

60 % českých firem využívá ke školení IT bezpečnosti jen interní zdroje

Moskva a Praha, 27. září 2013

Většina společností zadá školení bezpečnosti v IT pro zaměstnance svému IT oddělení, místo aby si na to najali externí odborníky. V Česku je jich 60 %, ve světě 65 %. Vyplývá to z průzkumu Kaspersky Lab a B2B International [Global Corporate IT Security Risks 2013](#). Toho se zúčastnilo na 3 000 IT podnikových profesionálů z 24 zemí, včetně České republiky.

Efektivní zaškolení zaměstnanců je důležitou součástí účinné strategie boje proti kybernetickým hrozbám. Dle průzkumu Kaspersky Lab čtyři z pěti nejběžnějších interních bezpečnostních incidentů za posledních 12 měsíců byly spojeny právě s jednáním personálu.

Čísla pro Českou republiku ukazují, že:

- 31 % dotázaných firem zaznamenalo nechtěný únik citlivých dat.
- 20 % respondentů uvedlo, že zaměstnanci ztratili mobilní zařízení, na nichž byla uložena klíčová data.
- U 26 % společností účastnících se průzkumu zaměstnanci nechali uniknout data záměrně.
- 14 % dotázaných firem muselo řešit problémy kvůli tomu, že se jejich tajná data dostala do nesprávných rukou kvůli špatnému nakládání s firemními mobilními zařízeními (prostřednictvím e-mailu, sms zprávy, apod.).

Ačkoli se podle průzkumu Kaspersky Lab a B2B International společnosti domnívají, že by měly zaměstnance školit jejich interní IT oddělení, pro tyto týmy to představuje pracovní zátěž navíc, která ovlivňuje jejich výkon. A také to má dopad na kvalitu školení. Daleko lepší výsledky mají tréninky IT bezpečnosti od specializovaných konzultantů. Přesto je využilo jen 14 % dotázaných českých firem.

5 % českých firem v průzkumu využilo k tréninku personální oddělení a podobný počet školícího oddělení. 3 % dotázaných českých firem neškolí své zaměstnance vůbec. Přitom 58 % účastníků výzkumu mezi českými firmami naznačilo, že zaměstnanci ne vždy dodržují bezpečnostní zásady v IT. To je o mnoho více, než je celosvětový průměr v průzkumu – 39 %.

V komplexním řešení korporátní IT bezpečnosti by neměla chybět technologie takzvaného dynamického whitelistingu, která pomáhá předcházet problémům plynoucím z chyb zaměstnanců. Brání spuštění malwaru a využívá vlastní databáze důvěryhodných aplikací, které operační systém jako jediné povolí spustit. To značně stěžuje jakýkoliv útok na podnikovou síť, včetně neznámých hrozeb. Databáze bezpečných aplikací Kaspersky Lab, která je k dispozici v korporátním řešení [Kaspersky Endpoint Security for Business](#) obsahuje 700 milionů unikátních souborů a je nepřetržitě aktualizována. Dle průzkumu B2B International 49 % českých firem technologii whitelistingu v různých podobách používá.

O společnosti Kaspersky Lab

*Kaspersky Lab je největším soukromě vlastněným poskytovatelem koncových bezpečnostních řešení na světě. Společnost se řadí mezi čtyři největší prodejce bezpečnostních řešení pro koncové uživatele.**

Již 15 let patří Kaspersky Lab mezi přední inovátory v oblasti informačních technologií a poskytuje efektivní digitální bezpečnostní řešení zákazníkům, malým a středním firmám i velkým podnikům. Aktuálně společnost působí v bezmála 200 zemích a oblastech a poskytuje ochranu více než 300 milionům uživatelů. Více informací o společnosti Kaspersky Lab najdete na www.kaspersky.cz.

**Společnost zařadil na čtvrté místo žebříček „IDC Worldwide Endpoint Security Revenue by Vendor, 2011“. Žebříček vyšel ve zprávě „IDC Worldwide IT Security Products 2012-2016 Forecast and 2011 Vendor Shares – December 2011“ a řadil poskytovatele software podle zisku z prodeje koncových bezpečnostních řešení v roce 2011.*

Pro další informace prosím kontaktujte:

Michal Malysa
PR Consultant
Grayling Czech Republic
Tel.: 224 251 555
Mobil: 775 708 086
michal.malysa@grayling.com
[Twitter.com/GraylingCZ](https://twitter.com/GraylingCZ)