OUCH! Styczeń 2025

SANS SECURITY AWARENESS

Smart Home - Inteligentne urządzenia domowe

Cyfrowy koszmar: cyberprzestępcy w twoim domu

Sara i jej rodzina byli zachwyceni swoimi nowymi inteligentnymi urządzeniami. Umożliwiają one w łatwy sposób m.in. sterowanie oświetleniem czy zamkami za pomocą kilku dotknięć lub poleceń głosowych. Ich podekscytowanie zmieniło się w niepokój, gdy pewnej nocy Sara zauważyła, że termostat grzejnikowy nieoczekiwanie sam zmienił ustawienia. Początkowo myślała, że może być to usterka. Jednakże przeraziła się, gdy światła w pokoju zaczęły migotać, a drzwi wejściowe się odblokowały. Sytuacja uległa eskalacji, gdy głos nieznajomego zaczął wydobywać się z elektronicznej niani, opisując szczegółowo pokój jej dziecka. W tym momencie Sara zdała sobie sprawę, że hakerzy uzyskali dostęp do jej inteligentych urządzeń. Cyberprzestępcy przejęli kontrolę nad urządzeniami, narażając tym samym prywatność i bezpieczeństwo jej rodziny. Myśl o obcych ludziach obserwujących sen jej dziecka sprawiła, że Sara poczuła się bezbronna. To niepokojące doświadczenie uświadomiło Sarę, że należy zabezpieczyć inteligentne urządzenia domowe. Wpłynie to przede wszystkim na bezpieczeństwo i spokój całej rodziny.

Czym są urządzenia Smart Home?

Inteligentne urządzenia domowe to podłączone do Internetu wszelkie urządzenia i sprzęty, takie jak termostaty, kamery bezpieczeństwa, inteligentne zamki, oświetlenie, a nawet pralka czy zmywarka, które sprawiają, że nasze domy są bardziej wydajne, wygodne, a czasem nawet bezpieczniejsze. Urządzenia te są sterowane za pomocą aplikacji, poleceń głosowych lub zautomatyzowanych systemów.

Jednak wygoda jaką zapewniają, wiąże się również z ryzykiem. Urządzenia te łączą się z Internetem i niestety są podatne na ataki, jeśli nie są odpowiednio zabezpieczone. Po włamaniu intruzi mogą uzyskać dostęp do danych osobowych, szpiegować codzienne czynności, a nawet kontrolować fizyczne urządzenia w domu.

Dlaczego zabezpieczenie urządzeń inteligentnego domu jest tak ważne?

Zabezpieczenie inteligentnych urządzeń domowych to nie tylko ochrona samych gadżetów, ale także całego gospodarstwa domowego. Cyberprzestępcy często szukają najsłabszych urządzeń, jakie mogą znaleźć i zaczynają od nich. Po złamaniu zabezpieczeń cyberprzestępca może uzyskać dostęp do innych urządzeń w sieci domowej, wykraść poufne dane lub np. odblokować drzwi wejściowe. W połączonym świecie zabezpieczenie inteligentnych urządzeń ma kluczowe znaczenie dla zachowania całościowego bezpieczeństwa, prywatności i spokoju ducha.

Oto pięć rzeczy, które warto zrobić, aby zabezpieczyć swoje urządzenia inteligentnego domu

1. **Zmień domyślne hasła**: Wiele urządzeń mają domyślne ustawione fabrycznie hasła, które są dobrze znane lub łatwe do odgadnięcia przez cyberprzestępców. Zmień je natychmiast na silne i unikalne, a jeśli masz problem z ich zapamiętaniem, skorzystaj z menedżera haseł.
2. **Włącz uwierzytelnianie wieloskładnikowe (MFA)**: Zazwyczaj urządzenia wymagają utworzenia konta w celu zarządzania nimi. Jeśli urządzenie to umożliwia, włącz uwierzytelnianie wieloskładnikowe. Sprawi to, że uzyskasz dodatkową warstwę zabezpieczeń, która wymaga zarówno hasła, jak i unikalnego jednorazowego kodu. Tym sposobem znacznie utrudnisz "pracę" przestępcom.
3. **Zapewnij urządzeniom inteligentnym własną sieć Wi-Fi**: Stwórz dedykowaną sieć dla urządzeń Smart Home, oddzielną od urządzeń osobistych. W wielu punktach dostępowych Wi-Fi lub routerach jest to często nazywane siecią dla gości. Pomaga to odizolować urządzenia i ograniczyć szkody, jeśli jedno z nich zostanie naruszone.
4. **Aktualizacje**: Producenci regularnie wydają aktualizacje w celu usunięcia luk w zabezpieczeniach. Upewnij się, że urządzenia z których korzystasz mają najnowsze aktualizacje oprogramowania. Pozwoli to zwiększyć ochronę przed nowymi znanymi zagrożeniami. Jeśli to możliwe, włącz automatyczną aktualizację na urządzeniach. Nie będziesz musiał o tym pamiętać. Rozważ również wymianę urządzeń, które nie są już obsługiwane lub nie otrzymują aktualizacji zabezpieczeń od swoich producentów.
5. **Wyłącz nieużywane funkcje**: Inteligentne urządzenia często wyposażone są w różne funkcje o istnieniu których możesz nie mieć pojęcia. Im więcej takich funkcji jest aktywnych, tym więcej potencjalnych drzwi mają cyberprzestępcy aby się do nich dostać. Wyłącz wszelkie niepotrzebne usługi, takie jak zdalny dostęp lub polecenia głosowe, aby zminimalizować punkty wejścia, które cyberprzestępcy mogliby wykorzystać.

Twój Smart Home nie musi stać się placem zabaw dla cyberprzestępców. Wykonując zaledwie tych kilka kroków, możesz cieszyć się wszystkim co technologia ma do zaoferowania, jednocześnie mając świadomość, że ją odpowiednio zabezpieczyłeś.

Redaktor gościnny

Sai Sujitha Venkatesan jest starszym inżynierem ds. bezpieczeństwa w zespole reagowania na incydenty związane z bezpieczeństwem produktów firmy Dell i członkiem zarządu WiCyS (Women in CyberSecurity) Silicon Valley. Pasjonuje się wszystkimi kwestiami związanymi z bezpieczeństwem, w tym różnorodnością pracowników. Linkedin: https://www.linkedin.com/in/saisujitha/

Źródła

Moc aktualizacji: https://www.sans.org/newsletters/ouch/power-updating/
Siła haseł: https://www.sans.org/newsletters/ouch/power-passphrase/
Menedżer haseł: https://www.sans.org/newsletters/ouch/power-password-managers/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz