DOXO LOGIC

METODIKA BEZPEČNÁ FIRMA

PRO ZAČÁTEČNÍKY

Čerpejte z našich zkušeností

Zabezpečte svou firmu adekvátně její velikosti a jejím potřebám

Obsah

Úvod do metodiky

Informační technologie jsou součástí každé firmy. Jsou to počítače, mobilní telefony, wi-fi nebo cloudové služby, jako jsou e-mail, kalendář, úložiště dat. Jak firma roste, roste i počet serverů s informačními systémy, požadavky na zálohování, počet zaměstnanců přistupujících k informacím, počet administrátorů, kteří mají přístup k většině, i těch nejcitlivějších, informací.

Organizace spolupracuje s více dodavateli, může mít i několik poboček a její stopa v kybernetickém prostoru se bude stále zvětšovat.

Jak vám bude Metodika Bezpečná firma prospěšná?

Bezpečná firma je návod, který vám pomůže s plánováním investic do zabezpečení dat a zařízení, na která svá data ukládáte.

S růstem vaší firmy se násobí množství dat, které je nezbytné chránit a zároveň roste množství zařízení, uživatelů a dodavatelů, kteří k těmto datům přistupují.

Bezpečná firma je plán rozvoje

Zajistí vám, aby byla vaše firma adekvátně chráněná před:

- **provozními výpadky** (tj. stav, kdy vám nefungují počítače, nejdou služby na internetu nebo máte nedostupná data, když je zrovna potřebujete),
- **ztrátou dat** (a tím i porušením a pracným ručním dohledáváním a opětovným přepisem do počítače, pokud jsou informace dohledatelné),
- **zpřístupněním dat nežádoucím lidem** (kteří by k nim přístup mít neměli).

„Bezpečná firma je způsob, jak se můžete soustředit na své podnikání bez obav z toho, že by vás IT technologie brzdily.“

Jak docílíte Bezpečné firmy?

Pomocí jednotlivých kroků Metodiky Bezpečné firma zajistíte svému podniku plynulé fungování vašeho IT a dalších jeho částí. Přiměřeně velikosti vaší společnosti a vašim potřebám. Od malých a středních podniků až po ty velké.

Provedeme vás jednotlivými kroky, které by měla projít každá firma, která si chce zachovat plynulý provoz. **Firma, která se chce spolehnout na to, že svou práci předává včas a v odpovídající kvalitě.** Taková společnost se kromě zaměstnanců musí spolehnout i na systémy a zařízení, které používá.

Koncept Bezpečné firmy respektuje, kde se jako firma v tuto chvíli nacházíte. Nasměruje vás na to, jak vhodně doplnit vaše stávající technologie, které už reálně využíváte.

Nečekejte, až se něco stane

Prevence je lepší než léčba. Začněte proto chránit své podnikání a své know-how hned.

Jak s metodikou pracovat?

Každá firma je specifická. Ať už velikostí nebo oborem, ve kterém se pohybuje. Proto se vás mohou týkat jen některé části z Metodiky Bezpečná firma a k některým teprve dospějete.

Nejdříve tedy projděte všechny body a pečlivě se věnujte těm, se kterými se shodujete. Každý bod je důležitý a obsahuje minimální kritéria, která byste měli splňovat.

Doporučujeme vám tento postup

- Poté projděte všechny části a jejich sekce „Pro koho je tato úroveň zabezpečení vhodná?“
- Pokud popis v této části odpovídá vašemu stavu, věnujte jí patřičný čas.
- V každém bodu najdete popis toho, čeho se tato oblast týká, proč ji máte chránit a nástroje, díky kterým toho docílíte.
- Na závěr si sepište a naplánujte kroky, které potřebujete ve firmě splnit.

Přejeme vám spoustu AHA momentů na cestě k vaší Bezpečné firmě.

Zjistěte svůj výchozí stav

1) Jak velká jste organizace – viz další body:
Kolik máte zaměstnanců?
Jaký máte roční obrat?
Kolik činil váš zisk za minulý rok?
Myslíte si, že jsou to výsledky, které stojí za to chránit? ANO - NE

2) Umíte si v dnešní době představit fungování vaší organizace bez IT technologií (PC, internet, servery, cloud, ...)? ANO - NE

3) Máte ve firmě stěžejní data, o která si nemůžete dovolit přijít (kontakty, smlouvy apod.)? Nebo u kterých by obnova byla příliš nákladná? ANO - NE

4) Zálohujete tato data? ANO - NE
Pokud ano, kam a jak často data zálohujete?
Jak rychle jsou tyto zálohy obnovitelné?

5) Kolik lidí se stará o vaše IT (interně nebo externě)?

