OCHRANA FIREMNÍCH DAT

před kybernetickými útoky

JAK ZAJISTIT KOMPLEXNÍ ZABEZPEČENÍ CITLIVÝCH DAT V MALÝCH A STŘEDNÍCH FIRMÁCH.

ESET®

Digital Security
Progress. Protected.

Proč **se chránit?**

Kyberzločince primárně zajímá finanční zisk, takže i když nemusí cílit konkrétně na vaši firmu, můžete být terčem útoku.

Úniky dat a kybernetické útoky nejsou nic nového, útočníci neustále vyvíjejí nové techniky a taktiky, které jim umožní zasáhnout co největší počet cílů jedním úderem. Logicky se proto zaměřují na malé a střední firmy, které reprezentuje více než 99 procent všech firem na světě.

“VAŠE FIRMA PRO NÁS NENÍ ZAJÍMAVÁ, JE PŘÍLIŠ MALÁ”

– tohle si žádný hacker rozhodně nemyslí.

Moderní metody útoků

Bezpečnostní hrozby jsou mnohem vážnějším a frekventovanějším problémem než v minulosti. Malé a střední firmy, s omezeným rozpočtem a zaměstnanci, jsou pro útočníky většinou snadným cílem. Na druhou stranu jsou obvykle flexibilnější v případě útoku i implementace bezpečnostních pravidel. Pokud provedou správná opatření, mohou i malé a střední firmy razantně omezit riziko potenciálního útoku.

- Pokročilé malwarové techniky (jako je polymorfismus a metamorfismus), ransomware, a trojské koně se vzdáleným přístupem (RAT)
- DHA (Directory harvest attack) útoky
- Masivní automatizované botnety
- DNS hijacking a DNS cache poisoning
- Port hopping a SSL maskování
- DDoS útoky

Do nákladů na obnovu počítáme

- ✓ Náklady na obnovu a forenzní náklady (obvykle největší část)
- ✓ Narušení podnikání (včetně ztráty času a produktivity)
- ✓ Přímé náklady (např. upozornění zákazníkům, následná zákaznická podpora, obnova a výměna platebních karet a podobně)
- ✓ Ztráta zákazníků, zničení značky, ztráta pověsti
- ✓ Soudní spory se zákazníky, obchodními partnery a investory
- ✓ Regulační pokuty
- ✓ Ztráta majetku (např. duševní vlastnictví)

Nejčastější typy útoků

MASIVNÍ AUTOMATIZOVANÉ ÚTOKY

- Útočníci využívají sofistikovaný malware a škodlivé botnetové sítě k narušení zabezpečení sítě. Obvykle necílí na konkrétní firmu.

RANSOMWARE

- Jeden z nejúspěšnějších typů útoků. Data obvykle zpět nezískáte ani po zaplacení tučného výpalného.

ZLOČIN JAKO SLUŽBA (CRIME-AS-A-SERVICE - CAAS)

- Zločinecké organizace vyvíjí škodlivý software stále sofistikovanějším způsobem. Kybernetické zbraně jako je ransomware jako služba (ransomware-as-a-service) umožňují provést kybernetický útok i skupinám bez potřebných znalostí.

INTERNET VĚCÍ (IOT)

- Zařízení jsou často nezabezpečená „přímo z výroby“, což zvyšuje jejich náchylnost ke zneužití. Útočníci v současné době testují trh internetu věcí, aby zjistili, zda se vyplatí investovat prostředky do útoků.

DODAVATELSKÝ ŘETĚZEC

- Přes zranitelnosti u některého z vašich dodavatelů, se kterými spolupracujete, se útočníci mohou dostat i do vaší firmy. Nehledě na to, že vaši partneři mohou mít uložená citlivá data i vašich zákazníků.

