

Domácnosti sú rajom pre útočníkov

ANKETA

Mobily, počítače a smart zariadenia sú už súčasťou domácností. A pribúda spolu so zariadeniami aj povedomie? Preto sa pýtame profesionálov: Aká je najväčšia bezpečnostná diera v domácnostiach?



Ivan Makatura,
generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nejestvuje nič také ako „najväčšia“ a už vôbec nie „jediná“ bezpečnostná diera. Ide vždy o kombináciu zraniteľností, ktorá vedie ku konkrétnym hrozbám. Zjednodušene povedané: domácnosti sú z hľadiska bezpečnosti deravé ako ementál. Presnejšiu odpoveď na túto otázku poskytuje prieskum, ktorý vykonávame každý rok.



Jaroslav Oster,
predseda správnej rady, Preventista.sk

Smart zariadenia boli a v nemalej miere sú stále vyvíjané a vyrábané so zámerom minimalizácie ceny, čo prirodzene znižuje alebo vylučuje smerovanie na ich bezpečnosť. A najväčšia bezpečnostná diera v realite? Zastarané smart zariadenia a používatelia nevenujú pozornosť aktualizácii ich systémov.



Richard Kiškovač,
generálny riaditeľ, Elkan

Najväčšia bezpečnostná diera v domácnostiach spočíva v stále veľmi nízkom bezpečnostnom povedomí jej obyvateľov. Pre to je príznačné aj ich správanie v online svete a minimálna ochrana. Často používajú starý, neaktualizovaný alebo nelegálny softvér, slabé heslá do systémov, aplikácií alebo do bezdrôtových sietí. Pravdou však je, že sa o tom reálne ani nemajú kde dozvedieť. Efektívne kampane v tomto smere v podstate neexistujú.



Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

Nápadne lacné zariadenia pôfidečných výrobcov s diskutabilnou mierou zabezpečenia predstavujú samy osebe bezpečnostné diery. Najväčšou slabinou je však zvyklosť pripájať rôznorodé zariadenia bez rozmyslu do siete. Som presvedčený, že ak by poznali základné riziká, ktorým sa vystavujú, boli by obozretnější. Pripojili by ste si domácu pestúňku do siete, ak by ste vedeli, že kamerový záznam nejde priamo na vaše zariadenia, ale aj cez servery výrobcu?



Katarína Kročková,
odborníčka na ochranu osobných údajov, Kročka & Partners

Najväčšou bezpečnostnou hrozbou je nedostatočné povedomie o ochrane súkromia. IoT zariadenia môžu totiž zhromažďovať obrovské množstvo osobných údajov vrátane hlasových správ, informácií z domácnosti, dokonca zdravotné údaje. Všetky tieto dáta môžu byť zdieľané s tretími stranami bez vedomosti používateľa. Odporúčam preto v týchto zariadeniach neustále kontrolovať nastavenia súkromia.



Roman Čupka,
hlavný konzultant, Progress a CSO Istrosec

Problémom je klasický „element medzi stoličkou a klávesnicou“. Jeho závislý vzťah k sociálnym médiám, ktoré poskytujú jednoducho stráviteľný obsah, spomienkové optimizmy a prehnaná dôverčivosť prehľbujú bezpečnostnú diery. Tá vytvára efekt snehovej gule formou nevyužívania a odlivu inováčného kapitálu. Následkom sú dlhodobé negatívne dosahy na ekonomickú a kybernetickú odolnosť domácností.



Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Stručne povedané – domácnosti zničí slepá dôvera v technológie. Ak hovoríme o smart zariadeniach, tak vzhľadom na ich pripojenie do internetu je ich slabinou nedostatočné zabezpečenie. Môže viesť k narušeniu súkromia a zneužitiu domácej infraštruktúry útočníkom.



Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC, Soitron

„Ocko, aké máme heslo na wifi-nu? Pýta sa kamoš z online hry.“ „Nechápem, že si ho už tri roky nevieš zapamätať, aj keď ho máme rovnaké ako na Netflix, Gmail a napísal som ti ho minule aj do poznámok v telefóne. Po kom si?!“



Jaroslav Ďurovka,
riaditeľ, Národné centrum kybernetickej bezpečnosti

Rizikom je, ak používate staré mobily a počítače, na ktoré nie sú aplikované bezpečnostné aktualizácie. Na zariadeniach by mali fungovať podporované operačné systémy alebo firmvér a mali by byť zapnuté automatické aktualizácie. Ohrozuje vás aj zlá konfigurácia routera, ktorým sa sieť pripája do internetu, a nechránená alebo zle nakonfigurovaná WiFi. Je dobré, ak sa váš poskytovateľ internetu stará aj o bezpečnosť routera – samozrejme, ak to robí dobre.



