Table of Contents

1. Podatności Systemów IoT 2
1.1. Typowe podatności IoT 2
1.2. Strategie ograniczania podatności IoT 5

1. Podatności Systemów IoT

Aby zabezpieczyć systemy IoT i zapewnić poufność, prywatność oraz integralność danych, należy zrozumieć różne podatności, czyli słabości bezpieczeństwa systemów IoT, które mogą wykorzystać cyberprzestępcy. Większość podatności IoT występuje w warstwie fizycznej architektury referencyjnej IoT, obejmującej urządzenia IoT. Jak omówiono w poprzednich rozdziałach, urządzenia IoT mają ograniczone zasoby obliczeniowe i komunikacyjne, co utrudnia wdrożenie silnych protokołów i algorytmów bezpieczeństwa, które zapewniają spełnienie wymagań poufności, integralności, dostępności, rozliczalności i niezaprzeczalności danych i systemów IoT. W efekcie środki bezpieczeństwa projektowane i wdrażane dla danych i systemów IoT często są niewystarczające, co czyni systemy IoT podatnymi na wiele rodzajów cyberataków i łatwiejszymi do skompromitowania.

Ponieważ urządzenia IoT są integrowane z istniejącymi systemami firm, urządzeniami osobistymi, systemami domowymi i infrastrukturą krytyczną, stają się atrakcyjnym celem dla cyberprzestępców i są narażone na ciągłe ataki. Cyberprzestępcy stale poszukują słabości bezpieczeństwa (podatności) urządzeń IoT, które mogą wykorzystać do kradzieży lub zniszczenia danych, obniżenia jakości usług lub skoordynowania urządzeń w celu przeprowadzenia ataków na dużą skalę, takich jak ataki DoS/DDoS, bądź dowolnych ataków kompromitujących inne systemy, zwłaszcza infrastrukturę krytyczną.

1.1. Typowe podatności IoT

Biorąc pod uwagę poważne ryzyko, jakie słabości bezpieczeństwa systemów IoT stwarzają dla usług IoT i innych usług w społeczeństwie – w tym możliwość utraty życia ludzkiego lub zakłócenia funkcjonowania społeczeństwa – kluczowe jest identyfikowanie i usuwanie podatności w systemach IoT, zanim wykorzystają je cyberprzestępcy. Rozpowszechnienie różnorodnych urządzeń IoT w wielu sektorach, przy niewielkiej standaryzacji i regulacjach lub ich braku, zwiększyło liczbę podatności i powierzchnię ataku, które cyberprzestępcy mogą wykorzystać do kompromitacji danych zbieranych przez urządzenia IoT oraz istniejących systemów. Do podatności IoT należą m.in. (rysunek 1):



Fig. 1: Typowe podatności IoT

- **Hasła wbudowane w urządzenia IoT**: aby umożliwić zdalne wsparcie techniczne, inżynierowie i deweloperzy IoT muszą mieć zdalny dostęp do urządzeń w celu ich konfiguracji podczas wdrożenia oraz rozwiązywania problemów podczas eksploatacji i utrzymania sieci IoT z wieloma urządzeniami. Ułatwia to cyberprzestępcom dostęp do urządzeń IoT i wykorzystywanie ich do złośliwych celów.
- **Brak uwierzytelniania**: niektórzy producenci IoT dostarczają urządzenia bez jakiegokolwiek mechanizmu uwierzytelniania, co czyni je podatnymi na nieuprawniony dostęp ze strony atakujących i narusza poufność, prywatność oraz integralność danych IoT. Atakujący mogą też przejąć urządzenia i wykorzystać je do celów złośliwych. Urządzenia bez jakiejkolwiek formy

uwierzytelniania mogą więc stać się elementem powierzchni ataku, wykorzystywanym do zaawansowanych ataków na systemy IoT oraz inne krytyczne zasoby.

