DOBRE PRAKTYKI

DLA PRACOWNIKÓW

DOBRE PRAKTYKI DLA PRACOWNIKÓW SĄ ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

SPIS TREŚCI

04

BEZPIECZEŃSTWO HASEŁ I UWIERZYTELNIANIA

Korzystaj z uwierzytelniania wieloskładnikowego (MFA)

Jeśli masz taką możliwość to korzystaj z uwierzytelniania wieloskładnikowego (MFA). Często w serwisach z wrażliwymi danymi jest dostępne uwierzytelnianie wieloskładnikowe z dwoma etapami – zazwyczaj nazywane jest wtedy uwierzytelnianiem dwuetapowym (2FA).

WYJAŚNIENIE

Standardowo określa się trzy rodzaje uwierzytelniania:

- czymś, co użytkownik zna (np. hasło),
- czymś, co użytkownik posiada (np. urządzenie mobilne, konto e-mail, sprzętowy klucz bezpieczeństwa),
- czymś, czym użytkownik jest (np. linie papilarne).

Uwierzytelnianie wieloskładnikowe wymaga użycia przynajmniej dwóch rodzajów uwierzytelnienia. Przykładowo może to być:

- hasło oraz kod wysyłany na e-mail lub SMS,
- hasło oraz kod generowany przez aplikację zainstalowaną na telefonie,
- hasło oraz sprzętowy klucz bezpieczeństwa (np. podłączony do USB),
- uwierzytelnianie wieloskładnikowe jest dodatkowym zabezpieczeniem chroniącym konto w momencie kiedy dane logowania zostaną skradzione lub upublicznione – atakujący nawet znając login i hasło nie będzie w stanie się zalogować bez drugiego rodzaju uwierzytelnienia.

ODNOŚNIKI (PRZYKŁADOWE APLIKACJE ORAZ URZĄDZENIA UŻYWANE DO MFA):

Konfiguracja 2FA dla konta Google
Konfiguracja 2FA dla konta Microsoft
FreeOTP – aplikacja generująca kody jednorazowe, może działać z wieloma aplikacjami i serwisami
Google Authenticator – aplikacja generująca kody jednorazowe, może działać z wieloma aplikacjami i serwisami
Authy – aplikacja generująca kody jednorazowe, podobnie jak Google Authenticator
YubiKey – sprzętowy klucz bezpieczeństwa, używany jako drugi składnik uwierzytelniania, może działać z wieloma aplikacjami i serwisami
Thetis Fido – sprzętowy klucz bezpieczeństwa, używany jako drugi składnik uwierzytelniania, podobnie jak YubiKey

05

BEZPIECZEŃSTWO HASEŁ I UWIERZYTELNIANIA

Twórz swoje hasła według dobrych praktyk

Dobre hasło powinno:

- być długie (najlepiej ponad 12 znaków) – długie hasła są dużo trudniejsze do złamania,
- nie zawierać informacji związanych z danymi użytkownika lub jego bliskich (np. imię, nazwisko, data urodzenia, itp) – atakujący może wykorzystać znajomość naszych danych do szybszego złamania hasła,
- nie zawierać znanych powiedzeń (np. “WlazlKotekNaPlotek”) – takie hasła są łatwiejsze do złamania przy wykorzystaniu ataku słownikowego,
- być łatwe do zapamiętania a jednocześnie trudne do odgadnięcia – w tym wypadku najlepiej sprawdza się zlepek słów, np. “na czerwonym drzewie siedzi biała krowa”. Takie hasła są trudne do złamania, a jednocześnie dużo łatwiej je zapamiętać niż losowy ciąg liter i cyfr. Jeśli używasz menedżera haseł możesz korzystać z haseł generowanych przez to oprogramowanie – ze względu na to, że hasła są przechowywane w menadżerze nie ma konieczności ich zapamiętywania.

WYJAŚNIENIE

Bardzo często narzucane użytkownikowi zasady dotyczące haseł wymagają znaków różnej wielkości, cyfr i znaków specjalnych. Jednakże NIST w dokumencie “SP 800-63B Digital Identity Guidelines; Appendix A” wskazuje, że w takich sytuacjach użytkownicy mają tendencję do tworzenia przewidywalnych haseł (np. password -> Password1!). To oznacza, że zysk płynący z takich wymagań jest bardzo mały. Jednocześnie im trudniejsze do zapamiętania hasło, tym większe prawdopodobieństwo, że zostanie ono zapisane analogowo lub cyfrowo, co stwarza kolejne zagrożenie. NIST rekomenduje zwrócenie uwagi przede wszystkim na długość hasła oraz na sprawdzenie czy hasło nie jest zbyt podatne na ataki słownikowe, nie zawiera konkretnych słów (jak np. nazwa serwisu) i czy nie jest jednym z popularnie używanych haseł.

