Zákon o kybernetické bezpečnosti

Spadá i vaše organizace do působnosti zákona o kybernetické bezpečnosti (ZoKB)? Chcete splnit jeho požadavky efektivně a navíc tím posílit informační a ICT bezpečnost vaší organizace?

Nabízíme vám efektivní soubor nástrojů a služeb, s jejichž pomocí spolehlivě obstojíte před požadavky zákona. Nejde nám jen o bezmyšlenkovité formální naplnění jeho požadavků, ale snažíme se o výběr a implementaci nástrojů a bezpečnostních opatření takovým způsobem, který je nejvhodnější pro vaši organizaci a současně bude mít maximální a dlouhodobý efekt.

Krátce k zákonu

Zákon o kybernetické bezpečnosti č. 181/2014 Sb. je platný od 1. 1. 2015. Do konce roku 2015, nebo do jednoho roku od svého určení, musí dotčené subjekty zapracovat do svých systémů řízení informační bezpečnosti povinnosti, které se na ně vztahují. Dotčenými subjekty dle zákona jsou:

- poskytovatelé služeb a provozovatele sítí elektronických komunikací a významných sítí,
- správci informačních a komunikačních systémů spadajících do kritické informační infrastruktury,
- správci významných informačních systémů.

Zákon a návazné prováděcí právní předpisy definují pro vybrané subjekty povinnost implementovat bezpečnostní opatření v oblasti organizační a technické. Navíc definují povinnosti těchto subjektů při hlášení a reakci na tzv. kybernetické bezpečnostní incidenty v interakci s určenými orgány CERT (Computer Emergency Response Team).

Řešení od AEC

Na základě našich dlouholetých zkušeností s implementací systémů řízení informační bezpečnosti, bezpečnostních nástrojů a technologií, navrhneme podle výsledků vstupní analýzy vhodný způsob naplnění požadavků zákona a souvisejících vyhlášek. Doporučíme nástroje odpovídající velikosti, typu a potřebám organizace. Navrhneme související procesy a bezpečnostní opatření tak, aby efektivně navazovaly na stávající procesy a byly v souladu s businessem organizace. Dále vypracujeme podrobný implementační plán, dohlédneme na jeho realizaci nebo realizujeme na klíč a na konec provedeme detailní kontrolu výsledného celkového stavu. Jsme schopni podpořit organizaci i v rámci periodických aktivit, případně je přímo realizovat formou outsourcingu.

Náš cíl

Vytvořit v organizaci systém pro efektivní plnění požadavků zákona, který bude mít předpoklady pro dlouhodobé fungování bez násilných zásahů do již fungujících procesů.

Procesy spojené s informační bezpečností je třeba chápat v širokých souvislostech - nejen technických, ale také organizačních, personálních a dalších. Efektivní ochrana informací vyžaduje detailní znalost existujících slabin informačního systému a bezpečnostních rizik.

Specialisté a konzultanti společnosti AEC jsou připraveni organizacím pomoci v různých oblastech informační bezpečnosti:

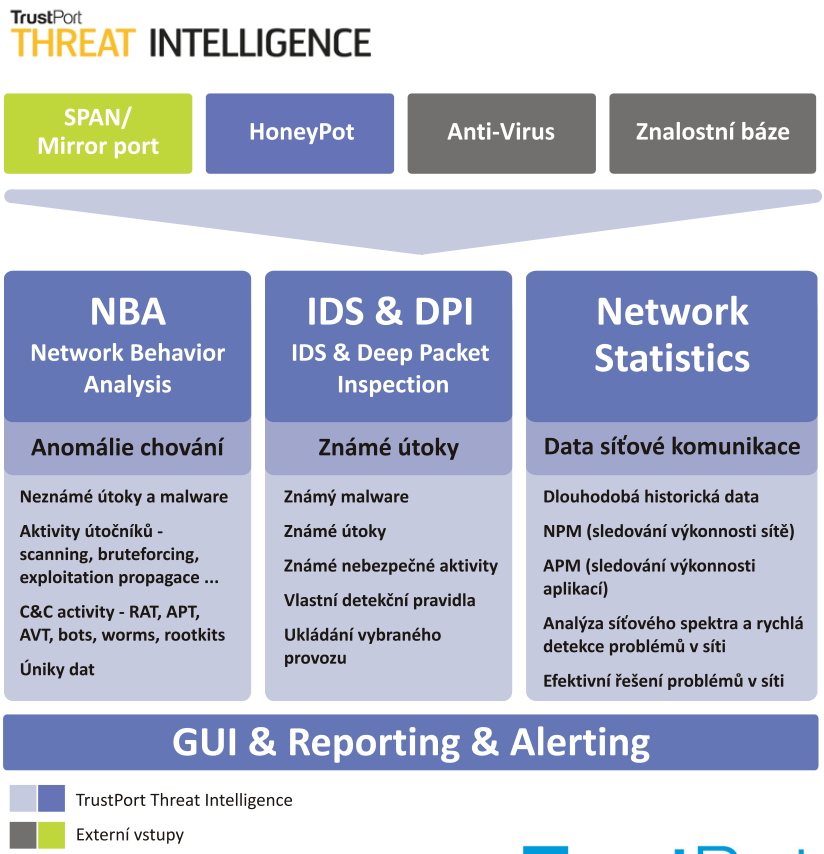
- identifikace a ohodnocení informačních rizik;
- definice a implementace vhodných protiopatření;
- návrh a implementace systému řízení informační bezpečnosti;
- penetrační testy, prověrky a audity informačních systémů;
- návrh bezpečnostních procesů a zpracování dokumentace
- implementace nástroje pro monitoring síťového toku a vyhodnocování kybernetických bezpečnostních událostí.

Vybrané společnosti musí od ledna 2015 používat nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který by v souladu s bezpečnostními potřebami měl splňovat následující požadavky:

- integrovaný sběr a vyhodnocení bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování;
- pravidelnou aktualizaci pravidel pro vyhodnocování událostí a včasné varování, aby byly omezovány případy tzv. „false positive“;
- zajištění odolnosti informačního systému vůči incidentům, které by mohly snížit dostupnost.
- monitoring provozu infrastruktury a chování uživatelů.

TrustPort Threat Intelligence umožňuje naplnit požadavky zákona o kybernetické bezpečnosti a zároveň přispívá ke zvýšení zabezpečení celé sítě. Využívá přitom nejrůznější detekční mechanismy (včetně vlastních), metody umělé inteligence, intrusion detection (IDS) či síťovou behaviorální analýzu (NBA).

Nástroj nabízí ochranu před moderními útoky, jakými jsou například malware psaný na míru, tzv. zero-day útoky, botnety nepodchycené běžným antivirem, kybernetická špionáž či sociální inženýrství.



TrustPort
Keep IT Secure

Přínosy řešení

- Trvalý přehled o stavu a rizikovosti sítě.
- Automatická detekce kybernetických bezpečnostních událostí a incidentů v síti.
- Významná úspora práce při řešení kybernetických incidentů.
- Snížení následků bezpečnostních průniků.
- Možnost forenzní analýzy i měsíce zpětně.
- Snadná kontrola účinnosti reaktivních opatření.
- Možnost poloautomatického hlášení vybraných incidentů určeným CERT orgánům.
- Řešení od české firmy – lokální podpora.
- Jednoduchá implementace do stávajícího systému.

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz