Table of Contents

1. Technologie bezpieczeństwa IoT 2
1.1. Technologie bezpieczeństwa dla różnych warstw IoT 2
1.2. Lekkie, energooszczędne algorytmy szyfrowania 2
1.3. Mechanizmy bezpiecznej weryfikacji i aktualizacji firmware'u 4
1.4. Narzędzia antymalware w bezpieczeństwie IoT 7
1.5. Wykorzystanie monitorowania SNMP w bezpieczeństwie urządzeń IoT 7
1.6. Bezpieczeństwo sieci IoT: wdrażanie solidnych protokołów szyfrowania 9
1.7. Technologie systemów SIEM w zintegrowanym bezpieczeństwie IoT 11
1.8. Metodyka bezpieczeństwa IoT: identyfikacja cyberzagrożeń IoT i zapobieganie im 13
1.9. Wzmacnianie bezpieczeństwa IoT: kluczowe strategie ochrony 14

1. Technologie bezpieczeństwa IoT

W poprzednich podrozdziałach omówiono podatności IoT, cyberataki i wektory ataku oraz dobre praktyki przeciwdziałania tym podatnościom, zagrożeniom i wektorom ataku. W tym podrozdziale przedstawiono technologie bezpieczeństwa IoT oraz ogólną metodykę zabezpieczania sieci i systemów IoT.

1.1. Technologie bezpieczeństwa dla różnych warstw IoT

Do zaprojektowania solidnego i kompleksowego systemu cyberbezpieczeństwa wykorzystuje się różne narzędzia. Żadne pojedyncze narzędzie nie jest w stanie obsłużyć zagadnień bezpieczeństwa we wszystkich warstwach architektury referencyjnej IoT. Dlatego w poszczególnych warstwach – od warstwy percepcji (urządzeń) po warstwę aplikacji – wdraża się odpowiednie narzędzia. Bezpieczeństwo IoT można zatem podzielić na następujące kategorie (rysunek 1):



Fig. 1: Technologie bezpieczeństwa dla różnych warstw IoT

- bezpieczeństwo urządzeń IoT,
- bezpieczeństwo sieci IoT,
- bezpieczeństwo mgły/chmury IoT,
- bezpieczeństwo aplikacji IoT.

Ograniczenia sprzętowe urządzeń IoT utrudniają stosowanie w nich tradycyjnych narzędzi bezpieczeństwa węzłów końcowych, takich jak zapory sieciowe i oprogramowanie antymalware. Trudno też aktualizować i łatać te urządzenia w taki sposób, w jaki aktualizuje się tradycyjne węzły końcowe. Wciąż podejmuje się jednak wiele wysiłków, aby dostosować konwencjonalne technologie bezpieczeństwa do ochrony urządzeń IoT. Rośnie przy tym zapotrzebowanie na technologie bezpieczeństwa, które zapewniałyby ochronę wszystkich węzłów IoT przy niższym koszcie energetycznym i komunikacyjnym. Do technologii zabezpieczania urządzeń IoT należą:

1.2. Lekkie, energooszczędne algorytmy szyfrowania

Aby zwiększyć bezpieczeństwo danych przesyłanych przez urządzenia IoT, kluczowe jest stosowanie lekkich algorytmów kryptograficznych, zaprojektowanych z myślą o wydajnym działaniu na urządzeniach o ograniczonej mocy obliczeniowej i zasobach energii. Algorytmy takie jak Data

Encryption Standard (DES), Advanced Encryption Standard (AES) i inne zoptymalizowane, energooszczędne schematy kryptograficzne chronią integralność i poufność danych.

Znaczenie lekkich algorytmów szyfrowania dla IoT

- Wydajność i przydatność: w odróżnieniu od tradycyjnych systemów komputerowych wiele urządzeń IoT działa przy ograniczonych zasobach obliczeniowych, ograniczonej pamięci i zmniejszonej pojemności baterii. Dlatego lekkie algorytmy kryptograficzne są niezbędne – zapewniają solidne szyfrowanie bez nadmiernego obciążania urządzenia. Algorytmy takie jak DES i AES zostały zaadaptowane do wersji lekkich, np. AES-128, które równoważą bezpieczeństwo i wydajność. Dzięki tym adaptacjom urządzenia IoT mogą skutecznie szyfrować dane bez znacznego zużycia energii czy opóźnień przetwarzania.
- Zabezpieczanie danych w transmisji: algorytmy szyfrowania chronią dane przesyłane z urządzeń IoT do serwerów centralnych, platform chmurowych lub innych punktów końcowych sieci. Kodując dane, algorytmy te zapobiegają ich nieuprawnionemu przechwyceniu lub modyfikacji podczas transmisji, zapewniając, że wrażliwe informacje – takie jak parametry zdrowotne, odczyty czujników przemysłowych czy nagrania z domowego monitoringu – pozostają poufne i nienaruszone.

Ochrona danych podczas przechowywania i transmisji

- Szyfrowanie danych w spoczynku: zastosowanie algorytmów szyfrowania wykracza poza transmisję – są one niezbędne również do zabezpieczania danych w spoczynku. Dane przechowywane w pamięci urządzeń, chmurowych bazach danych czy serwerach lokalnych muszą być szyfrowane, aby ograniczyć ryzyko wycieku. Jest to szczególnie ważne w zastosowaniach IoT w ochronie zdrowia, finansach i inteligentnych miastach, gdzie wycieki mogłyby prowadzić do poważnych naruszeń prywatności lub zakłóceń działania.
- Zabezpieczanie kanałów komunikacyjnych: protokoły szyfrowania zapewniają bezpieczeństwo kanałów komunikacyjnych dla danych w transmisji. Może to obejmować stosowanie Transport Layer Security (TLS) i lekkich algorytmów szyfrowania do utworzenia bezpiecznej ścieżki komunikacyjnej. Szyfrując pakiety danych przed wysłaniem i odszyfrowując je po stronie odbiorczej, systemy IoT mogą zapobiegać atakom man-in-the-middle (MitM) i innym formom podsłuchu.

Weryfikacja integralności firmware'u

- Zapewnienie autentyczności aktualizacji firmware'u: utrzymanie integralności firmware'u urządzeń IoT jest niezbędne, aby zapobiec instalacji złośliwych aktualizacji, które mogłyby zakłócić działanie urządzenia lub dać atakującym nieuprawniony dostęp. Kluczową rolę odgrywają tu kryptograficzne podpisy cyfrowe. Zanim urządzenie IoT zaakceptuje i zainstaluje aktualizację firmware'u, weryfikuje dołączony do niej podpis kryptograficzny.
- Proces weryfikacji: podpisy cyfrowe wykorzystują kryptografię klucza publicznego do zapewnienia autentyczności. Przy tworzeniu aktualizacji firmware'u jest ona podpisywana kluczem prywatnym posiadanym przez producenta lub zaufane źródło. Urządzenie IoT, które przechowuje odpowiadający mu klucz publiczny, weryfikuje podpis po otrzymaniu aktualizacji. Jeśli podpis jest zgodny, urządzenie potwierdza, że aktualizacja nie została zmodyfikowana i pochodzi z autentycznego źródła. Jeśli weryfikacja się nie powiedzie, urządzenie odrzuca aktualizację, zapobiegając instalacji potencjalnie szkodliwego oprogramowania.
- Ochrona przed nieuprawnionymi modyfikacjami: proces weryfikacji zapewnia, że aktualizacje firmware'u są zabezpieczone przed nieuprawnionymi modyfikacjami, co chroni urządzenia przed potencjalnym wykorzystaniem. Atakujący często próbują wstrzyknąć złośliwy kod za pomocą podrobionego lub zmodyfikowanego firmware'u. Ekosystemy IoT mogą bronić się przed tym

ryzykiem, wymagając weryfikacji podpisu kryptograficznego i utrzymując zaufanie do działania urządzeń.

Wzmocnienie bezpieczeństwa dzięki warstwowym rozwiązaniom kryptograficznym

- Łączenie szyfrowania z innymi środkami bezpieczeństwa: choć szyfrowanie jest potężnym narzędziem, kompleksowe bezpieczeństwo IoT wymaga podejścia warstwowego, łączącego szyfrowanie z innymi protokołami bezpieczeństwa. Mogą to być segmentacja sieci, uwierzytelnianie wieloskładnikowe (MFA) i systemy wykrywania włamań (IDS). Połączenie szyfrowania z tymi praktykami tworzy solidną strategię obrony, chroniącą dane i infrastrukturę przed różnymi wektorami ataku.
- Przygotowanie na przyszłość dzięki nowym technikom kryptograficznym: wraz z rozwojem technologii IoT ewoluują też metody cyberprzestępców. Aby ich wyprzedzać, organizacje powinny rozważyć stosowanie nowych technik kryptograficznych, takich jak kryptografia krzywych eliptycznych (ECC), która zapewnia wysokie bezpieczeństwo przy mniejszym narzucie obliczeniowym niż algorytmy tradycyjne. Takie rozwiązania zapewniają bezpieczeństwo systemów IoT nawet przy wzroście mocy obliczeniowej i wyrafinowania ataków.

Stosowanie lekkich algorytmów kryptograficznych, takich jak DES i AES, jest podstawą zapewnienia bezpieczeństwa danych przesyłanych przez urządzenia IoT. Algorytmy te chronią dane podczas przechowywania i komunikacji oraz odgrywają kluczową rolę w weryfikacji integralności aktualizacji firmware'u. Wykorzystując kryptograficzne podpisy cyfrowe, systemy IoT mogą potwierdzić, że aktualizacje są autentyczne i niezmienione, wzmacniając wiarygodność całego ekosystemu IoT. Dla kompleksowego bezpieczeństwa połączenie tych praktyk kryptograficznych z innymi środkami proaktywnymi zapewnia odporność na szereg cyberzagrożeń.

1.3. Mechanizmy bezpiecznej weryfikacji i aktualizacji firmware'u

Bezpieczeństwo i niezawodność urządzeń IoT w dużym stopniu zależą od ich firmware'u – podstawowej warstwy oprogramowania sterującej funkcjami sprzętu. Ponieważ urządzenia IoT są zazwyczaj podłączone do Internetu przez całą dobę, są narażone na szeroki zakres cyberzagrożeń. Regularne i bezpieczne aktualizacje firmware'u są kluczowe dla łatania podatności, rozszerzania funkcjonalności i obrony przed nowymi wektorami ataku. Bez bezpiecznych mechanizmów weryfikacji i aktualizacji firmware'u urządzenia IoT mogą stać się punktami wejścia dla atakujących, umożliwiając im naruszenie bezpieczeństwa sieci, zakłócenie usług lub kradzież wrażliwych danych.

Typowe zagrożenia bezpieczeństwa związane z firmware'em urządzeń IoT

- Słabe szyfrowanie lub jego brak: firmware wielu urządzeń IoT nie ma wystarczających protokołów szyfrowania. To przeoczenie czyni urządzenie podatnym na podsłuch i nieuprawniony dostęp ze strony atakujących, którzy mogą przechwycić niezaszyfrowane dane i wykorzystać je do kompromitacji urządzenia lub sieci. Wdrożenie solidnych standardów szyfrowania zapewnia bezpieczeństwo danych przesyłanych między urządzeniem a serwerami.
- Słabe mechanizmy uwierzytelniania: firmware IoT często zawiera wbudowane na stałe lub słabe dane uwierzytelniające, które atakujący mogą łatwo wykorzystać. Takie podatności dają nieuprawnionym użytkownikom możliwość przejęcia kontroli nad urządzeniem. Aby ograniczyć to ryzyko, firmware powinien obsługiwać silne, konfigurowalne metody uwierzytelniania, wymagające od użytkowników unikalnych, złożonych danych uwierzytelniających.

- Brak bezpiecznych mechanizmów aktualizacji: brak bezpiecznych procedur aktualizacji stwarza poważne ryzyko. Firmware, którego nie można bezpiecznie zaktualizować lub załatać, pozostawia urządzenia narażone na znane podatności, które atakujący mogą wykorzystać do cyberataków. Należy wdrożyć bezpieczne mechanizmy aktualizacji, wykorzystujące podpisy cyfrowe i kontrolę integralności, aby instalowane były wyłącznie autentyczne i autoryzowane aktualizacje.
- Ryzyko modyfikacji: urządzenia IoT bez bezpiecznego rozruchu i bezpiecznych procedur aktualizacji są bardzo podatne na modyfikacje. Atakujący mogą zmodyfikować lub zastąpić firmware złośliwym kodem, co pozwala im przejąć kontrolę nad urządzeniem lub utworzyć trwałe tylne furtki. Wdrożenie bezpiecznego rozruchu zapewnia, że urządzenie ładuje wyłącznie zweryfikowany i uwierzytelniony firmware, zapobiegając uruchomieniu nieautoryzowanego kodu podczas startu.
- Zagrożenia wynikające ze złych praktyk programistycznych: niewystarczające środki bezpieczeństwa na etapie tworzenia firmware'u mogą skutkować wbudowanymi podatnościami, które mogą wykorzystać atakujący. Złe praktyki programistyczne lub wprowadzanie luk przez nieuczciwych pracowników zwiększają ryzyko kompromitacji firmware'u. Solidne protokoły bezpieczeństwa w procesie rozwoju – przeglądy kodu, automatyczne testy bezpieczeństwa i bezpieczny cykl życia oprogramowania – minimalizują to ryzyko.

