



Klasifikácia ochrany informácií – štátna správa

Hodnotu informácií doceňujeme obvykle až vtedy, keď ich stratíme alebo keď ich únikom sú spôsobené závažné škody organizácii, spoločnosti, úradu. Súčasne môžu byť vo vybraných prípadoch uložené úradu sankcie vo forme pokuty pri porušení zákonov chrániacich vybrané druhy informácií (osobné údaje, utajované skutočnosti, spisová služba ...). Určite sa vyplatí nečakať až na tento okamžik a riešiť systém ochrany informácií skôr než problém nastane.

Táto ponuka je určená všetkým, ktorí nemajú zavedený komplexný systém ochrany dôležitých informácií. U úradov či spoločností, ktoré sa domnievajú, že ich systém ochrany informácií vyhovuje požiadavkám legislatívy a ich skutočnej hodnote na trhu odporúčame vykonanie aspoň prvej etapy našej ponuky. Práve audit ochrany informácií môže ukázať nielen na predpokladaný výklad legislatívy, ale tiež na to, že manipulácia s ďalšími citlivými informáciami sa nenachádza na takej úrovni, aby nemohli byť ľahko zneužitú.

Ponuka našej spoločnosti prezentuje skúsenosti odborníkov, ktorí sa dlhodobo zaoberajú problematikou ochrany informácií. Na základe syntézy ich skúseností s požiadavkami ochrany informácií v Európskej únii a vo svete vzniklo know-how, ktoré Vám ponúkame k širšiemu využitiu.

Predmet ponuky je rad postupných krokov (etáp), ktoré je účelové realizovať ako celok, ale súčasne je možné si objednať i jednotlivé z nich:

- **Vstupný audit ochrany informácií.** Výstupom je celkové zhodnotenie oblasti vrátane výpočtu nezhôd vzhľadom k platnej legislatíve a aktuálnej potrebe ochrany citlivých informácií zodpovedajúcich ich hodnote. V záverečnej správe sú tiež odporúčané opatrenia k odstráneniu nedostatkov.
- **Analýza citlivých informácií, s ktorými úrad (spoločnosť) pracuje a návrh ich kategorizácie.** Výstupom je návrh interného predpisu úradu (organizácie) „Kategorizácia informácií a zásady práce s citlivými písomnosťami“.
- **Analýza klasifikovaných informácií.** Etapa rieši ochranu informácií, ktorých podmienky sú stanovené zvláštnymi zákonmi (osobné údaje, utajované skutočnosti,). Výstupom etapy je **návrh interných predpisov pre ochranu osobných údajov a prípadne ďalších klasifikovaných informácií, ktoré sa u úradu (spoločnosti) vyskytujú** a návrh ďalších organizačných a technických opatrení k zaisteniu odstránenia zistených nezhôd.
- **Implementácia systému ochrany citlivých a klasifikovaných informácií.** Predmetom služieb v tejto etape je školenie zamestnancov úradu (spoločnosti) a školenie zamestnancov, ktorí budú mať zodpovednosť za oblasť ochrany citlivých a klasifikovaných informácií (pokiaľ nebude problematika outsourcovaná). Ďalej je predmetom služieb metodická pomoc pre zamestnancov, ktorí budú uvedenú oblasť riešiť. Súčasťou je tiež poradenstvo pri zaistení fyzickej a technickej bezpečnosti ochrany citlivých a klasifikovaných informácií.



- **Zavedenie systému ISMS.** Predstavuje komplexné riešenie ochrany informácií v digitálnej podobe (v IS) vo forme zavedenia systému manažmentu informačnej bezpečnosti (ISMS) podľa EN ITC 17799. Postupne sú realizované jednotlivé kroky, ktoré norma ukladá až po spracovanie požadovanej bezpečnostnej dokumentácie. **Výstupom je pripravenosť k certifikácii ISMS akreditovaným certifikačným orgánom.**
- **Chránená miestnosť.** V nadväznosti na analyzovanú hodnotu informácií a špecifiká činnosti úradu (spoločnosti) je vytipovaná chránená miestnosť, ktorá bude určená k prerokovávaniam zvlášť citlivých informácií. **Výstupom je návrh technického zabezpečenia a prevádzkového poriadku chránenej miestnosti. Po realizácii uvedených opatrení je vykonaná obranná technická prehliadka proti nasadeniu odposluchovej techniky.**
- **Periodický audit ochrany citlivých a klasifikovaných informácií.** Produkt je určený pre úrady (spoločnosti), u ktorých je uvedený systém už zavedený a predstavuje ročnú periodickú revíziu systému. Výstupom je prehľad nezhôd voči spracovanej dokumentácii a jej prípadná aktualizácia v nadväznosti na zmeny v legislatíve alebo nutná korekcia systému.
- **Ochrana informácií pre VIP.** Je základným kurzom ochrany informácií pre vedenie úradu (spoločnosti). Kurz možno začleniť do pravidelných porád vedenia alebo rokovaní predstavenstva ako 1 – 2 hodinové alebo ho zorganizovať samostatne až v rozsahu 8 hodín. Školenie obsahuje upozornenie na zodpovednosť vedenia úradu (spoločnosti) za povinnosti vyplývajúce k ochrane informácií z legislatívy a súčasne oboznamuje so zásadami bezpečnej manipulácie s informáciami (ochrana proti odposluchu, mobilná komunikácia ...).