McAfee
Together is power.

GDPR a bezpečnostní produkty pro ochranu dat

Jan Strnad, Sales Engineer, McAfee

GDPR – General Data Protection Regulation

Co je GDPR:

- Nařízení schválené Evropským parlamentem 14.4.2016 po 4 letém vyjednávání
- Nahrazuje Směrnici 95/46 EC s **účinností od 25.5.2018** a v ČR zákon č. 101/2000 Sb. na ochranu osobních údajů
- Nejkomplexnější soubor pravidel na ochranu osobních údajů na světě
- Výrazně povyšuje ochranu dat na úroveň evropského zákona a posiluje právo osob na lepší kontrolu nad jejich osobními údaji
- Představuje rovnováhu mezi legitimními zájmi správců a zpracovatelů dat s právem osob na soukromí
- Jedná se o **nařízení**, dokument přijatý na úrovni EU, není potřeba národní implementace a je **platné pro všechny**
- **Správní pokuta** za nedodržování **20 mil. Euro** nebo 4% z celkového obratu společnosti

GDPR – General Data Protection Regulation

Jakých údajů se GDPR nařízení týká:

- **Osobní údaje a citlivé osobní údaje** – veškeré informace vztahující se k identifikované nebo indentifikovatelné fyzické osobě:

Osobní údaje

- Jméno
- Pohlaví
- Věk a datum narození
- Osobní stav
- Občanství
- IP adresa
- Pracovní nebo osobní adresa
- Pracovní nebo osobní telefonní číslo
- Pracovní nebo osobní email
- Ověřovací identifikační údaje
- Identifikační čísla vydaná státem
- Fotografický údaj

Citlivé osobní údaje

- Rasový nebo etnický původ
- Politické názory
- Zdravotní stav
- Náboženské nebo filozofické vyznání
- Sexuální orientace
- Trestní delikty nebo pravomocné odsouzení
- Genetické nebo biometrické informace
- Členství v odborech
- Osobní údaje dětí

- Vztahuje se i na šifrované osobní údaje – vždy někdo zná klíč
- Vztahuje se jak na data v informačních systémech, tak na papírové dokumenty

GDPR – popis implementace v reálném prostředí

Jak by měla vypadat implementace GDPR v reálném prostředí:

1. Analýza existujícího prostředí:
   - Jaké jsou důvody pro sběr a zpracování osobních údajů?
   - Kde se zpracovávají a ukládají osobní údaje (PC, databáze, síťová úložiště, cloudové služby, emaily, mobilní zařízení, kartotéky, archivy…)
   - Existuje redundance osobních údajů?
   - Jaké procesy a technologie jsou v současné době používané pro zpracování osobních údajů?

2. Závěry a doporučení na základě analýzy:
   - Nové procesy
   - Nové technologie
   - Změny v IT infrastruktuře
   - Nová dokumentace: Data protection politiky, záznamy aktivit, kodexy chování

3. Implementace doporučených procesů a technologií

4. Pravidelná revize - nová doporučení, změna technologií a nastavení - DPO

Digitální transformace a GDPR

IT faktory, které je nutné řešit v souvislosti s dodržováním nařízení GDPR

Zařízení, infrastruktura, databáze

Osobní údaje uložené na interních i mobilních zařízeních, infrastruktuře a databázích jsou stále více cílem sofistikovaných útoků s cílem tyto data získat

Cloudové služby

Přemisťování dat a služeb do cloudu vede k vyššímu riziku ztráty nebo zneužití osobních údajů

Nové aplikace

Aplikace jsou často vyvýjeny a pouštěny do produkčního prostředí se zranitelnostmi nebo bez většího zabezpečení a tím zvyšují riziko ztráty nebo zneužití osobních údajů

Ochrana dat a GDPR

- **Ochrana dat by měla být samozřejmostí pro každou společnost** – ztráta reputace, ztráta intelektuálního vlastnictví, interních informací společnosti.
- **Ztráty a krádeže dat jsou každodenní problém**
- GDPR stanovuje povinnost chránit osobní údaje osob

Ztráta zařízení

Okolo 40% všech incidentů ztráty dat bylo reportováno na základě ztráty nebo krádeže zařízení – notebook, mobilní zařízení, externí paměťová média

