Tisková zpráva

Lenka Čermáková
EY
Tel.: +420 225 335 967
Mobile: +420 731 627 166
E-mail: lenka.cermakova@cz.ey.com

Roman Pavlík
Fleishman Hillard
Tel.: +420 224 232 650
Mobile: +420 777 791 878
E-mail: pavlik@fleishman.com

Firmy dokáží kybernetické útoky stále lépe předvídat, hůře se z nich však zotavují

- ***Polovina dotazovaných organizací se domnívá, že by se sofistikovanému kybernetickému útoku dokázala ubránit, což představuje nejvýraznější podíl od roku 2013***
- ***Přesto podle 86 % dotázaných nejsou jejich bezpečnostní opatření proti kybernetickým útokům na dostatečné úrovni***
- ***Výskyt závažného kybernetického incidentu potvrdilo 57 % společností, téměř polovina (48 %) uvedla v této souvislosti jako největší slabinu zastaralý kontrolní systém a bezpečnostní architekturu***
- ***42 % respondentů nedisponuje jasnou komunikační strategií či plánem pro případ významného kybernetického útoku***
- ***Zajištění kontinuity podnikání a program obnovy po havárii pokládá za prioritu 57 % účastníků průzkumu; navýšit objem investic do daných oblastí v nadcházejícím roce nicméně hodlá pouze 39 %***
- ***K nejobávanějším hrozbám patří již tradičně nedostatečné bezpečnostní povědomí či nedbalý přístup zaměstnanců či neoprávněný přístup k datům***

PRAHA, 9. února 2017 – Navzdory stále vyššímu počtu kybernetických hrozeb si nadnárodní společnosti víc než kdy jindy věří, že dokáží předvídat důmyslné kybernetické útoky a zároveň jim úspěšně čelit. Naopak mezery vidí v nedostatečných investicích a plánech na obnovení provozu, pokud již k narušení bezpečnosti dojde. Vyplývá to z pravidelného mezinárodního průzkumu o kybernetické bezpečnosti ve firmách *(Global Information Security Survey – Path to cyber resilience: Sense, resist, react)*, který každoročně provádí poradenská společnost EY a kterého se v roce 2016 zúčastnilo celkem 1 735 organizací.

Celá polovina respondentů (50 %) je přesvědčena, že by sofistikovaný kybernetický útok byla

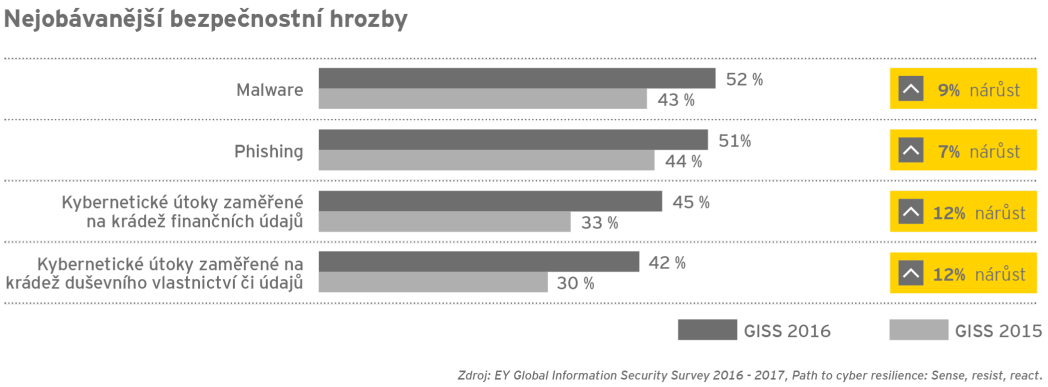
schopna odhalit, což představuje nejvýraznější podíl od roku 2013. Tento pozitivní trend odráží zejména investice firem do analýzy důvěryhodnosti a závažnosti údajů o hrozbách (tzv. *threat intelligence*), nepřetržitého monitoringu, centra pro řízení bezpečnosti provozu (SOC) a v neposlední řadě i na aktivní obranu.

Bez ohledu na uvedené investice se ale 86 % respondentů domnívá, že nástroje pro boj s kybernetickými hrozbami uplatňované jejich organizací současným nárokům nedostačují.

Téměř dvě třetiny společností (64 %) nedisponují žádným uceleným programem na analýzu relevantních hrozeb (threat intelligence), případně uplatňují pouze dílčí opatření. Pokud jde o identifikaci zranitelností, více než polovina (55 %) organizací nevyužívá žádné specifické metody, jejichž prostřednictvím by případné zranitelnosti mohly odhalit, přičemž centrum pro řízení bezpečnosti provozu (SOC) zcela chybí ve 44 % organizací.

Na přímý dotaz ohledně výskytu závažného incidentu v organizaci v nedávné době odpovědělo kladně 57 % respondentů; zastaralé kontroly nebo bezpečnostní architekturu označuje v dané souvislosti za nejzávažnější slabinu téměř polovina účastníků (48 %), tedy více než v minulém roce (34 %).

Respondenti se shodují, že největší hrozby – ať již malware, phishing, útoky prováděné s cílem obohatit se nebo pokusy o krádež duševního vlastnictví či údajů – jsou nadále na vzestupu:



Zdroj: EY Global Information Security Survey 2016 - 2017, Path to cyber resilience: Sense, resist, react.

Petr Plecháček, senior manažer oddělení IT poradenství společnosti EY v ČR, říká:

„V oblasti prevence prolomení bezpečnostních opatření dělají sice organizace značné pokroky, ať se však snaží sebevíc, útočníci přijdou vždy s novými a rafinovanějšími triky. Je proto zapotřebí, aby organizace uplatňovaná bezpečnostní opatření dále zesilovaly. Musí se také snažit uvažovat nad rámec pouhé ochrany či zabezpečení a zavádět komplexní bezpečnostní politiky, které jim umožní lépe se na kybernetické incidenty připravit a účinněji na ně reagovat. To, že přijdou, nemá smysl rozporovat. Ve chvíli, kdy se tak stane, musí mít společnost připravený plán a být schopna urychleně zajistit nápravu a obnovit provoz. Pokud to nedokáže, ohrozí nejen své zákazníky, zaměstnance a dodavatele, ale především svou vlastní budoucnost.“

Pro organizaci je z hlediska schopnosti reakce na napadení zcela zásadní prioritou zajištění kontinuity podnikání a program obnovy po havárii (57 %), stejně tak jako prevence úniku a ztráty dat (57 %). Zatímco na prevenci úniků a ztráty dat hodlá v roce 2016 vynaložit více prostředků 42 % respondentů, na zajištění kontinuity podnikání a program obnovy po havárii pouze 39 %.

Slabá místa ani překážky se téměř nemění

Pořadí nejobávanějších hrozeb zůstává v porovnání s předchozím rokem de facto neměnné. Respondentům tak největší obavy v souvislosti s kybernetickou bezpečností působí nedostatečné bezpečnostní povědomí či nedbalý přístup zaměstnanců (55 % oproti 44 % v roce 2015) a neoprávněný přístup k datům (54 % oproti 32 %). Také překážky implementace a rozvoje dedikované pracovní pozice pro zajišťování kybernetické bezpečnosti jsou stále tytéž:

- rozpočtová omezení (61 %, resp. 62 % v roce 2015);
- nedostatek kvalifikovaných odborníků (56 %, resp. 57 % v roce 2015); a

- nízké povědomí a podpora ze strany managementu (v obou letech shodně 32 %).

