system boost

Nabídka komplexní bezpečnostní analýzy v Domažlické nemocnici

Připraveno pro **Centrum sdílených služeb Klatovská nemocnice, a.s.**

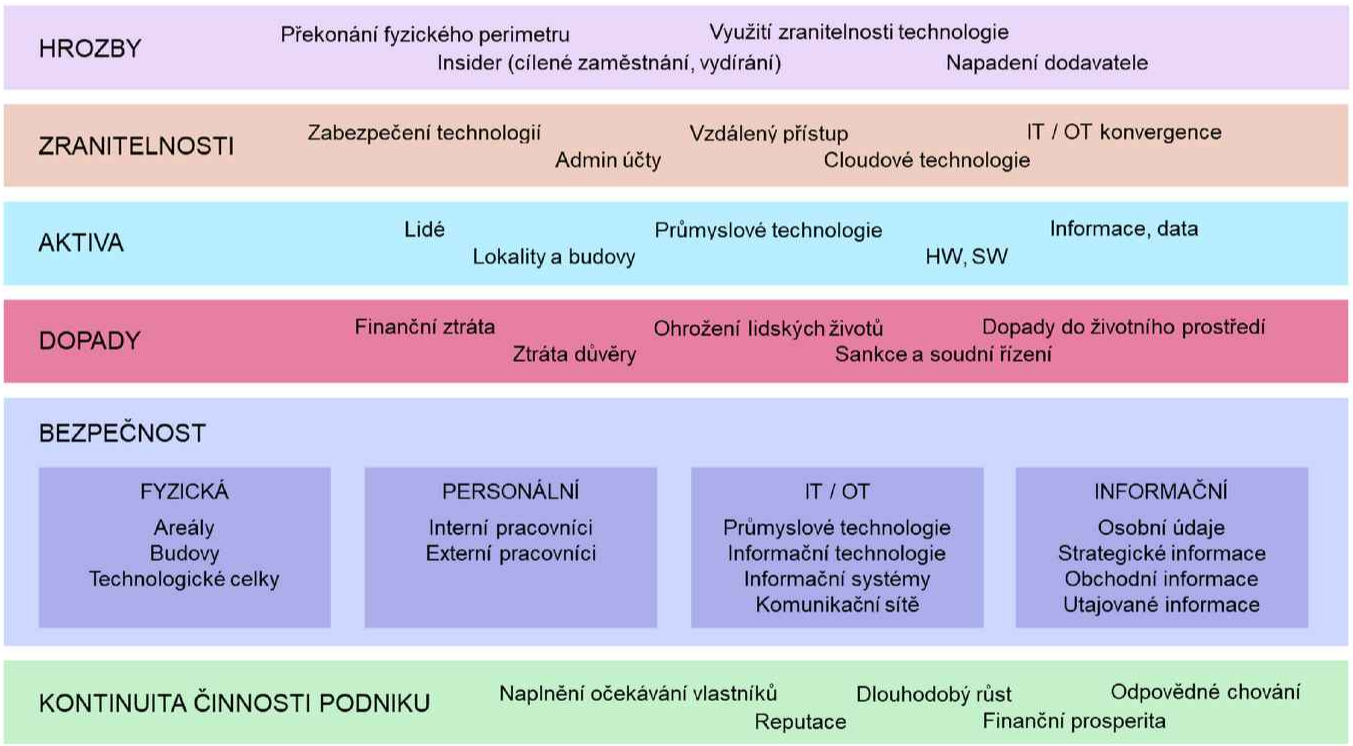
15.9.2022

system boost a.s.
Na Pankráci 1683/127, 140 00 Praha 4
IČO: 04641574
[redacted]

Úvod do problematiky

Přístup ke zdravotní péči patří mezi nedílné součásti našeho každodenního života. Bezpečnost je sice již nedílnou součástí procesů a kultury organizace, ale pro efektivní řízení bezpečnosti je nutné přijmout celou řadu adekvátních opatření. Pro tyto účely je vhodné využít dobrou praxi a některou z technických norem z oblasti bezpečnosti informací. Na tuto oblast myslí i zákon o kybernetické bezpečnosti č. 181/2014 Sb., kde v §2 odstavci i) a bodě 5 jmenuje zdravotnictví jako základní službu, pro kterou je potřeba zajistit odpovídající úroveň ochrany (fyzické, kybernetické i informační).

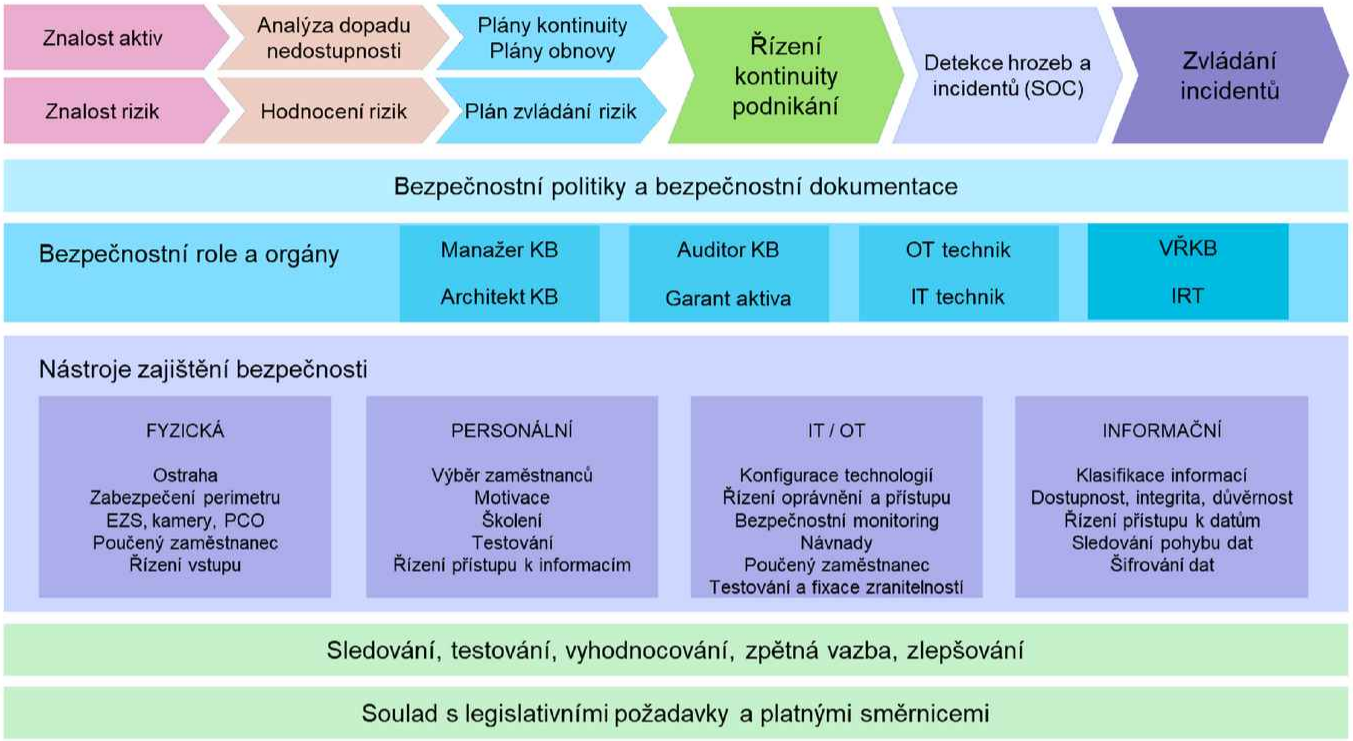
Bezpečnost je klíčová oblast pro zajištění kontinuity činností a služeb, je definována hrozbami, které přes zranitelnosti aktiv působí na aktiva formou méně či více závažných dopadů, před kterými je nutné se chránit. Obecné schéma bezpečnosti je uvedeno na obrázku níže. Řádné pokrytí všech těchto oblastí vyžaduje velké finanční, personální i časové zdroje, které v nemocnicích bohužel v současné době chybí. Je tedy vždy třeba hledat ekonomicky efektivní cesty, které zajistí řešení alespoň těch klíčových oblastí s největším potenciálním dopadem.



