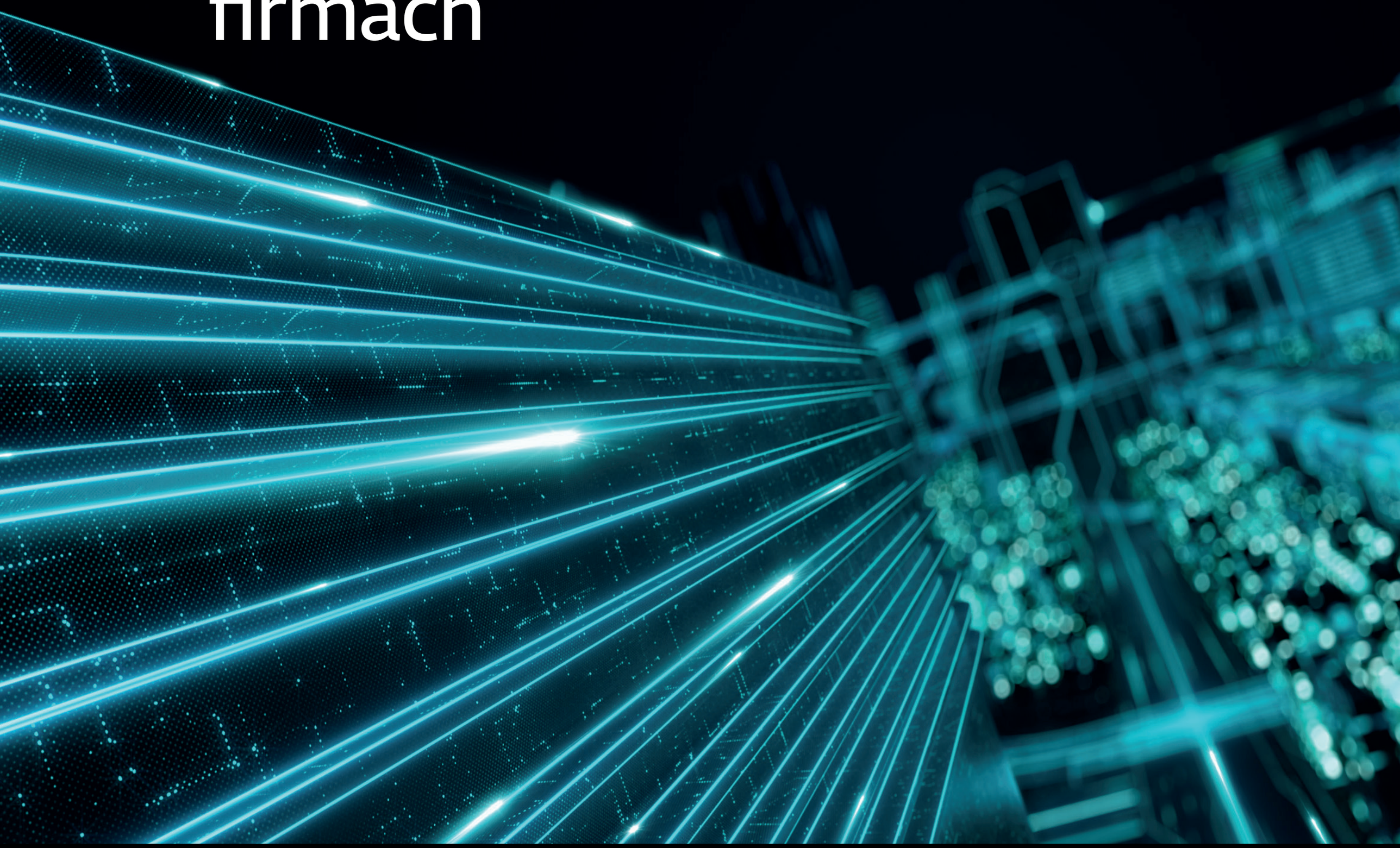
ENJOY SAFER TECHNOLOGY™

OCHRANA DAT

v malých a středně velkých firmách



kapitola 5

Organizační a procesní kontroly

V TÉTO KAPITOLE

- Doplnění technických kontrol organizačními kontrolami
- Rozpoznání potřeby kontroly procesu

Kapitola 5

ORGANIZAČNÍ A PROCESNÍ KONTROLY

V této kapitole se dozvíte, jak fungují organizační a procesní kontroly s technickými kontrolami, aby pomohly ochránit citlivé údaje vaší firmy.

Zavedení organizačních kontrol

Efektivní ochrana údajů vyžaduje více než jen technické kontroly. Je nutné zavést administrativní a organizační kontroly, které zajistí, že jsou technické kontroly řádně implementovány, nakonfigurovány a provozovány v souladu se strategií správy zabezpečení. Některé příklady organizačních kontrol zahrnují:

Soukromé a citlivé osobní údaje

Technické kontroly, jako je šifrování a software pro prevenci ztráty dat (DLP), musí být vzhledem k jejich nákladům používány s rozvahou. Šifrování vyžaduje dodatečné zpracování (šifrování a dešifrování), a DLP řešení potřebují neustále vyhledávat klíčová slova a vzorce k identifikaci soukromých a citlivých údajů, jako jsou čísla kreditních karet, zdravotních informací nebo čísla sociálního zabezpečení. Zřízení schématu pro klasifikaci údajů vám pomůže pochopit, jaká data potřebují být chráněna, proč a jakým způsobem.

Dokumentace dat a audit

Firmy, které sbírají, zpracovávají a/nebo uchovávají citlivé údaje, musí zdokumentovat, proč tyto údaje sbírají, jakým způsobem je sbírají (a z jakých zdrojů), jak jsou využívány a chráněny. Zdokumentování politik zabezpečení dat a soukromí vám pomůže zodpovědět dané otázky a splnit tak požadavky případného auditu, zejména s ohledem na právní předpisy jako je HIPAA nebo Nařízení EU o ochraně osobních údajů (GDPR).

Bezpečnostní politiky

Příprava bezpečnostních politik nemusí nutně být složitá věc. V mnoha případech je to pár odstavců, které je potřeba sepsat. Bezpečnostní politiky musí jasně definovat jednotlivé role a povinnosti, které se vztahují k ochraně osobních údajů. Příklady důležitých bezpečnostních politik, které by každá firma měla vytvořit:

- používání internetu a e-mailu
- BYOD – používání soukromých zařízení zaměstnanců
- vzdálený přístup
- autorizovaný software

Lidské zdroje

Politiky pro lidské zdroje (zaměstnanci) obsahují zásady a postupy, které zajišťují, že shromažďované osobní údaje (jako jsou žádosti o zaměstnání, mzdové údaje, školení, disciplinární záznamy), jsou řádně chráněny. To rovněž obsahuje postupy týkající se hledání informací před uzavřením pracovní smlouvy, drogové testy a pracovní rotace.

Úroveň zabezpečení

Tento model vám pomůže posoudit úroveň zabezpečení a identifikovat rizika, které je potřeba eliminovat. To závisí samozřejmě na celé řadě faktorů, jako jsou:

- Typy údajů - např. citlivé údaje, finanční informace, duševní vlastnictví, lékařské vybavení nebo zásadní infrastrukturu.
- Obory podnikání - např. zdravotnictví, finance, maloobchod, zadávání zakázek nebo veřejná služba.
- Regulační povinnosti - např. HIPAA, Nařízení EU o ochraně osobních údajů (GDPR), PIPEDA a podobně.
- Rizikové faktory útoku – např. geografická poloha na nepřátelském nebo nestabilním území, ve městě s vysokým stupněm kriminality, v rizikové nebo průmyslové oblasti a podobně.

Školení a testování zaměstnanců

Zaměstnanci patří mezi nejčastější cíle útočníků. Proto je důležité zaměstnance pravidelně školit a testovat jejich odolnost vůči sociálnímu inženýrství a phishingu. Školení by mělo minimálně obsahovat problematiku zabezpečení hesel, spamu a phishingu, ochrany proti malwaru, sociálního inženýrství, právní povinnosti, a ochrany údajů (např. klasifikace údajů, druhy citlivých údajů a technologie na ochranu údajů).

Posouzení dopadu na ochranu údajů (DPIA)

Povinnost vypracovat DPIA je vyžadováno nařízením GDPR u všech operací, kde „zpracování údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to zejména při využití nových technologií“ například profilování.

Implementace ochrany údajů

Nařízení GDPR vyžaduje ochranu údaj „by design a by default”, což v praxi znamená, že společnosti by měli implementovat takové technické a organizační opatření, které zredukují shromažďované, zpracovávané a uchovávané osobní údaje na minimum.

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. Konec konců, pokud nevíte, jaká zařízení ve firmě máte, nemůžete je ani chránit. Ujistěte se, že na seznamu máte i mobilní zařízení, jako jsou chytré telefony a tablety, které se ve firmě používají. Podle Ponemonova institutu, je to velmi důležité, protože odhadem asi 60 % zaměstnanců obchází bezpečnostní požadavky na svém mobilním zařízení a 48 % jich blokuje požadované bezpečnostní nastavení zaměstnavatelem. Nezapomeňte ani na cloudové služby jako je Box, Dropbox, iCloud, Google Docs, Office365, OneDrive a SalesForce.

Seznam projděte a zvažte nejen rizika spojená s každou položkou, ale i to, zda daný systém, software nebo službu vůbec potřebujete. Pokládejte si otázky typu:

- Kdo nebo co je hrozbou?
- Co se může pokazit?
- A podobně.

Výskyt některých rizik je pravděpodobnější než výskyt jiných, sepište všechny a seřaďte je podle toho, jak velkou škodu by mohly způsobit a jak velká je pravděpodobnost jejich výskytu.

K jednotlivým rizikům je nutné doplnit jejich zdroj zabezpečení. Tak zjistíte, zda jste schopni pokrýt zabezpečení sami nebo budete potřebovat externího odborníka.
Tím může to být někdo ze zaměstnanců, kdo má znalosti a schopnosti z oblasti zabezpečení nebo partner či prodejce.

B) Vytvoření bezpečnostních politiky

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. Například že neautorizovaná osoba nesmí přistupovat do interních systémů společnosti a k jejím datům, a že zaměstnanci nebudou moci obejít bezpečnostní nastavení např. pomocí pracovních mobilních zařízeních.

C) Kontrola dodržování politik

Pro dodržování a vynucování politiky zaveďte kontrolní mechanismy. Například k vynucení politiky nepovoleného přístupu do interních systémů společnosti můžete zavést mechanismus, který kontroluje veškerý přístup do systému společnosti pomocí unikátního uživatelského jména, hesla a tokenu (2FA).

V každém případě potřebujete minimálně tři základní bezpečnostní technologie:

- Software proti malwaru, který chrání zařízení proti škodlivému kódu.
- Šifrování, které zajistí, že údaje jsou 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, obchodních partnerů a prodejců

Zaměstnanci musí znát nejen firemní bezpečnostní politiky a postupy, ale také pochopit, proč je musí dodržovat. Toho dosáhnete vzděláváním a zvyšováním povědí o problematice IT bezpečnosti, které je často tím nejefektivnějším bezpečnostním opatřením, jaké můžete implementovat.

Jedním z nejčastějších vektorů útoku je phishingový e-mail. V nedávné zprávě společnosti Verizon (Data Breach Investigation Report - DBIR) se ukázalo, že 23 procent zaměstnanců otevřelo phishingový email a 11 % příjemců otevřelo i přílohu.

Vzdělávejte každého, kdo používá vaše systémy včetně výkonných pracovníků, prodejců a partnerů. Myslete i na to, že každé porušení bezpečnostních zásad musí mí následky. 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

Kybernetická bezpečnost je pro každou firmu, ať už velkou nebo malou, stále se opakující, nikdy nekončící proces. Alespoň jednou do roka si naplánujte pravidelné posouzení bezpečnostních opatření. Sledujte nově vzniklé hrozby pravidelným čtením bezpečnostních zpráv na webových stránkách typu WeLiveSecurity.com, KrebsOnSecurity.com nebo DarkReading.com.

Je možné, že z důvodu firemních změn budete muset aktualizovat bezpečnostní politiky a kontrolní mechanismy častěji než jedenkrát za rok. Jde o situace, kdy se například změní vztahy s prodejci, vzniknou nové projekty, přijdou noví zaměstnanci, odchází stávající a tak podobně. V případě ukončení spolupráce, zaměstnaneckého poměru nezapomeňte vždy zrušit všechny přístupy do systémů všem, kteří z firmy odchází. Zvažte najmutí externího poradce, který pro vás bude zabezpečovat penetrační testy a bezpečnostní audit za účelem detekce vašich slabých míst a jejich nápravě.

Procesní kontroly

Procesní kontroly pomáhají firmám minimalizovat negativní dopad porušení ochrany údajů nebo ztráty dat. Nedávná studie Ponemonova institutu ukazuje, že pokud firmy implementují efektivní proces reakce na incident, který sníží dobu potřebnou k identifikaci a zabránění šíření porušení, tak mohou snížit svůj průměrný náklad za porušení ochrany údajů (jeden záznam) z průměrných 141 USD na zhruba 122 USD. V případě, že by došlo k porušení u 10 000 záznamů jednalo by se o úsporu zhruba 190 000 USD, a to už se vyplatí. Tým (nebo jedinec), který bude mít incidenty na starosti, může být interní, externí nebo kombinací obojího.

Při vytváření procesních kontrol:

Zapojte lidi

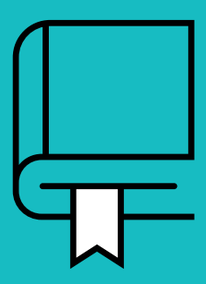
Návrh na procesní kontroly nemusí být řízen pouze shora dolů. Zapojení lidí, kteří přímo pracují s různými procesy a technologiemi, pomáhá zajistit, že kontroly dávají smysl a jsou efektivně implementovány.

Definujte odpovědnosti

Každý musí znát svou roli. Jasně a pochopitelně definujte jednotlivé odpovědnosti.

Vysvětlete, proč jsou procesní kontroly potřeba

Na bezpečnostní opatření je často nahlíženo negativně. Pokud zaměstnanci nerozumí, proč jsou kontroly pro firmu nutné a důležité, mohou je v konečném důsledku ignorovat nebo obcházet.



PAMATUJ

Podle Ponemonova institutu činí průměrný čas potřebný k identifikování bezpečnostního incidentu v průměru 191 dnů a v průměru dalších 66 dnů k přijetí opatření, které zabrání jeho šíření. Objem potřebného času k identifikaci a zabránění šíření porušení ochrany údajů má přímý dopad na jeho závažnost a výslednou cenu.

Firmy, které implementují procesy vedoucí k zabezpečení údajů, mohou snížit náklady na kybernetické útoky nebo ztrátu údajů prostřednictvím šifrování. Podle Ponemonova institutu šifrování snižuje průměrný náklad per 1 záznam o 16 USD. V mnoha případech může šifrování údajů (a také schopnost prokázat, že jsou data řádně zašifrované) pomoci naplnit hned několik předpisů o ochraně osobních údajů. Firmy tak mohou předejít oznámení o porušení, což jim výrazně snižuje náklady. A to jak přímé náklady (jako jsou oznámení, služby monitorující kredibilitu a soudní spory), tak nepřímé (poškození značky a ztráta zákazníků). Pokud tedy dojde k porušení u 10 000 záznamů, může šifrování snížit celkovou cenu až o zhruba 160 000 USD.

Důležité procesní kontroly zahrnují:

Politiky kontroly přístupu

Definují, kdo a k jakým systémům, aplikacím a údajům má přístup a za jakým účelem.

Řízení zdrojů a aktiv

Je důležité vědět, co chráníte a proč. Kromě udržování přesného soupisu počítačových a datových aktiv/zdrojů, musí společnosti také zajistit:

- aby byly systémy a aplikace vždy aktuální s nejnovějšími opravami chyb a bezpečnostními záplatami.
- okamžité vymazání nebo zničení citlivých údajů, které již nejsou vyžadovány v souladu s vytvořenými zásadami týkajících se držení, uchovávání a ničení údajů.

Řízení změn

Zajišťuje, že veškeré změny v systémech a aplikacích jsou zdokumentovány, otestovány a schváleny tak, aby jejich dopad neohrozil celkové zabezpečení firmy.

Reakce na incident

V případě bezpečnostního incidentu (malware útok nebo únik dat) jen nutné, aby firmy měly jasně definovaný a dobře srozumitelný plán reakce na incident. Tak zajistí okamžitou a efektivní reakci včetně zabránění šíření škody, analýzu základních příčin, zachování důkazů a také interní a externí komunikaci.

Kontinuita podnikání

Plán řízení kontinuity podnikání zajišťuje schopnost firmy pokračovat v provozu na předem definované úrovni po incidentu do doby, než je opět možné spustit běžný provoz. Plán minimalizuje dopad výpadku nebo kolapsu firmy.

Firmy mohou také využít profesionálních bezpečnostních služeb. Tyto služby obvykle zahrnují každodenní monitorování a zpravodajství o hrozbách, dále detekci a reakci na incident, což je obzvláště důležité pro:

- forenzní a vyšetřovací činnosti,
- hodnotící a auditové služby,
- řízení krizového týmu,
- komunikaci.

PAMATUJ

Implementované organizační a procesní kontroly by měly být přiměřené pro danou úroveň rizika.