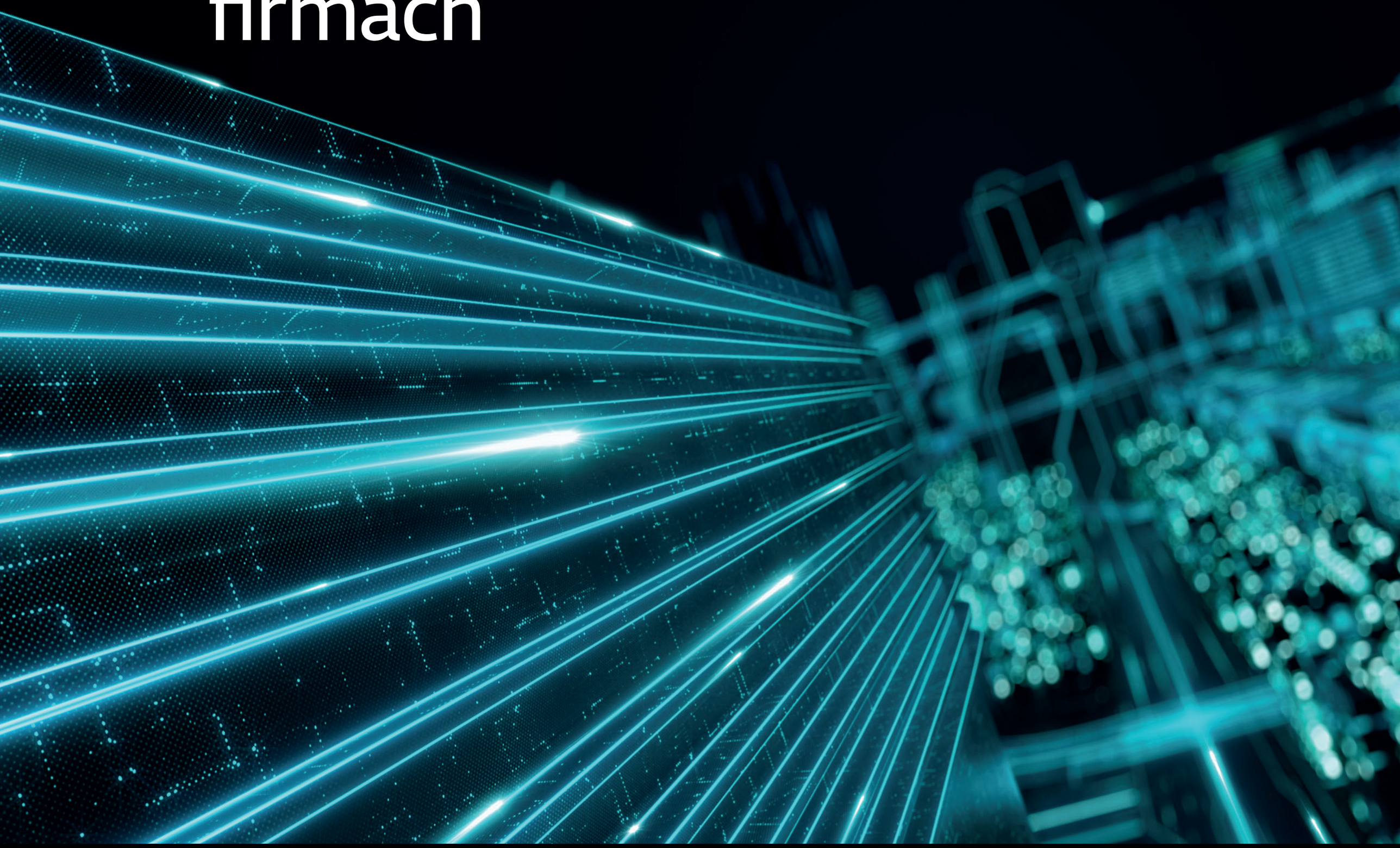
ENJOY SAFER TECHNOLOGY™

# OCHRANA DAT

## v malých a středně velkých firmách



kapitola 4

# Technologie pro ochranu dat

**V TÉTO KAPITOLE**

- Technologie pro ochranu dat
- Zabezpečení sítě

Kapitola 4

# TECHNOLOGIE PRO OCHRANU DAT

*V této kapitole se dočtete o různých možnostech zabezpečení a technologiích, která slouží k ochraně citlivých dat.*

## Ochrana dat je nutná

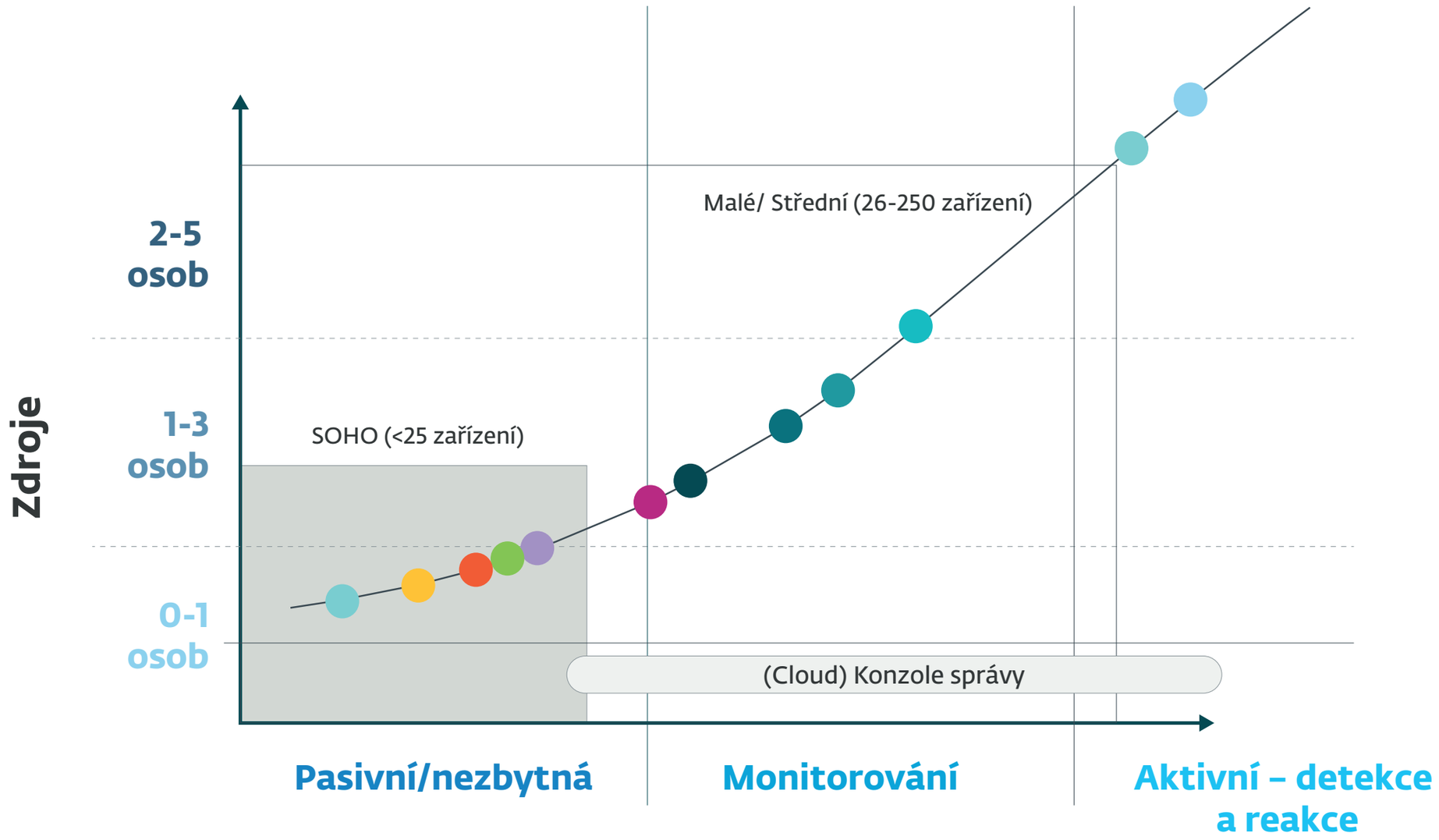
Data jsou kritickým aktivem, které může pro vaši firmu představovat vysoké riziko. Tomu odpovídá i velké množství bezpečnostních technologií, které lze použít k ochraně firemní IT infrastruktury (počítače, mobilní zařízení, servery, datová centra atd.) Obrázek níže zobrazuje různé bezpečnostní technologie, které je vhodné implementovat v závislosti na vaší úrovni rizika a dostupných zdrojích.

### Antivirus

Klasická antivirová ochrana v podobě, jak ji známe, je naprostým minimem, které byste měli instalovat na koncová zařízení. Dnešní moderní hrozby obvykle kombinují několik vektorů útoku, které obyčejný antivirus obvykle nepokryje. Proto většina firem rovnou implementuje internetovou ochranu.

### Internetová ochrana

Moderní bezpečnostní řešení kromě klasické antivirové ochrany obsahují i další technologie ochrany proti škodlivému kódu (včetně ransomwaru, malwaru zaměřeného na zranitelnosti v softwaru, detekci síťových útoků, botnet malwaru a mnohých dalších). Z pohledu zabezpečení koncových zařízení jde obvykle o nejlepší volbu cena/ výkon.




## Bezpečnostní technologie

- **Antivirus**
- **Internetová ochrana**
- **Vícefaktorová ochrana**
- **Firewall**
- **Šifrování**
- **Záloha a obnova**
- **Mobile Device Management (MGM)**
- **NAC (kontrola přístupu k síti)**
- **SIEM**
- **Správa aktualizací a záplat**
- **DLP**
- **EDR/EDTR**

## Úroveň kybernetické ochrany

- **Pasivní/nezbytná** – Automatické akce, ad-hoc reakce na identifikovaná rizika
- **Monitorování** – Automatické akce, aktivní monitorování současného stavu s reakcemi na upozornění o útocích nebo potenciálních rizicích
- **Aktivní** – detekce a reakce - Interní analýza údajů a monitorování stavu za účelem odhalení cílených útoků, reakce na základě bezpečnostních politik pro definované události v síti.

## Resources

- Formální tým – Specialista na plný úvazek **2-5 osob**
- Dedikovaný – Specialista na částečný úvazek **1-3 osoby**
- Podle potřeby – „nainstalovat a zapomenout“ **0-1 osoba**

**Obrázek 4-1:** Bezpečnostní technologie

## Vícefaktorová autentizace

Vylepšuje zabezpečení ověření přístupu k datům přidáním dalšího faktoru do procesu přihlášení. Obvykle jde o jednorázový kód, který se generuje v přidružené aplikaci, je zaslán na předem definovanou e-mailovou adresu, nebo prostřednictvím SMS na chytrý telefon. Kód lze použít pouze pro ověření jedné uživatelské relace s omezeným časovým rámcem (např. 60 sekund), což řeší situace, kdy se útočník snaží použít ukradený kód několikrát za sebou. Nejnovější forma autentizace (podporované i naším produktem ESET Secure Authentication) umožňuje uživateli jednoduše potvrdit ověření prostřednictvím spárovaného chytrého telefonu, takže nemusí kód opisovat.

### Firewall

Firewall stále zůstává základním stavebním prvkem bezpečné sítě a představuje nejdůležitější investicí, kterou firma může učinit pro bezpečnost sítě. Základní firewall obvykle poskytuje filtrování paketů a kontrolu stavu síťového provozu. Na trhu najdete i takzvané firewally příští generace (Next Generation Firewall - NGF), které nabízí navíc funkce pokročilého síťového zabezpečení včetně antimalwarové ochrany, filtrování obsahu, odhalování průniku (intrusion detection) nebo informace o hrozbách.

### Šifrování

Šifrování je další metodou, která posílí zabezpečení citlivých dat. Zašifrovaná data jsou bez znalosti šifrovacího klíče nečitelná, proto i při případném úniku dat jsou útočníkovi bez příslušného klíče k ničemu. Šifrování a dešifrování může být prováděno buď hardwarově (rychlejší) nebo softwarově (méně nákladné). Řešení na trhu mají různé funkce, ale téměř nikdy nechybí možnost šifrování celého disku, jednotlivých složek, souborů a také obsahu e-mailů, což umožňuje bezpečnou spolupráci napříč různými pracovními skupinami i mimo firemní síť. Šifrování citlivých dat je mimochodem jednou z doporučených metod pro ochranu citlivých dat v rámci nařízení GDPR.

### Zálohova a obnova

Systémy pro zálohu a obnovu obsahují software a zálohová média, jako je páska nebo fyzické disky. Zálohy byste měli pravidelně testovat, ať máte jistotu, že je lze kdykoli v případě potřeby obnovit. Zároveň budete mít jistotu, že se zálohují všechna kriticky důležitá data pro případ, že by například došlo k úspěšnému ransomwarovému útoku. Nejen že nebudete muset platit výpalné útočníkům, ale také se relativně rychle vrátíte do stavu před útokem.

