Table of Contents

1. Wektory ataku na IoT 2
1.1. Wektor ataku, powierzchnia ataku i wektor zagrożenia w IoT 2
1.2. Wybrane wektory ataku na IoT 3
1.3. Strategie obrony przed znanymi wektorami ataku na IoT 5

1. Wektory ataku na IoT

W tym rozdziale omówiono pojęcia wektora ataku, powierzchni ataku i wektora zagrożenia w kontekście IoT, aby wyjaśnić różnice między tymi terminami, często używanymi zamiennie. Przedstawiono wybrane wektory ataku na IoT, które należy uwzględnić przy projektowaniu strategii cyberbezpieczeństwa dla sieci i systemów IoT, oraz strategie pozwalające eliminować lub ograniczać związane z nimi ryzyko.

1.1. Wektor ataku, powierzchnia ataku i wektor zagrożenia w IoT

Wektory ataku na IoT to różne metody, za pomocą których cyberprzestępcy mogą uzyskać dostęp do urządzeń IoT w celu przeprowadzenia cyberataków na infrastrukturę IoT, inną infrastrukturę informatyczną organizacji lub Internet jako całość. Umożliwiają one cyberprzestępcom wykorzystanie podatności do naruszenia poufności, integralności i dostępności wrażliwych danych. Minimalizacja liczby wektorów ataku jest niezbędna do ograniczenia ryzyka naruszenia bezpieczeństwa, które może kosztować organizację dużo pieniędzy i zaszkodzić jej reputacji.

Liczba wektorów ataku stale rośnie, ponieważ cyberprzestępcy opracowują liczne proste i wyrafinowane metody wykorzystywania nieusuniętych podatności oraz podatności typu zero-day w systemach i sieciach komputerowych. Nie istnieje więc jedno rozwiązanie ograniczające ryzyko wynikające z rosnącej liczby wektorów ataku w klasycznych systemach i sieciach komputerowych. Wraz ze wzrostem liczby urządzeń IoT podłączonych do Internetu rośnie też liczba wektorów ataku związanych z IoT, co wymaga opracowania holistycznej strategii cyberbezpieczeństwa, obejmującej zarówno tradycyjne wektory ataku (np. złośliwe oprogramowanie, wirusy, załączniki e-mail, strony internetowe, okna pop-up, komunikatory, wiadomości SMS, socjotechnikę, kradzież danych uwierzytelniających, wykorzystanie podatności i niewystarczającą ochronę przed zagrożeniami wewnętrznymi), jak i wektory wymierzone w systemy IoT (np. wykorzystanie podatności typowych dla IoT, takich jak słabe hasła lub ich brak, brak aktualizacji firmware'u i oprogramowania czy niezaszyfrowana komunikacja).

Aby bronić sieci i systemów IoT, kluczowe jest zrozumienie różnych sposobów, w jakie cyberprzestępca może uzyskać do nich nieuprawniony dostęp. Termin wektor zagrożenia jest często używany zamiennie z terminem wektor ataku. Wektor zagrożenia IoT to zbiór potencjalnych sposobów lub metod, za pomocą których cyberprzestępcy mogą naruszyć poufność, integralność lub dostępność danych i systemów IoT. W miarę rozrastania się sieci IoT i ich integracji z innymi systemami IT i cyberfizycznymi rośnie złożoność zarządzania nimi oraz liczba wektorów zagrożeń lub ataku. Wyeliminowanie wszystkich wektorów jest więc bardzo trudne, ale systemy cyberbezpieczeństwa IoT projektuje się tak, aby eliminować je wszędzie tam, gdzie to możliwe.

Powierzchnia ataku IoT to zbiór wektorów ataku, które cyberprzestępcy mogą wykorzystać do manipulowania siecią lub systemem IoT w celu naruszenia poufności, integralności lub dostępności danych. Obejmuje ona wszystkie wektory ataku na IoT dostępne cyberprzestępcom. Oznacza to, że im więcej wektorów ataku ma organizacja w wyniku wdrożenia systemów IoT, tym większa jest jej powierzchnia ataku – i odwrotnie. Dlatego organizacje muszą minimalizować liczbę wektorów ataku, aby minimalizować powierzchnię ataku.

1.2. Wybrane wektory ataku na IoT

Aby eliminować wektory ataku na IoT, należy zrozumieć ich naturę i źródła, a następnie opracować kompleksowe strategie bezpieczeństwa. W tym podrozdziale omówiono wektory ataku od warstwy percepcji po warstwę aplikacji. Do wektorów ataku, czyli sposobów, w jakie cyberprzestępcy mogą uzyskać nielegalny dostęp do sieci i systemów IoT (w celu naruszenia bezpieczeństwa danych lub przeprowadzenia dalszych ataków), należą m.in.:

- **Skompromitowane dane uwierzytelniające użytkowników lub urządzeń**: kompromitacja haseł jest jednym z najczęstszych sposobów uzyskiwania przez cyberprzestępców nieuprawnionego dostępu do systemów IoT. Wynika to częściowo z faktu, że niektórzy producenci dostarczają urządzenia z hasłami wbudowanymi na stałe lub domyślnymi, które rzadko są zmieniane. Daje to cyberprzestępcom łatwy dostęp do urządzeń IoT, które wykorzystują do zaawansowanych ataków, np. DDoS. Dane logowania do aplikacji mobilnych i webowych IoT mogą też zostać skompromitowane w wyniku wycieków danych, oszustw phishingowych, złośliwego oprogramowania i ataków siłowych.
- **Słabe algorytmy kryptograficzne**: wdrożenie silnych algorytmów kryptograficznych w urządzeniach IoT jest bardzo trudne ze względu na ograniczenia sprzętowe. Ułatwia to cyberprzestępcom dostęp do danych IoT przesyłanych bezprzewodowo. Łatwo też naruszyć poufność wrażliwych danych przechowywanych w urządzeniach IoT. Słabe algorytmy kryptograficzne (lub brak szyfrowania) zachęcają więc cyberprzestępców do prób uzyskania dostępu do danych IoT za pomocą ataków man-in-the-middle.
- **Otwarte porty komunikacyjne**: cyberprzestępcy mogą wykorzystać niezabezpieczone i niepotrzebnie otwarte porty (wirtualne punkty wejścia do urządzenia, przypisujące ruch sieciowy do określonej aplikacji lub procesu) do uzyskania dostępu do urządzenia. Każdy niepotrzebnie otwarty i niezabezpieczony port jest wektorem zagrożenia, który cyberprzestępcy mogą wykorzystać do ataku na urządzenia, serwery i aplikacje IoT.
- **Błędna konfiguracja**: źle skonfigurowane urządzenia IoT, urządzenia sieciowe, serwery, węzły obliczeniowe i aplikacje mogą stanowić słabe punkty, które cyberprzestępcy wykorzystują do atakowania sieci i systemów IoT. Wykorzystanie podatności wynikających z błędnej konfiguracji jest więc jednym ze sposobów uzyskania nieuprawnionego dostępu do sieci i systemów IoT.
- **Podatności firmware'u**: ponieważ firmware i oprogramowanie IoT nie są regularnie aktualizowane w celu łatania luk i ochrony urządzeń przed nowo odkrytymi podatnościami, cyberprzestępcy mogą wykorzystać nieusunięte podatności firmware'u i oprogramowania do uzyskania nieuprawnionego dostępu do urządzeń i danych IoT. Jest to jeden ze sposobów łatwej kompromitacji bezpieczeństwa sieci i systemów IoT.
- **Podatności zero-day**: podatności (wady sprzętu lub oprogramowania) są regularnie odkrywane – codziennie, co tydzień, co miesiąc lub co rok. Jeśli istnieją podatności, dla których producent nie wydał poprawki bezpieczeństwa lub użytkownik nie zainstalował aktualizacji, atakujący prawdopodobnie je wykorzystają do uzyskania nieuprawnionego dostępu do sieci i systemów IoT. Atak zero-day wykorzystuje nieznane podatności lub wady oprogramowania przed wydaniem poprawki. Wykorzystanie nieusuniętych znanych podatności jest zatem jednym z wektorów ataku stosowanych przez cyberprzestępców do kompromitacji sieci i systemów IoT.
- **Cross-site scripting (XSS)**: wektor ataku wykorzystujący przeglądarkę, pozwalający wstrzyknąć złośliwy kod do aplikacji webowej, za pomocą której użytkownicy korzystają z usług IoT. W wielu zastosowaniach IoT użytkownicy końcowi korzystają z usług IoT hostowanych na platformach chmurowych za pośrednictwem aplikacji webowych i mobilnych w przeglądarce. Cyberprzestępcy mogą wstrzykiwać złośliwy kod do aplikacji webowych IoT, przekierowywać użytkowników na fałszywe strony i nakłaniać przeglądarkę do wykonania złośliwego kodu, który pobiera malware infekujące urządzenia użytkowników. Wstrzyknięty kod może uruchomić