ODNOŚNIK:

SP 800-63 Digital Identity Guidelines

06

BEZPIECZEŃSTWO HASEŁ I UWIERZYTELNIANIA

Nie używaj tego samego hasła w więcej niż jednym serwisie

Hasło powinno być unikatowe dla każdego serwisu.

WYJAŚNIENIE

Jest to zasada ograniczająca ryzyko – nawet jeśli Twoje hasło do jakiegoś serwisu zostanie upublicznione to nie będzie mogło zostać użyte do zalogowania się do innego serwisu. Upublicznienie hasła może nastąpić na skutek wielu zdarzeń, np. wycieku danych, ataku socjotechnicznego, itd. Jeśli korzystasz z tego samego hasła we wszystkich miejscach to wyciek danych np. z mało znaczącego forum lub portalu może skutkować poznaniem hasła do Twojego konta bankowego lub poczty elektronicznej.

Nigdy nie podawaj nikomu swojego hasła

WYJAŚNIENIE

Nikt nigdy nie powinien poprosić Cię o podanie Twojego hasła. Jeżeli ktoś to robi i przedstawia się np. jako pomoc techniczna Twojej firmy to najprawdopodobniej jesteś celem ataku phishingowego.

Dbaj o bezpieczeństwo swojego hasła

Dbaj o to, żeby nikt nie poznał Twojego hasła. Obejmuje to m.in.:

- nie zapisuj swojego hasła w miejscach, do których ktoś inny ma dostęp,
- przy wpisywaniu hasła uważaj, żeby nikt nie zobaczył co wpisujesz,
- nie loguj się do żadnych ważnych usług na publicznych komputerach.

07

BEZPIECZEŃSTWO HASEŁ I UWIERZYTELNIANIA

Korzystaj z menedżera haseł

Do zarządzania swoimi danymi logowania wykorzystuj menedżera haseł.

WYJAŚNIENIE

Zachowanie jednocześnie dobrych praktyk tworzenia haseł oraz zasady nie używania tego samego hasła w więcej niż jednym serwisie jest trudne ze względu na liczbę różnych serwisów wymagających logowania. Dużym ułatwieniem jest korzystanie z menedżera haseł – programu, który pozwala zarządzać danymi uwierzytelniającymi. Menedżer haseł działa zazwyczaj według następującego schematu:

- na początku swojego działania tworzy zaszyfrowany plik bazy, chroniony zazwyczaj tzw. hasłem głównym,
- w momencie logowania do jakiegoś serwisu lub zakładania w nim konta, menedżer haseł pozwala na zapisanie danych logowania,
- po zapisaniu danych logowania do danego serwisu można logować się za pomocą menedżera haseł (aby skorzystać z zapisanych w menedżerze danych trzeba podać swoje hasło główne).

Menedżer haseł pozwala na posiadanie innego hasła do każdego serwisu bez konieczności ich zapamiętywania – wystarczy pamiętać swoje hasło główne.

ODNOŚNIKI:

Przykładowe menedżery haseł z otwartym kodem źródłowym:

KeePass
KeePassXC
pass

08

BEZPIECZEŃSTWO PRACY ZDALNEJ

Łącząc się zdalnie korzystaj z VPN

Jeśli Twoja firma posiada VPN to za każdym razem gdy pracujesz zdalnie zacznij od połączenia z nim.

WYJAŚNIENIE

VPN zwiększa znacząco bezpieczeństwo pracy zdalnej (patrz: Poradnik techniczny: VPN).

Nie zostawiaj swojego urządzenia bez nadzoru w miejscach publicznych

Nigdy nie pozostawiaj swojego urządzenia w miejscach publicznych bez nadzoru osoby zaufanej. Pamiętaj, że Twoje urządzenie to nie tylko sprzęt, ale również dane, które często są dużo więcej warte, a ich utrata może spowodować duże straty dla Ciebie i Twojej firmy.

