BEZPEČNOSTNÍ IT EXPERTI NA VAŠEJ STRANE

# ZÁKLADNÁ BEZPEČNOSTNÁ PRÍRUČKA PRE MENŠIE FIRMY

Autor: Stephen Cobb, ESET Senior Security Researcher

Počítače a internet prinášajú malým firmám množstvo výhod, no s novými technológiami prichádzajú aj riziká. Niektoré riziká vyplývajúce z udalostí akými sú fyzická krádež a prírodné katastrofy, je možné znížiť alebo udržiavať pod kontrolou vďaka rozumnému správaniu a preventívnym opatreniam. Náročnejšie je zvládať riziká súvisiace s kybernetickým zločinom, akým je napríklad krádež informácií s cieľom speňažiť ich na čiernom trhu.

Viac ako 70 percent kybernetických útokov je zacielených na malé/stredné podniky, no množstvo majiteľov takýchto firiem si stále myslí, že im útok nehrozí práve pre malú veľkosť firmy a obmedzeným aktívam.[1] Bohužiaľ, nie je to pravda.

Táto základná bezpečnostná príručka vám pomôže chrániť vašu firmu pred kybernetickými hrozbami.

Častým cieľom kybernetických zločincov sú osobné údaje, t. j. informácie, ktoré sa dajú zneužiť na krádež identity. Aj tie najmenšie firmy s veľkou pravdepodobnosťou spracovávajú nejaké osobné údaje zákazníkov alebo dodávateľov, ktoré sú z pohľadu útočníkov výnosné. Ďalším obľúbeným cieľom kybernetických zločincov sú informácie o účtoch vrátane údajov z kreditných kariet, čísiel bankových účtov, hesiel k internetovému bankovníctvu, e-mailových kont a prihlasovacích údajov do služieb, ako sú eBay, PayPal, Amazon či AliExpress.

Takéto informácie sa dajú predať na čiernom trhu iným zločincom, ktorí sa špecializujú na ich zneužitie v rámci najrôznejších podvodov.

## Následky krádeže údajov

Väčšina malých firiem disponuje informáciami o účtoch a osobnými údajmi, ktoré by mohli zločinci zneužiť. Nezabúdajte preto na to, že zodpovednosť za následky krádeže údajov s vysokou pravdepodobnosťou bude niesť vaša firma – napríklad v prípade krádeže informácií o vašich zákazníkoch a ich zneužití na podvody.

Niektoré údaje sú chránené zákonmi a nariadeniami, akými sú napríklad nariadenie GDPR (o osobných údajoch) v Európskej únii (EÚ) alebo zákon HIPAA (o lekárskych údajoch) a štandardy PCI (o údajoch kreditných kariet) v Spojených štátoch amerických. Mnohé z týchto predpisov tiež vyžadujú, aby firmy oznamovali akékoľvek narušenie bezpečnosti, ktoré vystaví osobné údaje riziku možného zneužitia, či už je to stratený notebook obsahujúci údaje o zákazníkoch alebo USB kľúč s lekárskymi záznamami.

Znamená to, že aj keď je vaša firma malá, treba prijať systematický prístup k zabezpečeniu všetkých údajov, ktoré vám boli zverené. Pri riešení ochrany digitálneho majetku vašej firmy by ste si mali váš celkový prístup k informačnej bezpečnosti zdokumentovať. To vám následne pomôže aj pri vzdelávaní zamestnancov o ich zodpovednosti v oblasti kybernetickej bezpečnosti.

Okrem toho nie je neobvyklé, že väčšie spoločnosti požadujú od dodávateľov dôkaz o tom, že vyškolili svojich zamestnancov v oblasti bezpečnosti a že zaviedli náležité bezpečnostné opatrenia. Ak potom dôjde k narušeniu bezpečnosti, zdokumentovaná bezpečnostná politika vám pomôže dokázať, že ste vyvinuli potrebné úsilie na ochranu informácií.

1 Zdroj: U.S. Small and Medium Sized Business 2014 - 2018 Forecast – štúdia od spoločnosti IDC

## Aké kroky podniknúť

Pripravili sme pre vás systematický prístup ku kybernetickej bezpečnosti zhrnutý do šiestich krokov:

- **Posúďte** svoje aktíva, riziká a zdroje.
- **Vytvorte** si politiky.
- **Zvoľte** kontrolné prostriedky.
- **Nasaďte** kontrolné prostriedky.
- **Vzdelávajte** zamestnancov, riadiacich pracovníkov a dodávateľov.
- **Naďalej** vyhodnocujte, auditujte a testujte.

Poďme sa postupne pozrieť na každý z týchto krokov.

## Posúďte svoje aktíva, riziká a zdroje

Urobte si zoznam všetkých počítačových systémov a služieb, ktoré vaša firma používa. Koniec koncov, ak nemáte prehľad o tom, čo vlastníte, nedokážete to ochrániť. Nezabudnite zahrnúť mobilné zariadenia, ako sú smartfóny a tablety, ktoré vy alebo vaši zamestnanci využívate na prístup k firemným informáciám alebo údajom o zákazníkoch.

Toto je obzvlášť dôležité, keďže sa odhaduje, že 60 percent zamestnancov obchádza bezpečnostné prvky na svojich mobilných zariadeniach a 48 percent zamestnancov vypína bezpečnostné nastavenia, ktoré vyžaduje ich zamestnávateľ.[2]

Nezabudnite tiež na obchodné online služby, ako je SalesForce, webové stránky online bankovníctva a cloudové služby, ako sú iCloud a Google Docs.

Vytvorený zoznam si prejdite a zvážte riziká spojené s každou položkou. Položte si otázku, kto alebo čo predstavuje hrozbu. Dobré je tiež zamyslieť sa nad tým, čo zlé by sa potenciálne mohlo stať. Niektoré riziká majú väčšiu pravdepodobnosť výskytu ako iné, ale uveďte ich do zoznamu všetky a následne ich zoraďte podľa toho, aké veľké škody by mohli spôsobiť a aká je možnosť, že k daným rizikám skutočne dôjde.

Možno budete potrebovať externú pomoc s týmto procesom, a práve preto potrebujete ďalší zoznam: zdroje, ktoré môžete využiť na riešenie kybernetických problémov. Môže to byť niekto zo zamestnancov, kto má dobré znalosti a vyzná sa v bezpečnosti, alebo to môže byť obchodný partner či dodávateľ.

## PREČO POUŽÍVAŤ 2FA?

*Dvojfaktorová autentifikácia (2FA) sa stala základným prvkom ochrany údajov pred neoprávneným prístupom a zneužitím, a to obzvlášť pre malé firmy.*

*Implementácia 2FA pridáva dodatočnú vrstvu zabezpečenia tým, že sa od používateľa vyžaduje, aby okrem svojho prihlasovacieho mena a hesla zadal aj jednorazové, náhodne vygenerované heslo.*

*Mnohým únikom údajov, ktoré boli zverejnené v posledných mesiacoch, sa dalo predísť práve zavedením 2FA. Aj keby sa v takomto prípade útočníkom podarilo infikovať počítač a ukradnúť heslo, nedokázali by sa dostať do príslušného účtu, pretože by nepoznali jednorazový prístupový kód.*

*Pridanie 2FA do vášho súčasného bezpečnostného riešenia pomáha nielen chrániť údaje, ale taktiež dosiahnuť súlad s nariadeniami o viacfaktorovej autentifikácii a predchádzať neoprávnenému prístupu k strateným alebo odcudzeným notebookom a iným zariadeniam.*

Inštitúcie členských štátov EÚ a mimovládne organizácie taktiež poskytujú poradenstvo a zdroje. Obrátiť sa môžete napríklad na Europol, CERT-EU či Agentúru EÚ pre bezpečnosť sietí a informácií (ENISA).

Ak sa chcete uistiť, že vaši zamestnanci poznajú osvedčené bezpečnostné postupy, zorganizujte pre nich školenia.

## Vytvorte si politiky

Solídny bezpečnostný program začína bezpečnostnými politikami, ktoré majú podporu najvyššieho vedenia. Ak ste šéfom, musíte dať všetkým najavo, že beriete bezpečnosť vážne a že vaša spoločnosť je zaviazaná chrániť súkromie a bezpečnosť všetkých údajov, s ktorými zaobchádza. Ďalej treba jasne uviesť všetky politiky, ktoré chcete v rámci spoločnosti vynútiť, napríklad zákaz neoprávneného prístupu k firemným systémom a údajom a zákaz vypínania bezpečnostných nastavení na mobilných zariadeniach zamestnancov.

2 Zdroj: The Cost of Insecure Mobile Devices in the Workplace – štúdia inštitútu Ponemon z roku 2014

## Zvoľte kontrolné prostriedky

Na vynútenie politík slúžia kontroly. Ak chcete napríklad vynútiť politiku zakazujúcu neoprávnený prístup k firemným systémom a údajom, môžete zaviesť celkovú kontrolu nad prístupom k firemným systémom pomocou jedinečného prihlasovacieho mena, hesla a dvojfaktorovej autentifikácie (prečítajte si časť o 2FA).

Ak chcete mať kontrolu nad tým, ktoré programy je povolené spúšťať na firemných počítačoch, môžete sa rozhodnúť nedať zamestnancom administrátorské práva. Aby ste zabránili únikom údajov, ktoré môže zapríčiniť strata alebo krádež mobilných zariadení, môžete od zamestnancov vyžadovať, aby takéto udalosti hlásili ešte v ten istý deň, a zároveň môžete zaviesť okamžité vzdialené uzamknutie a vymazanie takýchto zariadení.

Potrebujete minimálne tri základné bezpečnostné technológie:

- antimalvérový softvér, ktorý ochráni firemné zariadenia pred škodlivým kódom,
- softvér určený na šifrovanie, ktorý znemožní prístup k údajom na stratených alebo ukradnutých zariadeniach (čo odporúča aj nariadenie GDPR),
- systém dvojfaktorovej autentifikácie, aby sa na získanie prístupu k firemným systémom a údajom okrem prihlasovacieho mena a hesla vyžadoval aj ďalší bezpečnostný prvok.

## Nasaďte kontrolné prostriedky

Pri nasadzovaní kontrolných prostriedkov sa uistite, že fungujú. Napríklad by ste mali mať zavedenú politiku, ktorá zakazuje použitie neoprávneného softvéru na firemných systémoch – jedným z vašich kontrolných prostriedkov bude antimalvérový softvér, ktorý kontroluje systém na prítomnosť škodlivého kódu. Antimalvérový softvér musíte nainštalovať a otestovať, či nezasahuje do bežných firemných operácií, ako aj zdokumentovať postupy, ktorými sa majú zamestnanci riadiť v prípade zachytenia malvéru.

## Vzdelávajte

Nestačí, ak budú zamestnanci vedieť, aké bezpečnostné politiky a postupy platia vo vašej spoločnosti. Musia tiež chápať, prečo sú nevyhnutné. Je preto potrebné investovať do zvyšovania povedomia o bezpečnosti a do vzdelávania v tejto oblasti – toto je zväčša to najúčinnejšie bezpečnostné opatrenie, ktoré môžete vo svojej spoločnosti implementovať.

Keď budete pracovať so svojimi zamestnancami, dokážete zvýšiť povedomie o problémoch, akými sú napríklad phishingové e-maily. Nedávna správa venovaná únikom dát ukázala, že zamestnanci otvorili 21 percent zaslaných phishingových e-mailov a 16 percent príjemcov otvorilo aj prílohu [3] – takéto správanie zamestnancov výrazne zvyšuje možnosť úniku údajov a krádeže informácií.

