COMGUARD **Expert Services**

…B2B
…..10 let na trhu
…..Bezpečnost ICT/Sítě/Služby

Téma: General Data Protection Regulation (GDPR)

Cíl nařízení GDPR: Nastolení rovnováhy mezi legitimními zájmy správců a zpracovatelů dat a právem osob na soukromí.

General Data Protection Regulation (GDPR) nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále OÚ) a volný pohyb těchto údajů, vstupuje v platnost s účinností od 25. 5. 2018, více na http://data.europa.eu/eli/reg/2016/679/oj. Nařízení GDPR, nahrazující směrnici 95/46 EC, v ČR zákon č. 101/2000 Sb. o ochraně OÚ, je dosud nejkomplexnějším souborem pravidel na ochranu dat v celosvětovém měřítku. Nařízení GDPR bude sloužit k narovnání vymahatelnosti práva přes všechny státy Evropské Unie.

DŮLEŽITÉ POŽADAVKY GDPR	ŘEŠENÍ
Oddělený souhlas se zpracováním OÚ za podmínek obecných, obchodních atd.	Organizační směrnice
Opatření pro požadavek "být zapomenut", resp. "být smazán" (*right to erasure*).	Správně vyřešená anonymizace dat - technologie schopné data najít a zajistit jejich vymazání nebo přesun.
Privacy by Design – zajištěná ochrana OÚ, tj. plánované a zabezpečené zpracování, využití dat pouze pro daný účel.	Organizační směrnice a následné procesy. Např. dávkové odstranění dat z DMZ do chráněné zóny.
Hlásit bezpečnostní incidenty „bez zbytečného odkladu" příslušnému dozorovému orgánu nejpozději do 72 hodin, a to náhodné či úmyslné zničení, ztrátu, změnu, neoprávněné vyzrazení nebo zpřístupnění dat při zpracovávání, uchovávání či přenosu.	Technologická opatření: • DLP • SIEM • Log & Security Data Management • Insider Threat Management
Proaktivní přístup včetně posuzování možných dopadů úniku OÚ. • Schopnost předejít bezpečnostním incidentům. • Schopnost upozornit na podezřelé chování, interní i externí krádež dat, infiltrování systému nebo neopatrné nakládání s daty (např. jejich nešifrované ukládání a sdílení na cloudová úložiště).	Technologická opatření: • DLP • Vulnerability management • šifrování • Antivirus & Application control • školení zaměstnanců a uživatelů, kteří jsou v kontaktu s OÚ
DATA PROTECTION OFFICER (DPO) Delegovaná funkce, kterou musí mít: • veřejné instituce, • společnosti zpracovávající OÚ (databáze od 5 tis. záznamů), • společnosti zpracovávající speciální kategorie (informace o rase, náboženství, etniku, politické orientaci atd.) Jedná se zejména o státní správu, nemocnice, banky a pojišťovny, velké firmy i větší e-shopy, marketingové firmy.	Funkci by měl zastávat expert v oblasti bezpečnosti a práva. Dohlíží na soulad s GDPR a náplní jeho činnosti je: • informovat, vzdělávat a kontrolovat zaměstnance při zpracování a nakládání s daty • monitorovat procesy a podezřelé aktivity • spolupracovat s kontrolními orgány

Možné sankce: na dodržování nařízení GDPR bude dohlížet státní kontrolní orgán zastřešující Evropský sbor pro ochranu osobních údajů.
Výše možných sankcí závisí na řadě faktorů, jako jsou např. úmysl / nedbalost, počet dotčených subjektů a míra škody, kategorie osobních údajů dotčených porušením, míra odpovědnosti s přihlédnutím na technické a organizační opatření atd.
Pokuta se může vyšplhat až na 20 mil. EUR nebo 4% z celkového ročního obratu za předchozí finanční rok. V případě bezpečnostního pochybení budou **manažeři vystaveni trestní odpovědnosti.**

Technologická opatření potřebná k naplnění shody s GDPR

1. **Šifrování**
2. **DLP (Data Loss prevention Technology)**
3. **SIEM, Security Data Management a Insider Threat Management**
4. **Vulnerability Management**
5. **Antivirus a Application control**

CO MUSÍ FIRMY UDĚLAT?

1. Zavést systém ochrany dat

Firmy, které pracují s **osobními daty občanů Evropské unie**, si budou muset ujasnit, **jaká data sbírají a k čemu je využívají.** Musí si určit **pravidla, jak s nimi budou pracovat**. Povinnost platí i pro ty společnosti, které sídlí mimo území unie, ale nabízí zboží nebo služby rezidentům EU.

2. Zajistit bezpečnost dat

Jednotlivé firmy musí **zaručit, že pro bezpečnost dat dělají skutečně maximum**. Očekává se, že budou investovat do nových systémů a posilovat opatření, která úniku dat zabrání. **Správu dat mohou přenést na specializované firmy, včetně firem nabízejících cloudová řešení**.

3. Získat od klientů souhlas

Lidem by **firmy měly jasně a srozumitelně říkat, jaká data od nich sbírají a za jakým účelem**. Nebude už proto možné dát klientům odsouhlasit mnohastránkový dokument s kompletními podmínkami napsaný nesrozumitelnými výrazy a drobným písmem.

4. Připravit se na možný audit

Všechny firmy, které pracují s OÚ, by se měly připravit na možný **audit** v míře, která odpovídá objemu a charakteru dat, se kterými společnost pracuje nebo která má k dispozici.

