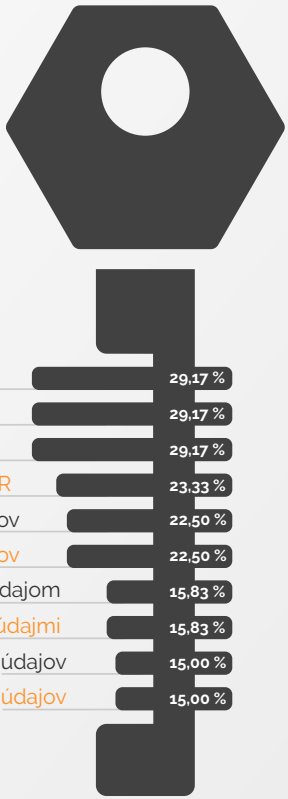
Šifrovanie v kontexte GDPR

Tempest
IT makes sense

Jedným zo spôsobov ochrany osobných údajov vyžadovaných nariadením je šifrovanie osobných údajov. Podľa našich prieskumov vyvoláva v súčasnosti šifrovanie najviac otázok predovšetkým v súvislosti s GDPR.

S ktorou časťou nariadenia GDPR máte problém?

*respondenti mohli označiť viacero odpovedí



Prieskum prebiehal v mesiacoch august a september 2017 a zúčastnilo sa ho 120 respondentov z radov manažérov IT, bezpečnosti, prevádzky, špecialistov na informačnú bezpečnosť a technologické právo.

Všeobecné nariadenie o ochrane osobných údajov (GDPR) vytvára právny rámec pre kontrolu a postihovanie neplnenia odporučených opatrení pri ochrane osobných údajov fyzických osôb zo strany spracovávateľov alebo sprostredkovateľov osobných údajov.

Či už hovoríme o šifrovaní údajov všeobecne alebo o šifrovaní len osobných údajov, pri implementácii aplikujeme rovnaké postupy a algoritmy. **Pri plánovaní implementácie šifrovania identifikujeme, čo, kde a ako budeme šifrovať.**

Čo budeme šifrovať?

V kontexte nariadenia je to dané – šifrujeme to, čo chránime. Chránime osobné údaje chápané ako „akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby“. Vymedzenie pojmu „osobné údaje“ možno nájsť v článku 4 Nariadenia*.

* Na účely tohto nariadenia „osobné údaje“:

- sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“);
- identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

Kde budeme šifrovať?

V rámci životného cyklu sa údaje nachádzajú v nasledovných stavoch:

1. Údaje v pokoji
2. Údaje počas prenosu
3. Spracovávané údaje

1

Údaje v pokoji sú krátkodobo alebo dlhodobo uložené na lokálnych diskoch serverov a/alebo koncových zariadeniach, zdieľaných diskoch, úložiskách alebo na prenosných pamäťových médiách. Rovnako sú za údaje v pokoji považované záložné kópie údajov. Najčastejšie ide o dátové pásky vytvárané pre potreby obnovy údajov alebo pre archívne účely.

Pričom šifrovať môžeme:

- celé úložné médium (disk, prenosné pamäťové médium, dátová páska) – každý súbor ukladaný na médium je automaticky zašifrovaný. Avšak pri presune na iné médium, ktoré šifrované nie je, súbor prestáva byť šifrovaným,
- jednotlivé súbory – šifrovanie a odšifrovanie je iniciované používateľom. Pri presune na iné médium súbor zostáva zašifrovaný,
- vybrané údajové atribúty v systémoch na správu údajov – databázach – alebo priamo v aplikáciách.

2 **Prenášané údaje sú údaje v pohybe** medzi údajovým úložiskom a spracovateľskou aplikáciou, medzi spracovateľskou aplikáciou a koncovým používateľom alebo medzi používateľmi.

