Průvodce kybernetickým zabezpečením

pro rok 2018:

# Hackeři a ochránci využívají návrhové a strojové učení

# Obsah

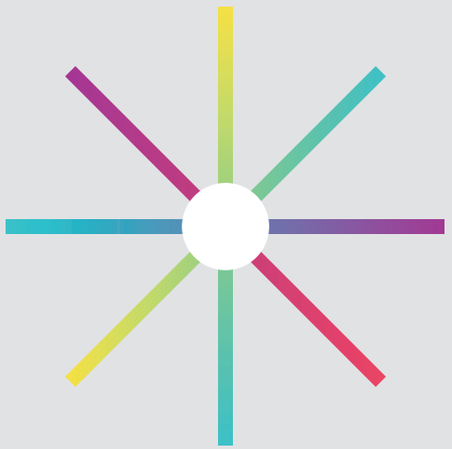

03 ⇨Úvod

04 ⇨Část 1: Zpráva o situaci

09 ⇨Část 2: Myslete jako da Vinci: Věda kybernetického zabezpečení potřebuje více umění

16 ⇨Část 3: Za zrcadlem: Strojové učení a umělá inteligence

21 ⇨Vysvětlivky

# Intro





Po celém světě se životy a živobytí čím dál více přesunují do online prostoru. Fyzický a digitální svět se začínají prolínat a za digitální peníze bez reálného ekvivalentu lze kupovat skutečné zboží a služby. Umělá inteligence stojí za rozhodováním autonomních vozidel, hledáním nových léčiv i přizpůsobováním lekcí, aby se mohli studenti více naučit.[1,2,3] Lékaři provádějí složité operace na druhé straně planety prostřednictvím internetu a robotických systémů, zatímco síťové senzory otřásají odvětvími od elektráren až po veřejnou dopravu.[4] Každým rokem se seznam odvětví transformovaných senzory, chytrými stroji a mikročipy rozšiřuje.

Asi tím jediným neměnným faktem je, že zločinci a manipulátoři využijí jakoukoli nabídnutou příležitost a zneužijí zranitelnosti k vlastnímu prospěchu. A celá řada nástrojů a technik, které přinášejí obrovské výhody celé společnosti, zároveň otevírá snazší cesty pro zlé úmysly a manipulaci s ještě většími škodami. Malwarové, phishingové a DDoS útoky jsou jen některé z triků, které se svezly na vlně digitálních pokroků posunujících náš svět kupředu.

Pro odborníky na informační bezpečnost je úspěšná obrana proti již neustálému přívalu útoků online zároveň noční můrou i motivací, proč ráno vstávat do práce. Kdo vyhrává – útočníci nebo obránci?
Vzhledem ke každodenním zprávám o úspěšných útocích, které ze dne na den ochromují společnosti a ubírají miliony dolarů z hodnoty akcií, je to složitá otázka.[5]

Abychom zaostřili na aktuální a budoucí stav kybernetické bezpečnosti, sestavili jsme společně s odborníky na kybernetické zabezpečení tohoto aktuálního průvodce. Společnost HP shromáždila názory těch největších mozků v oblasti zabezpečení informací, aby pomohla rozhodujícím pracovníkům zodpovědným za informační bezpečnost ve středních a velkých firmách porozumět všem dostupným možnostem, jak předcházet škodám způsobeným kybernetickými zločiny.

# Část 1:

# Zpráva o situaci

# Nový druh malwaru se na internetu objeví přibližně každé čtyři vteřiny.

Dnes bude zaznamenáno 6 až 11 milionů nových malwarových infekcí v počítačích používajících jen jeden z typů antivirového softwaru.[6] Přibližně 700 phishingových útoků bude spuštěno s úmyslem přimět nic netušící uživatele kliknout na klamavý odkaz, který podvodníkům umožní odcizit osobní data nebo získat přístup k firemní síti.[7] Nový druh malwaru se na internetu objeví přibližně každé čtyři vteřiny.[8]

Neznámý počet hackerů utratí přibližně 150 dolarů za pronájem botnetu na týden, aby spustili útok DDoS (Distributed Denial-Of-Service) s cílem uvést online službu nebo síť mimo provoz přetížením[9]. V součtu po celém světě vystřílí tyto útoky 500 gigabitů dat za sekundu na firemní a vládní servery za účelem vyčerpat provozní kapacitu sítě a znemožnit činnost cílů.[10,11]

Mezitím budou miliony počítačů a síťových tiskáren, kamer, termostatů a dalších zařízení internetu věcí (IoT) čekat nezabezpečené, bez instalace nejnovějších bezpečnostních záplat, na osobu se špatnými úmysly, která si díky nim najde otevřené dveře k těm nejcitlivějším datům organizace.[12]

Výsledkem je neustálý příval novinových zpráv o úspěšných vniknutích do sítí, které by měly být zabezpečené. Jen během prvních několika dnů roku 2018 zastavil ransomware provoz sítě regionálních nemocnic se žádostí o výkupné v bitcoinech. Napadeny byly také počítačové systémy jedné městské správy a všech škol jednoho okresu v USA.[13,14,15]
Zároveň byla objevena masivní chyba zabezpečení v mikročipech, kvůli které mohou být ohroženy všechny moderní počítače, na které nebude instalována oprava.[16]

Je zřejmé, že tyto útoky – téměř vždy finančně motivované – necílí pouze na skupiny jako únik dat indických bank z roku 2016 nebo velké organizace jako Sony, Equifax a Yahoo.[16] Hackeři se pokoušejí vydírat také malé a střední firmy, poskytovatele zdravotní péče, městské správní úřady a jiné sítě.[18]
Finanční lákavost je skutečně taková, že rozsah hrozby stále narůstá.
Jedna analýza odhaduje škody kyberzločinu do roku 2021 na neuvěřitelných 6 bilionů dolarů, což přesahuje i zisky celosvětového prodeje nelegálních drog.[19]

