fundacja instytut
CYBERBEZPIECZEŃSTWA

O zagrożeniach IoT w naszym domu

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Czy w ogóle zwykła lodówka może nas skrzywdzić? Wydaje się to czymś abstrakcyjnym i niezwiązanym ze sferą cyberbezpieczeństwa. Lodówka jest przecież urządzeniem obniżającym temperaturę, co pozwala zachować na dłużej świeżość przechowywanych tam produktów. I taka tradycyjnie pojmowana lodówka nie wyrządzi nam żadnej szkody. Jednak nawet lodówek, odkurzaczy i innych urządzeń codziennego użytku nie pominął postęp technologiczny. Inteligentne urządzenia potrafią w pewien sposób komunikować się ze sobą przez wbudowane komputery. Tak jak każdy sprzęt korzystający z przepływu danych, mogą one zostać przechwycone przez przestępców i wykorzystane przeciwko nam.

Czym jest IoT?

Internet rzeczy (Internet of things) jest to ogół urządzeń elektronicznych, które gromadzą dane i komunikują się ze sobą i tworzą sieć autonomicznych urządzeń ze zdolnością do wchodzenia w interakcje. Przykładowo lodówki mogą komunikować się z smartfonami i tabletami, piekarnikiem czy sklepami internetowymi. Pojęcia internetu rzeczy użył pierwszy raz już w roku 1999 przedsiębiorca Kevin Ashton. Jego koncepcję systemu, w którym urządzenia komunikują się ze światem, zaczęto realizować 10 lat później. Już wtedy liczba urządzeń podłączonych do Internetu przekroczyła liczbę ludzi na świecie! Jak to się dzieje, że lodówka potrafi podać nam przepis z wykorzystaniem produktów, jakie się w niej znajdują, a ekspres do kawy wie, o której godzinie przygotować nam ulubione latte? Schemat działania IoT można podzielić na kilka kroków. Po pierwsze, urządzenie na etapie produkcji wyposażone jest w specjalne sensory, czyli kamery, czujniki, termometry itp. Można je porównać do zmysłów u człowieka. Dzięki temu urządzenie może zbierać informacje. Po drugie, dzięki podłączeniu do sieci (Wi-Fi, LTE, Bluetooth) łączy się z Internetem, co umożliwia przepływ danych. Te z kolei są przetwarzane w chmurze i na tej podstawie urządzenie podejmuje decyzje, inicjuje działania lub przekazuje informacje zwrotne.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Dlaczego IoT zyskuje na popularności w gospodarstwie domowym?

IoT to już stały element postępu technologicznego. Jego głównym zadaniem jest poprawa jakości życia użytkowników. Dodatkowy atut to oszczędność czasu, który musielibyśmy przeznaczyć na zakupy czy planowanie posiłków. Inteligenta lodówka zrobi to za nas. Urządzenia IoT będą wysyłały nam także powiadomienia na smartfon, kiedy jakaś czynność z nimi związana będzie wymagała ingerencji człowieka. Takie rozwiązania wiążą się również z korzyściami finansowymi. Dzięki możliwości wyłączenia światła smartfonem lub opcji zdalnego sterowania domową klimatyzacją możemy osiągnąć większą kontrolę nad naszymi rachunkami oraz wesprzeć postawy ekologiczne. Atutem sprzętów IoT jest także umożliwienie łatwego i szybkiego zdobywania wiedzy, od nowych przepisów wygenerowanych przez naszą lodówkę, po stan naszego zdrowia zbadany przez zegarek. Sprzęt tego typu jest też coraz łatwiej dostępny, rozwijają się również sieci bezprzewodowe, jak 5G, co automatycznie wspomaga urządzenia w szybszym komunikowaniu się ze sobą i z chmurą.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Zagrożenia związane z internetem rzeczy