Zdravotnická zařízení využívají celou řadu specializovaných nemocničních informačních systémů využívaných při zabezpečování chodu zařízení, při výkonu lékařských úkonů, komunikace s pojišťovnami nebo pacienty. A všechny tyto systémy je nutné chránit. Kromě toho musí být chráněny také tisíce zařízení, které jsou součástí internetu věcí. Patří mezi ně inteligentní výtahy, inteligentní systémy vytápění, ventilace a klimatizace (HVAC), ale i infuzní pumpy, zařízení pro vzdálené monitorování pacientů a další.

Úvod do problematiky

Oblast řízení bezpečnosti je velmi široká (jak ukazuje následující schéma) a platí, že žádné z témat nesmí být opomenuto, protože jedna otevřená dvířka znamenají selhání celého systému.



Společnost system boost a.s. se v rámci řešení výzev v oblasti bezpečnosti nezaměřuje pouze na úzce zaměřenou část problematiky, ale problém vnímá v širším kontextu, který zahrnuje i netechnologické aspekty ovlivňující bezpečnost organizace. Z tohoto důvodu se v rámci řešení otázky kybernetické bezpečnosti zaměřuje na identifikaci zranitelných oblastní z technického, systémového, zaměstnaneckého, dodavatelského ale i klientského/uživatelského pohledu. Navrhovaná opatření se vždy snaží maximálně reflektovat specifické požadavky klienta a zjištění odhalená v průběhu analýz a fyzického testování kybernetického zabezpečení organizace.

Předmět nabídky

Předmětem nabízeného projektu je komplexní bezpečnostní analýza organizace Domažlická nemocnice a.s. Cílem projektu je posoudit všechny aspekty bezpečnosti organizace, odhalit hlavní zranitelnosti s potenciálně významným dopadem rizika a navrhnout vhodná a adekvátní opatření s ohledem na důležitost organizace, ale také dostupné zdroje a možnosti organizace.

Bezpečnostní analýza se, v souladu s požadavky zadavatele, zaměří na následující oblasti:

- Fyzická Bezpečnost
  - Fyzickou bezpečnost tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup do definovaného perimetru a definovanému okruhu informacím, popřípadě přístup nebo pokus o něj zaznamenat. Obsahem této analýzy bude popis lokality, popis zabezpečení vstupního prostoru, jak probíhá autentizace při vstupu do vyhrazených prostor, kde jsou umístěny klíče od prostor, EZS a kamerový systém, PCO, kde je umístěn a jak je zabezpečen router atp.
- Procesní bezpečnost
  - Procesní bezpečnost představuje soubor zejména organizačních opatření s cílem realizovat procesní kroky v souladu s normami a legislativou, a minimalizovat procesní pochybení při výkonu zdravotnických a podpůrných procesů. V rámci analýzy se zaměříme na prověření existujících opatření procesní bezpečnosti a aktuálního provázání procesní mapy organizace na organizační směrnice a zejména definovaná opatření. Samozřejmě prověříme také stav a aktuálnost analýzy rizik a dopadů jakožto podkladu pro definovaná opatření.
- Technická bezpečnost
  - Technická bezpečnost představuje soubor opatření s cílem zajistit shodu stavu zařízení (zdravotnických, režimových, bezpečnostních apod.) a příslušných technických norem. V rámci analýzy prověříme aktuální přístup a směrnice řízení technické bezpečnosti, aktuálnost dokumentace a pravidla jejího přezkumu. Dále pak prověříme úplnost stávající dokumentace s ohledem na postupy kontroly zařízení, postupy a školení pro řádné používání zařízení (i v souladu s bezpečností práce), atd.
- IT bezpečnost s návazností na ZoKB
  - ZoKB (zákon o kybernetické bezpečnosti) a VoKB (vyhláška o kybernetické bezpečnosti) definuje povinnosti subjektů v oblasti informační bezpečnosti. Prověříme stav dokumentace, organizačních a technických opatření v souladu se všechny požadavky specifikovanými v ZoKB a jeho prováděcích vyhláškách ve vztahu ke kontextu organizace. Zaměříme se zejména na aktuální stav analýzy aktiv, BIA, analýzy rizik, plánu zvládání rizik a řízení kontinuity (včetně existence, kvality, aktuálnosti a znalosti plánů kontinuity a plánů obnovy).
  - V rámci analýzy se zaměříme nejen na IT infrastrukturu, ale také na OT infrastrukturu (zdravotnická zařízení, průmyslovou komunikaci, proces Change managementu na OT prostředcích apod.)
- Ochrana osobních údajů
  - Ochrana osobních údajů patří mezi základní prvky informační bezpečnosti, zejména s ohledem na klasifikaci těchto informací a požadavky na jejich ochranu s ohledem na GDPR a zákon o ochraně osobních údajů. Tuto oblast tedy budeme řešit v rámci analýzy řízení informační bezpečnosti, klasifikace informací, příslušných pracovních postupů, vazby informací na technické prostředky, úroveň osvěty apod.