Július Selecký,
senior technický špecialista, ESET

Jedným z najväčších bezpečnostných „prúserov“ v domácnostiach je používanie nedostatočne zabezpečených IoT zariadení. Sú to rôzne zariadenia ako kamery, termostaty, inteligentné zámky a hlasoví asistenti. Sú navrhnuté pre pohodlie a často im chýbajú spoľahlivé bezpečnostné funkcie, čo ich robí zraniteľnými hackermi a neoprávneným prístupom.



Ivan Kopáček,
bezpečnostný expert, Gordias

Dnes takmer každá domácnosť disponuje pripojením na internet a WiFi sieťou spájajúcou aj IoT prvky. S tým sú spojené bezpečnostné nastavenia, pravidelné aktualizácie softvéru a podobne. Pri zanedbaní opatrení dochádza k situácii, ako keby sme nezamýkali dvere, iba ich privreli. Skôr či neskôr to niekto zneužije.



Roman Varga,
manažér kyberbezpečnosti, Dôvera, zdravotná poisťovňa

Tak ako si ceníme súkromie, tak aj bezpečnosť nášho smart sveta by mala byť prioritou. Smart zariadenia v domácnostiach prinášajú pohodlie, ale aj riziká. Hrozbou sú nežiaduce prístupy, útoky na súkromie a kyberútoky. Je dôležité zabezpečiť silné heslá, pravidelné aktualizácie softvéru a využívať bezpečnostné funkcie poskytované výrobcami.



Tomáš Valenta,
riaditeľ, Check Point Software Technologies na Slovensku

Za obrovské riziko považujem nechránené mobilné zariadenia a správanie ich majiteľov. Či už dospelých, alebo aj detí. Zamestnancov už vzdelávame, musíme však aj naše deti a celú rodinu.



Henrich Šnajder,
manažér IT bezpečnosti, Orange Slovensko

Podceňovanie aktualizácií softvéru a firmvéru, nedostatočná segmentácia sietí a používanie zastaralých zariadení zvyšuje zraniteľnosť voči kyberútokom. Rizikom sú slabé alebo predvolené heslá a vystavenie zariadení priamo do internetu.



Ivana Lysinová,
konzultantka, Cyllium

Ako častý problém vnímam to, že domácnosti si nezmenia prednastavené heslo na routeri. Je bránou k internej sieti domácnosti a narušiteľ tak dostáva „kľúče“ k všetkým zariadeniam, ktoré sú do siete pripojené. V prípade moderných smart domácností tak môže získať prístup aj k otváraní brán a dverí do domu.



Dominik Procházka,
riaditeľ odboru bezpečnosti, AGEL SK

Hrozbou je kombinácia faktorov – predvolené nastavenia, absencia aktualizácií, skenovanie sietí útočníkmi a riziko zneužitia získaných dát. Spolu s pripojením domáceho zariadenia na firemnú sieť cez VPN to môže viesť k útokom aj na firemné prostredie.



Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Za bezpečnostnú diery považujem nízke povedomie o informačnej bezpečnosti a bagatelizovanie dosahov nefundovaného správania v online svete. Bagatelizovanie trvá len dovtedy, kým sa člen domácnosti nestane obeťou. Rodina potom buď odmieta člena, alebo sa správa múdro, hľadajúc pomoc v odbornej komunite. Potrebuje neustále vysvetľovať, prečo sa musíme vzdelávať.



Diana Legdanová,
riaditeľka divízie pre bezpečnosť, Západoslovenská energetika

Neaktualizovaný softvér či anti-vírus, inštalácie dostatočne neoverených smart vychytávk, sťahovanie rôznych „užitočných“ aplikácií, ktoré sú z kyberpohľadu často čiernymi dierami, používateľské (ne)zručnosti členov domácnosti a monoheslové praktiky. Dosť dôvodov na to, aby niečo zlyhalo, keď sa to najviac nehodí.

INZERCIA

epi KONFERENCIA

Kybernetická bezpečnosť 2024

Novelizácia zákona akcentuje osobnú právnu zodpovednosť štatutárov za kybernetickú bezpečnosť. Zodpovednosť je neprenosná, ale výkonom môžete poveriť zamestnanca alebo dodávateľa.

O vedomosti a skúsenosti sa s vami podelia profesionáli z verejného aj súkromného sektora.

Riadenie rizík kybernetickej bezpečnosti.

Čo čaká štatutárov a manažérov v každodennej realite od januára.

9 prednášok

Odolnosť v kyberpriestore. Ako to robíť?

Praktiká a procesy v riadení informačných aktív, trendy a prax.

6 prednášok

Aby ste ostali na pulze dňa. Inšpirujte sa.

Hrozby a príležitosti umelej inteligencie, bezpečnosť očami hekerov.

10 prednášok a diskusia

30. 9 – 1. 10. 2024

Demänovská dolina,
Hotel Grand Jasná

Prezenčne alebo online.

Informácie o programe a spíkroch na www.epikyberbezpecnost.sk

epi KONFERENCIA

od spoločnosti Poradca podnikateľa

Odborný garant:



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti