Služby ověření úrovně kybernetické bezpečnosti

a porovnání s požadavky zákona 181/2014 Sb. - Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.

V pátek 29. 8. 2014 byl ve Sbírce zákonů pod č. 181/2014 Sb. publikován zákon o kybernetické bezpečnosti. Přijetím této normy Česká republika reaguje na rizika zneužití informačních a komunikačních technologií s potenciálně značnými škodami.
Zákon odráží vzrůstající závislost společnosti na informačních technologiích, kdy riziko zneužití těchto technologií může mít rozsáhlé dopady a může vést ke značným škodám. Všechny vyspělé země, mezi něž Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů. Zákon bude účinný od 1. ledna 2015.

Protože problematika kybernetické bezpečnosti je s ohledem na okruh dotčených odborností značně rozsáhlá, připravili jsme pro vás službu, která vám usnadní orientaci v tom, jakým způsobem se tato věc dotýká právě vaší organizace a nakolik je vaše organizace připravena vypořádat se s povinnostmi, které jí touto normou budou uloženy.

Zkušení odborní konzultanti vám pomohou ve spolupráci s vámi provést

Ověření organizačních opatření (§ 5, odst. 1 zákona)

- **Identifikace existujícího systému řízení bezpečnosti informací organizace**
- **Identifikace způsobu řízení rizik organizace**
- **Identifikace bezpečnostní politiky organizace a její aplikace**
- **Identifikace úrovně organizační bezpečnosti organizace a její aplikace**
- **Identifikace aplikované úrovně bezpečnostních požadavků na dodavatele**
- **Identifikace existujícího systému řízení informačních aktiv organizace**
- **Identifikace aplikovaných zásad bezpečnosti lidských zdrojů organizace**
- **Identifikace aplikovaných zásad řízení provozu a komunikací organizace**
- **Identifikace aplikovaných zásad řízení přístupu a bezpečného chování uživatelů**
- **Identifikace aplikovaných zásad řízení akvizic, vývoje a údržby**
- **Identifikace aplikovaných zásad zvládání kybernetických bezpečnostních událostí a incidentů**
- **Identifikace aplikovaných zásad řízení kontinuity činností**
- **Identifikace aplikovaných zásad kontroly a auditu**

Výstupem této činnosti bude souhrnný dokument, popisující rozsah toho, jaké má vaše organizace předpoklady i slabiny v připravenosti na plnění povinností z hlediska shora uvedeného zákona, který rovněž identifikuje případné hlavní nedostatky vaší připravenosti i jak se s nimi lze vypořádat.
Zákon ovšem nepracuje jen s organizační složkou bezpečnosti, ale definuje i technická opatření, kterými mají být opatření realizována. I zde vám můžeme pomoci. Tým zkušených techniků a odborníků společně s vámi může podobně provést srovnání i v oblasti technických opatření.

Ověření technických opatření (§ 5, odst. 2 zákona)

- **Identifikace aplikované úrovně fyzické bezpečnosti**
- **Identifikace aplikovaných nástrojů pro ochranu integrity komunikačních sítí**
- **Identifikace aplikovaných nástrojů pro ověřování identit uživatelů**
- **Identifikace aplikovaných nástrojů pro řízení přístupových oprávnění**
- **Identifikace aplikovaných nástrojů pro ochranu před škodlivým kódem**
- **Identifikace aplikovaných nástrojů pro zaznamenávání činností**
- **Identifikace aplikovaných nástrojů pro detekci kybernetických bezpečnostních událostí**
- **Identifikace aplikovaných nástrojů pro sběr a vyhodnocování kybernetických bezpečnostních událostí**
- **Aplikační bezpečnost**
- **Identifikace aplikovaných kryptografických prostředků**
- **Identifikace aplikovaných nástrojů pro zajištění vysoké úrovně dostupnosti**
- **Identifikace aplikovaných postupů a nástrojů pro zajištění bezpečnosti průmyslových a řídících systémů**

Také výstupem této činnosti bude souhrnná analýza, popisující rozsah toho, jaké má vaše organizace předpoklady i slabiny v připravenosti na plnění povinností z hlediska shora uvedeného zákona. I zde jsme schopni identifikovat případné hlavní nedostatky vaší připravenosti i způsoby a varianty postupů, jak se s nimi lze vypořádat.

S přihlédnutím k rozsahu pojednávaných částí předpokládáme jako nejvhodnější formu prezentace výstupů shora uvedených identifikací mimo uvedených dokumentů i formu prezentace a workshopu s vedením vaší organizace.

Předpokládaná doba realizace, při plné součinnosti objednatele je 2-3 pracovní dny.

Službu jsme připravili ve spolupráci s předními odborníky na oblast kybernetické bezpečnosti, se kterými rovněž spolupracujeme na přípravě a prosazování konceptu Aktivní bezpečnosti sítě.

Výhody:

- ✓ **služba poskytovatele s odborným zázemím**
- ✓ **výstupy ve struktuře a rozsahu porovnatelné s požadavky zákona**
- ✓ **ověřitelnost**
- ✓ **pevná cena**
- ✓ **čas**