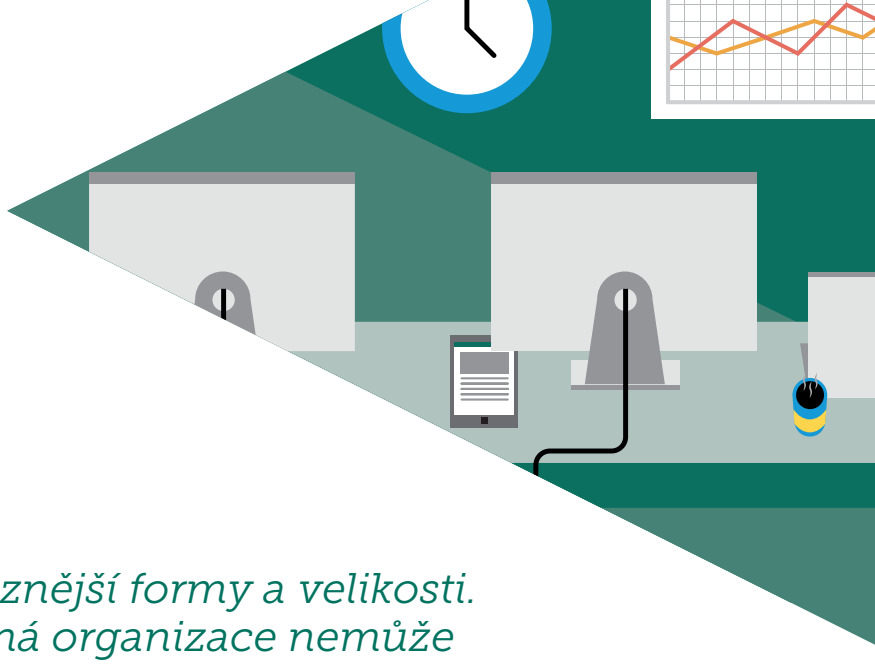
PRŮVODCE ZABEZPEČENÍM IT MALÝCH FIREM

Jak dosáhnout komplexního zabezpečení firemního IT

#protectmybiz

KASPERSKY lab



Malé firmy mohou mít nejrůznější formy a velikosti. V dnešním světě si však žádná organizace nemůže dovolit ignorovat internetové zabezpečení – ať už jste tým, který působí mimo kancelář, nebo jednotlivec pracující z domova. Je to problém, který se týká každého.

Počítačový zločin se na první stránky novin většinou dostane, až když se jeho obětí stane nějaká velká společnost nebo vláda. Opravdovou senzaci ale představují malé případy.

Jen v roce 2014 bylo objeveno 143 milionů nových výskytů malwaru.[1] A většina z nich byla namířena proti jednotlivcům a organizacím, které by ani nenapadlo, že by se to mohlo stát právě jim.

Terčem se však může stát každý. Dobrou zprávou je, že pořád existuje velký rozdíl mezi tím, když je někdo jen terčem a když se stane skutečnou obětí.

Hlavní je být pořád ve střehu. A právě proto jsme vytvořili tohoto průvodce: Chceme vám ukázat, jak udržet firmu v bezpečí.

? CO JE TO MALWARE?

Za termínem malware se skrývají počítačové programy, jejichž účelem je škodit. Tyto programy obvykle napadají zařízení bez vědomí jejich uživatelů. Společnost Kaspersky Lab je světová jednička na poli detekce malwaru a její produkty pravidelně v testech porážejí konkurenci.[2]

? PROČ SE MUSÍM CHRÁNIT?

Pokud počítačoví zločinci chtějí způsobit vašemu podniku citelné ztráty, nemusí jen vysát firemní účty. Malware může narušit chod vašeho podniku, snížit jeho produktivitu a cashflow a způsobit tak celý řetězec nežádoucích následků. I proti takto vážným hrozbám se však můžete chránit s využitím relativně jednoduchých postupů. Vcelku snadno si tak ušetříte pár bezesných nocí.

1. AV-Testy
2. Studie výsledků nezávislých testů TOP3, 2014

VÁŠ KONTROLNÍ SEZNAM

PRVNÍM KROKEM PŘI ZABEZPEČENÍ FIRMY JE PODÍVAT SE, JAK FUNGUJE A KDE JE PROSTOR PRO SNÍŽENÍ RIZIKA. PROVEĎTE TEDY RYCHLOU KONTROLU STAVU ZABEZPEČENÍ SVÉHO IT:

OCHRANA PROTI MALWARU ✔

Když se rozhodujete o zabezpečení podniku a produktech chránících vaši společnost, chcete samozřejmě to nejlepší. Pokud ještě nemáte vysoce kvalitní software schopný chránit zařízení před infekcí, měli byste to co nejdřív změnit.

Být na internetu obezřetní samo o sobě bohužel nestačí. Všichni víme, že bychom neměli otevírat přílohy od neznámých odesílatelů nebo stahovat soubory z podezřelých stránek. Pravdou ale je, že spousta infekcí pochází z důvěryhodných zdrojů, které někdo zneužil.

SURFOVÁNÍ NA INTERNETU ✔

Když svým zaměstnancům vysvětlíte, jaké dopady může mít jejich pohyb na internetu, ušetříte si tím spoustu vrásek. Nakonec snad vaši podřízení pochopí, že některé typy stránek by v práci prostě navštěvovat neměli. Pokud ale používají pracovní smartphone nebo tablet i pro osobní účely, můžou ve své obezřetnosti polevit, jakmile se za nimi zavřou dveře firmy. Není tedy od věci blokovat nežádoucí stránky, aby na pracovních zařízeních nebyly dostupné. Dalším způsobem, jak pomoci zaměstnancům zůstat v bezpečí i mimo práci, je zvyšovat jejich povědomí o hrozbách zabezpečení IT.

? CO BY SE MI MOHLO STÁT?

Už jste někdy od příbuzného nebo kamaráda dostali e-mail se zajímavým, ale podezřelým odkazem? Když malware pronikne do počítače, může začít v tajnosti škodit. Proto se nedá věřit ani důvěryhodným zdrojům.

HESLA ✔

Zaměstnanci by také měli používat silná, jedinečná hesla sestávající z kombinace znaků, čísel a malých i velkých písmen. Běžná slova mohou podlehnout rozluštění programy, které jednoduše prohledávají slovníky, než najdou to správné heslo. Jen jedno silné heslo však nestačí. Jeho prolomení totiž může mít za následek rozsáhlé narušení zabezpečení.

AKTUALIZACE ✔

Každou sekundu jsou odhaleny čtyři nové výskyty malwaru.[3] Musíte s nimi držet krok. Využijte každodenní automatické aktualizace řešení zabezpečení a pravidelně aktualizujte i ostatní software. A zejména pak dohlédněte na to, aby totéž dělali i všichni zaměstnanci. Nezapomeňte, že neaktualizované programy jsou nejčastější cestou, kudy počítačoví zločinci napadají podniky.

PŘI TVORBĚ HESEL SE VYVARUJTE TĚCHTO KLASICKÝCH CHYB:

1. používání snadno zapamatovatelných nebo odhalitelných hesel, jako třeba „heslo“ nebo „123456“;
2. používání e-mailové adresy, jména nebo jiného snadno zjistitelného údaje;
3. nastavení kontrolních otázek k heslu, které se dají snadno dohledat, jako třeba rodné příjmení matky;
4. pouze mírná úprava běžných slov, jako třeba přidání čísla „1“ za slovo;
5. používání běžných frází, snadno rozluštit lze i krátké věty, jako třeba „milujite“.

Rady, jak sestavit těžko rozluštitelné heslo, se dočtete v článku na našem blogu.

3 AV Test

V ROCE 2014

295 500

NOVÝCH MOBILNÍCH MALWAROVÝCH HROZEB[4]

BANKOVNICTVÍ ✔

Metody k jeho zneužití mají zločinci různé – od přesměrování na falešné verze důvěryhodných stránek po malware špehující vaše aktivity. Musíte tedy přijmout opatření, která zločince zastaví.

Mějte se na pozoru před phishingovými útoky, kdy se podvodníci vydávají za vaši banku. Používejte vždy bezpečný prohlížeč a před zadáním jakýchkoli údajů zkontrolujte adresu URL. Vyvarujte se také posílání osobních údajů e-mailem, nikdy nevíte, kdo by si je mohl přečíst.

