DOBRE PRAKTYKI

DLA ADMINISTRATORÓW IT

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

SPIS TREŚCI

1. ZARZĄDZANIE ZASOBAMI

1.1 Wprowadź mechanizmy zarządzania zasobami..... **03**

2. STACJE ROBOCZE I LAPTOPY

2.1 Ogranicz użytkownikom dostęp do kont administracyjnych mechanizmy zarządzania zasobami..... **04**

2.2 Zablokuj użytkownikom możliwość instalowania oprogramowania..... **04**

2.3 Wyłącz automatyczne uruchamianie i odtwarzanie nośników zewnętrznych..... **05**

2.4 Dbaj o aktualizację firmware, systemów operacyjnych oraz oprogramowania..... **06**

2.5 Zadbaj o ochronę antywirusową i antymalware'ową..... **07**

2.6 Wdróż odpowiedni monitoring logów i zdarzeń..... **08**

3. URZĄDZENIA MOBILNE I PRZENOŚNE

3.1 Skonfiguruj szyfrowanie dysku dla każdego urządzenia i nośnika danych objętego polityką szyfrowania..... **09**

3.2 Udostępnij VPN do pracy zdalnej..... **10**

3.3 Kasuj dane z każdego zgubionego lub skradzionego urządzenia..... **11**

4. WARTOŚCIOWE DANE

4.1 Wdróż automatyczne mechanizmy tworzenia kopii zapasowych..... **12**

4.2 Chroń dostępność, poufność i integralność kopii zapasowych..... **13**

4.3 Przed wyrzuceniem nośnika danych wyczyść go z wszelkich danych..... **14**

5. USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

4.1 Zapewnij szyfrowanie dla wszystkich usług sieciowych..... **15**

4.2 Skonfiguruj szyfrowanie w odpowiedni sposób..... **16**

4.3 Ogranicz dostęp do usług spoza sieci wewnętrznej..... **17**

4.4 Wdróż odpowiedni monitoring sieci..... **18**

4.5 Rozważ filtrowanie DNS..... **19**

4.6 Rozdziel różne domeny bezpieczeństwa..... **19**

6. USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

6.1 Rozważ wprowadzenie SSO (single sign-on)..... **20**

6.2 Wprowadź uwierzytelnianie dwuskładnikowe (2FA)..... **21**

7. POCZTA ELEKTRONICZNA

7.1 Zweryfikuj kto i kiedy ma dostęp do Twojej poczty w zewnętrznej usłudze hostingowej..... **22**

7.2 Zweryfikuj do jakiego maksymalnego czasu przestoju zobowiązuje się dostawca zewnętrznej usługi..... **22**

7.3 Zadbaj o regularne tworzenie kopii zapasowych..... **23**

7.4 Zapewnij szyfrowany transport wiadomości..... **23**

7.5 Zaimplementuj rozwiązania utrudniające podszywanie się pod twój serwer e-mail..... **24**

7.6 Zaimplementuj rozwiązania weryfikujące nadawcę wiadomości..... **24**

7.7 Upewnij się, że twój serwer nie jest open-relay..... **25**

03

ZARZĄDZANIE ZASOBAMI

Wprowadź mechanizmy zarządzania zasobami

Z punktu widzenia administratora istotne jest ciągłe zbieranie informacji o sprzęcie, oprogramowaniu i danych oraz ich właścicielach.

WYJAŚNIENIE

Samo zarządzanie zasobami jest czynnością raczej związaną z poziomem managerskim przedsiębiorstwa, jednakże powinno być wykonywane również (albo przynajmniej) na poziomie technicznym. Zasoby sprzętowe, programowe i dane powinny być zinwentaryzowane oraz mieć przypisanych właścicieli.

Oprogramowanie ułatwiające zarządzanie zasobami dostarczane jest przez wielu producentów. W odnośnikach pojawiają się tylko przykładowe darmowe i open-source'owe rozwiązania.

ODNOŚNIKI:

Snite-IT
GLPI
Ralph

04

STACJE ROBOCZE I LAPTOPY

Ogranicz użytkownikom dostęp do kont administracyjnych mechanizmy zarządzania zasobami

Konto z uprawnieniami administracyjnymi (np. Administrator na Windowsie albo root na Linuksie) powinny nie być domyślnie używane przez użytkowników.

WYJAŚNIENIE

W większości wypadków użytkownik prawdopodobnie w ogóle nie powinien mieć dostępu do konta administratora lokalnego, a w dopuszczalnych wyjątkach powinien korzystać z mechanizmu elewacji uprawnień wymagającego podania hasła. Z jednej strony ograniczy to możliwość wykonania błędnych akcji przez użytkownika, a z drugiej strony ograniczy ewentualne uprawnienia złośliwego oprogramowania, które może dostać się do systemu.

Zablokuj użytkownikom możliwość instalowania oprogramowania

Podobnie, jak uprawnienia administracyjne, możliwość instalowania nowego oprogramowania przez użytkowników powinna być wyjątkiem a nie regułą.

WYJAŚNIENIE

Administrator powinien kontrolować, co jest zainstalowane na komputerach pracowników. Ogranicza to ryzyko instalacji złośliwego oprogramowania oraz uszkodzenia systemu. Oczywiście od tej reguły istnieją wyjątki – np. programiści mogą mieć faktyczną potrzebę samodzielnej instalacji nowych aplikacji.

05

STACJE ROBOCZE I LAPTOPY

Wyłącz automatyczne uruchamianie i odtwarzanie nośników zewnętrznych

Stacje robocze powinny mieć wyłączoną funkcję automatycznego odtwarzania nośników zewnętrznych.

WYJAŚNIENIE

Funkcja automatycznego uruchamiania i odtwarzania nośników zewnętrznych może przyczynić się do zainstalowania złośliwego oprogramowania w momencie podłączenia zewnętrznego nośnika takiego jak pendrive.

ODNOŚNIK:

Instrukcja wyłączenia dla systemu Windows 10

06

STACJE ROBOCZE I LAPTOPY

Dbaj o aktualizację firmware, systemów operacyjnych oraz oprogramowania

Używany sprzęt powinien z reguły mieć zainstalowany najnowszy firmware a oprogramowanie powinno być zawsze aktualne.

WYJAŚNIENIE

Dbanie o aktualizacje – zwłaszcza systemów podłączonych do sieci Internet – to pewne minimum dbania o bezpieczeństwo infrastruktury. Zapewnia nam to najczęściej ochronę przed większością powszechnie znanych (a więc często najłatwiejszych do wykorzystania) podatności i błędów.

Nie oznacza to, że aktualizacje powinny być instalowane bezmyślnie i automatycznie. Warto zapoznać się ze zmianami wprowadzanymi w ramach nowej wersji i podjąć indywidualną decyzję, czy aktualizacja jest potrzebna i nie spowoduje problemów dla użytkowników.

Warto też mieć stały plan instalowania poprawek – np. instalować je wieczorem w jeden określony dzień tygodnia. Dobrą praktyką jest też wcześniejsze przetestowanie aktualizacji w testowym środowisku.

07

STACJE ROBOCZE I LAPTOPY

Zadbaj o ochronę antywirusową i antymalware'ową

Stacje robocze powinny być chronione przeciwko złośliwemu oprogramowaniu.

WYJAŚNIENIE

W wielu przypadkach oprogramowanie antywirusowe i antymalware'owe może powstrzymać infekcję stacji roboczej. Wybór konkretnego rozwiązania zależy od przypadku i dostępnych funduszy. Często wystarczającym rozwiązaniem będzie oprogramowanie ochronne wbudowane w system operacyjny lub w przeglądarkę internetową. W niektórych sytuacjach może potrzebny być zakup dodatkowego oprogramowania instalowanego na stacjach roboczych.

