

Citlivá data kanceláří i klientů může nejnáze ohrozit obyčejný router

V MINULÉM ROCE DOŠLO DLE BEZPEČNOSTNÍHO REPORTU SPOLEČNOSTI SYMANTEC K NAPADENÍ DAT VÍCE NEŽ 429 MILIONŮ UŽIVATELŮ INTERNETU

Rok 2016 se stal s trochou nadsázky rokem internetu věcí (IoT) a spolu s rostoucím počtem zařízení, která jsou připojena k Internetu, vzrůstá i množství bezpečnostních hrozeb. Útočníci již nevyužívají pouze osobní počítače, notebooky a mobilní telefony, ale čím dál tím častěji se zaměřují na chytré televizory, bezpečnostní kamery, termostaty a další přístroje spadající do kategorie internetu věcí. Každý z těchto přístrojů je připojený k internetu a současně má určité možnosti předávat informace ze svého okolí. Počítače jsou většinou chráněny antivirovými programy. IoT zařízení však v drtivé většině žádnou ochranu nemají a jsou tak snadným cílem.

Nejběžnějším rizikem je však obyčejný router. Toto zařízení většinou považujeme za „krabičku“, která nás jen propojuje, ale to je veliký omyl. Routerem totiž procházejí veškerá data, která kamkoli uživatelé odesílají třeba v podobě e-mailů a pokud je tento router napadený jsou antivirové programy v osobních počítačích úplně bezcenné. V ohrožení jsou data klientů uložená na síťových úložištích, ale i účetnictví či jakákoliv data, která nezabezpečeným routerem prochází a s možností ovládnout bezpečnostní kamery nebo chytrý televizor vybavený kamerou a mikrofonom je kompromitována třeba i bezpečnost zasedacích místností a kanceláří.

Na tuto alarmující situaci upozornilo neziskové sdružení CZ.NIC, které je od roku 1998 správcem národní domény .CZ, a v roce 2015 představilo řešení tohoto problému - projekt výkonného a špičkově zabezpečeného routeru Turrus Omnia. Hlavní devizou tohoto routeru je bezpečnost, která je zajištěna neustálým, automatickým přísunem bezpečnostních aktualizací systému, jenž vznikají přímo v centrále sdružení CZ.NIC, a které reagují na nejaktuálnější bezpečnostní hrozby. Jde o jedinečné funkční řešení, které umožňuje zapomenout na nejobvyklejší nešvar firemních sítí, kterým je neaktualizovaný router se zastaralým systémem umožňující útočníkům přístup k heslům, datům i dalším citlivým informacím.



Velmi zajímavou vlastností routeru Turrus Omnia je i možnost dozoru nad chováním zařízení ve firemní síti. Často se totiž může stát, že zaměstnanec používá notebook nebo služební telefon nejen ve firmě, ale i na domácí síti, která bezpečnostní standardy nemusí splňovat. Snadno se pak takové zařízení nakazí škodlivým softwarem, který ohrožuje bezpečnost firemních dat. S pomocí Turrisu Omnia je možné takové zařízení odhalit a následně nastatou situaci řešit.

O jedinečnosti tohoto routeru vypovídá i skutečnost, že se neziskovému sdružení CZ.NIC na jeho vývoj od podporovatelů podařilo během necelého roku vybrat na mezinárodní crowdfundingové platformě Indiegogo téměř 30 milionů korun, což zde z projektu Turrus Omnia udělalo nejúspěšnější českou kampaň.

Bezpečný český router Turrus Omnia se již prodává v e-shopu Alza.cz, a to za cenu od 7 518 Kč s DPH. ■