MOBILNÍ ZAŘÍZENÍ ✔

S tím, jak stále častěji pracujeme na cestách, se zvýšil zájem počítačových zločinců o mobilní zařízení. V roce 2014 bylo každý měsíc odhaleno 295 500 nových hrozeb z řad mobilního malwaru (tedy jeho varianty cílené speciálně na smartphony a tablety).[5] I když je ochrana mobilních zařízení stejně důležitá jako ochrana počítačů, jen 32 % malých firem přikládá tomuto riziku význam.[6]

ŠIFROVÁNÍ ✔

Pokud máte ve svých počítačích uložená citlivá data, měli byste je zašifrovat, aby v případě ztráty nebo krádeže nebyla k ničemu. Je důležité si uvědomit, že vaše firemní informace jsou vysoce cenné a žádají si ochranu.

? CO TO JE PHISHING?

Při phishingu se počítačoví zločinci vydávají za nějakou důvěryhodnou instituci a snaží se z vás vylákat hesla, čísla platebních karet a další údaje, s jejichž pomocí by vás mohli okrást.

4 a 5 Podle společnosti Kaspersky Lab
6 Průzkum globálních rizik zabezpečení podnikových systémů IT, 2014

POROZUMĚNÍ RIZIKŮM

O POČÍTAČOVÉM ZABEZPEČENÍ SE SICE HEZKY MLUVÍ, ALE POCHOPIT VŠECHNY JEHO ASPEKTY UŽ JE SLOŽITĚJŠÍ. JEDNOU Z MOŽNOSTÍ, JAK DO TÉTO PROBLEMATIKY PRONIKNOUT, JE DOSTAT TVRDOU LEKCI. ALE TENTO ZPŮSOB NENÍ ZROVNA PŘÍJEMNÝ. PROTO BYCHOM VÁM RÁDI NA PŘÍKLADECH ZE ŽIVOTA UKÁZALI, JAKÉ DOPADY MŮŽE MALWARE MÍT A JAK SE MU LZE VYHNOUT.

Káva, která vyšla draho

Tomáš se rozloučil s posledním zákazníkem a nechal v kanceláři už jen svého kolegu. Vydal se do kavárny přes ulici, kde se má setkat s kamarádem. V tom si uvědomil, že musí do zítřka zaplatit ještě jednu fakturu. Tak se rozhodl udělat to hned, než na to zapomene.

V kavárně vytáhl svůj notebook, připojil se k síti Wi-Fi, přihlásil se do internetového bankovnictví a převedl peníze. S dobrý pocitem, že se mu to nevykouřilo z hlavy, si udělal pohodlí a vychutnal si svůj šálek kávy.

Když se ale na podnikový účet podíval později, zjistil, že ho někdo vybílil. A to se jen chtěl podívat, proč jeho zaměstnancům nedošel plat.

