**Grange Insurance: Najczęstszą przyczyną naruszeń bezpieczeństwa sieciowego jest brak świadomości społecznej dot. zagrożeń cybernetycznych**

**Zdecydowana większość Amerykanów obawia się o swoje bezpieczeństwo w cyberprzestrzeni. Jako podstawowy problem wymieniają popularyzację inteligentnych urządzeń, które coraz częściej goszczą w ich domach.**

Wg badań zleconych przez amerykańską firmę ubezpieczeniową Grange Insurance, co czwarty Amerykanin padł ofiarą cyberataku. Większość z nich przyznało, że nie wie, jakie środki należy przedsięwziąć, by skutecznie chronić się przed zagrożeniami sieciowymi. Pozostali respondenci odpowiedzieli, że do momentu ataku żyli w przekonaniu, iż posiadają dostateczną wiedzę na ten temat. Jeden na pięciu badanych stwierdził, że podejmowanie działań mających chronić przed atakami hakerów stanowi dla nich zbędny wysiłek.

Wg Grange Insurance w przeciętnym amerykańskim domu znajduje się średnio sześć inteligentnych urządzeń, a 65 procent respondentów zadeklarowało, że planuje w niedalekiej przyszłości nabyć kolejne. Niestety, stale rosnąca w amerykańskich domach liczba urządzeń internetu rzeczy (IoT) otwiera hakerom kolejne furtki, przez które mogą się włamać do domowych sieci.

„Z przeprowadzonych badań jasno wynika, że większość konsumentów ma duże obawy związane z obecnością w naszym życiu coraz większej liczby inteligentnych urządzeń i wynikającymi z tego faktu zagrożeniami. Niestety, nie posiadają oni wystarczającej wiedzy, jak przeciwdziałać zagrożeniom i gdzie zwrócić się o pomoc. Mamy nadzieję, że nasze badania przyczynią się do zwiększenia świadomości nt. zagrożeń w cyberprzestrzeni, a w efekcie do podjęcia niezbędnych działań zapobiegawczych” – podsumował wyniki badań John North, Personal Lines President w Grange Insurance.

Podstawowym problemem bezpieczeństwa cybernetycznego wśród amerykańskich konsumentów jest fakt, że 81% z nich często korzysta z publicznego WiFi. Takie postępowanie, w połączeniu z niedostateczną wiedzą nt. zasad bezpieczeństwa sieciowego, prowadzi zwykle do nieodpowiedzialnych zachowani, np. korzystania z niezabezpieczonych hotspotów. Skrzętnie wykorzystują to hakerzy do kradzieży poufnych danych.

Wynikające z przeprowadzonych badań obawy łagodzi fakt, że aż 77% respondentów korzystających z publicznego Wi-Fi wyraża zaniepokojenie związane z ryzykiem wycieku wrażliwych danych i wykazuje dobrą znajomość zagadnień związanych z potencjalnymi zagrożeniami. Co dziesiąty badany stwierdził jednak, że nie wie, gdzie szukać pomocy w celu zapewnienia lepszej ochrony przez zagrożeniami cybernetycznymi.

„Na pytanie, jakie środki zaradcze badane osoby mają zamiar przedsięwziąć w najbliższej przyszłości, część respondentów udzieliła odpowiedzi, że planuje zwrócić się o pomoc do wyspecjalizowanych firm zajmujących się cyberbezpieczeństwem. Inni natomiast stwierdzili, że samodzielnie poszukają dodatkowych metod ochrony. Jedna trzecia badanych bierze pod uwagę wykupienie ubezpieczenia od następstw ataku” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.