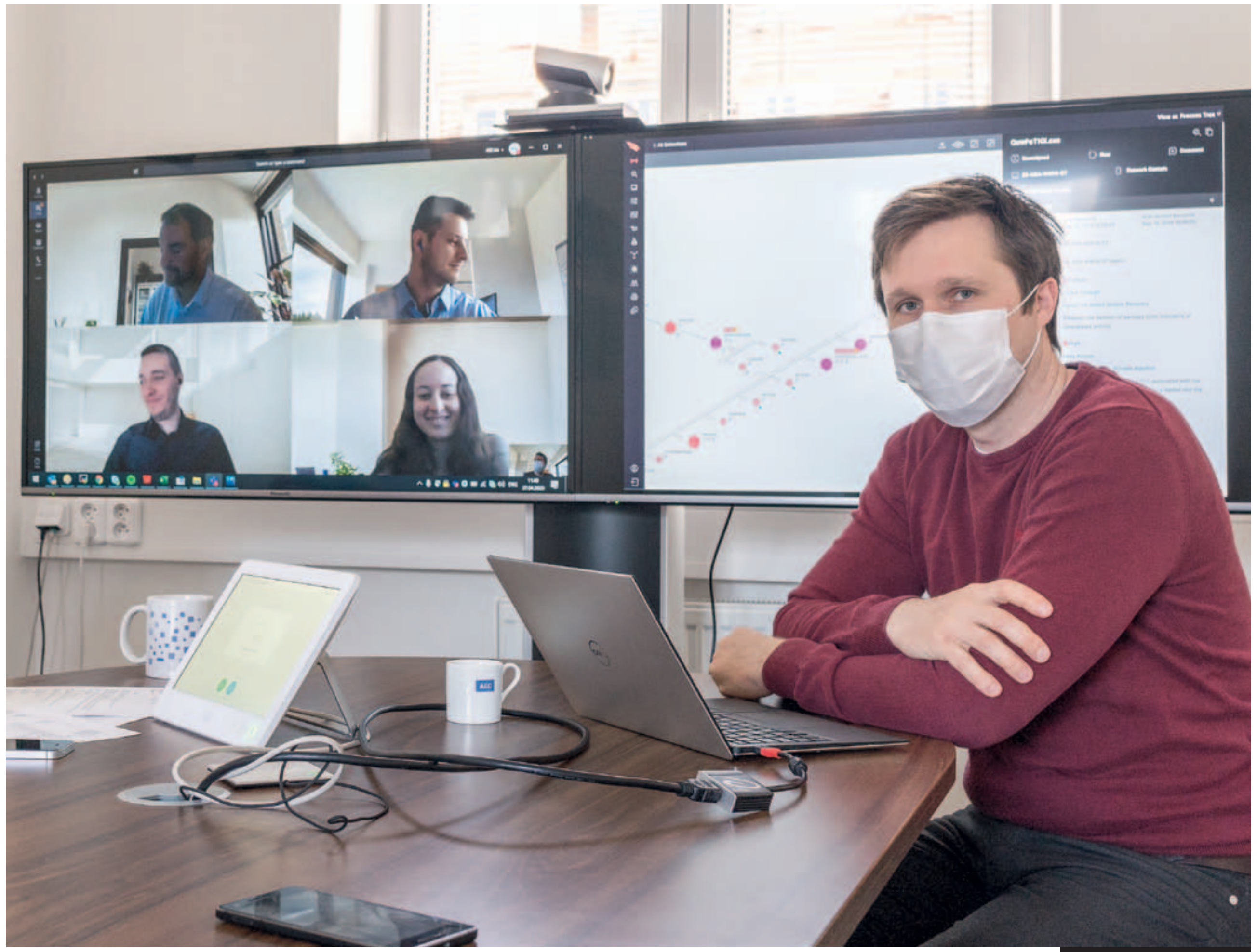
Nemocnice ochromily kybernetické útoky

Text David Zajíc
Foto AEC

Chod nemocnice zasažené kybernetickým útokem je paralyzovaný. Na sálech se operuje s tabletem nebo mobilem v ruce. Data mezi jednotlivými odděleními nemocnice a mezi nemocnicemi se posílají na CD anebo poštou. Podle Mateje Kačice, bezpečnostního experta společnosti AEC, je ale naštěstí zdravotnický personál na takovéto situace školený a péče o pacienty tedy přímo ohrožena není.



Matej Kačic, head of security technologies division, AEC

Myslím si, že pokud jsou bezpečnostní technologie správně poskládané a nasazené, dokážou už dnes efektivně chránit i svět IoT.

Během uplynulých měsíců hackeři úspěšně napadli několik českých nemocnic. Docházelo k tak závažným případům i v minulosti?
Incidenty ve zdravotnictví jsme samozřejmě řešili i dříve. Velmi často se však jednalo o snahu útočníků získat renomé v dané komunitě, pochlubit se velkým úlovkem, ceněnou trofejí. V současné době jsou běžnější dobře promyšlené útoky s cílem ukrást data, která by bylo možné následně použít při vydírání. Pohrůžka zveřejnění informací o zdravotních obtížích prominentního politika v době volební kampaně může být při vyjednávání o výši požadované částky poměrně pádným argumentem.

O jaké typy útoků šlo a byl způsob napadení v případě těch jednotlivých nemocnic stejný?
Vyšetřování všech nedávných incidentů ještě není uzavřeno, ale z toho, co momentálně víme, lze usuzovat na podobné scénáře. Prostřednictvím e-mailové komunikace se za pomoci techniky známé jako phishing dostal do interní sítě nemocnice takzvaný dropper. Tenhle velmi malý spustitelný soubor je standardně neškodný binární program, ale v tomto případě byl nasazen s jediným úkolem: stahovat a instalovat další nástroje a malware útočníka.

Útočníkem předem připravený a dropperem následně stažený malware se začal šířit přes zranitelné systémy napadené instituce. Ve zdravotnickém zařízení se většinou jedná o plochou a nekontrolovanou síť, takže šíření škodlivého programu zde probíhá velice rychle. Tak rychle, že celá síť je kompromitována během několika málo minut.

V případě některých zdravotnických zařízení byla už tak špatná situace umocněná ještě tím, že malware získal privilegovaný přístup do účtů správce celého systému a jeho administrátorů. Kvůli tomu se mohl rozšířit i na serverovou infrastrukturu a zálohy infrastruktury a dat.

Co se s takto napadenou nemocnicí děje? Co všechno selhává, co nefunguje?
Dovolím si to přirovnat k postupnému selhávání těžce nemocného organismu. Nejdříve jsou omezovány jednotlivé funkce, poté odumírají orgány a nakonec už nic nereaguje, nastává tma. Veškeré IT systémy napadené nemocnice přestanou fungovat, lékaři nemají přístup k nemocničnímu informačnímu systému, ke zdravotnické dokumentaci, nemohou vydávat recepty.

Nefunguje PACS, tedy technologie umožňující správu, archivaci a zobrazování rentgenových snímků či obrazové dokumentace z magnetické rezonance. Vzhledem k tomu, že nelze použít žádná zobrazovací zařízení, na sálech se operuje s tabletem nebo mobilem v ruce. Data mezi jednotlivými odděleními nemocnice a mezi nemocnicemi se posílají na CD anebo poštou. Zdravotnický personál je naštěstí na takovéto situace školený, pracuje skvěle, takže zdravotní péče přímo ohrožena není, ale běžný chod nemocnice je paralyzovaný.

Pro lékaře představuje v této situaci jeden z největších problémů nedostupnost starších dat a nemožnost sdílet informace, především snímky, ale i podrobné údaje z nejrůznějších vyšetření.

Daří se v těchto případech vypátrat útočníky? Na čem to závisí?
Nedaří se je dopadnout a mnohdy ani vypátrat. Moje zkušenosti jsou takové, že napadená organizace se zaměřuje primárně na zastavení útoku a rychlou obnovu. Je-li to možné, doporučuji provést tzv. triage. Tenhle proces spočívá ve vytřídění systémů podle určitých kritérií, kdy část z nich izolujeme, nasadíme specializované nástroje a některé ty separované systémy pak obětujeme s cílem přesně zmapovat prostředky, techniky a cíle útočníka. Představte si to tak, že díky tomuto postupu můžete kroky útočníka sledovat doslova v přímém přenosu. Následně může začít celkem složitá cesta trasování, která už probíhá ve spolupráci s policejními složkami.

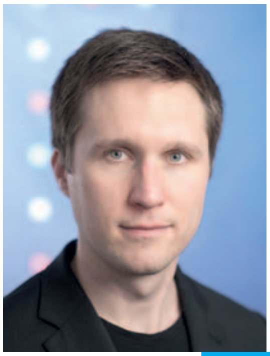
Zkušení útočníci samozřejmě naplno využívají veškeré dostupné anonymizační techniky, takže v některých případech je jejich odhalení téměř nemožné. Pokud se povede útočníka vypátrat, stane se to nejčastěji díky tomu, že se podaří najít jeho podpis, případně jiné silné vodítko. Úspěšní hackeři mívají silná ega, někdy jim to nedá a zanechají po sobě nějakou specifickou signaturu, rádi ji ukrývají do některého ze svých binárních programů. Záleží na každém detailu, mnohdy pro nás může být vodítkem drobná chybička, zapomenutý komentář ve zdrojovém kódu.

Jak je vůbec možné, že část kritické infrastruktury v České republice je stále v tak tristním stavu? Máme přece zákon o kyberbezpečnosti, který zavádí řadu opatření, na jejich dodržování dohlíží speciální úřad. Co je špatně?
Osobně si myslím, že nebýt zákona o kyberbezpečnosti, situace by byla ještě dramaticky horší. Je třeba si však uvědomit, že zákon o kyberbezpečnosti je jednoznačné minimum. Mnohé organizace tady stále ještě nemají ani základní IT, tuzemské nemocnice nedisponují dostatečnými preventivními opatřeními, která by vůbec mohla pomýšlet na ochranu před takovým typem útoků, jaké se tady teď udály.

A chválabohu, že máme Národní úřad pro kybernetickou bezpečnost, protože kupříkladu celá státní správa by byla bez jeho pomoci naprosto bezradná, o tom jsem přesvědčený. A to přesto, že jako každý úřad i tento potřebuje z principu na všechno o trochu více času.

Je třeba si uvědomit, že i ten nejlepší systém ochrany má jeden slabý článek a tím je vždycky lidský faktor. V nemocnicích nestojí v první linii ostřílení ajťáci, ale sestry a doktoři, kteří nejsou v oblasti bezpečnosti dostatečně kvalifikovaní, aby se mohli pokaždé rozhodnout správně.

Dalším hlavním problémem jsou finance. I když výzva Integrovaného regionálního operačního programu č. 10 je zaměřena speciálně na bezpečnost



ve zdravotnictví, mnohé organizace si za poskytované prostředky nakoupily hlavně infrastrukturní prvky, jako jsou disková pole, přepínače, virtualizaci apod. Podpora státu tady je, ale mnohdy je čerpána neefektivně. Podle mého názoru je klíčovým řešením dostat do těchto organizací odborníky, ale ti tam za tabulkový plat pracovat nebudou.

Vaši experti nedávno pomáhali s obnovou provozu počítačových systémů v brněnské fakultní nemocnici a poté i v Psychiatrické nemocnici Kosmonosy. V čem spočívá vaše role při takovém zásahu?

Náš úkol není nijak složitý. Během rychlého briefingu na místě musíme nasát veškeré informace, zhodnotit aktuální situaci a co nejdříve podniknout takové kroky, abychom útok v maximální možné míře oslabili. Jsme-li o to požádáni, nasazujeme forenzní nástroje, které nám pomohou podrobně zmapovat aktivity útočníka, a sestavujeme důkazní stopu.

V případě, že nejde o státní instituci, ale o soukromou firmu, máme v podstatě neomezené možnosti. Lidé z vedení jsou z nastalé situace většinou v šoku, obvykle komunikujeme s někým z topmanagementu. Ten dotyčný člověk od nás za pochodu dostává veškeré informace, může se na základě našich doporučení rychle rozhodovat o dalších krocích. A to včetně uvolnění finančních prostředků, například na nákup zahraničního specialisty nebo nějaké velice specifické technologie.

Všechno jde obvykle mnohem rychleji, protože čas znamená pro ty společnosti peníze. Na druhé straně, člověk by předpokládal, že soukromé firmy v České republice jsou na tom se zabezpečením systémů a dat mnohem dále než státní organizace, ale není tomu tak. Dokud nejsou napadeny, většinou šetří na nesprávném místě a kybernetickou ochranu těžce zanedbávají.

Jak tedy váš zásah v napadeném zařízení probíhá prakticky? Co je třeba udělat pro obnovu infrastruktury napadených systémů?

Poté co úspěšně eliminujeme útočníka, nastává plán obnovy kritických systémů. Je nutné si uvědomit, že v nezabezpečeném prostředí je velmi náročné identifikovat rozsah kompromitace systémů. I na první pohled zdravý systém může být napadnut, proto je nutné obnovit kompletně celé prostředí IT. Pokud jsou k dispozici funkční zálohy, obnovuje se většinou systém za systémem ze záloh. Velmi často se však stává, že útočník či malware poškodil anebo vymazal i zálohy. V tom případě se musí celé prostředí postavit, respektive nainstalovat úplně celé znovu.

Na některé informační systémy musí být povolány specializované firmy, což může celý proces obnovy pozdržet. My s touhle možností už dopředu počítáme a dokážeme celý proces zoptimalizovat tak, aby na sebe jednotlivé kroky navazovaly a časové prodlevy byly minimální. Ale upřímně řečeno, setkali jsme se i s tím, že IT manažeři některých nemocnic nebyli ani přes naléhavou situaci ochotni naše doporučení akceptovat.

MATEJ KAČIC

VE SPOLEČNOSTI AEC PŮSOBÍ OD ROKU 2013. ZAČÍNAL NA POZICI BEZPEČNOSTNÍHO KONZULTANTA, POTÉ PŮSOBIL JAKO ARCHITEKT BEZPEČNOSTI A OD ROKU 2017 JE VEDOUCÍM DIVIZE TECHNOLOGIÍ. MEZI JEHO HLAVNÍ OBLASTI PROFESNÍHO ZÁJMU PATŘÍ NÁVRHY A AUDITY BEZPEČNÉ SÍŤOVÉ INFRASTRUKTURY. SPECIALIZUJE SE NA NÁVRHY BEZPEČNOSTNÍCH ŘEŠENÍ ZALOŽENÝCH NA AUTOMATIZACI. MATEJ KAČIC VYSTUDOVAL FAKULTU INFORMAČNÍCH TECHNOLOGIÍ VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ.

Může se organizace nějak připravit na kritickou bezpečnostní situaci?

Bezesporu ano. Každá společnost by měla mít definovaný plán obnovy kritických systémů a infrastruktury. V praxi jde o popis závislostí, priorit a kroků vedoucích k obnově IT do provozuschopného stavu. Samozřejmostí je správné zálohování podle principu 321, což ve zkratce znamená, že si vždy uděláte minimálně tři kopie svých dat, z nichž dvě budou místní, ale na rozdílných zařízeních, a minimálně jedna kopie bude k dispozici mimo domov či kancelář. Důležité je i pravidelné testování záloh a plánu obnovy. Často se stává, že systém se nedaří ze zálohy obnovit, případně není funkční samotný plán obnovy.

Na základě zkušeností jsem zastáncem nového trendu, který nám umožňuje každý krok administrátora automatizovat už při nastavování systému, což jeho případnou obnovu velice usnadňuje. Představte si to tak, že někdo povolaný po útoku zmáčkne červené tlačítko a celý IT systém se sám, bez dalšího zásahu během několika hodin nainstaluje.

Jen pro připomenutí, intenzivní obnova základních dat v nemocnici v Benešově a poté i v Brně přesáhla pokaždé dobu čtrnácti dnů.

Nemocnice procházejí velkým technologickým rozvojem. Už dnes využívají řadu přístrojů komunikujících na dálku, do zdravotnictví přichází IoT. V čem spatřujete největší bezpečnostní rizika?

Ano, internet věcí je fenomén, který představuje bezpečnostní výzvu, a to nejen ve zdravotnictví. Nicméně se domnívám, že pokud jsou technologie, kterými disponujeme, správně poskládané a nasazené, dokážou už dnes efektivně chránit i svět IoT.

Hodně se dnes skloňuje telemedicína. Z libovolných inteligentních hodinek, mobilu či běžně dostupných senzorů se stane nástroj pro diagnostiku vašeho zdravotního stavu přímo z domova. Zdravotnictví se tím definitivně a naplno otevře internetu. Je třeba přijmout fakt, že ruku v ruce s tím se objeví nové cesty, jak do těchto systémů proniknout. To je samozřejmě velká výzva.