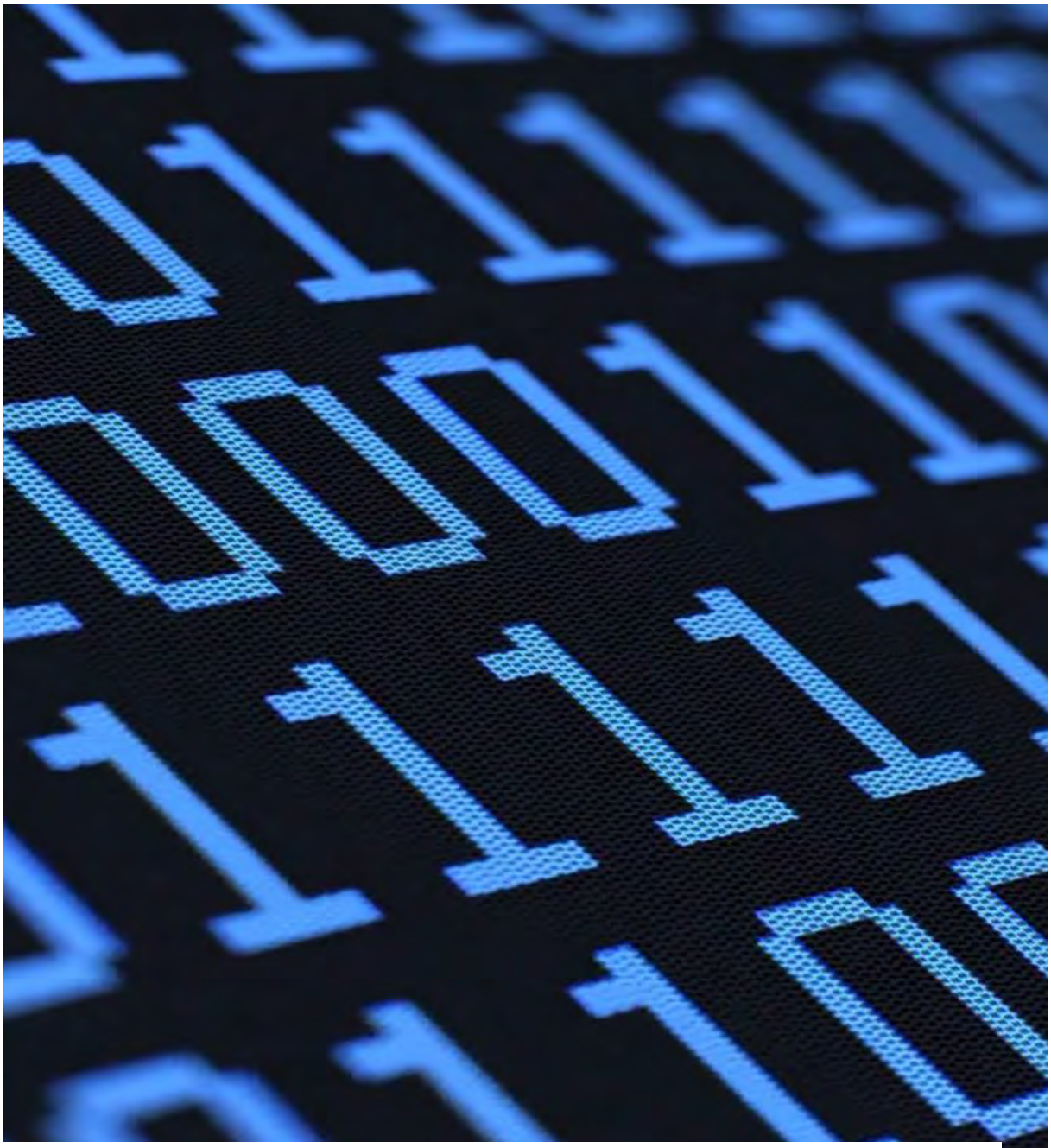
- Podczas przeglądania sieci, nie klikaj w podejrzane reklamy. Staraj się korzystać z zaufanych i zabezpieczonych stron. Pod żadnym pozorem nie wchodź na portale bez zabezpieczeń - zwłaszcza na te, które za zagrażające uważa sama przeglądarka.

- Unikaj instalacji nieznanych programów. Staraj się korzystać z komputera na koncie zwykłego użytkownika bez dodatkowych uprawnień. Korzystaj z konta administratora tylko podczas takiej potrzeby. Unikniesz wtedy wykorzystania uprawnień administratora przez programy trzecie i złośliwe oprogramowanie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

- Korzystaj z osobnych kont do różnych celów – załóż jedno do finansowych i wrażliwych operacji, a inne do prywatnych. Uniemożliwi to dostęp do wszystkich Twoich informacji przy zaatakowaniu jednego z kont.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.



Część II

Top 10 metod ochrony i detekcja ataków w cyberświecie

wybrane techniczne aspekty

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 10 - Zainstaluj ochronniki przeciwprzepięciowe i zasilacze awaryjne (UPS)

Wprowadzenie

Zastanówmy się, jak zachowują się nasze urządzenia pod wpływem skoków i spadków mocy bądź przy jej całkowitym odcięciu. Warto przyjrzeć się aspektowi zapisywania danych - czy nasz komputer zachowa postępy podczas takiego wypadku? Co zrobimy, jeśli w systemie pojawią się błędy wskutek odcięcia prądu? W celu uniknięcia powyższych sytuacji, przez które możemy utracić cenne osobiste informacje, należy zastosować ochronniki przeciwprzepięciowe oraz zasilacze bezprzerwowe (UPS). Umożliwią one naszym komputerom i serwerom pracę w przypadku krótkich przerw w dostawie prądu. Zapewnią również wystarczająco dużo czasu i mocy, aby urządzenia mogły zapisać zmiany.

Cyber Fakt

Od 15:30 23 grudnia 2015 r. w centrach sterowania energetycznego HMI na Ukrainie rozpoczęto otwieranie i zamykanie wyłączników zasilania bez udziału operatorów. Wynikające z tego nieautoryzowane operacje spowodowały utratę zasilania u ok. 225 000 klientów. Operatorzy w trzech centrach nie byli w stanie odzyskać kontroli nad 50 podstacjami. Po 6 godzinach i utracie 130 MW obciążenia, operatorzy przywrócili moc, wysyłając techników do podstacji i ręcznie sterując systemem elektroenergetycznym. Analiza sytuacji wykazała, że oprogramowanie zasilania awaryjnego (UPS) zostało zdalnie wyłączone - zarówno w serwerowni, jak i w systemach telefonicznych. Dodatkowo uszkodzeniu uległy dyski twarde wielu komputerów. To wydarzenie było pierwszą udaną przerwą w zasilaniu wywołaną przez hakerów.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

- Upewnij się, że każdy z komputerów i krytycznych urządzeń sieciowych jest podłączony do zasilacza UPS.
- Podłącz mniej wrażliwą elektronikę do zabezpieczeń przeciwprzepięciowych. Upewnij się, że działają poprawnie oraz że są podłączone według zaleceń producenta.
- Jeżeli używasz systemów do zdalnego zarządzania zasilaniem, zadbaj o bezpieczną komunikację między Twoim komputerem a systemem sterowania.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 9 - Bezpiecznie usuwaj stare komputery i nośniki

Wprowadzenie

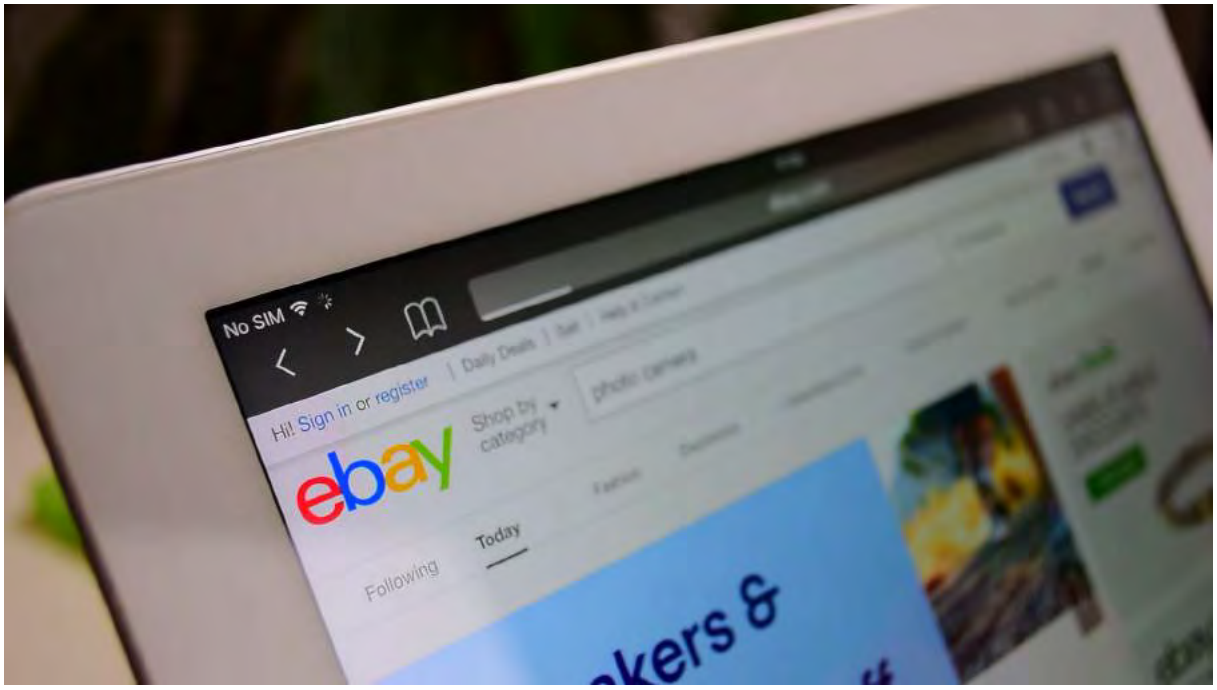
Sprzęt komputerowy jest nośnikiem, który zużywa się w miarę upływu czasu. Dość często zdarza się nam wymieniać i wyrzucać przestarzały sprzęt. Warto zauważyć, że na dyskach, których się pozbywamy, bardzo często nadal znajdują się dane. Zwykłe ich usunięcie nie będzie wystarczające, ponieważ mogą one być odzyskane przez specjalistyczne programy. Pozbywając się starego sprzętu, a zwłaszcza dysków twardych, należy skorzystać ze specjalnego oprogramowania usuwającego poufne informacje. Można również własnoręcznie rozmagnesować albo fizycznie zniszczyć dysk.

Cyber Fakt

Wyrzucenie dysku twardego z naszym systemem operacyjnym bez poprzedniego wyczyszczenia jego danych, może skutkować odczytaniem go na innym komputerze. Hakerzy, wchodząc w posiadanie naszego dysku, mogą łatwo odzyskać i wykorzystać wrażliwe, osobiste informacje. Według badań przeprowadzone przez Ontrack na potrzeby raportu Blancco Technology Group, ok. 42% używanych dysków twardych sprzedawanych w serwisie eBay zawiera wrażliwe dane. Ponadto każdy sprzedawca stwierdzał, że zastosowano odpowiednie metody sanityzacji danych tak, by nie dało się ich odczytać. Istnieje poważna obawa, że, chociaż sprzedawcy wyraźnie zdają sobie sprawę ze znaczenia usuwania danych, w rzeczywistości używają metod, które są niewystarczające. Przykładowo, wśród odzyskanych informacji znalazł się dysk od twórcy oprogramowania „z wysokim poziomem poświadczenia bezpieczeństwa przez rząd", zawierający: zeskanowane obrazy paszportów rodzinnych, aktów urodzenia, życiorysów i dokumentów finansowych; dokumenty studenckie i powiązane adresy e-mail; i 5 GB zarchiwizowanej wewnętrznej poczty e-mail

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

od dużego biura podróży. To naprawdę istotne, aby przed sprzedażą używanych nośników zastosować skuteczne środki niszczące zapisane na nich dane.



Dobre praktyki

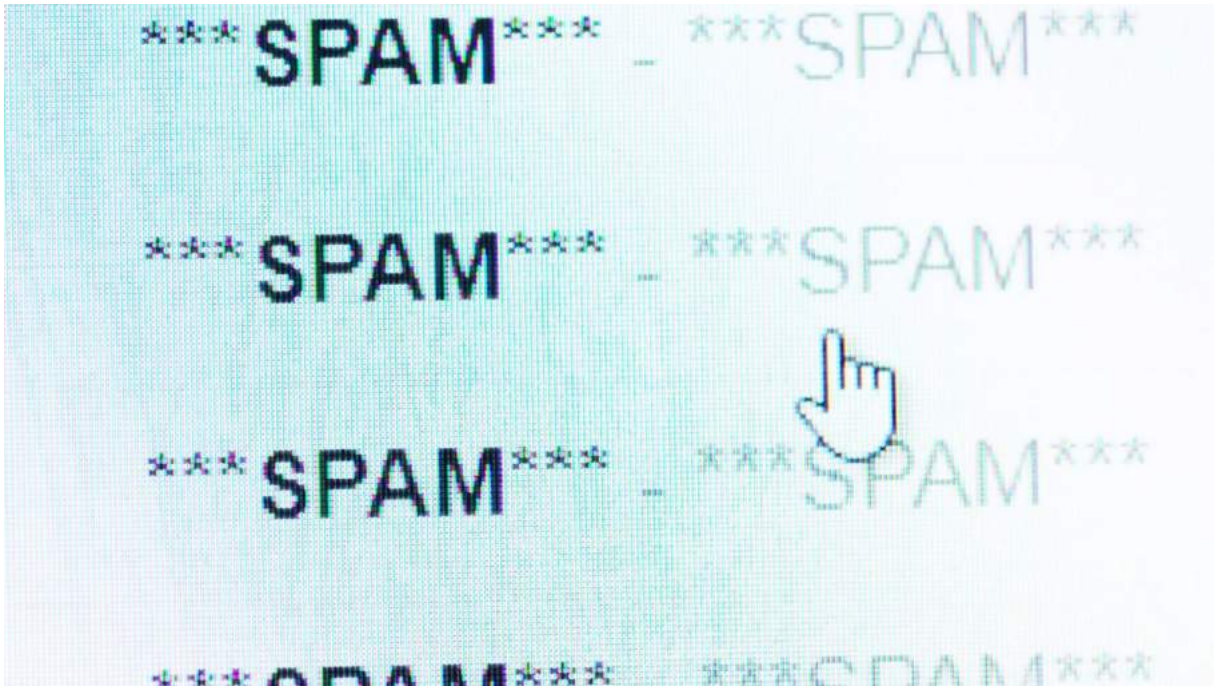
- Usuwając dane z dysków twardych, korzystaj ze specjalnego oprogramowania przeznaczonego do wypełniania i czyszczenia dysków.
- Wyrzucając nośniki DVD, CD, dyskietki, napędy USB usuń z nich swoje dane za pomocą skutecznego programu.
- Jeżeli twoja sytuacja nie pozwala Ci na wyczyszczenie dysku twardego, możesz rozważyć jego rozmagnesowanie lub fizyczne zniszczenie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 8 - Skonfiguruj filtry internetowe i e-mailowe

Wprowadzenie

Przeglądając sieć, często można natrafić na natrętne wyskakujące okienka. Istnieje możliwość edycji filtrów w programach, które blokują tego typu reklamy. Filtry nie mają jednak zastosowania tylko w blokowaniu reklam - możemy zastosować je również na naszej poczcie e-mail. Można z powodzeniem korzystać z nich w celu zredukowania wiadomości spam wysyłanych na skrzynkę. Większość serwisów e-mail oferuje możliwość edycji takich filtrów (np. w serwisie Gmail).



Cyber Fakt

Otrzymywanie wiadomości spam może prowadzić do wielu prób oszustw. Na przykład wyobraźmy sobie, że pewien mężczyzna uwierzył w wiadomości, które mówiły, iż jest jedynym spadkobiercą zmarłej rodziny. Przestępcy często wykorzystują specjalne haczyki, aby uzyskać wrażliwe dane. Przykładowo, ofiara ataku może podjąć spadek wyłącznie w banku, a w tym celu należy dopełnić kilku formalności i... wnieść kilka opłat. Wspomniane opłaty nie są małe, ale są zdecydowanie mniejsze od potencjalnej fortuny, którą może odziedziczyć mężczyzna. Przestępcy wysyłają informacje dotyczące przelewów, które mają uwiarygodnić fakt, że fortuna czeka na spadkobiercę. W jednym z prawdziwych przypadków oszustwa, opłaty konieczne do uzyskania spadku były równe aż 460 tys. zł. Oczywiście po wpłaceniu wspomnianej kwoty na wskazane konto, kontakt naciągaczy z ofiarą natychmiast się urwał.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

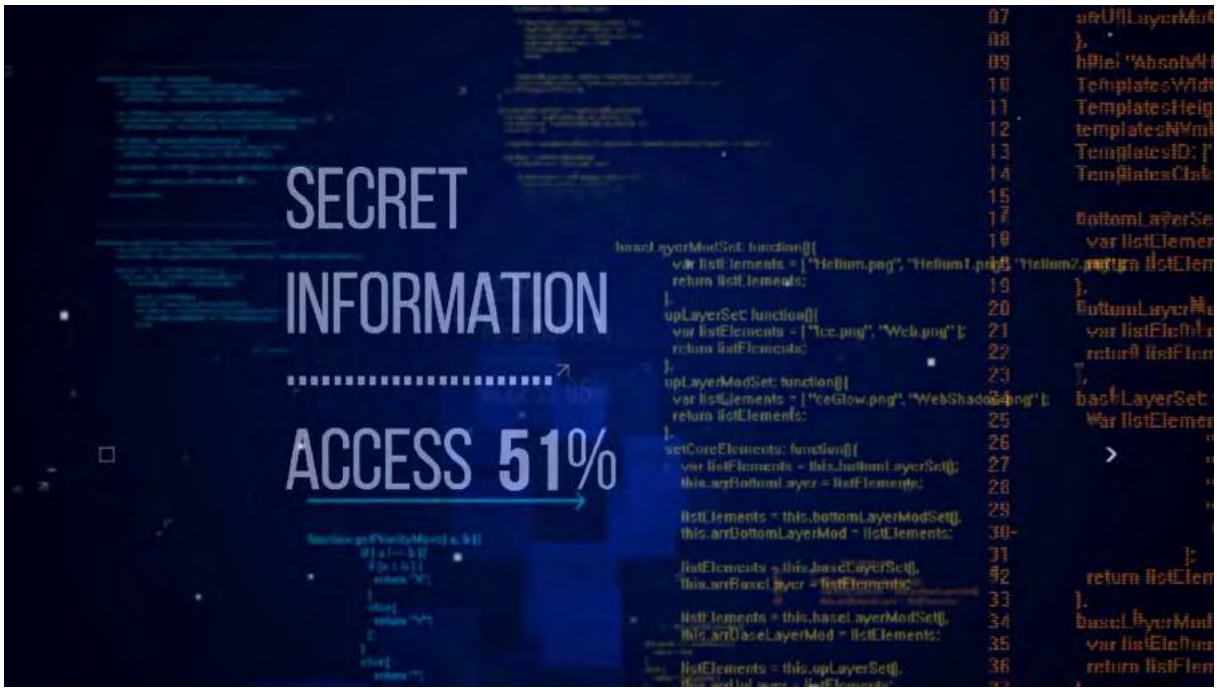
- Zainstaluj oprogramowanie blokujące reklamy oraz aktualizuj jego filtry.
- Skonfiguruj filtry poczty e-mail w celu zmniejszenia ilości wiadomości SPAM.
- Stale bądź uważny i podejrzliwy. Dzięki temu łatwiej będzie Ci określić, kiedy masz do czynienia z oszustwem.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 7 - Ogranicz dostęp do danych i informacji

Wprowadzenie

Administratorzy systemów są odpowiedzialni za ich konfigurację. To na ich barkach spoczywa obowiązek odpowiedniego zabezpieczenia komputerów lub serwerów pod względem dostępu do informacji. Mając swój osobisty komputer, przechowujemy na nim wrażliwe dane. Czasami zdarzają się sytuacje, w których pozwalamy innym osobom korzystać z naszego urządzenia. Należy uważać na to, do czego mają dostęp i z jakich informacji skorzystają. W tym celu ważne jest odpowiednie zabezpieczenie istotnych danych. Posiadając komputery firmowe, warto upewnić się, że pracownicy mają dostęp tylko do tych materiałów, do których są upoważnieni. Ponadto kiedy ktoś odchodzi z pracy, trzeba pamiętać o skutecznym odebraniu mu dostępu do firmowych zasobów.



Cyber Fakt

W 2016 roku Korea Północna uruchomiła serwis społecznościowy podobny do Facebooka. Został on zaatakowany przez 18-latka pochodzącego z Wielkiej Brytanii. Nastolatek zauważył, że na stronie widnieje link do panelu administracyjnego, do którego hasło i login były bardzo proste - brzmiały one „admin" i „password". Po wpisaniu owych danych, uzyskał pełen dostęp do serwisu: mógł dodawać i usuwać użytkowników, modyfikować treści postów, zarządzać reklamami. Posiadał również dostęp do prywatnych materiałów zarejestrowanych osób i mógł wykonywać wiele operacji, które są krytyczne z punktu widzenia działania portalu. Trudno tutaj mówić o zaawansowanym ataku hakerskim. W tym przypadku serwis nie został poprawnie skonfigurowany przez administratora i dostęp do wrażliwych danych uzyskała osoba do tego nieuprawniona.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Dobre praktyki

- Warto odpowiednio zabezpieczyć ważne dane na komputerze. Można w tym celu skorzystać z szyfrowania, ukrywania plików lub po prostu zabezpieczania ich hasłem.
- Zwracaj uwagę na to komu i w jakim celu udostępniasz swoje urządzenia. Ktoś może chcieć zainstalować oprogramowanie szpiegowskie i wykorzysta do tego Twoją chwilową nieuwagę.
- Będąc administratorem, upewnij się, że przeciętny użytkownik nie będzie w stanie uzyskać uprawnień, które pozwolą mu na wyrządzenie krzywdy w Twoich systemach.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 6 - Utrzymuj i monitoruj dzienniki

Wprowadzenie

Podczas korzystania z oprogramowania i sprzętu do ochrony lub wykrywania zagrożeń, istnieje możliwość prowadzenia dziennika aktywności. Taki dziennik przechowuje informacje na temat odnalezionych zagrożeń i czynności z nimi związanych. Służą one do identyfikowania podejrzanych działań i mogą być przydatne w przypadku prowadzenia dochodzenia. Jeżeli na Twoim komputerze dość często występują komunikaty o odnalezieniu nowego zagrożenia, powinieneś rozważyć przekazanie swoich dzienników specjaliście ds. bezpieczeństwa. Sprawdzi on dzienniki aktywności pod kątem wszelkich nietypowych lub niepożądanych trendów. Nie należy lekceważyć takich incydentów, ponieważ mogą one wskazywać na poważniejszy problem albo sygnalizować potrzebę silniejszej ochrony na określonym obszarze.

Cyber Fakt

Badania wskazują, że 85% właścicieli małych firm uważa, że ich biznes jest dobrze zabezpieczony przed hakerami, wirusami, złośliwym oprogramowaniem i wyciekiem danych. Takie przeświadczenie jest w dużej mierze spowodowane powszechnym przekonaniem, że niewielkie przedsiębiorstwa są mało prawdopodobnym celem cyberataków. W rzeczywistości cyberprzestępcy zazwyczaj szukają łatwego celu - miejsca, w którym nie będzie mechanizmów ochrony. Badanie firmy Symantec wykazało, że 40% ataków wymierzonych jest w organizacje zatrudniające mniej niż 500 pracowników.

