GDPR a informační systémy obcí, využívání IT & bezpečnost

Radek Brázda - KISMO

Cíl nás všech…

- Cílem implementace GDPR byla nejen ochrana osobních údajů a strašák vysokých pokut, ale správné používání osobních údajů ve veřejné správě. Ruku v ruce s tím se musí zvýšovat povědomí zaměstnanců – uživatelů informačních systémů obcí o rizicích spojených s používáním prostředků informačních technologií a informačních aktiv při práci s IT na obcích = zvýšení zabezpečení IT a bezpečnosti dat.

Co to je informační systém

- Informačním systémem nazýváme celý systém, ve kterém se informace v jakémkoliv tvaru a nebo na jakémkoliv médii (elektronické, papírové, multimediální):
  - vytvářejí nebo získávají
  - zpracovávají, modifikují
  - vystupují do jiných IS
  - jsou posílány do komunikačních systémů
  - jsou ukládány, zálohovány, obnovovány
  - jsou likvidovány.
- Nedílnou součástí pak jsou technologie, prostory a lidé.

Co to vlastně je bezpečnost

- Důvěrnost
  - Prozrazení, zcizení informace
- Integrita
  - Nežádoucí modifikace informace
- Dostupnost
  - Ztráta či úplné zničení informace

Příklady ochrany informací

•Uzamčení informace
•Přístupová oprávnění
•Šifrování souborů a přenosu (VPN)

•Elektronický podpis
•Přístupová oprávnění
•Monitorování přístupu a změn informací

•Zálohování
•Provoz IS a ukládání dat ve více lokalitách
•Rychlá obnova informačních systémů

Důvěrnost – Integrita – Dostupnost
(tzv. CIA model – Confidentiality – Integrity - Availability)

Bezpečnost a ochrana informací

V jakých oblastech informace musíme chránit.

Hlavní aspekty bezpečnosti:

- Fyzická bezpečnost,
- Organizační bezpečnost,
- IT bezpečnost,
- Personální bezpečnost

Žádná z nich není opominutelná, žádná nefunguje bez zbývajících

Kyberprostor

- *Kyberprostor je globální a vyvíjející se prostor jehož smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje:*
  - *a) fyzická i telekomunikační zařízení,*
  - *b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému,*
  - *c) spojení počítačových sítí,*
  - *d) uživatelské vstupy a uzly zprostředkovatelů spojení,*
  - *e) informace – uživatelská data.*
- *Význačnou a charakteristickou vlastností kyberprostoru je, že žádná jediná centrální moc nekontroluje všechny sítě, které tvoří tuto doménu, tudíž nekontroluje kyberprostor.*

Zdroj: cs.wikipedia.org/wiki/Kyberprostor

A tudíž v kyberprostoru není koho žalovat, na nikom se nic nedá vzít

Bezpečnostní incidenty

Bezpečnostní incident a událost

- Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
- Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací i v důsledku kybernetické bezpečnostní události.

Bezpečnostní incident – příklady

- Kybernetický útok na zařízení či informační systémy
- Prozrazení hesla (vlastního či spolupracovníka)
- Výskyt chráněných informací v síti Internet (web, blogy, diskuzní skupiny, sociální sítě, …)
- Proniknutí osoby bez vstupní karty a bez doprovodu do chráněné oblasti
- Připojení cizího počítače (soukromého nebo PC externisty) do interní sítě
- Výskyt viru či jiného škodlivého kódu
- Výskyt mailů obsahujících phishing nebo podezřelé přílohy
- … a další obdobné případy

Identifikace, Autentikace, Autorizace,

Jak se prokazuje, že jsem to skutečně já:

- **Identifikace** – určení identity uživatele,
- **Autentizace** uživatele – ověření identity uživatele (verifikace, autentifikace, autentikace)
  - Prostředky autentizace – metody ověření identity za pomocí hesla, předmětů, biometrických či behaviometrických systémů
- **Autorizace** – celý systém procesu vstupu např. do systému či objektu, zahrnuje identifikaci, autentikaci a úspěšné, či neúspěšné přijetí, vyjadřuje to k čemu je uživatel autorizován (oprávněn)

Hesla

Heslo je prvkem autentizace uživatele

- Heslo je důležitým bezpečnostním prvkem, proto musí splňovat následující parametry znesnadňující jeho snadné uhádnutí nebo prolomení
- Heslová politika – zásady pro bezpečné heslo:

Minimální délka:	8 znaků
Komplexnost:	Heslo musí obsahovat minimálně - jedno velké a jedno malé písmeno, - jednu číslici, - jeden speciální znak (. , - * _ + # $ apod.).
Pravidelná změna:	Minimálně 1x za 90 dnů.
Opakovatelnost:	Stejné heslo se nesmí opakovat min. 4 změny zpět.

Zásada !!!

- Pro heslo nesmí být použity snadno identifikovatelná jména (vlastní, rodičů, sourozenců, dětí, domácích zvířat apod.), datumy narození, názvy měsíců, a jiné snadno predikovatelné kombinace.

Doporučení !

- Je velice efektivní tvořit hesla na základě tzv. pas fráze, například:

Pas fráze: **S**nědl **P**epa osm **kn**edlíků **n**ebo čtrnáct **?** → Heslo: SP8kn14?

GDPR a IT……postřehy

Co znamená pro IT naplnění zásad a jejich doložení = kontrola a úprava IS, vlastní styl práce

- Osobní údaje se shromažďují pouze pro určité, výslovně vyjádřené a legitimní účely a jsou dále zpracovávány způsobem, který je s těmito účely slučitelný - „**účelové omezení**“
- Osobní údaje jsou ve vztahu k účelu, pro který jsou zpracovávány, přiměřené, relevantní a omezené na nezbytný rozsah - „**minimalizace údajů**“
- Osobní údaje jsou přesné a v případě potřeby aktualizované; nepřesné osobní údaje jsou bezodkladně vymazány nebo opraveny - „**přesnost**“
- Osobní údaje jsou uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány - „**omezení uložení**“
- Osobní údaje jsou zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů - „**integrita a důvěrnost**“

Jak implementujeme do IT práva subjektu osobních údajů? Úpravou IS.

- právo na informace o zpracování osobních údajů (OÚ)
- právo na přístup subjektu k OÚ (právo získat od správce OÚ potvrzení o zpracování OÚ, právo získat kopii zpracovávaných OÚ)
- právo na opravu
- právo vznést námitku
- právo na omezení zpracování
- právo na výmaz („právo být zapomenut“)
- právo na přenositelnost údajů
- právo nebýt předmětem automatizovaného rozhodnutí.

Závěr – ochrana osobních údajů není ale jen IS, směrnice či správné heslo….

- HW – od infrastruktury po koncová zařízení
- SW – systémový i aplikační
- Správně nastavené procesy v organizaci
- Dodržování bezpečnostních pravidel = směrnice = ISO
- Pravidelná kontrola všech úrovní prostředí organizace
- Plánování rozvoje, finančních prostředků, vzdělávání

……..

Děkuji za pozornost
Dotazy prosím?

Radek Brázda