- **Słabe hasła**: aby urządzenia były łatwe w użyciu, producenci dostarczają je z domyślnymi zabezpieczeniami, takimi jak hasła wbudowane na stałe, których użytkownik nie może zmienić, domyślne nazwy użytkownika i hasła lub uproszczone metody logowania. Ponieważ dane uwierzytelniające producenta są proste i nigdy nie są zmieniane, atakujący często wykorzystują je, aby uzyskać dostęp do urządzenia, naruszając poufność i integralność danych. Mogą też używać tych urządzeń do dalszych ataków.
- **Tylne furtki (backdoory)**: większość producentów IoT tworzy ukryte mechanizmy dostępu zwane tylnymi furtkami (identyfikator/hasło lub otwarte porty), aby móc serwisować urządzenia. Atakujący często uzyskują dostęp do tych furtek i wykorzystują je do przeprowadzania ataków (np. botnetów i innych ataków z użyciem złośliwego oprogramowania).
- **Brak instalacji poprawek i aktualizacji bezpieczeństwa:** niektórzy producenci IoT nie zapewniają prostego i skutecznego sposobu instalowania poprawek i aktualizacji bezpieczeństwa, co utrudnia dostawcom usług IoT usuwanie podatności, zanim cyberprzestępcy je wykorzystają. W przeciwieństwie do tradycyjnych systemów komputerowych, wyposażonych w mechanizmy ciągłej instalacji aktualizacji bezpieczeństwa i powiadamiania o zmianach, urządzenia IoT są proste i nie mają tych funkcji, co czyni je podatnymi na cyberataki. Ze względu na swoją prostotę urządzenia IoT są też podatne na ataki takie jak nieuprawnione aktualizacje oprogramowania i firmware'u. Producenci IoT często nawet nie publikują poprawek ani aktualizacji oprogramowania swoich urządzeń, co wykorzystują atakujący. A nawet jeśli poprawki i aktualizacje są publikowane, użytkownicy mają trudności z ich instalacją, przez co większość podatności tych urządzeń nigdy nie zostaje załatana.
- **Słabo chronione usługi sieciowe**: bezprzewodowy kanał komunikacyjny między urządzeniem IoT a punktem dostępowym lub bramą stanowi istotną powierzchnię ataku, często wykorzystywaną do ataków na urządzenia IoT. Niezaszyfrowane kanały komunikacyjne są jedną z podatności sieciowych wynikających z braku zabezpieczeń usług sieciowych. Ze względu na ograniczenia energii, kosztów i mocy obliczeniowej większość producentów IoT nie wdraża mechanizmów kryptograficznych zapewniających bezpieczną komunikację. Ułatwia to atakującym przeprowadzanie ataków typu man-in-the-middle w sieciach IoT. Bez ochrony komunikacji między urządzeniami IoT a serwerami poufne dane, w tym dane uwierzytelniające, mogą zostać skompromitowane i wykorzystane do dalszych ataków, np. DoS/DDoS. Istnieją też zbędne usługi, takie jak niechronione porty, które mogą zostać wykorzystane przez cyberprzestępców. Niewyłączenie nieużywanych portów lub niezabezpieczenie używanych portów zaporą sieciową czyni je podatnymi na cyberataki.
- **Ekspozycja w Internecie**: niektóre urządzenia IoT są podłączone bezpośrednio do Internetu bez zapór sieciowych czy jakichkolwiek mechanizmów bezpieczeństwa i są narażone na ataki.
- **Niechronione interfejsy**: część podatności systemów IoT wynika z obecności słabo zabezpieczonych lub niechronionych interfejsów (np. webowych, API zaplecza, interfejsów chmury i mgły), co czyni urządzenia IoT i inne zasoby podatnymi na cyberataki. Słabe (a czasem brak) mechanizmy uwierzytelniania, autoryzacji i kryptograficzne zabezpieczenia czynią komunikację przez te interfejsy podatną na cyberataki, ponieważ brakuje kontroli dostępu do istotnych zasobów, rozliczalności oraz ochrony danych i systemów przed kompromitacją.
- **Używanie przestarzałych komponentów**: czasem producenci urządzeń IoT nie są w stanie usunąć wykrytych podatności sprzętowych lub programowych, przez co dostawcy usług IoT muszą nadal używać tych urządzeń bez poprawek usuwających znane luki. Takie przestarzałe urządzenia ze znanymi podatnościami stają się łakomym kąskiem dla cyberprzestępców, którzy mogą je wykorzystać, skompromitować i uszkodzić systemy i zasoby IoT.
- **Podatności łańcucha dostaw**: łańcuch dostaw IoT obejmuje producentów (układów półprzewodnikowych, części sprzętowych, urządzeń IoT, oprogramowania), dystrybutorów, sprzedawców, dostawców usług i użytkowników. Podatności mogą zostać wprowadzone do

