6 KROKOV

ku kybernetickému zabezpečeniu malých a stredných firiem

Digital Security
Progress. Protected.

6 KROKOV KU KYBERNETICKÉMU ZABEZPEČENIU MALÝCH A STREDNÝCH FIRIEM

Počítače a internet prinášajú malým firmám množstvo výhod, no s novými technológiami prichádzajú aj riziká. Niektoré riziká, 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.

Podľa správy inštitútu Ponemon sa v roku 2019 stretlo s únikom údajov 63 percent malých a stredných firiem. Mnohé spoločnosti sa však domnievajú, že z dôvodu ich malej veľkosti a obmedzených aktív im kybernetické útoky nehrozia. Bohužiaľ, nie je to pravda.

Táto príručka vám pomôže chrániť vašu firmu pred kybernetickými hrozbami.

Častým cieľom kybernetických zločincov sú osobné údaje. 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 platobných kariet, čísiel bankových účtov, hesiel k internetovému bankovníctvu, e-mailových kont a prihlasovacích údajov do služieb, ako sú eBay, PayPal a TurboTax.

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

Digital Security
Progress. Protected.

43 %

kybernetických útokov je zameraných na malé firmy

40 %

malých a stredných firiem zaznamenalo v dôsledku kybernetického útoku výpadok v trvaní osem a viac hodín

zdroj: Agility SMB

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 zákazníkoch a ich zneužití na podvody.

Niektoré údaje sú chránené zákonmi a nariadeniami, akými sú napríklad nariadenie **GDPR v Európskej únii a CCPA v Kalifornii**. Mnohé štáty tiež vyžadujú, aby firmy nahlásili 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 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 otázkach 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.

Jedna tretina nákladov súvisiacich s únikom údajov vznikne viac ako 1 rok po incidente. Približne **22 %** týchto nákladov vznikne v druhom roku.

zdroj: ENISA

AKÉ KROKY PODNIKNÚŤ:

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

A. Posúďte svoje aktíva, riziká a zdroje.

B. Vytvorte si politiky.

C. Zvoľte kontrolné prostriedky.

D. Nasaďte kontrolné prostriedky.

E. Vzdelávajte zamestnancov, riadiacich pracovníkov a dodávateľov.

F. Naďalej vyhodnocujte, auditujte a testujte.

Digital Security
Progress. Protected.

POSÚĎTE SVOJE AKTÍVA, RIZIKÁ A ZDROJE

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 vzhľadom na to, že v prieskume **62 percent z 1 100 profesionálov uviedlo**, že v záujme efektivity opomínajú zabezpečenie mobilných zariadení.1

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

Vytvorený zoznam si prejdite a zvážte riziká spojené s každou položkou. Položte si otázku, kto alebo čo predstavuje hrozbu. Aké riziká sa spájajú s prácou na diaľku? 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 problémov kybernetickej bezpečnosti**. Môže to byť niekto zo zamestnancov, kto má dobré znalosti a vyzná sa v bezpečnosti, alebo to môže byť obchodný partner či dodávateľ. Kybernetické zabezpečenie svojej firmy môžete tiež zveriť do rúk poskytovateľovi spravovaných služieb (MSP), ktorý vám poskytne potrebnú podporu.

62 %
profesionálov priznalo, že v záujme efektivity opomínajú zabezpečenie mobilných zariadení

1) zdroj: Cyber Talk, marec 2020

3 VYTVORTE SI POLITIKY

VYTVORTE SI POLITIKY

Solídny bezpečnostný program sa zakladá na bezpečnostných politikách, 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.

Mali by ste zadefinovať, kto má prístup ku konkrétnym údajom v rámci organizácie a na aké účely má oprávnenie s týmito údajmi zaobchádzať. Je tiež dôležité zaviesť politiky týkajúce sa vzdialeného prístupu, autorizovaného softvéru alebo možnosti priniesť si do firmy vlastné zariadenie (BYOD).

ZVOĽTE KONTROLNÉ PROSTRIEDKY

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 dvojúrovňového overovania.

Ak chcete mať kontrolu nad tým, ktoré programy je povolené spúšťať na firemných počítačoch, môžete sa rozhodnúť nedať zamestnancom administrátorské práva. Aby ste zabránili úniku údajov, ku ktorému môže dôjsť v dôsledku straty alebo krádeže mobilného zariadenia, 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 tieto bezpečnostné technológie:

- **riešenie na ochranu koncových zariadení**, ktoré zabezpečí 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 dvojúrovňového overovania**, aby sa na získanie prístupu k firemným systémom a údajom okrem prihlasovacieho mena a hesla vyžadoval aj ďalší bezpečnostný prvok,
- **riešenie VPN**, ktoré poskytne dodatočnú vrstvu ochrany pre zamestnancov pracujúcich na diaľku.

