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

Petr Cícha
CoLin
Mobil: +420 603 193 245
petr.cicha@colin.cz

Kyberbezpečnostní předpověď společnosti Check Point pro rok 2016

Praha, 15. prosince 2015 – Jestli je týden dlouhá doba v politice, jak poznamenal bývalý britský premiér Harold Wilson, rok v kyberbezpečnosti se může zdát jako věčnost. Ale navzdory rychlým změnám, mnoho věcí zůstává stejných. Tři klíčové bezpečnostní předpovědi společnosti Check Point pro rok 2015 byly: Rychlý růst neznámého malwaru, nárůst mobilních hrozeb a kritických zranitelností v běžně používaných platformách (Android, iOS a dalších). Všechny tři se bohužel potvrdily a je pravděpodobné, že i nadále se bude jednat o významné hrozby. Hra na kočku a myš, která je typická pro kyberbezpečnost posledních let, pokračuje a hackeři stále hledají nové způsoby, jak napadnout sítě. Ukázalo se to letos například u masivních narušení bezpečnosti společností Anthem, Experian, Carphone Warehouse, Ashley Madison a TalkTalk.

Stejně jako většina bezpečnostních IT profesionálů, i Check Point si přeje, aby se předpovědi o nárůstu hrozeb nevyplnily a žádná společnost nebyla hacknuta a nedošlo k žádnému úniku dat. Ale předpovídat další vlnu hrozeb by mohlo, doufejme, pomoci organizacím vylepšit bezpečnostní strategie.

Očekávaných 10 bezpečnostních IT hrozeb a trendů pro rok 2016:

Cílený a masivní malware
Jsme přesvědčeni, že větší narušení bezpečnosti v roce 2016 budou výsledkem speciálně upravených škodlivých kódů, které budou vytvořené tak, aby u konkrétních organizací obelstily zabezpečení, podobně jako tomu bylo u útoku na americký prodejní řetězec Target. Uživatele a malé podniky budou i nadále ohrožovat masivní globální útoky, ale při útocích na velké organizace zvýší hackeři svou šanci na úspěch pokročilými útočnými technikami. Útočníci budou pro krádeže dat využívat stále sofistikovanější phishing a další triky spojené se sociálním inženýrstvím.

Přesun k mobilitě
Mobilní útoky přibývají, protože mobilní zařízení jsou stále běžnější ve firemním prostředí, což hackerům nabízejí přímý a potenciálně lukrativní přístup k osobním a firemním datům. Podle zprávy Check Point 2015 Security Report má 42 % organizací zkušenosti s mobilními bezpečnostními incidenty, u nichž jsou náklady na nápravu vyšší než 250 000 dolarů, a 82 % organizací očekává, že počet mobilních incidentů ještě vzroste. V letošním roce došlo k odhalení také několika nebezpečných mobilních zranitelností, včetně Certifigate, zranitelnosti ohrožující stovky milionů zařízení se systémem Android, a XcodeGhost, první velké malwarové infekce zaměřené na iOS zařízení bez jailbreaku. V průběhu příštího roku očekáváme další podobné vážné zranitelnosti.

Prevence hrozeb
V pokračující bitvě mezi hackery a bezpečnostními odborníky využívají útočníci stále sofistikovanější vlastní varianty stávajícího malwaru a zranitelností nultého dne, takže často mohou obejít tradiční sandboxingové technologie. Tyto nové útoky vyžadují proaktivní a pokročilá řešení, která zajistí, že se malware bezpečnostnímu řešení nevyhne. Sandboxing na úrovni CPU je schopen identifikovat nejnebezpečnější hrozby už v zárodku, dřív než se mohou pokusit vyhnout detekci a infikovat síť.

Útoky na kritickou infrastrukturu
V prosinci 2014 byla hackery napadena ocelárna v Německu. Útočníci získali přístup do výrobní sítě elektrárny a způsobily značné škody. Podle Ministerstva vnitřní bezpečnosti Spojených států amerických infikoval trojan Havex průmyslové řídicí systémy více než 1000 energetických společností v Evropě a Severní Americe. Útoky na veřejné služby a klíčové průmyslové procesy budou i nadále pokračovat. Pro útok je obvykle použit malware cílený na SCADA systémy, které řídí nejrůznější průmyslové procesy. A jelikož jsou řídící systémy stále častěji připojeny k internetu, rozšíří se i možnosti útoků, což bude vyžadovat lepší ochranu.