### Správa mobilních zařízení (MDM)

Firmy stále častěji povolují pro účely práce zaměstnancům používat svá osobní mobilní zařízení (Bring Your Own Device - BYOD). S tím je samozřejmě spojeno potenciální bezpečnostní riziko v případě ztráty nebo odcizení zařízení, kdy může rovnou dojít k úniku citlivých dat nebo neautorizovanému přístupu do sítě. S pomocí správy mobilních zařízení můžete obvykle zařízení nejen nadefinovat politiky pro bezpečné používání (např. požadavek na délku hesla), ale v případě potřeby vzdáleně zamknout, vymazat, nebo lokalizovat polohu.

### Prevence ztráty údajů (DLP)

DLP systémy chrání firmy proti náhodnému (nebo úmyslnému) úniku citlivých dat, jako jsou čísla sociálního zabezpečení, zdravotní informace, finanční údaje a podobně.

**UPOZORNĚNÍ**

*DLP monitoruje chování uživatelů (a procesy), jakým způsobem pracují s citlivými daty, umožňuje monitorovat nebo rovnou blokovat nežádoucí komunikace a připojená zařízení. Zjištěné bezpečnostní incidenty reportuje do vzdálené správy nebo nástrojů SIEM.*

# VÝBĚR BEZPEČNOSTNÍHO ŘEŠENÍ

Bezpečnostní řešení na počítačích, mobilním zařízení a serverech představuje první obrannou linii proti kyberútokům. Moderní bezpečnostní řešení obsahují sofistikované technologie ochrany, jako je strojové učení, detekce malwaru před spuštěním, sandbox, a mnohé další. A není pravda, že tradiční výrobci bezpečnostních řešení už nemají co nabídnout. O takzvaných „nextgen“ produktech, které jsou dnes na trhu, se často mluví jako o revolučních. Přitom aby mohly být produkt označen jako “nextgen”, obvykle stačí (z technického hlediska) implementovat jediný aspekt ochrany pro koncová zařízení, jako je například strojové učení. Při výběru bezpečnostního řešení proto hledejte řešení, které obsahuje minimálně následující technologie: strojové učení, detekci malwaru v celém jeho cyklu (před, během i po spuštění), sandbox, a časem prověřenou a stále velmi efektivní detekci škodlivého kódu založenou na signaturách, která je v reálném čase aktualizovaná na základě analýzy škodlivého kódu v cloudu.

Co nesmí chybět:

**Nízké systémové nároky**
Bezpečnostní řešení, které vyžaduje velké místo na disku, paměťové zdroje a zbytečně vytěžuje procesor, může způsobit problémy s výkonem stanic, zpomalování celého počítače a podobně.

**Pravidelné a časté aktualizace**
Bezpečnostní software musí být schopen v reálném čase získat aktuální informace o hrozbách i v případech, že je lokální aktualizační server nedostupný.  Stále větší význam při distribuci aktualizací virových databází a informací o hrozbách hraje cloud.

**Odolnost**
Produkt musí být efektivní i v případě odpojení od sítě a musí být odolný proti malwaru, který konkrétně cílí na používané bezpečnostní řešení.

**Produktová stabilita**
Produkty uvedené na trh musí mít doložitelný záznam o tom, že jsou bezpečné, stabilní a neobsahují chyby.

**Centrální vzdálená správa**
Mimo samotnou instalaci bezpečnostního řešení, musí produkt umožnit správci ověřit, že software je správně nainstalován, řádně funguje a je pravidelně aktualizován. Správce musí mít zároveň přehled o stavu zabezpečení na všech firemních zařízeních a mít možnost rychle reagovat v případě bezpečnostního incidentu a to vzdáleně odkudkoli.

# Zabezpečení sítě

Zabezpečení firemní sítě je v posledních letech stále větší výzvou i díky rostoucímu počtu mobilních zařízení mezi zaměstnanci a vzestupu popularity cloudových služeb. Některé příklady technologií pro ochranu údajů:

## Systémy odhalování průniku a prevence (IDS a IPS):

IDS a IPS vyhledávají škodlivý síťový provoz založený na přednastavených signaturách a pravidlech. IDS je pasivní systém, který pouze upozorňuje IT tým na možný neoprávněný průnik. IPS je aktivní systém, který vykonává konkrétní činnosti jako je přerušení nebo blokace škodlivé komunikace.