WYJAŚNIENIE

Pozostawienie swojego urządzenia bez nadzoru w miejscu publicznym niesie za sobą wiele zagrożeń takich jak:

- kradzież urządzenia,
- kradzież danych z urządzenia,
- instalacja złośliwego oprogramowania.

09

BEZPIECZEŃSTWO PRACY ZDALNEJ

Pracując w miejscu publicznym zwracaj uwagę na otoczenie

Jeśli pracujesz w miejscu publicznym zwracaj uwagę co i kto znajduje się obok Ciebie. Pilnuj, aby nikt nie mógł zobaczyć ani nagrać wpisywanych haseł lub innych wrażliwych danych, a najlepiej unikaj pracy nad wrażliwymi danymi w miejscach, w których łatwo podejrzeć zawartość ekranu (np. pociąg, kawiarnia).

WYJAŚNIENIE

“Podglądnięcie” to bardzo prosty a jednocześnie trudny do wykrycia sposób wycieku danych. Nawet jeśli dane wyświetlające się na ekranie nie wydają się być szczególnie ważne to mogą zostać potem wykorzystane do ataków socjotechnicznych.

Stwórz osobne konto na swoim urządzeniu

Jeśli pracujesz z urządzenia używanego też przez inne osoby (np. domowy komputer), stwórz osobne konto, do którego nikt poza Tobą nie będzie miał dostępu.

WYJAŚNIENIE

Nawet jeśli ufasz swojej rodzinie to nadal istnieje możliwość, że ktoś będzie w stanie poznać hasło do konta kogoś z rodziny. Posiadanie osobnego konta będzie minimalizować ewentualne zagrożenie i podejrzenia w razie jakiegoś incydentu

10

BEZPIECZEŃSTWO PRACY ZDALNEJ

Do pracy zdalnej używaj jedynie urządzeń zatwierdzonych przez politykę firmy

Stosuj się do polityki firmy w zakresie urządzeń, które można używać do pracy zdalnej.

WYJAŚNIENIE

Niektóre firmy mogą dostarczać sprzęt firmowy i wymagać pracy tylko na nim, inne mogą pozwolić na pracę na urządzeniach pracowników. Takie zasady mają służyć zabezpieczeniu firmowych danych oraz usług przed włamaniem.

Unikaj używania nieznanych Ci urządzeń do jakichkolwiek czynności związanych z danymi firmowymi

Do wykonywania jakichkolwiek czynności związanych z danymi firmowymi (jak np. sprawdzenie skrzynki mailowej) używaj jedynie znanych i zaufanych urządzeń – własnych, Twojej firmy lub powiązanej organizacji (np. partner biznesowy).

WYJAŚNIENIE

Nie wiadomo czy nieznane urządzenie jest odpowiednio zabezpieczone oraz czy nie zostało zainfekowane złośliwym oprogramowaniem. Skorzystanie z takiego urządzenia może powodować kradzież danych takich jak hasła, wiadomości e-mail, itd.

11

BEZPIECZEŃSTWO PRACY ZDALNEJ

Zadbaj o zabezpieczenie swojej domowej sieci

Jeśli korzystasz z domowej sieci do pracy zdalnej to:

- Zmień domyślne hasło na urządzeniach tworzących sieć.
- Wyłącz możliwość konfiguracji urządzeń spoza wnętrza sieci.
- Jeśli nie używasz sieci WiFi upewnij się, że Twoje urządzenia jej nie dostarczają. Jeśli jej używasz zadbaj o odpowiednie zabezpieczenie (patrz: Zadbaj o zabezpieczenia swojej domowej sieci WiFi).
- Dbaj o aktualność oprogramowania na urządzeniach tworzących sieć.
- Nie podpinaj bezpośrednio swojego komputera lub laptopa do sieci dostarczanej przez dostawcę, używaj jakiegoś urządzenia pośredniczącego (router). Dzięki temu możesz chronić swój komputer przed niespodziewanym połączeniem z zewnętrza sieci.

WYJAŚNIENIE

Jeśli Twoja sieć domowa używana do pracy nie zostanie odpowiednio zabezpieczone to może być słabym punktem całego systemu i pozwolić na przechwycenie przesyłanych danych lub ataki typu Man in the middle (patrz Poradnik techniczny: Man in the middle).

