Inteligentne sprzęty domowe zbierają nasze dane

Kategoria: Styl życia
Opublikowano: czwartek, 17, październik 2024 12:57
Patrycja Grebla-Tarasek

Szczoteczka do zębów połączona z aplikacją, odkurzacz automatyczny rozpoznający ilość brudu, lodówka która sama zamawia brakujące jedzenie, pralka który uczy się Twoich nawyków – brzmi znajomo? Dla wielu z nas tak, bowiem inteligentne sprzęty coraz częściej pojawiają się w naszych domach. Niestety, gdy podłączymy te wszystkie sprzęty do tego samego wifi co nasz komputer czy telefon, wówczas otwieramy furtkę do wykradnięcia naszych danych przez cyberprzestępców.

Inteligentny dom umożliwia zdalne sterowanie oświetleniem, ogrzewaniem, klimatyzacją czy urządzeniami gospodarstwa domowego. Urządzenia elektroniczne połączone w sieć tworzą tzw. Internet Rzeczy (ang. Internet of Things, IoT) - wymieniają się informacjami, współpracują ze sobą, mogą automatyzować wiele czynności, słowem - ułatwiając nam życie.

Każde urządzenie podłączone do naszej sieci wifi może stać się celem cyberprzestępców. Nawet inteligentny odkurzacz może zostać botem zombie w ich rękach.

Pierwszym punktem styku między atakującym a naszymi urządzeniami inteligentnymi jest router. Umożliwia on urządzeniom takim jak smartfony, tablety, inteligentne żarówki, pralki, lodówki i inne inteligentne urządzenia domowe, łączenie się z siecią i komunikowanie się ze sobą. Zatem najprostszym sposobem na włamanie się do naszej sieci domowej jest zhakowanie routera. Najłatwiej zhakować router wykorzystując słabe hasła lub luki w zabezpieczeniach urządzeń czy oprogramowania. Routery mają zazwyczaj domyślne hasła administracyjne, które nie dość, że są łatwe do odgadnięcia i zapamiętania, to jeszcze są zapisane w instrukcji obsługi routera. Dzięki temu, w razie problemów z konfiguracją, można się do niej odwołać. Jeśli domyślne hasło administratora nie zostanie zmienione, cyberprzestępcy mogą je łatwo złamać.

Kolejna istotna kwestia to nazwa naszej sieci (tzw. SSID). Routery mają swoje domyślne identyfikatory, na podstawie których cyberprzestępca może się zorientować, jakiego rodzaju jest to urządzenie. Ułatwia mu to włamanie się do naszej sieci, ponieważ pierwszy krok, czyli sprawdzenie, z jakiego rodzaju urządzeniem ma do czynienia i od jakiego producenta, zapewnił mu już użytkownik, który nie zmienił nazwy urządzenia.

Najlepszym rozwiązaniem, które nas chroni, jest stworzenie osobnej sieci na urządzenia, które potrzebują do działania sieci wifi. Wówczas, gdy ktoś włamie się np. do naszego odkurzacza, nie dostanie się przez sieć do komputera i zapisanych/zapamiętanych tam haseł dostępu do naszych kont.

Przestępcy coraz chętniej wykorzystują inteligentne urządzenia gospodarstwa domowego do przeprowadzania ataków, ponieważ są one coraz bardziej powszechne, a użytkownicy wciąż jeszcze nieświadomie narażają się na kłopoty.

Oddzielną kwestią jest przetwarzania przez producenta urządzenia danych, które na nasz temat gromadzi urządzenie. Na przykład inteligentny odkurzacz może gromadzić dane o metrażu i rozkładzie naszego mieszkania, a inteligentny zamek do drzwi o tym, o której wracamy codziennie do domu. Dlatego należy sprawdzić, jakie dane są gromadzone przez to urządzenie oraz w jaki sposób są one przetwarzane, czyli przechowywane, wykorzystywane i udostępniane.

Źródło: NASK