Rekomendacje w zakresie zabezpieczania infrastruktury sieciowej

Spis treści

1. Wprowadzenie

W dzisiejszych czasach, gdy cyberzagrożenia są coraz bardziej powszechne i zaawansowane, niezwykle istotne jest zapewnienie najwyższego poziomu bezpieczeństwa sieciowego. Nasze zalecenia, opracowane na podstawie najlepszych praktyk w branży, mają na celu pomóc w ochronie firm przed potencjalnymi zagrożeniami.

Wydajna i funkcjonalna infrastruktura sieciowa stanowi fundament każdej nowoczesnej organizacji. Jest ona unikatową kompozycją **sprzętu** (np. serwerów komunikacyjnych, switchy, routerów), okablowania, a także **oprogramowania** (np. narzędzia do monitorowania i zarządzania) oraz **usług sieciowych** (protokoły sieciowe, takie jak TCP, UDP i adresowanie IP). Podstawową funkcją infrastruktury sieciowej jest zapewnienie łączności pomiędzy urządzeniami w firmie i poza nią. Zagwarantowanie bezpiecznej infrastruktury sieciowej jest obecnie niezbędnym warunkiem dla zapewnienia ciągłości działania przedsiębiorstw.

Niniejszy dokument prezentuje kluczowe zasady zabezpieczania środowiska sieciowego. Pozwolą one zrozumieć najważniejsze aspekty w obliczu występujących zagrożeń oraz wskażą najlepsze praktyki w budowaniu i utrzymaniu bezpiecznej, lepiej chronionej infrastruktury sieciowej. Dokument jest praktycznym przewodnikiem dla zarządzających, który ma budować świadomość w zakresie bezpieczeństwa IT, tak istotnego z punktu widzenia każdej firmy. Zachęcamy do zapoznania się z naszymi zaleceniami i wdrożenia ich w swoich organizacjach.

2. Jakie zagrożenia bezpieczeństwa wiążą się z urządzeniami infrastruktury sieciowej?

Urządzenia infrastruktury sieciowej, odpowiedzialne za przekazywanie ruchu, mogą być narażone na różnorodne zagrożenia bezpieczeństwa, w tym ataki z zewnątrz i ataki wewnątrz organizacji. Atakujący infrastrukturę sieciową, który uzyskał nieautoryzowany dostęp do routera, będącego punktem brzegowym organizacji, może monitorować, modyfikować i blokować ruch przychodzący i wychodzący. Podobnie, osoby obecne w wewnętrznej sieci organizacji, takie jak pracownicy lub osoby mające dostęp do tej sieci, mogą stanowić zagrożenie poprzez wykonywanie prób nieautoryzowanego dostępu do niedostatecznie zabezpieczonych urządzeń sieciowych. Takie działania mogą obejmować monitorowanie, skanowanie, modyfikowanie i blokowanie ruchu do i z kluczowych hostów w sieci, a także wykorzystywanie zaufanych relacji wewnętrznych do atakowania innych hostów w organizacji.

Wiele urządzeń sieciowych po ich zainstalowaniu nie jest utrzymywanych na tym samym poziomie bezpieczeństwa, co komputery i serwery ogólnego przeznaczenia. Do podatności mogą przyczyniać się także inne sytuacje lub czynniki, na przykład:

- Tylko niektóre urządzenia sieciowe, szczególnie małe routery biurowe i domowe, obsługują narzędzia antywirusowe, narzędzia do kontroli integralności oraz inne narzędzia zabezpieczające.

- Producenci dystrybuują urządzenia sieciowe z już uruchomionymi usługami, które mają ułatwić instalację, obsługę i konserwację. Takie usługi zazwyczaj są domyślnie włączone na urządzeniu i dostępne zaraz po podłączeniu urządzenia do źródła zasilania.
- Właściciele i administratorzy urządzeń sieciowych często pozostawiają domyślne ustawienia dostawcy, nie stosują dodatkowych zabezpieczeń oraz nie dokonują regularnych aktualizacji.