6) Kolik z nich se zabývá přímo kybernetickou bezpečností?

7) Monitorujete bezpečnostní události ve vaší síti? ANO - NE
Vyhodnocujete pravidelně zdroje těchto událostí (logy, varování)? ANO - NE

8) Řešíte bezpečnost informací (analýza rizik, audit IT bezpečnosti atp.)? ANO - NE

9) Která bezpečnostní řešení se vám nepodařilo interně prosadit?

10) Kolik bezpečnostních událostí jste odhadem řešili v minulém roce?

11) Kolik používáte ve vaší organizaci bezpečnostních technologií?
Jaké to jsou?

12) Máte zpracovaný plán rozvoje pro IT na 2-3 roky? ANO - NE
Obsahuje i část pro rozvoj kybernetické bezpečnosti? ANO - NE

Oblasti, které je potřeba chránit

Pokud chcete být Bezpečnou firmou, procházejte postupně těmito kroky (s ohledem na velikost a míru rozvoje vaší firmy).

1) Inteligentní ochrana koncových bodů

Zabezpečení notebooků a mobilních telefonů

Pro koho je tato úroveň zabezpečení vhodná?

- První bod je vhodný pro každou firmu v jakékoliv fázi růstu. Dokonce i pro živnostníky a běžné uživatele.
- Je to základní bod ochrany před kybernetickými útoky.

Proč řešit tuto oblast?

Když firma začíná, pořídí počítače a mobilní telefony, které obsahují veškeré firemní know-how, e-mailovou komunikaci, smlouvy a jejich návrhy nebo podklady pro účetnictví. Prvním krokem je tedy Inteligentní ochrana koncových bodů – Zabezpečení notebooků a mobilních telefonů.

S napadením nebo zablokováním těchto zařízení můžete čelit těmto situacím:

- Ztráta dat
- Pracovní prostoje
- Nedodržení stanovených termínů vaší práce
- Nečekané výdaje na opravu zařízení apod.

Sepište si, kolik počítačů, notebooků, telefonů a tabletů ve firmě používáte:

Počet počítačů: _____

Počet notebooků: _____

Počet mobilních telefonů: _____

Počet tabletů: _____

Používají je vaši zaměstnanci i pro soukromé účely? ANO - NE

Chráníte tato zařízení? ANO - NE

Pokud ano, jak: _____

_____

Jak správně chránit koncové body?

Pouhý antivir už v dnešní době nestačí. Obzvlášť nedostačující je verze zdarma.

Antivir odhalí pouze známé útoky, takže před těmi novými zůstáváte nechráněni. Hackeři jsou navíc vynalézaví a neustále přicházejí s novinkami. Kromě virů existuje malware, ransomware, spyware, adware, phishing a další metody útoků.

Útoky navíc probíhají plošně a nevybírají si, kdo zařízení používá. Hledají jakoukoliv slabinu, kterou mohou zneužít. Ať už technickou nebo v chování uživatele.

Naše doporučení:
používejte ochranný software nebo aplikaci od renomovaných IT bezpečnostních společností.

Pokročilé ochrany blokují online hrozby, jako jsou viry a malware pomocí chytrého strojového učení, sledování chování, analýzy reputace souborů a dalších vícevrtsvých technologií.

Chraňte svá koncová zařízení specializovanou aplikací nebo softwarem.

- Bitdefender
- Trend Micro Apex One
- ReaQta

Tip:

Nezapomeňte na správu uživatelů a nastavení politik.
Je možné, že někteří uživatelé budou potřebovat v nastavení ochrany koncového zařízení výjimky nebo zvláštní pravidla.

Šifrovaná data
Pamatujte na šifrování dat na notebooku. Např. na všech Windows můžete využít standardní šifrování nástrojem BitLocker.

2) Chytré firewally pro firmy a datová centra

Víceúrovňová ochrana proti moderním hrozbám

Pro koho je tato úroveň zabezpečení vhodná?

- Máte ve firmě více počítačů, které se připojují k internetu.
- Chcete bezpečně rozdělit síť.
- Chcete, aby návštěvníci měli svou oddělenou wi-fi, která nebude mít přístup k firemním datům.
- Máte více poboček.
- Vaši zaměstnanci se potřebují vzdáleně připojit do firemních systémů (např. na služebních cestách).

Pro koho není tato úroveň zabezpečení vhodná?

- Pokud máte pouze jeden počítač a dobře jej chráníte.

Proč řešit tuto oblast?

Většina firemních dat se poměrně rychle přesune na cloud nebo na první vlastní server. Vaše IT by v tu chvíli mělo začít **rozlišovat „firemní IT“ a „zbytek světa“**.