Systemami, które pozwolą wykryć atak na podstawie analizy dzienników systemowych (ang. system logs), są systemy typu SIEM (ang. Security Information and Event Management). SIEM, zainstalowany w środowisku organizacji, pomoże w wykrywaniu poten-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

cjalnych zagrożeń cyberbezpieczeństwa. Gdy wykryje on potencjalny obszar zagrożenia, sztuczna inteligencja wbudowana w SIEM wyśle alert do personelu IT lub specjalisty ds. bezpieczeństwa w celu dalszej analizy. Dzięki takiemu działaniu, mającemu miejsce przed faktycznym wystąpieniem ataku, można zmniejszyć jego wpływ i straty lub nawet całkowicie go zablokować.

Dobre praktyki

- Upewnij się, że Twój system i oprogramowanie ochronne korzysta z dzienników aktywności.
- W miarę możliwości archiwizuj dzienniki aktywności. Mogą one przydać się w przyszłości.
- Przechowuj zarchiwizowane dzienniki przez co najmniej rok. Niektóre rodzaje informacji mogą wymagać przechowywania przez co najmniej sześć lat.
- Zainstaluj system SIEM, który automatycznie analizuje zapisy kontrolne różnych urządzeń oraz sieci wchodzących w skład Twojej organizacji.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 5 - Zabezpiecz bezprzewodowy punkt dostępowy i sieci

Wprowadzenie

Podczas instalacji sieci bezprzewodowej, jedną z podstawowych czynności, którą musimy wykonać, jest konfiguracja punktu dostępowego (routera WiFi). Aby go poprawnie skonfigurować, upewnij się, że zapoznałeś się z instrukcją obsługi. Dodatkowo zalecana jest zmiana hasła administracyjnego na urządzeniu oraz wyłączenie rozgłosu identyfikatora zestawu usług (SSID). W kolejnym kroku zmień nazwę użytkownika z uprawnieniami administratora oraz zablokuj dostęp z zewnętrznej sieci do strony konfiguracyjnej Twojego urządzenia.

Cyber Fakt

W 2009 roku John Matherly opracował wyszukiwarkę Shodan. W przeciwieństwie do innych popularnych wyszukiwarek, znajduje ona konkretne informacje, które mogą być bezcenne dla hakerów. Shodan pobiera banery usług z serwerów i urządzeń w Internecie - głównie z portu 80, ale także z portów 21 (ftp), 22 (SSH), 23 (telnet), 161 (SNMP) i 5060 (SIP). Ponieważ prawie każde nowe urządzenie ma teraz interfejs sieciowy (nawet lodówka), aby ułatwić zdalne zarządzanie, możemy uzyskać dostęp do niezliczonych serwerów internetowych, domowych systemów bezpieczeństwa itp.

Wśród urządzeń, które możemy znaleźć na Shodan, są niezabezpieczone kamery internetowe. Wyszukiwarka ta kataloguje tysiące, jeśli nie miliony routerów, z których wiele nie jest chronionych. Jednymi z najbardziej intrygujących rzeczy, które możemy tam znaleźć, są sygnalizacja świetlna i kamery monitorujące ruch na oświetlonych skrzyżowaniach. Jednak najbardziej przerażającym i potencjalnie najszkodliwszym zastosowaniem Shodan jest znajdowanie urządzeń SCADA (kontrola nadzorcza i pozyskiwanie danych) z interfej-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

sami internetowymi. Urządzenia SCADA kontrolują np. sieć elektryczną, elektrownie wodne, oczyszczalnie ścieków, elektrownie atomowe itp.

Dobre praktyki

- Skonfiguruj router tak, aby korzystał z Wi-Fi Protected Acces 2 (WPA-2), z szyfrowaniem Adavanced Encryption Standard (AES).
- Ustaw trudne hasło na urządzeniach dostępowych (takich jak router Wi-Fi).
- Nie podawaj głośno swojego hasła do sieci bezprzewodowej. Staraj się uwierzytelniać urządzenia osobiście.
- Zalecane jest także wyłączenie usługi WPS, która pozwala na podłączenie się urządzenia po wciśnięciu przycisku na routerze.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 4 - Używaj szyfrowania dla poufnych informacji

Wprowadzenie

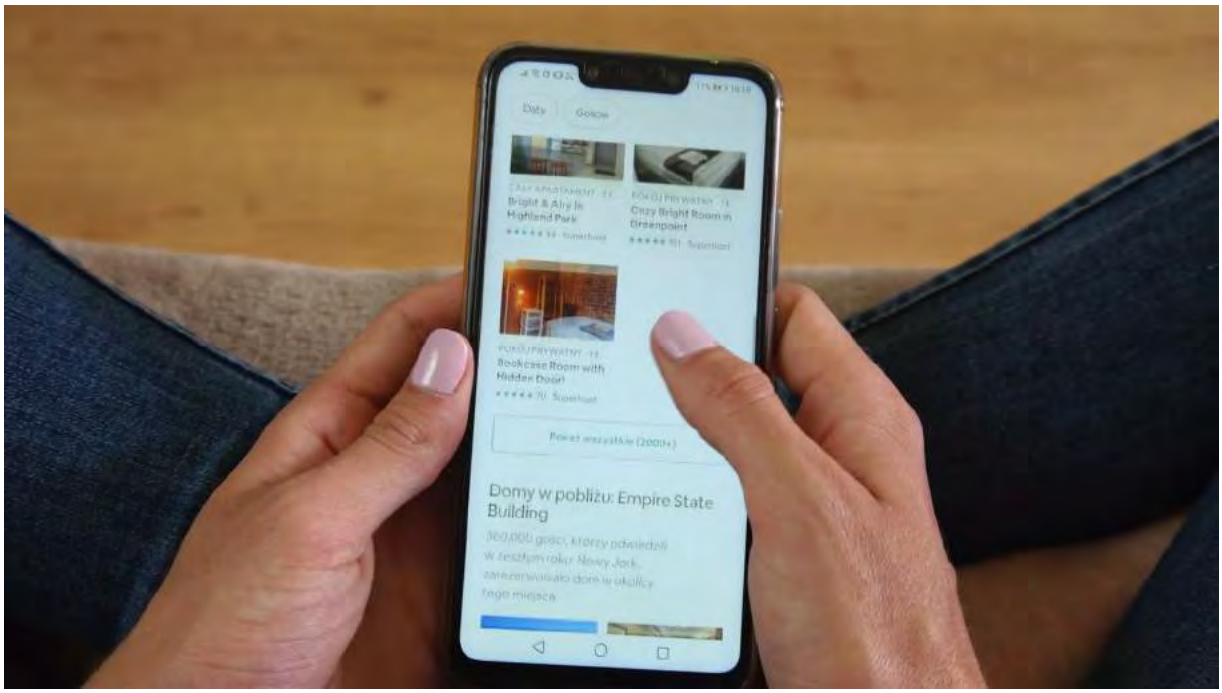
Szyfrowanie to proces powodujący, że przechowywane w formie elektronicznej informacje stają się nieczytelne dla osoby, która nie posiada prawidłowego hasła lub klucza. Korzystając z szyfrowania, możemy zabezpieczyć wszystkie dane znajdujące się na naszym nośniku. Wiele systemów wyposażonych jest w funkcje szyfrowania całego dysku. Niestety, nie jest to możliwe na wszystkich urządzeniach mobilnych. Tu warto wspomnieć o odpowiednim przechowywaniu klucza szyfrującego - jeżeli go zgubisz lub zapomnisz, utracisz możliwość odszyfrowania informacji.

Cyber Fakt

Większość z nas funkcjonuje z założeniem, że aplikacje na naszych telefonach są bezpieczne i że możemy ich używać do wykonywania zadań, do których zostały zaprojektowane, bez narażania nas na ryzyko. Jednak najnowsze badania (przeprowadzone przez firmę NowSecure zajmującą się bezpieczeństwem aplikacji mobilnych) sugerują, że tak nie jest. Firma ta przetestowała 250 najpopularniejszych aplikacji na Androida dostępnych w sklepie Google Play i stwierdziła, że aż 70% z nich ma luki, które narażają poufne dane użytkownika. Wyniki sugerują, że miliony użytkowników Androida mogą być zagrożeni. Badacze z NowSecure wykazali, że 45% wszystkich 250 najczęściej stosowanych aplikacji mobilnych używa słabego szyfrowania, pozostawiając dane klientów w postaci zwykłe go tekstu. Zdarza się również, że są one chronione przez łatwą do złamania formę szyfrowania, która naraża dane osobowe na ryzyko. Dodatkowo stwierdzono, że 20 testowanych aplikacji było podatnych na **ataki typu man-in-the-middle, przez które osoba atakująca może przechwycić dane.** Tego typu ataki mogą prowadzić do dalszych zagrożeń poprzez phishing – a to pro-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

sta droga do infiltracji systemów firmowych i kradzieży prywatnych danych.



Dobre praktyki

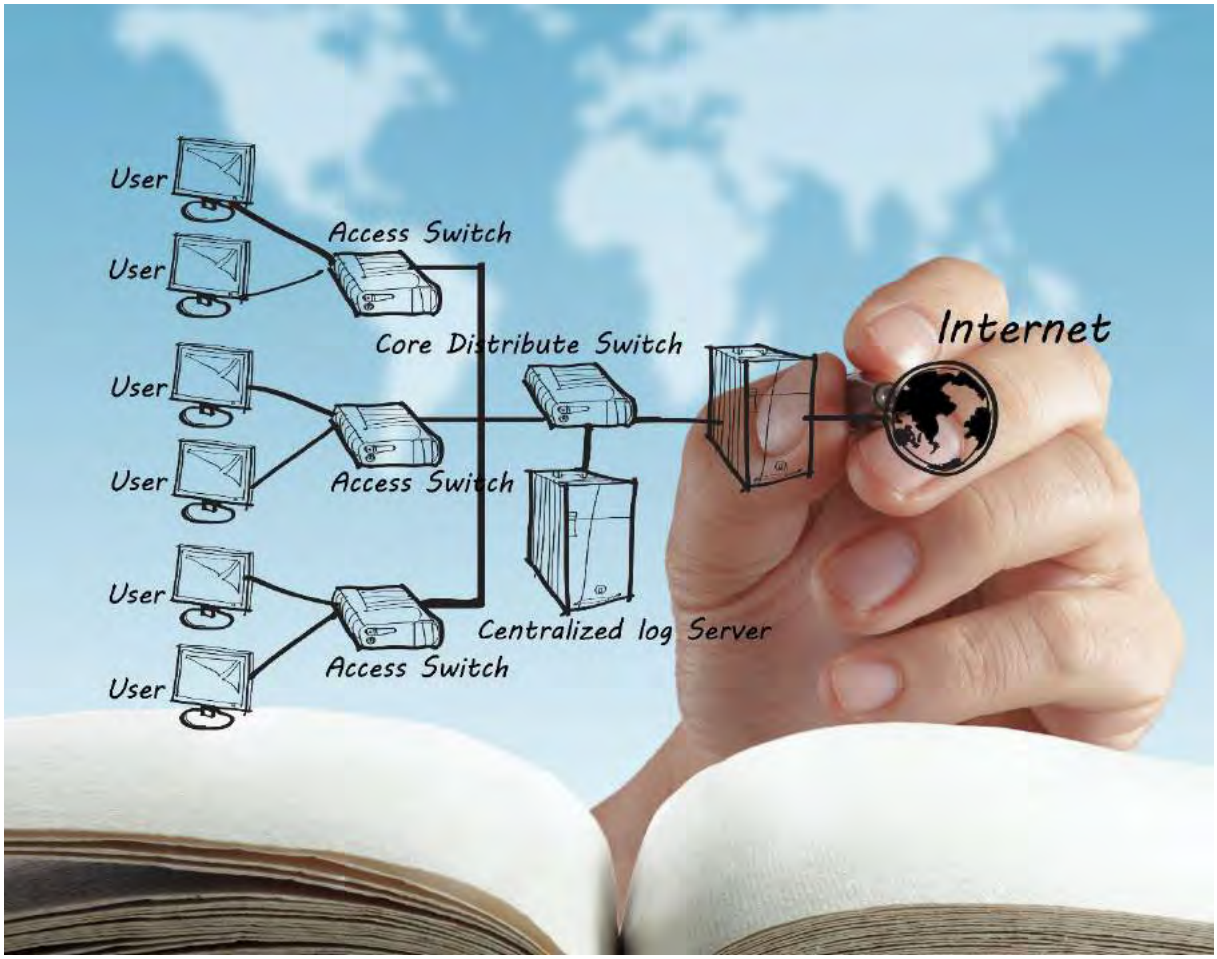
- Korzystaj z szyfrowania danych na swoim urządzeniu.
- Przechowuj klucz szyfrujący dla swojego urządzenia w bezpiecznym miejscu.
- Nie podawaj nikomu swojego klucza szyfrującego - jest on niczym hasło do Twojej skrzynki e-mail.
- Kiedy wysyłasz poufne informacje, możesz je zaszyfrować. Należy wtedy podać klucz Twojemu odbiorcy. Nie należy natomiast podawać go w tej samej wiadomości co zaszyfrowane dane. Postaraj się przekazać go telefonicznie lub inną drogą.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 3 - Zainstaluj i aktywuj zapory sieciowe oraz oprogramowanie wykrywające ataki

Wprowadzenie

Systemy operacyjne oraz urządzenia sieciowe korzystają z domyślnie wbudowanych zapór sieciowych. Nie są one bardzo zaawansowane, ale mogą uchronić przed pewnymi atakami. Dlatego warto upewnić się, że korzystamy z ich aktualnych wersji. Warto zadbać również o systemy wykrywania i przeciwdziałania atakom. Działają one w czasie rzeczywistym, czyli na bieżącą chronią nasz system przed atakami. Dodatkowo można także skorzystać z zapór pomiędzy Internetem a siecią wewnętrzną. Może to być funkcja bezprzewodowego punktu dostępowego/routera lub routera dostarczanego przez dostawcę usług internetowych (ISP). Istnieje wielu dostawców tego typu oprogramowania i sprzętu. Korzystając z takiego urządzenia, należy pamiętać o odpowiedniej konfiguracji - zmianie domyślnych haseł oraz zmiany nazwy użytkownika z uprawnieniami administratora. Należy pamiętać o zablokowaniu dostępu do strony konfiguracyjnej z zewnątrz.



© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Cyber Fakt

W roku 2016 tradycyjny sklep jubilerski z siedzibą w Delaware stracił dostęp do swoich zasobów online w efekcie wieloetapowego ataku DDoS. DDoS zatrzymuje działanie serwerów poprzez wysyłanie ogromnej liczby jednoczesnych żądań. Głównym winowajcą tego konkretnego ataku był botnet składający się z 25 000 skompromitowanych kamer przemysłowych (CCTV), posiadających łączność o dużej przepustowości i rozproszonych po całym świecie. Z atakami o takiej skali mogą poradzić sobie systemy wykrywania włamań połączone z zaporami sieciowymi, które oparte są na sygnaturach i wykrywaniu anomalii. Nowe zagrożenia wykrywane są przez **sieć honeypot** urządzeń wchodzących w skład Internetu Rzeczy (ang. Internet of Things). **Honeypot to fałszywa sieć, która jest przynętą dla hakerów. Na podstawie ich działań system uczy się nowych ataków).** Sieć ta działa na podstawie wykrywania anomalii, które są identyfikowane poprzez profilowanie zachowania poszczególnych urządzeń.

Dobre praktyki

- Korzystaj z zapór sieciowych, które chronią dostęp do Twojego systemu z Internetu.
- Sprawdzaj, czy programy chroniące Twój system są zaktualizowane oraz czy są włączane przy starcie systemu.
- Warto skorzystać z usług systemów wykrywania włamań, ostrzegających użytkownika przed atakiem i przejęciem kontroli nad systemem.
- Regularnie korzystaj z funkcji skanowania w programie ochronnym.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 2 - Instalacja i aktualizacja programów antywirusowych i programów antyszpiegowskich

Wprowadzenie

Malware to kod komputerowy napisany w celu kradzieży lub wyrządzenia szkody. Obejmuje wirusy, oprogramowanie szpiegujące i ransomware. Czasami złośliwe oprogramowanie zużywa tylko zasoby obliczeniowe (np. pamięć), a innym razem może rejestrować Twoje działania lub wysyłać cyberprzestępcom osobiste i wrażliwe informacje. Aby nie paść ofiarą podobnego ataku, należy korzystać z programów typu antywirus i antyspyware. Oferują one ochronę w czasie rzeczywistym, co oznacza, że na bieżąco sprawdzają czynności zachodzące w systemie, informują o niepożądanych, a następnie blokują je lub poddają kwarantannie.

Cyber Fakt

W 2019 roku użytkownicy WhatsApp zostali zaatakowani przez oprogramowanie szpiegujące, które potrafiło włączyć kamerę i mikrofon ich telefonu, a także zbierać dane o lokalizacji. Owe oprogramowanie o nazwie Pegasus zostało stworzone przez prywatną izraelską firmę NSO Group. Może ono wykorzystać lukę w zabezpieczeniach funkcji połączeń głosowych WhatsApp w celu przeprowadzenia ataku. Pegasus potrafi również przeszukiwać e-maile i wiadomości. Atakujący mogli więc wezwać użytkownika do zainstalowania oprogramowania monitorującego, nawet jeśli połączenie nie zostało odebrane. Raport mówi, że fałszywe połączenie czasami nawet nie pojawiało się w rejestrze połączeń. Oprogramowanie spyware prowadziło do przepełnienia bufora w stosie WhatsApp VOIP i umożliwiło zdalne wykonanie kodu poprzez specjalnie spreparowaną serię pakietów SRTCP wysy-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

łanych na docelowy numer telefonu. Firma Facebook, która jest właścicielem aplikacji WhatsApp, informowała użytkowników o ataku i prosiła ich o aktualizację aplikacji, którą opublikowała w krótkim czasie. Po zainstalowaniu poprawki, telefony i komputery nie są już podatne na opisywane oprogramowanie szpiegujące w aplikacji WhatsApp.

Dobre praktyki

- Instaluj i aktualizuj oprogramowanie typu antywirus i antyspyware.
- Ustaw automatyczną aktualizację w tych programach, aby mogły one samodzielnie uaktualniać bazy sygnatur wirusów.
- Skanuj swój system za pomocą tych narzędzi regularnie, przynajmniej raz w miesiącu.
- Rozważ użycie rozwiązań ochronnych od dwóch producentów. Może to zwiększyć szanse na wyłapanie wirusa lub niepożądanych procesów.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Top 1 - Instaluj aktualizacje bezpieczeństwa w swoich systemach operacyjnych i aplikacjach

Wprowadzenie

Wykupując oprogramowanie (np. system operacyjny), możemy liczyć na wsparcie techniczne firmy je tworzącej. Do takiego wsparcia zaliczamy również dbanie o jego bezpieczeństwo. Co jakiś czas wypuszczane są pakiety z aktualizacjami oprogramowania, które możemy pobrać za darmo i zainstalować na naszym urządzeniu. Dzięki temu zabezpieczamy się na wypadek nowo odkrytych wad i podatności naszego systemu. Dostawcy jednak nie są zobowiązani do dostarczania aktualizacji zabezpieczeń dla nieobsługiwanych produktów. Na przykład 8 kwietnia 2014 r. Microsoft zakończył wsparcie dla systemu Windows XP. Warto korzystać ze wspieranego oprogramowania, które dostaje aktualizacje bezpieczeństwa i funkcjonalności.

Cyber Fakt

Globalny atak ransomware, zwany *Petya* lub *NotPetya*, wykorzystywał lukę w zabezpieczeniach protokołu Microsoft Server Message Block 1.0 (SMBv1) w systemie operacyjnym Windows. Dzięki niej pozwalał uzyskać dostęp do zdalnego wykonania dostarczonego kodu na komputerze ofiary. W miarę jak Petya rozprzestrzeniał się po całej Europie, stało się jasne, że niewiele osób i firm - w tym dużych korporacji - faktycznie aktualizuje swoje oprogramowanie, nawet po poważnych cyberatakach. Ciekawostką jest to, że atak WannaCry, który miał miejsce znacznie później, wykorzystywał tę samą podatność co wcześniejszy atak Petya. WannaCry można było uniknąć lub przynajmniej uczynić go znacznie mniej uciążliwym, gdyby ludzie (i firmy) po prostu aktualizowali swoje oprogramowanie

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

komputerowe. Atak ten wykazał, że na setkach tysięcy komputerów w ponad 150 krajach działa przestarzałe oprogramowanie, które naraża je na ataki. Wśród ofiar była brytyjska służba zdrowia, gigant logistyczny FedEx, hiszpańska potęga telekomunikacyjna Telefonica, a nawet rosyjskie Ministerstwo Spraw Wewnętrznych. Luka w zabezpieczeniach, która pozwalała na wystąpienie obu ataków, została naprawiona przez Microsoft - ale tylko Ci, którzy aktualizują swoje komputery, byli chronieni.

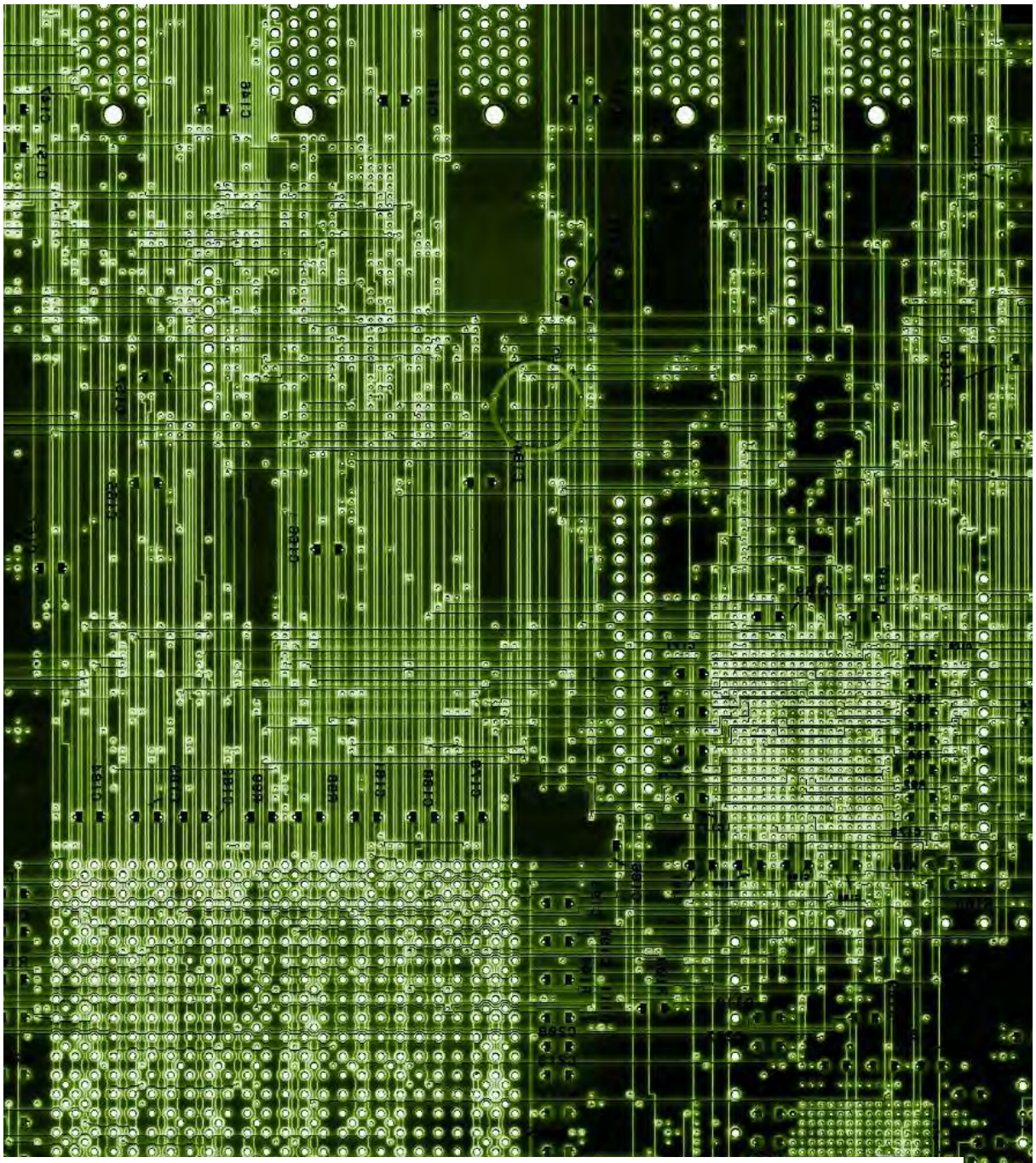
Dobre praktyki

- Staraj się sprawdzać aktualizacje Twojego oprogramowania - nie tylko systemu operacyjnego, ale także aplikacji, z których korzystasz. Postaraj się wyznaczyć konkretny dzień na uaktualnienia - najlepiej robić to regularnie.

