
Tlačová správa

Dátum	13. októbra 2014
Kontakt	Pavol Adamec, Direktor, PwC Tel.: +421 (0)2 59350 042 pavol.adamec@sk.pwc.com
alebo	Zuzana Sehnalová, Marketing & Communications Leader, PwC Tel.: +421 (0)2 59350 133 Mobil: +421 (0)911 357 151 zuzana.sehnalova@sk.pwc.com

Kybernetické bezpečnostné incidenty sú čoraz častejšie a nákladnejšie, no rozpočty na ich odhaľovanie sa stále znižujú, tvrdia PwC, CIO a CSO v spoločnej štúdii s názvom „Global State of Information Security® Survey 2015”

Dopady siahajú až k vrcholovému vedeniu firiem a dozorným orgánom, narastá počet incidentov spôsobených vlastnými zamestnancami i ich rafinovanosť

Bratislava, New York, NY a Framingham, MA, 13. októbra 2014 – Podľa prieskumu s názvom [The Global State of Information Security® Survey 2015](#), ktorý realizovala spoločnosť PwC spolu s časopismi CIO a CSO, a ktorého výsledky boli zverejnené v septembri, vzrástol v roku 2014 počet nahlásených kybernetických bezpečnostných incidentov oproti roku 2013 na celom svete o 48 % na celkových 42,8 mil. Získané údaje naznačujú, že odhalené kybernetické bezpečnostné incidenty rástli od roku 2009 medziročne v priemere o 66 %.

„Nikoho zrejme neprekvapuje, že počty nahlásených incidentov kybernetickej bezpečnosti a s tým spojené finančné dopady každým rokom rastú,“ vraví David Burg z PwC, svetový líder pre oblasť poradenstva pri kybernetickej bezpečnosti. *„Skutočný počet týchto incidentov je však oveľa vyšší, keď vezmeme do úvahy povahu odhalených a nahlasovaných týchto incidentov.“*

Keďže prípady narušenia kybernetickej bezpečnosti sú čoraz častejšie, rastú aj s tým spojené náklady na ich zvládnutie a zmiernenie výsledných dopadov. Podľa odhadov dosiahli v celosvetovom meradle nahlásené priemerné finančné straty z kybernetických bezpečnostných incidentov výšku 2,7 mil. USD – čo predstavuje nárast o 34 % oproti roku 2013. V tomto roku sa veľké straty vyskytovali bežnejšie, pretože počet organizácií, ktoré nahlásili finančné útoky nad 20 mil. USD, sa takmer zdvojnásobil.

Bez ohľadu na svoju veľkosť či sféru pôsobenia si organizácie a firmy uvedomujú závažnosť rizík spojených s útokmi na kybernetickú bezpečnosť, väčšie spoločnosti však celkom prirodzene odhaľujú viac bezpečnostných incidentov. Veľké firmy – s hrubými ročnými tržbami najmenej 1 miliardu USD – odhalili tohto roku o 44 % viac incidentov než rok predtým. Stredne veľké spoločnosti – s hrubými ročnými tržbami od 100 mil. USD do 1 miliardy USD – zaznamenali 64 % nárast počtu odhalených incidentov. A zatiaľ čo riziko sa stalo univerzálnym, prieskum zistil, že finančné straty sa značne rôznia v závislosti od veľkosti organizácie.

„Naše skúsenosti zo slovenského trhu získané diskusiami s klientmi poukazujú na to, že nárast počtu incidentov sa v plnej miere týka aj Slovenska“, komentuje výsledky prieskumu z perspektívy Slovenska **Pavol Adamec**, direktor v PwC Slovensko a špecialista na riadenie rizík. Pre mnohé spoločnosti na Slovensku doposiaľ platilo, že boli príliš malé alebo "vzdialené" od medzinárodného kybernetického zločinu. S nárastom miery ochrany u veľkých globálnych spoločností a zvýšením dostupnosti nástrojov pre cieľené útoky mnohé slovenské firmy zistili, že sa zrazu ocitli na radare kybernetických útočníkov. A tento trend má perspektívu rásť.

Medzi najzriedkavejšie sa vyskytujúce incidenty zatiaľ patria sofistikované útoky zo strany štátom podporovaných útočníkov, organizovaného zločinu či konkurencie, no napriek tomu sú najrýchlejšie rastúcimi kybernetickými hrozbami. Počet respondentov, ktorí tohto roku uviedli, že sa stali obeťou kybernetického útoku zo strany nejakého štátu, vzrástol o 86 % – a pritom takéto incidenty ostávajú taktiež s najväčšou pravdepodobnosťou nenahlásené. Prieskum takisto odhalil ohromujúci 64 % nárast bezpečnostných incidentov zo strany konkurencie, pričom niektoré útoky mohli byť dokonca vedené s požehnaním štátu.

V tejto súvislosti je veľmi zaujímavé porovnanie s výsledkami Globálneho prieskumu hospodárskej kriminality 2014 za Slovensko. Podľa prieskumu hospodárskej kriminality je podiel počítačovej kriminality v slovenských spoločnostiach dosť výrazne pod regionálnym a globálnym priemerom. Slovensko sa postupne mení z výrobnéj linky Európy na krajinu s rastúcou znalostnou bázou a podielom tvorivých činností. „Spoločnosti na Slovensku musia počítať aj s tým, že sa začnú stávať častejším terčom pre kybernetické útoky z úplne nového dôvodu a od úplne nových útočníkov - krádež know-how od veľkých nadnárodných alebo štátom podporovaných útočníkov“ dodáva **Pavol Adamec**. Je tiež možné, že už dnes sú cieľom tohto typu kriminality, len o tom nevedia alebo sa k tomu nepriznávajú.

„Kybernetické riziká sa nikdy nepodari úplne eliminovať. S vzostupom kybernetického zločinu si tak musia organizácie dávať veľký pozor a byť neustále v strehu, aby dokázali pružne a rýchlo reagovať na neustále sa meniacu situáciu v tejto oblasti,“ vysvetľuje **Pavol Adamec** z PwC Slovensko. „Od bezpečnosti, ktorá sa sústreďuje na prevenciu a kontroly, musia organizácie prejsť na rizikovo orientovaný prístup, ktorého ťažiskom záujmu sú tie najcennejšie aktíva organizácie a najzávažnejšie hrozby, ktorým je vystavená. Masívne investície do plne funkčných postupov a procesov na zabezpečenie povedomia o vnútornej bezpečnosti budú rozhodujúce pre ďalšie úspešné fungovanie každej organizácie.“ uzatvára **Pavol Adamec**.

KONIEC

Poznámky vydavateľom:

Ak si chcete stiahnuť výstupnú správu z prieskumu *Global State of Information Security® Survey 2015* a dozvedieť sa viac o poznatkoch PwC, navštívte stránku <http://pwc.to/GSISS15>.

Korektná citácia štúdie znie takto: „Globálna štúdia stavu informačnej bezpečnosti® pre rok 2015, celosvetová štúdia z dielne CIO, CSO a PwC.“ Zdroj musí obsahovať CIO, CSO a PwC. O výsledkoch prieskumu podrobne informujú aj stránky CIO.com a CSOnline.com.

Metodika

Globálna štúdia stavu informačnej bezpečnosti® pre rok 2015 je celosvetová štúdia z dielne CIO, CSO a PwC. Bola realizovaná on-line formou od 27. marca do 25. mája 2014. Čitatelia časopisov CIO a CSO ako aj klienti PwC na celom svete boli e-mailom požiadaní, aby sa daného prieskumu zúčastnili. Výsledky, ktoré sa dôkladne rozoberajú v tejto správe, sa opierajú o odpovede vyše 9 700 respondentov (generálnych riaditeľov firiem CEOs), finančných riaditeľov (CFOs), riaditeľov odboru informačných technológií (CIOs), vedúcich úseku informačnej bezpečnosti (CISOs), šéfov bezpečnosti (CSOs) a riaditeľov informačných a bezpečnostných kancelárií zo 154 krajín. 35 % respondentov pochádza zo Severnej Ameriky, 34 % z Európy, 14 % z Ázie a Tichomoria, 13 % percent z Južnej Ameriky a 4 % zo Stredného východu a Afriky. Možná chyba je menšia než 1 %.

O CIO a CSO

Časopis CIO je po obsahovej stránke hlavným zdrojom odborných informácií pre komunitu riadiacich pracovníkov a lídrov v oblasti informačných technológií v tejto hektickej ére transformácie IT prostredia vo firmách. Oceňované portfólio CIO – CIO.com, časopis CIO (vydávaný od roku 1987), exekutívne programy CIO, marketingové služby CIO, fórum CIO na LinkedIn a primárny výskum CIO – poskytujú vedúcim pracovníkom pre oblasť podnikových technológií analýzy a všeobecný prehľad o tom, aké sú trendy v informačných technológiách, a pomáha im jasne pochopiť úlohu informačných technológií pri dosahovaní obchodných cieľov. Navyše CIO dáva poskytovateľom IT riešení možnosti priblížiť sa okruhu čitateľov z radov výkonných IT pracovníkov. Časopis CIO vydáva IDG Enterprise, dcérska

spoločnosť International Data Group ([IDG](http://www.idgenterprise.com)), ktorá je poprednou svetovou mediálnou, eventovou a výskumnou spoločnosťou. Informácie o spoločnosti nájdete na stránke www.idgenterprise.com.

Časopis CSO je po obsahovej stránke hlavným zdrojom odborných informácií pre komunitu osôb prijímajúcich rozhodnutia v oblasti bezpečnosti, ktoré stoja v rámci svojich organizácií čele snáh o „riadenie podnikateľských rizík“. Už vyše 10 rokov sa vďaka jeho oceňovanej webovej stránke (CSOonline.com), konferenciám pre výkonných pracovníkov, marketingovým službám a výskumu darí zodpovedným pracovníkom prijímajúcim rozhodnutia v oblasti bezpečnosti zmierňovať vo svojich organizáciách tak IT riziká ako aj podnikateľské a fyzické riziká, a obchodníci v oblasti bezpečnosti zasa majú príležitosť získať dosah na svoju potenciálnu klientelu. CSO tiež štvrťročne vydáva bulletin *Security Smart*, aby ním pomáhal šéfom bezpečnosti vzdelávať zamestnancov ich organizácií v oblasti postupov a praktík na zaistenie korporátnej i osobnej kybernetickej bezpečnosti. Časopis CSO vydáva IDG Enterprise, dcérska spoločnosť International Data Group ([IDG](http://www.idgenterprise.com)), ktorá je poprednou svetovou mediálnou, eventovou a výskumnou spoločnosťou. Informácie o spoločnosti nájdete na stránke www.idgenterprise.com.

The Global State of Information Security[®] je registrovanou obchodnou značkou International Data Group, Inc.

O sieti PwC

Firmy PwC pomáhajú organizáciám i jednotlivcom vytvárať tú hodnotu, ktorú hľadajú. Sme sieťou firiem v 157 krajinách s vyše 195 000 pracovníkmi, ktorí robia všetko pre to, aby poskytovali kvalitné audítorské, daňové a poradenské služby. Viac sa dozviete na našej webovej stránke www.pwc.com/sk.

Označenie PwC sa vzťahuje na sieť PwC a/alebo jednu či viacero jej členských firiem, z ktorých každá je samostatným právnym subjektom. Ďalšie informácie nájdete na stránke www.pwc.com/structure.

2014 PwC. Všetky práva vyhradené.