Nařízení GDPR

GDPR bylo přijato za účelem ochrany soukromí jednotlivců v EU tím, že jim přiznává větší práva a kontrolu nad svými osobními údaji. Subjekty například mohou:

- požadovat, aby jim firmy poskytly kopii jejich údajů ve strukturovaném, běžně používaném a strojově čitelném formátu
- požadovat, aby jejich údaje byly předány jinému správci (“právo na přenositelnost údajů”)
- požadovat, aby jejich údaje byly vymazány (“právo být zapomenut”)

GDPR zavádí mnohem přísnější pravidla, pokud jde o souhlas, oznámení o úniku citlivých dat, povinné dopadové studie na soukromí údajů a požadavek “záměrné a standardní ochrany osobních údajů”.

Nesplnění zajištění souladu s GDPR může vyústit v uložení pokuty až do výše 4 procent ročního celosvětového příjmu firmy nebo 20 milionů EUR - podle toho, která částka je vyšší.

GDPR rovněž navrhuje řadu bezpečnostně technických opatření, která mohou být použita k zajištění ochrany údajů, včetně:

- pseudonymizace a šifrování osobních údajů
- schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- schopnosti obnovit dostupnost osobních údajů a včasného přístupu k nim v případě fyzických či technických incidentů
- procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování

5 tipů, jak být v souladu s GDPR

ZJISTĚTE A POSUĎTE, JAK ÚDAJE ZPRACOVÁVÁTE

Musíte si určit, zda je vaše firma zpracovatelem údajů nebo správcem údajů, přičemž je třeba mít na paměti, že může být obojí. Zásadní je vědět, kde se údaje uchovávají, zda je toto místo zabezpečené a zda se tyto údaje sdílí.

POUČTE SE Z PŘEDCHOZÍCH ZKUŠENOSTÍ

Pro zjištění vašich možností reagovat na budoucí útok je nejprve potřeba vyhodnotit, co se stalo při případných předchozích útocích. Zásadním krokem k zajištění souladu s GDPR je aktualizace (nebo vytvoření) reakčního plánu v případě incidentů a pravidelné testování vašich schopností na incidenty reagovat.

JMENUJTE POVĚŘENCE NA OCHRANU ÚDAJŮ

Pověřenec na ochranu údajů jedná nezávisle a tím, že odpovídá nejvyšší úrovni managementu, může pomoci implementovat dané požadavky. Významně se tak sníží riziko udělení pokuty.

VZDĚLÁVEJTE OHLEDNĚ PRAVIDEL SEBE I SVÉ ZAMĚSTNANCE

Jedním z hlavních cílů GDPR je posílit možnost, aby lidé měli právo být zapomenuti a jejich údaje byly vymazány. Společnosti rovněž budou muset před zpracováním jejich údajů získat “jasnou, pozitivní reakci”.

POZNEJTE HLAVNÍ KONTROLNÍ AUTORITU

Příslušnost autority, která se zabývá stížnostmi proti vaší společnosti, je závislá na místu sídla vaší společnosti, ne na místě, kde jednotlivé osoby podaly stížnost. V různých zemích navíc mohou platit i přísnější směrnice nebo nařízení.

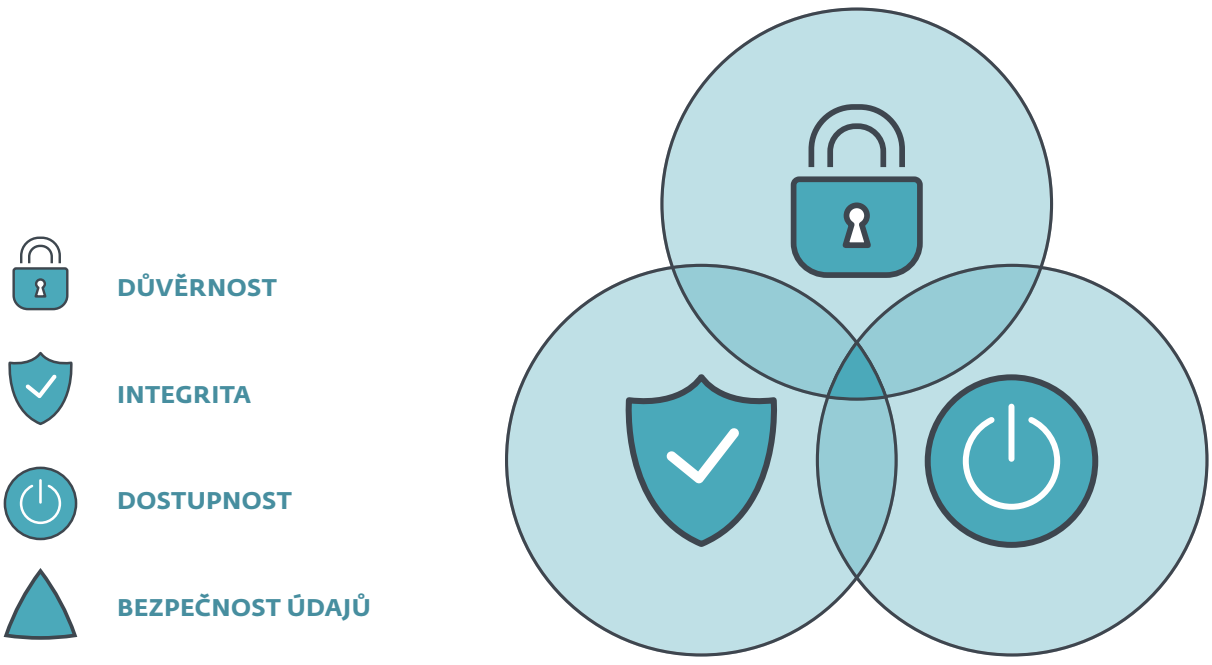
Základy ochrany údajů

Ochrana údajů (a v širším smyslu zabezpečení informací) zahrnuje veškeré administrativní, logické a technické kontroly potřebné k ochraně informací.

Jako návod pro tvorbu a implementaci pravidel potřebných k zajištění bezpečnosti informací v rámci organizace se běžně používá C-I-A diagram.

- **Důvěrnost**
  Data jsou přístupná a sdělená pouze autorizovaným osobám.
- **Integrita**
  Data jsou správná (tzn. nezměněná) a úplná.
- **Dostupnost**
  Autorizovaní uživatelé mají spolehlivý a včasný přístup k údajům.

C-I-A diagram



Zajištění bezpečnosti údajů

Pro důvěrnost informací se typicky používají různé bezpečnostní politiky a zásady ochrany osobních údajů, které určují, kdo má přístup k jakým údajům, za jakým účelem a k jakým činnostem s daty má oprávnění.

Pro ochranu integrity údajů je možné implementovat různá technická řešení, jako jsou kontrolní součty a ověření vstupních dat na formulářích a v databázích.

K ochraně dostupnosti údajů proti náhodnému zničení (například smazání) nebo úmyslnému zničení (například ransomwarový útok) se implementují systémy zálohy a obnovy.

Pro zajištění bezpečnosti údajů musíte vzít v potaz všechny tři aspekty diagramu (důvěrnost, integrita a dostupnost). Včetně systémů a aplikací, které zpracovávají a uchovávají údaje, po celou dobu životního cyklu.

S použitím přístupu založeného na míře rizika potom můžete implementovat vhodné kontrolní mechanismy, které řeší zranitelná místa. Získáte tak přijatelnou úroveň rizika proti konkrétním hrozbám.

ČÍM VĚTŠÍ RIZIKO, TÍM DOKONALEJŠÍ BY MĚLA BÝT OPATŘENÍ.

4 fáze řízení bezpečnostního rizika

1. Posouzení

Pro posouzení rizika existuje mnoho metod s různou úrovní nákladů a složitosti.

Základní postup se však obvykle skládá z:

IDENTIFIKACE AKTIV
Identifikuje všechny aktiva společnosti (hmotné i nehmotné), která vyžadují ochranu, včetně kvantitativních hodnot (náklady nebo přispění k výnosům) a/nebo kvalitativních hodnot (relativní důležitost).

ANALÝZA HROZEB
Definuje možné nepříznivé přirozené a/nebo umělé okolnosti nebo události, potenciální dopad nebo následky, pravděpodobnost a frekvenci výskytu.

POSOUZENÍ ZRANITELNOSTI
Určuje, které záruky a/nebo kontroly v aktivech nejsou přítomné nebo jsou slabé.

2. Řešení

Vyhodnocení rizika poskytuje základ pro rozhodnutí, co dělat s konkrétními riziky.

ZMÍRNĚNÍ RIZIKA
Implementace strategií, kontrolních mechanismů a/nebo jiných opatření za účelem snížení dopadu nebo pravděpodobnosti určité hrozby pro daná aktiva.

PŘEVEDENÍ RIZIKA
Převedení potenciálního rizika na třetí stranu, jako je například pojišťovna, poskytovatel služby nebo jiná osoba, která výslovně souhlasí s přijetím rizika.

VYHNUTÍ SE RIZIKU
Odstranění rizika, například provedením aktualizace nebo odstraněním aktiva, nebo ukončením činnosti, která riziko zavádí.

3. Přijetí

Je formální schválení implementovaných opatření pro řešení daného rizika a přijetí zbývajících rizik, která nelze zmírnit, převést nebo se jim nelze vyhnout.

4. Komunikace

Příslušné zúčastněné strany je nutno uvědomit o všech rozhodnutích o řešení a/nebo přijetí rizika, včetně definice jednotlivých rolí a povinností s ohledem na konkrétní rizika.

Jak identifikovat operace zpracování údajů?

Dříve než začnete posuzovat rizika, je důležité, abyste porozuměli, jakým způsobem se údaje v rámci vaší firmy zpracovávají. V malé nebo střední firmě se obvykle jedná o operace, které se týkají:

LIDSKÝCH ZDROJŮ

- ✓ správa výplat, přijímání nových a udržení stávajících zaměstnanců, záznamy o školení nebo vyhodnocení pracovních výsledků.

SPRÁVY ZÁKAZNÍKŮ A DODAVATELŮ

- ✓ informace o zákaznících, objednávkách, fakturách, seznamy e-mailových adres atd.

BEZPEČNOSTI ZAMĚSTNANCŮ A FYZICKÉHO ZABEZPEČENÍ

- ✓ různé bezpečnostní protokoly o aktivitě zaměstnanců, záznamy o návštěvách, video monitorování.

U každé operace zpracování údajů si položte následující otázky:

- Jaké osobní údaje se zpracovávají?
- Za jakým účelem se zpracovávají?
- Kde zpracovávání probíhá?
- Kdo je za zpracování odpovědný?
- Kdo má k údajům přístup?

Zásada minimálních práv je osvědčený postup, kdy je koncovým uživatelům udělena pouze minimální úroveň přístupu nezbytná pro výkon jejich konkrétní pracovní funkce.

Jak vyhodnotit potenciální dopad na firmu?

Dopad daného rizika je obvykle vyjádřen ve smyslu škody, kterou by společnost utrpěla, jako je ztráta nebo zničení fyzického aktiva (server, kopírka nebo vozidlo, atd.)

Dopad na firmu může být i nepřímý. V případě citlivých osobních údajů je totiž subjekt (např. zákazník), jehož údaje byly odcizeny nebo kompromitovány, přímou obětí. V takových případech může být ukradena identita nebo finanční aktivum jednotlivce a/nebo narušeno jeho soukromí.

Dopad na firmu je méně přímý než dopad na jednotlivce, ale i tak potenciálně velmi nákladný a může mimo jiné zahrnovat:

- Ztrátu zákazníků a příjmu
- Poškození značky a negativní PR
- Regulační pokuty a soudní spory
- Náklady spojené s oznámením úniku údajů
- Forenzní analýzy a obnovy

Jak identifikovat možné hrozby a vyhodnotit pravděpodobnost?

Hrozbou mohou být jakékoliv události nebo okolnosti (přírodní nebo uměle vytvořené), které mohou negativně ovlivnit důvěrnost, integritu a dostupnost osobních nebo citlivých dat.

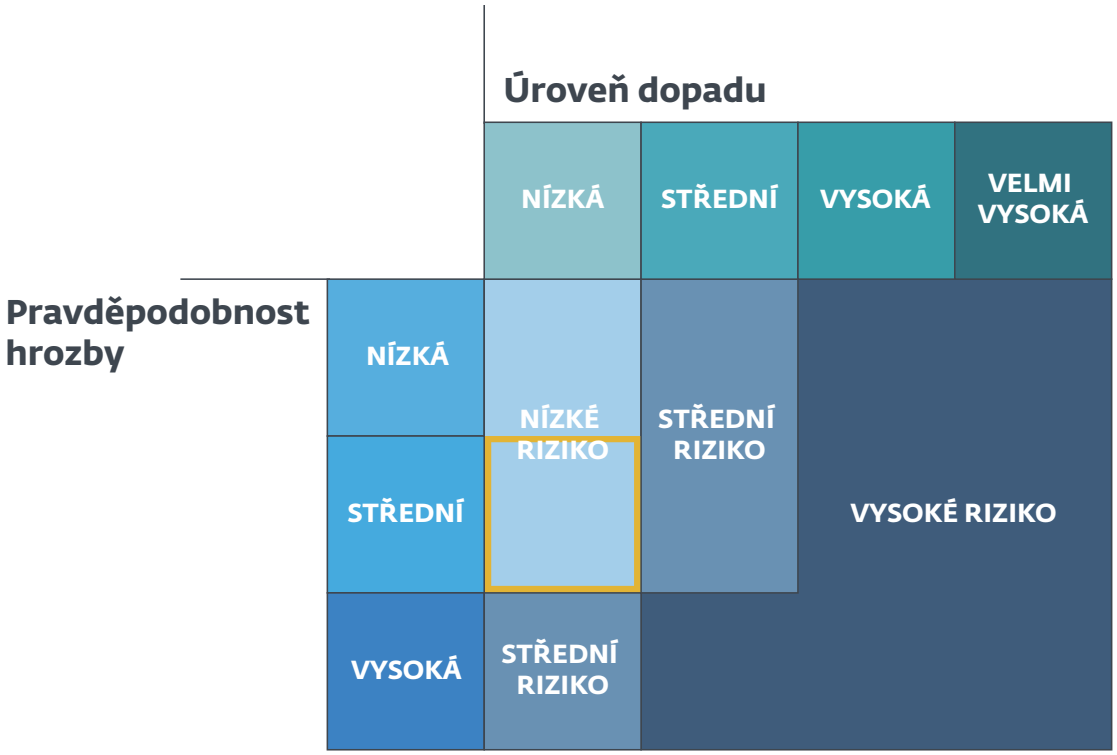
Může jít o kybernetické útoky, náhodné ztráty nebo krádeže firemních IT zařízení, interní hrozby, požáry a záplavy, zemětřesení, vlivy extrémního počasí, pracovní spory a podobně.

Firmy musí identifikovat možné hrozby a vyhodnotit pravděpodobnost (včetně frekvence výskytu). Musíte mít jistotu, že máte hrozby zařazeny do konkrétně definovaných oblastí, včetně hrozeb ze síťových a technických zdrojů (software/hardware), souvisejících procesů a postupů, lidských zdrojů a hrozby vyplývající z rozsahu zpracování.

Pro každou identifikovanou hrozbu můžete pravděpodobnost klasifikovat obdobným způsobem jako u dopadu na firmu: nízká, střední a vysoká. Při vyhodnocování pravděpodobnosti výskytu hrozby je potřeba zvážit, jak pravděpodobnost výskytu hrozby obecně, tak i to, jak často je pravděpodobné, že se hrozba vyskytne během určité doby (například během jednoho roku).

Jak vyhodnotit riziko?

Jako poslední budete hodnotit riziko spojené s každou operací a v závislosti na výsledku hodnocení implementovat vhodné technologické kontrolní mechanismy a organizační postupy.



Pravděpodobnost hrozby

Pro konkrétní operaci zpracování projděte seznam možných hrozeb a vyhodnoťte jejich pravděpodobnost. Výsledná pravděpodobnost by měla být součtem hodnot ze všech hrozeb ze seznamu.

- **Nízká** – Není pravděpodobné, že hrozba nastane.
- **Střední** – Je důvodná šance, že hrozba nastane.
- **Vysoká** – Je pravděpodobné, že hrozba nastane.

Výsledná úroveň rizika

- **Nízká**
- **Střední**
- **Vysoká**

Úroveň dopadu

Pro konkrétní operaci zpracování vyhodnoťte možný dopad na důvěrnost, integritu a dostupnost dat (C-I-A diagram). Výsledná úroveň dopadu je nejvyšší ze všech tří úrovní.

- **Nízká** – Drobné obtíže, které lze bez problému překonat.
- **Střední** – Zásadní obtíže, které lze překonat i přes několik nesnází.
- **Vysoká** – Zásadní důsledky, které lze překonat, ale s vážnými obtížemi.
- **Velmi vysoká** – Zásadní nebo dokonce nezvratné důsledky, které nelze překonat.

OCHRANA ÚDAJŮ OD A DO F

A. POSOUZENÍ AKTIV, RIZIK A ZDROJŮ

Nejprve si vytvořte seznam veškerého používaného softwaru, počítačových systémů a služeb, které používáte (včetně mobilních zařízení a cloudových služeb jako je Dropbox, iCloud, Google Docs, Office365 a podobně. Seznam projděte a zvažte nejen rizika spojená s každou položkou, ale i to, zda daný systém, software nebo službu vůbec potřebujete.

Některá rizika jsou pravděpodobnější než jiná. Sepište všechny a seřaďte je podle škody, kterou by mohly způsobit a pravděpodobnosti jejich výskytu. K jednotlivým rizikům doplňte zdroj zabezpečení. Tak zjistíte, zda jste schopni pokrýt zabezpečení sami nebo budete potřebovat externího odborníka.

B. VYTVOŘENÍ BEZPEČNOSTNÍCH POLITIK

Zabezpečení firemní sítě stojí a padá na dodržování a vynucování bezpečnostních politik, které odsouhlasilo vedení. Pokud jste manažer, musíte všem dát vědět, že berete bezpečnost vážně, a že je vaše společnost odhodlaná chránit soukromí a bezpečnost všech údajů, které shromažďuje. Musíte určit kritické politiky, které budete vynucovat.

C. KONTROLA DODRŽOVÁNÍ POLITIK

Pro dodržování a vynucování politiky zaveďte kontrolní mechanismy. Budete potřebovat minimálně tři základní bezpečnostní technologie:

- Software proti malwaru, který chrání zařízení proti škodlivému kódu.
- Šifrování, které zajistí, že údaje budou na ztracených nebo ukradených zařízeních nečitelné.
- Vícefaktorovou autentizaci, kdy je nutné pro přihlášení kromě uživatelského jména a hesla použít např. jednorázový přístupový kód zaslaný na autorizovaný mobilní telefon.

D. NASAZENÍ KONTROL

Kontroly musí být samozřejmě funkční a neměly by nijak omezovat produktivitu, proto je nutné je před nasazením do ostrého prostředí otestovat.

E. VZDĚLÁVÁNÍ ZAMĚSTNANCŮ A PRODEJCŮ

Zaměstnanci musí znát nejen firemní bezpečnostní politiky a postupy, ale také pochopit, proč je musí dodržovat. Vzdělávejte každého, kdo používá vaše systémy včetně výkonných pracovníků, prodejců a partnerů. Pokud se vám nepodaří nastavit a vynutit dodržování potřebných bezpečnostních politik, je pravděpodobné, že dříve nebo později dojde k bezpečnostnímu incidentu.

F. PRAVIDELNÉ POSOUZENÍ, AUDIT A TESTOVÁNÍ

Alespoň jednou do roka si naplánujte pravidelné posouzení bezpečnostních opatření. Je možné, že z důvodu firemních změn budete muset aktualizovat bezpečnostní politiky a kontrolní mechanismy častěji než jedenkrát za rok. Zvažte najmutí externího poradce, který pro vás bude zabezpečovat penetrační testy a bezpečnostní audit za účelem detekce vašich slabých míst a jejich nápravě.

10 KLÍČŮ K EFEKTIVNÍ OCHRANĚ ÚDAJŮ

1. VYTVOŘTE BEZPEČNOSTNÍ POLITIKY

Mnoho firem nebere v úvahu důležitost psaných bezpečnostních politik a rovnou se zabývá technickými kontrolami. Technické kontroly (firewall, anti-malware ochrana koncového zařízení a podobně) implementované bez administrativních kontrol (tj. politik a postupů) jsou téměř vždy implementovány reaktivním způsobem bez podrobně promyšlené, komplexní strategie. To může znamenat, že se budete příliš zabývat technickými kontrolami, které nejsou efektivně (nebo správně) nasazeny a poskytují nekompletní ochranu.

2. IDENTIFIKUJTE AKTIVA

Na počátku musíte vědět, co chcete nebo musíte chránit. Proto je důležité mít a průběžně aktualizovat přesný seznam veškerého IT hardwaru a softwaru. Bez kompletního seznamu nemusíte o zranitelných systémech ve vaší síti vědět, což samozřejmě zvyšuje riziko útoku. Skenovat síť a koncová zařízení můžete s pomocí mnoha volně dostupných nástrojů. Komerční řešení vám ale mohou pomoci pravidelně aktualizovat i seznam vašich aktiv, a obvykle nabízí i možnost vzdálené správy, instalace, odstranění a aktualizaci softwaru atd. Aktiva, jež jsou připojená na internet (včetně mobilních zařízení), představují největší riziko, a proto se jim musíte primárně věnovat.

3. DEFINUJTE PŘÍSTUP K ZABEZPEČENÍ

V závislosti na riziku identifikujte hrozby a zranitelnosti aktiv a najděte pro ně vhodná bezpečnostní opatření. Následně můžete provést rozdílovou analýzu a rozhodnout, jaké kroky bude potřeba učinit a kam je potřeba zainvestovat.

4. KLASIFIKUJTE VŠECHNY ÚDAJE

Citlivé zákaznické údaje jsou pro mnoho firem „to nejdůležitější“, co potřebuje ochranu. Poskytování rovnocenné ochrany a kontroly pro všechny údaje během celého jejich životního cyklu není nejen praktické, ale ani žádoucí. Místo toho se zamyslete, která data jsou opravdu důležitá a cenná, pokud by došlo k jejich ztrátě nebo odcizení.

Položte si otázku, jaký dopad by mělo porušení ochrany údajů na vaši značku, zákaznickou loajalitu nebo dokonce životaschopnost firmy? Vytvořte intuitivní politiky klasifikace údajů, které budou obsahovat názvy (jako třeba “Pouze pro interní použití”, “Citlivé údaje” a “Schváleno ke zveřejnění”), čímž zároveň specifikujete požadavky na ochranu údajů (jako je šifrování, zálohování, schválení ke zveřejnění a zničení) pro danou kategorii.

5. ŠIFRUJTE CITLIVÉ ÚDAJE

Šifrování přeměňuje čitelný formát dat do nečitelné podoby, která je pro osoby bez příslušného klíče bezcenná. Zapomenout byste neměli na údaje, které jsou tzv. na odpočinku” (nemůžete je smazat, musíte je archivovat). Pro „používaná data“ byste měli využít šifrování v aplikaci, pokud je k dispozici, a pro údaje “v pohybu” (nebo v “přenosu”) můžete použít dodatečné šifrování např. pomocí SSL šifrování. Šifrovat můžete hardwarově i softwarově.

6. ZÁLOHUJTE CENNÁ DATA

Pravidelné a spolehlivé zálohování cenných dat je základní a nezbytnou technikou ochrany dat. Kvalitní záloha vám vyřeší spoustu starostí při bezpečnostních incidentech, kdy dojde k poškození nebo zablokování přístupu k aktuálním datům. A nemusí jít nutně jen o malware útok, může jít například i o „pouhé“ selhání hardwaru.

7. INVESTUJTE DO OCHRANY KONCOVÝCH ZAŘÍZENÍ

Bezplatný anti-malwarový software může znamenat zbytečné riziko. Nic totiž není zadarmo, ani bezpečnostní řešení. Proto se vyplatí investovat do bezpečnostního řešení od renomovaného výrobce, které kromě ochrany zařízení obvykle nabízí i nástroje pro vzdálenou správu.

8. PLÁNUJTE A PŘIPRAVUJTE

Každá firma musí mít plán reakce na incident a plány kontinuity činnosti a obnovy po bezpečnostním incidentu. Odpovědný tým musí být proškolen v základních forenzních postupech, aby ke každému bezpečnostnímu incidentu přistupoval jako k potenciálnímu právnímu případu a zajistil, aby byly všechny kroky evidovány jako potenciální důkazy. Plány kontinuity činnosti a obnovy po incidentu pomohou vaší firmě spustit běžné firemní operace v co nejkratším čase.

9. ŠKOLTE UŽIVATELE

Nejslabším článkem v bezpečnosti jakékoliv společnosti byl a vždy bude koncový uživatel, což není nutně jeho chyba. Je velmi nepravděpodobné, že každý, kdo pracuje pro vaši firmu, je zároveň bezpečnostním expertem. Útočníci to vědí a používají techniky sociálního inženýrství, které „donutí" uživatele kliknout na zákeřný odkaz ve spamu nebo phishingovém e-mailu a navštívit škodlivé webové stránky. Proto pořádejte pravidelná školení o bezpečnostní problematice, aby uživatelé znali kybernetické nástrahy a zodpovědným přístupem přispívali k ochraně vašich firemních dat.

10. NESPOLÉHEJTE JEN NA SEBE

Kyberzločinci nepracují sami. Ale i na druhé straně barikády jsou lidé, kteří vám pomohou. Využijte široké komunity bezpečnostních expertů, od externích služeb třetí strany, zpravodajství o hrozbách v reálném čase založené na cloudu, až po podporu výrobce vašeho bezpečnostního řešení.

O ESETu

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která díky vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100.

Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

ESET V ČÍSLECH

1mld+
uživatelů po celém světě

400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

VYBRANÁ OCENĚNÍ

AV comparatives APPROVED Business Security DEC 2021

ESET získal v prosinci 2021 ocenění „APPROVED" za ochranu koncových řešení v business security testu společnosti AV-Comparatives.

G2 Leader WINTER 2022

ESET trvale dosahuje špičkových výsledků na celosvětové platformě hodnocení uživatelů G2 a jeho řešení jsou oceňována zákazníky po celém světě.

FORRESTER®

Řešení ESET jsou pravidelně oceňována předními analytickými firmami, včetně „The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021".

eset® Digital Security
Progress. Protected.