W niektórych konfiguracjach ochrona może być zrealizowana poza systemem użytkownika – będzie tak w przypadku wdrożenia wirtualizacji komputerów pracowniczych (technologie typu VDI) albo w przypadku, gdy zagrożeniem mogą być tylko pliki z zewnątrz (wtedy wystarczy np. system antymalware na wejściu do sieci firmy).

08

STACJE ROBOCZE I LAPTOPY

Wdróż odpowiedni monitoring logów i zdarzeń

Stacje robocze powinny być monitorowane – logi systemowe powinny być regularnie przeglądane a co poważniejsze zdarzenia powinny wzbudzać alarm, który może być łatwo zauważony przez administratora. Idealną sytuacją jest, gdy logi gromadzone są w jednym miejscu – w aplikacji ułatwiającej ich analizę i korelację zdarzeń (SIEM).

WYJAŚNIENIE

Włamania do infrastruktury potrafią być niewykryte miesiącami. Dyski twarde potrafią niepostrzeżenie przestać działać. Administrator nie zauważa tego, gdyż nie monitoruje w żaden sposób tego, co dzieje się na stacjach roboczych.

Monitoring infrastruktury to krytyczny element bezpieczeństwa. W przypadku stacji roboczych najwięcej informacji dostarczają logi. Powinny one być gromadzone w jednym, centralnym punkcie, który pozwala na korelację i analizę zdarzeń w kontekście innych zdarzeń w sieci. Takim punktem będzie najczęściej SIEM (Security information and event management).

Odnośniki kierują do darmowych, open-sourcowych rozwiązań, ale istnieje też wiele komercyjnych SIEM-ów.

ODNOŚNIKI:

Apache Metron
OSSEC
OSSIM

09 URZĄDZENIA MOBILNE I PRZENOŚNE

Skonfiguruj szyfrowanie dysku dla każdego urządzenia i nośnika danych objętego polityką szyfrowania

Włącz szyfrowanie dysków na wszystkich urządzeniach, dla których polityka tego wymaga.

WYJAŚNIENIE

Szyfrowanie dysków, pendrive'ów i innych urządzeń wewnętrznych i zewnętrznych, na których mogą być przechowywane dane jest aktualnie bardzo proste – wymaga tylko podjęcia kilku decyzji.

Dla dysków wewnętrznych komputerów osobistych i urządzeń mobilnych typu smartfon często najlepszym rozwiązaniem będzie włączenie szyfrowania udostępnionego przez twórców systemu operacyjnego i wbudowanego w system:

- Bitlocker dla systemów Windows,
- LUKS dla systemów Linux,
- FileVault dla systemów macOS.

Konfiguracja smartfonów z systemem Android zależy znacznie od ich producenta, ale w większości wypadku szyfrowanie danych (w starszych wersjach jest to szyfrowanie całego dysku, a w nowszych szyfrowanie plików) wymaga ustawienia kodu blokady.

W przypadku nośników zewnętrznych decyzja zależeć będzie od stopnia kompatybilności z różnymi systemami, w których nośnik będzie używany. Jeżeli będzie to jednolite środowisko, to możemy wykorzystać mechanizmy systemowe, podobnie jak w przypadku dysków wewnętrznych. Dla bardziej zróżnicowanych wdrożeń warto wybrać rozwiązanie działające pod różnymi systemami. Dobrym wyborem będzie z reguły VeraCrypt.

Należy też podjąć decyzję, kto i kiedy może odszyfrować dane – czy tylko ich użytkownik znający hasło, czy też administrator, czy też może dane powinny być odszyfrowywane automatycznie przy starcie urządzenia (póki dysk znajduje się we właściwym urządzeniu).

ODNOŚNIKI:

Jak włączyć szyfrowanie danych w iOS
VeraCrypt

10

URZĄDZENIA MOBILNE I PRZENOŚNE

Udostępnij VPN do pracy zdalnej

Jeżeli Twoja firma dopuszcza pracę zdalną lub wykonywanie pracy spoza biura, zadbaj o to, aby pracownicy łączyli się z biurem tylko za pomocą wirtualnej sieci prywatnej (VPN).