Posilnite IT bezpečnosť svojej firmy

Oblasť kybernetickej bezpečnosti sa neustále vyvíja, pričom útočníci využívajú čoraz sofistikovanejšie techniky maskovania. Ich hlavným cieľom je nepozorovane dostať malvér na koncové zariadenie a obísť detekciu antimalvérového riešenia vytvorením úplne nových, doposiaľ neznámych alebo tzv. zero day hrozieb.

Cloudový sandbox predstavuje obrannú vrstvu fungujúcu mimo firemnej siete. Zabezpečuje, aby sa ransomvér a zero day hrozby nikdy nespustili priamo v produkčnom prostredí. Podozrivý súbor sa na koncovom zariadení zablokuje ešte pred spustením, aby mohla najskôr prebehnúť jeho analýza.

NASAĎTE KONTROLNÉ PROSTRIEDKY

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.

Pri výbere správneho riešenia na ochranu koncových zariadení si treba všímať niekoľko kľúčových aspektov. Hľadať by ste mali riešenie s čo **najvyššou úspešnosťou detekcie** a zároveň čo najnižším počtom falošných poplachov, čo sú vlastne upozornenia na nesprávne identifikované súbory alebo odkazy, ktoré v skutočnosti nie sú škodlivé. Zvolené riešenie by tiež **nemalo mať výrazný vplyv na výkon systému** a malo by byť jednoduché na správu aj údržbu

Konzola na správu zabezpečenia koncových zariadení

Pri nasadzovaní bezpečnostných riešení na koncové zariadenia je veľkou výhodou, keď máte z jedného miesta prehľad o všetkých firemných zariadeniach. Takúto funkcionalitu ponúka cloudová konzola, akou je ESET PROTECT.

Umožňuje dohliadať na zariadenia v rámci priestorov firmy aj mimo nej v reálnom čase, ako aj vytvárať komplexné reporty a spravovať zabezpečenie pre všetky operačné systémy.

Zaisťuje prevenciu, detekciu a reakciu na hrozby na všetkých platformách vrátane stolových počítačov, serverov, virtuálnych počítačov a dokonca aj spravovaných mobilných zariadení.

VIAC INFORMÁCIÍ

ZABEZPEČTE VZDELÁVANIE

ZABEZPEČTE VZDELÁVANIE

Nestačí, ak budú zamestnanci vedieť, aké bezpečnostné politiky a postupy platia vo vašej spoločnosti. Musia tiež chápať, prečo sú nevyhnutné. Treba preto **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 aktívne pracovať so svojimi zamestnancami, dokážete zvýšiť povedomie o problémoch, akými sú napríklad phishingové e maily. Štúdia ukázala, že 43 percent zamestnancov si nie je istých, čo phishingový útok vlastne je2.

Preto je dôležité pre zamestnancov organizovať pravidelné školenia, napríklad vo forme kvízu na tému phishingu, aby ste ich naučili, aké techniky útočníci používajú. Oboznámte nových zamestnancov so základmi kybernetickej bezpečnosti už pri ich nástupe do firmy a bezpečnostné tipy spíšte aj na intranetovej stránke.

Vzdelávajte každého, kto používa 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.

Bezplatný online kurz na zvyšovanie povedomia o kybernetickej bezpečnosti, ktorý poskytuje spoločnosť ESET, predstavuje jednoduchý a efektívny spôsob, ako vzdelávať svojich zamestnancov. Kurz trvá menej ako 60 minút a pokrýva rôzne témy od phishingu cez pravidlá silných hesiel až po bezpečnosť pri práci na diaľku.

69 %

organizácií zaznamenalo narušenie bezpečnosti v dôsledku vnútornej hrozby, a to aj napriek preventívnym opatreniam[3]

Digital Security
Progress. Protected.

ZAČAŤ TERAZ

2) zdroj: ZD Net, október2020
3) zdroj: Sapio Research Study, UK

NAĎALEJ VYHODNOCUJTE, AUDITUJTE A TESTUJTE

NAĎALEJ VYHODNOCUJTE, 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.

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

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.

Ak chcete mať vždy aktuálne informácie o najnovších hrozbách, sledujte správy zo sveta kybernetickej bezpečnosti a prihláste sa na odber noviniek z webových stránok, ako sú:

WeLiveSecurity.com

DataSecurityGuide.eset.com

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

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 dvojúrovňové overovanie prináša ESET svojim 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.

© 1992 - 2021 ESET, spol. s r.o. - Všetky práva vyhradené. Použité ochranné známky sú ochrannými známkami alebo registrovanými ochrannými známkami spoločnosti ESET, spol. s r. o., alebo ESET North America. Všetky ostatné názvy a značky sú registrovanými ochrannými známkami príslušných spoločností.