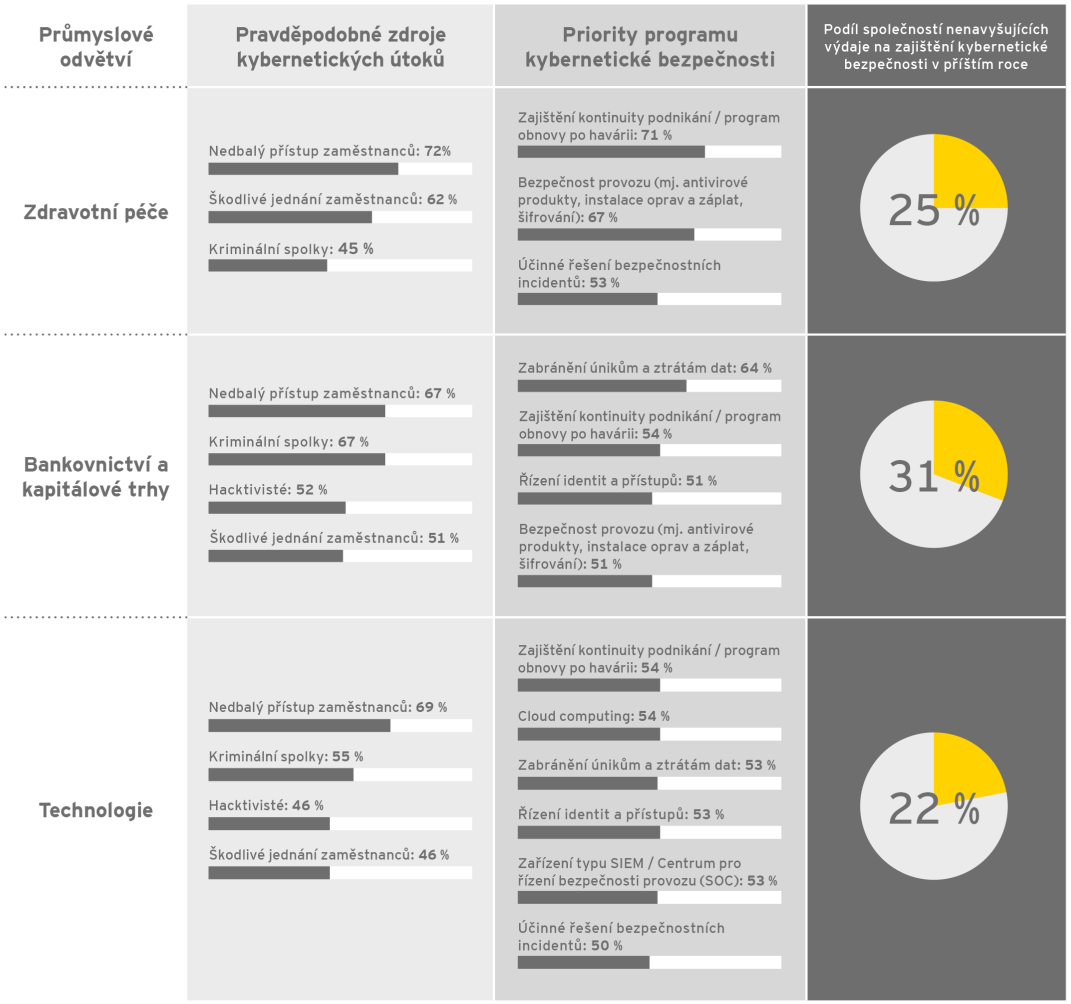
Úskalí inherentních rizik digitálního ekosystému a propojených zařízení

Bez ohledu na provázanost současného digitálního světa nepokládá 62 % respondentů za pravděpodobné, že by navýšili výdaje na kybernetickou bezpečnost v případě narušení, které by z hlediska provozu nezpůsobilo zjevné škody. Stejné přesvědčení vyslovilo 58 % respondentů v souvislosti s případným útokem na konkurenční podnik a 68 % zúčastněných organizací by pravděpodobně částku na zabezpečení nezvýšilo ani v případě kybernetického útoku na svého dodavatele. Pokud by útočníci uspěli při krádeži dat, dotčené klienty by o prokazatelném zcizení údajů do týdne od takového incidentu neinformovala téměř polovina účastníků průzkumu (48 %). Celkem 42 % respondentů nemá schválenou komunikační strategií, resp. připravený plán pro případ významného útoku.

V souvislosti s přenosnými zařízeními se pak organizace dle vlastních slov potýkají především se stále rostoucím počtem zařízení, které do jejich infrastruktury pronikají. Téměř tři čtvrtiny (73 %) podniků znepokojuje nedostatečné povědomí a chování uživatelů týkající se zacházení s mobilními zařízeními jako jsou notebooky, tablety a smartphony. Ztrátu chytrého zařízení vnímá v tomto ohledu jako nejvyšší riziko celá polovina dotázaných (50 %), jelikož většinou představuje jak ztrátu údajů, tak identity.

Building a better working world

Kybernetické útoky a priority kybernetické bezpečnosti v jednotlivých odvětvích



Zdroj: EY Global Information Security Survey 2016 - 2017, Path to cyber resilience: Sense, resist, react.

Informace o průzkumu

Již 19. ročník mezinárodního průzkumu kybernetické bezpečnosti (Global Information Security Survey) provedla společnost EY v roce 2016. Zachycuje názory celkem 1 735 respondentů z řad vrcholového managementu, vedoucích pracovníků a manažerů IT reprezentujících největší a nejuznávanější světové firmy.

O EY

EY je předním celosvětovým poskytovatelem odborných poradenských služeb v oblasti auditu, daní, transakčního a podnikového poradenství. Znalost problematiky a kvalita služeb, které poskytujeme, přispívají k posilování důvěry v kapitálové trhy i v ekonomiky celého světa. Výjimečný lidský a odborný potenciál nám umožňuje hrát významnou roli při vytváření lepšího prostředí pro naše zaměstnance, klienty i pro širší společnost.

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global

Building a better working world

Limited, z nichž každá je samostatnou právnickou osobou. Ernst & Young Global Limited, britská společnost s ručením omezeným garancí, služby klientům neposkytuje. Pro podrobnější informace o naší organizaci navštivte prosím naše webové stránky www.ey.com/CZ.

EY Česká republika na Twitteru: @EY_CeskaRep