Výstup a cena

Výstupem analýzy bude závěrečná zpráva, která bude obsahovat posouzení celkového stavu analyzovaných oblastí bezpečnosti v prostředí organizace. Závěrečná zpráva bude členěna následovně:

- Manažerské shrnutí,
- Účel a předmět provedení analýzy,
- Analýza aktuálního stavu oblastí bezpečnosti, zejména se zaměřením na
  - oblast organizačních požadavků a opatření na IT a OT prostředí,
  - oblast technických požadavků a opatření na IT a OT prostředí,
- Shrnutí analýzy a systematizace zjištění,
- Doporučení dalšího postupu (prioritizace).

Časovou náročnost realizace analýzy bezpečnosti v Domažlické nemocnici, zpracování závěrečné zprávy a prezentace závěrů projektu určeným osobám zadavatele odhadujeme na 4-8 týdnů dle dostupných podkladů a součinnosti, kterou na počátku projektu po vzájemné dohodě definujeme.

Nabídková cena za zpracování analýzy bezpečnosti v Domažlické nemocnici činí 100 000 Kč bez DPH.

Doporučení nad rámec předmětu nabídky

Nad rámec specifikovaných požadavků zadavatele pro tuto nabídku doporučujeme v budoucnu realizovat i ověření skutečného stavu zabezpečení perimetru organizace a její IT a OT infrastruktury, což poskytne nejen ověření závěru zde nabízené analýzy, ale také skutečné zranitelnosti organizace proti cílenému útoku.

Jako základní techniky pro posouzení zranitelnosti organizace proti vnějšímu i vnitřnímu útoku nabízíme:

- Zpracování digitálního profilu organizace a analýzy uniklých hesel, tedy uvěření volně dostupných informacích z internetu, darknetu a darkwebu o uživatelích, jejich přístupových údajích; o systémech, jejich verzích a případných zranitelnostech; plánky budov, jejich technického vybavení, zázemí atd.
- Bezpečnostní sken perimetru s cílem identifikace maximálního množství zranitelností, které byly zveřejněny ve veřejných databázích. V rámci skenování využíváme renomované komerční i open-source nástroje, kterými jsou například Nessus, OpenVAS, OWASP ZAP, BurpSuite, Nikto a další. Nálezy následně posoudíme dle celosvětově uznávaného standardu NIST CVSSv3.
- Ověření možnosti uzamčení účtů a napadení VPN s cílem ověření, zda může být VPN zneužita k napadení společnosti a k průniku útočníka skrze perimetr.
- Digital Red Team Operations (neinvazivně) z pracovní stanice společnosti, kdy se za pomoci běžných hackerských technik pokusíme o provedení eskalace oprávnění v rámci operačního systému a o následnou kompromitaci systémů, na které je tento systém napojen
- Penetrační test z našeho pracovního zařízení s VPN přístupem do společnosti (simulace přístupu dodavatele), kdy provedeme sadu útoků a skenů interní sítě, abychom ověřili, kam dodavatel může a čeho by se mohl zmocnit útočník, jestliže by kompromitoval počítač dodavatele nebo získal přístup dodavatele do VPN.
- Spear Phishing a Spear Vishing.

Vybrané referenční projekty

[redacted]

Posouzení stavu řízení, provozu a rozvoje ICT

Realizace: 06 / 2021 – 09 / 2021

Cílem projektu bylo provedení IT auditu společnosti Nemocnice Plzeňského kraje a provozovaných zdravotnických zařízení.

Analýza stavu řízení bezpečnosti pro oblast OT

Realizace : 10 / 2021 – 02 / 2022

Cílem projektu bylo zpracování analýzy stavu řízení fyzické a kybernetické bezpečnosti v oblasti OT.

Fyzická bezpečnost - Definice primárních aktiv SSV

Realizace: 09 / 2021 – 10 / 2021

Cílem projektu bylo zpracování definice, evidence a popisu primárních a sekundárních aktiv Skupiny Severočeská voda v rámci koncernového projektu fyzické bezpečnosti.

Zpracování digitálního profilu nemocnice

Realizace: 05 / 2021 – 06 / 2021

Cílem projektu bylo sestavení digitálního profilu společnosti a související profilování k identifikaci relevantních, zneužitelných či využitelných informací. Ze získaných informací byla vytvořena mapa artefaktů, slabin nebo chyb v konfiguraci, které by mohl potenciální útočník zneužít při přípravě a plánování kybernetického útoku na společnost.

Zpracování BIA

Realizace: 02 / 2022 – 03 / 2022

Cílem projektu bylo definovat klíčová aktiva, na jejichž ochranu musí společnost zacílit své úsilí, aby činnost společnosti zůstala zachována v požadovaném rozsahu a kvalitě. Následně byla nad těmito klíčovými aktivy zpracována analýza rizik pro identifikaci hlavních rizik, která je třeba řešit a ošetřit, a dále analýza dopadu.

Penetrační test mobilní aplikace

Realizace: 12 / 2021 – 01 / 2022

Cílem projektu byla realizace testování API vrstvy určené pro provoz mobilní aplikace společnosti dle celosvětově uznávaného standardu OWASP. Byla zpracována kontrola všech oblastí definovaných v metodice OWASP s hlubším zaměřením se na exfiltraci dat z aplikace, chyby v session managementu a možnosti manipulace s API vrstvou pomocí metod injektáže.

Vybrané referenční projekty

[redacted]

Zpracování analýzy rizik a BIA

Realizace: 09 / 2021 – 12 / 2021

Cílem projektu bylo definovat klíčová aktiva, na jejichž ochranu musí společnost zacílit své úsilí, aby činnost společnosti zůstala zachována v požadovaném rozsahu a kvalitě. Následně byla nad těmito klíčovými aktivy zpracována analýza rizik pro identifikaci hlavních rizik, která je třeba nějakým způsobem řešit a ošetřit, a dále analýza dopadu.

Zpracování nové bezpečnostní dokumentace dle VoKB

Realizace: 06 / 2022 – 08 / 2022

Cílem projektu bylo zpracovat bezpečnostní dokumentaci včetně organizačních a technických opatření v souladu s požadavky zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti.

Outsourcing role MKB

Realizace: 05 / 2022 – doposud

Předmětem projektu je poskytování komplexních služeb role manažer kybernetické bezpečnosti v souladu s požadavky zákona o kybernetické bezpečnosti.

Testování kybernetické bezpečnosti

Realizace: 06 / 2022 – 09 / 2022

Cílem projektu bylo realizovat balíček bezpečnostních testů pro ověření skutečné zranitelnosti organizace. Mezi testy bylo provedeno mapování digitálního profilu a uniklých hesel, testování zranitelnosti organizace, digital red teaming pracovní stanice a digital red teaming přístupu dodavatele.

Strategie kybernetické bezpečnosti skupiny Veolia

Realizace: 10 / 2021 – 03 / 2022

Předmětem projektu bylo zpracování komplexní strategie kybernetické bezpečnosti. Strategie kybernetické bezpečnosti skupiny Veolia se zaměřením na oblast IT a průmyslových řídících systémů (OT) navrhuje dlouhodobý a udržitelný přístup v oblasti řízení bezpečnosti pro IT a OT.

Audit kybernetické bezpečnosti

Realizace: 05 / 2021 – 06 / 2021

Cílem projektu bylo posouzení aktuálního stavu nastavení systému řízení bezpečnosti ve společnosti a zpracování doporučení dalšího postupu.