Bezpečnostní monitoring zdravotnických zařízení

-

Jak na to

Michal Čábela

Nutné kroky k bezpečnému zdravotnictví, část III.

Agenda

1	2	3	4	5
Představení	Rizika	Technika	Integrace	Příklad

Představení: Michal Čábela

Cyber Security Lead

Cyber Security team – Czechia & Slovakia

Deloitte Advisory s.r.o.

Rizika: opakování

Oblast zabezpečení zdravotnických prostředků (modality, analyzátory a další) je pro poskytovatele zdravotní péče dosud **neřešeným problémem**. Tyto prostředky však představují kritická kybernetická rizika.

Na tyto prostředky se pro jejich neřešené zranitelnosti útočníci stále častěji zaměřují.

Ke kompromitaci zdravotnických prostředků však nemusí dojít pouze cílenou aktivitou útočníka, ale i jen aplikací automatizovaného nástroje, který se samovolně šíří internetem. Dalším vektorem útoku jsou nekontrolované VPN přístupy dodavatelů zdravotnických prostředků.

S kompromitací zdravotnických prostředků jsou spojená významná rizika pro jejich provozovatel:

Rizika spojená s IT

- Výpadek fungování služeb IT a zdravotnických prostředků
- Propagace hrozeb do infrastruktury partnerských organizací
- Únik osobních a citlivých dat pacientů
- Významné náklady nutné na obnovu po incidentu
- Nesoulad s regulatorními požadavky

Ostatní rizika

- Škody na zdraví nebo životech pacientů a zaměstnanců
- Právní postihy
- Poškození dobrého jména
- Zvýšení pojistných nákladů

Rizika: běžné problémy

(Ne)znalost prostředí	Řízení bezpečnosti	Životní cyklus zařízení	Bezpečnost dodavatelů	Zodpovědnost
• Neznalost všech zdravotnických a jiných IT prostředků, která jsou organizací provozována • Neznalost struktury sítě (topologie) z pohledu kybernetické bezpečnosti • Nedostatečné personální obsazení oblasti IT a kybernetické bezpečnosti a kumulace znalostí u jednotlivců	• Neplnění legislativy, standardů, procesů a postupů vyžadovaných pro řízení kybernetické bezpečnosti • Nedostatečná znalost, zkušenost a počet pracovníků zodpovědných za oblast kybernetické bezpečnosti • Nedostatečné povědomí o kybernetických rizicích a jejich dopadech mezi zaměstnanci	• Zastaralá zařízení s ukončenou podporou bezpečnostních záplat • Nejasné vlastnictví (z pohledu IT) zařízení v síti • Organické a spontánní pořizování a připojování nových zařízení do sítě bez znalosti jejich zabezpečení	• Nedostatečné nebo žádné bezpečnostní požadavky na třetí strany • Nedostatečná kontrola aktivit třetích stran • Nekontrolované VPN přístupy • Vytváření “shadow IT” bez vědomí a kontroly centrální správy IT a kybernetické bezpečnosti	• Nejasné pochopení důsledků potenciálního kybernetického útoku na organizaci • Veškerá formální zodpovědnost přenesena na statutárního zástupce organizace • Nedostatečné smluvní vztahy, které nezahrnují oblast kybernetické bezpečnosti

Rizika: Běžné chyby

- Plochá síťová infrastruktura
- Neexistující dynamický katalog všech zařízení v infrastruktuře
- Minimální investice v oblasti IT Bezpečnosti
- Neexistují kontrola dodavatelů přes VPN
- Chybějící zodpovědnost za oblast IT bezpečnosti
- Chybějící plán “B” – nedostatečná příprava na incident
- Nesledování chování IT infrastruktury
- Neexistují proces řízení změn

Technika: jaké nástroje použít

Armis	Cyber MXD	Medigate
Claroty	Cyberio	Dragos

Nástroje umožňující identifikaci a průběžný monitoring IoMT (“Internet of Medical Things”)

Technika: společné vlastnosti

Bezagentní nástroj, který odhaluje a sleduje zařízení, která jsou zapojená do sledované sítě. Bezpečnostní monitoring probíhá pasivně sledováním a vyhodnocováním dat, která generují ostatní prvky v monitorované síti. Pro provoz není nutné instalovat dodatečný software na sledovaná zařízení.

3 základní funkční celky:

1. Inventarizace	2. Správa rizik	3. Monitoring

• Identifikace všech zařízení nezávisle na jejich umístění a připojení v monitorované síti (výrobce, model, operační systém, a další)
• Klasifikace zařízení - Managed, Unmanaged, IoMT a IoT
• Obohacení dat skenerů zranitelností a nástrojů pro inventarizaci
• Nezávislé na prostředí a odvětví
	• Identifikace rizik a zranitelností s využitím rozsáhlé databáze CVE zranitelností a základních bezpečnostních praktik
	• Adaptivní hodnocení rizik
	• Sledování porušování pravidel na základě míry rizika
	• Sledování úniků osobních dat
		• Aktivní hlášení
		  • hrozeb a jejich napravování
		  • anomálií chování zařízení
		  • výskytu malware
		  • narušení bezpečnostních pravidel
		  • nestandardní komunikace
		• Poskytování kontextu zařízení do všech bezpečnostních nástrojů a procesů

Technika: Procesní zajištění

1. Inventarizace

- Inventarizace, katalogizace a verifikace všech zařízení v síti – vytvoření registru zařízení nebo CMDB
- Definice kritičnosti připojených zařízení
- Definice ochranných opatření zajišťující míru kybernetické bezpečnosti v závislosti na kritičnosti jednotlivých zařízení
- Návrh bezpečné architektury
- Posouzení aktuálnosti softwarového vybavení zařízení a jeho správa
- Zavedení procesů správy aktiv

2. Správa rizik

- Zavedení komplexního a kompletního řízení rizik v prostředí zdravotnických zařízení
- Definice procesů zvládání rizik a hrozeb
- Vytvoření risk registru
- Vytvoření plánu zvládání rizik a hrozeb
- Mitigace identifikovaných rizik
- Definice automatizovaných procesů zvládání a reportingu rizik

3. Monitoring

- Sledování datových toků mezi zařízeními
- Provázání s nadřazeným SIEM nástrojem a integrace celého řešení do SOCu organizace
- Reportování aktuálních zranitelností s rozřazením do kategorií dle jejich kritičnosti
- Analýza síťových aktivit a druhů komunikace mezi zařízeními
- Tvorba návrhu strategie odstranění zranitelností a prioritizace
- Návrh postupů pro remediaci zranitelnosti
- Verifikace odstranění zranitelnosti
- Hlídání stávajících i všech nových hrozeb
- Řešení nových bezpečnostních upozornění a zneužitých hrozeb
- Asistence při aktivně probíhajícím útoku
- Definice automatizačních procesů a integrací

Metamorfosa

Integrace: Jak na to

	GAP Analýza	TOM	PoC	Procesy	Rollout
Trvání	4 týdny	6 týdnů	8 týdnů	8 týdnů	4 týdny
Aktivity	• Pochopení prostředí organizace • Identifikace slabých míst • Zhodnocení v kontextu očekávaných změn v oblasti monitoringu medicínských zařízení • Příprava doporučení pro mitigaci rizik	• Výběr vhodného nástrojového vybavení • Popis cílového řešení – Target Operating Model (“TOM”) • Příprava plánu implementace všech následujících fází včetně změn v procesech a organizaci řízení IT a kybernetické bezpečnosti • Definice prostředí pro integrace Proof of Concept (“PoC”)	• Implementace PoC zvoleného nástrojového vybavení • Zkušební provoz na omezeném rozsahu infrastruktury • Příprava závěrečné zprávy o provedeném PoC	• Realizace potřebných úprav ostatních IT a bezpečnostních procesů tak, aby bylo možné adoptovat monitoring medicínských zařízení v plném rozsahu • Integrace monitoringu medicínských zařízení do ostatních struktur organizace – typicky SOC.	• Příprava prostředí pro kompletní nasazení zvoleného řešení • Validace všech předchozích kroků • Integrace zvoleného řešení do organizace
Výstupy	• Report GAP analýzy • Akční plán	• Vybraný monitorovací nástroj • Popis řešení pro integraci • Plán integrace	• Zkušenosti z provozu PoC • Závěrečná zpráva a doporučení	• Upravené nebo nové procesy řízení IT / kybernetické bezpečnosti	• Dokumentace řešení • Funkční monitoring všech medicínských zařízení v organizaci

Příklad: Fakultní nemocnice Plzeň

Inventarizace

Systém je schopný rozpoznat jak medicinská tak i IT zařízení a je možné sytém použít k vytvoření IT a medicinského inventáře pro FNP.

Systém dokáže uspokojivě kategorizovat rozpoznaná zařízení a zobrazit jejich detailní parametry v závislosti na informacích poskytnutých v zachyceném datovém provozu.

Bezpečnostní alerty

Systém schopný generovat relevantní bezpečnostní aletry pro medicinská, tak i IT zařízení v rozsahu který je očekáván od pasivního nástroje pro bezpečnostní sledovaní provozu.

Během sledování systém pracoval s přednastavenou sadou pravidel, která produkovala výše zmíněné alerty.

Aby bylo dosaženo co nejlepších výsledků v produkčním nasazení, je nutné bezpečnostní pravidla pravidelně udržovat a rozvíjet.

Zranitelnosti

Systém je schopen identifikovat zranitelnosti ze zachyceného provozu a to nejen pro medicinská ale i pro IT zařízení.

Pomocí tohoto systému tak FNP může zavézt management zranitelnosti pro medicinská zařízení a tím zamezit hrozbě potencionálního zneužití aktivních zranitelnosti.

Kontakt: Michal Čábela

mcabela@deloittece.com

+420 775 214 115

https://www.linkedin.com/in/michal-cabela/