- Jeżeli posiadasz wiele aplikacji, możesz skorzystać z narzędzia, które pobierze i zainstaluje wszystkie aktualizacje dla Twojego oprogramowania.

- Aktualizacje sprawdzaj przez strony producentów lub dedykowane programy, aby instalować tylko oryginalne oprogramowanie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.



Część III

Kilka technicznych aspektów Cyberbezpieczeństwa

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie
za uprzednią zgodą Cyberskiller Sp. z o.o.

Triada bezpieczeństwa IT

Realizując program bezpieczeństwa informacji w dowolnej organizacji, należy zwrócić szczególną uwagę na zapewnienie trzech podstawowych usług bezpieczeństwa, które określanesą jako triada bezpieczeństwa. Są to poufność, (ang. confidentiality), integralność (ang. integrity) i dostępność (ang. availability).

Poufność

Poufność jest zasadą, która mówi, że tylko upoważnione osoby, procesy i systemy mogą mieć dostęp do informacji na podstawie ustalonych zasad ograniczonego dostępu. Łączy się ona również z prywatnością informacji i koniecznością jej ochrony przed osobami, które mogą być w stanie popełnić przestępstwo, uzyskując dostęp do prywatnych danych. Informacje powinny być klasyfikowane, aby określić wymagany poziom poufności oraz to, a kto powinien mieć dostęp do informacji (do publicznego użytku, do użytku wewnętrznego lub poufne). Procesy identyfikacji, uwierzytelniania i autoryzacji, które realizowane są przy pomocy metod kontroli dostępu, są praktykami pozwalającymi zachować poufność informacji. Poufność można zachować również poprzez szyfrowanie, które ogranicza możliwość dostępu do jawnych danych. Dodatkowo, nieautoryzowani użytkownicy powinni mieć z założenia zakaz dostępu do informacji. Zagrożenie stanowią też autoryzowani użytkownicy, ponieważ mogą mieć złe zamiary i wykorzystać zdobyte dane nie tylko do osiągnięcia celów firmy, a dla własnej wiedzy lub osobistego zysku.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Integralność

Integralność jest zasadą, która mówi, że informacje powinny być chronione od zamierzonych, nieautoryzowanych lub przypadkowych zmian. Informacje przechowywane w plikach, bazach danych, systemach i sieciach muszą być integralne, aby dokładnie je przetworzyć przez różne transakcje systemowe, które następnie dostarczają dokładne dane potrzebne do podejmowania decyzji biznesowych. W systemie muszą zostać wprowadzone mechanizmy kontrolne w celu zapewnienia, że informacja nie jest modyfikowana niezgodnie z przyjętymi dostępami i praktykami. Warto więc wprowadzić jasny podział obowiązków iwdrożyć praktyki testowania systemów, które zapewniają integralność informacji.

Dostępność

Dostępność jest zasadą, która mówi, że informacja jest dostępna dla użytkowników zawsze wtedy, gdy jest potrzebna. Dwa główne obszary, wpływające na dostępność systemów, to: a) atak odmowy usługi (ang. Denial of service, DoS) ze względu na brak odpowiednich mechanizmów kontroli bezpieczeństwa oraz b) utrata możliwości realizacji usługi z powodu katastrofy, takiej jak trzęsienie ziemi, tornado, huragan, pożar, powódź i tak dalej. W obu przypadkach użytkownik nie ma dostępu do informacji niezbędnych do wykonywania swoich obowiązków zawodowych. Znaczenie takich incydentów dla organizacji jest uzależnione od krytyczności systemu, który został poddany atakowi odmowy dostępu lub zagrożeniu zewnętrznemu.

Podczas tworzenie projektu systemu oraz wdrożenia aplikacji lub procesów zarządzania, wpływ poszczególnych elementów na zagwarantowanie usług poufności, integralności i dostępności powinien być dobrze przeanalizowany. Różne mechanizmy bezpieczeństwa odnoszą się do zagwarantowania różnych usług bezpieczeństwa. Na przykład - określenie procedury tworzenia kopii zapasowej oprogramowania i określenie sprzętu do wykony-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

wania kopii zapasowych będzie najbardziej zorientowane w aspekcie dostępności bezpieczeństwa informacji; za to wybór silnego uwierzytelniania dwuskładnikowego będzie najbardziej związany z zagwarantowaniem poufności informacji poprzez wzmocnienie procesu uwierzytelniania.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Systemy detekcji oraz zapobiegania włamaniom

Wykrywanie włamań jest procesem monitorowania zdarzeń występujących w systemie komputerowym lub sieci i ich analizą pod kątem pewnych oznak odwołujących się do konkretnych zdarzeń. Są one są naruszeniem bezpieczeństwa lub grożą naruszeniem zasad bezpieczeństwa komputerowego, polityk dopuszczalnych wykorzystania lub standardowych praktyk bezpieczeństwa. Incydenty mogą mieć wiele przyczyn, takich jak złośliwe oprogramowanie (np. robaki, spyware) lub atakujących, którzy uzyskują nieautoryzowany dostęp do systemów z Internetu. Mogą być również związane z naruszeniami wykonanymi przez uprawnionych użytkowników systemu, którzy nadużywają lub próbują uzyskać dodatkowe przywileje, do których nie są upoważnione.

System wykrywania włamań (IDS) to oprogramowanie, które automatyzuje proces wykrywania intruzów. System zapobiegania włamaniom (IPS) to oprogramowanie, które posiada wszystkie funkcje systemu wykrywania włamań, a także może próbować zatrzymać ewentualne incydenty.

Systemy wykrywania włamań koncentrują się głównie na identyfikacji ewentualnych incydentów. Na przykład mogą wykryć, kiedy intruz próbuje zaatakować zagrożony system, wykorzystując lukę w nim. System ten może następnie zgłosić incydent do administratorów bezpieczeństwa, którzy szybko inicjują działania związane z reagowaniem na tego typu problemy w celu zminimalizowania szkód przez nie spowodowanych. Wiele systemów wykrywania włamań można również skonfigurować do monitorowania naruszeń polityki bezpieczeństwa. Przykładowo - konfigurujączestaw reguł na zaporze ogniowej, co pozwoliokreślić naruszający zasady bezpieczeństwa ruch w sieci. Ponadto niektóre systemy mogą monitorować przesyłanie plików i zidentyfikować te, które mogą być podejrzane, np.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

kopiowanie dużej bazy danych na laptopie użytkownika.

Wiele systemów wykrywania włamań może również określić aktywność rozpoznawczą atakującego - co wskazuje na to, że atak jest nieunikniony. Na przykład niektóre narzędzia i formy ataku szkodliwego oprogramowania, w szczególności robaki, wykonują skanowanie architektury IT w poszukiwaniu słabości systemowych, by zidentyfikowaćcele doataków. System może być w stanie zablokować taki rekonesans i poinformować administratorów bezpieczeństwa, którzy wówczas mogą podjąć odpowiednie działania.

Oprócz identyfikacji i wspierania wysiłków reagowania na incydenty, organizacje mogą znaleźć inne zastosowania dla systemów wykrywania włamań. Są to:

- Identyfikacja problemów w zakresie polityki bezpieczeństwa. System może zapewnić pewien stopień kontroli jakości w celu realizacji polityki bezpieczeństwa, poprzez powielanie zestawów reguł zapory i alarmowanie, gdy widzi ruch w sieci, który powinien być zablokowany przez zaporę.
- Dokumentowanie istniejącego zagrożenia dla organizacji. Systemy wykrywania włamań wykonują zapisy kontrolne danych mówiących o potencjalnych zagrożeniach w organizacji. Zrozumienie i charakterystyka określająca częstotliwość wykonywanych ataków jest pomocna w identyfikacji odpowiednich środków bezpieczeństwa dotyczących ochrony zasobów. Informacje te mogą być również wykorzystywane do edukacji na temat zagrożeń, jakie stoją przed organizacją.
- Odstraszanie osób chcących naruszyć zasady bezpieczeństwa. Jeśli ludzie są świadomi, że ich działania są monitorowane przez wewnętrzne systemy, mogą być mniej skłonni do popełniania takich naruszeń ze względu na ryzyko wykrycia.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Metodologie wykrywania włamań

Systemy wykrywania włamań używają wielu metod. Wśród nich można wymienić: oparte na sygnaturach, oparte na anomaliach oraz analizę stanu protokołów.

Wykrywanie oparte na sygnaturach

Sygnatura to wzór odpowiadający znanemu zagrożeniu. Wykrywanie na nich oparte jest procesem porównywania posiadanych sygnatur zagrożeń z zaistniałymi w celu identyfikacji ewentualnych incydentów.

Przykładowymi sygnaturami może być próba nawiązania połączenia przy użyciu aplikacji ftp z nazwą użytkownika „root", co stanowi naruszenie polityki bezpieczeństwa danej organizacji. Inny przykład to wiadomość e-mail z tematem „poufne" i nazwą pliku w załączniku „tajne.exe", które są charakterystyką znanej postaci złośliwego oprogramowania.

Wykrywanie oparte na sygnaturach jest bardzo skuteczne w znajdowaniu znanych, ale w dużej mierze nieskuteczne w wykrywaniu nieznanych wcześniej lub ukrytych zagrożeń. Owy brak skuteczności wynika ze stosowania technik unikania i modyfikacji tylko dobrze poznanych nieprawidłowości. Na przykład, jeśli atakujący zmodyfikuje nazwę złośliwego oprogramowania wużywając nazwy pliku „tajne2.exe", sygnatura będzie szukała „tajne.exe" i nie zidentyfikuje zagrożenia.

Wykrywanie oparte na sygnaturach jest najprostszą metodą detekcji, ponieważ porównuje bieżącą jednostkę działalności z wykazem sygnatur za pomocą operacji porównania ciągów. Technologie wykrywania oparte na sygnaturach słabo sprawdzają się w analizie wielu protokołów sieciowych lub aplikacji oraz nie potrafią skutecznie śledzić złożonych komunikatów. Brakuje im na przykład możliwości zapamiętania wyniku wcześniejszej analizy podczas rozpatrywania bieżących pakietów. To ograniczenie metod wykrywania

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

ataków, nie pozwala im analizować incydentów obejmujących wiele zdarzeń, jeśli żadne z nich nie wskaże na konkretny atak.

Detekcja bazująca na anomaliach

Wykrywania anomalii oparte jest na procesie analizy tego, co jest uważane za normalną aktywność wobec zaobserwowanych zdarzeń w celu identyfikacji istotnych odstępstw. System wykrywania włamań posiada profile poprawnych zdarzeń systemowych, które stanowią opis normalnych zachowań użytkowników, hostów, połączeń sieciowych lub aplikacji.

Profile są tworzone przez monitorowanie charakterystyki typowej aktywności w danym czasie.Na przykład profil dla sieci może pokazać, że aktywność internetowa zawiera średnio 15% przepustowości sieci na granicy Internetu podczas typowych godzin pracy. Następnie systemy wykrywania włamań używają metod statystycznych w celu porównania cech bieżącej działalności do progów związanych z profilem, takich jak wykrywanie, gdy aktywność internetowa obejmuje znacznie większą przepustowość niż oczekiwano i ostrzeganie administratora o anomalii. Profile mogą być opracowane dla wielu atrybutów behawioralnych, przykładowo: liczby e-maili wysyłanych przez użytkownika, ilości nieudanych prób logowania do serwerów czy poziomu wykorzystania procesora dla hosta w danym okresie czasu.

Główną zaletą metody wykrywania opartej na anomaliach jest to, że mogą być bardzo skuteczne w wykrywaniu nieznanych wcześniej zagrożeń. Załóżmy na przykład, że komputer zostanie zainfekowany nowego typu złośliwym oprogramowaniem. Wirus może zużywać zasoby urządzenia, wysyłać dużą liczbę wiadomości e-mail, zainicjować dużą liczbę połączeń sieciowych i wykonywać inne działania, które znacznie różnią się od tych ustalonych w profilu dla danego komputera.

Początkowy profil jest generowany przez pewien czas(zwykle dni, czasem tygodnie), czasami zwany okresem szkolenia. Profile do wykrywania anomalii mogą być zarówno statycz-

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

ne, jak i dynamiczne. Po wygenerowaniu statycznego profilu nie jest on już dalej uaktualniany, chyba że system wykrywania włamań będzie wykonywał nowy profil. Dynamiczny profil jest regulowany nieustannie. Uwzględnia on wówczas nowe wydarzenia. Ponieważ systemy i sieci zmieniają się w czasie, statyczne profile w końcu stają się niedokładne, a więc muszą być okresowo regenerowane. Profile dynamiczne nie mają tego problemu, ale są podatne na próby oszustw z napastnikami. Na przykład, atakujący początkowo może wykonać złośliwe działanie od czasu do czasu, a następnie powoli zwiększać częstotliwość i ilość złośliwych aktywności. Jeśli tempo zmian jest bardzo powolne, wówczas system wykrywania włamań może uznać złośliwą działalność za normalne zachowanie i umieścić go w swoim profilu.

Analiza stanu protokołu

Analiza stanu protokołów jest procesem porównania z góry określonych profili ogólnie przyjętych definicji poprawnego działania protokołów dla każdego stanu protokołu z obserwowanymi zdarzeniam w celu identyfikacji różnic. W przeciwieństwie do wykrywania anomalii, które wykorzystują profile komputera lub sieci, analiza stanu protokołów opiera się na profilu uniwersalnym, który określa, jak protokoły powinny i nie powinny być stosowane. W analizie stanowej system wykrywania włamań jest zdolny do zrozumienia i śledzenia stanu protokołów sieci transportowej oraz aplikacji. Na przykład, gdy użytkownik uruchamia sesję FTP, jest ona początkowo w stanie nieuwierzytelnionym. Nieuwierzytelniony użytkownik powinien móc wykonać tylko kilka poleceń w tym stanie, takich jak wyświetlanie ogólnych informacji lub podanie nazwy użytkownika i hasła. Ważnym elementem jest powiązanie stanu żądania z odpowiedziami. Gdy wystąpi próba uwierzytelniania FTP, system wykrywania (znając budowę protokołu FTP), może określić, czy został wykonany poprawnie.

Analiza stanu protokołów może zidentyfikować nieoczekiwane sekwencje poleceń, takich jak wydawanie tego samego polecenia wielokrotnie lub wydawanie polecenia bez uprzedniego wydania polecenia, od któregojest ona zależna. Inną funkcją śledzenia stanu

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

protokołów jest to, że dla protokołów, które wykonują uwierzytelnianie, system wykrywania włamań może śledzić uwierzytelnianie dla wszystkich wykonywanych sesji i wykonać zapisy kontrolne tego procesu, które następnie mogą posłużyć do wykrycia podejrzanych aktywności.

Metody analizy stanu protokołów używają takich modeli, które są zwykle oparte na standardach protokołów przede wszystkim od dostawców oprogramowania i organizacji normalizacyjnych (np, Internet Engineering Task Force [IETF] Request for Comments [RFC]). Standardy te zazwyczaj biorą pod uwagę rozbieżności w realizacji każdego protokołu. Niestety, wiele norm nie opisuje w sposób wyczerpujący wszystkich możliwych stanów protokołu. Prowadzi to do różnic między implementacjami. Również wielu producentów albo narusza normy, albododaje własne funkcje, z których niektóre mogą zastąpić funkcje opisane w standardach. Protokoły, które są tworzone przez firmy prywatne, często nie są szczegółowo opisane, a czasami nawet są niedostępne - co utrudnia systemom wykrywania włamań wykonanie kompleksowej i dokładnej analizy.

Typy systemów IDS

Istnieje wiele typów systemów wykrywania włamań. Można je podzielić na cztery grupy w zależności od rodzaju rejestrowanych zdarzeń oraz sposobu ich rozmieszczenia:

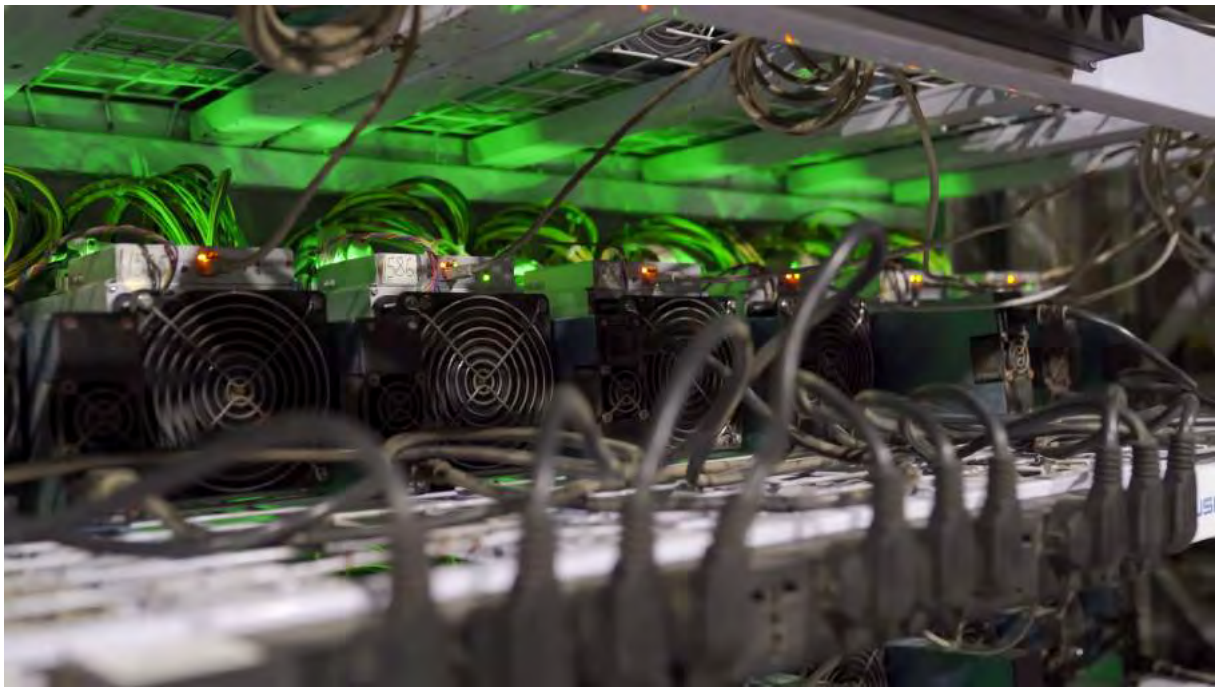
1. **Oparte na sieci** (ang. *Network-based*) - to systemy, które monitorują ruch w sieci dla poszczególnych segmentów lub urządzeń sieciowych oraz analizują aktywność protokołów i aplikacji w celu identyfikacji podejrzanej aktywności. Są one najczęściej stosowane na granicy między sieciami, na przykład w sąsiedztwie zapór granicznych lub routerów, wirtualnych sieci prywatnych (VPN), serwerów, serwerów zdalnego dostępu i sieci bezprzewodowych.

2. **Bezprzewodowe** (ang. *Wireless*) - to systemy, które monitorują ruch sieciowy i analizują bezprzewodowe protokoły sieciowe, aby zidentyfikować podejrzane działania z udziałem samych protokołów. Systemy te nie mogą zidentyfikować podejrzanych działań na warstwie aplikacji lub protokołów sieciowych wyższych warstw (np, TCP, UDP). Są one najczęściej stosowane w zasięgu sieci bezprzewodowej przez organizacje, które kontrolują daną sieć. Mogą być również stosowane w nieautoryzowanych sieciach bezprzewodowych, np. w przestrzeni publicznej.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

3. **Analiza zachowania w sieci** (ang. *Network Behavior Analysis*, NBA) - to systemy, które analizują ruch sieciowy w celu identyfikacji zagrożeń generujących przepływy nietypowego ruchu, takich jak: atak Distributed Denial of Service (DDoS), niektóre formy złośliwego oprogramowania (np. robaki, backdoory) czy naruszenia zasad (np. system klienta świadczący usługi sieciowe do innych systemów). Systemy NBA są najczęściej stosowane do monitorowania przepływów w sieciach wewnętrznych danej organizacji. Czasami stosowane są również do monitorowania ruchu pomiędzy sieciami danej organizacji w sieci zewnętrznej (np. Internet, sieci partnerów biznesowych).

4. **Oparte na urządzeniach** (ang. *Host-Based*) - to systemy monitorujące charakterystyki zachodzących wydarzeń na pojedynczym hoście czy urządzeniu. Przykładowymi elementami, które mogą być monitorowane, są; ruch sieciowy (tylko dla tego hosta), logi systemowe, uruchomione procesy, aktywność aplikacji, dostęp do plików i ich modyfikacja, zmiany w konfiguracji aplikacji lub systemu operacyjnego. Systemy te są stosowane najczęściej na krytycznych hostach, takich jak publicznie dostępne serwery czy serwery zawierające poufne informacje.



Niektóre typy systemów wykrywania włamań są bardziej rozwinięte technologicznie niż inne, ponieważ były używane oraz rozwijane od dłuższego czasu. Systemy oparte na sieci oraz niektóre oparte na urządzeniach są dostępne na rynku już od ponad dziesięciu lat. Oprogramowania analizujące zachowanie w sieci są stosunkowo nowymi produktami, które stosowane są głównie do wykrywania ataków DDoS, a częściowo do monitorowania ruchu w sieci wewnętrznej. Technologie bezprzewodowe są równie młodym rodzajem systemów wykrywania. Zostały one opracowane w odpowiedzi na popularność lokalnych sieci bezprzewodowych (WLAN) oraz rosnącą liczbą zagrożeń przeciwko samym sieciom i użytkownikom sieci WLAN.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Bezpieczeństwo sieci komputerowej

W dzisiejszych świecie wszystkie systemy IT są powiązane między sobą i komunikują się stale, wymieniając różne dane. Fakt ciągłej wymiany informacji sprawia, że jednym z kluczowych zagadnień jest bezpieczeństwo sieci komputerowej. Specjaliści ds. ochrony informacji powinni znać podstawowe klasy nadużyć sieci oraz umieć je odwzorować na uznawany standard, np. modelu OSI.

Podstawowe klasy nadużyć w sieci

1. **Nieuprawniony dostęp do usług sieciowych przez obejście zabezpieczenia kontroli dostępu.**

Ten atak odnosi się do legalnych użytkowników, którzy uzyskali dostęp do usług sieciowych, do których zwykle tego dostępu nie mają. W przeciwieństwie do włamania do sieci, ten rodzaj przemocy koncentruje się przede wszystkim na tych użytkownikach, którzy mają dostęp do zasobów z sieci wewnętrznej (zazwyczaj mających niską klauzulą tajności).

2. **Nieautoryzowane korzystanie z sieci dla pozazawodowych celów.**

Ten styl nadużyć w sieci odnosi się do niebiznesowego lub osobistego użytku sieci przez autoryzowanych użytkowników. Korzystanie z usług sieciowych do celów innych niż biznesowe, może być uznane za nadużycie systemu.

