Table of Contents

1. Bezpieczeństwo systemów i Internetu Rzeczy 2
1.1. Bezpieczeństwo IoT 2

1. Bezpieczeństwo systemów i Internetu Rzeczy

1.1. Bezpieczeństwo IoT

Systemy i usługi IoT są szeroko stosowane w wielu branżach, takich jak ochrona zdrowia, rolnictwo, inteligentna produkcja, inteligentne systemy energetyczne, inteligentne systemy transportowe, logistyka (zarządzanie łańcuchem dostaw), inteligentne domy, inteligentne miasta oraz bezpieczeństwo i ochrona. Głównym celem włączania IoT do istniejących systemów w różnych branżach jest poprawa produktywności i efektywności. Mimo ogromnych korzyści płynących z integracji IoT z istniejącymi systemami w wielu sektorach, w tym w infrastrukturze krytycznej, istnieją obawy dotyczące podatności systemów IoT. Firmy coraz bardziej niepokoją się możliwymi zagrożeniami, jakie systemy IoT wprowadzają do ich infrastruktury, oraz sposobami ich ograniczania.

Jedną ze słabości urządzeń IoT jest łatwość ich kompromitacji. Wynika to z faktu, że niektórzy producenci urządzeń IoT nie wbudowują w nie mechanizmów bezpieczeństwa, co prowadzi do podatności łatwych do wykorzystania. Niektórzy producenci i deweloperzy koncentrują się na użyteczności urządzenia i dodawaniu funkcji zaspokajających potrzeby użytkowników, poświęcając niewiele uwagi środkom bezpieczeństwa lub całkowicie je pomijając. Innym powodem jest dążenie do jak najszybszego wprowadzenia urządzenia na rynek. Ponadto część użytkowników IoT zwraca uwagę głównie na cenę urządzeń i ignoruje wymagania bezpieczeństwa, co skłania producentów do minimalizowania kosztów kosztem bezpieczeństwa.

Także ograniczenia sprzętowe IoT utrudniają wdrożenie niezawodnych mechanizmów bezpieczeństwa, przez co urządzenia są podatne na ataki cybernetyczne. Ponieważ urządzenia IoT są zasilane z baterii o ograniczonej pojemności, mają energooszczędne systemy obliczeniowe i komunikacyjne, w których trudno wdrożyć wystarczające mechanizmy bezpieczeństwa. Zastosowanie energochłonnych systemów obliczeniowych i komunikacyjnych, umożliwiających wdrożenie niezawodnych zabezpieczeń, znacząco skróciłoby czas życia urządzenia (czas od jego wdrożenia do całkowitego wyczerpania energii zgromadzonej w baterii). W efekcie producenci i deweloperzy mają tendencję do poświęcania bezpieczeństwa urządzenia na rzecz jego niezawodności i czasu życia.

Udany atak na system IoT może skutkować kradzieżą danych, utratą prywatności oraz uszkodzeniem innych krytycznych systemów połączonych z systemami IoT. Systemy IoT są coraz częściej celem ataków ze względu na względną łatwość ich kompromitacji. Są one również coraz częściej włączane do infrastruktury krytycznej – energetycznej, wodociągowej, transportowej, ochrony zdrowia, edukacyjnej, komunikacyjnej, bezpieczeństwa i wojskowej – co czyni je atrakcyjnym celem, zwłaszcza w czasie wojny konwencjonalnej, hybrydowej i cybernetycznej. W takim przypadku celem atakujących jest nie tylko kompromitacja systemów IoT, ale także wykorzystanie podatności urządzeń IoT do kompromitacji lub uszkodzenia infrastruktury krytycznej. Przykłady ataków przeprowadzonych z wykorzystaniem podatności urządzeń IoT:

- Atak botnetu Mirai: botnet IoT (sieć urządzeń IoT, na których działają boty) posłużył w październiku 2016 r. do przeprowadzenia zmasowanego ataku rozproszonej odmowy usługi (DDoS) na firmę Dyn, dostawcę usług systemu nazw domenowych (DNS). Ruch z botnetu IoT, obejmującego m.in. kamery i rejestratory DVR, został skoordynowany tak, aby zalać serwery DNS firmy Dyn, aż do ich przeciążenia i awarii. Atak, trwający kilka godzin, zakłócił działanie