## Nezanedbávejte samozřejmé

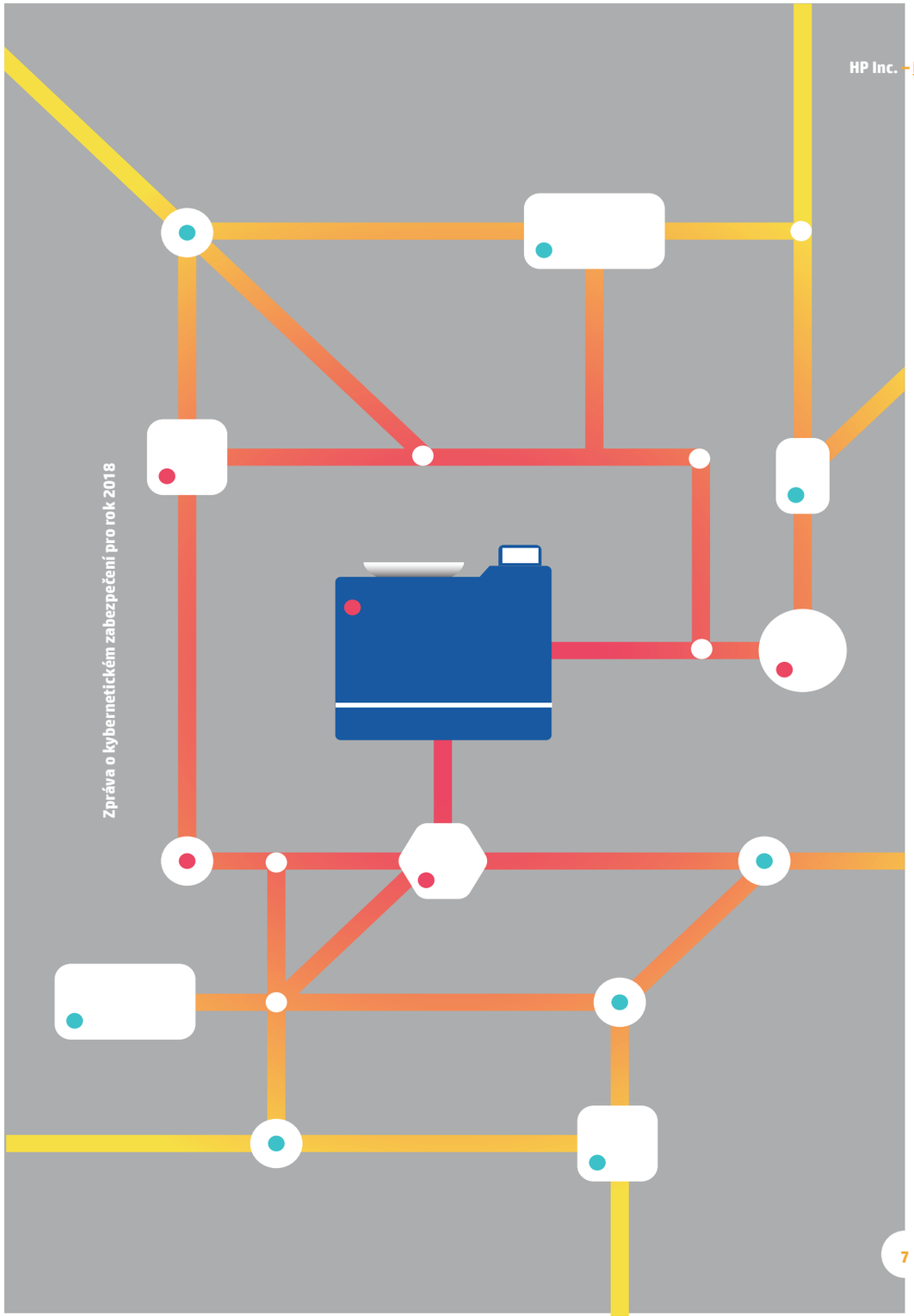
Jason O'Keeffe, odborník na informační bezpečnost a poradce pro zabezpečení tisku ve společnosti HP, tyto hrozby důvěrně zná. Ví, že pachatelům hodně pomáhá nedbalé chování počítačových uživatelů a nedostatečná ochrana proti kybernetickým útokům způsobená neexistujícím nebo přetíženým personálem, který má mít kybernetické zabezpečení na starosti.[20]

Při vyhodnocování zranitelnosti počítačových sítí firem viděl pan O'Keeffe všemožné problémy, které hackerům usnadňují práci, včetně do očí bijících opomenutí, kterých by se IT oddělení neměla dopouštět.

Při jednom takovém auditu byl pan O'Keeffe požádán, aby proslídil infrastrukturu IT obrovského výrobce. Kromě mnoha jiných problémů zjistil, že výchozí továrně nastavená hesla nebyla u 90 procent z 36 000 tiskáren v rámci celé sítě společnosti změněna, takže mohl kdokoli s patřičnými znalostmi obejít veškeré zabezpečení těchto zařízení. Dalším zkoumáním pan O'Keeffe odhalil, že mnohé z tiskáren byly nesprávně nakonfigurované, což by mohlo umožnit nepovolané osobě získat přístup k tiskárnám a překonfigurovat je za účelem krádeže dat ze sítě – nebo je dokonce zneužít jako botnet. „Viceprezident tehdy praštil do stolu a řekl mi: ‚Jasone, to snad nemyslíš vážně!?'" vzpomíná O'Keeffe. „Byl vzteky bez sebe."

A kvůli rychlému rozšiřování zařízení IoT a dalších přístrojů připojených k externímu internetu i k interní firemní síti bez nutnosti odpovídajícího ověření mají zločinci k dispozici rychle se rozrůstající paletu přístupových bodů. Doba, kdy mohl mít manažer informační bezpečnosti pocit, že je jeho práce hotová, když jsou dostatečně chráněny klíčové servery v jádru firemního systému, je nenávratně pryč. Nyní musí tento štít zabezpečení zahrnovat někdy i miliony připojených zařízení ve vzdálených pobočkách – a také v kapsách zaměstnanců.

„Snažíme se chránit počítače, servery a další klíčové součásti sítí, ale právě zařízení IoT jsou ta, která nyní zvyšují riziko v sítích," říká Shivaun Albright, hlavní technoložka společnosti HP pro zabezpečení tisku.[21] „Na každých 100 řádků napsaného zdrojového kódu obvykle připadne jedna chyba. Takže jediné, co musí hacker udělat, je najít chybu, která mu umožní přístup do systému. Snažíme se proto zajistit, aby potenciálně zranitelných míst bylo co nejméně."





# Přístup odkudkoli

Obrovský potenciál zisku je to, co podporuje inovaci a kreativitu dnešních hackerů. Jednou z největších hrozeb jsou podle Albrightové botnety – automatické nástroje vytvořené z tisíců napadených zařízení IoT. Aby podvodník vytvořil botnet, unese procesory nezabezpečených přístrojů, které pak použije k těžbě bitcoinu. Také může botnet pronajmout jiné osobě, která ho použije k uskutečnění útoku DDoS s cílem získat výkupné.[22]

Vzhledem k objemu neustále probíhajících pokusů o vniknutí a rostoucímu počtu vstupních cest tvrdí pan O'Keeffe spolu s dalšími odborníky, že mají manažeři zabezpečení raději považovat své okrajové sítě za již prolomené. „Členové komunity zabezpečení musí plně přijmout skutečnost, že jejich sítě jsou možná již narušené, i když o tom ještě neví," prohlašuje O'Keeffe.

Z protokolů kybernetického zabezpečení více než 50 malých firem i velkých podniků, které pan O'Keeffe analyzoval, měla prý každá zranitelná místa, která by hackerovi umožnila získat přístup do sítě prostřednictvím některé z tiskáren, kamer, mobilních zařízení či jiných připojených koncových bodů.

Klíč k udržování sítě v bezpečí tedy spočívá v poskytnutí nástrojů pro pracovníky IT, které jim umožní detekovat vniknutí a chránit koncové body – snadno přehlédnutelné příležitosti k přístupu, které odhodlaný nepřítel zneužije, pokud nejsou správně chráněny. A pokud k vniknutí dojde, zdůrazňuje O'Keeffe, je zásadní mít zavedenou robustní obnovovací reakci pro rychlé zastavení útoku a navrácení škod.

Daniel Kalai, zakladatel společností poskytujících služby správy IT, ke kterým patří firma Shieldly zabezpečující domácnosti a malé firmy, souhlasí jako paní Albrightová a pan O'Keeffe, že je třeba se zaměřit na zabezpečení okrajů a koncových bodů sítí.[23] Věří však, že kyvadlo se již zhouplo příliš daleko od přemýšlení nad prevencí k přehnanému zaměření na následnou obnovu. Nesouhlasí s představou, že síť s narušenou bezpečností je v dnešním digitálním prostředí nevyhnutelná.