Externí útočník

Okolo 59% reportovaných incidentů způsobených malware nebo zneužitím zranitelnosti aplikace externími útočníky, obsahovaly citlivá data

Zaměstnanci a dodavatelé

Okolo 57% reportovaných incidentů, které mají na svědomí interní zaměstnanci, ať již vědomě nebo nevědomě, obsahovaly citlivá data

Více než 50% incidentů ztráty dat bylo publikováno externě

Co je nutné zvážit při návrhu zabezpečení IT v souvislosti s GDPR

Pokrytí možných útoků

Mobilní zařízení a firemní služby

Cloudové úložiště

Databáze

Cloudové služby

Aplikace, API

Práva

Pokrytí vektorů ztráty dat

Náhodná ztráta zařízení

Porušení pravidel a politiky

Cloudové služby

Škodlivá infiltrace Malware, APT

Interní hrozby

Jaké nástroje nabízí McAfee na ochranu osobních údajů?

Vektory ztráty a úniku dat

Fyzická ztráta zařízení

File and Removable Media Protection

Full Disk Encryption

Management of Native Encryption

ePO for Compliance Reporting

Detekce a prevence úniku dat zaměstanci a hackery

DLP Endpoint, DAM, DLP Network, Web Gateway

ENS, Adaptive Treat Protection
Application Control

ESM pro sběr logů a montorování

Sledování uživatelské aktivity - User Behavior Analytics – ESM, DLP Monitor, IPS

Cloudové služby a aplikace

DLP Endpoint, Web Gateway, DLP Network a CASB

Data Center Security Suite

ESM pro sběr logů a montorování

Sledování uživatelské aktivity - User Behavior Analytics – ESM, DLP Moniror, IPS

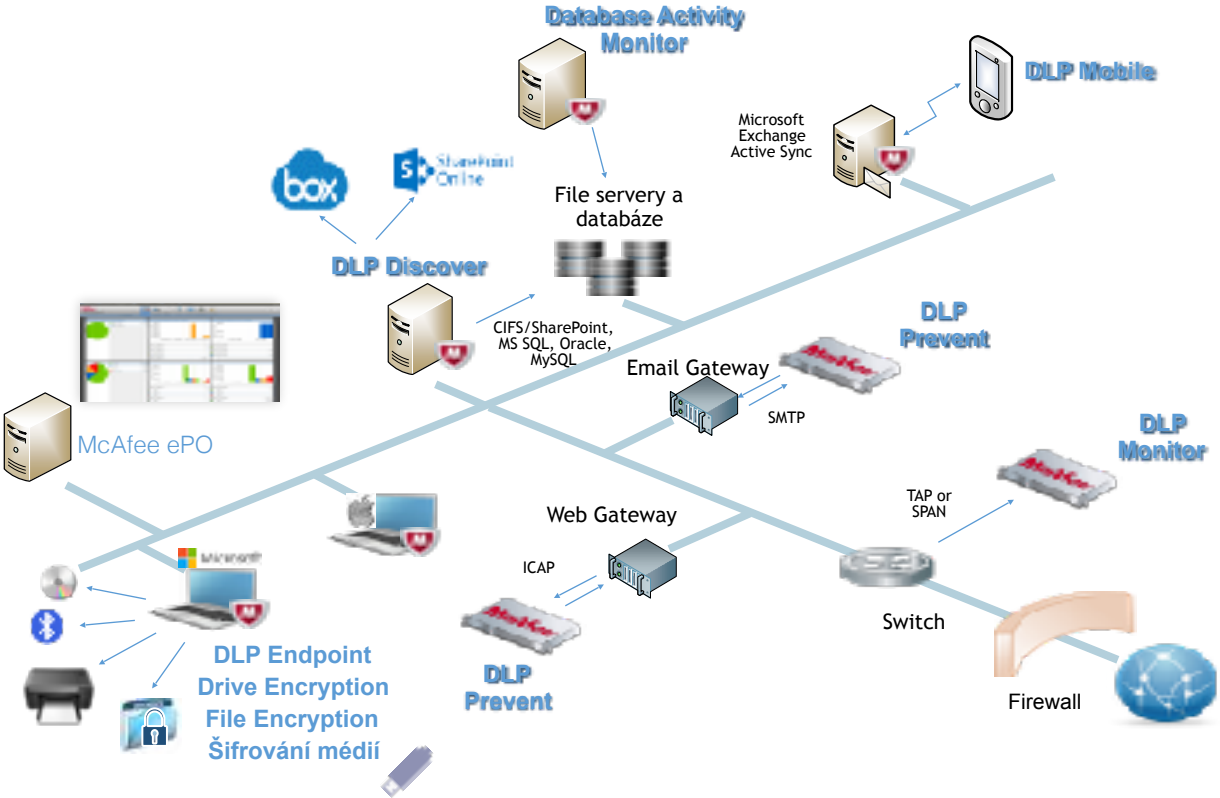
Ochrana aplikací a databází

Database Activity Monitoring

ENS, Adaptive Treat Protection
Application Control

ESM pro sběr logů a monitorování

Komplexní ochrana dat s McAfee produkty



Osobní údaje definované GDPR

Jakých údajů se GDPR nařízení týká:

- **Obecné osobní údaje a citlivé osobní údaje** – veškeré informace vztahující se k identifikované nebo indentifikovatelné fyzické osobě:

Obecné osobní údaje

- Jméno
- Pohlaví
