IMPLEMENTACE KYBERNETICKÉ BEZPEČNOSTI

Téma kybernetické bezpečnost úzce souvisí s dynamickým rozvojem moderních technologií a jejich každodenním využíváním ve všech oblastech lidského působení. To, co dříve bylo obyčejnou elektronikou nebo ještě dále v čase pouhým mechanickým předmětem, má dnes „vlastní mozek", což je nesporně velkou výhodou a ulehčením obrovského výčtu činností, potažmo povinností.
Nové technologie, ale v dnešním světě neustále čelí bezpečnostním hrozbám, jejichž objem stále narůstá, a proto je zavedení kyberbezpečnosti nutností každé společnosti.

Cílem implementace kybernetické bezpečnosti do společnosti je zavedení:

- bezpečnostních opatření,
- schopnosti detekovat a reagovat na kybernetické hrozby,
- hlášení bezpečnostních incidentů,
- systému opatření k reakci na kybernetické bezpečnostní incidenty.

NAŠE SLUŽBY

- **Posouzení stavu dokumentace** související s řízením bezpečnosti informací v rozsahu požadavků Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a Vyhlášky č. 82/2018 o kybernetické bezpečnosti ve formě rozdílové analýzy a vytvoření plánu projektu ISMS.
- **Propracování nebo rozšíření stávající bezpečnostní strategie** na základě zjištěných rozdílů pro dosažení shody s požadavky zákona ve formě politik a navazující dokumentace dle rozsahu, hranic a vazeb ISMS, zahrnující minimálně:
  - Vytvoření nebo aktualizace politik v rozsahu přílohy č. 5 Vyhlášky č. 82/2018 sb.,
  - Identifikaci informačních a podpůrných aktiv,
  - Vyhodnocení a vypracování analýzy rizik, odpovídající požadavkům normy ČSN ISO/IEC 27001:2014,
  - Plánu zvládání rizik formou návrhu opatření navazujících na výsledky analýzy rizik,
  - Prohlášení o aplikovatelnosti dokládající, které části ISMS a jak jsou zavedené.
- **Vytvoření programu a postupů interního auditu kybernetické bezpečnosti** systémů kritické informační infrastruktury a významných informačních systémů v rozsahu dle vyhlášky č. 82/2018 o kybernetické bezpečnosti a jeho provedení s popisem zjištění neshod a vytvořením plánu na jejich vyřešení.
- **Provedení penetračního testu** pro odhalení chyb a zranitelností a výstupní je zprávy s popisem průběhu, identifikovanými zranitelnostmi a jejich vyhodnocením podle závažnosti a doporučeními k jejich odstranění.
- **Zavedení řízení vztahů s dodavateli** informačních systémů a technologií v kontextu systému řízení bezpečnosti v celém životním cyklu odběratelsko-dodavatelského vztahu v souladu s požadavky Zákona o kybernetické bezpečnosti.

PROČ JE KYBERBEZPEČNOST DŮLEŽITÁ?

Významní dodavatelé nejsou v drtivé většině dostatečně řízeni a kontrolováni a tento nedostatek je při kontrole NÚKIB hodnocen jako Významný viz ukázka části auditního záznamu provozovatele VIS v souvislosti s § 8 odst. 1 písm. f) a g), odst. 2 písm. b) až d) VKB:

„Významní dodavatelé nejsou dostatečně řízeni a kontrolováni. Smlouvy uzavřené s významnými dodavateli jsou z pohledu KB nedostatečné, neobsahují relevantní oblasti z přílohy č. 7 VKB či jakákoliv jiná pravidla a požadavky…"

„V rámci smluvních vztahů s významnými dodateli nejsou stanoveny způsoby a úrovně realizace bezpečnostních opatření a určení vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření…"

„V rámci řízení významných dodavatelů není prováděno pravidelné hodnocení rizik a kontrola zavedených bezpečnostních opatření u poskytovaných plnění. Vzhledem k tomu, že rozsah bezpečnostních opatření není ve smlouvách definován a pravidla pro dodavatele nejsou v tuto chvíli závazná, neexistují kritéria případné kontroly/auditu dodavatele, jejichž dodržování by bylo posuzováno."

Kombinace výše uvedených nedostatků představuje pro organizace riziko, a proto je nezbytné se jím zabývat a aktivně pracovat na jeho řešení.

PRO KOHO JSOU NAŠE SLUŽBY URČENY?

Naše poradenské služby jsou určeny hlavně pro správce informačních systémů kritické informační infrastruktury, správce komunikačních systémů kritické informační infrastruktury a správce významných informačních systémů.

Tomáš Kubíček, Partner
e tomas.kubicek@bdo.cz
m +420 737 210 682

Audit | Daně | Poradenství
www.bdo.cz