Je to ze stejného důvodu, jako si nepřejete, aby vám kdokoliv prohledával kanceláře či sklady, nebo aby v nich třeba přespával. Stejně si určitě nepřejete, aby kdokoliv cizí zneužíval vaše počítače, které máte v kanceláři nebo aby měnil či odposlouchával vaši komunikaci.

Firewally zajišťují omezení přístupu mezi internetem a interní sítí, případně mezi jednotlivými částmi interní sítě. Významným způsobem chrání uživatele od hrozeb a neznámých útoků, které se dokážou vyhnout tradičním bezpečnostním řešením.

Zaměřuje se na eliminaci hrozeb víceúrovňovou Next Generation ochranou.

Jak se chránit pomocí firewallu?

K ochraně vaší firmy nebo organizace slouží Chytré firewally pro firmy a datová centra – víceúrovňová ochrana proti moderním hrozbám. Firewally pak také umožňují bezpečně propojovat jednotlivé firemní pobočky.

Naše doporučení:
používejte firewall společností prověřených testováním NSS Labs.

Firewally jsou první ochranou, hradbou, vašich serverů a počítačů před automatizovanými útoky, nevyžádanou komunikací, externími skeny a snahou propašovat do vaší společnosti malware.

- Next-generation znamená ochranu všech vrstev komunikace
- Check Point Firewall

Tip:

Při segmentaci sítě je vhodné dávat „stejné ke stejnému“, tedy zvlášť uživatele, servery, tiskárny, IP telefony, interní wi-fi, externí wi-fi, DMZ, atp.

Každé pravidlo je vhodné popsat nebo mu alespoň přiřadit číslo interního požadavku na zřízení takového přístupu.

Pravidelná kontrola firewallových pravidel je více než doporučována.

3) Ochrana kritických serverů v interní síti

Enterprise zabezpečení serverů se snadnou implementací a správou

Pro koho je tato úroveň zabezpečení vhodná?

- Pořídili jste si první server nebo servery, protože jste zjistili, že je pro své podnikání potřebujete.
- Chápete, že server je výkonnější počítač obsahující větší množství firemních dat, která nepovažujete za veřejná.
- Chcete své servery chránit lépe než počítače a notebooky.

Pro koho není tato úroveň zabezpečení vhodná?

- Nemáte vlastní serverovou infrastrukturu.

Proč řešit tuto oblast?

Firemní informace ukládáte na serverech. Servery se tak stávající informační studnou, do které stále přesouváte nové informace. Také z ní chcete informace čerpat, když potřebujete, v podobě jaké jste je uložili, aniž by k nim měl přístup kdokoliv nepovolaný.

Z počítačů a mobilních telefonů se již staly zabezpečené prostředky, které slouží k bezpečnému vzdálenému připojení k firemním datům. Jenže tato data na serverech jsou (zatím) nezabezpečená.

Data jsou srdcem vaší firmy – přijdete-li o účetnictví, Finanční úřad vás šetřit nebude. Přijde-li o osobní data zákazníků, přijde Úřad pro ochranu osobních údajů. Ztratíte-li plány či návrhy nebo další vlastní práci, můžete ji dělat znovu. Nebude vám fungovat e-shop, který vás živí a v tu ránu je vaše firma odstřižena od zdroje příjmů. Tomu všemu se dá předejít ochranou kritických serverů v interní síti a v cloudu – Enterprise zabezpečení serverů se snadnou implementací a správou.

Máte vlastní servery? Pokud ano, kolik?

_____

Máte externí servery? Pokud ano, kolik?

_____

Garantuje vám provozovatel externích serverů jejich bezpečnost a dostupnost?

_____

Jak správně chránit kritické servery?

Chránit servery antivirovou ochranou je sice možný, ale nikoliv nutně nejlepší nápad. Obzvláště u kritických serverů se střetávají myšlenky „stále aktualizovat pro co největší bezpečí“ a „dokud to funguje, tak na to nesahejme“. Odpovědí může být tzv. **virtuální patching**.

Patch, neboli záplata je změna v softwaru, jejímž cílem je ho updatovat, opravit nebo vylepšit. Její součástí je oprava chyb a zlepšení použitelnosti, bezpečnosti a výkonu softwaru. Virtuální patching je vrstva pro vynucení bezpečnostní politiky, která chrání před zneužitím známé zranitelnosti a oznamuje pokus o její zneužití.

Naše doporučení:
jistě se najdou ajťáci, kteří brání instalaci bezpečnostních technologií na servery, s poukazem na ztrátu výkonu nebo ohrožení fungování celého serveru, není potřeba se bát. Ochrana serverů je nezbytná.