WYJAŚNIENIE

Najprościej rzecz ujmując, VPN rozszerza sieć prywatną firmy na zdalne komputery. Może być wykorzystywany zarówno do zabezpieczania protokołów dostępu zdalnego (jak RDP i VNC) ale też do zabezpieczania dostępu do zdalnych plików (CIFS, NFS). Przy dobrze skonfigurowanym VPN-ie pracownik nie będzie widział różnicy w pracy w biurze a np. w domu. Dodatkowo, jego połączenia i używane pliki będą chronione na takim samym (lub podobnym) poziomie jak gdyby był w pracy.

Konkretne rozwiązania zależeć będą od budżetu i środowiska sprzętowo-programowego w firmie. Praktycznie każdy dostawca sprzętu sieciowego będzie miał też wersje sprzętu pozwalające na konfigurację dostępowego VPN. Budżetowym, ale całkiem dobrym rozwiązaniem będzie też wykorzystanie OpenVPN.

ODNOŚNIK:

OpenVPN

11

URZĄDZENIA MOBILNE I PRZENOŚNE

Kasuj dane z każdego zgubionego lub skradzionego urządzenia

W przypadku zgubienia lub kradzieży urządzenia wykonaj zdalne usunięcie danych.

WYJAŚNIENIE

Urządzenia mobilne – zwłaszcza smartfony – mają często wbudowaną możliwość zdalnego skasowania danych na wypadek utraty sprzętu. Oczywiście działa to tylko w przypadku, gdy urządzenie jest włączone. Warto z tej funkcji skorzystać zawsze, gdy podejrzewamy, że na urządzeniu mogły znajdować się dane firmowe albo zapamiętane dane do kont mających związek z naszą firmą.

Należy tylko pamiętać, że funkcje te wymagają najczęściej wcześniejszej (czyli przed utratą urządzenia) konfiguracji.

ODNOŚNIKI:

Znajdowanie lub blokowanie utraconego urządzenia z Androidem bądź kasowanie z niego danych
iCloud: Erase your device with Find My iPhone

12

WARTOŚCIOWE DANE

Wdróż automatyczne mechanizmy tworzenia kopii zapasowych

Upewnij się, że automatycznie wykonywane jest stworzenie kopii zapasowych (wg odpowiedniej ustalonej polityki) oraz przenoszenie tych kopii w odpowiednie miejsce.

WYJAŚNIENIE

Regularne, zaplanowane kopie zapasowe powinny praktycznie zawsze być wykonywane automatycznie. Wykonywanie ich ręcznie spowoduje prawie na pewno wystąpienie sytuacji, że ktoś zapomni je zrobić albo będzie na urlopie, albo nie będzie miał czasu.

Nie ma znaczenia, jakie narzędzie zostanie wykorzystane do ich tworzenia – praktycznie każde z nich będzie posiadało możliwość automatycznego uruchamiania w zadanych terminach.

Upewnij się też, że cały proces jest zautomatyzowany – zarówno wykonanie kopii lokalnej jaki jej skopiowanie na zdalną lokalizację.

Usuwanie starych kopii również powinno być zautomatyzowane – lepiej, aby nie zabrakło miejsca na nowe kopie.

13

WARTOŚCIOWE DANE

Chroń dostępność, poufność i integralność kopii zapasowych

Dbaj o kopie zapasowe w podobnym stopniu jak o aktywnie używane dane, w tym między innymi:

- regularnie testuj integralność kopii i regularnie testuj odzyskiwanie z nich danych.
- zadbaj o ochronę przed nieupoważnionym dostępem do kopii – kopie przechowywane np. w usługach zewnętrznych powinny być szyfrowane, a na lokalnych zewnętrznych nośnikach – zamknięte w bezpiecznym miejscu.