12

BEZPIECZEŃSTWO KORZYSTANIA Z SIECI WIFI

Unikaj korzystania z publicznych sieci WiFi na tym samym urządzeniu, na którym przechowujesz dane firmowe

Jeśli na Twoim urządzeniu przechowywane są dane firmowe to unikaj łączenia się z publicznymi sieciami WiFi.

WYJAŚNIENIE

Jeśli sieć będzie sfałszowana lub przejęta przez atakującego, Twoje urządzenie może zostać zainfekowane złośliwym oprogramowaniem, a przesyłane dane mogą zostać przechwycone.

Wyłącz automatyczne łączenie się z publicznymi sieciami WiFi

WYJAŚNIENIE

Automatyczne łączenie się z publicznymi sieciami WiFi może skutkować połączeniem się ze specjalnie spreparowaną przez atakującego siecią, a w efekcie zainfekowaniem urządzenia malwarem lub wyciekiem przesyłanych danych (patrz: Poradnik techniczny: Fałszywa sieć WiFi).

ODNOŚNIKI:

Instrukcja zmiany ustawień łączenia się do otwartych sieci dla Windowsa, Androida i IOS

13

BEZPIECZEŃSTWO KORZYSTANIA Z SIECI WIFI

Nie łącz się do nieznanych i niezaufanych sieci WiFi

Nigdy nie łącz się z siecią WiFi jeśli nie jesteś pewien jej autentyczności. W hotelach, pociągach, itp. upewnij się, że dana sieć jest dostarczana przez usługodawcę.

WYJAŚNIENIE

Sieć WiFi może być specjalnie spreparowana w celu przechwycenia danych lub zainfekowania urządzeń złośliwym oprogramowaniem (patrz: Poradnik techniczny: Fałszywa sieć WiFi).

Wyłącz WiFi jeśli wychodzisz poza obszar ze znaną Ci siecią WiFi

Jeśli opuszczasz obszar, w którym jesteś połączony ze znanym Ci WiFi (np. biuro), wyłącz WiFi na swoim urządzeniu.

WYJAŚNIENIE

Celem jest uniknięcie automatycznego łączenia się urządzenia ze sfałszowaną siecią WiFi (patrz: Poradnik techniczny: Fałszywa sieć WiFi).

Zwracaj uwagę na to do jakiej sieci WiFi jesteś podłączony

Jeśli Twoje urządzenie automatycznie łączy się ze znanymi sieciami WiFi to powinieneś zwracać uwagę do jakiej sieci WiFi jesteś podłączony. Jeśli Twoje urządzenie będzie korzystało z sieci WiFi, która nie powinna być dostępna w danym miejscu to znaczy, że jesteś połączony ze sfałszowaną siecią (patrz: Poradnik techniczny: Fałszywa sieć WiFi).

14

BEZPIECZEŃSTWO KORZYSTANIA Z SIECI WIFI

Zadbaj o zabezpieczenia swojej domowej sieci WiFi

Jeśli korzystasz ze swojej domowej sieci WiFi do pracy to powinieneś wdrożyć podstawowe zabezpieczenia takie jak:

- zmień nazwę sieci (SSID),
- wyłącz rozgłaszanie nazwy sieci. Utrudni to podłączenie się do sieci osobom nieautoryzowanym,
- używaj silnego szyfrowania przesyłanych danych. NIST rekomenduje WPA2 with AES jako preferowany sposób szyfrowania,
- do łączenia z siecią WiFi używaj hasła spełniającego dobre praktyki wskazane w tym dokumencie,
- wyłącz możliwość bezprzewodowej konfiguracji Access Pointa.

WYJAŚNIENIE

Jeśli sieć WiFi używana do pracy nie zostanie odpowiednio zabezpieczone to może być słabym punktem całego systemu i pozwolić na przechwycenie przesyłanych danych lub ataki typu Man in the middle (patrz Poradnik techniczny: Man in the middle).

15

BEZPIECZEŃSTWO STACJI ROBOCZYCH

Nigdy nie podłączaj nieznanych i niezaufanych nośników danych/urządzeń

Jeśli nie jesteś całkowicie pewien co do zawartości nośnika danych lub urządzenia to nigdy nie podłączaj go do swojego komputera. Zastosuj się do obowiązujących w firmie procedur reagowania na takie sytuacje.

