Jak je to možné?

Celé zdravotnictví bylo v bojové pohotovosti. Nemocnice proti globální pandemii rychle vybudovaly RED ZÓNY a připravily se na léčbu těžkých případů. Nepřítelem je neviditelná nanočástice neznámého viru COV-19. Šíří se rychle a nemilosrdně zabíjí.

Jak je ale možné, že si v této těžké době někdo dovolí napadnout informační infrastrukturu nemocnic, které jsou plné pacientů, nebo výzkumné ústavy, které usilovně hledají vakcínu proti COV-19? Proč ransomware gangy útočí v době, když celý svět trpí? Vždyť ani ve středověku si vojska navzájem neútočila na polní lazarety.

Od kyberútoku v nemocnici v Benešově uplynulo již téměř půl roku. Od kyberútoku na FN Brno to budou tři měsíce. Jak jsme se z útoků poučili a co jsme udělali, aby se to neopakovalo? V kyberprostoru ani u viru nejsou definované hranice. Bohužel doposud si nikdo nepřipouštěl negativní stránky moderních informačních technologií ani ohrožení z globálních pandemií.

Ale co je pro naše nemocnice nebezpečnější, kybernetický nebo biologický virus? Na detekci a prevenci COV-19 jsme investovali miliardy, ale kolik na boj s kybervirusy? Panika, ekonomické ztráty a dopad na pacienty jsou v obou případech podobné. Kybernetická bezpečnost je neviditelná. Nepotřebuje sice roušky, ale detekci a prevenci proti virům ano. Není založena na moderní chemii, ale na moderních, složitých a drahých technologiích. Ovládat ji můžou jen specializovaní odborníci na kyberbezpečnost, kterých je bohužel v České republice žalostně málo. Žádná nemocnice si ale sama ze svého rozpočtu nemůže dovolit platit super drahé technologie ani tým specializovaných analytiků a kybermanažerů.

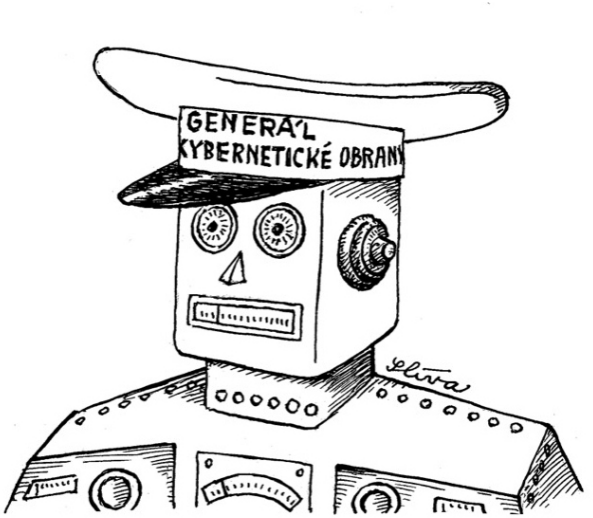
Je potřeba najít rozumný a ekonomicky zvládnutelný model sdílení ochrany kyberprostorů nemocnic. Tak jako z jednoho místa Řízení letového provozu hlídá bezpečnost vzdušného prostoru nad Českou republikou, je potřebné vybudovat „Speciální hlídání kyberprostorů nad zdravotnickými zařízeními“.

Jak a kdo by to ale měl realizovat? NÚKIB, MZ ČR, nemocnice samotné?

Na instituci nezáleží. Je však už nejvyšší čas, aby si kompetentní uvědomili, že poučení již bylo dost. Je potřeba konečně jednat. Neslibovat kyberaudity v nemocnicích, které se doteď pořádně neudělaly. Nepsat žádosti a výzvy. Nečekat na dotace z EU. Protože kdo bude platit škody z dalších kyberútoků? Nemocnice? Pacienti? My všichni. A to proto, že jsme nic pro obranu neudělali, resp. jsme kyberobranu svěřili lidem, kteří pro to nic nedělají.

V době COV-19 výrobní a obchodní společnosti a také úřady bleskově implementovaly nové mechanismy práce, tzv. homeoffice. Notebooky se staly nedostatkovým zbožím a raketově narostl počet VPN připojení. THP a administrativní pracovní síla „jede remote“.

Jaká je ale bezpečnost domácího homeoffice, mají všichni uživatelé bezpečná hesla a updatované operační systémy a aplikace? Jak je ochráněna online mediální komunikace (audio/video) mezi kolegy na homeoffice, aby nebyla kompromitována? Jak jsou zaměstnanci poučeni o sofistikovaných tricích spam



© Jiří Sliva & DSM

a phishing kampaní? Jak funguje systém proaktivní detekce a resortního varování proti kybernetickým útokům? Jak jsou ochráněni ICT administrátoři klíčových aplikací v nemocnicích, aby se neinfikovali nákazou biologického viru COV-19? Nedají se totiž rychle nahradit. Jsou pro nemocnici jedineční, klíčoví. Celá nemocnice je na nich závislá.

Pro zdravotnictví dozrál čas, potřebuje nový leadership v kybernetické obraně. Nemocnice potřebují pro kyberobranu jasné velení, ne úředníky rozesílající dotazníky, které nakonec neumějí vyhodnotit.

Moderní a rozumná architektura kybernetické obrany nemocnic, její důsledná a ekonomická implementace bude pak jasnou zprávou od CIO a kybermanažerů nemocnic, MZ ČR a NÚKIB pro ransomware gangy.

Ing. Dušan Chvojka, MBA
Náměstek ředitele pro ICT
Nemocnice Na Homolce