Internet věcí a chytrá zařízení
Internet věcí se stále vyvíjí a nějaký velký dopad v roce 2016 je tak poměrně nepravděpodobný. Nicméně organizace musí přemýšlet o tom, jak mohou chránit chytrá zařízení a připravit se na širší přijetí internetu věcí. Klíčové otázky, které si musí uživatelé položit, jsou: „Co se děje s mými daty?“ a „Co by se stalo, kdyby se někdo k těmto datům dostal?“ Před rokem objevil Check Point chybu v routerech pro malé a domácí kanceláře, která by mohla umožnit hackerům zneužít router pro útoky na všechna zařízení k němu připojená - a budeme vidět více a více podobných zranitelností u zařízení s připojením k internetu.

Nositelné technologie
Nositelné technologie, jako například chytré hodinky, si nachází cestu do organizací a přináší nová bezpečnostní rizika a výzvy. Existuje celá řada obav o data, ale chytré hodinky a další nositelné technologie by mohly být hackery dokonce zneužity pro zachycení videa a zvuku, takže organizace, které povolují tato zařízení, musí zajistit, že jsou chráněna šifrováním a silným heslem.

Vlaky, letadla a automobily
V roce 2015 jsme viděli vzestup hackování aut a převzetí kontroly nad autem pomocí kyberútoku. V červenci 2015 nechal Fiat Chrysler stáhnout v USA 1,4 milionu vozů Jeep Cherokee, když bezpečnostní experti zjistili, že je auta možná hacknout prostřednictvím zábavního systému s připojením k internetu. Moderní automobily přináší dosud nevídané množství technologií a možností připojení k internetu, takže je nutné do automobilových systémů implementovat od začátku i zabezpečení. A to samé platí i pro komplexní systémy v osobních letadlech, vlacích a jiných dopravních prostředcích.

Skutečné zabezpečení pro virtuální prostředí
Virtualizace se v posledních letech stala v organizacích velmi oblíbenou technologií, ať už se jedná o SDN, NFV nebo cloud computing. Virtualizovaná prostředí jsou složitá a vytváří nové síťové vrstvy, takže při přesunu do virtualizovaného prostředí musí být bezpečnost klíčovým faktorem hned od počátku, aby ochrana byla efektivní.

Nová prostředí, nové hrozby
V roce 2015 byla představena řada nových operačních systémů, jako jsou Windows 10 a iOS 9. Většina útoků na organizace se v posledních letech zaměřovala na systém Windows 7, protože přechod na Windows 8 nebyl tak masivní, ale s bezplatným přechodem na Windows 10 se pozornost kyberzločinců obrátí tímto směrem a pokusí se zneužít slabiny v nových operačních systémech, kde je větší množství aktualizací a uživatelé jsou méně obeznámeni s prostředím.

Konsolidace zabezpečení – důležitá je jednoduchost
Pro ochranu proti sofistikovaným hrozbám se bezpečnostní experti pravděpodobně více spolehnou na centralizovaná řešení pro správu zabezpečení. Velké organizace mají mnoho různých bezpečnostních produktů v síti, takže konsolidace nabízí snížení složitosti i nákladů. Množství specializovaných produktů a řešení se stává nezvladatelným a často takový systém přidělává spíše problémy, než aby ve výsledku zlepšil bezpečnost.

Sjednocení zabezpečení je klíčové, aby vše bylo přehledné a pod kontrolou a nové hrozby se neschovaly v mezerách mezi systémy.

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 největší celosvětový dodavatel čistě bezpečnostních řešení. Chrání zákazníky před kyberútoky prostřednictvím unikátních řešení, která nabízí bezkonkurenční úspěšnost zachycení malwaru a jiných typů útoků. Check Point nabízí kompletní bezpečnostní architekturu, která chrání vše od podnikových sítí až po mobilní zařízení, a navíc Check Point poskytuje i nejkomplexnější a nejintuitivnější správu zabezpečení. Check Point chrání více než 100 000 organizací všech velikostí. Ve společnosti Check Point zabezpečujeme budoucnost.