Dobre praktyki bezpiecznej weryfikacji i aktualizacji firmware'u

- Bezpieczny rozruch (Secure Boot): proces bezpiecznego rozruchu chroni urządzenia IoT przed uruchomieniem nieautoryzowanego lub złośliwego firmware'u podczas startu. Obejmuje weryfikację kryptograficzną, w której producent cyfrowo podpisuje firmware urządzenia. Sprzęt urządzenia sprawdza ten podpis przed załadowaniem firmware'u, dzięki czemu uruchomić można wyłącznie firmware zweryfikowany przez producenta. Zapobiega to modyfikacjom, nieuprawnionym zmianom i atakom wstrzykiwania złośliwego oprogramowania.
- Podpisy cyfrowe do weryfikacji: podpisy cyfrowe zapewniają dodatkową warstwę bezpieczeństwa, uwierzytelniając źródło i integralność aktualizacji firmware'u. Kryptografia klucza publicznego zapewnia, że firmware nie został zmieniony w transmisji i pochodzi z zaufanego źródła. Każda aktualizacja, która nie przejdzie weryfikacji podpisu, jest odrzucana, co chroni urządzenie przed potencjalnie szkodliwym kodem.
- Bezpieczne mechanizmy aktualizacji bezprzewodowej (OTA): aktualizacje OTA umożliwiają sprawne dostarczanie poprawek firmware'u i aktualizacji bezpieczeństwa bez fizycznej interwencji. Aktualizacja OTA (ang. *over-the-air*) to metoda zdalnej aktualizacji oprogramowania lub firmware'u urządzenia IoT bez konieczności fizycznego dostępu. Aktualizacje OTA pozwalają producentom i administratorom sieci efektywnie dystrybuować poprawki, nowe funkcje, poprawki bezpieczeństwa i usunięcia błędów do urządzeń IoT podłączonych do sieci. Ta możliwość zdalnej aktualizacji jest kluczowa dla utrzymania wydajności urządzeń, usuwania nowych podatności i zapewnienia, że urządzenia działają z najnowszymi protokołami bezpieczeństwa. Dzięki aktualizacjom OTA urządzenia IoT mogą bezproblemowo otrzymywać istotne usprawnienia, co ogranicza przestoje związane z ręczną aktualizacją i trudności logistyczne. Aby zapewnić bezpieczeństwo, aktualizacje OTA powinny obejmować szyfrowaną transmisję danych, protokoły uwierzytelniania weryfikujące źródło aktualizacji oraz kontrolę integralności potwierdzającą, że aktualizacja nie została zmodyfikowana podczas transmisji. Właściwa implementacja mechanizmów OTA zwiększa funkcjonalność i bezpieczeństwo urządzeń IoT oraz wzmacnia ogólną odporność ekosystemu IoT.
- Kontrola integralności i mechanizmy awaryjne: kontrola integralności w procesie aktualizacji pomaga upewnić się, że firmware nie został zmieniony ani uszkodzony. Urządzenia powinny mieć mechanizmy wycofania (ang. *rollback*), przywracające znany bezpieczny stan, jeśli aktualizacja nie przejdzie walidacji lub zakłóci działanie urządzenia. Zapewnia to ciągłość

działania i chroni przed przypadkowym lub złośliwym uszkodzeniem firmware'u.
- Regularne audyty bezpieczeństwa i zarządzanie poprawkami: firmware powinien być regularnie audytowany pod kątem podatności, również po wdrożeniu. Producenci powinni proaktywnie identyfikować potencjalne słabości i niezwłocznie publikować poprawki. Urządzenia IoT powinny obsługiwać zautomatyzowane zarządzanie poprawkami, usprawniające dystrybucję i instalację aktualizacji, przy czym każda aktualizacja musi przejść kontrolę bezpieczeństwa przed instalacją.

Rola norm i regulacji

Przestrzeganie norm i regulacji branżowych, takich jak wytyczne Internet Engineering Task Force (IETF) i National Institute of Standards and Technology (NIST), może wzmocnić bezpieczeństwo firmware'u IoT. Wytyczne te opisują dobre praktyki bezpiecznego wytwarzania oprogramowania, protokołów szyfrowania i mechanizmów uwierzytelniania. Zgodność z tymi normami pomaga budować zaufanie użytkowników i odpowiada globalnym oczekiwaniom w zakresie cyberbezpieczeństwa.

Producenci i firmy wdrażające urządzenia IoT powinni zadbać o to, aby ich procesy aktualizacji firmware'u i mechanizmy weryfikacji były zgodne z odpowiednimi normami bezpieczeństwa. Chroni to urządzenia przed cyberatakami, świadczy o zaangażowaniu w bezpieczeństwo i może dawać przewagę konkurencyjną w branżach, w których ochrona danych ma kluczowe znaczenie.

Mechanizmy bezpiecznej weryfikacji i aktualizacji firmware'u są niezbędne do utrzymania bezpieczeństwa i integralności urządzeń IoT. Wdrożenie bezpiecznego rozruchu, który ładuje i uruchamia wyłącznie zaufany, cyfrowo podpisany firmware, jest kluczowe dla zapobiegania uruchomieniu nieautoryzowanego lub zmodyfikowanego firmware'u. Środek ten chroni urządzenia IoT przed atakami wstrzykiwania złośliwego oprogramowania podczas startu. Ponadto należy wdrożyć bezpieczne mechanizmy aktualizacji OTA, umożliwiające bezpieczne dostarczanie poprawek i aktualizacji bezpieczeństwa do urządzeń IoT i chroniące przed atakami man-in-the-middle oraz nieuprawnionymi modyfikacjami w procesie aktualizacji [1)]. Strategie te, w połączeniu z rygorystycznymi praktykami programistycznymi i zgodnością z normami branżowymi, tworzą solidne ramy bezpieczeństwa wspierające bezpieczne działanie ekosystemów IoT.

** Aktualizacje firmware'u oparte na blockchainie **

Regularne aktualizacje firmware'u urządzeń IoT są niezbędne do utrzymania bezpieczeństwa i funkcjonalności, jednak zapewnienie autentyczności, integralności i zgodności tych aktualizacji stanowi istotne wyzwanie. Wykorzystanie technologii blockchain może zwiększyć bezpieczeństwo i niezawodność całego procesu aktualizacji – od generowania i podpisywania, przez dystrybucję i weryfikację, po instalację. Podejście to radykalnie zmniejsza ryzyko złośliwych modyfikacji, nieuprawnionych zmian lub błędów, które mogłyby skompromitować urządzenia lub sieci.

Technologia blockchain umożliwia przejrzystą współpracę wielu interesariuszy, pozwalając im współtworzyć i przeglądać kod firmware'u przy zachowaniu jasnego, możliwego do prześledzenia zapisu wersji i zmian kodu. Do potwierdzenia tożsamości źródła i integralności aktualizacji można wykorzystać podpisy cyfrowe i skróty kryptograficzne. Ponadto mechanizmy konsensusu blockchain i inteligentne kontrakty (ang. *smart contracts*) zapewniają solidne ramy weryfikacji i wykonywania aktualizacji oraz rejestrowania i audytu wyników. Zapewnia to kompleksowy i bezpieczny proces aktualizacji firmware'u, chroniący zarówno urządzenia, jak i połączone sieci.