- Věk a datum narození
- Osobní stav
- Občanství
- IP adresa
- Pracovní nebo osobní adresa
- Pracovní nebo osobní telefonní číslo
- Pracovní nebo osobní email
- Ověřovací identifikační údaje
- Identifikační čísla vydaná státem
- Fotografický údaj

Citlivé osobní údaje

- Rasový nebo etnický původ
- Zdravotní stav
- Sexuální orientace
- Politické názory
- Náboženské nebo filozofické vyznání
- Trestní delikty nebo pravomocné odsouzení
- Genetické nebo biometrické informace – Členství v odborech
- Osobní údaje dětí

- Vztahuje se i na šifrované osobní údaje – vždy někdo zná klíč

- **Jednoznačně definované informace, které se musí chránit**
- **McAfee DLP umožňuje relativně jednoduše vytvářet klasifikační pravidla pro tento druh informací – RegEx výrazy, slovníky, manuální klasifikace**

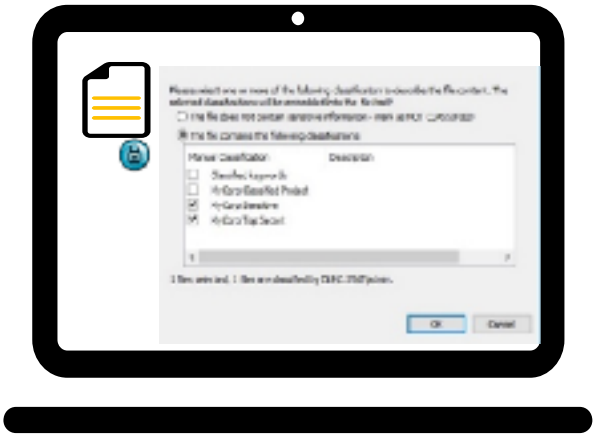
Klasifikace dat v DLP systému

- **Klasifikace dat je nejdůležitější a nejnáročnější část implementace DLP systému !!!**
- Klasifikace dat musí pokrýt veškerá citlivá data, jak osobní údaje, tak interní informace společnosti

ALE

- Vždy je nutné pečlivě zvážit, jaká data jsou ve společnosti citlivá a je nutné je chránit
  - Data definovaná vedením společnosti
  - Data, která definují normy a regulace – PCI DSS, **GDPR**, SOX.....
  - Data důležitá pro chod společnosti.
- Klasifikace dat v McAfee DLP může být provedena několika způsoby
  - **Fingerprint klasifikace dat**
  - **Obsahová klasifikace dat**
  - **Manuální klasifikace dat**
  - **Discovery klasifikace dat**
- Klasifikace dat se provádí jak na koncových zařízeních, tak na síťových sondách

Manuální klasifikace dat uživatelem



- Uživatel musí klasifikovat ukládaný soubor
- Pokud neklasifikuje, systém přidává klasifikátor „Not Classified“ – DLP snadno najde takto označený dokument
- Neklasifikovaný dokument je možné i nadále sledovat obsahovými klasifikačními pravidly
- Nabízí flexibilitu v nasazení DLP