WYJAŚNIENIE

Nieznane urządzenie może zawierać złośliwe oprogramowanie. Jedną z metod wykorzystywanych przez atakujących jest podrzucanie zainfekowanych nośników podpisanych np. “Zarobki w firmie” z nadzieją na to, że któryś z zaciekawionych pracowników podepnie taki nośnik do swojego komputera.

Nie uruchamiaj ani nie instaluj nieznanych i niezaufanych programów

WYJAŚNIENIE

Uruchomienie niezaufanego programu może prowadzić do zainfekowania urządzenia złośliwym oprogramowaniem, a w następstwie nawet do zainfekowania całej firmy.

16

BEZPIECZEŃSTWO STACJI ROBOCZYCH

Zawsze blokuj swoje urządzenie gdy z niego nie korzystasz

Blokuj swoje urządzenie gdy z niego nie korzystasz. Używaj silnego zabezpieczenia (dobre hasło, skomplikowany wzór, itd). Dodatkowo włącz automatyczną blokadę urządzenia po określonym czasie nieaktywności.

WYJAŚNIENIE

Z niezablokowanego urządzenia znacznie łatwiej pozyskać dane np. w przypadku kradzieży lub chwilowego "pożyczenia". Z tego względu należy blokować urządzenia nawet jeśli wychodzi się "tylko na chwilę". Ponieważ każdy popełnia błędy i czasem zapomina o włączeniu blokady, warto ustawić automatyczną blokadę urządzenia po określonym czasie (np. 1 min).

17

BEZPIECZEŃSTWO PRZEGLĄDANIA STRON INTERNETOWYCH

Weryfikuj czy odwiedzane strony internetowe korzystają z bezpiecznego połączenia

Sprawdzaj czy odwiedzane strony przesyłają dane korzystając z protokołu HTTPS, a więc czy dane są przesyłane w formie zaszyfrowanej. Dotyczy to w szczególności stron z formularzami, przez które wysyłane są dane.

WYJAŚNIENIE

Przesyłanie danych w formie zaszyfrowanej zabezpiecza przed odczytem i modyfikacją danych w trakcie przesyłu. Zmniejsza również prawdopodobieństwo padnięcia ofiarą Man in the middle (patrz Poradnik Techniczny: Man in the middle).

Weryfikuj szczegóły certyfikatów stron internetowych

Poza sprawdzeniem czy dane są przesyłane za pomocą protokołu HTTPS weryfikuj też szczegóły certyfikatu strony internetowej. W przypadku instytucji operujących wrażliwymi danymi powinien być używany certyfikat OV SSL lub EV SSL (patrz Poradnik techniczny: Typy certyfikatów SSL). Szczegóły certyfikatu zazwyczaj są dostępne po kliknięciu w "kłódkę" znajdującą się obok paska adresu.

WYJAŚNIENIE

Certyfikaty OV i EV SSL dostarczają informację o autentyczności organizacji zarządzającej domeną, dzięki czemu można upewnić się z kim się komunikujemy.

ODNOŚNIKI:

Certyfikat bezpieczeństwa strony w Mozilla Firefox
Sprawdzanie czy połączenie jest bezpieczne w Google Chrome
Certyfikat bezpieczeństwa strony w Safari
Certyfikat bezpieczeństwa strony w Microsoft Edge

18

BEZPIECZEŃSTWO PRZEGLĄDANIA STRON INTERNETOWYCH

Weryfikuj poprawność adresów stron internetowych

Przed podaniem swoich danych logowania lub przesłania jakichś danych zweryfikuj czy adres strony jest poprawny. Dla często używanych stron (np. strona banku, dostawcy poczty) wykorzystaj zakładki w przeglądarce lub wpisuj adresy ręcznie – unikaj klikania w odnośniki przesyłane za pomocą poczty elektronicznej (istnieje możliwość, że przesłana wiadomość została sfałszowana i zawiera niepoprawny odnośnik).

WYJAŚNIENIE

Niektóre ataki opierają się o tworzenie sfałszowanych stron podobnych do oryginału i jednocześnie umieszczonych pod adresem bardzo zbliżonym do oryginalnego. Atakujący zbiera dane wpisywane na takiej stronie (np. dane logowania) i wykorzystuje je w dalszych atakach. Przykładem niepoprawnych a jednocześnie trudnych do zauważenia adresów są: gogle.pl, rnbank.pl.

Włącz blokowanie wyskakujących okienek (popup windows)

Upewnij się, że w przeglądarce masz włączone blokowanie wyskakujących okienek (popup windows).

