

Základní informace o pojištění kybernetických rizik



V současnosti jsou stále častější hackerské útoky na informační systémy nejrůznějších institucí a firem. Také požadavky na ochranu a zabezpečení osobních údajů klientů jsou stále vyšší. Nabízíme komplexní pojištění kybernetických rizik pro případ hackerského útoku či nároku souvisejícího s ochranou (nejen) osobních údajů a souvisejících sankcí od ÚOOÚ. Nové nařízení EU o ochraně osobních údajů (GDPR) navíc přímo ukládá povinnost adekvátně zabezpečit osobní data a v případě podobného útoku a absence zabezpečení hrozí vysoké pokuty.

Ztráta dat, důvěry zákazníků a často i finančních prostředků může být pro vaše podnikání fatální.

Pro koho je pojištění určeno

- pro všechny kdo uchovává osobní i jiná data svých zákazníků, pacientů, žáků, zaměstnanců a obchodních partnerů a pracují s nimi. Mohou to být i další „chráněné“ informace, např. to, co je předmětem obchodního tajemství, což pro mnoho firem je klíčové a důležité.

Co pojištění kryje

- škody na datech v elektronické podobě, nefunkčnost počítačového systému
- náklady regulatorního řízení
- náklady public relations – obnovu dobrého jména
- odpovědnost za újmu způsobenou únikem dat v elektronické podobě
- přerušování provozu (volitelné připojištění)

Aby byla škoda z pojištění likvidní, musí nastat tzv. kybernetický incident

- poškození, zničení, ztráta nebo odcizení dat v elektronické podobě způsobené úmyslným jednáním jako např.:
 - hackerský útok, malware, ransomware
 - nespokojený nebo zhrzený zaměstnanec vynese data v elektronické podobě
- nedbalostní pochybení vedoucí k poškození či ztrátě dat v elektronické podobě, např.:
 - zaměstnanec omylem pošle dokument s citlivými osobními údaji klienta na neoprávněnou osobu
 - zaměstnanec nechá PC nebo notebook bez dozoru a v nezabezpečeném režimu

- DOS útok – úmyslné přetížení nebo zahlcení počítačového systému, které způsobí odepření služby (nefunkčnost, zablokování systému)

Rozšířené krytí kybernetických rizik

- náklady na znalce v oblasti kybernetiky při podezření na neoprávněné vniknutí do systémů společnosti
- zveřejnění digitálního obsahu v jehož důsledku dojde k neúmyslnému narušení autorského práva, plagiátorství, zásahu do soukromí či zásahu do pověsti právnické osoby nebo důstojnosti fyzické osoby
- ztráty vzniklé vydíráním prostřednictvím počítačové sítě
- ztráty způsobené výpadkem počítačového systému v důsledku selhání zabezpečení

Toto pojištění je pro všechny, kteří chtějí být připraveni na rostoucí kybernetické hrozby a na novou EU směrnici GDPR.

Pro vypracování nabídky je nezbytné vyplnění dotazníku.