Umožňuje nebo vynucuje klasifikaci MS Office souborů –
Word, Excel, PowerPoint
nebo emailů v MS Outlook uživatelem

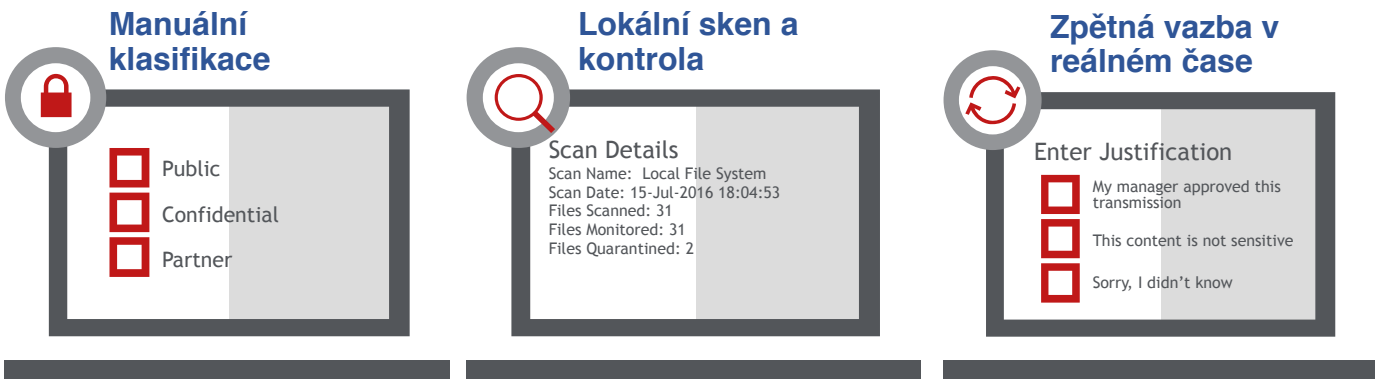
Vytvořit

Odeslat
Uložit
Tisknout

Klasifikovat

Řízení a monitorování uživatelské aktivity s DLP systémem

Vzdělávání zaměstnanců, zmírnění administrativní zátěže, snížení rizikového chování



Zpětná vazba v reálném čase: ~75% snížení rizikového chování

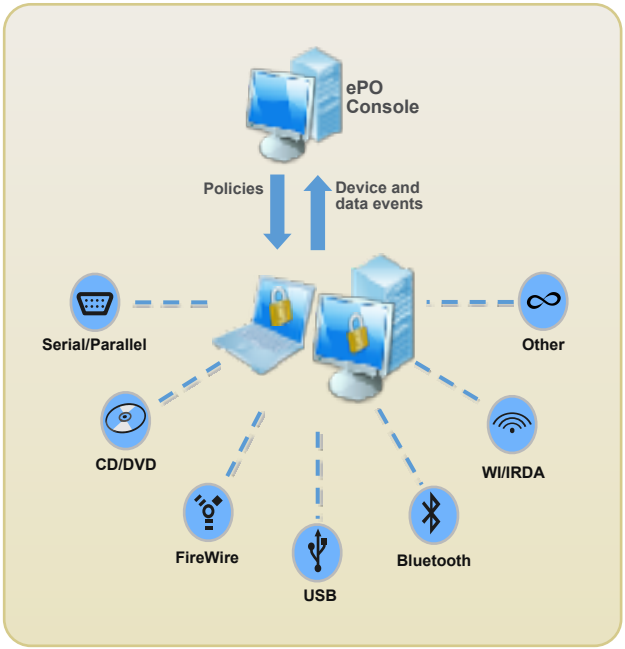
Ochrana dat v Cloudu

- Cloud Discovery sken– Box, SharePoint
- Cloud Protection pravidla – Box, DropBox, GoogleDrive, iCloud, OneDrive - personal, business, Syncplicity

Device Control

Kontrola připojovaných externích zařízení

- Je součástí DLP Endpoint, ale je dostupný jako samostatný produkt nebo je součástí dalších balíčků.
- Monitoruje, blokuje připojitelná zařízení, nebo je dělá read-only.
- Blokuje spouštění souborů z připojených zařízení.
- Možnost nastavení pravidel pro uživatele nebo uživatelské skupiny
- Možnost definovat globální pravidla, nebo konkrétní pravidla pro specifická zařízení – sběrnice, výrobce, sériové číslo, typ souborového systému.....



Definuje různé politiky, které blokují, povolují nebo nastavují zařízení pouze pro čtení na základě typu zařízení.

Device Control – definice zařízení

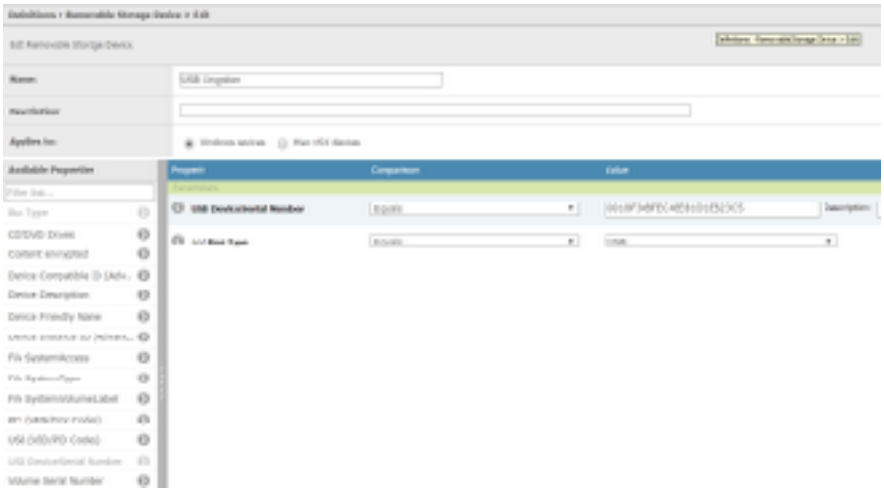
- **Systém pro správu I/O zařízení**

Možnost specifikovat obecné zařízení:

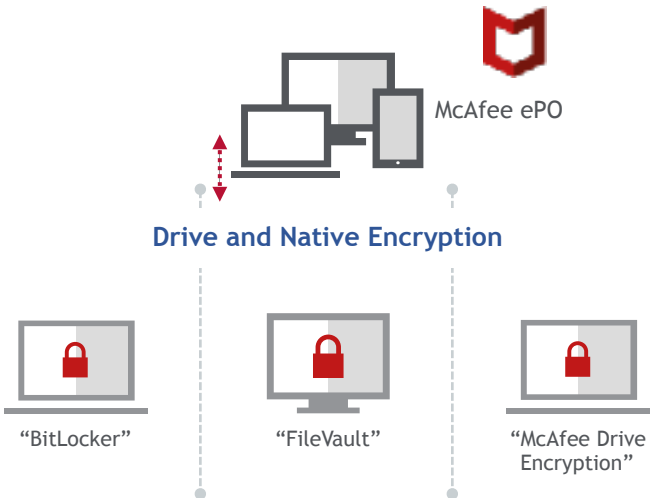
- Vyjímatelná média
- Plug-and-play zařízení
- Sběrnice
- Souborový systém

Možnost specifikovat preferované zařízení:

- Sériové číslo
- Výrobce
- Model
- Device ID
- ……..



Hard Drive Encryption zamezuje ztrátě dat

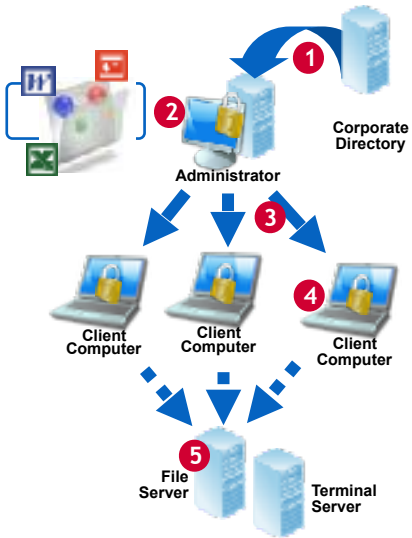


Ochrana osobních údajů před ztrátou nebo odcizením zařízení. Data jsou šifrována a tím automaticky chráněna před zneužitím cizí osobou