~ 300.. partnerů/resellerů
~ 3.000.. spokojených klientů
~ 300.000……. zachráněných dat

COMGUARD **Expert Services**

…B2B
…..10 let na trhu
…..Bezpečnost ICT/Sítě/Služby

Technologická doporučení společnosti COMGUARD pro zajištění shody s GDPR

DLP (DATA LOSS PREVENTION)

McAfee Host & Network DLP

- Identifikace a prevence neúmyslných úniků dat.
- Prosazuje mnohostranné, vysoce flexibilní politiky s možností využití sofistikovaných předvoleb pro shodu se standardy (jednotné nastavení u network i endpoint řešení).
- Pokročilý reporting incidentů a monitoring se sběrem důležitých dat pro analýzu.
- Řízení souborů při ukládání na cloudové služby, jako jsou OneDrive, Office 365 apod.
- Možnost nastavení manuální klasifikace souborů.

SIEM

LogRhythm SIEM

- Nezávislá forenzní analýza koncových zařízení a File Integrity Monitoring.
- Pokročilá korelace a rozpoznání vzorků (pattern).
- Vícerozměrné analýzy a detekce anomálií chování na úrovni uživatele, sítě i koncových zařízení.
- Analýzy velkých objemů dat, jejich vizualizace, procházení k detailnějším vrstvám.
- Integrovaný „Case Management".

McAfee Security Information and Event Management

- Jednotný a komplexní pohled na bezpečnost sítě.
- Snížení náročnosti auditů – integrace aktivit pro audity a dosažení shody se standardy díky vestavěné možnosti průběžné kontroly a pravidelného reportingu.
- Splnění standardů o uchovávání log záznamů, compliance a integrity.
- Korelace síťových a bezpečnostních událostí s reálnými business procesy a politikami.

INSIDER THREAT MANAGEMENT

ObserveIT

- Sofistikovaný systém pro audit: videozáznam a textové logy všech aktivit uživatelů i z aplikací bez interních logů.
- Anonymizace osobních údajů – je možné konfiguračně vynutit anonymizaci osobních údajů a zřídit roli Privacy Officer, který schvaluje požadavky na odkrytí identity.
- Detecting Data Loss – pomocí agenta lze detekovat možnou exfiltraci kritických nebo citlivých dat.

ENCRYPTION

McAfee Drive Encryption

- Přináší transparentní šifrování bez narušení práce uživatele či zpomalení systémů.
- Zaručuje konzistentní ochranu na všech zařízeních.
- Umožňuje prosadit určenou bezpečnostní politiku společnosti.
- Zajišťuje možnost šifrování pro soubory také v cloudovém prostoru: Box, Dropbox, Google Drive a OneDrive.

Sophos SafeGuard Enterprise

- Detailní reporty a audity.
- Centrální správa s možností nastavení různých úrovní administrátorských práv.
- Díky „always-on" technologii je šifrování automatické a transparentní pro koncového uživatele.
- Uživatelé mohou šifrované soubory otevřít, měnit a sdílet v rámci organizace bez jakéhokoliv omezení. Pro sdílení mimo organizaci jednoduše vytvoří heslo během pár vteřin.

SECURITY DATA MANAGEMENT

Rapid7 InsightIDR

- Velmi dobře škálovatelná cloudová služba sloužící k detekci a vyšetřování bezpečnostních rizik.
- Služba je licencovaná per asset a má velice jednoduché nasazení, proto je vhodná i pro malé a střední podniky.
- Dokáže zpracovávat data získaná z koncových stanic do smysluplného kontextu, a to bez narušení uživatelské aktivity.
- Spolehlivě dokáže vystopovat zneužití lokálních účtů, nebezpečné procesy nebo manipulaci s logy.
- Využívá technologii machine-learning, díky čemuž se celé řešení průběžně vyvíjí společně s proměnným chováním útočníků.

VULNERABILITY MANAGEMENT

Rapid7 Nexpose

- Cílené skenování a reportování – skenování a reportování zaměřené na určité oblasti (interní a externí síť, webové aplikace, databáze atd.)
- Bezpečnostní kontroly – poskytuje přehled o výsledku a stavu kontrol.
- Analýza zranitelnosti – pomáhá stanovit priority a přijmout rozhodnutí na základě prioritního plánu, kategorizace dat a ověřování zranitelností v aktuálním softwaru.
- Automatizovaný ticketing – při zjištění hrozby automaticky vytvoří ticket a po jeho vyřešení jej zruší.
- Asset Management – pomáhá odhalit, kdo a co vlastní, dále určí, která aktiva je pro společnost více či méně důležitá a automaticky zvýší/sníží risk skóre.

ANTIVIRUS & APPLICATION CONTROL

Sophos Enduser Protection

- Všechna zařízení chráněná pomocí jediné licence.
- Ochrana kdekoliv – bez ohledu na to, kde se právě uživatel nachází.
- Komplexní ochrana proti hrozbám – antivirus, správa zařízení, aplikací, dat, síťových a webových přístupů, šifrování, DLP apod.
- Jednoduché a efektivní šifrování disků, mobilních zařízení a emailů.
- Licencování na uživatele – bez ohledu na to, kolik zařízení využívá.

McAfee Endpoint Security & Application Control

- Zajišťuje provozování pouze důvěryhodných aplikací na koncových stanicích pomocí Application Whitelisting agenta.
- Jediná řídící konzole pro celé spektrum ochran šetří čas, náklady i kapacitu linek.
- Jedno integrované řešení pokryje bezpečnost celé vnitřní sítě.

~ 300.. partnerů/resellerů
~ 3.000.. spokojených klientů
~ 300.000……. zachráněných dat