WYJAŚNIENIE

Niewiele rzeczy jest gorszych niż uświadomienie sobie w momencie dużej awarii, że kopie zapasowe, które myśleliśmy, że mamy, okazują się nieużywalne. Podstawą weryfikacji, że nasze kopie zapasowe działają są regularne próby odzyskania z nich danych.

Problemem innego rodzaju jest przechowywanie kopii w sposób mniej bezpieczny niż oryginalnych danych – np. na serwerze, do którego dostęp ma więcej osób niż do pierwotnego źródła albo na płytach CD leżących w niezamykanej szufladzie. O poufność kopii zapasowych powinniśmy dbać poprzez odpowiedni wybór miejsca ich przechowywania, poprzez odpowiednią kontrolę dostępu lub też np. przez ich szyfrowanie.

Oczywiście nie należy zapominać, że zawsze powinniśmy mieć do kopii dostęp gdy są potrzebne – dobrze jest zadbać o to, aby nie było sytuacji, gdy jedynym pracownikiem mającym dostęp do kopii jest administrator znajdujący się akurat na urlopie.

14

WARTOŚCIOWE DANE

Przed wyrzuceniem nośnika danych wyczyść go z wszelkich danych

Przed wyrzuceniem jakiegokolwiek nośnika danych uprzednio wymaż z niego wszystkie dane. W przypadku dysku HDD wykonaj przynajmniej jedno nadpisanie całego dysku. Dla nośników SSD wykonaj czyszczenie dysku za pomocą narzędzi dostarczanych przez producenta.

WYJAŚNIENIE

Kasowanie plików to skomplikowana sprawa. Samo skasowanie pliku oznacza zazwyczaj jedynie oznaczenie danego pliku jako usuniętego, nie kasuje jednak jego zawartości z dysku. Miejsce zajmowane przez zawartość pliku dopiero po jakimś czasie zostanie ponownie użyte. Sprawa komplikuje się jeszcze bardziej z dyskami SSD, które starają się równoważyć zużycie komórek pamięci, brak jest więc kontroli nad miejscem zapisu danych na dysku.

W przypadku dysków HDD nadpisanie danych za pomocą zer, jedynek lub losowych wartości znacząco utrudni proces odzyskiwania danych. Jednokrotne wykonanie procesu nadpisywania utrudnia odzyskanie danych, ale istnieją metody, które nawet wtedy częściowo odzyskać dane. Aby zmniejszyć prawdopodobieństwo zaistnienia takiej sytuacji warto kilkukrotnie powtórzyć proces nadpisywania.

Do usunięcia danych z dysku SSD najlepiej wykorzystać mechanizmy dostarczone przez producenta dysku. Mechanizm taki będzie często nazywał się ”Secure Erase”. Ostatecznie dysk można także zniszczyć fizycznie (ale w przeciwieństwie do dysków HDD nie zadziała tutaj demagnetyzacja).

Dosyć pewną metodą jest też szyfrowanie danych na dysku od pierwszego jego użycia.

15

USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

Zapewnij szyfrowanie dla wszystkich usług sieciowych

Czy to usługi dla pracowników (VPN, poczta elektroniczna), czy też dla klientów – wszystkie powinny korzystać z szyfrowanych połączeń odpowiednich dla rodzaju usługi (np. HTTPS, SMTP z użyciem TLS, itd.).

WYJAŚNIENIE

Aktualnie nie ma już praktycznie argumentów przeciwko korzystaniu z szyfrowania w każdej usłudze sieciowej. Nawet w większości wypadków certyfikaty TLS są darmowe, gdyż można je pozyskać z Let's Encrypt – projektu stworzonego m.in. przez Mozillę, który dostarcza darmowych certyfikatów i oprogramowania do automatycznego ich odnawiania.

Ponadto, przeglądarki internetowe traktują szyfrowanie jako normę i aktywnie komunikują użytkownikowi, że strona nie korzystająca z HTTPS jest niezaufana.