„Kybernetické zabezpečení kdysi spočívalo v prevenci," říká pan Kalai. „Dnes se však obrovská část zabývá nápravou škod. Je to smutný pohled na věc, který vyplývá ze ztráty důvěry v preventivní nástroje. Za účelem předcházení útokům však lze udělat mnoho."

## Cena za selhání

Lepší využití zabezpečovacích zařízení, standardů a protokolů by jistě zlepšilo výhledy pro ty, kteří přistupují ke svým programům kybernetického zabezpečení pečlivě, reálná čísla však ukazují, že existuje obrovská mezera mezi plánováním a realizací.[23] A přestože jsou na všechny organizace cíleny stejné hrozby, problém je větší u menších firem, protože nemají stejné finanční prostředky, časové možnosti a nástroje školení jako větší organizace.[25]

Proto musí každá osoba, která má na starosti informační bezpečnost společnosti, pamatovat na možné důsledky: potenciální ztráty v řádu milionů dolarů, snížení důvěryhodnosti v očích zákazníků, soudní procesy a obrovské narušení běžného provozu.

Podle zprávy institutu Ponemon, nezávislé skupiny zkoumající informační bezpečnost, dosahovaly v roce 2017 průměrné náklady spojené s únikem dat výše 3,62 milionů USD.[26] Výzkumníci se ptali výkonných pracovníků ve 419 společnostech ze 13 zemí a zjistili, že každý ztracený nebo ukradený záznam stál přibližně 141 dolarů, takže se konečné číslo s rostoucím rozsahem těchto incidentů rychle znásobí. Tato studie navíc zjistila, že velikost průměrného narušení bezpečnosti se v roce 2017 zvýšila meziročně o 1,8 procenta.

Každá ze společností, které poskytly informace institutu Ponemon, uvedly narušení v důsledku zločinného útoku, poruchy systému nebo lidské chyby, přičemž počet záznamů zasažených každým incidentem se pohyboval od 2 600 do téměř 100 000. Zjištění a zastavení úniku informací trvalo respondentům studie průměrně více než dva měsíce.

## Malware je stále chytřejší

Jonathan Griffin, vyšší výzkumník zabezpečení v laboratořích HP, říká, že přibývá široce medializovaných útoků, které dosahují „šokující úrovně škod", včetně útoku NotPetya z roku 2017, který ovlivnil společnosti v USA i celé Evropě a jehož primární účel byl zřejmě čistě destruktivní.[27] Stejně jako v případě mnoha jiných úspěšných útoků byla i ochrana proti útoku WannaCry dostupná před epidemií. Mnohé organizace, malé i velké, však bohužel nenainstalovaly jednoduché softwarové opravy, které byl vniknutí zabránily.

Úspěšné vniknutí však není jen znakem nedostatečného zabezpečení. V malwarové laboratoři společnosti HP si pan Griffin a jeho tým všimli, že za poslední tři roky narostla velikost a složitost malwaru. Tyto programy mají nyní výrazně lepší funkce srovnatelné s dobře navrženým a vysoce kvalitním komerčním softwarem. Griffin tvrdí, že zločinci a státem placení hackeři jsou dobře organizovaní a velmi schopní technici, kteří neustále zdokonalují své dovednosti a zahrnují nové nástroje, mezi které patří i strojové učení umožňující systémům učit se ze zkušeností a samostatně se zdokonalovat bez explicitního programování.

> Kombinace rostoucí složitosti útoků a nedostatečného důrazu na kybernetické zabezpečení zvyšuje riziko pro firemní sítě.

Kombinace rostoucí složitosti útoků a nedostatečného důrazu na kybernetické zabezpečení zvyšuje riziko pro firemní sítě. Pan Griffin však dodává, že mnoho počítačových inženýrů a vědců po celém světě ale pracuje na zdokonalování obrany. A odborníci se shodují, že si organizace konečně začínají uvědomovat, že nasazení brány firewall a antivirového softwaru je jen začátkem efektivního programu, pro který jsou nezbytné další ochranné vrstvy a detekce vniknutí.

Část 2:

# Myslete jako da Vinci: Věda kybernetického zabezpečení potřebuje více umění

# Současné a budoucí hrozby kybernetické bezpečnosti vyžadují kombinaci vědy a umění.





Výraz „renesanční člověk“ pro někoho, jehož schopnosti a dovednosti zahrnují rozličná odvětví, byl stvořen v souvislosti s Leonardem da Vinci. Autor mistrovských děl, mezi které patří Poslední večeře či Mona Lisa, byl stejně tak inženýrem, jako umělcem.
Během téměř dvaceti let, kdy byl vojenským inženýrem, posílil da Vinci obranný systém Milána a zároveň také vynalezl a zdokonalil jeho zbraně. Během svého života také vytvářel a zdokonaloval techniky stavby mostů a vylepšoval součásti strojů, například šneková soukolí a setrvačníky. Byl odborníkem na hydrauliku a navrhl dokonce i pružinou poháněný automobil.

Svět kybernetického zabezpečení by potřeboval pár lekcí od mistra. Současné a budoucí hrozby kybernetické bezpečnosti vyžadují kombinaci vědy a umění – obzvláště s ohledem na návrh.

Osoby pověřené zabezpečením informací v podniku musejí brát do úvahy všechny fyzické a digitální prostředky připojené k organizaci, jejich umístění v rámci sítě, jejich způsob připojení a také jejich vzájemné vztahy. Možná ještě důležitější je, aby bylo skutečné pracovní používání koncových bodů (smartphonů, tiskáren a notebooků) ze strany zaměstnanců v jádru návrhu zabezpečení a architektury.

Koneckonců, nejlepší ochrana udrží síť v bezpečí bez toho, aby o ní uživatelé vůbec věděli. Užitečná mantra pro manažery informační bezpečnosti:
Chytré technologie, nenápadná řešení a přizpůsobení hrozbám.

## Aktivní monitorování je zásadní

Allen Kent je konzultant v oblasti kybernetické bezpečnosti pracující pro společnost NAES Corporation, která poskytuje řadu služeb pro odvětví od elektráren až po papírny.[28] Pan Kent zkoumá elektrárny až dvakrát ročně, přičemž hledá mezery v kybernetickém zabezpečení. Je povoláván k auditu výrobců elektřiny, vlastníků přenosových soustav a distributorů, aby byli připraveni na povinné federální kontroly kybernetické ochrany.

Tyto federální audity jsou prováděny jednou za tři až šest let v závislosti na tom, jaký dopad by narušení činnosti dané entity pravděpodobně mělo na stabilitu celé elektrické sítě. U většiny výrobců elektřiny jsou dopady překvapivě považovány za nízké. Potenciál většího dopadu by vznikl v případě systémového problému v rámci takzvaného řídicího střediska vyrovnávací autority, které řídí kolísající dodávky a poptávky elektrické energie mezi různými oblastmi a celou zemí.

Než začal pan Kent pracovat v rámci klíčové infrastruktury výroby elektrické energie, zabýval se kybernetickou bezpečností v oblasti bankovnictví. Způsoby, jak bránit útokům organizovaných zločineckých syndikátů i státních aparátů, už tedy hledá celá léta. Prohlašuje, že navzdory výrazně většímu objemu práce, kterou musejí energetické společnosti vykonat, aby vyhověly federálním standardům, je jejich kybernetické zabezpečení ve srovnání s finančním sektorem docela v pořádku. „Nic skvělého," říká, „ale OK."