urządzeń IoT na dowolnym etapie łańcucha dostaw. Może to być skompromitowane oprogramowanie lub sprzęt, zmanipulowany lub zainstalowany w celu wprowadzenia słabości bezpieczeństwa, które czynią urządzenia IoT podatnymi na ataki lub łatwymi do skompromitowania. Celem ataków na łańcuch dostaw może być cyberszpiegostwo (kradzież lub kompromitacja danych) oraz wykorzystanie urządzeń do przeprowadzania zaawansowanych ataków cybernetycznych. Źle zaprojektowane oprogramowanie zewnętrzne (np. biblioteki, sterowniki, jądra systemu lub komponenty sprzętowe) zainstalowane na urządzeniach lub stanowiące część innych aplikacji lub firmware'u może wprowadzać podatności, które mogą zostać ostatecznie wykorzystane do kompromitacji urządzeń lub ataków na infrastrukturę. Jednym ze źródeł podatności łańcucha dostaw jest stosowanie zewnętrznych komponentów programowych i sprzętowych bez odpowiedniego sprawdzenia ich pod kątem podatności i usunięcia ich przed włączeniem komponentów do produktów IoT. Zdarza się też, że twórcy urządzeń IoT kopiują kod ze źródeł internetowych do swoich programów, aby uzyskać pożądaną funkcjonalność. Inną formą podatności łańcucha dostaw jest wdrażanie przez producentów lub deweloperów (podczas instalacji urządzenia) bardzo niewielu mechanizmów bezpieczeństwa lub ich brak, co czyni urządzenia podatnymi na ataki. Jednym z istotnych problemów ataków na łańcuch dostaw jest to, że użytkownicy nie są świadomi tych słabości ani tego, ile urządzeń różnych producentów w ich infrastrukturze je posiada.

- **Przestarzałe oprogramowanie układowe (firmware)**: po wdrożeniu urządzeń IoT niektórzy dostawcy usług IoT przez długi czas nie aktualizują działającego na nich firmware'u ani oprogramowania. Niektórzy nie aktualizują go wcale, pozostawiając podatności, które mogą zostać wykorzystane.
- **Słabe strategie i polityki zarządzania urządzeniami**: niektóre urządzenia IoT są wdrażane bez unikalnych identyfikatorów umożliwiających ich śledzenie, monitorowanie i zarządzanie. W rezultacie część węzłów IoT funkcjonuje w infrastrukturze bez odpowiedniego monitorowania i zarządzania, które pozwoliłoby wykrywać i usuwać podatności. Jeśli dział cyberbezpieczeństwa nie wie o istnieniu niektórych węzłów IoT, nie może ich chronić, co pozostawia je podatnymi na ataki. Niektórzy administratorzy IT zaniedbują węzły IoT, nie poświęcając im takich samych wysiłków jak tradycyjnym węzłom obliczeniowym i sieciowym, i nie umieszczają ich w ewidencji chronionych zasobów; w efekcie urządzenia te są rzadko aktualizowane i konserwowane w sposób zapobiegający ich kompromitacji lub wykorzystaniu.
- **Słabe protokoły zarządzania kluczami**: jeśli klucze kryptograficzne zostaną skompromitowane, urządzenia IoT stają się podatne na ataki typu man-in-the-middle i inne ataki, które mogą zakłócić działanie usług IoT lub skompromitować dane IoT.
- **Słabe fizyczne zabezpieczenie urządzeń IoT**: węzły IoT są często rozmieszczane na zewnątrz lub w odległych lokalizacjach, co czyni je łatwo dostępnymi dla złodziei. Przestępca może fizycznie uszkodzić urządzenie, wydobyć z niego informacje lub zmanipulować je tak, aby nie mogło wykonywać swoich normalnych funkcji. Na przykład atakujący może skopiować dane zapisane w pamięci urządzenia, a nawet wymienić niektóre komponenty na skompromitowane, co może dać mu zdalny dostęp do urządzenia.
- **Podatności zarządzania danymi**: w przypadku wdrożeń IoT na dużą skalę, liczących tysiące, dziesiątki tysięcy lub setki tysięcy węzłów, ilość zbieranych danych jest tak ogromna, że tradycyjne systemy zarządzania danymi mogą nie być w stanie bezpiecznie ich obsłużyć. Poufność i integralność danych mogą zostać naruszone z powodu podatności w zakresie przechowywania, przetwarzania i odczytu danych w systemach zarządzania danymi, które pogłębiają się wraz ze skalowaniem zasobów IoT.
- **Standaryzacja podatności**: mimo wielu działań na rzecz standaryzacji w ekosystemie IoT nadal występują problemy ze standaryzacją i interoperacyjnością. Zaprojektowanie zintegrowanego systemu bezpieczeństwa chroniącego urządzenia IoT różnych producentów, o zróżnicowanych podatnościach, jest trudne. Różnorodność urządzeń IoT różnych producentów utrudnia ich integrację z istniejącymi ramami bezpieczeństwa, co skutkuje słabym

