Vážené čtenářky, vážení čtenáři,

internet věcí (IoT) stále více promlouvá nejen do životů běžných uživatelů, ale i firem. Stává se novodobým fenoménem, který ještě umocňuje očekávaný příchod sítí 5G. Je ale i dostatečně zabezpečený?

Nejnovější zpráva společnosti Zscaler odhaluje některá znepokojující fakta o rizicích, která zařízení IoT v podnikové infrastruktuře představují. Výzkumníci analyzovali desítky milionů spojení ze zařízení IoT ve více než tisícovce podnikových sítích a zjistili, že více než 40 % z nich svůj provoz vůbec nešifruje.

To znamená, že velký počet těchto systémů se může vystavit útokům typu man-in-the-middle (MITM). Útočník, který získá přístup k místní síti – například prostřednictvím útoku škodlivého softwaru – by mohl použít spoofing adres ARP (Address Resolution Protocol) nebo by mohl ohrozit lokální router a poté ovlivnit provoz IoT, tak aby vykonal škodlivé aktualizace nebo ukradl citlivá data.

Zkoumaná zařízení zahrnovala IP kamery, chytré hodinky, chytré tiskárny, chytré televizory, set-top boxy, digitální domácí asistenty, IP telefony, zdravotnická zařízení, videorekordéry a přehrávače médií, terminály pro sběr dat, chytré brýle, průmyslová a síťová zařízení, 3D tiskárny, a dokonce i inteligentní auta – to vše od 153 výrobců.

Největším zjištěním bylo, že 91,5 % datových transakcí uskutečněných IoT zařízeními v podnikových sítích nebylo vůbec šifrováno. Pokud jde o samotná zařízení, 41 % nepoužívá šifrování TLS vůbec, stejné množství jen pro některá připojení a pouze 18 % používá TLS pro veškerý provoz.

Znepokojující je i fakt, kolik firemních sítí obsahuje spotřebitelská IoT. To ukazuje na problém stínového IoT, kdy společnosti mohou těžko kontrolovat, jaká zařízení jejich zaměstnanci připojují k síti – od nositelné elektroniky až po automobily.

Podle Zscaleru je navíc většina IoT zařízení připojená ke stejné síti jako obchodní aplikace či jiné klíčové firemní systémy. Pokud je jedno ze zařízení IoT rizikové, útočníci se pak mohou zaměřit na všechny ostatní systémy. Kompromitaci IoT je také mnohem těžší odhalit a navíc mnoho IoT zařízení nemá automatické aktualizace a jejich uživatelé zřídka kontrolují a nasazují aktualizace ručně.

Organizace by měly mít k dispozici řešení, které umožní neustále skenovat síť a identifikovat taková stínová zařízení, a pak vytvořit politiku, kdy se taková zařízení povolí pouze pro připojení k samostatnému síťovému segmentu nezahrnujícímu kritickou infrastrukturu.

Zscaler detekuje v průměru 6 000 transakcí IoT za čtvrtletí, které jsou výsledkem infekcí škodlivým softwarem. Mezi nejčastější skupiny škodlivého softwaru, které se zaměřují na takováto zařízení, patří Mirai, Rift, Gafgyt, Bushido, Hakai nebo Muhstik.

Pokud se chcete o tom, jak chránit IoT v korporátním prostředí a jak zabránit šíření stínového IoT, dozvědět více, přečtěte si článek *„Měli byste se bát stínového IoT?"* v tomto vydání Security Worldu.

S přáním příjemně stráveného léta třeba i nad stránkami našeho časopisu

Pavel Louda, vedoucí projektu

Obsah