



Poradenství v oblasti kybernetické bezpečnosti pro kraje a obce.

Podporujeme Váš úřad již více než 30 let. Digitalizujte s námi!

Pomáháme krajům a obcím splnit nové požadavky zákona o kybernetické bezpečnosti a směrnice NIS2. Nabízíme právní a IT podporu, která zajistí soulad s legislativou a ochrání před kybernetickými hrozbami.

Proč využít naše služby?

- > **Zákonné povinnosti:** Nová legislativa NIS2 a český zákon zavádí povinnost zavést systém řízení kybernetické bezpečnosti. Nedodržení může vést k sankcím až do výše 250 milionů Kč.
- > **Řízení dodavatelů:** Veřejné subjekty musí chránit nejen své systémy, ale také dodavatelský řetězec prostřednictvím smluvních ustanovení a kontrol.

Klíčové benefity

- > **Revize bezpečnostní dokumentace:** Aktualizace interní dokumentace v souladu s novými požadavky.
- > **Právní poradenství:** Analýza smluv s dodavateli a zavedení povinných ustanovení.
- > **IT bezpečnostní služby:** Technická analýza bezpečnostních opatření a jejich audit.
- > **Komplexní přístup:** Propojení právního a IT poradenství pro efektivní řízení kybernetické bezpečnosti.
- > **Minimalizace rizik:** Identifikace a snížení kybernetických rizik a prevence sankcí.

Naše služby zahrnují

- > **Analýzu smluv s dodavateli:** Kontrola smluv podle nové legislativy a doplnění povinných bezpečnostních ustanovení.
- > **IT bezpečnostní audit:** Posouzení a zlepšení bezpečnostních opatření u dodavatelů.
- > **Implementaci technických opatření:** Zabezpečení sítí, správa identit, šifrování a bezpečnostní monitoring.
- > **Revizi a tvorbu bezpečnostní dokumentace:** Úpravy a aktualizace dokumentů v souladu s legislativou.
- > **Školení a vzdělávání:** Školení zaměstnanců o kybernetických hrozbách a řízení dodavatelů.

Proč zvolit nás?

- > **Individuální přístup:** Přizpůsobíme služby potřebám Vašeho úřadu a jeho dodavatelského řetězce.
- > **Ochrana před škodami:** Snižujeme riziko kybernetických incidentů.
- > **Prevence sankcí:** Pomáháme dodržet všechny povinnosti a vyhnout se sankcím.



Kybernetické útoky se čím dál častěji zaměřují na organizace veřejné správy, které uchovávají obrovské množství citlivých dat. Naše řešení Vám pomohou tyto situace nejen detekovat, ale také eliminovat.



Kybernetický útok typu malware zasáhl jednu z jihočeských nemocnic, která navíc neměla správně nastavené zálohování.

Se **zálohováním Geetoo S3** získáte spolehlivé zálohování všech Vašich dat v bezpečném cloudovém úložišti.



Riziko kybernetických útoků ohrožuje nejen online účty, ale i celý lokální systém, čímž může zablokovat komunikaci organizace s klienty.

Portálové řešení Safety4file garantuje bezpečnou distribuci souborů z Vaší organizace ke koncovým uživatelům.



Agenda **eCYS** je klíčovým nástrojem pro **systémové řízení kybernetické bezpečnosti** – pokrývá procesy od sestavení katalogu hrozeb přes implementaci kontrolních opatření až po vzdělávací modul pro ISMS.



Balíček **Phishingové kampaně** pomůže **odhalit bezpečnostní rizika** ve Vašich systémech, a to s **přehlednými reporty** a analýzami.