ODNOŚNIKI:

Let's Encrypt

16

USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

Skonfiguruj szyfrowanie w odpowiedni sposób

Usługi wykorzystujące szyfrowanie powinny być na bieżąco dostosowywane do nowych standardów konfiguracji.

WYJAŚNIENIE

Standardy doboru funkcji kryptograficznych często się zmieniają. Trudno jest śledzić te zmiany i nadążać za nimi, często więc korzysta się z konfiguracji domyślnej lub przez lata używa takiej, która została kiedyś ustalona. Jednakże funkcje i protokoły kryptograficzne się starzeją i mają swoje błędy. Stąd też należy aktualizować odpowiednie konfiguracje raz na jakiś czas (np. raz na rok).

Pomagają w tym co najmniej dwa serwisy: Qualys SSL Server Test i Mozilla SSL Configuration Generator – pierwszy testuje naszą aktualną konfigurację, a drugi dostarcza gotowe dyrektywy do konfiguracji najpopularniejszych serwerów.

ODNOŚNIKI:

Qualys SSL Server Test
Mozilla SSL Configuration Generator

17

USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

Ogranicz dostęp do usług spoza sieci wewnętrznej

Innymi słowy: odpowiednio skonfiguruj firewall na wejściu do sieci firmowej.

WYJAŚNIENIE

Podstawową zasadą konfiguracji firewalla jest blokowanie całego ruchu a dopiero później dodawanie wyjątków dla potrzebnych usług. Firewall powinien być wdrożony na każdym możliwym wejściu do sieci firmowej a także pomiędzy różnymi domenami bezpieczeństwa wewnątrz sieci. Z punktu widzenia bezpieczeństwa nie ma większego znaczenia, czy będzie to dedykowane rozwiązanie sprzętowe czy np. dedykowany węzeł Linuksowy oparty o iptables (aczkolwiek, z punktu widzenia wydajności już może mieć to znaczenie).

ODNOŚNIK:

Guidelines on Firewalls and Firewall Policy

18

USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

Wdróż odpowiedni monitoring sieci

Sieć powinna być monitorowana: zarówno na wejściu do sieci firmowej jak i wewnątrz.

WYJAŚNIENIE

Monitoring sieci to, obok monitoringu logów na hostach, jedna z podstawowych metod zapewniania bezpieczeństwa.

W tym punkcie chodzi nam głównie o obserwację pakietów i ruchu sieciowego. Wykorzystuje się do tego systemy IDS (Intrusion detection system), które w najczęstszej konfiguracji, otrzymują kopię całego ruchu i analizują go. Rezultaty analizy warto wysyłać do systemu typu SIEM (Security information and event management), który pozwoli na korelację różnych innych zdarzeń z ruchem sieciowym.

Odnośniki kierują do darmowych, open-sourcowych rozwiązań, ale istnieje też wiele komercyjnych IDS-ów i SIEM-ów.

ODNOŚNIKI:

Apache Metron
Zeek
Snort
Suricata

19

USŁUGI INTERNETOWE I INFRASTRUKTURA SIECIOWA

Rozważ filtrowanie DNS

Jeżeli brak ku temu przeciwwskazań, warto scentralizować dostęp do DNS w firmie w jednym serwerze (rekursywny DNS) a następnie wprowadzić filtrowanie adresów niebezpiecznych i niepożądanych.

WYJAŚNIENIE

Filtrowanie DNS pozwala ograniczyć prawdopodobieństwo infekcji złośliwym oprogramowaniem – może zablokować działanie instalatora (który np. nie będzie mógł pobrać dalszej części wirusa) albo uniemożliwić komunikację już zainfekowanego komputera z osobą kontrolującą malware.

Dodatkowe zalety, to możliwość blokowania potencjalnych źródeł infekcji – np. reklam lub stron phisingowych.