- Chraňte své servery a mějte přehled o dění na nich, abyste předešli nepříjemnostem.
- Trend Micro Deep Security

Tip:

Důkladně vyšetřujte všechny bezpečnostní události a pravidelně prohlížejte logy. Nastavení ochrany serverů věnujte velkou pozornost, řešení často podporuje specifické ochrany pro jednotlivé operační systémy.

4) Bezpečné aplikace a cloud

Pro koho je tato úroveň zabezpečení vhodná?

- Využíváte cloudových aplikací (Office 365, G-suite, Raynet, atp.).
- Využíváte cloudovou serverovou infrastrukturu (např. Azure, AWS).
- Máte publikované aplikace a servery do internetu.

Pro koho není tato úroveň zabezpečení vhodná?

- Do internetu máte vystavené pouze vzdálené připojení do sítě, ale jinak žádnou službu.
- Vaše webové stránky jsou pouze statické.

Proč řešit tuto oblast?

Cloud zvyšuje efektivitu vašeho podnikání, navíc jej obklopuje aura bezpečnosti a zajištění stále dostupnosti. **Lidé mají často pocit, že cloud se nedá napadnout a že se v něm nemůže nic špatného stát.** Útočníci se snaží napadnout i cloudy. Chraňte firemní data v cloudu a chraňte e-mailová řešení.

Můžete být firma, která preferuje věci nevlastnit, ale pronajímat si je na základě potřeby. Pak je vhodné chránit vaše data, abyste využívali Bezpečný cloud – Zabezpečení aplikací, elektronické pošty a diskových úložišť.

S cloudem přichází několik otázek, které byste si měli zodpovědět:

Bude cloud dostupný vždy, když potřebujeme svá data?

_____

Co je v cloudu zálohováno a kam – co když se data v cloudu „ztratí“?

_____

Můžete data v cloudu zálohovat na svou infrastrukturu?

_____

Šifrujete svá data, která do cloudu nahráváte?

_____

Jak je cloud chráněn před útoky zvenčí nebo proti jejich šíření uvnitř cloudu?

_____

Jak správně chránit svá data v cloudu?

Chraňte své virtuální servery v cloudu jako by stály u vás v serverovně.
Pro cloudové aplikace, kde je to možné, využívejte nadstavbové bezpečnostní opatření. Před webovými formuláři a aplikacemi je vhodné mít webový aplikační firewall (WAF).

Naše doporučení:
nastavte si pro každou příležitost trochu jinou ochranu.

- Chraňte své cloudové servery technologií Trend Micro Deep Security
- Využívejte pro své aplikace web aplikační firewall Incapsula od společnosti Imperva
- Pro ochranu Office 365 a Google světa je zde Trend Micro Smart Protection

Tip:

Vícefaktorová autentizace.
Velké množství útoků na cloud je vedena přes ukradená hesla zaměstnanců. Hackeři dnes objevují techniky na získání i druhého ochranného faktoru (např. generovaného kódu zaslaného na mobil), přesto je dvoufaktorové ověřování bezpečnostním opatřením se skvělým poměrem cena/výkon.

5) Informační bezpečnost

Nástroje a procesy pro naplnění požadavků na plynulý a zabezpečený chod firmy

Pro koho je tato úroveň zabezpečení vhodná?

- Chcete své IT začít skutečně řídit vlastními požadavky.
- Chcete mít jasně definované procesy jak má IT fungovat.
- Chcete dát do pořádku zákonné požadavky.
- Chcete řídit rizika.

Pro koho není tato úroveň zabezpečení vhodná?

- Pro každého, kdo vydává své pokyny pouze formálně, aniž by kdy kontroloval jejich dodržování.

Proč řešit tuto oblast?

Informační bezpečnost je v prostředí firem klíčovou záležitostí strategického významu. Vypracujte a nastavte si strategii informační bezpečnosti a nebojte se pojmů jako business impact analýza, analýza rizik, bezpečnostní směrnice a standardy nebo informační bezpečnostní politika.

Jste-li chráněni pomocí technologií, je to skvělý první krok, který vaší firmě umožňuje nerušeně růst. A to beze strachu z běžných automatizovaných útoků, které se šíří přes internet.

Váš management a všichni zaměstnanci se mohou vzdáleně připojit kdykoliv a odkudkoliv k firemním datům, aniž by je vystavovali ohrožení ze ztráty dostupnosti, důvěrnosti nebo integrity. Může se zdát, že firma je zabezpečená a má vystaráno. Opak je pravdou, nastal nejvyšší čas, aby se o bezpečnost začal zajímat i management firmy.

Z bezpečnosti – nákladové položky se stává bezpečnost – součást firemní kultury.