bezpieczeństwem IoT lub traktowaniem bezpieczeństwa jako oczywistość, pozostawiając urządzenia podatne na ataki.

1.2. Strategie ograniczania podatności IoT

Choć nie da się wyeliminować wszystkich podatności IoT, istnieją dobre praktyki, które utrudniają ich wykorzystanie do kompromitacji danych i systemów IoT. Do środków i technik bezpieczeństwa, które można zastosować w celu wzmocnienia bezpieczeństwa IoT i ograniczenia ryzyka ataku wynikającego z wykorzystania którejkolwiek z podatności, należą m.in. (rysunek 2):



Fig. 2: Strategie ograniczania podatności IoT

- **Stosowanie zasad security by design**: na każdym etapie cyklu życia systemów IoT – od projektowania, produkcji, wdrożenia, eksploatacji i utrzymania po wycofanie i utylizację – należy uwzględniać i wdrażać środki kontroli bezpieczeństwa, aby dane IoT nie zostały skompromitowane, a urządzenia nie zostały wykorzystane do zaawansowanych ataków. Dzięki temu każdy interesariusz w łańcuchu dostaw urządzeń IoT jest świadomy różnych podatności i wdraża odpowiednie środki w celu ich usunięcia i uniemożliwienia ich wykorzystania. Security by design wymaga ścisłej współpracy projektantów i inżynierów IoT z ekspertami ds. cyberbezpieczeństwa, tak aby bezpieczeństwo było jednym z kluczowych kryteriów projektowych. Zanim urządzenia IoT trafią na rynek i zostaną wdrożone, należy przeprowadzić wymagającą ocenę bezpieczeństwa (np. testy penetracyjne lub skanowanie podatności), aby zidentyfikować potencjalne luki w sprzęcie, oprogramowaniu i protokołach komunikacyjnych IoT. Wykryte podatności należy usunąć jak najszybciej.
- **Opracowanie i egzekwowanie polityk silnych haseł**: urządzenia z hasłami wbudowanymi na stałe nie powinny być wdrażane w infrastrukturze IoT; zamiast wbudowywać hasła, producenci powinni być zobowiązani do zapewnienia użytkownikom możliwości utworzenia własnych nazw użytkownika i haseł. Domyślne nazwy użytkownika i hasła urządzeń IoT, punktów dostępowych i bram należy zmienić. Hasła powinny być wystarczająco silne, a proste i nadużywane hasła należy wykluczyć. Kluczowe jest stosowanie nowych, unikalnych i złożonych haseł zgodnych z polityką silnych haseł. Należy wdrożyć skuteczne polityki zarządzania hasłami, umożliwiające ich szybką i bezpieczną zmianę i resetowanie.
- **Obowiązkowe uwierzytelnianie**: każde urządzenie IoT powinno być zobowiązane do uwierzytelnienia przed dołączeniem do sieci, a urządzenia bez mechanizmów uwierzytelniania należy odrzucać. Oznacza to, że każde urządzenie IoT musi być identyfikowalne i może zostać dopuszczone do sieci dopiero po prawidłowym uwierzytelnieniu. Jeśli to możliwe, należy wdrożyć uwierzytelnianie wieloskładnikowe (np. dwuskładnikowe). Środki te zapewnią, że dostęp do zasobów IoT mają wyłącznie uprawnieni użytkownicy i urządzenia, co zmniejsza ryzyko naruszenia bezpieczeństwa.
- **Wdrożenie skutecznych mechanizmów bezpieczeństwa sieci**: usługi i protokoły sieciowe IoT powinny być odpowiednio zabezpieczone. Należy wyłączyć przekierowanie portów i zamknąć niepotrzebne porty. Dostęp do sieci IoT powinien wymagać uwierzytelnienia. Należy też stosować narzędzia bezpieczeństwa sieci, takie jak zapory sieciowe, systemy wykrywania włamań i systemy zapobiegania włamaniom, do inspekcji ruchu z różnych źródeł i blokowania