ODNOŚNIK:

Response Policy Zones

Rozdziel różne domeny bezpieczeństwa

Rozdziel hosty i usługi o różnym poziomie bezpieczeństwa do osobnych sieci wirtualnych lub fizycznych.

WYJAŚNIENIE

Usługi oraz hosty mające różne poziomy bezpieczeństwa, różne pochodzenie, różnych właścicieli powinny być separowane od siebie. Najprostszy przykład to separacja sieci WiFi, do której pracownicy mogą łączyć się z prywatnych urządzeń albo dla gości od właściwej sieci firmowej, w której znajdują się hosty z usługami wewnętrznymi. Taka separacja redukuje prawdopodobieństwo, że zarażone lub złośliwe hosty, uzyskają kontrolę nad urządzeniami bardziej zaufanymi.

20

IDENTYFIKACJA I UWIERZYTELNIANIE

Rozważ wprowadzenie SSO (single sign-on)

W systemach, gdzie użytkownicy korzystają z więcej niż jednego zasobu (np. oprócz swojej stacji roboczej mają dostęp do zasobów sieciowych) rozważ wprowadzenie scentralizowanego, jednokrotnego logowania (single sign-on, SSO).

WYJAŚNIENIE

Single sign-on ma co najmniej dwie zalety:

1. Użytkownik rzadziej musi wpisywać swoje hasło i nie musi pamiętać wielu haseł.
2. Aplikacje nie muszą zapisywać hasła użytkownika – redukuje to ilość miejsc, gdzie hasło zapisane jest w jakiejkolwiek formie.

W praktyce najczęściej wykorzystywane są wdrożenia bazujące na Kerberosie i LDAP-ie. Są to, na przykład:

1. Microsoft Active Directory,
2. RedHat Identity Manager,
3. Oracle Identity Management.

ODNOŚNIKI:

Microsoft Active Directory
RedHat Identity Management
Oracle Identity Management

21

IDENTYFIKACJA I UWIERZYTELNIANIE

Wprowadź uwierzytelnianie dwuskładnikowe (2FA)

Rozważ wprowadzenie uwierzytelniania dwuskładnikowego – zwłaszcza w usługach zdalnych.

WYJAŚNIENIE

Uwierzytelnianie dwuskładnikowe znacząco podnosi bezpieczeństwo użytkowników i zmniejsza ryzyko phishingu. Aczkolwiek często spotykane głównie przy usługach webowych, to jest również łatwe do skonfigurowania w przypadku dostępu zdalnego do stacji roboczych (np. RDP, SSH) lub plików.

Pamiętaj jedynie, że gdy wdrażasz też SSO, to uwierzytelnianie dwuskładnikowe ma sens tylko, jeżeli wdrożone dla wszystkich usług lub przynajmniej wszystkich usług z jednej chronionej domeny (np. wszystkich usług zdalnych).

ODNOŚNIKI:

Konfiguracja YubiKey jako drugiego składnika w systemie Windows

22

POCZTA ELEKTRONICZNA

Zweryfikuj kto i kiedy ma dostęp do Twojej poczty w zewnętrznej usłudze hostingowej

Jeśli korzystasz z zewnętrznej usługi mailingowej lub hostingu zwróć uwagę na to kto i w jakich sytuacjach może uzyskać dostęp do Twoich danych. Poufne dane najlepiej przesyłać w postaci zaszyfrowanej.

WYJAŚNIENIE

W wielu serwisach z darmową pocztą przychodzące maile są skanowane przez automaty firmy dostarczającej usługę. Istotne jest zorientowanie się jakie są warunki udostępnienia przez danego operatora Twoich danych podmiotom trzecim.

Zweryfikuj do jakiego maksymalnego czasu przestoju zobowiązuje się dostawca zewnętrznej usługi

Jeśli korzystasz z zewnętrznej usługi mailingowej lub hostingu zwróć uwagę na maksymalny downtime (czas przestoju) lub zapewniany uptime (czas działania).