McAfee File & Removable Media Protection

Ochrana souborů a složek šifrováním

- Ochrana citlivých dat šifrováním na lokálních i sdílených úložištích
  - Ochrana citlivých dat před zneužitím neoprávněnou osobou – zaměstnanec, externí útočník
  - Centrální správa a přidělování klíčů uživatelům nebo uživatelským skupinám z AD
- Ochrana citlivých dat šifrováním, která jsou odesílána na USB zařízení
- Ochrana citlivých dat šifrováním, která jsou odesílána na Cloudové služby
- Šifrování externích datových úložišť připojených přes USB rozhraní
  - USB disky, flash disky
  - Ochrana citlivých dat přímo na externím úložišti
- Centrální definice politiky umožňuje detailnější nastavení i ve velké společnosti
- Ochrana souborů a složek na stanicích, laptopech a serverech



Proaktivní ochrana dat s integrací TIE technologie

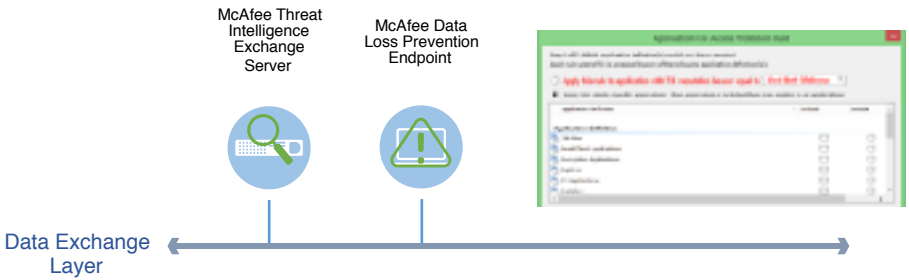
1 DLPE identifikuje spuštění nového procesu Proces A.exe

2 DLPE odesílá požadavek na TIE server pro získání reputace ProcesA.exe

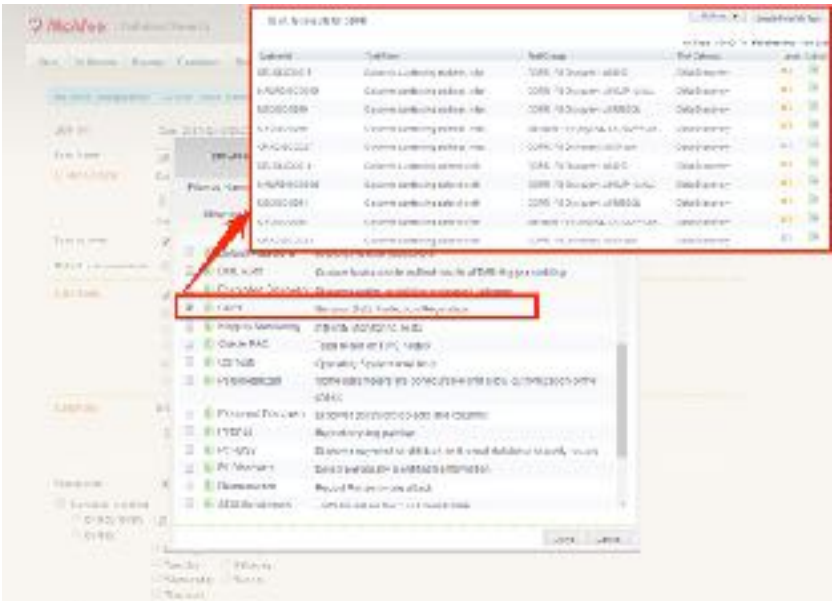
3 TIE server vyhledá reputaci o procesu Proces A.exe

4 TIE server vrací reputaci procesu: Proces A.exe Most Likely Malicious

5 DLPE monitoruje Proces A.exe a blokuje procesu přístup k citlivým datům



McAfee Database Security



Speciální sken pro GDPR

Zobrazuje veškeré databázové aktivity

Automatizovaný DB discovery sken

Možnost blokování přístupu nebo získávání dat z databází

Ochrana nezáplatovaných databází – virtual patching