3. Jak można poprawić bezpieczeństwo urządzeń infrastruktury sieciowej?

Agencja ds. Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) zaleca użytkownikom i administratorom sieci wdrożenie następujących praktyk w celu zwiększenia bezpieczeństwa infrastruktury sieciowej:

- Segmentacja infrastruktury sieciowej i jej funkcji.
- Ograniczenie niepotrzebnej komunikacji pomiędzy hostami w sieci.
- Wzmacnianie zabezpieczeń urządzeń sieciowych.
- Zapewnienie bezpiecznego dostępu do urządzeń infrastruktury.
- Zarządzanie siecią poza pasmem (Out-of-Band).
- Weryfikacja integralności sprzętu i oprogramowania.

3.1. Segmentacja infrastruktury sieci i jej funkcji

Podczas projektowania zabezpieczeń należy uwzględnić ogólny układ infrastruktury, w tym segmentację sieci. Właściwa segmentacja sieci stanowi jeden z podstawowych mechanizmów bezpieczeństwa, który zapobiega rozprzestrzenianiu się zagrożeń oraz nieautoryzowanemu dostępowi do elementów sieciowych. W słabo podzielonej sieci jednostki nieuprawnione mogą łatwo uzyskać dostęp do krytycznych urządzeń w celu przejęcia nad nimi kontroli lub też pozyskać poufne dane lub własność intelektualną. Segregacja oddziela segmenty sieci na podstawie ich roli i funkcjonalności.

3.1.1. Fizyczne oddzielenie informacji wrażliwych

Tradycyjne urządzenia sieciowe, takie jak routery, mogą separować segmenty sieci lokalnej (LAN). Organizacje mogą wykorzystać routery do sieci, co umożliwia tworzenie granic między segmentami oraz zwiększanie liczby domen w celu skutecznej filtracji ruchu rozgłoszeniowego użytkowników.

Zalecenia

- Zaimplementuj zasady najmniejszych uprawnień i minimalnej wiedzy wymaganej podczas projektowania segmentów sieci.
- Oddziel poufne informacje oraz wymagania dotyczące bezpieczeństwa na osobne segmenty sieci.
- Stosuj zalecenia dotyczące zabezpieczeń i bezpieczne konfiguracje do wszystkich segmentów sieci oraz warstw sieciowych.

3.1.2. Wirtualna separacja poufnych informacji

Wraz z postępem technologicznym rozwijane są nowe strategie mające na celu poprawę wydajności technologii informatycznych oraz kontrolę bezpieczeństwa sieci. Jedną z takich strategii jest separacja wirtualna, która polega na logicznej izolacji sieci w obrębie tej samej sieci fizycznej. Segmentacja wirtualna opiera się na tych samych zasadach projektowania, co segmentacja fizyczna, jednakże nie wymaga dodatkowego sprzętu. Istniejące technologie mogą być wykorzystane do uniemożliwienia nieuprawnionym jednostkom włamania się do innych wewnętrznych segmentów sieci.

Zalecenia

- Użyj prywatnych wirtualnych sieci lokalnych (VLAN), aby odizolować użytkowników od pozostałych domen rozgłoszeniowych.
- Wykorzystaj technologię wirtualnego routingu (VRF), która umożliwia segmentację ruchu sieciowego w wielu tabelach routingu jednocześnie na jednym routerze.
- Używaj wirtualnych sieci prywatnych (VPN), aby bezpiecznie tunelować ruch przez sieci publiczne lub prywatne.

3.2. Ochrona punktu brzegowego sieci oraz segmentacja

Wdrożenie separacji sieci oraz ochrony punktu brzegowego zapewniają izolację od zagrożeń pochodzących z Internetu oraz podział sieci w organizacji na logiczne segmenty. Jednocześnie umożliwiają przypisanie odpowiednich dostępów oraz uprawnień do zasobów wewnętrznych i Internetu. Taki podział sieci w przypadku ataku ogranicza jego zakres do wydzielonych segmentów, co z kolei minimalizuje potencjalne szkody, ułatwia reakcję i odzyskiwanie sieci po incydencie.

