Z praxe: Bezpečnost a monitoring nemocniční sítě

Závislost na informačních technologiích je zejména v prostředí nemocnic velmi vysoká. Nedávné kybernetické incidenty v českých nemocnicích názorně ukázaly, jak dokáže nefunkční IT ochromit jejich fungování.

Nemocniční infrastruktura totiž představuje specifické heterogenní prostředí, které je velmi obtížné spravovat, zabezpečit a také udržet aktualizované. Nachází se zde velké množství různých operačních systémů, aplikací a jiných proprietárních systémů. Například rentgen – to není v podstatě nic jiného než PC s typicky zastaralým operačním systémem na bázi Windows nebo Linux. Na takové zařízení však nemůžete nainstalovat antivirus, nemůžete nainstalovat aktualizace, ale zároveň jej potřebujete zabezpečit a připojit do nemocniční sítě. A podobných zařízení se v nemocnicích vyskytují desítky až stovky. Rizika jsou přitom vysoká. Od ochromení provozu přes úniky dat až po ohrožení života pacientů z důvodů omezení zdravotní péče.

Řešení problematiky provozu datové sítě v KNL

Pod Krajskou nemocnici Liberec (KNL) spadají celkem tři zařízení – v Liberci, Turnově a ve Frýdlantu. Cílem bylo propojit všechna zařízení a vytvořit homogenní síť pod jednou bezpečnostní architekturou a jednotným systémem.

„Původně jsme měli jen základní přehled nad síťovou infrastrukturou. Věděli jsme, že switch funguje a že jím něco protéká, uměli jsme vyhodnotit, že konkrétní linka je přetížená, a to bylo ve stručnosti vše. Chyběla komplexní viditelnost do sítě a že se něco děje, musela obsluha zjišťovat manuálně. Jednoduše chyběl nástroj, který by dokázal upozornit na podezřelou aktivitu uvnitř sítě, zachytit ji a případně také nahrát pro další analýzu,“ uvedl Michal Krejčí, vedoucí střediska ICT Turnov.

V rámci zavádění bezpečnosti se v Krajské nemocnici Liberec snažili poučit z většiny incidentů, které měli možnost vidět. Zajistili dostatečnou ochranu sítě zvenčí, aktualizovali firewally, nasadili nové řešení, nový analytický antivirus, který řešil i chování aplikací a uživatelů, dokázali detekovat zranitelnosti, skenovat prvky a vytvořili mnohonásobně více vnitřních segmentů sítě. Nicméně vždy je to o lidech a o tom, zda nakonec otevřou podezřelou přílohu nebo prozradí citlivé údaje, jako jsou login a heslo.

Museli tedy své bezpečnostní opatření doplnit o nástroj, který je schopný detekovat anomálie v síti, aktivně o nich informovat a taky je řešit. V podstatě je to jedna z věcí, kterou po vybraných nemocničních zařízeních vyžaduje i kybernetický zákon. Ten se aktuálně v ČR týká 16 zařízení, ale již se vedou diskuze o rozšíření určujících kritérií, což by se ve výsledku dotklo až 50 zařízení u nás.

Nasazení Flowmonu v Krajské nemocnici Liberec

Nakonec bylo vybráno a úspěšně nasazeno ve všech třech zařízeních řešení Flowmon. Hardwarové sondy jsou zde připojené přímo k hlavním core switchům (předávají do sondy sledované VLAN) a stejná situace je i ve virtualizačním prostředí, kde každý ESXi, každý virtuální server má svou sondu a jejich výstupy se sbíhají v jednom centrálním bodu – ve Flowmon kolektoru. Ten tedy vidí provoz napříč celou sítí a veškerý dodaný materiál zde efektivně zpracovává a ukládá pro další využití.

Jaké praktické problémy zde Flowmon pomáhá řešit:

1 Problémy s aplikací. Uživatelé hlásí problém s dlouhými reakcemi SW i pády aplikace. Ukázalo se, že jedna aplikace začala způsobovat výpadky na výstupních bufferech switchů. Po navýšení serverových kapacit a rychlostí se problém prohloubil. Flowmon na dvě kliknutí odhalil, kde je problém – 2 s latence. Nastavení QOS nebylo optimální a problém se posunul jinam. Došlo na úpravu topologie a upgrade access switche.

2 Retransmise. Rentgenová technika typicky generuje ohromné množství dat oproti běžnému provozu. Uživatel si na nic nestěžuje, ale problém se zbytečným opakováním přenosu zatěžuje všechny prvky v síti a zhoršuje provoz standardním aplikacím, kterým chybí šířka pásma. Flowmon přehledně ukáže zařízení s relativně vysokým přenosem dat, které mají problémy.

3 Detekce událostí. Pokud nemáte zkušeného experta, který může neustále sledovat vývoj na síti a z několika neúspěšných pokusů o přihlášení na SSH vyvodit, že pravděpodobně probíhá útok na servery, potřebujete nástroj, který to udělá za něj. Flowmon ADS sbírá data, srozumitelně informuje, že k něčemu dochází, a umí na zjištěné události aktivně zareagovat. Využívá se zde mimo jiné také k prověřování indikátorů kompromitace podle požadavků přicházejících z NÚKIB.