zainfekowany skrypt, infekując urządzenie użytkownika i wykradając informacje. Ponieważ usługi IoT są udostępniane użytkownikom przez aplikacje webowe, ten wektor ataku będzie celem cyberprzestępców.

- **Wstrzykiwanie SQL (SQL injection)**: wiele danych IoT jest przechowywanych w ustrukturyzowanych bazach danych, do których użytkownicy i inne aplikacje uzyskują dostęp przez aplikacje webowe i mobilne. Dane w ustrukturyzowanych bazach są często zarządzane za pomocą SQL (ang. *Structured Query Language*) – języka służącego do administrowania bazą danych lub interakcji z nią w celu przechowywania, odczytu i modyfikacji danych. Wektor ataku SQL injection polega na wykorzystaniu znanych podatności do wstrzyknięcia złośliwych instrukcji SQL do aplikacji, aby nakłonić serwer do umożliwienia atakującemu nielegalnego odczytu, zmiany lub usunięcia informacji. W zastosowaniach IoT, w których dane z czujników są zbierane i przechowywane w ustrukturyzowanych bazach danych, ten wektor ataku jest prawdopodobnym celem.
- **Ataki rozproszonej odmowy usługi (DDoS)**: ten wektor ataku polega na wykorzystaniu botów do infekowania urządzeń IoT i utworzenia botnetu (sieci botów), którym można sterować, aby zalać bramy, usługi, centra danych i aplikacje webowe IoT ogromną ilością ruchu lub żądań. Celem ataku jest doprowadzenie do awarii bram, usług, centrów danych i aplikacji webowych IoT, pozbawiając użytkowników dostępu do usług IoT. Atakujący przejmuje wiele urządzeń IoT, tworzy botnet i kieruje ruch z tych urządzeń do bram, usług, centrów danych i aplikacji webowych IoT, aby zakłócić usługi IoT.
- **Przejmowanie sesji (session hijacking)**: cyberprzestępcy mogą uzyskać nieuprawniony dostęp do wrażliwych danych IoT poprzez przejęcie sesji. Gdy użytkownicy IoT logują się do usług IoT, otrzymują klucz sesji lub plik cookie, dzięki czemu nie muszą logować się ponownie. Atakujący może przejąć ten plik cookie i wykorzystać go do uzyskania dostępu do wrażliwych informacji IoT [1)].
- **Infekcja złośliwym oprogramowaniem**: ten wektor ataku polega na wykorzystaniu złośliwego oprogramowania (malware) zaprojektowanego w celu przejęcia kontroli nad siecią lub systemem IoT. Malware może uszkadzać i wykradać dane, a także służyć do przeprowadzania ataków na wiele urządzeń IoT i inne systemy. Przykładami malware, które może być wymierzone w sieci i systemy IoT, są ransomware (szyfrujące cenne dane IoT lub dane użytkowników IoT, aby pozbawić ich legalnego dostępu do czasu zapłacenia okupu) oraz trojany (tworzące tylną furtkę dającą atakującym nieuprawniony dostęp do sieci i systemów IoT).
- **Phishing**: ten wektor ataku może być wymierzony w pracowników organizacji IoT lub użytkowników w celu przejęcia ich danych logowania. Wykorzystuje strategie socjotechniczne, w których z celem kontaktuje się – przez e-mail, telefon lub SMS – ktoś podszywający się pod współpracownika lub instytucję, aby nakłonić go do przekazania wrażliwych danych, danych uwierzytelniających lub danych osobowych (PII). Jest to jeden z najczęściej stosowanych wektorów ataku w celu uzyskania nieuprawnionego dostępu do wrażliwych informacji, a także punkt wyjścia wielu form ataków, takich jak ransomware (często rozpoczynany kampanią phishingową) i spyware (malware przekazujące atakującym wrażliwe dane IoT).
- **Atak siłowy (brute-force)**: kolejny wektor ataku, mający na celu kompromitację danych uwierzytelniających i kluczy szyfrujących w celu uzyskania nieuprawnionego dostępu do danych IoT. Może być przeprowadzany metodą prób i błędów w celu odgadnięcia hasła lub klucza szyfrującego. Jeśli hasło i klucz szyfrujący nie są wystarczająco silne, atakujący może nielegalnie uzyskać dostęp do urządzeń IoT. Stosowanie haseł domyślnych i słabych schematów szyfrowania w urządzeniach IoT czyni je podatnymi na takie ataki.
- **Ataki fizyczne**: ten wektor ataku obejmuje fizyczny dostęp przeciwnika do urządzenia IoT. Jeśli atakujący może fizycznie dostać się do wdrożonych urządzeń IoT, może wykraść wrażliwe dane, skompromitować urządzenia, a następnie wykorzystać je do ataków na sieci IoT i inne systemy.
- **Atak wewnętrzny (insider attack)**: należy również uwzględnić, że uprawnieni użytkownicy

lub pracownicy mogą zdecydować się na przekazanie wrażliwych danych IoT podmiotom zewnętrznym, naruszając ich poufność. Osoba z wewnątrz może też usunąć wrażliwe dane – celowo lub przypadkowo. Ten wektor ataku należy uwzględnić przy projektowaniu strategii cyberbezpieczeństwa dla sieci i systemów IoT.
- **Wykorzystanie podatności łańcucha dostaw**: ten wektor ataku polega na wykorzystaniu podatności występujących w sprzęcie i oprogramowaniu dostarczanym przez strony trzecie. Ataki mogą być wymierzone w podatności, których dostawca sprzętu lub oprogramowania mógł nie wykryć. Podatności produktów zewnętrznych mogą więc stać się punktami wejścia dla atakujących do sieci i systemów IoT.

Omówione wektory ataku można podzielić na dwie kategorie: pasywne i aktywne. Pasywne wektory ataku pozwalają atakującym uzyskać nieuprawniony dostęp do sieci i systemów IoT bez ingerencji w ich działanie. Przykładami są phishing i inne wektory oparte na socjotechnice. Aktywne wektory ataku zakłócają natomiast działanie sieci i systemu IoT. Przykładami tej kategorii są ataki DDoS, ataki siłowe, ataki z użyciem złośliwego oprogramowania itp.

1.3. Strategie obrony przed znanymi wektorami ataku na IoT

Aby przeciwdziałać typowym wektorom ataku, należy zrozumieć naturę ich wykorzystania – zarówno pasywnego, jak i aktywnego. Większość takich ataków ma pewne wspólne cechy:

- Atakujący najpierw identyfikują cele, które zamierzają zaatakować.
- Atakujący wykorzystują strategie socjotechniczne, złośliwe oprogramowanie, phishing i narzędzia do skanowania podatności, aby przeskanować sieć IoT i inne systemy informatyczne ofiary w celu zidentyfikowania podatności, które zamierzają wykorzystać.
- Atakujący wyznaczają zbiór wektorów ataku, które zamierzają wykorzystać, a następnie poszukują narzędzi potrzebnych do przeprowadzenia ataku.
- Atakujący uzyskują nieuprawniony dostęp do systemów IoT, wykradają wrażliwe dane, instalują złośliwe oprogramowanie i czasem eskalują atak, wykorzystując skompromitowane urządzenia do dalszych ataków na inne zasoby systemu.
- Atakujący starają się zatrzeć ślady, aby pozostać niewykrytymi. Wykradają też cenne dane lub wykorzystują zasoby obliczeniowe i komunikacyjne.

Niezbędne jest zidentyfikowanie i wdrożenie praktycznych narzędzi i polityk bezpieczeństwa przeciwdziałających wektorom ataku na IoT. Powinny one eliminować lub ograniczać ryzyko związane z wektorami ataku od warstwy percepcji po warstwę aplikacji. Do strategii obrony sieci i systemów IoT przed znanymi wektorami ataku należą m.in.:

- **Tworzenie bezpiecznych polityk uwierzytelniania**: zastąpienie haseł domyślnych silnymi hasłami. Zachęcanie do korzystania z menedżerów haseł, aby dane logowania były silne i odporne na ataki siłowe.
- **Wdrożenie silnych, energooszczędnych schematów kryptograficznych**: dane IoT przechowywane w urządzeniach IoT, urządzeniach obliczeniowych, urządzeniach sieciowych i bazach danych powinny być szyfrowane, czyli przekształcane do postaci niezrozumiałej dla podmiotów nieuprawnionych. Dane powinny być szyfrowane przed przesłaniem przez sieci komunikacyjne.
- **Zabezpieczenie portów komunikacyjnych**: wszystkie porty komunikacyjne powinny być zabezpieczone, a nieużywane – zamknięte, aby zapobiec ich wykorzystaniu.
- **Identyfikacja i usuwanie podatności**: należy stosować narzędzia monitorowania bezpieczeństwa do jak najszybszego wykrywania i usuwania podatności, aby nie zostały

wykorzystane do kompromitacji sieci i systemów IoT. Należy też instalować aktualizacje bezpieczeństwa niezwłocznie po ich wydaniu, aby szybko łatać podatności, które mogą być celem atakujących.