Zalecenia

- Ogranicz komunikację poprzez wykorzystanie dostępnych metod filtrowania, takich jak reguły zapory sieciowej, aby zablokować zbędny przepływ pakietów z innych hostów w sieci. Reguły te, w zależności od urządzenia, mogą być tworzone w oparciu o adresy/nazwy hostów, użytkownika, program, typ programu lub adres protokołu internetowego (IP), co umożliwia ograniczenie dostępu do usług i systemów.
- Zaimplementuj listę kontroli dostępu do sieci VLAN (VACL), która stanowi filtr kontrolujący dostęp do i z sieci VLAN. Należy utworzyć filtry VACL, aby uniemożliwić pakietom przepływ do innych sieci VLAN.
- Logicznie segreguj sieć za pomocą separacji fizycznej lub wirtualnej, co umożliwia administratorom sieci odizolowanie krytycznych urządzeń od segmentów sieci.

3.3. Wzmacnianie zabezpieczeń urządzeń sieciowych (hardening)

Podstawowym sposobem zwiększenia bezpieczeństwa infrastruktury sieciowej jest zabezpieczenie urządzeń sieciowych za pomocą bezpiecznych konfiguracji. Administratorzy powinni wdrożyć następujące zalecenia w połączeniu z przepisami prawa, regulacjami, zasadami zabezpieczeń witryny, standardami i najlepszymi praktykami branżowymi.

Zalecenia

- Wyłącz nieszyfrowane protokoły zdalnego dostępu używane do zarządzania infrastrukturą sieciową (np. Telnet, protokół przesyłania plików [FTP]).
- Wyłącz niepotrzebne usługi (np. protokoły wykrywania [ICMP], protokół przesyłania hipertekstu [HTTP], prosty protokół zarządzania siecią [SNMP], protokół Bootstrap).
- Używaj protokołu SNMPv3 (lub późniejszej wersji), ale nie używaj domyślnych „community".
- Zabezpiecz dostęp do konsoli, pomocniczych i wirtualnych linii terminalowych.
- Wdrażaj solidne zasady dotyczące haseł i korzystaj z najsilniejszego dostępnego szyfrowania haseł.
- Chroń routery i przełączniki, kontrolując listy dostępu do zdalnej administracji oraz koniecznych serwisów.
- Ogranicz fizyczny dostęp do routerów i przełączników.
- Twórz kopie zapasowe konfiguracji i przechowuj je w trybie offline. Korzystaj z najnowszej wersji systemu operacyjnego urządzenia sieciowego i aktualizuj go o wszystkie poprawki.
- Okresowo testuj konfiguracje zabezpieczeń pod kątem wymagań dotyczących zabezpieczeń.
- Chroń pliki konfiguracyjne za pomocą szyfrowania lub kontroli dostępu podczas wysyłania, przechowywania i tworzenia kopii zapasowych plików.
- Regularnie weryfikuj możliwość występowania podatności i w razie konieczności aktualizuj oprogramowanie lub zastosuj „workaround" w celu ich usunięcia.

3.4. Bezpieczny dostęp do urządzeń infrastrukturalnych

Ograniczenie uprawnień administracyjnych dla urządzeń infrastruktury jest kluczowym elementem bezpieczeństwa, ponieważ nieuprawnieni użytkownicy sieci mogą wykorzystać nadane uprawnienia administracyjne, które są niewłaściwie autoryzowane, przyznawane powszechnie lub nie są dokładnie kontrolowane. Atakujący mogą posłużyć się przechwyconymi uprawnieniami do poruszania się po sieci, rozszerzania dostępu oraz przejmowania pełnej kontroli nad szkieletem infrastruktury. W związku z tym istotne jest ograniczenie nieautoryzowanego dostępu do infrastruktury poprzez wdrożenie odpowiednich zasad i procedur zapewniających bezpieczny dostęp.

Zalecenia

- **Zaimplementuj uwierzytelnianie wieloskładnikowe (MFA)**.
  Uwierzytelnianie to proces weryfikowania tożsamości użytkownika. Atakujący często wykorzystują słabe procesy uwierzytelniania. Uwierzytelnianie wieloskładnikowe wymaga użycia co najmniej dwóch składników do potwierdzenia tożsamości użytkownika. Składniki tożsamości mogą obejmować:
  - element, który użytkownik zna (np. hasło),
  - element, który użytkownik posiada (np. token),
  - cechę unikalną dla użytkownika (np. odcisk palca).
- **Stosuj zarządzanie uprzywilejowanym dostępem**.
  Jeżeli to możliwe, wykorzystaj serwer zapewniający usługi uwierzytelniania, autoryzacji i ewidencjonowania aktywności (AAA) do przechowywania danych dotyczących dostępu do zarządzania urządzeniami sieciowymi. Serwer AAA umożliwia administratorom sieci przypisanie użytkownikom różnych poziomów uprawnień zgodnie z zasadą najmniejszych uprawnień. W przypadku próby wykonania nieautoryzowanego polecenia przez użytkownika, zostanie ono odrzucone. Jeśli to możliwe, zaimplementuj serwer

uwierzytelniania wykorzystujący tokeny wraz z serwerem AAA. Użycie uwierzytelniania wieloskładnikowego utrudnia atakującym kradzież i wykorzystanie poświadczeń w celu uzyskania dostępu do urządzeń sieciowych.

- **Zarządzaj poświadczeniami administracyjnymi.**
  W przypadku braku możliwości wdrożenia najlepszych praktyk uwierzytelniania wieloskładnikowego, należy podjąć następujące działania:
  - Zmień domyślne hasła.
  - Upewnij się, że hasła mają co najmniej osiem znaków i zezwalaj na hasła o długości do 64 znaków (lub dłuższe), zgodnie z wytycznymi dotyczącymi tożsamości cyfrowej SP 800-63C National Institute of Standards and Technology oraz kanadyjskimi wytycznymi dotyczącymi uwierzytelniania użytkowników dla systemów informatycznych ITSP.30.031 V3.
  - Przeprowadzaj kontrole haseł pod kątem list odrzuconych, zawierających niedopuszczalne wartości, takie jak powszechnie używane, przewidywalne lub naruszone hasła.
  - Upewnij się, że wszystkie przechowywane hasła są odpowiednio zabezpieczone za pomocą silnych mechanizmów szyfrowania (i mają zastosowane mechanizmy zwiększające losowość, ang. salt).
  - Przechowuj hasła przeznaczone do awaryjnego dostępu w bezpiecznej lokalizacji poza siecią, np. w sejfie.

3.5. Zarządzanie poza pasmem OoB

Zarządzanie OoB (Out-of-Band) polega na wykorzystaniu alternatywnych „ścieżek komunikacyjnych" do zdalnego zarządzania urządzeniami infrastruktury sieciowej. Te dedykowane „ścieżki komunikacyjne" mogą mieć różną konfigurację, począwszy od wirtualnego tunelowania, aż po fizyczną separację. Korzystanie z dostępu OoB do zarządzania infrastrukturą sieciową wzmacnia bezpieczeństwo poprzez ograniczenie dostępu oraz oddzielenie ruchu użytkowników od ruchu związanego z zarządzaniem siecią. Zarządzanie OoB umożliwia także monitorowanie bezpieczeństwa i może ułatwiać prace utrzymaniowe.

Zarządzanie OoB może być realizowane fizycznie, wirtualnie lub w hybrydowy sposób łączący obie te metody. Chociaż budowa dodatkowej fizycznej infrastruktury sieciowej może być kosztowna we wdrożeniu i utrzymaniu, jest to najbezpieczniejsza opcja z punktu widzenia menedżerów sieci. Wirtualna implementacja jest z kolei mniej kosztowna, ale nadal wymaga znacznych zmian w konfiguracji i administracji. W niektórych sytuacjach, takich jak dostęp do zdalnych lokalizacji, wirtualne tunele szyfrowane mogą być jedyną realną opcją.

Zalecenia

- Rozdziel standardowy ruch sieciowy od ruchu związanego z zarządzaniem.
- Upewnij się, że ruch związany z zarządzaniem na urządzeniach pochodzi tylko z usługi OoB.
- Zastosuj szyfrowanie do wszystkich kanałów zarządzania.
- Szyfruj cały zdalny dostęp do urządzeń infrastrukturalnych takich, jak serwery terminali.
- Zarządzaj wszystkimi funkcjami administracyjnymi z dedykowanego, w pełni zabezpieczonego hosta za pośrednictwem bezpiecznego kanału, najlepiej w OoB.
- Wzmocnij urządzenia do zarządzania siecią, testując poprawki, wyłączając niepotrzebne usługi na routerach i przełącznikach oraz egzekwując silne zasady haseł. Monitoruj sieć i przeglądaj dzienniki. Zaimplementuj kontrolę dostępu, która zezwala tylko na wymagane usługi administracyjne lub usługi zarządzania (np. SNMP, Network Time Protocol, Secure Shell, FTP, Trivial FTP, Remote Desktop Protocol [RDP], Server Message Block [SMB]).

3.6. Sprawdzanie integralności sprzętu i oprogramowania

Nabywanie urządzeń z nieautoryzowanych kanałów sprzedaży stanowi coraz większy problem. Nielegalny sprzęt i oprogramowanie stwarzają poważne zagrożenia dla informacji użytkowników oraz ogólnej integralności środowiska sieciowego. Zakup produktów z rynku wtórnego, urządzeń podrobionych, skradzionych lub używanych potencjalnie narusza łańcuch dostaw i otwiera możliwości do instalacji złośliwego oprogramowania. Skutkiem tego może być obniżenie wydajności sieci oraz zagrożenie poufności, integralności i dostępności zasobów sieciowych. Ponadto, urządzenia mogą zostać zainfekowane nieautoryzowanym lub złośliwym oprogramowaniem po ich użyciu operacyjnym, dlatego organizacje powinny regularnie monitorować integralność oprogramowania.

Zalecenia

- Prowadź ścisłą kontrolę nad łańcuchem dostaw i dokonuj zakupów wyłącznie od autoryzowanych sprzedawców.
- Wymagaj od sprzedawców przestrzegania procedur zapewniających integralność łańcucha dostaw w celu potwierdzenia autentyczności zarówno sprzętu, jak i oprogramowania.
- Po zainstalowaniu sprawdź wszystkie urządzenia pod kątem ewentualnych zmian lub manipulacji.
- Dokonuj weryfikacji numerów seryjnych urządzeń z różnych źródeł.
- Pobieraj oprogramowanie, aktualizacje, poprawki i uaktualnienia jedynie ze zweryfikowanych źródeł.
- Regularnie przeprowadzaj weryfikację sum kontrolnych i porównaj wartości z bazą danych dostawcy w celu wykrycia nieautoryzowanych modyfikacji oprogramowania układowego.
- Regularnie monitoruj i rejestruj urządzenia, aby zweryfikować ich konfiguracje sieciowe.
- Przeprowadzaj szkolenia dla właścicieli sieci, administratorów oraz personelu zaopatrzeniowego, aby zwiększyć świadomość na temat urządzeń pochodzących z szarej strefy.

Źródła:

Dokument powstał na podstawie rekomendacji NIST, CISA, NSA.

https://media.defense.gov/2020/Aug/18/2002479461/-1/1/0/HARDENING_NETWORK_DEVICES.PDF
https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices