ZABEZPEČENÍ IT INFRASTRUKTURY:
STUDIE STAVU A ANALÝZA SHODY

DATA SYS

Narušení zabezpečení IT infrastruktury mívá pro společnosti fatální následky. Výsledkem bývá **přerušení provozu, únik dat, finanční ztráta, poškození značky i dobré pověsti a problémy s úřady**. S přibývající digitalizací každodenní procesů je velmi prozíravé mít zpracovanou analýzu a implementovanou strategii předcházení a řešení narušení zabezpečení IT infrastruktury.

Nechcete-li čekat na reálný bezpečnostní incident, jedinou správnou odpovědí je:
STUDIE STAVU A ANALÝZA SHODY

CO TO JE?

V obecné rovině jde o nezávislé posouzení, zda je informační bezpečnost organizace společně s bezpečnostními charakteristikami systémů nastavena v souladu s akceptovanou dobrou praxí a s platnou legislativou, zejména pak s tzv. zákonem o kybernetické bezpečnosti a jeho doprovodnou vyhláškou.

CO JE DŮLEŽITÉ?

- S každoročním nárůstem kybernetických útoků by zabezpečení IT infrastruktury mělo být jednou z hlavních priorit.
- Pro povinné orgány a osoby stanovuje zákon o kybernetické bezpečnosti řadu povinností v oblasti zajištění bezpečnosti informačních systémů.
- Bezpečnostní opatření by měla být zavedena až na základě analýzy současného stavu a hodnocení rizik.
- Spolupráce s externími subjekty může být podmíněna doložením bezpečnostní politiky a dodržováním bezpečnostních opatření.
- Zavedení vhodných bezpečnostních opatření působících proti informačním hrozbám a útokům zajišťuje důvěrnost, integritu a dostupnost zpracovávaných informací.
- Z pohledu bezpečnosti je potřeba dbát i na to, aby bylo IT oddělení dostatečně provázáno s „byznysem".
- Vhodná analýza přispívá k řízení dodavatelů a minimalizaci rizik spojených s dodávkami služeb externích subjektů.

NAŠE ŘEŠENÍ PŘINÁŠÍ:

- **posouzení požadavků zákona o kybernetické bezpečnosti,**
- **zohlednění doporučení dle normy ISO 27001 a ISO 27002,**
- **mapování a analýza aktuálního stavu IT infrastruktury,**
- **zpracování katalogu primárních aktiv,**
- **příprava bezpečnostní dokumentace,**
- **hodnocení kybernetické bezpečnosti,**
- **plán zvládání rizik,**
- **zajištění shody v souladu s GDPR, ZKB atd.**

VAŠE BEZPEČNOST SI ZASLOUŽÍ DALŠÍ STRATEGICKÝ KROK

ZREALIZUJEME PRO VÁS STUDII STAVU A ANALÝZU SHODY NA MÍRU!

77 % firem nemá plán pro případ kybernetického bezpečnostního incidentu

pravidla pro firemní IT bezpečnost zná jen **12 %** zaměstnanců

83 % zaměstnanců důvěřuje e-mailovým přílohám

30 % uživatelů klikne na odkaz v phishingovém mailu

70 % úspěšných průniků začíná u koncového uživatele

63 % úniků dat je spojeno se slabými, defaultními nebo zcizenými hesly