Dôležité je vzdelávať všetky osoby, ktoré používajú vaše firemné systémy, vrátane vedúcich pracovníkov, dodávateľov a partnerov. A pamätajte, že porušenie bezpečnostných politík musí mať svoje následky. Neschopnosť presadzovať politiky totiž podkopáva celé úsilie vynaložené na zvyšovanie IT bezpečnosti.

## Naďalej prehodnocujte, auditujte a testujte

Kybernetická bezpečnosť je pre každú firmu, či už veľkú alebo malú, dlhodobým procesom, nie jednorazovým projektom. Mali by ste si preto naplánovať pravidelné prehodnotenie firemného zabezpečenia aspoň raz ročne. Pravidelne sledujte informácie o novovznikajúcich hrozbách čítaním bezpečnostných správ na webových stránkach, akými sú napríklad WeLiveSecurity.com, KrebsOnSecurity.com a DarkReading.com.

Vaše bezpečnostné politiky a kontrolné prostriedky budete pravdepodobne musieť aktualizovať viac ako raz ročne v závislosti od zmien vo firme, akými sú napríklad vzťahy s novými dodávateľmi, nové projekty, noví zamestnanci alebo odchádzajúci zamestnanci (v tomto prípade treba tiež zabezpečiť, aby bol prístup odchádzajúcich zamestnancov do všetkých systémov zrušený). Zvážte prijatie externého konzultanta, ktorý vykoná penetračný test a bezpečnostný audit, čím zistíte, kde sú vaše slabé miesta, a následne ich budete môcť riešiť.

3 Zdroj: The Cost of Insecure Mobile Devices in the Workplace – štúdia inštitútu Ponemon z roku 2014

Súčasná vlna kybernetického zločinu sa tak skoro neskončí, takže je potrebné, aby ste neustále vyvíjali maximálne úsilie na ochranu údajov a systémov, ktoré sú z pohľadu dnešných malých firiem životne dôležité.

*Stephen Cobb už viac ako 25 rokov skúma zabezpečenie dát a ochranu osobných údajov a poskytuje vládnym inštitúciám USA a niektorým z najväčších svetových spoločností poradenstvo v oblasti stratégie informačnej bezpečnosti. Cobb je tiež spoluzakladateľom dvoch úspešných IT bezpečnostných firiem, ktoré sa akvizíciou stali súčasťou verejne obchodovaných spoločností, a je autorom niekoľkých kníh a stoviek článkov o informačnej bezpečnosti. Od roku 1996 je certifikovaným profesionálom v oblasti informačnej bezpečnosti (CISSP) a pôsobí v San Diegu v rámci globálneho výskumného tímu spoločnosti ESET.*

*Už viac ako 30 rokov ESET® vyvíja popredný bezpečnostný softvér pre firmy a domácnosti na celom svete. V rámci širokej škály riešení určených pre koncové pracovné stanice a mobilné zariadenia až po šifrovanie a dvojfaktorové overovanie prináša ESET zákazníkom vysokovýkonné a zároveň jednoducho použiteľné produkty, vďaka ktorým firmy aj domácnosti môžu bez obáv využívať celý potenciál svojich technológií. ESET chráni používateľov bez zbytočného rušenia 24 hodín denne, pričom ochranné mechanizmy sa aktualizujú v reálnom čase, aby boli používatelia vždy v bezpečí a firemná prevádzka mohla fungovať bez prerušení. Viac informácií nájdete na stránke [www.eset.sk](http://www.eset.sk).*

## UROBTE ĎALŠÍ KROK

*Prezrite si IT bezpečnostné riešenia, ktoré pre malé firmy ponúka spoločnosť ESET.*

ZISTIŤ VIAC

*Objavte dvojfaktorovú autentifikáciu od spoločnosti ESET, ktorá vám poskytne vyššiu úroveň ochrany údajov a umožňuje overiť identitu používateľa jediným ťuknutím na mobilnom zariadení.*

ZISTIŤ VIAC

*Naštudujte si potrebné informácie o všeobecnom nariadení Európskej únie o ochrane osobných údajov (GDPR) a zistite, ako si zaistiť súlad s týmto záväzným nariadením.*

ZISTIŤ VIAC