- **Egzekwowanie zasady najmniejszych uprawnień**: należy stosować zasadę najmniejszych uprawnień (ang. *principle of least privilege*), zgodnie z którą komponentom i procesom firmware'u przyznaje się tylko niezbędne uprawnienia. Użytkownicy również powinni otrzymywać jedynie wymagane uprawnienia w warstwach sieciowej i aplikacji. Gdy użytkownik nie potrzebuje już określonych uprawnień, należy je dezaktywować.
- **Identyfikowalność wszystkich urządzeń IoT w sieci**: aby uniknąć niepożądanego dostępu, każde urządzenie powinno mieć unikalną tożsamość, umożliwiającą jego skuteczne monitorowanie, i musi się uwierzytelnić, zanim uzyska dostęp do sieci i systemów IoT.
- **Stosowanie bezpiecznych metod wytwarzania oprogramowania**: kod powinien być dobrze przetestowany i poddany przeglądowi, aby wykryć i usunąć podatności. Należy też upewnić się, że biblioteki wykorzystywane do implementacji firmware'u urządzenia są bezpieczne i dobrze przetestowane. Przy programowaniu urządzeń IoT należy minimalizować kopiowanie gotowego kodu z Internetu, aby nie wprowadzać podatności.
- **Ciągłe monitorowanie urządzeń IoT**: utrzymywanie aktualnej ewidencji wszystkich podłączonych urządzeń i monitorowanie aktywności urządzeń IoT i innych systemów. Należy stosować zautomatyzowane narzędzia do wykrywania wszystkich podłączonych urządzeń i ich ciągłego skanowania w celu identyfikacji i usuwania podatności.
- **Regularne aktualizacje bezpieczeństwa i łatanie**: choć zarządzanie i instalowanie aktualizacji bezpieczeństwa oraz łatanie luk na tysiącach urządzeń bywa trudne, regularne aktualizacje i łatanie mogą realizować narzędzia do zdalnego zarządzania i monitorowania (ang. *Remote Management and Monitoring*, RMM). Zapewni to, że firmware i oprogramowanie urządzeń IoT będą zawsze aktualne.
- **Wycofywanie nieużywanych urządzeń IoT**: nieużywane urządzenia IoT należy usuwać z sieci IoT. Nieużywane urządzenie może nie być regularnie aktualizowane ani odpowiednio zabezpieczone, co stwarza ryzyko dla sieci i systemów IoT. Dlatego każde nieużywane urządzenie IoT oraz każdy inny nieużywany system sprzętowy lub programowy należy usunąć z sieci IoT.
- **Wdrożenie scentralizowanego zarządzania urządzeniami IoT**: zarządzanie urządzeniami IoT, ruchem sieciowym i przepływem danych z jednego miejsca ułatwia wykrywanie złośliwych zdarzeń i szybkie reagowanie na nie. Sprzyja też wdrażaniu zintegrowanych systemów cyberbezpieczeństwa, egzekwujących mechanizmy kontroli bezpieczeństwa w całej sieci.
- **Izolowanie urządzeń IoT od krytycznych zasobów systemowych i danych**: izolując urządzenia IoT od kluczowych zasobów systemowych i danych, zapewniamy, że nawet w przypadku kompromitacji sieci IoT atakujący nie będzie mógł przemieszczać się lateralnie w sieci i kompromitować krytycznych zasobów i sieci. Segmentacja sieci i izolacja urządzeń IoT od części sieci organizacji daje jej lepszą widoczność i kontrolę nad siecią.
- **Stosowanie aktualnego oprogramowania antymalware**: należy zapewnić aktualność oprogramowania antymalware, aby chroniło ono przed najnowszym złośliwym oprogramowaniem.
- **Wdrożenie narzędzi wykrywania ataków i reagowania na nie**: należy wdrożyć zautomatyzowane narzędzia wykrywania i reagowania, zdolne wykryć i zatrzymać cyberataki natychmiast po ich rozpoczęciu. Do projektowania zautomatyzowanych narzędzi zapobiegania, wykrywania i reagowania na ataki w IoT należy wykorzystywać AI i uczenie maszynowe.
- **Regularne i skuteczne szkolenia pracowników**: pracownicy powinni być dobrze przeszkoleni w obsłudze narzędzi cyberbezpieczeństwa oraz w rozpoznawaniu ataków socjotechnicznych i phishingowych, mających na celu nakłonienie ich do ujawnienia wrażliwych informacji.
- **Zapewnienie bezpieczeństwa łańcucha dostaw**: sprzęt i oprogramowanie stron trzecich

powinny być dobrze zabezpieczone, aby nie wprowadzały podatności, które mogą wykorzystać atakujący. Należy też zapewnić terminową aktualizację oprogramowania stron trzecich.
- **Podejście zero-trust**: należy stosować ramy bezpieczeństwa Zero Trust (ZT), zgodnie z którymi wszyscy użytkownicy – wewnątrz i na zewnątrz sieci organizacji – są uwierzytelniani, autoryzowani i stale weryfikowani pod kątem konfiguracji i stanu bezpieczeństwa, zanim otrzymają lub zachowają dostęp do sieci, systemów, aplikacji i danych IoT.
- **Podejście systemowe do bezpieczeństwa**: krajobraz bezpieczeństwa IoT jest bardzo złożony i stale się zmienia, wymagając integracji narzędzi i polityk bezpieczeństwa, ludzi oraz różnych rodzajów systemów informatycznych i cyberfizycznych. Najlepszym sposobem zarządzania złożonymi i dynamicznymi interakcjami komponentów tworzących infrastrukturę IoT jest podejście systemowe. Do modelowania i projektowania solidnych i bezpiecznych systemów cyberbezpieczeństwa dla sieci i systemów IoT można wykorzystać koncepcje z rozwijających się dziedzin myślenia systemowego, dynamiki systemów i inżynierii oprogramowania.

1)

Abi Tyas Tunggal, What is an Attack Vector? 16 Critical Examples, https://www.upguard.com/blog/attack-vector, 2024

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

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures:cybersecurity_issues_and_threats_in_iot_systems?rev=1793526306

Last update: **2026/11/01 10:45**