Jednou z největších výzev, kterým Kent čelí, je podle něj přesvědčit manažery, že neexistuje dostačující instantní řešení kybernetické bezpečnosti, které by mohli nainstalovat a zapomenout na něj. „Obranu je třeba neustále monitorovat," tvrdí. „Většina menších společností v jakémkoli odvětví však nechce platit někoho, kdo to bude dělat. Jedná se o trvalý výdaj bez návratnosti – dokud nedojde k události se škodami, které mnohonásobně překročí ušetřené mzdové náklady.

Pan Kent říká společnostem, že mají zahájit svůj program kybernetické bezpečnosti provedením čtyř kroků: nainstalujte bránu firewall a zajistěte její konfiguraci pro správnou funkci; zaveďte systémy monitorující a filtrující nebezpečný či podezřelý obsah z e-mailů a webových prohlížečů; oddělujte chráněné prostředky od těch, které nemají stejnou úroveň ochrany (například v případě výrobce elektřiny by měly být počítače řízení elektrárny oddělené od počítačů používaných pro obchodní provoz); a stanovte protokoly, osoby a software pro aktivní monitorování všeho. Toto je standardní model kybernetického zabezpečení, který se nazývá „obvodová ochrana". Tvoří digitální stěny a systémy detekce vniknutí, aby se vetřelci nedostali dovnitř.

Nyní jsou však k dispozici nové zbraně, které manažerům kybernetické bezpečnosti nabízejí možnost útoku. Není tomu příliš nedávno, kdy odborníci věřili, že žádná preventivní strategie nedokáže zachytit všechny nové hrozby na internetu. Dnešní automatizované detekční nástroje však začínají sledovat své sítě v akci a učí se, jak se v nich normálně pohybují data, takže mohou detekovat a zastavit vniknutí, než přerostou v incidenty se škodami. Zdánlivě bezvýznamná událost, jako například notebook odesílající gigabajty dat mimo síť, přestože běžně přenáší stovky megabajtů, může spustit výstrahu.

**Čtyři pilíře kybernetického zabezpečení sítě:**

**01** **Instalace brány firewall**

**02** **Monitorování a filtrování nebezpečného či podezřelého obsahu**

**03** **Samostatné chráněné prostředky**

**04** **Stanovení protokolů**



**„Musíte mít schopnost detekce, reakce a obnovení ve vysoké rychlosti a měřítku.“**

**VALI ALI**
**člen vědecké skupiny a hlavní technolog společnosti HP**

## Vrstvy nejsou jen u zimního oblečení

„Potřebujeme budovat zařízení tak, aby měla několik úrovní ochrany,“ říká paní Albrightová ze společnosti HP. „Říkáme tomu hloubková ochrana. Protože se nelze chránit proti všemu, je třeba mít schopnost rozpoznat nenormální chování zařízení, které by mohlo ukazovat na útok.“

Ještě o krok dále jde Vali Ali, člen vědecké skupiny a hlavní technolog společnosti HP, který tvrdí, že bezpečnostní a detekční možnosti musejí být integrovány do zařízení pracujících v síti, ne přidávány dodatečně.[29] Inteligentní zabezpečení, tedy software, který detekuje příchozí hrozby, automaticky je zastaví a vymaže malware z přístroje, dosáhly během posledních let rychlého pokroku. Aby však fungovaly optimálně, musejí být integrovány tak, aby byly pro uživatele neviditelné, a zároveň dostatečně flexibilní pro odražení celé řady útoků.

Nákupy pro prostředí IT musejí být také uskutečňovány pouze po pečlivém zvážení a vyhledání vybavení, které zároveň udělá svou práci a ochrání uživatele a data. „Každý nákup zařízení je rozhodnutím o zabezpečení,“ prohlašuje pan Ali a dodává, že zabezpečení je kombinací technologie, přehledu, zpracování a řízení.

Kromě inteligentní detekce, reakce a možností učení musejí být sítě a zařízení odolné – aby bylo možné po vniknutí rychle obnovit provoz. „Útok určitě přijde,“ tvrdí Ali. „Musíte mít schopnost detekce, reakce a obnovení ve vysoké rychlosti a měřítku.“

# Nebezpečí na okraji sítě

Některé velké podnikové organizace mají prostředky k rozšíření ochrany i na okraje svých sítí. Mnoho středních firem a podniků však neuzamklo všechny své smartphony, skenery, tiskárny a zařízení IoT.[30] Paní Albrightová ze společnosti HP říká, že při rozhovorech se zákazníky často naráží na nečekaný nedostatek zájmu o zabezpečení koncových bodů složitých sítí.

„Překvapuje mne, že mnoho zákazníků si velmi dobře uvědomuje, že existuje riziko pro jejich počítače, servery a síťová zařízení, jako jsou přepínače a směrovače, obvykle však nemají žádné obavy o tiskárny či jiná zařízení IoT," prohlašuje. „A právě v této oblasti se snažíme zvyšovat povědomí a informovanost o tom, že jakýkoli koncový bod ve vaší síti, který je odhalený nebo nezabezpečený může ohrozit celou vaši infrastrukturu."

Nejprve se však musí oddělení IT ujistit, že jsou pokryty základy: 1) vývoj a dodržování přísných protokolů zabezpečení, včetně požadavků na okamžitou změnu továrně nastavených hesel a přístupových kódů údržby ve všech zařízeních; 2) dodržování plánů včasné instalace bezpečnostních oprav a aktualizací všech zařízení v síti; 3) nastavení automatické či naléhavé aktualizace operačních systémů a aplikací, bran firewall a antivirových definic. Společnosti musejí také pečlivě udržovat aktuálnost svých seznamů zaměstnanců a rychle odstraňovat přístupová oprávnění bývalých zaměstnanců.

Pan Ali tvrdí, že je také nezbytné zahrnout aktuální chápání rozvoje moderní kanceláře. Zaměstnanci stále častěji očekávají možnost pracovat kdykoli a odkudkoli, a jejich pracovní doba a volný čas se prolínají – práci mohou udělat na pláži, zatímco čas na odpočinek si mohou najít v kanceláři. „Kanceláře budoucnosti mají otevřené hranice," říká Ali. „Je to prostředí typu 24/7, 365, ve kterém se osobní a pracovní život mísí dohromady." Síťová infrastruktura, zařízení a technologie musejí s touto změnou udržet krok.

Výzkumník zabezpečení, pan Griffin, upozorňuje, že odborníci na kybernetické zabezpečení vedou asymetrickou válku, ve které musejí mít úspěchy každý den, zatímco nepříteli stačí jen jeden úspěch. Nabízí sedm doporučených postupů, které dlouhodobě posílí kybernetickou bezpečnost:

**01** Nastavte snadno proveditelné procesy, které nejsou příliš složité a nepůsobí jako „magie“.

**02** Poskytujte uživatelům jednoduché a konzistentní rady.

**03** Kdykoli je to možné, používejte dvouúrovňové ověřování, protože existuje velké množství problémů s hesly a zásadami firemních hesel.

**04** Nenakupujte jen podle ceny. Proměňte dobré bezpečnostní zásady v dobré bezpečnostní produkty a v dobrá rozhodnutí nákupu zabezpečení.

**05** Nespokojte se s „bezpečnostním divadýlkem“ a zaškrtáváním políček, když jde o nastavení zásad zabezpečení vaší společnosti. Ujistěte se, zda funkce zabezpečení, za které platíte skutečně zajišťují bezpečnost vaší organizace.

**06** Vytvářejte smysluplnější zprávy díky analytickým nástrojům, které informují nejen o tom, kolik útoků a virů váš bezpečnostní systém zastavil za měsíc, ale také o tom, kolik z nich bylo nových a jedinečných.

**07** Výrobci zařízení IoT by měli integrovat zabezpečení do svých produktů už od začátku a ujistit se, že jsou „bezpečné v jádru“.

## Důležitost školení zaměstnanců

Moderní boření kancelářských stěn zvýrazňuje problém, který byl vždy v jádru nedostatečného zabezpečení – lidské chování. Zaměstnanci vynechávají zdržující protokoly zabezpečení v zájmu produktivity a často si neuvědomují, že některé jejich internetové návyky jsou nebezpečné. Proto jsou drobné, nedbalé prohřešky vůči online hygieně častou příčinou spadlých sítí, odcizeného duševního vlastnictví nebo citlivých údajů o zákaznících a koncových bodů zneužitých botnety. „Vždy se najde někdo, kdo klikne na škodlivý odkaz v e-mailu,“ uzavírá paní Albrightová.

Jedna dobře známá antimalwarová společnost hlásí, že jen 3 procenta zaznamenaného malwaru se zaměřuje na technické nedostatky.[31] To znamená, že 97 procent těchto hackerů používá sociální inženýrství, aby přiměli nic netušící oběti ke kliknutí na odkaz ve phishingovém e-mailu nebo k odhalení citlivých údajů, jako jsou hesla a čísla bankovních účtů.

Proto jsou iniciativy školení klíčové jak pro personál oddělení IT vyvíjející a udržující solidní protokoly a postupy zabezpečení informací, tak pro ostatní zaměstnance za účelem minimalizace neopatrného chování, které představuje obrovskou zranitelnost zabezpečení.

Klíčové body pro školení zaměstnanců mimo oblast IT:

- Nepoužívejte stejné heslo v rámci různých osobních a pracovních systémů.
- Neponechávejte citlivé materiály v tiskárnách.
- Uzamkněte svůj počítač a zařízení, když je nepoužíváte.
- Používejte ochranné prvky na displeje, které brání jiným osobám číst informace z vaší obrazovky.
- Nikdy, nikdy, nikdy neklikejte na odkazy bez rozmyslu.

Jak návrháři, architekti a inženýři těch nejlepších systémů zahrnují chování uživatelů za účelem zdokonalení způsobu, jakým organizace zabezpečují své sítě a prostředky?

# Budoucí zbraně již dnes

Pan Ali a výzkumník zabezpečení, pan Griffin, ukazují na řadu inovací společnosti HP, které jsou nyní k dispozici pro veřejnost a které nepřekážejí produktivitě uživatelů, takže je pracovníci pravděpodobně nebudou ignorovat či obcházet.

Jeden takový pokrok je HP Secure, sada počítačových ochranných nástrojů včetně Sure View, Sure Click a Sure Start.

HP Sure View, integrovaný filtr ochrany soukromí pro počítače, který zabrání cizím osobám ve čtení informací z displeje uživatele. „To je vynikající bezpečnostní prvek," říká Griffin. „Použití je snadné, uživatelé o filtru vědí a vědí, co dělá."

HP Sure Click je hardwarově vynucené bezpečnostní opatření pro webové prohlížeče, které izoluje malware ve virtuálním počítači, aby nenakazil celý systém. „Kolikrát se vám stalo, že jste klikli na odkaz a okamžitě si řekli, ouha, na to jsem neměl klikat?' ptá se Ali. „S nástrojem Sure Click malware nevidí do vašeho skutečného počítače. Pokud dojde k neúmyslnému stažení malwaru, uživatel jednoduše zavře kartu a malware je pryč. Je to skvělé, protože tak uživatel nemusí kvůli bezpečnému brouzdání měnit své chování."

Tento druh kybernetického zabezpečení dokáže výrazně omezit faktor lidské chyby v kontextu narušení bezpečnosti sítí.

**Integrovaný ochranný filtr obrazovky HP Sure View** je volitelné příslušenství, které je třeba přidat do konfigurace při nákupu. K dispozici pouze u vybraných notebooků HP.

**Aplikace HP Sure Click** je dostupná pro vybrané platformy HP a podporuje prohlížeče Microsoft® Internet Explorer a Chromium™. Na této stránce naleznete všechny kompatibilní platformy, jakmile budou k dispozici.

**HP Sure Start Gen4** je k dispozici pro zařízení HP Elite a HP Pro 600 vybavená procesory Intel® 8. generace nebo procesory AMD.

HP Sure Start se na ochranu proti malwaru dívá novým způsobem. Analyzuje firmware systému BIOS, nejzákladnější součást operačního systému počítače – a zároveň místo, které je čím dál častěji podrobováno útokům, protože je zde detekce vniknutí velmi složitá. Bez odpovídající ochrany je malware nainstalovaný v systému BIOS neviditelný, takže může útočník získat stálou přítomnost v síti. Jedna studie, zpráva Data Breach Investigations Report společnosti Verizon z roku 2016 zjistila, že tento přístup je útočníky používán stále častěji: Analytici zaznamenali od předchozího roku 132procentní nárůst incidentů zacílených na notebooky a stolní počítače.[32]

HP Sure Start brání podvodníkům usídlit se uvnitř systému BIOS v síti. Když se počítač spouští, tato integrovaná funkce ověří, zda je systém BIOS v pořádku. Pokud není, funkce HP Sure Start automaticky obnoví kód na čistou verzi, aniž by se museli uživatel nebo oddělení IT čímkoli zabývat. „Toto je zabezpečení přímo v jádru," říká pan Ali.

Část 3:

# Za zrcadlem: Strojové učení a umělá inteligence

# Udržování digitálního prostředí v bezpečí začíná dostávat pomoc od umělé inteligence prostřednictvím strojového učení.

Zatímco současné doporučené postupy kybernetické ochrany zahrnují vrstvené technologie, biometrické přihlašování a monitorování sítě v kombinaci se školením o dobré online hygieně pro zaměstnance, udržování digitálního prostředí v bezpečí začíná dostávat pomoc od umělé inteligence prostřednictvím strojového učení.

Další pokrok společnosti HP dokáže ochránit zranitelné koncové tiskárny připojené k síti. V laboratořích společnosti HP vyvinutá a nyní dostupná – HP Connection Inspector je inteligentní, integrovaná funkce zabezpečení, která se naučí, jak vypadá normální chování tiskárny v síti a poté dává pozor na podezřelé změny. Když zjistí neobvyklá odchozí data, upozorní správce, zastaví podezřelou komunikaci a poté vynutí opravný restart, aby odstranila malware a útoku zabránila.

Tyto novinky dávají Allenu Kentovi ze společnosti NAES dávku opatrného optimismu. Čeká na dobu, kdy budou moci technici do sítě připojit zařízení, které bude hledat hrozby skryté v proudech datové komunikace, v případě zjištění vniknutí bude moci výměnu dat okamžitě zastavit a poté dokáže prostudovat podrobnosti útoku a vydedukovat, jak by podobný útok vypadal už v začátku. „Krabička s umělou inteligencí, která by vše monitorovala a zastavila by hrozbu automaticky ihned po jejím vzniku – to by bylo skvělé," míní.

## Zařízení IoT pod deštníkem zabezpečení

Zahrnutí procesorů a internetového přístupu do termostatů, pohybových snímačů, osvětlení a dalších systému umožňuje kancelářským budovám dosahovat výrazných energetických úspor podle obsazenosti, denní doby a dokonce i počasí.[33] Větrná turbína může správce upozornit, že její převodové soukolí vykazuje přílišnou míru vibrací a potřebuje pozornost.[34] Komerční proudový motor a letový počítač spolupracují na drobných změnách, které sníží spotřebu paliva a přitom zkrátí dobu trvání cesty.[35]

Tato chytrá zařízení míří také do vašich domácností v podobě chytrých termostatů, chytrých lednic, chytrých žárovek a digitálních asistentů s umělou inteligencí. V budoucnosti budeme mít také chytré protézy a oční implantáty, které budou obsahovat miniaturní procesory a umožňovat připojení k internetu. Co se ale stane, když se na ně zaměří hackeři?

„Představte si oční implantát nebo osobu s nohou z 3D tiskárny a pak si představte, že tato protéza utrpí útok na firmware nebo bude infikována ransomwarem," říká Vali Ali ze společnosti HP. „Jak by taková situace vypadala? Co by člověk dělal, kdyby najednou přišel o zrak a zobrazila se mu zpráva: ‚Zaplať, nebo nebudeš vidět'?"

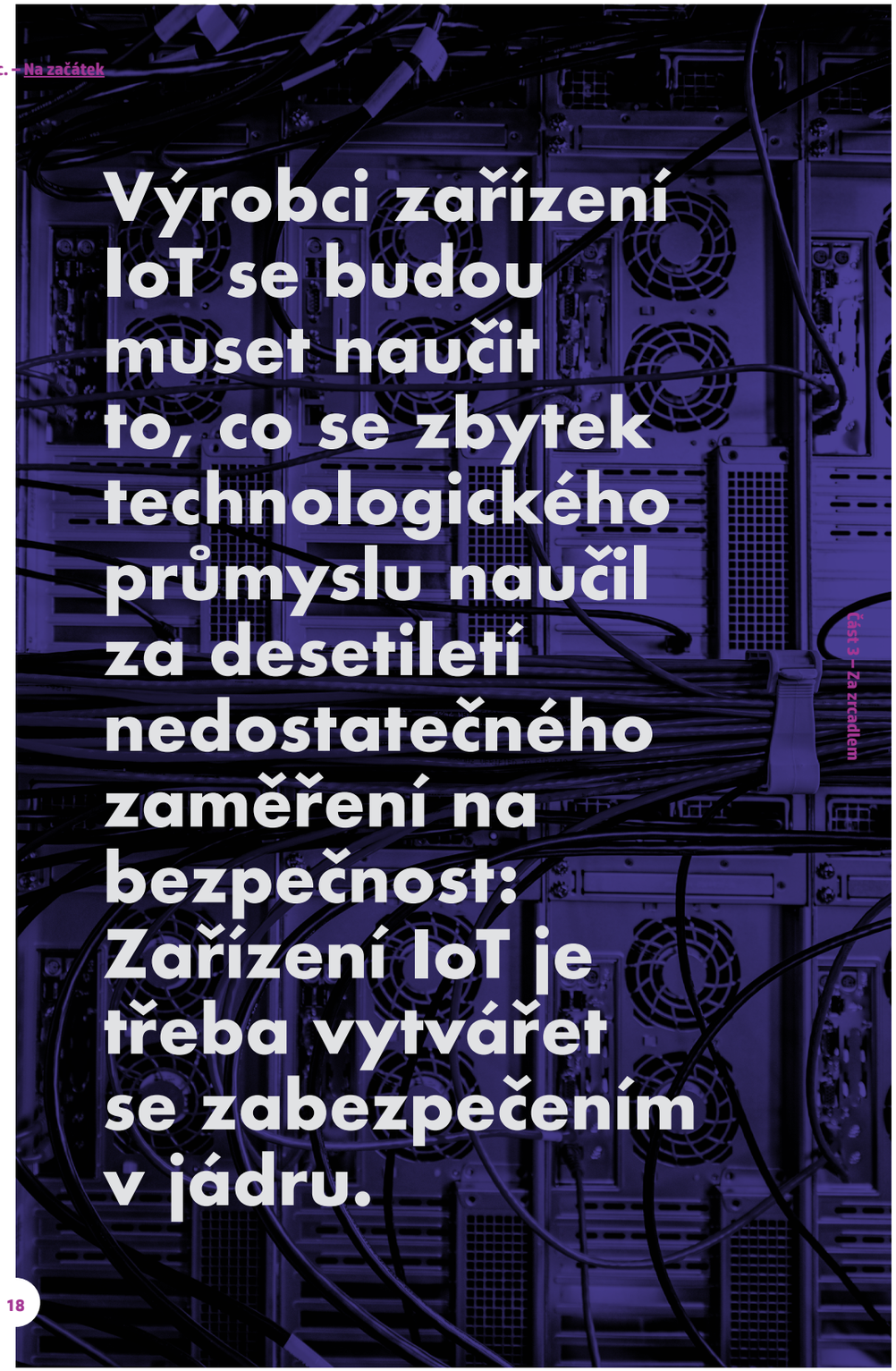
V takovém případě přichází na řadu odolnost, která infikovanému stroji umožní rychle malware vymazat a obnovit provoz v původním stavu. „V okamžiku, kdy by došlo k infikování vašeho očního implantátu malwarem nebo ransomwarem, by stačilo mrknout, malware by byl pryč a váš zrak by byl zpět," dodává Ali.

Aby to bylo možné, budou se podle Jonathana Griffina muset výrobci zařízení IoT naučit to, co se zbytek technologického průmyslu naučil za desetiletí nedostatečného zaměření na bezpečnost: Zařízení IoT je třeba vytvářet se zabezpečením v jádru. Takže pokud malware napadne chytrou žárovku, měla umět zhasnou, restartovat se, vymazat cizí kód a znovu se rozsvítit.

## Jednoduchost použití chrání proti špatnému chování

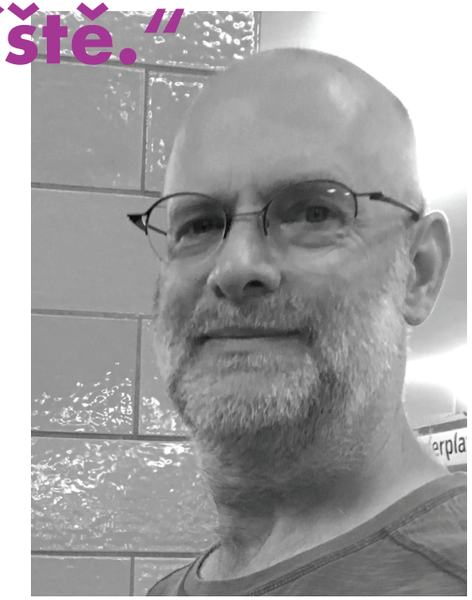
„Kdybych musel strčit klíč do dveří a potom počkat na SMS zprávu k ověření, že jsem se o vstup do svého domu pokoušel skutečně já, bylo by to pro mě nepřijatelné," říká Griffin. „Takový systém nesmí být překážkou v běžném životě."

Aby tento dlouhotrvající problém vyřešili, pracují inženýři už dlouhá léta na zdokonalení přihlašování, a počítačové rozpoznávání obličejů a snímání otisků prstů či očních sítnic konečně pomalu začíná nahrazovat zastaralá alfanumerická hesla.[36]



# „Je to závod ve zbrojení a vždy je těžké odhadnout, kam se útočníci vydají příště.“

**JONATHAN GRIFFIN,**
vyšší výzkumník zabezpečení v laboratořích HP



Další řešení, technologie WorkWise společnosti HP, kterou tvoří bezplatná aplikace dostupná v obchodě Google Play, vytváří bezpečné kryptografické spojení mezi smartphonem a počítačem zaměstnance. Díky tomuto spojení dokáže počítač poznat, když od něj uživatel odejde, a automaticky se uzamknout, aby k němu neměli přístup cizí osoby. Když se uživatel vrátí, počítač ho rozpozná a znovu ho přihlásí, aniž by vyžadoval heslo. Tato technologie je samou definicí nenápadnosti a pomáhá uživatelům zůstat v bezpečí, aniž by museli dělat něco navíc.

„Existují dva typy technologie,“ tvrdí Ali. „Ten typ, který lidé chtějí používat, a ten otravný typ, který používat musejí. Pokud se jedná o nepraktické zabezpečení, k jehož používání jsou nuceni, nakonec si najdou způsob, jak ho obcházet.“

## Strojové učení je oboustranný meč

Možnosti testování přítomnosti malwaru jako hlavního nástroje proti útočníkům jsou omezené.[37] Antimalwarový software vyžaduje aktualizaci obsahující známý kód malwaru, aby věděl, co hledat. To je však k ničemu, když se na web dostane nový škodlivý kód, což se děje s rychlostí, na kterou výzkumníci nestačí.

Na straně obránců se začíná využívat datové a strojové učení k automatické síťové analýze, která zpracovává data z neustálého toku dat tam, zpět a skrz firemní síť a hledá anomálie. Takovéto výpočetní možnosti budou jednou sledovat například výkyvy v aktivitě procesorů, což může signalizovat začínající problém. Na straně útočníků lze samozřejmě použít strojové učení k automatizaci sondování, prozkoumávání a zneužívání sítí.

Jonathan Griffin ze společnosti HP tvrdí, že strojové učení a další formy umělé inteligence již obráncům poskytují výhodu. Varuje však, že nástroje jako strojové učení nejsou všelékem. Ve skutečnosti strojové učení pravděpodobně poskytne nový prostor pro hackery, kteří se budou snažit hledat slabiny ochran na něm založených a kteří budou sami používat strojové učení a umělou inteligenci k navrhování levnějších a efektivnějších útoků. „Je to závod ve zbrojení a vždy je těžké odhadnout, kam se útočníci vydají příště,“ tvrdí.

## Vyřeší nebo zhorší umělá inteligence problém kybernetické bezpečnosti?

Pokročilé algoritmy v jádru řešení problémů strojovým učením se postupně vyvinou v robustnější systémy umělé inteligence. Útočníci s dostatečnými prostředky budou umělou inteligenci používat k sondování a útočení na sítě. Tato mocná technologie jim umožní zdokonalit triky používané k oklamání, takže budou phishingové a malwarové útoky nerozpoznatelné od legitimních e-mailů a webových stránek. Útočníci i ochránci budou umělou inteligenci používat k inteligentnímu přesměrování síťových datových proudů během útoků DDoS za účelem posílení či potlačení dopadu.

„Budeme žít ve světě umělou inteligencí umožněných chytrých útoků," tvrdí pan Ali. „Možná už k tomu dochází, ale daný systém je dostatečně chytrý na to, že jej zatím nikdo neodhalil."

V budoucnosti by měli inženýři rozvíjet možnosti dynamického učení umělé inteligence dostatečně na to, aby mohly systémy obránců používat historická data a aktuální trendy k předvídání útoků, jejich potlačování a možná dokonce k odhalování polohy pachatelů.

Prozatím se výrobci hledící kupředu jen začínají vydávat na cestu k produkci zařízení, o jakém sní pan Kent ze společnosti NAES: krabičky s umělou inteligencí. Prvním krokem je zahrnutí zabezpečení do jádra produktu od začátku procesu navrhování.

## Vítězství v nikdy nekončícím souboji se zlem

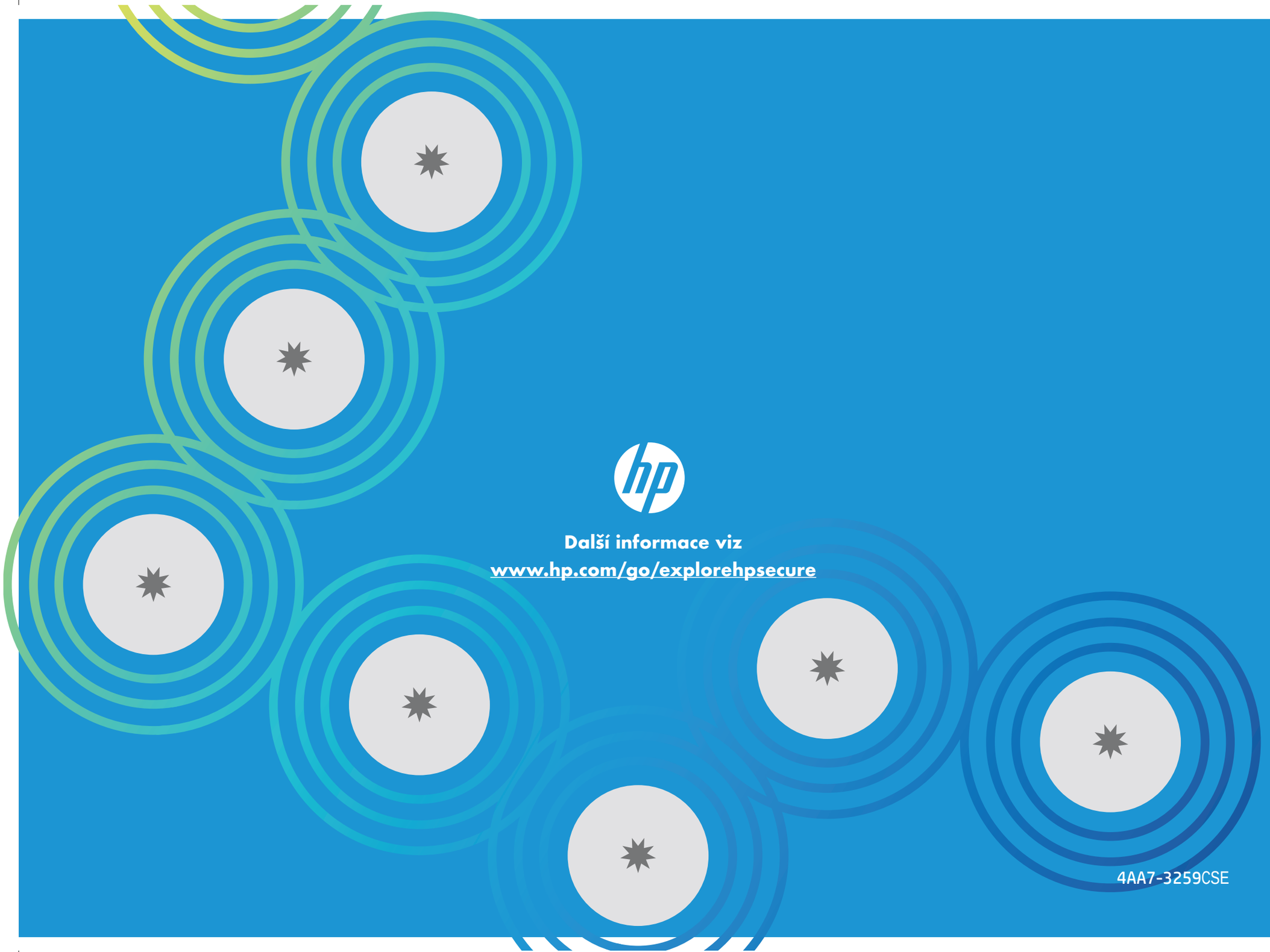
Kybernetická válka mezi dobrem a zlem nadále zuří a výsledky jsou v různých oborech velmi nevyrovnané. Zločinecké a manipulátorské skupiny se všemožně snaží infiltrovat a narušovat sítě, ve hře je hodně a hrozby nezmizí samy od sebe.