## Software jako služba (SaaS)

SaaS aplikace jsou mezi uživateli velmi populární, jelikož jde o snadný způsob, jak zefektivnit každodenních pracovní aktivity. Příkladem jsou například Dropbox, Google dokumenty, nebo OneDrive. Firmy musí mít přehled, jaké SaaS aplikace uživatelé používají, zajistit jejich bezpečné používání, případně jejich používání kontrolovat nebo rovnou blokovat.

## VLAN segmentace

Segmentace lokální virtuální sítě (Virtual Local Area Network - VLAN) rozděluje síť na logické celky (jako je finanční, personální nebo obchodní oddělení), za účelem prevence nepovoleného přístupu k určitým údajům a nadměrného síťového provozu (přetížení sítě), které mohou systém zpomalovat.

## Virtuální privátní síť (VPN)

VPNka umožňuje uživatelům připojit se vzdáleně k firemní síti přes internet pomocí zašifrované komunikace. VPN může být také využita k propojení partnerské sítě a/nebo sítě poskytovatele, jako je prodejce ve vašem dodavatelském řetězci nebo poskytovatel cloudových služeb.

## Řízení přístupu na síť (NAC)

Systémy řízení přístupu k síti, umožňují vynucení bezpečnostní politiky pro koncové pracovní stanice. Ta se připojí do sítě pouze v případě, že je v souladu s definovanými zásadami (poslední aktualizace operačního systému a/nebo bezpečnostního řešení a podobně).

## Řízení bezpečnosti informací a událostí (SIEM)

Nástroje SIEM slučují a analyzují do jednoho místa informace z mnoha datových zdrojů, jako jsou firewally, IDP/IPS, WAF, servery a koncová zařízení. Pro administrátora je potom mnohem jednodušší zavádět preventivní opatření nebo reagovat na bezpeč-nostní incidenty.

## Správa aktualizací

Pravidelná instalace opravných balíčků a aktualizací používaného softwaru je zásadním předpokladem prevence proti hrozbám. Jak velikost vaší společnosti roste, manuální

instalace softwarových záplat na stovkách serverů a koncových zařízení, často na různých pracovištích, je velmi problematická. Instalace řešení pro správu aktualizací a záplat pomáhá společnostem automatizovat procesy, na které by jinak musel administrátor neustále myslet a manuálně provádět.

### Správce hesel

Slabé přístupové heslo může být vstupní branou pro neautorizovaný přístup do interní sítě. Používání správce hesel eliminuje slabá hesla napříč celou společnostní a uživateli stačí si pamatovat pouze jedno „master“ heslo.

### Ochrana systému doménových jmen (DNS)

Služba DNS, pokud není nijak chráněna, umožňuje potenciálnímu útočníkovi celou řadu možností, jak škodit. Proto je užitečné implementovat asymetrickou kryptografii (jeden klíč na šifrování, jiný klíč na dešifrování) v podobě DNSSEC, díky které budete mít jistou, že uživatel získá z DNS správné a důvěryhodné údaje.

### Filtrování obsahu webu

Filtrování obsahu brání uživatelům navštěvovat nepovolené, potenciálně škodlivé nebo škodlivé webové stránky na základě webové adresy (IP nebo URL) nebo konkrétním obsahu.

## Proč automatizovat?

Potřeba automatizovat a koordinovat IT procesy je důležitá zejména v případech, kdy máte málo IT zaměstnanců a omezené zdroje. Ruční instalace a konfigurace koncových zařízení je v rostoucí firmě dlouhodobě neudržitelná. Pokud má firma zároveň i více poboček, jde víceméně o nutnost.

Vedle časové neefektivity spojené s manuální obsluhou každého koncového zařízení je zde možnost vzniku chyb, které v konečném důsledku vedou například k nekonzistentnímu nebo špatně nakonfigurovanému nastavení stanic.

Nástroje pro automatizaci zlepšují efektivitu IT týmu, zvyšují produktivitu pro koncové uživatele (snižováním nečinnosti), a snižují potenciálně náklady s odstraňováním chyb.

**TIPY**

*Pro malé a střední firmy, které postrádají zdroje (ať již lidské nebo finanční), může být řešením pořízení cloudového nebo MSP řešení třetí strany.*