serwisów takich jak Twitter, The Guardian, Netflix, Reddit, CNN i wielu innych w Europie i USA.
- Atak Stuxnet: jeden z najbardziej znanych ataków na IoT. Jego celem był irański zakład wzbogacania uranu w Natanz. Atak skompromitował oprogramowanie Siemens Step7 działające w systemie Windows, dając złośliwemu oprogramowaniu (robakowi) dostęp do przemysłowych sterowników PLC. Atak uszkodził wiele wirówek do wzbogacania uranu, pokazując, w jakim stopniu ataki z wykorzystaniem IoT mogą zaszkodzić systemom energetycznym i infrastrukturze krytycznej.
- Włamanie do Jeepa: ten testowy atak przeprowadzili badacze w lipcu 2015 r. na SUV-ie marki Jeep. Udało im się przejąć kontrolę nad pojazdem, wykorzystując podatność w mechanizmie aktualizacji oprogramowania układowego. Wykazali, że atak pozwala sterować prędkością pojazdu i zjechać nim z drogi. Wraz z dodawaniem do samochodów kolejnych czujników IoT istnieje więc poważne ryzyko, że zostaną one wykorzystane do zmasowanego ataku na pojazdy, który mógłby doprowadzić do poważnych wypadków. Tego rodzaju podatność może zostać wykorzystana do zamachów terrorystycznych lub zabójstw na zlecenie.
- Zimno w Finlandii: cyberprzestępcy przeprowadzili atak z wykorzystaniem IoT na systemy grzewcze w fińskim mieście Lappeenranta, wyłączając ogrzewanie. Przeprowadzili też atak DDoS na infrastrukturę grzewczą, zmuszając sterowniki do ciągłego restartowania systemu i uniemożliwiając jego uruchomienie. Był to poważny atak, biorąc pod uwagę niskie temperatury w Finlandii zimą. Podobny atak może zostać przeprowadzony na systemy klimatyzacji w gorącym klimacie, co może spowodować poważne problemy u mieszkańców. Systemy IoT mogą więc posłużyć do ataków na krytyczną infrastrukturę cywilną, aby zakłócić prawidłowe funkcjonowanie społeczeństwa.
- Włamanie do Verkada: atak przeprowadzono na firmę Verkada, dostawcę chmurowej usługi monitoringu wideo. Atakujący naruszyli prywatność jej klientów (m.in. fabryk, szpitali, szkół i więzień), uzyskując dostęp do obrazu na żywo z około 150 000 kamer. Pokazuje to ryzyko, jakie pełna kompromitacja dostawcy usług IoT w chmurze/mgle stwarza dla jego klientów, zwłaszcza tych świadczących usługi krytyczne dla społeczeństwa.

Wymienione ataki to tylko kilka przykładów tego, jak cyberprzestępcy mogą wykorzystać podatności urządzeń IoT do kompromitacji i zakłócania usług w innych sektorach, zwłaszcza w infrastrukturze krytycznej. Przykłady te pokazują pilną potrzebę wbudowywania mechanizmów bezpieczeństwa w infrastrukturę IoT, zwłaszcza tę zintegrowaną z infrastrukturą kluczową. Wskazują też, że zagrożenie ze strony IoT jest realne i może poważnie zakłócić funkcjonowanie społeczeństwa oraz spowodować znaczne straty finansowe i materialne, a nawet utratę wielu ludzkich istnień. Jeśli bezpieczeństwu IoT nie poświęci się należytej uwagi, IoT wkrótce stanie się Internetem Zagrożeń (ang. *Internet of Threats*), a nie Internetem Rzeczy (ang. *Internet of Things*).

Bezpieczeństwo IoT obejmuje zatem strategie projektowe i operacyjne służące ochronie urządzeń IoT oraz innych systemów przed cyberatakami. Obejmuje różne techniki i systemy opracowane w celu zapewnienia poufności i integralności danych IoT oraz dostępności danych i systemów IoT. Strategie i systemy te mają zapobiegać atakom wykorzystującym IoT oraz zapewniać bezpieczeństwo infrastruktury IoT. W tym rozdziale omówiono pojęcia bezpieczeństwa IoT, wyzwania związane z bezpieczeństwem IoT oraz techniki, które można zastosować, aby zabezpieczyć dane i systemy IoT przed kompromitacją i wykorzystaniem do złośliwych celów.

Szczegółowe zagadnienia cyberbezpieczeństwa systemów IoT omówiono w następujących podrozdziałach:

- Pojęcia Cyberbezpieczeństwa
- Sprzęt IoT, a Cyberbezpieczeństwo
- Wyzwania Cyberbezpieczeństwa IoT
- Podatności Systemów IoT

- Wektory Ataku Na IoT
- Technologie Bezpieczeństwa IoT
- Bezpieczeństwo Przechowywania Danych IoT

Źródło: tłumaczenie rozdziału IoT Security z podręcznika IoT-Reloaded (Roboticlab DokuWiki).

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

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures?rev=1793539719

Last update: **2026/11/01 14:28**