simac

Vyberte správný Systém pro řízení informační bezpečnosti

s partnerem Simac Technik ČR

Informační a kybernetická bezpečnost je dnes již nezbytnou součástí managementu každé organizace. Jedná se o důležitou součást fungování podniku i veřejné správy a její organizace se stává integrální součástí činnosti každé složky. Jednotlivé složky Systému pro řízení informační bezpečnosti (ISMS) jsou popsány mezinárodní normou ISO/IEC 27001. Ta poskytuje model ustavení, implementování, zpracovávání, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik a úrovní akceptace rizik organizace navržených k efektivnímu ošetření a řízení rizik ztráty dostupnosti, důvěrnosti a integrity informace.

V čem vám pomůžeme

Zákon o kybernetické bezpečnosti:

Zákon je speciálním případem implementace informační bezpečnosti v organizacích a informačních systémech důležitých pro fungování informační a komunikační infrastruktury země. Tyto organizace a systémy jsou taxativně určeny v navazujících vyhláškách.

Bezpečnostní standard PCI DSS:

(Payment Card Industry Data Security Standard) představuje mezinárodní pravidla definující podmínky nakládání s údaji držitelů platebních karet, které jsou obsaženy na platebních kartách.

Vyhlášky ČNB:

Ty stanovují některé povinnosti bank a finančních institucí v oblastech kybernetické a informační bezpečnosti a řízení operačních rizik. A právě ty by měly být v souladu s celkovou bezpečnostní politikou organizace.

Výhody našeho přístupu

- Poskytujeme komplexní konzultace, máme k dispozici adekvátní studie
- Implementujeme ISMS v organizaci, aby odpovídal Zákonu o kyberbezpečnosti (ZoKB)
- Vytvoříme a zrevidujeme podnikové dokumentace pro ISMS, ZoKB, GDPR i ePrivacy
- Zajistíme bezpečnostního manažera, interního auditora, architekta, manažera, auditora kybernetické bezpečnosti
- Analyzujeme rizika i dopady
- Testujeme zranitelnosti, které se v podniku mohou vyskytovat (penetrační, sociální inženýrství) v sektorech jako jsou bankovnictví, zdravotnictví, telekomunikace či veřejná správa

Jaké jsou hlavní důvody zavádění kybernetické bezpečnosti?

Ekonomický

mezi nejvýznamnější rizika patří zastavení produkce a z toho přímo vzniklé ztráty z hlediska ušlé fakturace nebo odškodnění klientům.

Kybernetická kriminalita

organizace se může stát snadno obětí kriminálních činů, jako je vydírání či zcizení dat o klientech konkurencí nebo nespokojeným zaměstnancem.

Průmyslová špionáž

pro organizace je v dnešní době extrémně důležité dokázat si udržet svoje know-how, strategické záměry, obchodní nabídky, výsledky interního výzkumu a vývoje.

Ztráta kredibility

podvržení internetových stránek organizace, zastavení výroby nebo zneužití dat klientů mohou mít velmi negativní dopad na spokojenost stávajících zákazníků nebo odrazení nových.

Legislativní důvody

vedle stávající legislativy (ZoKB), je to i postupné zavádění evropské legislativy (GDPR, ePrivacy, eIDAS), která stanovuje odpovědnosti i na další veřejné a soukromé subjekty.

simac

Simac Technik ČR, a. s.
Radlická 740/113c, 158 00 Praha 5
Email: consulting@simac.cz **Tel.:** +420 283 061 281

www.simac.cz