1.4. Narzędzia antymalware w bezpieczeństwie IoT

Cyberprzestępcy tworzą coraz bardziej wyrafinowane złośliwe oprogramowanie, wymierzone w specyficzne podatności urządzeń IoT. Ataki te mogą mieć różną wagę – od niegroźnych żartów, takich jak zmiana temperatury na inteligentnym termostacie, po poważne zagrożenia, jak przejęcie kontroli nad kamerami monitoringu czy kompromitacja przemysłowych systemów sterowania. Malware IoT znacząco różni się od tradycyjnych wirusów komputerowych. Takie złośliwe programy są zazwyczaj projektowane do działania na urządzeniach o ograniczonej mocy obliczeniowej i pamięci, co utrudnia ich wykrycie i usunięcie. Ponadto mogą szybko rozprzestrzeniać się w sieciach połączonych urządzeń, tworząc rozległe botnety zdolne do przeprowadzania potężnych ataków rozproszonej odmowy usługi (DDoS).

Różnorodność malware IoT pokazuje pomysłowość cyberprzestępców, którzy stale wymyślają nowe metody wykorzystywania tych urządzeń – często szybciej, niż producenci są w stanie publikować poprawki podatności [2)]. Zaleca się wdrożenie kompleksowych technologii bezpieczeństwa chroniących urządzenia IoT przed zagrożeniami ze strony złośliwego oprogramowania. Wdrożenie solidnych rozwiązań antymalware – oprogramowania antywirusowego, antyspyware, antyransomware i antytrojanowego – może znacząco poprawić ochronę urządzeń IoT. Środki te pomagają wykrywać, zapobiegać i neutralizować złośliwe programy, zanim naruszą one działanie urządzenia lub integralność danych. Biorąc pod uwagę specyficzne podatności i ograniczoną moc obliczeniową wielu urządzeń IoT, kluczowy jest wybór lekkich, wydajnych rozwiązań dostosowanych do ich potrzeb. Integracja narzędzi antymalware z monitorowaniem zagrożeń w czasie rzeczywistym i automatycznymi aktualizacjami może dodatkowo wzmocnić obronę przed szybko ewoluującymi cyberzagrożeniami.

Aby zapewnić solidne mechanizmy kontroli dostępu chroniące prywatność i poufność danych IoT, należy stosować skuteczne technologie zarządzania uwierzytelnianiem, takie jak systemy zarządzania hasłami i uwierzytelnianie wieloskładnikowe.

Bezpieczne zarządzanie danymi uwierzytelniającymi: należy unikać stosowania domyślnych lub wbudowanych na stałe danych uwierzytelniających w firmware, ponieważ atakujący mogą je szybko odkryć i uzyskać nieuprawniony dostęp. Zamiast tego należy wdrożyć silne mechanizmy uwierzytelniania, takie jak uwierzytelnianie wieloskładnikowe. Należy zachęcać użytkowników do zmiany haseł domyślnych podczas wstępnej konfiguracji urządzenia IoT, aby zapobiec atakom opartym na znanych danych uwierzytelniających.

1.5. Wykorzystanie monitorowania SNMP w bezpieczeństwie urządzeń IoT

Protokół SNMP (ang. *Simple Network Management Protocol*) odgrywa istotną rolę w utrzymaniu bezpieczeństwa i integralności działania urządzeń IoT w sieci. Ten powszechnie stosowany protokół służy do zbierania danych i zarządzania urządzeniami podłączonymi do sieci, pomagając chronić je przed nieuprawnionym dostępem i innymi zagrożeniami. Aby jednak skutecznie wykorzystać możliwości SNMP, organizacje powinny stosować solidne narzędzia monitorowania i zarządzania, zapewniające kompleksowy nadzór.

Znaczenie monitorowania i zarządzania za pomocą SNMP: SNMP to protokół komunikacyjny ułatwiający wymianę informacji zarządczych między urządzeniami sieciowymi a systemami

monitorowania. Pozwala administratorom sieci nadzorować szereg podłączonych urządzeń, takich jak routery, przełączniki, czujniki IoT i inny sprzęt. Informacje zbierane przez SNMP mogą być nieocenione przy identyfikacji potencjalnych zagrożeń bezpieczeństwa, wykrywaniu wąskich gardeł wydajności i wyprzedzającym rozwiązywaniu problemów, zanim się nasilą.

Kluczowe cechy i możliwości rozwiązań monitorowania SNMP

Scentralizowana platforma monitorowania: rozwiązania monitorowania SNMP zapewniają administratorom jednolitą platformę do śledzenia wszystkich urządzeń podłączonych do sieci. Takie scentralizowane podejście upraszcza zarządzanie różnorodnymi urządzeniami IoT, umożliwiając monitorowanie w czasie rzeczywistym ruchu urządzeń, punktów dostępowych i ogólnej aktywności. Pełna widoczność pozwala szybko reagować na potencjalne naruszenia bezpieczeństwa lub nietypowe zachowania.

- **Analiza ruchu i aktywności**: za pomocą narzędzi SNMP można analizować ruch sieciowy w celu wykrycia nietypowych wzorców wskazujących na złośliwą aktywność lub próby nieuprawnionego dostępu. Administratorzy mogą identyfikować skoki przepływu danych, nieoczekiwaną komunikację z zewnętrznymi serwerami lub inne anomalie sugerujące obecność złośliwego oprogramowania lub cyberatak.
- **Monitorowanie wydajności sprzętu**: poza bezpieczeństwem rozwiązania SNMP pomagają monitorować stan i wydajność urządzeń sieciowych. Obejmuje to śledzenie kluczowych parametrów, takich jak użycie procesora, obciążenie pamięci i czas pracy urządzenia. Ciągła ocena tych parametrów pozwala wykrywać oznaki awarii sprzętu lub spadku wydajności, umożliwiając terminową konserwację i minimalizując ryzyko przestojów.
- **Niestandardowe alerty i powiadomienia**: jedną z wyróżniających cech zaawansowanych narzędzi zarządzania SNMP jest możliwość tworzenia własnych alertów. Administratorzy mogą ustawiać progi dla różnych wskaźników wydajności i bezpieczeństwa, takich jak wykorzystanie pasma czy liczba prób logowania. Po przekroczeniu progów system wysyła alerty, umożliwiając zespołowi szybką reakcję. Konfigurowalne powiadomienia zapewniają, że zagrożenia nie zostaną przeoczone, a zespoły proaktywnie usuwają podatności.
- **Wykrywanie i klasyfikacja urządzeń**: wysokiej jakości rozwiązania zarządzania SNMP, takie jak NinjaOne, oferują automatyczne wykrywanie urządzeń. Oznacza to, że nowe urządzenia dodane do sieci są natychmiast identyfikowane i rejestrowane. System może następnie klasyfikować je według danych uwierzytelniających, typu urządzenia i innych kryteriów. Funkcja ta jest przydatna do utrzymania dokładnej ewidencji wszystkich zasobów sieciowych i zapewnienia, że nieznane lub nieautoryzowane urządzenia są niezwłocznie oznaczane do weryfikacji.