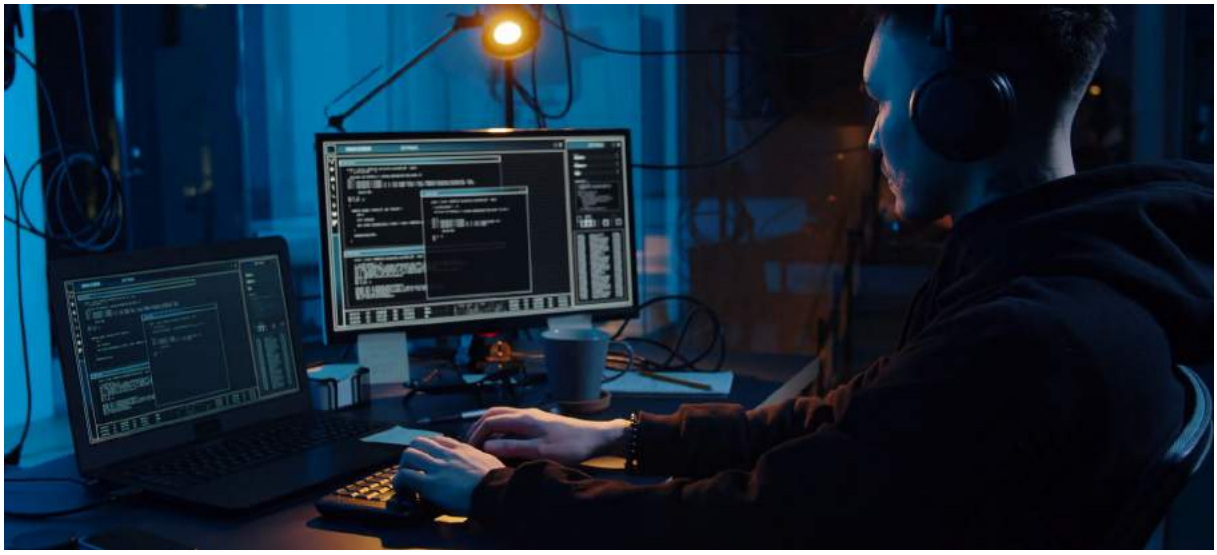
3. **Podsłuch.**

Ten rodzaj ataku sieciowego polega na nieuprawnionym przechwytywania ruchu sieciowego. Niektóre metody transmisji sieciowych, np. droga satelitarna, telefon komórkowy, PDA itp., są narażone na podsłuch. Istnieje również możliwość fizycznegoprzechwycenia medium transmisyjnego (jak składanie kabla, utworzenie pętli indukcyjnej, odebranie

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

emanacji elektromagnetycznej).

Podsłuch pasywny - Potajemne monitorowanie lub słuchanie transmisji przez osoby do tego nieuprawnione.
Podsłuch aktywny - Manipulowanie przy transmisji lub aktywne sondowania sieci w poszukiwaniu informacji wewnątrz infrastruktury.



4. **Ataki typu DoS oraz inne związane z zakłóceniami dostępu do usługi.**

Ataki tego typu powodują przerwy w dostępie do usługi z powodu intensywności wykorzystania zasobów sieciowych. Może być on skierowany na urządzenia sieciowe, serwery lub przepustowość sieci bez względu na obszar, w którym takie natężenie ruchu może w znacznym stopniu wpłynąć negatywnie na pracę sieci. Atak tego typu stosowany jest również jako sabotaż, umożliwiający umyślne uzyskanie informacji z różnych źródeł w systemie.

5. **Włamania do sieci.**

Ten rodzaj ataków odnosi się do użycia nieautoryzowanego dostępu w celu włamania się do sieci - najczęściej z „zewnątrz". W przeciwieństwie do ataku na login, tu intruzi są obcy. Najczęstsze ataki hakerskie zaliczają się właśnie do tej kategorii.. Określa się go również jako atak penetracji, który wykorzystuje znane luki bezpieczeństwa w danym systemie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

6. **Sprawdzanie, badanie, skanowanie.**

Taki atak jest aktywną odmianą podsłuchu. Zwykle używany w celu uzyskania przez atakującego mapy sieciw ramach przygotowań do włamania lub ataku DoS. W jego wyniku podsłuchujący może uzyskać listę dostępnych usług sieciowych. Analiza ruchu za pomocą sniffera jest jednym z typów podsłuchu, gdzie, poprzez skanowanie hostów w celu znalezienia dostępnych serwisów, można uzyskać informację o tym, jakie systemy są aktywne w sieci oraz jakie porty są otwarte. Atak ten może być przeprowadzony „ręcznie" lub „automatycznie". „Ręczne" wyszukiwanie słabych punktów sieci wykonywane jest za pomocą narzędzi takich jak Telnet do połączenia się ze zdalnym hostem, aby sprawdzić, na jakich portach dana maszyna nasłuchuje. „Automatyczne" skanery luk bezpieczeństwa to programy, które same wykonują wszystkie możliwe skany, raportując użytkownikowi znalezione błedy. Ze względu na ich dostępność w Internecie, liczba takich automatycznych testów w ostatnim czasie znacznie wzrosła.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Uwierzytelnienie i sygnatura cyfrowa

Kolejnym z kluczowych zagadnień w dziedzinie bezpieczeństwa informacji są autentykacja oraz uwierzytelnienia podmiotu. Podmiotem może być nie tylko użytkownik, ale również proces albo cały system. Analityk systemowy (a często i programista) powinien wiedzieć, jakich modułówkryptograficznych może użyć do tego celu i jakie są różnice pomiedzy nimi - zarówno funkcjonalne, jak i wydajnościowe.

Funkcje uwierzytelniające

Każdy mechanizm uwierzytelniania lub sygnatury cyfrowej ma dwa podstawowe poziomy:

- Poziom niższy - funkcja tworząca wartość uwierzytelniającą (ma posłużyć do uwierzytelnienia).
- Poziom wyższy - protokół uwierzytelnienia używający wartości uwierzytelniającej. Odbiorca może zweryfikować autentyczność komunikatu dzięki uzyskanej wartości uwierzytelniającej.

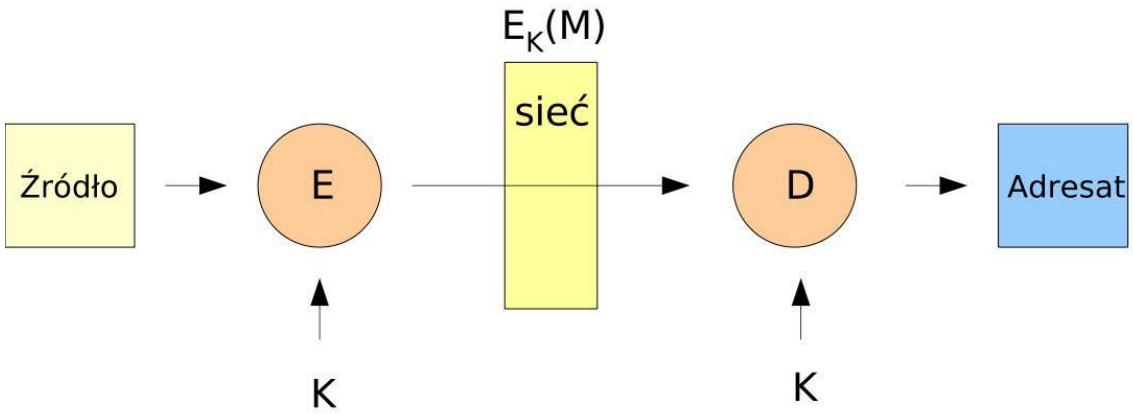
Wartość uwierzytelniająca

- Szyfrowanie komunikatów - zaszyfrowany tekst całego komunikatu pełni funkcje wartości uwierzytelniającej
- Kryptograficzna suma kontrolna - jawna funkcja komunikatu i tajnego klucza, która produkuje wartość o ustalonej długości służącej jako wartość uwierzytelniająca
- Funkcja haszujaca - jawna funkcja, która przekształca komunikat dowolnej długości na wartość o długości ustalonej . Element ten pełni rolę wartości uwierzytelniającej.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Protokoły uwierzytelniające – szyfrowanie

Podstawową formą szyfrowania jest szyfrowanie konwencjonalne (Rys.1). Cechy tej operacji zostały opisane poniżej.



Rysunek 1. Szyfrowanie konwencjonalne.

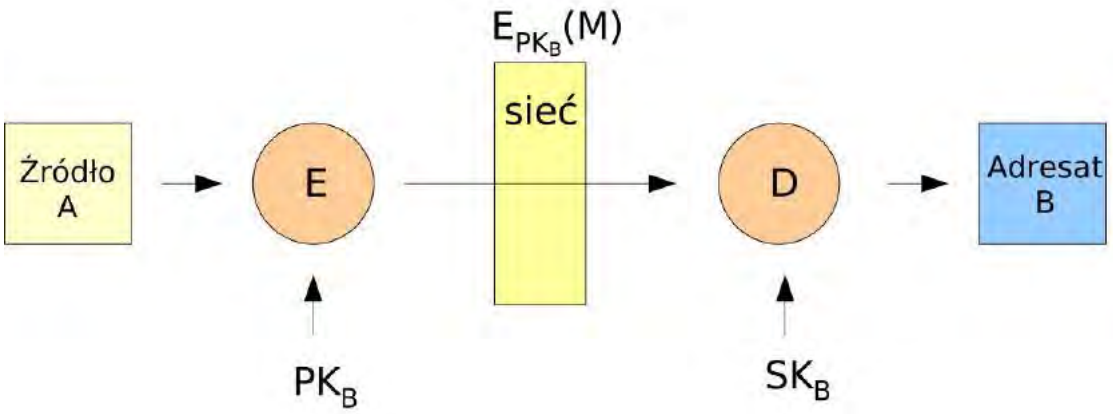
1. **Zapewnia poufność**:
   - Tylko A i B maja K.

2. **Zapewnia pewien poziom uwierzytelnienia**:
   - Wiadomość może pochodzić tylko od A.
   - Nie została zmieniona podczas przesyłania.
   - Wymaga pewnego formatowania (nadmiarowość) – określenie czy uzyskany ciąg bitów jest poprawny

3. **Nie zapewnia sygnatury**:
   - Odbiorca może sfałszować komunikat.
   - Nadawca może zaprzeczyć wysłaniu komunikatu.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Inną formą szyfrowania jest wykorzystanie kryptografii klucza publicznego (Rys.2). W tym przypadku wiadomość zostanie zaszyfrowana kluczem publicznym.



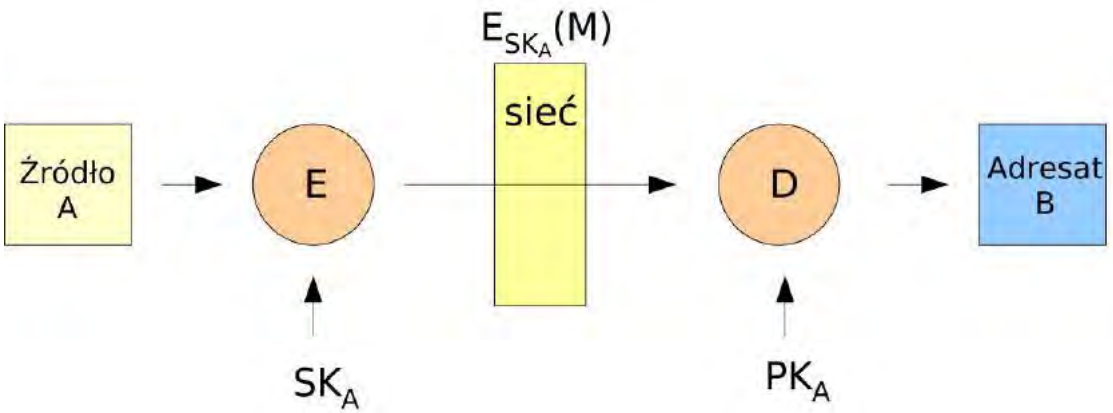
Rysunek 2. Szyfrowanie z kluczem publicznym.

1. **Zapewnia poufność**:
   - Tylko B ma SKB do deszyfrowania.

2. **Nie zapewnia uwierzytelnienia**:
   - Każdy może użyć PKB do zaszyfrowania komunikatu i udawać, że jest A.

3. **Nie zapewnia sygnatury**:
   - Odbiorca może sfałszować komunikat.
   - Nadawca może zaprzeczyć wysłaniu komunikatu.

Szyfrowanie z użyciem klucza prywatnego: uwierzytelnienie i sygnatura cyfrowa (Rys.3).



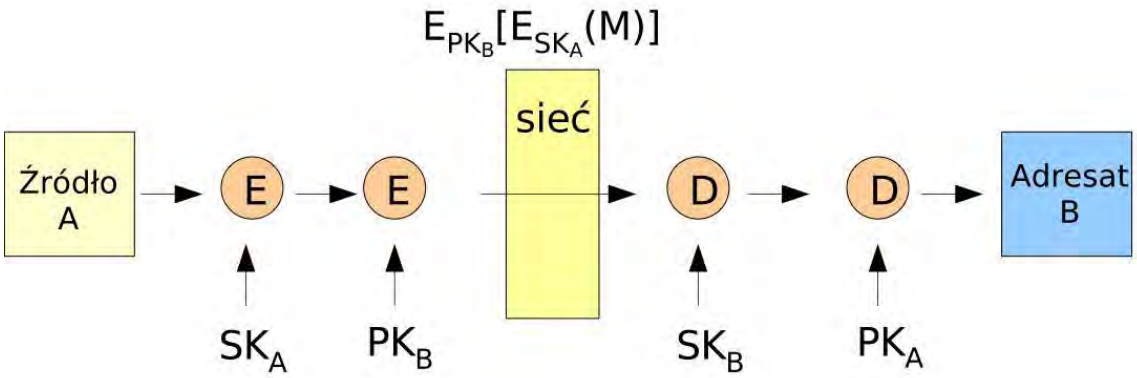
Rysunek 3. Szyfrowanie kluczem prywatnym.

1. **Zapewnia poufność**:
   - Każdy może użyć PKA do deszyfrowania.

2. **Zapewnia uwierzytelnienie i sygnaturę cyfrową**:
   - Tylko A ma SKA do deszyfrowania.
   - Komunikat nie został zmieniony podczas przesyłania.
   - Każda ze stron może użyć PKA do weryfikacji sygnatury.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Szyfrowanie z kluczem jawnym (Rys.4): poufność, uwierzytelnienie i sygnatura cyfrowa.



Rysunek 4. Szyfrowanie kluczem prywatnym i publicznym.

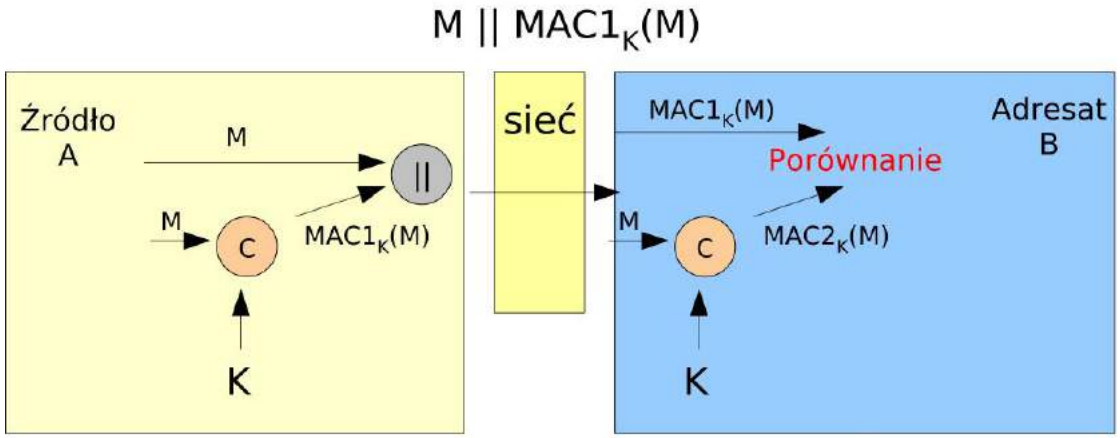
1. **Zapewnia poufność**:
   - Dzięki PKB, tylko B posiada SKB do deszyfrowania.

2. **Zapewnia uwierzytelnienie i sygnaturę cyfrową**:
   - Tylko A ma SKA do deszyfrowania.

Kryptograficzna suma kontrolna – MAC

Technika ta zakłada, że dwie strony A i B mają wspólny tajny klucz K. Polega ona na zastosowaniu tajnego klucza do stworzenia niewielkiego bloku danych o ustalonym rozmiarze (MAC). MAC dodaje się do komunikatu. Odbiorca otrzymuje komunikat oraz wartość MAC. Następnie generuje ze swojej strony wartość MAC i porównuje z otrzymaną. Jeżeli wiadomości są takie same, wówczas odbiorca uzyskuje pewność, że wiadomość nie została zmodyfikowana. Inaczej suma kontrolna nie zgodzi się. Odbiorca uzyskuje więc pewność, że komunikat pochodzi od nadawcy - tylko nadawca zna K.

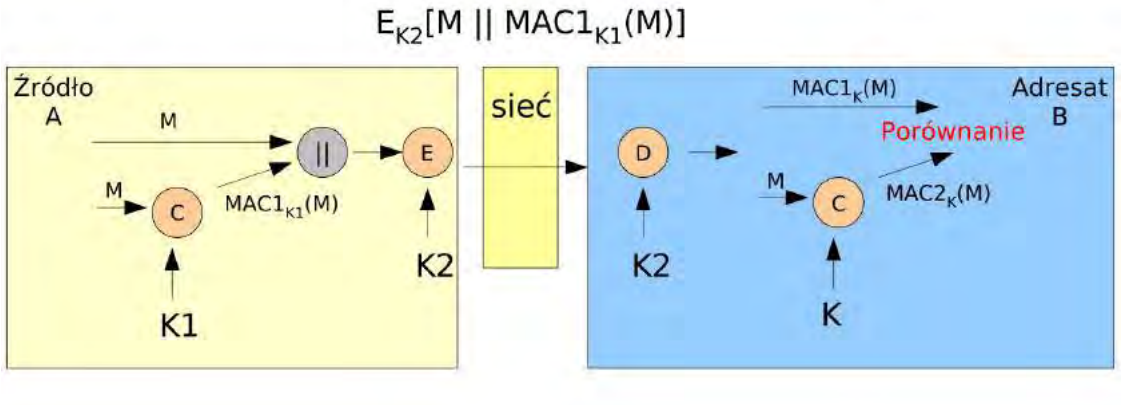
Protokół pozwalający zrealizować usługę uwierzytelnienia został przedstawiony na Rysunku 5.



Rysunek 5. Uwierzytelnienie przy użyciu funkcji MAC.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Na Rysunku 6 został przedstawiony protokół, gdzie oprócz uwierzytelnienia zagwarantowana jest poufność.



Rysunek 6. Uwierzytelnienie oraz gwarancja poufności przy użyciu funkcji MAC.

Funkcje haszujące

Wartość funkcji haszującej generuje się przy pomocy funkcji $h = H(M)$, gdzie M jest zmiennej długości, a uzyskany skrót h jest długości stałej. Wartość skrótu dodaje się do komunikatu w źródle (strona A) w chwili gdy mamy pewność, że jest ona poprawna. Odbiorca (strona B) uwierzytelnia komunikat przez samodzielne obliczenie wartości funkcji haszującej (obliczenie skrótu) i porównanie z otrzymanym skrótem. Wynik haszowania jest funkcją wszystkich bitów komunikatu i zapewnia wykrywanie modyfikacji: zmiana bitu lub bitów w komunikacie spowoduje zmianę w wyniku funkcji.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.

Funkcje haszujące - cechy

M – wiadomość o zmiennej długości
H – funkcja haszująca

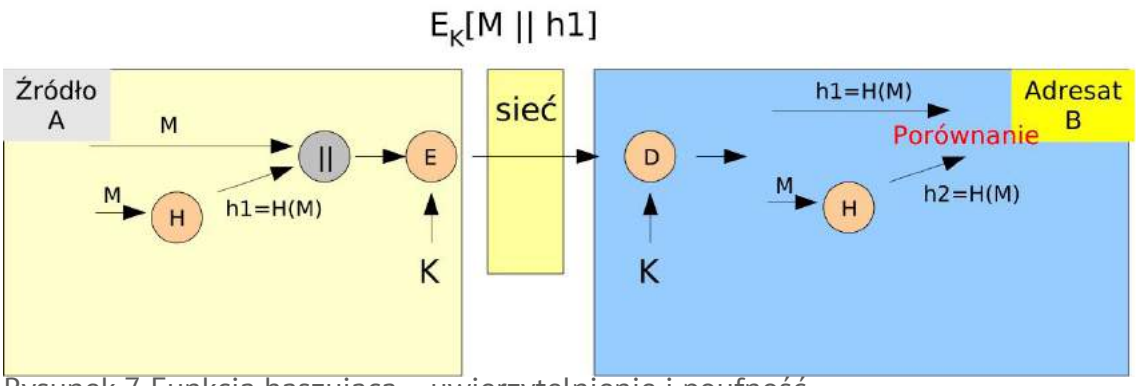
$h = H(M)$ – wartość funkcji haszującej (ustalona długość)

Cechy:

- H można zastosować do dowolnej wielkości bloku danych.
- H produkuje dane o ustalonej długości.
- $H(M)$ jest stosunkowo łatwo obliczyć dla każdego M.
- Dla każdego danego bloku M znalezienie takiego bloku N różnego od M takiego że: $H(M) = H(N)$ jest niewykonalne na drodze obliczeń (nie można znaleźć innego komunikatu, którego wynik haszowania będzie taki sam jak komunikatu pierwotnego).
- Dla każdej wartości funkcji haszującej $h = H(M)$ znalezienie danego M jest niemożliwe na drodze obliczeń (*jednokierunkowość*).
- Znalezienie takiej pary (x,y), że $H(x) = H(y)$ jest niewykonalne na drodze obliczeń (zwana kolizją).

Protokoły uwierzytelniające z funkcją haszującą

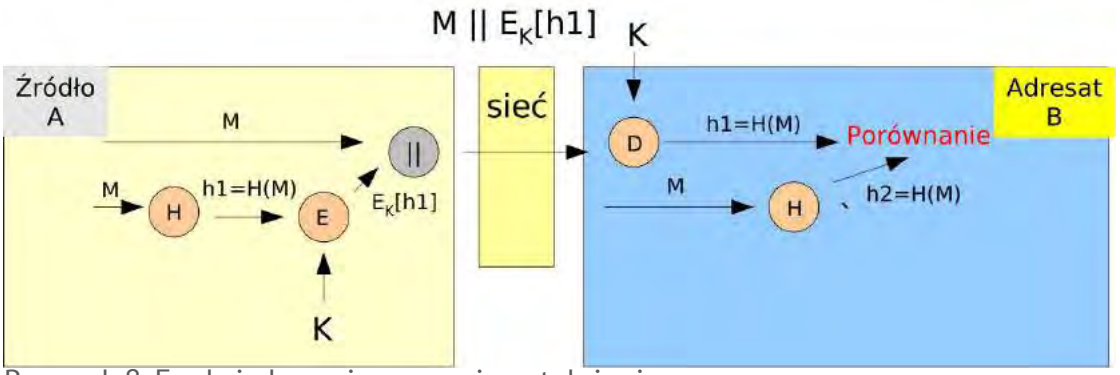
Na Rysunku 7 został przedstawiony protokół wykorzystania funkcji haszującej do zagwarantowania usługi uwierzytelnienia oraz poufności. Wówczas zapewniona jest poufność, ponieważ tylko A i B mają K. Zapewnione jest również uwierzytelnienie, ponieważ $h_1 = H(M)$ jest kryptograficznie zabezpieczone.



Rysunek 7. Funkcja haszująca – uwierzytelnienie i poufność.

Jeżeli nie jest wymagana usługa poufności, wówczas można zrezygnować z szyfrowania (Rysunek 8). Zapewnia się uwierzytelnienie, ponieważ $h_1 = H(M)$ jest kryptograficznie zabezpieczone.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie za uprzednią zgodą Cyberskiller Sp. z o.o.



Rysunek 8. Funkcja haszująca – uwierzytelnienie.

© copyright by Cyberskiller Sp. z o.o.
Wszystkie prawa zastrzeżone.
Wszelkie zmiany, kopiowanie i wykorzystywanie dozwolone wyłącznie
za uprzednią zgodą Cyberskiller Sp. z o.o.