WYJAŚNIENIE

Wyskakujące okna często służą do ataków phishingowych, np. pokazując użytkownikowi informację, że na jego komputerze znaleziono wirusy i pytając użytkownika czy pozwoli na usunięcie wirusów. Użytkownik klikając guzik potwierdzający nieświadomie pozwala na zainfekowanie komputera.

ODNOŚNIKI:

Konfiguracja blokowania wyskakujących okienek w Mozilli Firefox
Konfiguracja blokowania wyskakujących okienek w Google Chrome
Konfiguracja blokowania wyskakujących okienek w Microsoft Edge
Certyfikat bezpieczeństwa strony w Microsoft Edge

19

BEZPIECZEŃSTWO PRZEGLĄDANIA STRON INTERNETOWYCH

Jeśli przeglądarka zapamiętuje Twoje dane logowania to włącz dodatkowe zabezpieczenie hasłem głównym

WYJAŚNIENIE

Jeśli przeglądarka przechowuje dane uwierzytelniające bez ustawionego hasła głównego to zapisane hasła mogą zostać odczytane przez każdą osobę, która uzyska dostęp do przeglądarki na danym komputerze. Ustawienie hasła głównego jest dodatkowym zabezpieczeniem uniemożliwiającym odczyt haseł nawet jeśli ktoś uzyska dostęp do konta użytkownika na komputerze.

ODNOŚNIKI:

Konfiguracja hasła głównego w Mozilli Firefox
Google Chrome, Microsoft Edge oraz Safari automatycznie używają hasła do konta użytkownika jako hasła głównego

Usuń nieużywane dodatki do przeglądarki

Zweryfikuj wszystkie dodatki zainstalowane w przeglądarce i usuń te niepotrzebne.

WYJAŚNIENIE

Dodatki do przeglądarki mogą posiadać podatności lub same w sobie być złośliwym oprogramowaniem. Dlatego istnieje potrzeba regularnego sprawdzania które dodatki są potrzebne i usuwania wszystkich niepotrzebnych lub nieznanych.

ODNOŚNIKI:

Usuwanie dodatków w Mozilli Firefox
Zarządzanie dodatkami w Google Chrome
Rozszerzenia w Microsoft Edge
Zarządzanie dodatkami w Safari

20

ZABEZPIECZENIE DANYCH

Nie kopiuj danych na niezabezpieczone nośniki, nie przesyłaj ich na swoje prywatne konta

Jeśli polityka firmy tego zabrania to nigdy nie kopiuj firmowych danych na nośniki nieprzeznaczone do tego celu (jak np. prywatny pendrive) ani nie przesyłaj ich na swoje prywatne konta (np. mailowe lub na google drive).

WYJAŚNIENIE

Takie nośniki mogą zostać podłączone do zainfekowanego komputera, zgubione lub ukradzione i w efekcie doprowadzić do wycieku danych. Podobnie wygląda sytuacja w przypadku przesyłania firmowych danych na swoje prywatne konta.

Nie podłączaj nośników danych do niezaufanych urządzeń

Nie podłączaj nośników danych do urządzeń, jeśli nie jesteś pewien co do ich bezpieczeństwa.

WYJAŚNIENIE

Jeśli nośnik danych zostanie podłączony do zainfekowanego urządzenia to dane przechowywane na tym nośniku mogą zostać wykradzione, a ponadto sam nośnik może zostać zainfekowany i w efekcie doprowadzić do skompromitowania systemów firmy.

21

OCHRONA POCZTY ELEKTRONICZNEJ

Nie otwieraj załączników pochodzących z niepewnych źródeł

Jeśli nie masz pewności co do autentyczności wiadomości nie otwieraj załączonych plików i zastosuj się do obowiązującej w firmie polityki reagowania na takie sytuacje. Nigdy nie otwieraj plików .exe jeśli masz jakiekolwiek wątpliwości. Przed skorzystaniem z przesłanych plików sprawdź je programem antywirusowym.