Pričom si môžeme zvoliť šifrovanie:

- medzi komunikujúcimi koncovými bodmi – end-to-end.
  K zašifrovaniu údajov dochádza pred ich vstupom do komunikačného kanála a údaje zostávajú zašifrované aj po jeho opustení. Čitateľné sú len pre príjemcu s platným šifrovacím kľúčom. Príkladom môže byť posielanie zašifrovaných súborov pomocou PGP cez e-mail.
- komunikačného kanála.
  Komunikujúce strany si dohodnú spôsob, akým budú šifrovať údaje v komunikačnom kanáli. Prenášané údaje vstupujú do komunikačného kanála nešifrované. Rovnako nešifrované zostávajú aj na strane príjemcu po opustení šifrovaného komunikačného kanála. To znamená, že sú čitateľné pre príjemcu, ale aj pre správcu služby, ktorá komunikačný kanál vytvorila. Príkladom je použitie SSL/TLS pri web komunikácii alebo VPN (Virtual Private Network).

3

Spracovávané údaje sú údaje, ktoré aplikácia a/alebo systém používa na správu údajov a má ich uložené v operačnej alebo vyrovnávacej pamäti. Rovnako môžu niektoré údaje krátkodobo zostať ako súčasť dočasných súborov vytváraných databázami, aplikáciami, nástrojmi na „medzispracovanie“ alebo počas ich spracovania v súborovom systéme.

Šifrovanie môže byť použité na ochranu údajov v operačnej pamäti, pričom môže byť opäť zvolený prístup šifrovania celej pamäte alebo šifrovania aplikáciou spracovávaných vstupov s vygenerovaním šifrovaného výstupu bez odšifrovania vstupných údajov, napr. s použitím homomorfného šifrovania.

Ako budeme šifrovať?

Šifrovanie je proces transformácie vstupných údajov na výstupné aplikovaním šifrovacieho kľúča alebo kľúčov podľa definovaného postupu – algoritmu. Existuje niekoľko typov šifrovania v závislosti od počtu šifrovacích kľúčov – symetrické a asymetrické šifry, alebo od spôsobu spracovania vstupných údajov – prúdové a blokové šifry.

Odporúčania pri šifrovaní

Nariadenie vyžaduje ochranu údajov v pokoji, ale aj počas spracovania a prenosu. V existujúcich prostrediach, kde pri úvodnej implementácii nebola na šifrovanie kladená priorita, nemusí byť zavedenie, resp. zosúladenie s nariadením jednoduchou zmenou. Pokiaľ ide o údaje v pokoji, vhodnou cestou môže byť použitie šifrovania celých súborových systémov, priečinkov alebo súborov. Pri údajoch počas prenosu možno využiť šifrované komunikačné kanály, napr. už spomínané SSL/TLS.

Nech už aplikujeme na šifrovanie údajov ktorýkoľvek algoritmus využívajúci šifrovací kľúč alebo kľúče, je potrebné riešiť bezpečné uloženie a zdieľanie práve šifrovacích kľúčov, pretože kľúče sprístupňujú zašifrované údaje. Dodávatelia vo svojich riešeniach často podporujú viaceré spôsoby a algoritmy šifrovania. Pri voľbe treba zohľadňovať najnovšie poznatky na poli šifrovania. Dôležité je predovšetkým nevyberať tie algoritmy, v ktorých už existujú spôsoby, ako sa dostať k zašifrovanému obsahu.
TEMPEST má v tejto oblasti certifikované kompetencie a dlhoročné skúsenosti. Vieme pomôcť konzultovať, vybrať, nasadiť i prevádzkovať nástroje viacerých svetových výrobcov IT.

Odporúčame zvážiť implementáciu alebo urobiť zmeny napríklad s použitím nasledovných nástrojov:

- CheckPoint Endpoint Security – Full Disk Encryption, Media Encryption
- Symantec Whole Disc Encryption, PGP Universal Server
- Eset Endpoint Encryption

info@tempest.sk
www.tempest.sk

Text: Miloslav Leporis
miloslav_leporis@tempest.sk