

Ochrana dat a informací

Podniková data a informace jsou v dnešní době nejcennějším obchodním artiklem a kdo je vlastní a umí jich správně využít, má v mnohdy tvrdém konkurenčním boji značnou výhodu. Tato skutečnost s sebou však nese rizika nechtěných úniků a krádeží dat způsobených at' již vnějšími útočníky jako je konkurence, tak i mnohdy interními pracovníky. Ochrana podnikových dat a informací proto patří mezi priority v zájmech organizace po celém světě a neměla by být nikdy opomíjena.

Možné dopady krádeže či úniku informací a dat

- klesá důvěryhodnost
- finanční ztráty na smluvních pokutách
- ohrožení činnosti společnosti
- nedodržení platné legislativy

V současnosti nabírají pojmy jako Data Leakage Protection nebo Data Loss Prevention patřičnou váhu a důležitost. Již mnohokrát jsme se na příkladech velkých mezinárodních hráčů mohli přesvědčit, jak může být poškozena jejich pověst a jak jednoduše se k nim mohou zákazníci obrátit zády, pokud dojde ke ztrátě, poškození nebo jinému zneužití dat jejich zákazníků.

Chránit svá data však neznamená jen uzamknout si notebooku heslem, či opatřit soubor heslem. Oblast ochrany dat a informací je mnohem komplexnější. Obsahuje celou řadu interních pravidel a instrukcí, stejně jako využití vhodného SW a možností šifrování splňující nejpřísnější armádní standardy. Pomůžeme Vám s implementací systému ochrany dat.

Přínosy Ochrany dat a informací

- striktní nastavení uživatelských přístupů
- nastavení klasifikačního schématu a pravidel
- zavedení funčního systému šifrování dat
- dodržení platné legislativy k ochraně informací

“ Ochrana informací a dat na prvním místě při plánování každé organizace.

5 základních principů ochrany dat

- Zpracovávat data a informace společnosti pouze v nejnútnejším rozsahu a dodržovat u toho platné podnikové instrukce a příslušnou legislativu.
- Data a informace uchovávat pouze z jasného a specifického účelu.
- Data mají být aktuální a nezměněná. Přístup k nim musí být řízen a musí být dostupná v okamžiku, kdy je to vyžadováno.
- Data a informace by neměla by být uchovávány déle, než je nezbytně nutné pro jejich zpracování.
- Implementovat technická a organizační opatření k zabránění neautorizovanému nebo nelegálnímu zpracování dat a zároveň by měla data ochránit před ztrátou, zničením nebo poškozením.