Nie klikaj w odnośniki umieszczone w wiadomości

Jeśli nie jesteś pewien autentyczności otrzymanej wiadomości to nie klikaj w odnośniki w niej umieszczone, szczególnie uważaj na strony skracające linki (np. tinyurl.com). Jeśli otrzymujesz wiadomość od banku lub jakiegokolwiek innego serwisu wejdź na stronę manualnie przez swoją przeglądarkę, nie klikaj ani nie kopiuj przesłanego linku. Jeśli po otwarciu odnośnika rozpocznie się pobieranie pliku zachowaj ostrożność: przed otwarciem pliku upewnij się, że pochodzi on od zaufanego odbiorcy, przeskanuj plik programem antywirusowym.

WYJAŚNIENIE

Otrzymana wiadomość może być sfałszowana a odnośnik prowadzić do specjalnie przygotowanej strony, której celem jest kradzież Twoich danych lub pieniędzy. Sfabrykowana strona może dokładnie odwzorowywać wygląd witryny banku w celu nakłonienia Cię do podania swoich danych logowania.

22

OCHRONA POCZTY ELEKTRONICZNEJ

Zadbaj o szyfrowanie wiadomości i załączników

W przypadku przesyłania szczególnie istotnych danych skorzystaj z opcji szyfrowania wiadomości i załączników (end-to-end encryption) lub z szyfrowania załączników.
Do szyfrowania wiadomości możesz wykorzystać technologię PGP lub S/MIME (opisaną w sekcji PGP oraz S/MIME w Poradniku technicznym). Klucz publiczny służy do zaszyfrowania przesyłanej informacji. Klucz prywatny pozwala na jej odczyt. Ze względu na to, że klucz prywatny posiada jedynie jedna osoba (odbiorca), nikt inny nie może rozszyfrować wiadomości. Zaszyfrowaną wiadomość może wysłać każdy posiadający klucz publiczny odbiorcy. Większość nowoczesnych klientów pocztowych dostarcza opcję szyfrowania wiadomości, potrzebne są wygenerowane klucze oraz odpowiednia konfiguracja (zależna od klienta pocztowego).

Możesz również szyfrować przesyłane pliki ręcznie (np. za pomocą darmowego programu 7zip lub za pomocą mechanizmów wbudowanych w pakiety biurowe). Odbiorca będzie mógł odszyfrować plik korzystając z hasła, które powinieneś mu dostarczyć innym kanałem komunikacji niż mail.

WYJAŚNIENIE

Szyfrowanie wiadomości i załączników pozwoli uchronić się przed potencjalnym kradzieżą lub wyciekiem danych. Nawet jeśli wiadomość zostanie przechwycona to nie będzie mogła zostać odczytana przez nikogo poza odbiorcą. Szyfrowanie end-to-end zabezpiecza też przed odczytaniem danych w przypadku włamania na serwer pocztowy.

ODNOŚNIKI:

Konfiguracja szyfrowania wiadomości w Mozilli Thunderbird
Konfiguracja szyfrowania wiadomości w Microsoft Outlook
Konfiguracja szyfrowania wiadomości w Outlook Web App
Szyfrowanie plików w pakiecie MsOffice
Szyfrowanie plików w pakiecie LibreOffice

23

OCHRONA POCZTY ELEKTRONICZNEJ

Weryfikuj nadawcę wiadomości oraz podpisuj cyfrowo własne maile

Sprawdzaj czy otrzymane wiadomości są podpisane cyfrowo. Korzystaj z podpisu cyfrowego do podpisywania własnych maili.
W tym celu możesz wykorzystać technologię PGP lub S/MIME (opisaną w sekcji PGP oraz S/MIME w Poradniku technicznym). Aby podpisać wiadomość nadawca oblicza jej hash, który następnie szyfruje używając swój klucz prywatny. Odbiorca wiadomości może zweryfikować czy wiadomość nie została zmieniona w trakcie przesyłu rozszyfrowując hash za pomocą klucza publicznego nadawcy oraz własnoręcznie obliczonego hasha z otrzymanej wiadomości.

Do podpisywania i weryfikacji podpisów potrzebny jest zestaw kluczy prywatnego i publicznego. Większość nowoczesnych klientów pocztowych dostarcza opcję podpisywania wiadomości, potrzebne są wygenerowane klucze oraz odpowiednia konfiguracja (zależna od klienta pocztowego).

WYJAŚNIENIE

Podpis cyfrowy z użyciem zaufanego certyfikatu zapewnia:
Autentyczność – pewność co do nadawcy wiadomości.
Integralność – pewność, że treść wiadomości nie została zmieniona w trakcie przesyłu.
Niezaprzeczalność – utrudnia wyparcie się autorstwa przez nadawcę wiadomości.

