

AC

Analýza rizik osobních údajů

ZNÁTE RIZIKA SPOJENÁ SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ? POTŘEBUJETE VĚDĚT, V JAKÉM STAVU JE OCHRANA OSOBNÍCH ÚDAJŮ A JAKÁ NEBEZPEČÍ JIM HROZÍ? POTŘEBUJETE TA SPRÁVNÁ ORGANIZAČNÍ NEBO TECHNICKÁ OPATŘENÍ A NEVÍTE, KTERÁ TO JSOU?

Co přináší analýza rizik osobních údajů?

Ochrana osobních údajů (OÚ) je nutností, ale k jejímu skutečnému vybudování musí každá organizace pochopit hrozby, které jsou součástí prostředí, v němž organizace působí. Hrozby jsou obvykle určovány pomocí metodického hodnocení bezpečnostních rizik. A právě analýza rizik slouží k nalezení těchto hrozeb a zranitelností, a zároveň přináší řešení, jak je eliminovat.

Popis řešení

Analýzu rizik chápeme jako komplexní proces, který zahrnuje identifikaci aktiv (v tomto případě osobních údajů), hrozeb a zranitelností ve spojitosti s osobními údaji, posouzení pravděpodobností a dopadů hrozeb na OÚ a identifikaci a ohodnocení rizik. Cílem analýzy rizik je odhalit rizika a navrhnout účinná a efektivní opatření k minimalizaci potenciálních škod hrozících informačním aktivům v podobě osobních údajů.

Komu je řešení určeno?

Řešení je určeno všem organizacím, ať už v roli správců nebo zpracovatelů OÚ, které chtějí čelit hrozbám a eliminovat bezpečnostní rizika a současně vyhovět požadavkům nařízení EU (GDPR). Velmi přínosné je také pro společnosti, které se snaží ochránit své investice do ICT nejen pro zpracování OÚ (a to i vzhledem k významným sankcím, které hrozí v případě nedodržování nařízení EU), záleží jim na důvěryhodnosti a chtějí chránit své dobré jméno.

PŘÍNOSY

- povědomí o hodnotě osobních údajů
- přehledné informace o rizicích OÚ a možnostech jejich eliminace
- sjednocená metodika hodnocení rizik (využitelná nejen pro OÚ)
- účinná ochrana OÚ před aktuálními hrozbami
- schopnost určit vhodná opatření k zabezpečení OÚ
- účelné vynakládání prostředků na ochranu OÚ
- naplnění požadavků GDPR (prevence sankcí)

Jaké jsou výstupy z analýzy rizik?

Analýzu rizik realizujeme prostřednictvím chronologicky na sebe navazujících kroků, jejichž výstupem je zpráva o stavu zabezpečení osobních údajů s přehledem identifikovaných rizik a úrovně jejich významnosti. Zpráva obsahuje standardní kapitoly:

- identifikaci výskytu analyzovaných informačních aktiv (osobních údajů);
- zařazení OÚ do odpovídajícího klasifikačního stupně;
- identifikaci hrozeb vůči posuzovaným OÚ;
- návrh katalogu hrozeb, podmínky, pravděpodobnost a předpokládané dopady jejich realizace (zranitelnost);
- identifikaci rizik a stanovení hodnoty rizik působících na posuzovaná aktiva (OÚ);
- návrh základních opatření na snížení rizik.

Použitá metodika k provedení analýzy rizik

Pro zpracování analýzy rizik využíváme kombinovaný přístup a semikvantitativní metodu, která umožňuje redukovat subjektivitu hodnocení (riziko čistě kvalitativní metody). Realizace probíhá formou účelových interview (metoda Delphi), která lépe zohledňuje specifika zpracování osobních údajů, jejich správce, zpracovatele, uživatele, okolí apod.

