Otázky, odpovědi a komentáře

Q: Jak se Mendel profiluje z pohledu Zákona o kybernetické bezpečnosti?

A: *GreyCortex Mendel je jedním z technických opatření, které pokrývá především následující požadavky vyhlášky 82/2018 sb. v platném znění:*

$18 Bezpečnost komunikačních sítí *zajišťuje* ***plně*** *požadavky uvedené u písmena*

b) tj. zajistí řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě a

d) tj. aktivně blokuje nežádoucí komunikaci

§ 21 Ochrana před škodlivým kódem *zajišťuje* ***plně*** *požadavky uvedené u písmena*

a) tj. s ohledem na důležitost aktiv zajišťuje použití nástroje pro nepřetržitou automatickou ochranu u bodu číslo

5. komunikační sítě a prvků komunikační sítě a

6. obdobných zařízení,

e) *tj.* provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů *zajišťuje* ***plně, nebo napomáhá splnit*** *požadavky uvedené u písmena*

a) tj. zaznamenává bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému a

b) tj. na základě hodnocení důležitosti aktiv aktualizuje rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.

§ 23 Detekce kybernetických bezpečnostních událostí *zajišťuje* ***plně***

§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí *zajišťuje* ***plně nebo napomáhá splnit*** *uvedené požadavky.*

***§ 25 Aplikační bezpečnost** zajišťuje **plně nebo napomáhá splnit** požadavky uvedené u*

> *(2) tj. Povinná osoba dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací a transakcí před*
>
> *a) neoprávněnou činností a*
>
> *b) popřením provedených činností.*

***§ 28 Průmyslové, řídicí a obdobné specifické systémy** zajišťuje **plně** mimo fyzické bezpečnosti v bodu b).*

Q: Na základě jakého paragrafu je zaplacení výkupného trestným činem?

A: Po důkladné diskusi z právního hlediska je nutné konstatovat, že by samotná platba ransomu bez dalšího neměla být považována dle českého trestního práva za trestně-právně relevantní jednání. Rovněž neoznámení takového činu nelze obecně bez dalšího považovat za trestný čin, pokud se neprokáže, že došlo k napomáhání takovému jednání ze strany zodpovědné osoby organizace, která o platbě rozhodla. Nicméně řada zemí skutečně považuje zaplacení výkupného po útoku ransomwmare za trestný čin, některé to omezují pouze na kritickou infrastruktury.

Jinou otázkou ovšem je, jestli zaplacení pomůže. Řada ransomware vůbec dešifrování neumožňuje anebo je napsána tak špatně, že to nelze provést.

Dále se v případě zaplacení výkupného organizací veřejné správy ten, kdo by zaplatil, může vystavit minimálně riziku porušení povinnosti z hlediska nakládání s veřejnými zdroji s péčí řádného hospodáře. Obdobně pak může podobná situace nastat také v komerční sféře, kdy by vlastníci mohli vinit statutárního zástupce z porušení povinností pečovat o svěřený majetek s péčí řádného hospodáře.

Q: RDP servery zmiňované v prezentaci vystavené do internetu byly přímo v LAN, nebo tam měli nějakou DMZ od lokální sítě oddělenou firewallem?

A: V tomto případě byly RDP servery vystavené přímo do internetu. Více informací v čase 33:50

Q: Často se mluví o problematických zdravotnických systémech (modalitách, medical devices), ale byly už zaznamenány/potvrzeny nějaké úspěšné průniky přes tato zařízení?

A: V České republice o nich nevíme. Zařízení samotná kompromitovaná byla, ale k průniku přes ně zatím u nás nedošlo.

Comment: Zatím mám pocit (z veřejně dostupných informací), že vektorem útoku bylo administrativní rozhraní přístupné z Internetu či lidský faktor.

A: Doložení konkrétních případů není snadné, a to z několika důvodů: v případě útoku nastává v nemocnici poněkud nepřehledná situace, dochází k vypnutí a odpojení zařízení, pokud nemocnice nemá nástroj pro monitorování sítě, nemá mnoho možností zpětně rozklíčovat celou historii útoku od okamžiku průniku; není neobvyklé, že se zpočátku snaží

interní tým zakrýt skutečný stav, takže než se k síti dostane odborník, jsou napáchány ještě následné škody, které opět ztěžují forenzní analýzu. V neposlední řadě - pokud se i zjistí skutečný vstup, je to pod NDA, takže nelze sdílet s veřejností. Stručně - nemáme jednoznačný konkrétní podložený důkaz v rukou o takovém incidentu.

Comment: Jeden z méně známých problémů zařízení pořizující snímky je to, že často ukládají data někam na internet, aby bylo umožněno sdílet informace mezi zdravotnickými zařízeními.

A: Tato problematika by si zasloužila samostatnou diskusi; mnohdy jsou také ukládána v jiném zařízení z důvodu nedostatečné storage v dané nemocnici.

Comment: Pokud jde o hardening IoMT je tam stejná situace jako s aktualizací - výrobce dá ruce pryč od čehokoliv, co neschválí. A ne nepodstatný moment - jak aktualizace tak hardening je možné dělat v OT prostředí jenom během odstávky - má vůbec nemocnice odstávky

A: Ano, i nemocnice musí občas přistoupit k odstávce, i z důvodu aktualizace NIS. Ale dostane takové prostor třeba 1x za rok, obzvlášť v dnešní "covid" době, tzn. bezpečnostní patche aplikují skutečně s dlouhým odstupem od zjištění.

Q: Jaký vendor je nejčastěji používán v nemocnicích pro FW?

A: Na tuto otázku nedokážeme bohužel odpovědět, protože neznáme infrastrukturu nemocnic a pokud ji známe, tak není v naší kompetenci ji zveřejňovat. Velmi často se ale potkáváme s produkty společnosti Fortinet.