

**ČLÁNEK**

**Nejchytřejší útoky na chytrou domácnost a nepříliš chytrá zařízení, která je umožnila**

**AUTOR**: Neil Patel, Director of European Marketing and Business Development, D-Link Europe

*Hackeři v oblasti chytrých domácností jsou čím dál odvážnější a vychytralejší než kdykoli předtím. Abychom vám usnadnili orientaci v těchto neustále se vyvíjejících útocích, sepsali jsme pro vás nejznámější útoky na chytré domácnosti za poslední roky.*

Když Adama a Heather Schreckovi probudil uprostřed noci hlasitý zvuk vycházející z dětského pokoje, nebyl to jako obvykle pláč jejich desetiměsíčního dítěte. Rodiče, kteří spěchali do dětského pokoje, ke svému zděšení brzy zjistili, že hluk je ve skutečnosti hlas dospělého muže, který křičí "Probuď se, dítě!" a že vychází z jejich kamery pro sledování dětí.

A co bylo nejhorší? Jakmile vešli dovnitř, kamera se odvrátila od dítěte a podívala se na rodiče. U kamery, která byla naprogramovaná pouze na hlídání kojence, tato samostatná akce signalizovala, že se [do dětské chůvičky někdo naboural a převzal nad ní kontrolu](https://www.dailymail.co.uk/news/article-2614462/Wake-baby-The-chilling-words-couple-heard-middle-night-man-hacked-daughters-baby-monitor-WATCHING-sleep.html) přes internet.

K tomuto šokujícímu incidentu došlo v roce 2014 a byl bohužel jen prvním z mnoha [útoků na chytré domácnosti](https://www.networkworld.com/article/3285968/strange-and-scary-iot-hacks.html#slide1). Nyní se píše rok 2021 a hackeři chytrých domácností jsou odvážnější a zákeřnější než kdy dříve. Abychom vám pomohli udělat si obrázek, jakým typům útoků chytré domácnosti čelí, přinášíme vám přehled těch nejznámějších, které se v posledních letech odehrály po celém světě. Pokud náhodou vlastníte některé ze zde uvedených chytrých zařízení, měli byste zvážit [posílení ochrany domácí sítě, počínaje routerem](https://www.dlink.com/en/exo).

**Největší a nejrozsáhlejší únos v historii**

Všichni jsme ve zprávách slyšeli o únosu letadel, ale v říjnu 2016 došlo k jinému druhu únosu. Rozsáhlý kybernetický útok, který využíval zranitelnosti v chytrých videorekordérech a webových kamerách, srazil na kolena velkou část internetu v Evropě a USA tím, že stovky tisíc zařízení byly „uneseny“ v rámci útoku, který bezpečnostní experti označili jako [Distributed Denial of Service (DDoS) útok pomocí botnetů Mirai](https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html).

Zjednodušeně řečeno, hackeři se zmocnili připojených zařízení, jako jsou chytré videorekordéry a webové kamery, a pak je použili k zahlcení serverů společnosti Dyn, která dříve spravovala většinu infrastruktury systému názvů domén (DNS) na internetu. A výsledek? Webové stránky včetně Twitteru, The Guardian, Netflixu, Redditu, CNN a několika dalších v Evropě i USA byly po většinu dne mimo provoz.

Je to tak, někteří hackeři chtějí víc než jen údaje o vašich kreditních kartách a neváhají využít vaše chytrá domácí zařízení k rozsáhlým útokům. Mnozí se domnívají, že útok botnetu Mirai byl největším útokem DDoS svého druhu a že je důrazným varováním pro regulační orgány a výrobce zařízení, aby vyvíjeli silnější a komplexnější ochranu chytrých domácností IoT na úrovni sítě.

**Chytré vytápění, které zamrzlo**

Další útok DDoS (Distributed Denial of Service), který se v roce 2016 dostal do zpráv, se týkal dvou bytových domů v Lappeenrantě, městě s přibližně 60 000 obyvateli na východě Finska.

Tentokrát se útok zaměřil na systémy, které v budovách řídily centrální vytápění a cirkulaci teplé vody. Tím, že hackeři donutili topné systémy vstoupit do nekonečné restartovací smyčky, účinně přerušili distribuci centrálního vytápění pro obyvatele, a to v době, kdy se teploty ve Finsku pohybovaly pod bodem mrazu. Stejný systém, který byl vyvinut na podporu automatizace a snížení neefektivity a nepohodlí ručně udržovaného vytápění, nechal obyvatele na holičkách.

Naštěstí po odpojení [dotčených systémů inteligentní domácnosti](https://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639) od internetu se vytápění obnovilo v normálním režimu. Specialista na údržbu budov Sami Orasaari situaci komentoval, že skutečný [problém spočívá v přístupu lidí k zabezpečení chytrých zařízení](http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter), protože mnoho bytových společností nebo soukromých vlastníků nechce investovat do síťových firewallů a zabezpečení obecně bývá laxní.

Není to však jen chytré ústřední topení, které je náchylné k napadení. Obětí hackerů se staly i [chytré termostaty renomovaných značek](https://www.chicagotribune.com/business/ct-biz-nest-cameras-hacked-20190204-story.html). Internetoví záškodníci nyní mohou převzít kontrolu nad vaším termostatem a zvýšit teplotu, když zrovna nejste doma a vy o tom nebudete vědět, dokud vám nepřijde šokující účet za elektřinu nebo plyn.

**Hazard s internetem věcí, který se nevyplatil**

Ačkoli tento útok technicky vzato neovlivnil chytrou domácnost, tento typ útoku by mohl snadno ovlivnit milovníky akvárií v jejich vlastním domě. V roce 2018 bylo jedno [kasino napadeno prostřednictvím chytrého teploměru](https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4) v akváriu ve vstupní hale.

Podle Nicole Eaganové, CEO kyberbezpečnostní společnosti Darktrace, hackeři použili teploměr připojený k internetu, aby se dostali do sítě, "našli databázi významných hráčů a pak ji přenesli zpět přes síť ven z termostatu a do cloudu".

Představte si, že by se to stalo s vaší kreditní kartou a osobními identifikačními údaji. Najednou už nadšení z toho, že je váš domov chytřejší, není tak velké. Naštěstí existuje řada způsobů, jak můžeme posílit zabezpečení našich chytrých domácností proti hackerům. Například aplikace mydlink společnosti D-Link umožňuje uživatelům ovládat a monitorovat zařízení mydlink pro chytré domácnosti – například videokamery, chytré zástrčky nebo senzory, a to přímo z chytrého telefonu nebo tabletu.

**Hacky, které mohou ovlivnit váš život i mimo chytrý domov**

Chytrá auta technicky nespadají do útulné sféry domácích chytrých domácích spotřebičů. Přesto si myslíme, že vzhledem k tomu, že stále více výrobců automobilů, jako je například Tesla nebo Ford, rozšiřuje nabídku chytrých vozů, stojí za to zmínit tento případ z hlediska chytré a propojené domácnosti.

V roce 2015 bezpečnostní výzkumníci demonstrovali, jak snadné je [nabourat se do vozu Jeep Cherokee](https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/) a převzít kontrolu nad vším od klimatizace až po stěrače. Testovací řidič si všiml, že ačkoli se nedotkl přístrojové desky, ventilační průduchy v Jeepu Cherokee začaly pouštět studený vzduch na maximální nastavení, stejně tak se na maximum spustilo i chlazení v sedadle řidiče. Dále se přepnulo rádio na místní hiphopovou stanici hrající na plnou hlasitost a nereagovalo na řidičovy pokusy o vypnutí.

Zatímco se testovací řidič věnoval těmto problémům, zapnuly se stěrače a ostřikování, které zhoršilo výhled z auta. Přestože nedošlo k zásahu do volantu a brzd, jiné poruchy by stačily k tomu, aby došlo k nehodě. Chytrému hackerovi ve skutečnosti stačí, aby řidiče rozptýlil drobnostmi, jako je zhoršení výhledu nebo stahování oken proti řidičově vůli. Dokud je vozidlo připojeno k internetu, například když se nabíjí v garáži, stává se potenciální vstupní branou pro hackery, kteří mohou proniknout dovnitř a proměnit radostnou jízdu v noční můru.

**Závěrem**

Je snadné mávnout rukou nad některým z těchto útoků na chytré domácnosti a internet věcí a říkat si, že nám se to nestane. Ale upřímně, neříkáme si to všichni? Sníme o chytrém, propojeném životním stylu, který nám usnadňuje život. Bohužel zkušenosti ukazují, že hackeři chytrých domácností a internetu věcí jsou sofistikovanější než kdy dříve a jsou ochotni zkoumat vaše chytrá domácí zařízení jen aby objevili sebemenší slabiny.

Když chcete do své domácnosti přidat a nastavit chytrá zařízení, můžete myslet na několik jednoduchých věcí, které minimalizují pravděpodobnost výše zmíněných scénářů. Například při výběru kamer pro sledování domácnosti nebo chůviček volte čistě cloudová řešení, jako je například [mydlink](https://eu.dlink.com/cz/cs/for-home/smart-home). Ta poskytují end-to-end šifrování prostřednictvím cloudu, které eliminuje riziko hacknutí kamer a přístupu přímo z internetu. Takové řešení může také nabídnout kompletní ekosystém chytré domácnosti, který vám umožní sledovat váš domov a také přidat další senzory a chytré zástrčky pro zapínání a vypínání spotřebičů, ať už jste v domě nebo mimo něj.

Vždy se také vyplatí aktualizovat hesla a firmware, abyste průběžně obnovovali ochranu zařízení. Také vždy změňte všechna výchozí hesla zařízení a služeb. Starší zařízení mají často výchozí heslo nastavené výrobcem a často bývá stejné napříč produkty. Pokud není změněno, může být zařízení velmi náchylné k útokům.

Důležitým faktorem je také seznámení se s bezpečnostními ovládacími prvky routeru a jeho konfigurace pro regulaci vystavení internetu. Například pouhé zakázání vzdáleného přístupu na směrovači může zabránit možnosti, že by nad ním hacker převzal kontrolu. Samozřejmě se ujistěte, že máte i odpovídající antivirovou a antimalwarovou ochranu na všech počítačích a laptopech v domácnosti, protože i ty mohou být pro hackera cestou, jak se dostat k vašim chytrým domácím zařízením.

A konečně, před nákupem nového zařízení do vaší domácnosti je užitečné zjistit si, jakými funkcemi je vybavené. Ujistěte se, že vybíráte zařízení, která zahrnují kvalitu a zabezpečení jako hlavní funkce. Provedení inventury a průzkumu zařízení, která již vlastníte a zjištění, jak fungují ve spojení s vaší chytrou domácností může být také velmi přínosné pro zlepšení zabezpečení vaší domácnosti.

**O společnosti D-Link**

Společnost D-Link již více než 30 let navrhuje, vyvíjí a vyrábí oceňovaná síťová a bezdrátová zařízení, zabezpečovací řešení pro IP kamerové systémy a technologie pro automatizaci domácnosti. Jako světový lídr v oblasti konektivity, společnost D-Link transformuje firemní sítě a jejich vybavení tak, aby fungovaly efektivněji. Je také klíčovým inovátorem v oblasti chytrých domácností. Umožňuje majitelům nemovitostí monitorovat, automatizovat a ovládat domácnost kdykoliv a kdekoliv i pomocí chytrého telefonu nebo tabletu.

D-Link nabízí své rozsáhlé produktové portfolio organizacím a spotřebitelům prostřednictvím své globální sítě obchodních partnerů a poskytovatelů služeb.

Pro více informací o společnosti D-Link navštivte [www.dlink.cz](http://www.dlink.cz) nebo [www.facebook.com/dlinkcz](file:///C%3A%5CUsers%5CLucie%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CN1THH0N2%5Cwww.facebook.com%5Cdlinkcz) nebo [www.linkedin.com/company/dlinkcz](http://www.linkedin.com/company/dlinkcz)

V případě zájmu o další informace prosím kontaktujte:

**D-Link s.r.o.** **Taktiq Communications s.r.o.**

Na Strži 1702/65 Ondřej Mádle

140 62 Praha 4 Tel.: +420 739 610 370

Tel.: +420 224 247 500 E-mail: ondrej.madle@taktiq.com

E-mail: info@dlink.cz

<http://www.dlink.cz/>

D-Link a loga D-Link jsou ochranné známky nebo registrované ochranné známky společnosti D-Link Corporation nebo jejích poboček. Všechny ostatní zde zmíněné značky třetích stran mohou být ochrannými známkami příslušných vlastníků. Copyright © 2020. D-Link. Všechna práva vyhrazena.