źródeł złośliwego ruchu. Do zabezpieczenia kanałów komunikacyjnych należy stosować bezpieczne protokoły sieciowe, takie jak TLS/SSL, oraz protokoły kryptograficzne. Należy również stosować techniki segmentacji sieci, aby odizolować sieci IoT od reszty infrastruktury oraz od siebie nawzajem (zwłaszcza te zintegrowane z krytycznymi zasobami), co pozwala ograniczyć potencjalne ataki do izolowanych segmentów i zmniejszyć ryzyko kompromitacji krytycznych zasobów.

- **Regularna aktualizacja oprogramowania i firmware'u**: regularna instalacja aktualizacji oprogramowania i firmware'u zapewnia zastosowanie najnowszych poprawek bezpieczeństwa łatających luki, co zmniejsza ryzyko wykorzystania istniejących podatności. Producenci powinni maksymalnie uprościć proces instalacji aktualizacji lub poprawek. Najlepiej, aby był automatyczny lub wymagał jednego kliknięcia, bez skomplikowanych procedur instalacji.
- **Nieprzedkładanie wygody użytkowania nad bezpieczeństwo**: urządzenia typu plug-and-play wymagają niewielu dodatkowych ustawień lub konfiguracji albo nie wymagają ich wcale, co wprowadza podatności, ponieważ łatwo je wykorzystać. Należy unikać urządzeń plug-and-play i innych systemów, które są łatwiejsze we wdrożeniu i użyciu, ale również łatwiejsze do skompromitowania.
- **Zabezpieczenie interfejsów API**: interfejsy API umożliwiające komunikację między urządzeniami IoT, punktami zbierania danych i interfejsami użytkownika powinny być odpowiednio zabezpieczone poprzez silne uwierzytelnianie (np. OAuth), szyfrowanie (HTTPS) i mechanizmy kontroli dostępu (np. walidację wszystkich danych wejściowych w celu zapobiegania atakom wstrzykiwania) [1)]. Wdrożenie technik bezpieczeństwa API uniemożliwia nieuprawnionym urządzeniom i użytkownikom dostęp do urządzeń IoT oraz kompromitację systemów lub danych IoT.
- **Weryfikacja firmware'u mechanizmem bezpiecznego rozruchu (Secure Boot)**: zapewnia, że urządzenie uruchamia autoryzowany firmware, chroniąc je przed złośliwym oprogramowaniem i nieautoryzowanymi modyfikacjami firmware'u. Urządzenie weryfikuje podpis cyfrowy firmware'u podczas rozruchu, co zapobiega uruchomieniu nieautoryzowanego lub zmodyfikowanego firmware'u i zapewnia integralność urządzenia. Producenci powinni więc wbudowywać mechanizmy weryfikacji autentyczności firmware'u przy uruchamianiu oraz bezpiecznej aktualizacji urządzenia, co zapewni bezpieczeństwo urządzeń przez cały cykl ich życia [2)].
- **Stosowanie bezpiecznych systemów zarządzania kluczami**: klucze kryptograficzne powinny być odpowiednio zarządzane. W przypadku asymetrycznego schematu szyfrowania zabezpieczającego komunikację z serwerami w infrastrukturze IoT należy stosować PKI i infrastrukturę certyfikatów cyfrowych, aby zapewnić bezpieczne zarządzanie kluczami i utrzymać zaufanie.
- **Ograniczanie ryzyka przestarzałych komponentów**: podatne urządzenia należy zaktualizować, wymienić lub usunąć z sieci. Można to osiągnąć, wdrażając skuteczny system monitorowania, zapewniający ściślejszy nadzór i kontrolę oraz umożliwiający szybkie wykrywanie i usuwanie podatności.
- **Wdrażanie i egzekwowanie polityk zero-trust**: oznacza to, że wszystkie urządzenia i użytkownicy wewnątrz i na zewnątrz sieci/infrastruktury IoT muszą być stale weryfikowani, autoryzowani i oceniani, aby mieć pewność, że nie stanowią zagrożenia i nie wprowadzają podatności. Z czasem użytkownicy lub urządzenia mogą zostać skompromitowani i stać się zagrożeniem dla krytycznych zasobów. Dlatego zautomatyzowane polityki zero-trust są kluczowe i muszą być egzekwowane.
- **Wykorzystanie narzędzi uczenia maszynowego**: należy stosować narzędzia uczenia maszynowego do automatyzacji zadań bezpieczeństwa, takich jak wykrywanie podatności i ataków oraz stosowanie technik ich łagodzenia. Narzędzia AI są praktycznym sposobem wykrywania podatności i ataków w sieciach IoT, szczególnie użytecznym w bardzo dużych sieciach. Włączono je do systemów bezpieczeństwa, takich jak systemy SIEM, w celu

wykrywania podatności, zagrożeń i ataków.
- **Szkolenie personelu**: ciągłe szkolenie projektantów, deweloperów i inżynierów IoT w zakresie dobrych praktyk bezpieczeństwa zapewni, że nie będą projektować, produkować ani wdrażać urządzeń z podatnościami wynikającymi z błędów lub nieuwagi w procesie projektowania, produkcji i wdrażania.
- **Ciągła edukacja konsumentów**: wielu producentów zaniedbuje funkcje bezpieczeństwa, ponieważ użytkownicy skupiają się głównie na pożądanej funkcjonalności, łatwości użycia i cenie, a rzadko zwracają uwagę na bezpieczeństwo. Użytkownicy czasem niewłaściwie korzystają z urządzeń i nie instalują aktualizacji ani poprawek. Ciągła edukacja użytkowników może przynieść korzyści.
- **Fizyczna ochrona urządzeń**: należy podjąć odpowiednie środki, aby urządzenie nie zostało fizycznie skompromitowane, a jeśli do tego dojdzie – aby zdarzenie można było łatwo wykryć. Należy też zadbać o to, aby dane nie zostały skompromitowane, a urządzenie nie zostało wykorzystane do dalszych ataków.
- **Wdrażanie dobrych praktyk bezpieczeństwa cyber-łańcucha dostaw**: aby ograniczyć podatności łańcucha dostaw, należy stosować metody bezpiecznego cyklu życia oprogramowania, przeprowadzać dokładne przeglądy kodu ze źródeł wewnętrznych i zewnętrznych, unikać podrabianego sprzętu i oprogramowania z niezaufanych źródeł oraz weryfikować procesy projektowania i wytwarzania oprogramowania i sprzętu dostarczanych przez strony trzecie. Należy też sprawdzać procesy usuwania podatności przez dostawców [3].

[1] , [2]
Bruno Rossi, Top 10 IoT Vulnerabilities and How to Mitigate Them, https://sternumiot.com/iot-blog/top-10-iot-vulnerabilities-and-how-to-mitigate-them/
[3]
Anna Chung and Asher Davila, Risks in IoT Supply Chain, https://unit42.paloaltonetworks.com/iot-supply-chain/

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

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures:vulnerabilities_in_iot_systems?rev=1793542499

Last update: **2026/11/01 15:14**