CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

Kontakt pro média:
David Řeháček
Check Point Software Technologies
Mobil: +420 603 536 812
drehacek@checkpoint.com

Petr Cícha
Senior Account Manager
Mobil: +420 603 193 245
petr7cicha@gmail.com

Od prvního firewallu a virů až po umělou inteligenci a megaútoky: 25 let a 5 generací kyberhrozeb a bezpečnosti

Jak se za uplynulé čtvrtstoletí vyvíjely kyberhrozby a jak se vyvíjela obrana proti nim?

Praha, 19. prosince 2018 – Byla před 25 lety vaše společnost on-line? Pravděpodobně ne. Koneckonců web byl stále v plenkách, první prohlížeč byl představen v roce 1993 a jen malé procento organizací si vůbec uvědomovalo existenci internetu, natož aby si uvědomovaly potenciální bezpečnostní rizika.

Ale i v těchto počátcích veřejného internetu existovaly průkopnické společnosti, které si uvědomily, že spojení se světem může pro podnikovou síť a data představovat hrozbu. Antivirové řešení se objevilo koncem osmdesátých let a v roce 1994 se objevil první komerční firewall od společnosti Check Point. Firewall umožnil organizacím oddělit sítě a datovou komunikaci od internetu a chránit se před různými on-line riziky. I když skutečná rizika byla na začátku velmi omezená.

25 let uteklo velmi rychle a hrozby se výrazně proměnily. Rok 2017 byl z pohledu online kyberútoků nejhorším rokem, tvrdí Online Trust Alliance, počet hlášených kyberincidentů se oproti roku 2016 zdvojnásobil. Zažili jsme globální megaútoky ransomwarů WannaCry a NotPetya i úniky dat u společností Equifax a Uber. I když rok 2018 doposud nebyl tak temný, ani zdaleka také nebyl klidný. Too potvrzují například úniky dat ze společností British Airways, Under Armor nebo Ticketmaster.

Takže co předcházelo současné situaci a jak se vyvíjely hrozby a kyberbezpečnostní řešení během posledních 25 let?

První generace kyberhrozeb
I do kybersvěta můžeme přenést zákon akce a reakce. Větší dostupnost a využití osobních počítačů v 80. letech přímo souvisí s počátečním vývojem kybernástrojů a hrozeb.

První generace útoků byly počítačové viry – škodlivé programy, které se replikují na každém infikovaném počítači. Přestože sítě byly stále ještě v plenkách a viry se mohly přenášet pouze z počítače na počítač pomocí disket, napadení virem bylo natolik rušivé, že vedlo k rozvoji první generace kyberzabezpečení: Komerčních antivirových softwarových produktů.

Počátky kyberzločinu
Druhá generace útoků se objevila v 90. letech s příchodem sítí a internetu. Rozmach konektivity byl i počátkem kyberzločinu, jak ho známe dnes. Ukázkovým příkladem je krádež z roku 1994, kdy kyberútočníci ukradli přes 10 milionů dolarů ze Citibank.

Check Point v této době vyvinul a představil vůbec první stavový firewall. Vzhledem k propojování interních sítí s internetem se stala kombinace stavových firewallů a antivirového softwaru základem podnikové ochrany. I dnes se jedná o jeden ze základů každé bezpečnostní infrastruktury.

Boom exploitů
Nová generace kyberbezpečnosti se objevila na počátku roku 2000, když se útočníci naučili využívat zranitelností ve všech částech IT infrastruktury, napříč operačními systémy, hardwarem i aplikacemi. Příkladem je červ SQLSlammer, který útočil na zranitelná místa v Microsoft SQL Server a MSDE a stal se nejrychleji šířeným červem všech dob. Útočníci byli organizovanější a sofistikovanější a zaměřovali se na získání financí nelegálními prostředky. Popularita e-mailů dala kyberzločincům do rukou nové možnosti sociálního inženýrství, jak šířit útoky napříč organizacemi i zeměmi.

Tato éra také znamenala explozi technologií a služeb, což vedlo k nárůstu počtu bezpečnostních dodavatelů a produktů. Každý nový bezpečnostní produkt měl ale vlastní uživatelské rozhraní a konzoli pro správu, což přidělávalo bezpečnostním a IT týmům práci, zvyšovala se složitost bezpečnostních systémů a rostla neefektivnost. A co je nejdůležitější, bezpečnostní infrastruktury v organizacích začaly zaostávat za rychlostí, s jakou se vyvíjela sofistikovanost a rafinovanost útoků.

Detekční řešení na zastavení kyberútoků nestačí
Rok 2010 znamenal začátek další etapy kyberútoků, protože se objevily skutečně organizované a profesionální skupiny. Útoky plnily stránky novin, měly dopad na veřejnost, organizace i vlády. Příkladem je masivní narušení bezpečnosti u amerického prodejce Target, kdy unikly informace o 40 milionech kreditních kartách a soukromé informace o 110 milionech lidí.

Kyberútoky se maskovaly a pro zaměstnance byly obtížně identifikovatelné. Malware se skrýval ve všem, od falešných obchodních dokumentů až po obrázky. Jediné, co musel uživatel udělat, bylo neúmyslně otevřít e-mailovou přílohu, stáhnout soubor z internetu nebo připojit USB do svého notebooku a útok byl nepozorovaně spuštěn. Tyto útoky čtvrté generace znamenaly, že detekční zabezpečení už na ochranu organizací nestačí. Produkty určené pouze k detekci mohou rozpoznat signatury známých útoků a ty jsou vytvořeny pouze po objevení a analýze útoku. Organizace jsou tak zranitelné dny, týdny a někdy i měsíce, dokud není k dispozici aktualizace – přestože útok může způsobit kritické škody během několika vteřin či minut. Nový a důmyslnější malware (bez signatur pro detekci) byl vyspělejší než signaturové zabezpečení. Byly proto vyvinuty nové technologie, jako je sandboxing, aby bylo možné se bránit před zero-day exploity. Ale tím ještě vzrostla složitost bezpečnostních infrastruktur.

Prevence současných megaútoků
Současná pátá generace útoků se objevila velmi nekompromisně na začátku roku 2017. Dostupnost sofistikovaných pokročilých hackovacích nástrojů vedla k masivním multivektorovým kyberkampaním, které zločincům generovaly příjmy a způsobily obrovské finanční škody a poškození pověsti. Dnešní neustále se měnící malware se může infiltrovat a rozšířit napříč prakticky jakoukoli částí IT infrastruktury, včetně on-premise sítí, cloudových prostředí, vzdálených kanceláří, mobilních zařízení atd. Příkladem jsou útoky WannaCry, který postihl 300 000 počítačů ve 150 zemích, a NotPetya, který způsobil škody ve výši 300 milionů dolarů.

Tyto útoky se pohybují s nebývalou rychlostí a snadno překonávají dřívější generace bezpečnostních technologií založených na pouhé detekci. Proto i nadále způsobují po celém světě takové škody. Podle bezpečnostní zprávy Check Point 2018 Security Report používá 97 % organizací antivir a firewall, což ale ochrání před hrozbami maximálně druhé a třetí generace. Jen 21 % respondentů používá sandboxing a ochranu proti botům, což zastaví

pokročilé hrozby čtvrté generace. Pouze 3 % společností využívá aktivní prevenci hrozeb s vrstvami pro cloudovou a mobilní bezpečnost, což je nezbytné pro ochranu před současnými kyberútoky 5. generace.

Vzhledem k rychlosti, s jakou se tyto útoky mohou šířit, už si nemůžeme dovolit po proniknutí zabezpečením čekat, než přijde reakce na hrozbu, jak bylo běžné ještě před několika lety. Místo toho musíme klást důraz na prevenci a zastavení útoků v reálném čase. Organizace musí přejít od předchozí generace neintegrovaného nasazení jednotlivých řešení ke konsolidované infrastruktuře, která přináší prevenci hrozeb napříč celou IT infrastrukturou s centralizovaným managementem pro správu, monitoring i reakci.

Tato integrovaná architektura poskytuje ochranu v reálném čase proti známým i neznámým hrozbám, využívá pokročilou prevenci před hrozbami a zero-day technologie. Informace o hrozbách jsou automaticky sdíleny napříč sítěmi, koncovými body, cloudem a mobilními zařízeními. Schopnost utěsnit mezery je kritická, protože kybernetické útoky jsou čím dál automatizovanější, používají boty, kteří skenují sítě organizací a nacházejí nejslabší místa. Abychom tomu mohli čelit, je potřeba využívat umělou inteligenci a machine learning, což pomůže rozpoznat rychle se měnící modely útoků a automatizovat reakce.

Vývoj kybernetických útoků i kyberbezpečnosti za posledních 25 let byl rychlý a stále se zrychluje. V počátku se nedalo předvídat, jak moc bude současný svět propojen a jaké kyberhrozby nás budou ohrožovat. Rozvíjení nových způsobů ochrany před těmito hrozbami je neustálou výzvou. Nicméně jedna věc je jistá: Další generace útoků bude ještě sofistikovanější, a proto musíme zajistit, aby příští generace obranných prostředků byla ještě chytřejší a budoucnost byla bezpečná.

Sledujte Check Point online:
Check Point Blog: http://blog.checkpoint.com/
Twitter: http://www.twitter.com/checkpointsw a www.twitter.com/CheckPointCzech
Facebook: http://www.facebook.com/checkpointsoftware
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies
YouTube: http://www.youtube.com/user/CPGlobal

O společnosti Check Point Software Technologies
Check Point Software Technologies Ltd. (www.checkpoint.com) je přední poskytovatel kyberbezpečnostních řešení pro vlády a organizace po celém světě. Chrání zákazníky před kyberútoky 5. generace prostřednictvím unikátních řešení, která nabízí bezkonkurenční úspěšnost zachycení malwaru, ransomwaru a jiných cílených útoků. Check Point nabízí víceúrovňovou bezpečnostní architekturu s pokročilou prevencí hrozeb 5. generace pro podnikové sítě, cloud a mobilní prostředí, Check Point navíc poskytuje nejkomplexnější a nejintuitivnější nástroje pro správu zabezpečení. Check Point chrání více než 100 000 organizací všech velikostí.