ODNOŚNIKI:

Konfiguracja podpisywania wiadomości w Mozilli Thunderbird
Konfiguracja podpisywania wiadomości w Microsoft Outlook
Konfiguracja podpisywania wiadomości w Outlook Web App

24

OCHRONA POCZTY ELEKTRONICZNEJ

Weryfikuj czy wysyłając wiadomość do wielu osób nie udostępniasz adresów e-mail odbiorców

Wysyłając wiadomość do wielu osób za każdym razem weryfikuj czy poprawnie adresujesz wiadomość i czy nie udostępniasz adresów e-mailowych odbiorców wszystkim pozostałym.

WYJAŚNIENIE

Błędy w adresowaniu mogą prowadzić do udostępnienia całej twojej listy adresów każdemu z odbiorców wiadomości. Efektem mogą być poważne konsekwencje, zarówno prawne jak i związane z potencjalną utratą klientów i ich zaufania.
W celu uniknięcia wycieków danych należy zrozumieć trzy pola adresowe używane w wiadomościach e-mail:

- TO (w wersji polskiej: “Do”) – umieszczone w tym polu adresy będą widoczne dla wszystkich odbiorców wiadomości.
- CC (w wersji polskiej: “Do wiadomości”) – umieszczone w tym polu adresy będą widoczne dla wszystkich odbiorców wiadomości. Zazwyczaj tego pola używa się jeśli ktoś nie jest bezpośrednim adresatem naszej wiadomości, natomiast chcemy aby został o tej wiadomości poinformowany.
- BCC (w wersji polskiej: “Ukryte do wiadomości”) – umieszczone w tym polu adresy również otrzymają wiadomość, ale nie będą widoczne dla nikogo.

W przypadku wysyłania wiadomości do wielu osób musisz zastanowić się czy wszyscy adresaci Twojej wiadomości powinni wiedzieć o sobie nawzajem. Jeśli nie to zamiast umieszczać adresy e-mail w polu TO wpisz je do BCC. Dzięki temu każdy z odbiorców dostanie wiadomość adresowaną tylko i wyłącznie do niego oraz nie będzie widział pozostałych odbiorców.

Przykładem szkodliwych efektów związanych z błędnym adresowaniem wiadomości może być udostępnienie całej swojej listy klientów, co może zostać wykorzystane przez konkurencję.

25

OCHRONA POCZTY ELEKTRONICZNEJ

Upewnij się, że twój serwer nie jest open-relay

Upewnij się, iż Twój serwer pocztowy pozwala na wysyłkę poczty tylko Twoim użytkownikom. Wymagaj uwierzytelniania użytkownika do wysyłki poczty oraz ogranicz zakres adresów, z których może być wysyłana poczta tylko do adresów wewnętrznych.

WYJAŚNIENIE

Open-relay to określenie na serwer pocztowy, który pozwala na wysyłanie przez niego poczty, która nie pochodzi od jego użytkowników. Innymi słowy, każdy może wysłać z jego pomocą wiadomość podszywając się pod inną osobę (w szczególności pod jakiegoś prawdziwego użytkownika, którego on obsługuje).
To takie serwery są głównym źródłem SPAM-u i sfałszowanych wiadomości. Jednym z wielu efektów takiej konfiguracji, będzie dodanie serwera do czarnych list, co będzie skutkować ignorowaniem poczty z niego wychodzącej przez odbiorców.

Podstawowym sposobem ochrony jest wprowadzenie wymaganego uwierzytelniania do wysyłki poczty. Podobnie, można ograniczyć listę adresów, z których dozwolona jest wysyłka, tylko do adresów wewnętrznych w sieci przedsiębiorstwa.

Weryfikuj podejrzane wiadomości nawet jeśli pochodzą od znanych adresów

Po otrzymaniu niespodziewanej wiadomości, w której jesteś proszony o podjęcie jakichś nieoczekiwanych działań, najpierw zweryfikuj autentyczność polecenia z nadawcą.

WYJAŚNIENIE

Wiadomość może być sfałszowana, wynikać z włamania na czyjeś konto lub utraty urządzenia. Przykładem nieoczekiwanej wiadomości może być prośba przełożonego o nagły przelew środków firmy na inne konto, wysłana przez złodzieja ze skradzionego urządzenia.

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.