Wzmocnienie bezpieczeństwa IoT za pomocą SNMP: Włączając narzędzia monitorowania SNMP do szerszej strategii bezpieczeństwa, organizacje mogą wzmocnić swoje mechanizmy obronne i zwiększyć odporność ekosystemu IoT. Regularne audyty i nadzór w czasie rzeczywistym zapewniane przez rozwiązania SNMP ułatwiają przestrzeganie protokołów bezpieczeństwa i pomagają chronić integralność wrażliwych danych przesyłanych przez urządzenia IoT. Ponadto integracja danych SNMP z innymi narzędziami cyberbezpieczeństwa, takimi jak systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), może zapewnić głębszy wgląd i usprawnić reagowanie na incydenty.

Dobre praktyki wdrażania rozwiązań SNMP

- **Konfiguracja kontroli dostępu**: dostęp do SNMP należy ograniczyć do zaufanych administratorów. Aby chronić przesyłane dane, zaleca się stosowanie SNMPv3, który obsługuje szyfrowanie i rozszerzone funkcje bezpieczeństwa.

- **Regularna aktualizacja oprogramowania SNMP**: narzędzia zarządzania SNMP należy aktualizować, aby chronić je przed znanymi podatnościami i zapewnić zgodność z najnowszym firmware'em urządzeń.
- **Wielowarstwowe bezpieczeństwo**: monitorowanie SNMP należy łączyć z innymi środkami bezpieczeństwa, takimi jak zapory sieciowe, systemy wykrywania włamań (IDS) i ochrona punktów końcowych, tworząc wielowarstwową strategię obrony.
- **Szkolenia i budowanie świadomości**: zespoły IT powinny mieć wiedzę i przeszkolenie pozwalające skutecznie korzystać z narzędzi SNMP. Umiejętność interpretacji danych SNMP i reagowania na alerty jest kluczowa dla utrzymania bezpieczeństwa sieci.

Monitorowanie i zarządzanie za pomocą SNMP ma więc kluczowe znaczenie dla organizacji chcących chronić swoją infrastrukturę IoT. Wdrażając zaawansowane rozwiązania SNMP, firmy mogą uzyskać lepszą widoczność, proaktywnie wykrywać zagrożenia i sprawować kompleksową kontrolę nad siecią, zwiększając ogólne bezpieczeństwo i efektywność działania.

1.6. Bezpieczeństwo sieci IoT: wdrażanie solidnych protokołów szyfrowania

Bezpieczeństwo komunikacji między urządzeniami IoT a serwerami zaplecza jest fundamentem solidnych ram bezpieczeństwa sieci. W miarę wzrostu złożoności i skali ekosystemów IoT ochrona integralności, poufności i autentyczności transmisji danych staje się coraz ważniejsza. Jedną z najskuteczniejszych strategii zabezpieczania tych interakcji jest wdrożenie solidnych protokołów szyfrowania, takich jak Transport Layer Security (TLS).

Znaczenie solidnego szyfrowania w bezpieczeństwie IoT: Urządzenia IoT często przesyłają wrażliwe dane – od informacji osobowych użytkowników po przemysłowe sygnały sterujące. Przechwycenie lub zmodyfikowanie tych danych może mieć poważne konsekwencje, w tym wycieki, nieuprawniony dostęp i zakłócenie kluczowych usług. Protokoły szyfrowania stanowią barierę ochronną, zapewniając, że dane pozostają poufne i niezmienione na drodze między urządzeniami a serwerami. Szyfrując dane w transmisji i zapewniając bezpieczną komunikację, organizacje mogą minimalizować ryzyko związane z przechwyceniem danych.

Jak TLS zwiększa bezpieczeństwo IoT

Transport Layer Security (TLS) to powszechnie uznany protokół szyfrowania, przeznaczony do zabezpieczania danych przesyłanych przez sieci. TLS ustanawia szyfrowane połączenie między urządzeniami IoT a serwerami zaplecza, chroniąc dane przed podsłuchem i modyfikacją. TLS wzmacnia bezpieczeństwo sieci w ekosystemach IoT w następujący sposób:

- **Szyfrowanie danych**: TLS wykorzystuje algorytmy kryptograficzne do szyfrowania danych przed ich wysłaniem. Dzięki temu nawet jeśli atakujący przechwyci komunikację, nie odczyta jej treści bez odpowiedniego klucza deszyfrującego. Zaszyfrowane dane wyglądają jak losowy, nieczytelny ciąg, co czyni je wysoce odpornymi na nieuprawniony dostęp.
- **Uwierzytelnianie**: TLS obsługuje mechanizmy uwierzytelniania weryfikujące tożsamość komunikujących się stron. Zapobiega to atakom man-in-the-middle (MitM), w których atakujący mógłby podszyć się pod urządzenie lub serwer, aby przechwycić i zmienić dane. Uwierzytelnianie wzajemne, które może wykorzystywać certyfikaty urządzenia i serwera, wzmacnia zaufanie w sieci, potwierdzając, że dane są wymieniane wyłącznie między zweryfikowanymi stronami.

- **Integralność danych**: protokoły TLS wykorzystują funkcje skrótu utrzymujące integralność danych podczas transmisji. Funkcje te generują unikalną sumę kontrolną lub wartość skrótu dla każdego pakietu danych. Po dotarciu do celu wartość skrótu jest porównywana, aby upewnić się, że dane nie zostały zmienione w transmisji. W przypadku wykrycia niezgodności transmisja jest oznaczana jako skompromitowana.

Wdrażanie TLS w sieciach IoT

Wdrożenie TLS w sieci IoT wiąże się z szeregiem dobrych praktyk i uwarunkowań:

- Stosowanie TLS 1.2 lub nowszego: kluczowe jest używanie najnowszych wersji TLS (najlepiej TLS 1.2 lub TLS 1.3), aby korzystać z rozszerzonych funkcji bezpieczeństwa i unikać podatności starszych wersji. Na przykład TLS 1.3 upraszcza proces uzgadniania połączenia (handshake) i usuwa przestarzałe algorytmy, co zapewnia większe bezpieczeństwo i szybsze nawiązywanie połączeń.
- Zarządzanie certyfikatami: wdrożenie TLS opiera się na certyfikatach cyfrowych wydawanych przez zaufane urzędy certyfikacji (CA). Właściwe zarządzanie certyfikatami jest niezbędne do utrzymania bezpiecznej komunikacji. Organizacje powinny zautomatyzować odnawianie certyfikatów, aby uniknąć zakłóceń spowodowanych ich wygaśnięciem. Ponadto urządzenia IoT muszą umożliwiać bezpieczne przechowywanie certyfikatów i zarządzanie nimi, aby chronić je przed kradzieżą lub nadużyciem.
- Zgodność urządzeń i ograniczenia zasobów: wiele urządzeń IoT ma ograniczoną moc obliczeniową, pamięć i czas pracy na baterii, dlatego kluczowa jest optymalizacja implementacji TLS, aby uniknąć problemów z wydajnością. Aby zachować równowagę między bezpieczeństwem a funkcjonalnością urządzenia, można stosować lekkie wersje TLS i sprzętową akcelerację operacji kryptograficznych.
- Regularne aktualizacje bezpieczeństwa i zarządzanie poprawkami: aby TLS pozostał bezpieczny i skuteczny, organizacje muszą pilnować instalowania poprawek i aktualizacji bezpieczeństwa. Cyberprzestępcy stale opracowują nowe techniki wykorzystywania podatności, dlatego aktualność urządzeń i serwerów zaplecza zapewnia odporność mechanizmów szyfrowania na nowe zagrożenia.

Uzupełniające środki bezpieczeństwa

Choć TLS jest potężnym narzędziem zabezpieczania danych w transmisji, powinien być częścią kompleksowej strategii bezpieczeństwa obejmującej:

- Szyfrowanie end-to-end (E2EE): należy wdrożyć E2EE, aby zabezpieczyć dane od momentu opuszczenia źródła aż do dotarcia do celu. Dodatkowo zapobiega to ujawnieniu danych w pośrednich punktach sieci.
- Silna kontrola dostępu: należy wdrożyć ścisłą kontrolę dostępu i uwierzytelnianie wieloskładnikowe (MFA) dla ról administracyjnych, aby ograniczyć dostęp do kluczy szyfrujących i certyfikatów.
- Praktyki bezpiecznej konfiguracji: wszystkie urządzenia IoT powinny być bezpiecznie skonfigurowane, aby zapobiec podatnościom, które mogłyby osłabić szyfrowanie TLS, takim jak słabe hasła domyślne czy otwarte porty.

Solidne protokoły szyfrowania, takie jak TLS, są niezbędne do zabezpieczenia kanałów komunikacyjnych między urządzeniami IoT a serwerami zaplecza. Szyfrując dane, uwierzytelniając strony i zapewniając integralność danych, TLS minimalizuje ryzyko nieuprawnionego dostępu i wycieku danych. Skuteczne wdrożenie TLS powinno jednak być uzupełnione ciągłym monitorowaniem, aktualizacjami i warstwowym podejściem do bezpieczeństwa, aby zmaksymalizować ochronę w coraz

bardziej połączonym świecie.

1.7. Technologie systemów SIEM w zintegrowanym bezpieczeństwie IoT

Rejestrowanie zdarzeń i monitorowanie w kompleksowym zarządzaniu zagrożeniami

Systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (ang. *Security Information and Event Management*, SIEM) odgrywają kluczową rolę w ochronie ekosystemów IoT, łącząc rejestrowanie zdarzeń, monitorowanie i zaawansowaną analizę danych w celu zabezpieczenia urządzeń i sieci. Technologie te zapewniają jednolitą platformę do zbierania i analizowania danych bezpieczeństwa, niezbędną do utrzymania bezpiecznego środowiska w coraz bardziej połączonym świecie. Poniżej wyjaśniono, w jaki sposób rejestrowanie i monitorowanie przyczyniają się do kompleksowego bezpieczeństwa IoT i dlaczego są niezbędne dla współczesnych organizacji.

Monitorowanie i śledzenie w czasie rzeczywistym

- Ciągłe monitorowanie umożliwiające szybką reakcję: systemy SIEM umożliwiają śledzenie w czasie rzeczywistym aktywności urządzeń IoT i ruchu sieciowego, pozwalając zespołom bezpieczeństwa szybko wykrywać incydenty i na nie reagować. Ciągłe monitorowanie zapewnia szybką identyfikację wszelkich odstępstw od normalnej aktywności, pomagając zapobiegać naruszeniom, zanim się nasilą. Jest to kluczowe w ekosystemie IoT, gdzie zachowanie urządzeń może być bardzo zróżnicowane, a nowe zagrożenia mogą pojawić się w każdej chwili.
- Szczegółowa widoczność: systemy SIEM dają organizacjom szczegółowy wgląd w sieć IoT, obejmujący monitorowanie przepływów danych między urządzeniami, interakcji z serwerami zaplecza i komunikacji z sieciami zewnętrznymi. Dzięki temu wszelkie nieprawidłowości, takie jak nieoczekiwane transmisje danych czy próby nieuprawnionego dostępu, są natychmiast oznaczane do dalszego zbadania.

Kompleksowe zbieranie i analiza dzienników

- Agregacja dzienników z różnych źródeł: rozwiązania SIEM zbierają dzienniki z wielu źródeł w sieci IoT, w tym dzienniki zdarzeń urządzeń, dane o ruchu sieciowym, aktywność aplikacji i rejestry dostępu użytkowników. Agregacja ta zapewnia holistyczny obraz sieci, ułatwiając wykrywanie skoordynowanych ataków lub wzorców, które w przeciwnym razie mogłyby pozostać niezauważone.
- Wykrywanie anomalii przez analizę dzienników: analizując dzienniki, systemy SIEM mogą rozpoznawać odstępstwa od ustalonych wzorców bazowych i identyfikować nietypowe zachowania wskazujące na incydenty bezpieczeństwa. Na przykład nagły skok transferu danych z określonego urządzenia lub napływ nieudanych prób logowania może wskazywać na skompromitowane urządzenie lub atak siłowy. Zaawansowane platformy SIEM często wykorzystują algorytmy uczenia maszynowego do usprawnienia wykrywania anomalii, ucząc się na danych historycznych, aby lepiej odróżniać aktywność nieszkodliwą od podejrzanej.
- Wgląd w zachowania: dzienniki dostarczają cennego wglądu w zachowania, pomagając organizacjom zrozumieć typowe działanie urządzeń i dostrzec odstępstwa. Pozwala to zespołom bezpieczeństwa identyfikować potencjalnie złośliwe zachowania, takie jak próby łączenia się urządzeń IoT z nieautoryzowanymi punktami końcowymi lub wykorzystywanie ich jako punktów wejścia do ruchu lateralnego w sieci.

Mechanizmy alertów i reagowanie na incydenty

- Automatyczne alerty skracające czas reakcji: kluczową cechą systemów SIEM są automatyczne mechanizmy alertów. Powiadamiają one administratorów w czasie rzeczywistym o wykryciu potencjalnych naruszeń bezpieczeństwa lub nietypowej aktywności. Alerty można konfigurować według różnych kryteriów, takich jak próby dostępu z nierozpoznanych adresów IP, nietypowe transfery danych czy nieuprawnione zmiany konfiguracji urządzeń.
- Konfigurowalne progi alertów: organizacje mogą dostosować ustawienia alertów SIEM do swoich profili ryzyka i potrzeb operacyjnych. Konfigurowalne progi pomagają odfiltrować szum i skupić się na alertach o wysokim priorytecie, dzięki czemu zespoły bezpieczeństwa mogą skutecznie reagować na krytyczne incydenty, nie będąc przytłoczonymi fałszywymi alarmami.
- Wsparcie skoordynowanego reagowania na incydenty: dzięki scentralizowanym danym i alertom w czasie rzeczywistym systemy SIEM dostarczają narzędzi usprawniających reagowanie na incydenty. Zespoły bezpieczeństwa mogą szybko badać alerty, korzystając z danych kontekstowych z dzienników SIEM, co pozwala ustalić źródło naruszenia, ocenić jego zakres i podjąć działania naprawcze. Skoordynowane podejście minimalizuje potencjalne szkody i przestoje związane z incydentami bezpieczeństwa.

Korzyści z wdrożenia SIEM w bezpieczeństwie IoT

- Skuteczniejsze wykrywanie zagrożeń: ciągłe monitorowanie, analiza dzienników i mechanizmy alertów pozwalają systemom SIEM wykrywać zagrożenia, które mogłyby ominąć tradycyjne zabezpieczenia. Jest to szczególnie ważne w środowiskach IoT, w których konwencjonalne rozwiązania antywirusowe mogą być niemożliwe do zastosowania ze względu na ograniczoną moc obliczeniową urządzeń.
- Zgodność z przepisami i raportowanie: wiele branż podlega regulacjom wymagającym prowadzenia kompleksowych dzienników i ścieżek audytu. Systemy SIEM wspierają zgodność, automatyzując zbieranie i przechowywanie dzienników, dostarczając jednoznacznych dowodów stosowania środków bezpieczeństwa i generując raporty wymagane przez regulatorów. Funkcje raportowania zgodności pomagają organizacjom wykazać, że spełniają branżowe standardy bezpieczeństwa i prywatności danych. Systemy SIEM umożliwiają więc generowanie raportów, które można przedstawić wewnętrznym i zewnętrznym audytorom bezpieczeństwa jako dowód zgodności z wymaganiami regulacyjnymi.
- Skalowalność dla rozrastających się sieci IoT: wraz z rozwojem sieci IoT systemy SIEM mogą skalować się, obsługując rosnące wolumeny danych i nowe typy urządzeń. Dzięki temu organizacje mogą nadal monitorować rozrastający się ekosystem IoT bez utraty widoczności i szybkości reakcji.
- Proaktywne poszukiwanie zagrożeń: oprócz zautomatyzowanego monitorowania systemy SIEM umożliwiają zespołom bezpieczeństwa proaktywne poszukiwanie zagrożeń (ang. *threat hunting*). Analitycy mogą korzystać z funkcji wyszukiwania i zapytań do przeglądania dzienników i odkrywania potencjalnych zagrożeń, które nie wywołały automatycznych alertów, co pozwala na wyprzedzające działania zaradcze.
- Automatyczne wykrywanie ataków i reagowanie: systemy SIEM umożliwiają automatyczne wykrywanie cyberataków i reagowanie na nie, ograniczając wyrządzane przez nie szkody. Silnik korelacji zdarzeń, analizujący ogromne ilości dzienników generowanych przez urządzenia IoT i inne narzędzia cyberbezpieczeństwa (np. systemy wykrywania i zapobiegania włamaniom, aplikacje antymalware, zapory sieciowe i honeypoty), może zostać zastąpiony modelami AI lub uczenia maszynowego, co zwiększa szybkość i dokładność wykrywania ataków i reagowania na nie.

Systemy SIEM są integralną częścią bezpieczeństwa IoT, zapewniając skuteczne połączenie rejestrowania zdarzeń, monitorowania w czasie rzeczywistym i automatycznych alertów, które pomagają organizacjom sprawnie wykrywać zagrożenia i na nie reagować. Agregując dane z wielu

źródeł, analizując dzienniki pod kątem anomalii i zapewniając kompleksowe alerty, rozwiązania SIEM zwiększają zdolność organizacji do bezpiecznego działania w coraz bardziej połączonym świecie. Wdrożenie wysokiej jakości systemu SIEM sprawia, że działania firm w zakresie bezpieczeństwa IoT są zarówno reaktywne, jak i proaktywne, co pozwala im pewnie mierzyć się z obecnymi i przyszłymi wyzwaniami.

1.8. Metodyka bezpieczeństwa IoT: identyfikacja cyberzagrożeń IoT i zapobieganie im

Poruszanie się w nieprzewidywalnym krajobrazie zagrożeń cyfrowych jest trudne, ale skuteczne zarządzanie ryzykiem w ekosystemie IoT jest osiągalne. Firmy każdej wielkości muszą włączyć solidne protokoły bezpieczeństwa do swojej działalności, koncentrując się na usprawnieniu wykrywania zagrożeń i reagowania na nie. Dedykowani administratorzy IT lub wyspecjalizowane zespoły bezpieczeństwa (np. centra operacji bezpieczeństwa, SOC) powinni zabezpieczać sieci, w tym wszystkie urządzenia IoT. Aby zaprojektować i wdrożyć solidne narzędzia i polityki cyberbezpieczeństwa chroniące sieci i systemy IoT, analitycy lub zespoły cyberbezpieczeństwa powinni przeprowadzać kompleksowe oceny ryzyka sieci i oprogramowania, wdrażać solidne środki obronne oraz wykorzystywać rozwiązania SIEM i inne narzędzia monitorowania bezpieczeństwa. Część tych strategii omówiono w [3)].

Przeprowadzanie kompleksowych ocen ryzyka sieci i oprogramowania. Praktyczny wywiad o cyberzagrożeniach (ang. *cyber threat intelligence*) polega na wyszukiwaniu i usuwaniu podatności w ramach przyjętego modelu cyberbezpieczeństwa. Proces ten powinien być ciągły i obejmować planowanie, zbieranie danych, analizę i raportowanie. Wynikowy raport powinien zostać oceniony i uzupełniony o nowe ustalenia, zanim zostanie uwzględniony w decyzjach strategicznych.

Oceny ryzyka można podzielić na trzy główne rodzaje:

- Ocena strategiczna: dostarcza kadrze zarządzającej wiedzy o długoterminowych wyzwaniach i wczesnych ostrzeżeń. Informuje decydentów o zamiarach i możliwościach cyberprzestępców w obecnym krajobrazie IoT.
- Ocena taktyczna: zapewnia analizę zdarzeń, działań i raportów w czasie rzeczywistym, wspierając bieżącą działalność i potrzeby klientów. Często obejmuje dane z czujników i inteligentnych liczników w przemysłowych systemach IoT.
- Ocena operacyjna: śledzi potencjalne incydenty na podstawie powiązanych działań i raportów, umożliwiając proaktywne strategie zarządzania przyszłymi incydentami i utrzymanie konserwacji predykcyjnej.

Wdrażanie solidnych środków obronnych. Kompleksowa polityka cyberbezpieczeństwa jest niezbędna do ochrony ekosystemu IoT. Powinna ona obejmować szereg strategii minimalizujących ryzyko. Standardowe praktyki obronne obejmują:

- Wdrożenie skutecznego oprogramowania antywirusowego i antymalware.
- Włączenie uwierzytelniania dwuskładnikowego (2FA) lub wieloskładnikowego (MFA).
- Aktualizowanie całego oprogramowania w celu łatania znanych podatności.
- Stosowanie narzędzi zarządzania powierzchnią ataku.
- Wdrożenie segmentacji sieci w celu ograniczenia rozprzestrzeniania się zagrożeń.
- Przyjęcie modelu bezpieczeństwa zero-trust.
- Zapewnienie ciągłych szkoleń i programów podnoszenia świadomości cyberbezpieczeństwa dla

pracowników i użytkowników końcowych.

Wykorzystanie rozwiązań SIEM. Systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) mają kluczowe znaczenie dla zarządzania cyberbezpieczeństwem w czasie rzeczywistym. Rozwiązania te zwiększają bezpieczeństwo, integrując wywiad o zagrożeniach z reagowaniem na incydenty, co czyni je nieocenionym narzędziem analizy działań bezpieczeństwa w ekosystemie IoT.

Platformy SIEM zbierają dane o zdarzeniach z aplikacji, urządzeń i innych systemów w infrastrukturze IoT i konsolidują je w przejrzystej, użytecznej formie. System generuje konfigurowalne alerty dostosowane do różnych poziomów zagrożenia. Kluczowe korzyści ze stosowania rozwiązań SIEM to:

- Wykrywanie podatności.
- Identyfikacja potencjalnych zagrożeń wewnętrznych.
- Agregacja i wizualizacja danych zapewniająca lepszy nadzór.
- Zapewnienie zgodności z przepisami.
- Skuteczne zarządzanie dziennikami i ich analiza.

1.9. Wzmacnianie bezpieczeństwa IoT: kluczowe strategie ochrony

Skuteczna obrona przed malware IoT wymaga kompleksowego, wielowarstwowego podejścia, łączącego zaawansowane technologie i solidne praktyki bezpieczeństwa. Poniżej przedstawiono rekomendowane przez ekspertów dobre praktyki omówione w [4)]:

- **Wdrożenie segmentacji sieci**: bardzo skutecznym sposobem ograniczania malware IoT i ataków wykorzystujących ruch sieciowy (np. DDoS) jest segmentacja sieci. Umieszczając urządzenia IoT w oddzielnych segmentach sieci lub sieciach VLAN, organizacje mogą zapobiec rozprzestrzenianiu się malware i chronić infrastrukturę krytyczną. Segmentacja pozwala też zapobiec przekształceniu urządzeń IoT w botnety wykorzystywane do ataków DDoS na bramy sieciowe i serwery w infrastrukturze IT organizacji lub innych organizacji. Można to porównać do tworzenia cyfrowych stref izolacji: zainfekowane urządzenie IoT nie może skompromitować całej sieci, a skompromitowane urządzenia IoT nie mogą posłużyć do ataków na resztę sieci i jej systemy.
- **Terminowe aktualizacje firmware'u i zarządzanie poprawkami**: wiele ataków na IoT wykorzystuje znane podatności, które producenci już załatali. Opóźniona instalacja aktualizacji i poprawek bezpieczeństwa pozwala atakującym wykorzystywać nowo odkryte podatności, które zostały już usunięte w najnowszych aktualizacjach. Aby zamknąć te luki, niezbędne jest wprowadzenie zdyscyplinowanego procesu aktualizacji i zarządzania poprawkami. Użytkownicy powinni traktować urządzenia IoT tak samo jak komputery i smartfony – regularna aktualizacja urządzeń to pierwsza linia obrony przed nowymi zagrożeniami.
- **Wzmocnienie uwierzytelniania i kontroli dostępu**: słabe lub domyślne hasła są częstym punktem wejścia dla malware IoT. Niezbędne jest wdrożenie skutecznych mechanizmów kontroli dostępu, ograniczających dostęp do sieci, urządzeń, serwerów i aplikacji IoT wyłącznie do uprawnionych urządzeń i użytkowników. Stosowanie silnych, unikalnych haseł dla każdego urządzenia i włączenie uwierzytelniania dwuskładnikowego może znacząco zmniejszyć ryzyko nieuprawnionego dostępu.
- **Wdrożenie monitorowania sieci i wykrywania anomalii**: zaawansowane narzędzia monitorowania sieci, wykrywające nietypowy ruch lub nietypowe zachowanie urządzeń IoT, są kluczowe dla wczesnej identyfikacji zagrożeń. Systemy oparte na uczeniu maszynowym mogą

pomóc oznaczyć potencjalne malware, zanim się rozprzestrzeni. Zaletą narzędzi monitorowania sieci i wykrywania anomalii opartych na uczeniu maszynowym jest to, że – w przeciwieństwie do narzędzi sygnaturowych – potrafią wykrywać nowe ataki.

- **Prowadzenie kompleksowej ewidencji urządzeń**: aktualna ewidencja wszystkich urządzeń IoT w sieci jest kluczowa dla zarządzania bezpieczeństwem. Powinna obejmować typy urządzeń, wersje firmware'u i znane podatności. Innymi słowy, każde urządzenie łączące się z siecią IoT powinno być identyfikowalne, skutecznie monitorowane i zabezpieczone, aby zapewnić bezpieczeństwo sieci. Potrzeba widoczności urządzeń wynika z tego, że nie można chronić czegoś, o czego istnieniu się nie wie i czego się nie widzi. Pełna ewidencja urządzeń stanowi podstawę każdego skutecznego planu bezpieczeństwa IoT.
- **Przeprowadzanie ocen bezpieczeństwa dostawców**: część podatności urządzeń IoT jest wprowadzana przez różnych interesariuszy cyklu rozwoju urządzeń IoT – od producenta sprzętu po twórców firmware'u i oprogramowania. Przed wprowadzeniem nowych urządzeń IoT organizacje powinny dokładnie ocenić dostawców i ich produkty, w tym ich środki bezpieczeństwa, polityki aktualizacji i historię usuwania podatności.
- **Edukacja i budowanie świadomości pracowników**: błąd ludzki jest jedną z głównych przyczyn incydentów bezpieczeństwa. Regularne szkolenia z dobrych praktyk bezpieczeństwa IoT pomagają pracownikom rozpoznawać zagrożenia i rozumieć swoją rolę w utrzymaniu bezpiecznego środowiska. Szkolenia pracowników zapewniają też przestrzeganie polityk bezpieczeństwa IoT podczas wdrażania i eksploatacji sieci i systemów IoT.

1)

Lauren Ballejos, How to Secure IoT Devices, 2024

2) 4)

Duplocloud, Defending Against IoT Threats: A Comprehensive Guide to IoT Malware Protection, https://duplocloud.com/blog/defending-against-iot-threats-a-comprehensive-guide-to-iot-malware-protection/

3)

Kyle Chin, What is the Internet of Things (IoT)? Definition and Critical Risks, https://www.upguard.com/blog/internet-of-things-iot, 2024

From:
https://dokuwiki.zmitac.aei.polsl.pl/ - **RAU6 Dokuwiki**

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures:typical_attack_patterns_on_iot_systems?rev=1793526468

Last update: **2026/11/01 10:47**