Management začíná řídit bezpečnost informací. Požadavek **„chci, aby IT nějak fungovalo“ se mění na „chci, aby IT fungovalo jako servisní organizace, která plní požadavky“**. Tyto požadavky pak nejsou rozmary managementu firmy, ale generují je jednotlivá vaše oddělení.

Obchodní oddělení chce, abyste zákazníkům služby dodávali v požadované kvalitě a včas. Finanční nebo účetní oddělení požaduje, abyste v termínu vypláceli mzdy a platili faktury. Výkonný ředitel bude trvat na dodržování smluvních a legislativních požadavků.

Informační bezpečnost to jsou nástroje a procesy pro naplnění požadavků na plynulý a zabezpečený chod firmy.

Jak správně dělat informační bezpečnost?

Postupně, s rozvahou a velkou měrou zapojení zaměstnanců do tohoto procesu. Zaměstnancům je potřeba vše trpělivě vysvětlit. **Vedení by pak v dodržování předpisů mělo jít příkladem.**

První kroky nemusí být nákladné. Sepište si:

1. Informační systémy, které používáte.
2. Ke každému připište, kdy by měl být dostupný.
3. Jak dlouho mohou být v případě výpadku nedostupné (jak rychle mají být opravené).
4. O kolik práce můžete přijít – tzn. nevadí vám, když se do systémů bude muset zadat znovu.

Tyto požadavky předložte vašemu IT oddělení a zeptejte se, jestli jsou splnitelné a za jakých podmínek.

Naše doporučení:
přestože normy jsou dostupné pro každého, raději si pozvěte bezpečnostního konzultanta. Přeci jen zkušenost je v této oblasti často k nezaplacení. Vyhnete se prošlapávání slepých uliček a získáte životaschopné dokumenty, které vám práci usnadní, místo toho, aby vám ji přidělávaly.

- Chraňte své cloudové servery technologií Trend Micro Deep Security
- Využívejte pro své aplikace web aplikační firewall Incapsula od společnosti Imperva
- Pro ochranu Office 365 a Google světa je zde Trend Micro Smart Protection

Tip:

Security Assessment za využití metodiky Bezpečná firma vám pomůže rychle zhodnotit aktuální stav vaší kybernetické bezpečnosti.

Nakreslí startovací čáru, tzn. ukáže vám stav, kde se v IT bezpečnosti nacházíte a kde by společnost vašeho typu měla být.

6) Visibilita a logování v síti

Ochrana před kybernetickými útoky zvenku i zevnitř

Pro koho je tato úroveň zabezpečení vhodná?

- Chcete začít sledovat a vyhodnocovat dění ve vašich sítích a aplikacích.
- Jste ochotní na tuto činnost vyhradit čas svého zaměstnance (nebo pořídit externí službu).

Pro koho není tato úroveň zabezpečení vhodná?

- Pokud kontrolu logů a vyšetřování považujete za činnost, která nepotřebuje svůj čas.

Proč řešit tuto oblast?

IT oddělení ve své práci postupuje metodicky, i v případě, že máte informační aktiva chráněna. **Pro svou práci potřebuje vědět, co se kde v počítačové síti a v informačních systémech děje a kdo co udělal.**

Visibilita a logování – **Ochrana před kybernetickými útoky zvenku i zevnitř vám dodá všechny potřebné informace o pokusech o kybernetický útok**, všechny relevantní informace pro vyšetření bezpečnostních událostí (tj. podezření na narušení bezpečnosti informací – jejich dostupnosti, důvěrnosti nebo integrity). Také vám umožní získat důkazy o činnosti zaměstnanců a administrátorů, kdybyste museli bránit svá práva.

Jak správně zavádět visibilitu a logování v síti?

- Začněte se síťovými událostmi, které budete schraňovat na jednom místě, např. v log managementu.
- Zaveďte postupy pro pravidelnou kontrolu těchto logů a vyhledávání bezpečnostních událostí v nich.
- Ať už automatizovaným způsobem pomocí nástroje SIEM nebo ručně.
- Postupně přidávejte další zdroje a pište si scénáře útoků, které v nich hledáte.

Naše doporučení:
zaveďte si vlastní log management – oddělený server nebo úložiště pro sběr logů ze všech klíčových zdrojů. Pokud budete logy schraňovat mimo aplikace a servery, zabráníte útočníkovi, aby je v případě úspěšného útoku po sobě smazal.

Tip:

- Nasaďte ve vaší síti Intrusion Detection Sondu, jako například Deep Discovery od Trend Micro, nebo alespoň Open-Source Suricatu. Na tuto sondu budete posílat kopii provozu ve vaší síti (pomocí mirror portu na switchi) a ona se postará o bezpečnostní analýzu datových toků. Dozvíte se o tom, co u vás létá po síti.

- Sledujte také co se děje na klíčových serverech, jaké na nich byly instalovány aplikace, vytvářeny nové soubory nebo kdo se na ně hlásil. Pomoci vám může třeba i Open-Source Wazuh nebo OSSEC. Existuje ale i řada pokročilých komerčních nástrojů, které mají výhodu v pokročilejší automatické detekci bezpečnostních problémů, hledání anomálií a korelaci dat.

- Sledujte, co se ve vaši síti děje pomocí služby Security Insight.

7) Ochrana privilegovaných účtů

Řízená ochrana externích administrátorů

Pro koho je tato úroveň zabezpečení vhodná?

- Přistupuje do vašeho IT velké množství externistů?
- Máte obavu z chybné správy vašeho klíčového serveru?

Pro koho není tato úroveň zabezpečení vhodná?

- Pokud máte vlastní IT oddělení do tří pracovníků.

Proč řešit tuto oblast?

Zaměstnanci, dodavatelé a další osoby mají často zbytečný administrátorský přístup k systémům a datům.

Hesla jsou vytvářena a sdílena, aktivita externích administrátorů není kontrolována ani auditována. **Ochranou privilegovaných účtů získáte přehled a kontrolu nad všemi privilegovanými uživateli s přístupem na kritické systémy.**

Když už je řeč o administrátorech – to jsou lidé, kteří z podstaty práce „musí vidět vše a musí mít přístup ke všemu“, jak s oblibou tvrdí. Důvěřovat administrátorům (především externím, když si najmete společnost na správu IT), že jsou poctiví a dělají pouze věci, které dělat mají je nezbytné.

Přesto je možné tyto privilegované účty chránit – řídit ochranu (externích) administrátorů před nařčením, že dělají věci, které jsou v rozporu se zadáním nebo obyčejnou lidskou slušností.

Jak správně chránit privilegované účty?

Pro správu privilegovaných účtů existují softwarové nástroje, které umí monitorovat a kontrolovat aktivitu prováděnou pomocí privilegovaných účtů.

V případě správců sítě se jedná o informace, kdy a jak se přihlašují k privilegovaným účtům nebo jaké aktivity pomocí těchto účtů prováděli.

Takový monitoring by neměl být chápán jako nedůvěra ze strany správců sítě (hlavně pokud se jedná o externí firmu), ale jako nedílná součást monitoringu změn a aktivit na firemní IT infrastruktuře.

Mimo to může být tento monitoring nástrojem pro interní vzdělávání správců sítě v případě ukládání záznamů o aktivitách prováděných pomocí privilegovaných účtů.

Naše doporučení:
monitorujte práci externích administrátorů, abyste měli přehled o jejich činnosti a dokázali jste zpětně rekonstruovat provedené kroky. Nejde ani tak o kontrolu, jako spíš o možnost učit se z chyb, které nastaly, usnadnit si řešení problémů mezi stavy „fungovalo to“ a „už to nefunguje“.

Tip:

- Privileged Access Management Platform (PAM) od společnosti BeyondTrust
- Privileged Account Security od společnosti CyberArk

8) Bezpečnostní centra

Ochrana firmy 24x7, 365 dní v roce

Pro koho je tato úroveň zabezpečení vhodná?

- Pro všechny bez ohledu na velikost, každý má data, která musí chránit.

Pro koho není tato úroveň zabezpečení vhodná?

- Živnostník bez zaměstnanců s jedním počítačem.

Proč řešit tuto oblast?

Sledujte, co se děje ve vaší síti a předcházejte škodám. S aktivním bezpečnostním centrem včas zareagujete na objevené bezpečnostní hrozby.

Stejně jako firmy chrání svůj majetek připojením na pult centrální ochrany (PCO), tak i vaše firemní IT můžete napojit na AI bezpečnostního centra, která vám poskytnou ochranu 24 hodin denně, 7 dní v týdnu, 365 dní v roce.

Budete mít jistotu, že jste stále hlídáni a jakýkoliv náznak problémů bude řešený s odbornou péčí.

Bezpečnostní událost bude prošetřena, vyhodnocena a pokud se bude jednat o bezpečnostní incident, bude zjištěna jeho příčina, průběh a navrženo bezpečnostní opatření, aby bylo zabráněno opakování takového bezpečnostního incidentu.

Jak správně provozovat bezpečnostní centra?

Centrum IT bezpečnostního monitoringu stojí na třech hlavních pilířích:

- technologiích,
- expertech na kybernetickou bezpečnost,
- dokumentovaných procesech.

Centrum bezpečnostního monitoringu je místo, kde specialisté z praxe sledují, vyhodnocují a chrání informační systémy zákazníků, které jsou do centra připojeny.

Spojuje lidi, procesy a technologie s cílem zajištění okamžitého odhalení bezpečnostních incidentů prostřednictvím detekce, kontroly a odstranění IT hrozeb.

Naše doporučení:
sledujte, co se ve vaši síti děje pomocí služby Security Insight.
Díky tomu odhalíte kybernetický útok včas.

- Zavedení bezpečnostního dohledu do vaší společnosti, 24/7.
- Reporting a alerting od lidí, nikoliv od robotů či strojů, které musíte kontrolovat.

Tip:

Pro vytvoření účinně fungujícího Centra bezpečnostního monitoringu nestačí, aby přidružené procesy, lidé a technologie existovali. Musí být na pokročilé úrovni.

Kvalitně fungující Centrum bezpečnostního monitoringu je páteří nejúčinnější detekce a prevence hrozeb a slabých míst. Umožní vám, aby procesy informační bezpečnosti reagovaly rychleji, více spolupracovaly a účinněji sdílely poznatky.

To ve výsledku posune vaši IT bezpečnost vysoko nad průměr. Pro útočníky už nebude tak snadné napadnout vás.

9) Školení zaměstnanců a trénink specialistů bezpečnosti

Pro koho je tato úroveň zabezpečení vhodná?

- Školení základů kybernetické bezpečnosti je vhodné pro každou firmu v jakékoliv fázi růstu. Dokonce i pro živnostníky a běžné uživatele.
- Pro firmu, která chce předcházet chybám svých zaměstnanců, které by ji mohly ohrozit.
- Specializovaná odborná školení vyžije firma, která má své vlastní oddělení, která v něm chce mít specialistu na IT bezpečnost.

Pro koho není tato úroveň zabezpečení vhodná?

- Pro firmy, které nevěří ve svůj lidský kapitál a nechtějí do něj investovat.

Proč řešit tuto oblast?

V jakýkoliv okamžik je vhodné pravidelně školit zaměstnance, pracovníky IT a management v oblasti kybernetické bezpečnosti.

Naneštěstí jsou to právě zaměstnanci, kteří mohou svým chováním výrazně usnadnit získání kontroly nad firemními počítači nebo firemními daty.

Tato školení nejsou jednorázová. Je nezbytné, aby se pravidelně opakovala, alespoň jednou za rok.

Školením snížíte riziko

95 % všech kybernetických útoků zneužívá zaměstnance. Útočník ho vypočítavým způsobem přiměje udělat to, co útočník chce, aby udělal. Hacker se tak dostane do firemní sítě jako pozvaný a vážený host. Pak si tam samozřejmě může dělat, co se mu zlíbí.

- **Školte své zaměstnance**, aby dokázali včas nahlásit podezřelé osoby, e-maily nebo činnosti ve společnosti. Tím zachytíte problémy v době jejich vzniku a dokážete jim efektivně předcházet, než když pouze odstraňujete důsledky.
- **Školte své administrátory** – člověk se dokáže bránit jen takovým útokům, které si dovede představit nebo o kterých někdy v životě slyšel.

Naše doporučení:
nabídněte svým zaměstnancům školení jako bonus, který zvýší bezpečnost jejich domácích počítačů a domácností. Pokud získají bezpečnostní návyky pro ochranu domácích zařízení, lépe si je zapamatují, budou nad nimi přemýšlet a budou je používat také ve vaší firmě.

Za vše mluví reference po našem školení Základů kybernetické bezpečnosti:

Chtěl jsem vám jménem celé naší organizace poděkovat za boží seminář. Váš školitel je opravdu profík s obrovským přehledem. Bezpečně, srozumitelně, zábavně a s respektem nás provedl i těmi nejtemnějšími zákoutími internetu. Dokázal i na papírově nutná témata naroubovat takové perly a zajímavosti, že jsme tady neměli absolutně nikoho, koho by seminář od začátku do konce nebavil. Takže moc děkujeme!

Vyškolte i vy své zaměstnance a zvyšte skokově svou kybernetickou ochranu.
Více informací o školení najdete zde >>>

Tip:

Zdůrazněte svým zaměstnancům důležitost silných hesel. Ideální jsou hesla dlouhá a náhodná, se speciálními znaky.

Naučte je používat správce hesel – uložíte si v něm všechna hesla, která chráníte jedním silným heslem a frází. Např. Passpack.com

10) Pravidelné testování bezpečnosti systémů a aplikací

Externí a interní penetrační testy

Pro koho je tato úroveň zabezpečení vhodná?

- Pro všechny, kteří chtějí zjistit výchozí stav zabezpečení firmy nebo organizace.
- Pro ty, kteří zavádějí nové systémy, aplikace, weby, atd. a chtějí je mít dobře zabezpečené.

Pro koho není tato úroveň zabezpečení vhodná?

- Pro malou firmu (nebo živnostníka), která nemá ani webové stránky.

Proč řešit tuto oblast?

Znát své nedostatky je vždy prvním krokem k jejich nápravě.

Může se stát, že si management neumí představit, jak kybernetický útok nebo hrozba vypadá. Jak se vloupá zloděj do domu je každému jasné. Jak se vloupá hacker do firmy, to je pro někoho magie.

Abyste věděli, které oblasti kybernetické bezpečnosti zvládá vaše IT oddělení dobře a **kde má rezervy a prostor pro zlepšení, je potřeba pravidelně získávat zpětnou vazbu**. Nejlépe formou pravidelného testování bezpečnosti systémů a aplikací – skenování zranitelností.

Penetrační testy slouží k ověření úrovně bezpečnosti simulací hackerského útoku. Úkolem etických hackerů je objevit slabá místa v zabezpečení organizace, zaútočit na ně a získat kompletní přístupy.

Díky penetračním testům jsou odhaleny zranitelnosti, které je možné v praxi zneužít k útoku. Na základě testů může investovat do IT bezpečnosti efektivně - tam, kde je to nejvíce potřeba.

Rozlišujeme externí a interní penetrační testy

U externích testů etický hacker atakuje systémy z internetu, přičemž většinou nemá předběžné znalosti o IT infrastruktuře a nemá přístupové údaje k IT službám publikovaným z interního prostředí do Internetu. Tester vyhledává zranitelnosti, které se dají zneužít k napadení systémů publikovaných do internetu či v horším případě k získání přístupu do samotné interní sítě organizace.

Interní penetrační testy jsou prováděny z prostředí sítě organizace.
Jsou zaměřeny na testování používané infrastruktury (interní servery, koncové stanice uživatelů, či switche), ale také na zabezpečení bezdrátové sítě bez a se znalostí hesla.

Jejich součástí je i pokročilá detekce na odhalení známých či neznámých hrozeb, které se již mohou vyskytovat ve firemní síti (pokročilý malware, ransomware, apod.).

Jak správně provádět penetrační testování?

Penetrační testování by měl **provádět specialista či proškolený zaměstnanec**, který absolvoval školení týkající se penetračního testování či etického hackingu.

Testování svépomocí bez předchozích znalostí či zkušeností může způsobit omezení chodu či zhroucení interních IT služeb organizace, které je nežádoucí. Odstraňování škody může navíc být jak časově, tak i finančně náročné.

Pro penetrační testování lze využít komerčních softwarových či hardwarových nástrojů, ale také tzv. open-source softwarových nástrojů.

Testování provádějte pouze na systémech, které vám buďto patří (interní systémy ve vaší organizaci), nebo pokud k tomu dostanete výslovný souhlas (například pokud jsou vaše webové stránky hostované u externí firmy).

Naše doporučení:

- vyškolení vlastního „penetračního testera“ z jednoho či více interních zaměstnanců IT oddělení. Vybraní zaměstnanci by měli projít alespoň základním školením na téma penetrační testování či etický hacking,
- provádějte pravidelně penetrační testy externím dodavatelem.

Naplánuje si své další kroky

Stanovte si cíl, kam chcete svou bezpečnost posunout. Sepište si kroky, kterými po přečtení metodiky začnete realizovat vaši Bezpečnou firmu. Rozpracujte i jednotlivé činnosti, které bude potřeba provést.

Tip:

Doporučujeme vám napsat si ke každému kroku datum, do kdy jednotlivé aktivity splníte a také zodpovědného pracovníka, který je bude mít na starosti.

Závěr

Kybernetická bezpečnost je jako živý organismus, ať se nám to líbí, nebo ne. Proto nedoporučujeme pouze jednorázově nakoupit technologie, nastavit je a myslet si, že jste v bezpečí napořád. Nebo opačný případ - pořídíte vysoce sofistikované řešení, ale nezabýváte se upozorněním a hlášeními, které vám poskytuje.

Pamatujte, že zabezpečení má být přiměřené, ale zároveň se musí stále rozvíjet, protože i vaše firma se neustále mění a rozvíjí. Stejně tak se vyvíjí i možnosti hackerských útoků a k nim adekvátní bezpečnostní opatření.

Proto neusínejte na vavřínech a udržujte povědomí o dění v kybernetické bezpečnosti. Sledujte média a odborné články nebo blogy bezpečnostních firem. Případně si domluvte schůzku a stav vaší kybernetické bezpečnosti pravidelně konzultujte.