WYJAŚNIENIE

Oba te pojęcia określają tzw. dostępność usługi, czyli czas bezawaryjnego działania usługi w stosunku do całości czasu, w którym usługa ta powinna być klientom świadczona.
Downtime (czas przestoju) to maksymalny czas, w którym dana usługa może być niedostępna (ze względu na awarie, itd) bez ponoszenia przez dostawcę kary.
Uptime (czas działania) to z kolei wartość mówiąca przez jaki najmniejszy procent czasu usługa będzie dostępna. Uptime o wartości 99.9% oznacza, że dostawca deklaruje dostępność usługi przez 99.9% czasu – czyli np. w trakcie jednego roku usługa może być niedostępna maksymalnie przez 8 godzin i 20 minut.

ODNOŚNIK:

Klasy dostępności

POCZTA ELEKTRONICZNA

Zadbaj o regularne tworzenie kopii zapasowych

Jak w przypadku wszystkich ważnych danych zadbaj o regularne tworzenie kopii zapasowych. W przypadku korzystania z zewnętrznych usług upewnij się, że dostawca dostarcza również usługę tworzenia kopii zapasowych.

Zapewnij szyfrowany transport wiadomości

Dla połączeń dostępowych (IMAP, POP3, SMTP dla użytkowników) wymuszaj użycie szyfrowania. Dla połączeń pomiędzy serwerami (SMTP) preferuj użycie szyfrowania.

WYJAŚNIENIE

Użytkownik końcowy komunikuje się ze swoim serwerem mailowym za pomocą protokołów IMAP i POP3 (odbieranie poczty) oraz SMTP (wysyłka poczty). Komunikacja ta powinna być szyfrowana za pomocą protokołu TLS.

Podobnie, komunikacja pomiędzy serwerami za pomocą protokołu SMTP powinna być szyfrowana. Jednakże nie wszystkie serwery wspierają taką komunikację. Dlatego zalecane jest wspieranie o ogłaszanie STARTLS w przypadku poczty przychodzącej oraz preferowanie szyfrowania dla poczty wychodzącej przy jednoczesnym dopuszczeniu komunikacji nieszyfrowanej.

Dla indywidualnych serwerów można również w wymusić komunikację szyfrowaną w politykach serwera SMTP.

POCZTA ELEKTRONICZNA

Zaimplementuj rozwiązania utrudniające podszywanie się pod twój serwer e-mail

Zaimplementuj SPF, DKIM i DMARC.

WYJAŚNIENIE

W swojej podstawowej formie protokoły wykorzystywane w poczcie elektronicznej nie zapewniają weryfikacji pochodzenia wiadomości. W szczególności, adres nadawcy może być sfałszowany. Rozwiązania typu SPF, DKIM i DMARC wdrożone po stronie właściciela serwera poczty umożliwiają serwerom odbiorców weryfikację, czy wiadomość, którą otrzymały faktycznie pochodzi z miejsca, które deklaruje.

Zaimplementuj rozwiązania weryfikujące nadawcę wiadomości

Zaimplementuj weryfikację poprawnego SPF, DKIM i DMARC oraz skonfiguruj filtry antyspamowe w serwerze poczty.

WYJAŚNIENIE

W swojej podstawowej formie protokoły wykorzystywane w poczcie elektronicznej nie zapewniają weryfikacji pochodzenia wiadomości. W szczególności, adres nadawcy może być sfałszowany. Jeżeli nadawca wiadomości wdrożył SPF, DKIM i DMARC, to odbiorca może zweryfikować, czy wiadomość faktycznie od niego pochodzi i na tej podstawie zdecydować, czy ją odrzucić czy też oznaczyć jako spam.

Filtry antyspamowe stanowią dodatkową ochronę i na podstawie wielu parametrów wiadomości są w stanie wyeliminować znaczną ilość niechcianej poczty, a w szczególności prostych ataków phishingowych i malware.

25

POCZTA ELEKTRONICZNA

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.

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.