Poważne niebezpieczeństwo stanowi brak świadomości użytkowników, którzy nie zdają sobie sprawy z zagrożeń związanych z IoT. W przypadku wspomnianego przykładu inteligentnej lodówki niepokojąca jest możliwość późniejszego wykorzystania danych zebranych przez urządzenie. Taka lodówka zna nasze nawyki i preferencje żywieniowe, a także zbiera informacje o zakupach. Zapisane dane mogą zostać wykorzystane w celach marketingowych, a nawet sprzedane innym firmom. Użycie zebranych informacji bez zgody użytkownika może stanowić naruszenie prywatności. Jednak znacznie poważniejsze konsekwencje grożą nam, gdy ktoś będzie chciał zaatakować nas przy użyciu takiego sprzętu, co jest jak najbardziej możliwe. Urządzenia IoT mają wbudowane swego rodzaju komputery, więc oczywistym zagrożeniem będzie wykorzystanie przez cyberprzestępców wirusa komputerowego, który zainfekuje nasz inteligentny sprzęt. Cyberprzestepcy w ten sposób z łatwością zniszczą lub wykradną przechowywane dane, zakłócą pracę urządzenia atakiem DDoS czy ransomware, który szyfruje ważne informacje. Jeśli cyberprzestępca przejmie nasze sprzęty, mogą być one złośliwie użyte przeciwko nam. Zhakowana lodówka może podnosić temperaturę na tyle, by żywność się psuła, a przejęty system oświetlenia – włączać się i gasić według zachcianek przestępcy, co dla właściciela będzie zapewne bardzo uciążliwe. Urządzenia zintegrowane z internetowymi platformami zakupowymi mogą zostać wykorzystane do złożenia nieupoważnionych zamówień lub dokonania oszustw na konto właściciela. Jeśli w gospodarstwie domowym znajduje się więcej połączonych ze sobą inteligentnych systemów, cyberprzestępcy, przechwytując jeden z nich, z łatwością opanują kolejne, przez ich wzajemne połączenia. W ten sposób skutecznie podszyją się pod właściciela i uwiarygodnią wykonywane operacje. Sprzęt monitorujący naszą codzienność rejestruje także anomalie, czyli odstępstwa od codziennej normy jego użytkowania. Jeśli dane te przechwyci potencjalny włamywacz, otrzyma on informacje, w jakich dniach i godzinach nikogo nie ma w domu. Jeżeli zaatakowane zostanie urządzenie przemieszczające się, jak na przykład odkurzacz, przestępca może poznać także nasz układ pomieszczeń, co dodatkowo ułatwi mu włamanie. Co więcej, komunikacja urządzeń nie jest szyfrowana, a poziom uwierzytelniania zazwyczaj dość niski.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Ryzyko z życia wzięte

Ofiarą cyberataku na urządzenia IoT może być każdy posiadacz takich udogodnień. Aby to udowodnić, badacz bezpieczeństwa z firmy Avast udokumentował, jak przejmuje kontrolę nad ekspresem do kawy, stosując atak typu ransomware. Chcąc odzyskać kontrolę nad sprzętem, właściciel, zgodnie z komunikatem, który wyświetlała maszyna, musiałby najpierw zapłacić okup. W tym przypadku atak był kontrolowany i przeprowadzony w celu zobrazowania realnego zagrożenia. Istnieje jednak wiele przypadków autentycznych przestępstw dokonanych za pomocą inteligentnych urządzeń. Zdecydowanie najbardziej medialny jest atak na kasyno, skutecznie przeprowadzony przy użyciu termometru w akwarium. Korzystając z podłączenia urządzenia do Internetu, włamano się do sieci kasyna i wykradziono dane, nieocenione z komercyjnego punktu widzenia, które właśnie przez termometr zostały przesłane do chmury. Obecnie celów cyberataków nie stanowią tylko wielkie korporacje. Przestępcy coraz częściej stawiają na ilość, wykradając mniejsze sumy z wielu gospodarstw domowych, do czego sprzęty IoT mogą być bardzo łatwą drogą.

Jak chronić się przed atakiem?

Pierwszym krokiem jest edukacja i zwiększanie świadomości użytkowników urządzeń IoT. Konsument musi podjąć ostateczną decyzję, czy akceptuje możliwe ryzyko i chce korzystać z urządzenia. Większość urządzeń IoT zawiera okrojone zabezpieczenia wbudowane lub jest ich całkowicie pozbawiona. Nie oznacza to jednak, że ochrona naszych sprzętów jest niemożliwa. Już na etapie kupna należy się upewnić, że produkt pochodzi od pewnego producenta i kupujemy go z legalnego źródła (zwłaszcza przy zamówieniach internetowych). Następnie powinno się zadbać o prawidłowe skonfigurowanie urządzenia. Wyłączmy funkcje dostępu, z których nie planujemy korzystać. Koniecznie zmieńmy domyślne hasła w urządzeniu. Silne hasło dostępu powinno zawierać duże oraz małe litery, cyfry i znaki specjalne. Jeśli urządzenie posiada opcję dwuskładnikowego uwierzytelniania, nie bójmy się z niego skorzystać. Polega ono na wzmocnieniu tradycyjnego logowania dodatkowym zabezpieczeniem, takim jak potwierdzenie operacji smartfonem czy zastosowanie klucza biometrycznego. Jeśli nie używamy akurat danego urządzenia, odłączenie go od sieci również zminimalizuje ryzyko ataku. Monitorujmy nasze sprzęty IoT i sięgajmy po systemy zabezpieczające typu firewall. Zabezpieczenia powinny być regularnie sprawdzane przez profesjonalne testy penetracyjne (kontrolowane próby ataków mające zweryfikować skuteczność wprowadzonych zabezpieczeń i wykryć luki podatne na atak hakerski). Tak jak każde urządzenie IT, nasze domowe sprzęty wymagają aktualizacji. Producenci, wykrywając lukę w zabezpieczeniach, powinni udostępnić aktualizację oprogramowania. Jeśli widzimy, że jest ona dostępna, natychmiast ją zainstalujmy. Warto ustawić na rządzeniu automatyczną aktualizację, chociaż aktualizacje oprogramowania urządzeń IoT nie są nadal tak częste, jak na komputerach czy smartfonach. Błędem w zabezpieczeniu urządzenia byłoby skupienie się wyłącznie na nim. Sercem łączności urządzeń jest router, którego zabezpieczeń nie można tu pominąć. Oprócz silnego hasła do niego można użyć szyfrowania WPA2 lub WPA3. Bezpiecznym rozwiązaniem będzie też utworzenie drugiej sieci dla urządzeń IoT. Dzięki osobnemu łączu z Internetem zainfekowany sprzęt nie da hakerom dostępu do laptopa czy smartfona. Na koniec zwróćmy uwagę na umiar w użytkowaniu. Zanim dokonamy zakupu inteligentnego urządzenia, przeanalizujmy wiążące się z nim ryzyko, sprawdźmy, jakie zabezpieczenia możemy zastosować, i zastanówmy się, czy naprawdę potrzebujemy tego typu sprzętu i czy jesteśmy w stanie utrzymać je w standardach bezpieczeństwa.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Źródła:

[1] *Zagrożenia inteligentnych urządzeń domowych*, Wojsko Polskie, https://www.wojsko-polskie.pl/woc/articles/publikacje-r/zagrozenia-inteligentnych-urzadzen-domowych/

[2] *Kradzież przez termometr, czyli o bezpieczeństwie Internetu Rzeczy*, Exatel, 17 IV 2018 r., https://exatel.pl/wiedza/materialy/artykuly/kradziez-przez-termometr-czyli-o-bezpieczenstwie-internetu-rzeczy/

[3] *Bezpieczeństwo IoT: Jak chronić urządzenia Internet of Things?*, Orange, 2 VII 2023 r., https://www.orange.pl/poradnik-dla-firm/cyberbezpieczenstwo/bezpieczenstwo-iot/

[4] *Zhakowany ekspres do kawy żąda okupu, czyli przyszłość IoT poważnie zagrożona*, Bulldogjob, 29 IX 2020 r., https://bulldogjob.pl/readme/zhakowany-ekspres-do-kawy-zada-okupu-czyli-przyszlosc-iot-powaznie-zagrozona

[5] *Co to jest Internet Rzeczy i jak szybko się rozwija?*, APA, 31 X 2019 r., https://apagroup.pl/apalab/co-to-jest-internet-rzeczy-i-jak-szybko-sie-rozwija/

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości