6 MILIARDÓW URZĄDZEŃ A BEZPIECZEŃSTWO. RAJ DLA CYBERPRZESTĘPCÓW?

Liczba urządzeń łączących się z internetem używanych w przedsiębiorstwach w 2020 roku osiągnie prawie 6 miliardów. Każde z nich może być potencjalnym celem cyberataku. Czy w takim razie, świat czeka nowa fala cyberataków?

Każde urządzenie, które łączy się z siecią, może być potencjalnym celem ataku - przestrzegają specjaliści z zakresu cyberbezpieczeństwa. Ochrony wymagają nie tylko komputery i smartfony, ale również inne sprzęty działające online, takie jak drukarki, kamerki Wi-Fi, routery czy Smart TV.

"Należy pamiętać, że cyberprzestępcom wystarczy jedno zainfekowane urządzenie, aby zniweczyć wszelkie wysiłki włożone w zabezpieczenie sieci. Żadne nieznane urządzenie nie powinno mieć prawa dostępu do infrastruktury firmowej, zaś dopuszczone urządzenia muszą podlegać automatycznej segmentacji – podkreśla Jolanta Malak, dyrektor Fortinet w Polsce.

Według prognoz firmy Gartner, liczba urządzeń z zakresu internetu używanych w przedsiębiorstwach w przyszłym roku wyniesie w 2020 roku prawie 6 miliardów, co w istotny sposób zwiększa obszar potencjalnego ataku, podnosi również wewnętrzne koszty konfigurowania, zarządzania i zapewnienia zgodności urządzeń IoT z przepisami.

Tymczasem, według badania firmy Forrester, aż 82 proc. przedsiębiorstw zmaga sie z problemami już na etapie identyfikacji wszystkich urządzeń mających dostęp do ich sieci. Zdaniem specjalistów strategia bezpieczeństwa powinna obejmować nie tylko ochronę sprzętu i urządzeń, ale i edukację pracowników w zakresie odpowiedniego korzystania z urządzeń i internetu.

Eksperci firmy Fortinet zwracają uwagę na niebezpieczeństwa związane z wykorzystywaniem przez pracowników swoich prywatnych urządzeń, np. smartfonów i tabletów, do łączenia się z firmową siecią. Zjawisko BYOD (ang. Bring Your Own Device) może narażać przedsiębiorstwa na cyberzagrożenia.

"W sytuacji, gdy smartfon pracownika zostanie zainfekowany, cyberprzestępca zyskuje dostęp nie tylko do jego prywatnych informacji, ale też firmowej sieci i danych. Każde przedsiębiorstwo, w którym stosowany jest model BYOD, powinno dbać o stałe monitorowanie ruchu sieciowego i ochronę punktów końcowych, czyli np. smartfonów, tabletów czy komputerów" - podkreślają specjaliści.