HACKEŘI STÁLE UNIKAJÍ

Hospodářské noviny | 26.5.2020 | Rubrika: Panorama | Strana: 10 |
Autor: Markéta Řeháková | Téma: Masarykova univerzita, vysoké školy

POZADÍ SÉRIE KYBERÚTOKŮ NA ČESKÉ NEMOCNICE V DOBĚ KORONAVIROVÉ PANDEMIE ZŮSTÁVÁ PŘEDMĚTEM VYŠETŘOVÁNÍ. INCIDENT, KTERÝ POHORŠIL ZAHRANIČÍ VČETNĚ VLÁDY USA, MOHL BÝT SNAHOU VYDĚLAT NA KRIZOVÉ SITUACI I PROVOKACÍ CIZÍHO STÁTU.

Březnová zpráva Evropského policejního úřadu popisuje, jak kriminálníci vydělávají na koronavirové krizi. Data sbírá ze všech zemí EU. Uvádí ale jediný příklad kyberútoků na klíčovou zdravotnickou infrastrukturu a tím jsou české nemocnice. Série kyberútoků z března a dubna byla výjimečná v mnoha ohledech. Načasování na začátek nouzového stavu, zacílení na zdravotnická zařízení i důsledek v podobě paralyzované klíčové brněnské nemocnice nemají v evropském kontextu obdoby.
„Útoky v nemocnicích nejsou obecně pro dobu pandemie specifické. Možná zvýšila jejich efekt, protože nemocnice jsou pod vyšším tlakem. Nejde ale o specialitu současného prostředí," říká pro HN Fernando Ruiz, vedoucí oddělení kyberkriminality Europolu.
S útokem na lékařská zařízení podobného rozsahu se nepotýkal ani žádný ze spojenců v Severoatlantické alianci. „Některé země hlásily útoky na zdravotnický sektor, ale nešlo o nic, co bychom neviděli už před krizí," potvrzuje Chelsey Slacková, šéfka kybernetické bezpečnosti NATO. „Obecně jde o podobné aktéry, kteří používají podobné metody, jenom je tematicky přizpůsobili, aby souvisely s covidem-19," vysvětluje v rozhovoru pro HN.
Slacková poukazuje na bezpečnostní incidenty v USA a Velké Británii. Skupina Maze Team, známá právě útoky na zdravotnická zařízení a laboratoře prostřednictvím ransomwaru (programu, který zablokuje počítačový systém nebo šifruje data a pak požaduje výkupné za jejich zpřístupnění), ukradla záznamy z pohotovosti na Floridě a v Texasu. Ve Velké Británii zablokovala systémy Hammersmith Medicines Research, která se podílí na testování vakcíny proti koronaviru. Londýnská společnost počítače znovu rozjela ještě tentýž den. Maze Team se k útokům přihlásil na svém webu.
Začátkem května bezpečnostní agentury obou zemí varovaly, že hrozí pokusy o krádeže informací o vývoji léků na koronavirus. Spojené státy z těchto pokusů následně obvinily Čínu. Útok podobných rozměrů jako v Česku ale žádná země neohlásila. Spekulace, že za útoky stojí Ruská federace, policie ani ministerstvo zahraničí zatím nekomentují.

Někdo si s tím dal práci

Hackeři zašifrovali počítače brněnské fakultní nemocnice v noci po vyhlášení nouzového stavu v pátek 13. března. Lékaři nemohli zaznamenat výsledky vyšetření, v nemocnici nefungovaly klíčové přístroje jako CT či rentgen. Nebylo možné odesílat zprávy ani vystavovat neschopenky. Část pacientů z Bohunic posílali jinam a museli odložit plánované zákroky. Podobný dopad měl i útok na psychiatrickou nemocnici v Kosmonosech u Mladé Boleslavi o několik dní později.
Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v polovině dubna varoval před kyberútoky na nemocnice a jiné významné cíle v Česku. Doporučil, aby se lépe zabezpečily. Za pár hodin hlásily pokus o útok nemocnice v Ostravě, Olomouci, Karlových Varech a Pardubicích. Podle informací HN jich bylo ještě více. Útoky se díky varování podařilo odrazit. Hackeři se ale nevzdali a testovali i jiné systémy, například ministerstva zdravotnictví a Letiště Václava Havla.
Podobné varování vydal NÚKIB poprvé od svého vzniku v roce 2017. Informaci, že se útok chystá specificky na zdravotnická zařízení v Česku, a také o konkrétním čase, získal od spolupracujících partnerů. Patří k nim například bezpečnostní a zpravodajské služby v Česku i zahraničí, armády či mezinárodní organizace jako NATO a EU.
„V kybernetickém prostoru vidíme útoky běžně, často jde o roboty. Tady je ale situace jiná, někdo si s tím musel dát práci," myslí si Tomáš Plesník, vedoucí kyberbezpečnostního týmu **Masarykovy univerzity**. „Útok měl několik fází, skenovali si infrastrukturu a identifikovali její zranitelnosti. Je tam vidět plán i to, že nejde o začátečníka," upozorňuje. Web Seznam Zprávy minulý týden informoval, že útoky mají původ v Rusku a že jeden z možných aktérů pracuje pro firmu spoluvlastněnou státem. NÚKIB uvedl, že se informacemi zabývá, s mediálními výstupy ale „pracuje

běžně“.

Proč paralyzovat nemocnice?

Když loni v prosinci hackeři na několik týdnů zablokovali systémy benešovské nemocnice (jiný útok zasáhl těžařskou společnost OKD), policie prošetřovala možnost, že jde o vyděračský pokus, jaké se po síti dějí častěji. Pachatel se přihlásí s žádostí o výkupné za rozšifrování dat, a jestliže si majitel napadeného systému poradí sám, vyhrožuje jejich zveřejněním. Případně ukradené informace prodá. Podle zprávy FBI náklady na nápravu škod způsobených podobnými útoky v USA loni dosáhly 3,7 miliardy dolarů, ať už šlo o peníze na zprovoznění systémů nebo platby výkupného. Studie společnosti Sophos ukázala, že vyděračský software loni zasáhl přes polovinu českých společností ve veřejném i soukromém sektoru. Průměrné náklady na eliminaci následků byly zhruba šest milionů korun.
Jenže v Benešově to tak nebylo. „Podle informací, které máme, výkupné nikdo přímo nevyžadoval,“ uvádí Petr Ballek, tiskový mluvčí nemocnice, s tím, že útočník se do systému pravděpodobně dostal přes nakaženou přílohu. Také policie vydala v únoru prohlášení, že o výkupné nešlo. Ministr zdravotnictví Adam Vojtěch (za ANO) pak prohlásil, že incident je ponaučením i varováním pro ostatní zdravotnická zařízení.
Brzy nato přišla karanténa a s ní byla napadena nemocnice v Brně. Tam nechtějí záležitost komentovat s odkazem na probíhající vyšetřování. „Už dneska si ale můžeme říct, že šlo o cílený útok a jeho záměrem bylo nemocnici paralyzovat,“ usuzuje Petr Hladík (KDU-ČSL), náměstek brněnské primátorky pro zdravotnictví. „Paralyzovat nemocnici z ekonomických důvodů mi připadá opravdu zvláštní, neznám mnoho případů, kdy by se dělalo ekonomické vydírání takovým způsobem,“ míní Hladík.
Motivace může být i politická. Některé státy financují nelegální skupiny, aby získávaly strategické informace nebo vyvolaly nedůvěru ve státní instituce. Například součástí armády Čínské lidové republiky jsou i speciální jednotky hackerů. Média spekulují, že jich je 50 až 100 tisíc. Začátkem letošního roku USA obvinily čínské důstojníky z útoku na americký registr dlužníků Equifax v roce 2017. Šlo o jeden z největších úniků dat v historii. Čína obvinění odmítla.
O motivaci hackerů diskutovali na začátku května účastníci on-line debaty Hospodářských novin a Aspen Institute Central Europe. „Státní aktéři se snaží rozšířit a maximalizovat svůj vliv,“ popsal v ní Lukáš Kintr, náměstek ředitele NÚKIB. Takové útoky jsou masivní, jejich původci navázaní na stát mají silné finanční i technologické zázemí.
Známý je vyděračský kyberútok WannaCry. Šířil se v květnu 2017, zasáhl více než 200 tisíc společností ve 150 zemích. Výrazně dolehl na zdravotnické služby Spojeného království, včetně zařízení magnetické rezonance či lednic pro ukládání krve. V prosinci téhož roku britská vláda spolu s USA a Austrálií veřejně přisoudily odpovědnost za útok Jižní Koreji. Ta ji popřela. Následující rok pak americké úřady obvinily i konkrétní útočníky.
„Když v jiném státě shodíte pár nemocnic, ukazujete obyvatelům, že se politická reprezentace o něco špatně stará,“ vysvětluje Aleš Špidla, prezident Českého institutu manažerů informační bezpečnosti. „Také to může být varovný prst. Vzkaz, že se někdo umí dostat do nemocnice. Příště může jít o jinou instituci, například chemičku. Ty jsou často na kraji velkých měst, když k tomu shodíte systém v nemocnici, vyvoláte chaos.“

Opatrné ministerstvo a mlčící vláda

Nemocnice nejsou jediným případem napadení citlivých cílů v Česku hackery. Loni v červenci pronikli skrytí agresoři do systému ministerstva zahraničních věcí. Senátní výbor pro obranu a bezpečnost v prohlášení uvedl, že podle informací NÚKIB byl za útokem cizí stát. Média i tehdy zveřejnila, že šlo o Rusko. Ruské velvyslanectví to označilo za spekulace.
Senát také vyzval vládu, aby věnovala zvýšenou pozornost a odpovídající část rozpočtu na posílení kybernetické bezpečnosti.
HN se obrátily na vládu i ministerstvo zahraničí s dotazem, zda se české úřady chystají označit, kdo byl za útoky odpovědný. Úřad vlády na dotazy neodpověděl. Zástupci ministerstva zahraničí se k incidentům z předešlých let nevyjádřili. K útokům na nemocnice uvedli, že vyšetřování stále probíhá, proto otázky na možné pachatele nebudou komentovat. „Označit je musí experti a policie. Ministerstvo do procesu vstupuje teprve v další fázi, ve které se vyhodnocuje, zda útok – ať už byl proveden

kteroukoliv osobou – lze přičíst konkrétnímu státu," ozvala se mluvčí Zuzana Štíchová.
Ministerstvo má několik možností, jak v takovém případě jednat. Může se ohradit v diplomatické komunikaci s dotyčným státem nebo veřejným prohlášením. Může také vést společný postup například v EU nebo NATO. Veřejně se k tomu čeští diplomaté nikdy neodhodlali. Zda k tomu došlo při soukromých jednáních, diplomaté nekomentovali.
Štíchová pouze tlumočila, že útoky na nemocnice v době, kdy společnost bojuje s koronavirem, ministerstvo považuje za hyenismus: „Nejedná se o pročítání mailů, hovoříme o sabotáži kritické infrastruktury, jejímž důsledkem mohly být ztráty na životech."
Označit veřejně, kdo je za útok odpovědný, je ukázkou, že vláda daného státu odmítá útoky tolerovat a že může sáhnout k nějakým sankcím. „Stát může mít různé důvody, proč odpovědnost nepřisoudit, ale každý takový krok pomáhá nastavovat pravidla a činí útočníky zranitelnějšími a obránce bezpečnějšími," zdůrazňuje český velvyslanec při NATO Jakub Landovský. Odkazuje na nedávný příklad, kdy Nizozemsko, Velká Británie a USA obvinily ruské zpravodajce z útoků na Organizaci pro zákaz chemických zbraní a Světovou antidopingovou agenturu.
Důležitá je podle něj také reakce ostatních zemí. Po útocích na české nemocnice byla mimořádně silná. Americký ministr zahraničí Mark Pompeo prohlásil, že USA nebudou tolerovat žádné škodlivé kybernetické aktivity, které podlamují bezpečnost Spojených států a jejich mezinárodních partnerů. „Kdokoli se na takových útocích podílí, musí očekávat následky," řekl. Veřejné prohlášení podporující Česko vydalo také Estonsko a Austrálie s Lotyšskem vyjádřily solidaritu na sociálních sítích. Další země se přidaly přes EU a NATO.
Mezinárodní spolupráce je důležitá také při vyšetřování. Hackeři útočí v jedné zemi přes IP adresy registrované v mnoha jiných, aby zahladili stopy.
S kyberútoky na kritickou infrastrukturu státu podobných dopadů nemá Česko mnoho zkušeností. Policie vyšetřovala jednotky případů. Národní centrála proti organizovanému zločinu jich HN potvrdila šest. Policisté dosud nikdy nezahájili trestní stíhání proti konkrétní osobě.
Je navíc možné, že i když se podaří útočníky vypátrat, nakonec se trestu vyhnou. Jestliže se zdržují na území EU, policie může požádat o jejich předání k trestnímu stíhání do Česka na základě evropského zatýkacího rozkazu. Jinak záleží na tom, jestli má Praha s konkrétním státem dohodu o vydávání nebo alespoň praxi vzájemného vydávání zločinců. Pokud by šlo například o Rusko nebo Čínu, ani jedna z těchto zemí své občany nevydává. Nezbývá tedy než čekat, zda někam vycestují. „Je možné na ně vydat zatýkací rozkaz. Pokud k zadržení občanů Ruské federace dojde mimo Rusko nebo k zadržení občanů Číny mimo Čínu, může vydávací řízení proběhnout," vysvětluje Petr Malý, tiskový mluvčí Nejvyššího státního zastupitelství.
Policie zatím nikdy nepožádala o vydání občana nečlenské země EU k trestnímu stíhání ani justici takové země o zahájení trestního stíhání.
Předtím by se muselo povést vypátrat hackery, kteří útočili v nemocnicích, což bude složité. České úřady mají tentokrát ale mimořádně silnou zahraniční podporu, která by mohla pomoci k úspěchu. Pokud policie viníky označí, bude na české diplomacii, aby sebrala odvahu a o jejich motivech nemlčela. Nelze před nimi totiž zavírat oči, protože bezpečnost českých nemocnic zůstává křehká a je pravděpodobné, že útoky se budou opakovat.

HACKEŘI V BRNĚ Hackeři zaútočili na druhou největší nemocnici v Česku 13. března kolem druhé hodiny ráno. Kyberútok zasáhl i Dětskou nemocnici a Porodnici na Obilním trhu, které pod FN Brno spadají. Situaci řešili experti z Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), **IT** oddělení nemocnice a následně dobrovolníci z **Masarykovy univerzity**. Administrativa nemocnice funguje stále jen na 70 procent. Vedení očekává plně funkční systémy v červenci. V Bohunicích přišli například o některá právní a ekonomická data nebo o internetový objednávkový systém dárců krve. Škody půjdou do desítek milionů korun. Virus se do systému dostal pravděpodobně ze zavirované přílohy e-mailu. Na první pohled vypadá taková příloha důvěryhodně, třeba jako neuhrazená faktura. Jestli hackeři žádali o výkupné a zda jim ho někdo zaplatil, vedení nemocnice nepotvrdilo. Trestní řízení k brněnskému případu dozoruje krajské státní zastupitelství. Útoky šetří Národní centrála proti organizovanému zločinu ve spolupráci s NÚKIB. Útoky na zdravotnická zařízení v době, kdy Česko bojuje s koronavirem, považujeme za hyenismus. Zuzana Štíchová tisková mluvčí ministerstva zahraničí

K tématu čtěte ve středečním vydání HN: Rozhovor s Karlem Řehkou, novým ředitelem Národního

úřadu pro kybernetickou a informační bezpečnost

Foto popis| Zranitelná místa IT oddělení Fakultní nemocnice Brno dostalo těžký úkol – odstranit následky kyberútoku, jenž v březnu její chod paralyzoval. S tímtéž problémem se na sklonku minulého roku potýkala Nemocnice Rudolfa a Stefanie Benešov. Vrátit se do běžného provozu trvalo tři týdny.
Foto autor| Foto: HN – Tomáš Škoda, ČTK

O autorovi| Markéta Řeháková, marketa.rehakova@economia.cz