> Zuří neustálý souboj mezi dobrem a zlem. Je to souboj, který jako ti dobří nemůžeme prohrát. Je to souboj, který nesmíme prohrát. Ve společnosti HP jsme odhodlaní: Je to souboj, který neprohrajeme.

Ochrana spolehlivosti digitálních systémů, na kterých jsou vybudovány klíčové infrastruktury a správní orgány a také malé i velké firmy, je nedílnou součástí moderního života a celé společnosti. „Říkáme si, že svět tam venku je děsivý, ale je v něm i dobro," říká pan Ali ze společnosti HP. „Zuří neustálý souboj mezi dobrem a zlem. Je to souboj, který jako ti dobří nemůžeme prohrát. Je to souboj, který nesmíme prohrát. Ve společnosti HP jsme odhodlaní: Je to souboj, který neprohrajeme."

# Vysvětlivky


1. Robotics Business Review, „Robot Investments Weekly: AI, Industrial Automation, Mobility Market Drive Spending," https://www.roboticsbusinessreview.com/financial/robot-investments-weekly-ai-industrial-automation-mobility-market-drive-spending/ (ke 26. únoru 2018)
2. TechEmergence, „Machine Learning Drug Discovery Applications – Pfizer, Roche, GSK, and More," https://www.techemergence.com/machine-learning-drug-discovery-applications-pfizer-roche-gsk/ (ke 26. únoru 2018)
3. Popular Mechanics, „The Surgeon Will Skype You Now," https://www.popularmechanics.com/science/health/a19208/the-surgeon-will-skype-you-now/ (ke 26. únoru 2018)
4. CFO, „Cyber Attacks Can Cause Major Stock Drops," http://ww2.cfo.com/cyber-security-technology/2017/04/cyber-attacks-stock-drops/ (ke 26. únoru 2018)
5. Kaspersky, „Cyberthreat Real-Time Map: Local infections in the last week," https://cybermap.kaspersky.com/stats/ (ke 26. únoru 2018)
6. Anti-Phishing Working Group, „Global Phishing Survey," https://apwg.org/resources/apwg-reports/domain-use-and-trends
7. G DATA Security Blog, „Malware Trends 2017," https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017
8. Digital Attack Map, „What is a DDoS Attack?" http://www.digitalattackmap.com/understanding-ddos/
9. Digital Attack Map, „Top Daily DDoS Attacks Worldwide," http://www.digitalattackmap.com/
10. U.S. Department of Defense, „'Terabyte of Death' Cyberattack Against DoD Looms, DISA Director Warns," https://www.defense.gov/News/Article/Article/1414146/
11. HP, „HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676
12. Greenfield Daily Reporter, „Hospital Falls Victim To Hacker Attack; No Patient Records Compromised," http://www.greenfieldreporter.com/2018/01/12/hospital-falls-victim-to-hacker-attack-no-patient-records-compromised-officials-said/
13. Black Hills Pioneer, „Belle Fourche City Servers Hacked," http://www.bhpioneer.com/local_news/belle-fourche-city-servers-hacked/article_7254ad36-f576-11e7-8ed7-e31c3ee0da87.html
14. Columbia Daily Herald, „MCPS Experiences Cyber Attack," http://www.columbiadailyherald.com/news/20180105/mcps-experiences-cyber-attack
15. Bloomberg Technology, „'It Can't Be True.' Inside the Semiconductor Industry's Meltdown," https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown
16. The Economic Times of India, „3.2 Million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis Worst Hit," (placené) https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms
17. CNBC, „Virtual Extortion a Big Business for Cyber Criminals," https://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html
18. Cybersecurity Ventures, „Cybercrime Report," https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
19. Telefonický rozhovor, Jason O'Keeffe, HP (14. prosince 2017)
20. Telefonický rozhovor, Shivaun Albright, HP (15. prosince 2017)
21. CoinDesk, „Botnet Infects Half a Million Servers to Mine Thousands of Monero," https://www.coindesk.com/botnet-infects-half-million-servers-mine-thousands-monero/
22. Telefonický rozhovor, Daniel Kalai, Shieldly (10 ledna 2018)
23. Financial Times, „'Essential' services face fines for poor cyber security," (placené) https://www.ft.com/content/f2faf8cc-7b79-11e7-ab01-a13271d1ee9c
24. Houston Chronicle, „Consequences of Poor Security in a Company," http://smallbusiness.chron.com/consequences-poor-security-company-70227.html
25. IBM a Ponemon Institute, „2017 Ponemon Cost of Data Breach Study," https://www.ibm.com/security/data-breach
26. Telefonický rozhovor, Jonathan Griffin, HP (21. prosince 2017)
27. Telefonický rozhovor, Allen Kent, NAES (15. ledna 2018)
28. Telefonický rozhovor, Vali Ali, HP (15. prosince 2017)
29. Keeper Security, „2017 State of Cybersecurity in Small & Medium-sized Businesses," https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html
30. Digital Guardian, „Social-Engineering Attacks: Common Techniques & How to Prevent an Attack," https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
31. Verizon, „2016 Data Breach Investigations Report," http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
32. Intel, „Reduce Energy Costs and Carbon Footprint with Smart Building Management," https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/iot-ecs-tatung-reduce-carbon-footprint-solution-brief.pdf
33. Industrial Internet Consortium, „The Benefits of IoT Analytics for Renewable Energy," https://www.iiconsortium.org/case-studies/ParStream_Envision_Energy_Case_Study.pdf
34. Aviation Week, „Internet Of Aircraft Things: An Industry Set To Be Transformed," http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed
35. Global Cyber Alliance, „How Biometrics Can Replace Passwords," https://www.globalcyberalliance.org/how-biometrics-can-replace-passwords.html
36. Wall Street Journal, „The Limits of Antivirus Software," (placené) https://www.wsj.com/articles/the-limits-of-antivirus-software-1505700000



Další informace viz
www.hp.com/go/explorehpsecure

4AA7-3259CSE