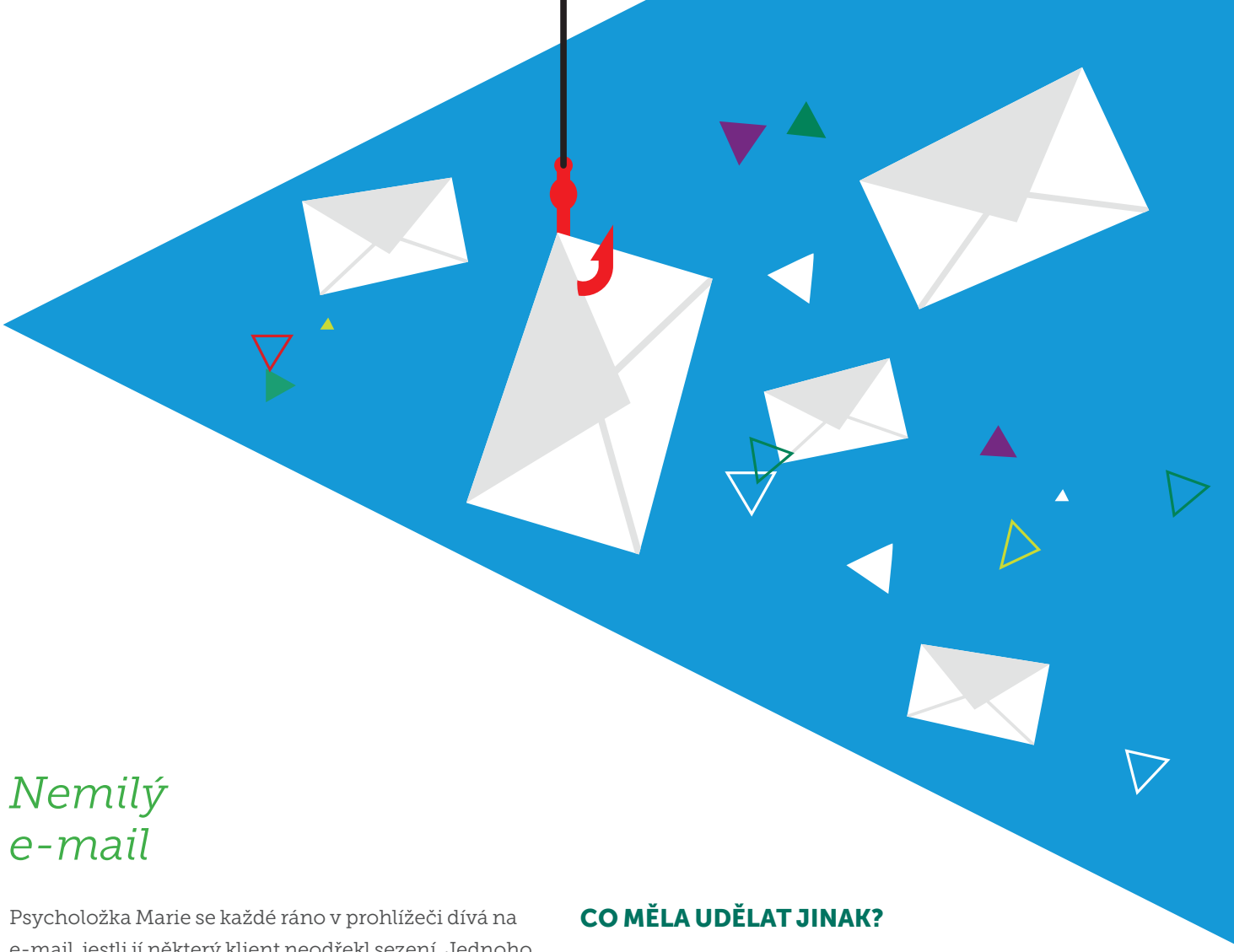
JAK SE TO MOHLO STÁT?

Bohužel neměl nainstalovaný žádný antimalware a stáhl si škodlivý program zaznamenávající stisknuté klávesy. Autor programu tak získal záznam všech údajů, které Tomáš zadal. A to se nebavíme o riziku zachycení dat transakce v nechráněné veřejné síti Wi-Fi.

CO MĚL UDĚLAT JINAK?

Když se rozhodl provést finanční transakci, měl k tomu využít zařízení s antimalwarem a zabezpečený prohlížeč. Kdyby využil technologii Safe Money od společnosti Kaspersky Lab, měl by naprostou jistotu, že by transakce proběhla bezpečně.

Dále nesmíme zapomínat, že v nezabezpečené veřejné síti můžou zločinci zachytit přenášená data o dost snáz než v privátní síti. Pokud by Tomáš měl Safe Money nebo podobnou technologii, mohl by internetové bankovnictví využívat bez starostí.



Nemilý e-mail

Psycholožka Marie se každé ráno v prohlížeči dívá na e-mail, jestli jí některý klient neodřekl sezení. Jednoho dne jí přijde žádost ze sociální sítě, aby si tam nastavila nové, silnější heslo. Marie klikne na příslušný odkaz, zadá své stávající heslo a pak vloží nové (jednotlivá písmenka nahradí hvězdičky).

S dobrý pocitem, že se teď jen tak někdo do jejího účtu nedostane, začne vyřizovat zbývající resty a brzy na vše zapomene...

... ale jen do chvíle, než přijde vyděračský dopis, kde jí někdo vyhrožuje, že zveřejní údaje všech klientů, kteří k ní chodí na terapii.

JAK SE TO MOHLO STÁT?

Marie se stala obětí phishingu. I když stránka sociální sítě byla k nerozeznání podobná té pravé, jednalo se jen o napodobeninu. Jakmile se zločinci zmocnili jejího profilu, zjistili, že Marie má psychologickou praxi. Pak zkusili získané heslo použít i k jejímu pracovnímu e-mailu a dostali se i tam. Protože pro oba účty měla heslo stejné, přečetli si všechny její zprávy včetně příloh a v jedné našli seznam klientů i s kontaktními údaji.

CO MĚLA UDĚLAT JINAK?

Zaprvé si měla uvědomit, že důvěryhodné stránky a organizace nikdy nežádají o osobní údaje e-mailem. Kdyby měla dobré řešení zabezpečení, upozornilo by ji, že za odkazem se skrývá podvodná stránka.

A samozřejmě další chybou bylo, že pro osobní i pracovní potřeby používala stejné heslo.

PROČ SI VYBRAT PRODUKTY KASPERSKY LAB

NAŠÍM CÍLEM JE POSKYTOVAT VŮBEC NEJÚČINNĚJŠÍ, NEJPOHOTOVĚJŠÍ A NEJEFEKTIVNĚJŠÍ OCHRANU PŘED POČÍTAČOVÝMI HROZBAMI. SVÉ ZKUŠENOSTI JSME PŘETAVILI V ŘEŠENÍ KASPERSKY SMALL OFFICE SECURITY, KTERÉ JE JAK UŽITEČNÉ, TAK SNADNO POUŽITELNÉ. MŮŽETE SE TAK SOUSTŘEDIT NA TO, V ČEM JSTE NEJLEPŠÍ – NA ŘÍZENÍ SVÉHO PODNIKU.

Ve společnosti Kaspersky Lab chápeme, že počítačové zabezpečení malých firem má svá specifika. Tyto společnosti čelí stejným hrozbám jako velké korporace a současně je trápí ta samá zranitelná místa jako běžné uživatele. Jsme přesvědčeni, že tato specifická situace si žádá vlastní přístup k zabezpečení.

Pokud bychom vzali produkt pro běžné uživatele a nabídli ho malým firmám, nebylo by jim to moc platné. Takový produkt by třeba nenabízel ochranu serverů, kterou malé společnosti potřebují nebo brzo potřebovat budou. Na rozdíl od běžných uživatelů potřebují firmy chránit víc zařízení najednou.

Moc by nepomohlo ani to, kdybychom zredukovali nějaké řešení určené pro velké podniky. Malé firmy většinou nemají ani speciální oddělení IT, ani čas zápasit se složitým softwarem určeným pro specialisty.

Řešení Kaspersky Small Office Security je navrženo tak, aby nabízelo maximum funkcí a současně nebylo složité. Nebude vám tak přidělávat vrásky ani vysávat zdroje. Takové řešení vás nebude brzdit a pokryje pestrou paletu zařízení, takže zůstanete chráněni, ať už vás podnikání zavane kamkoli.

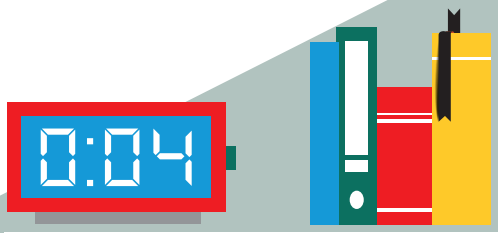
COŽPAK SE NEMŮŽU NĚJAK CHRÁNIT ZDARMA?

I když jsou na trhu k dispozici bezplatná řešení, nemůžou se nabídkou funkcí placeným produktům vůbec rovnat. Ve skutečnosti dokonce schválně v bezplatné verzi nenabízí to nejlepší. Tímto způsobem se pak snaží vytáhnout z kapes uživatelů peníze za placenou verzi.

Pokud váš podnik zrovna prochází náročným obdobím, potřebujete tu nejlepší ochranu, na kterou se budete moct vždy spolehnout.

ZAČNĚTE JEDNAT

TEĎ KDYŽ JSME SI PŘEDSTAVILI OBLASTI, KTERÉ BY MĚLY BÝT SOUČÁSTÍ ZÁSAD ZABEZPEČENÍ, JE TEN PRAVÝ ČAS SI POVĚDĚT, JAK BYSTE JE MOHLI IMPLEMENTOVAT S VYUŽITÍM ŘEŠENÍ ŠITÉHO NA MÍRU.



PRAVIDELNĚ AKTUALIZUJTE

S aplikací Kaspersky Small Office Security vás aktualizace trápit nebudou. O automatickou aktualizaci vašeho zabezpečení se postaráme v reálném čase a vy tak budete před novým hrozbami o krok napřed.

POUŽÍVEJTE SILNÁ HESLA

S tím vašim zaměstnancům pomůže aplikace Kaspersky Password Manager. Ta automaticky generuje silná hesla a uchovává je v zašifrované databázi. Zaměstnancům pak bude stačit si zapamatovat jen jedno hlavní heslo a vám bude odměnou vyšší zabezpečení.

ŠIFRUJTE A ZÁLOHUJTE CITLIVÁ A DŮLEŽITÁ DATA

S aplikací Kaspersky Small Office Security můžete své důležité informace ukládat do šifrovaných schránek. A díky funkci obnovení o svá data nepřijdete ani v případě selhání počítače nebo serveru.

CHRAŇTE VŠECHNA SVÁ ZAŘÍZENÍ

Aplikace Kaspersky Small Office Security nabízí zabezpečení podporovaných chytrých telefonů a tabletů. A pokud nějaké zařízení ztratíte nebo vám ho ukradnou, aplikace vám pomůže ho najít nebo z něj vymazat všechna citlivá data.

NEDEJTE ŠANCI ZLODUCHŮM

Stačí několik kliknutí a už s naší oceňovanou technologií Safe Money surfujete na webu naprosto bezpečně. Tato technologie ověří bezpečnost navštívených stránek a okamžitě předejde pokusům o prolomení zabezpečení. A naše funkce ochrany proti malwaru a spamu a brána firewall vás při pohybu na internetu dokonale ochrání.

CHRAŇTE SVŮJ PODNIK JIŽ NYNÍ

Aplikace Kaspersky Small Office Security byla navržena tak, aby splňovala specifické požadavky menších podniků. Kombinuje propracovanou ochranu a snadné použití nezbytné pro společnosti, jako je ta vaše.

Navštivte web **www.kaspersky.com/cz/mojefirma** a dozvíte se, jak může aplikace Kaspersky Small Office Security chránit právě váš podnik.

CHRAŇTE SVŮJ PODNIK JIŽ NYNÍ

PŘIPOJTE SE K DISKUZI.

#protectmybiz

Sledujte nás na YouTube.

Dejte nám Like na Facebooku.

Podívejte se na náš blog.

Sledujte nás na Twitteru.

Připojte se k nám ve službě LinkedIn.

Víc se dozvíte na webu kaspersky.com/cz/mojefirma.

O SPOLEČNOSTI KASPERSKY LAB

Společnost Kaspersky Lab je světově největším soukromě vlastněným prodejcem řešení pro ochranu koncových bodů. Společnost se řadí mezi čtyři nejvýznamnější světové prodejce bezpečnostních řešení pro uživatele koncových bodů.* Společnost Kaspersky Lab poskytuje efektivní digitální řešení zabezpečení pro spotřebitele a malé, střední i velké podniky a ve své více než 17leté historii byla vždy inovátorem v oblasti zabezpečení IT. Společnost Kaspersky Lab, spolu se svou holdingovou společností registrovanou ve Velké Británii, působí v současné době v téměř 200 zemích a územích na celém světě, přičemž poskytuje ochranu více než 400 milionům uživatelů z celého světa. Více informací najdete na adrese www.kaspersky.cz.

* V hodnocení „IDC Worldwide Endpoint Security Revenue by Vendor" (Příjmy dodavatelů zabezpečení koncových bodů, celosvětový přehled) v roce 2013 byla společnost hodnocena jako čtvrtá nejlepší. Toto hodnocení bylo zveřejněno ve zprávě „IDC Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (Podíl prodejců zabezpečení koncových bodů v roce 2013 a odhad na roky 2014–2018, celosvětový přehled od společnosti IDC, IDC #250210, srpen 2014). Prodejci softwaru byli ve zprávě uvedeni v pořadí podle příjmů z prodeje řešení pro zabezpečení koncových bodů v roce 2013.