■ Kyberútoky

Firmy platí hackerům milionové výpalné a pak řeší, jak ho dát do účetnictví

Michael Mareš, Marek Pokorný
autori@hn.cz

Byla sobota, jedenáct dopoledne, když šéfovi jedné z největších českých projekčních kanceláří zazvonil telefon. Volal mu ajťák, že všechny firemní systémy jsou zašifrované a nic nejde otevřít. Ukázalo se, že jde o vyděračský program, takzvaný ransomware, a útočníci za odblokování požadují výkupné: 1,5 milionu korun v bitcoinech. „Sehnali jsme odbornou firmu, která s nimi složitě vyjednávala. Po zaplacení určité sumy nám otevřeli část a ukázali, že to jde. Jakmile jsme doplatili zbytek, celé se to odšpuntovalo," vzpomíná ředitel napadené projekční kanceláře, který Hospodářským novinám popsal detaily loňského útoku pod podmínkou anonymity. Podle svých slov si je vědom, že se společnost stala obětí trestného činu, ale výkupné se mu vzhledem k tržbám společnosti zdálo přiměřené. Bylo o něco menší, než činí jejich denní příjmy.

Nejnebezpečnější z útoků

Ransomware je slovo, které se v českém jazyce i byznysu rychle zabydluje. O co jde? Je to kybernetický útok, kterým hackeři omezí uživatelům přístup k jejich počítačovému systému nebo souborům a za obnovení přístupu požadují zaplacení výkupného. I když u nás neexistuje přesná statistika, kolik takových útoků v Česku proběhne, kolik jich je úspěšných nebo kolik vede k zaplacení, odborníci se shodují, že jejich počet rychle stoupá. Ačkoli se množí veřejně známé případy, kdy byli útočníci úspěšní, velká část firem ani státních institucí a organizací na ně stále není připravena.

Ruku v ruce s tím razantně roste počet uzavřených pojistek, které firmám kryjí škody způsobené kybernetickým útokem. Pojišťovny už několik let evidují zvýšený zájem, nově zesílený po incidentu z letošního května, kdy hackeři napadli servery Ředitelství silnic a dálnic. Organizaci, která pracuje s šedesátimiliardovým rozpočtem, vyřadili z provozu tisícovku serverů a všechny aplikace. O část dat nenávratně přišla a z útoku se dodnes plně nevzpamatovala.

Podobných útoků už se přitom v Česku odehrálo více. Za poslední tři roky internetoví vyděrači prostřednictvím ransomwaru dočasně ochromili nemocnici v Benešově, špitál sv. Anny v Brně i těžební společnost OKD. Ve většině případů se policii nepodaří identifikovat pachatele a případ odkládá. Škody přitom jdou do desítek milionů korun – v případě benešovské nemocnice šlo téměř o 60 milionů, ŘSD zatím mluví o 30 milionech.

Ransomwarová hrozba je v tuzemském byznysu rozšířenější, než by se na mohlo zdát. Nedávný průzkum společnosti Acronis ukázal, že pětina českých organizací zažila v posledních 12 měsících výpadek provozu kvůli ransomwarovým útokům a o mnoho víc jich bylo napadeno, přičemž firmy incidenty – úspěšné i neúspěšné – v 68 procentech případů nikam nehlásí.

Jak potvrzují údaje softwarové společnosti Cisco, ransomware je ze všech druhů kybernetických útoků největší hrozbou. Nejčastěji míří na oblast zdravotnictví a do státní správy, ovšem proniká prakticky do všech odvětví. „Některé firmy spoléhají na to, že nejsou zajímavými cíli. Ale jak ví každý sekuriťák – otázkou není zda, ale kdy budete napadeni," říká Michal Stachník, generální ředitel české pobočky společnosti Cisco.

Na přelomu minulého a letošního roku počet ransomwarových útoků globálně mírně klesal, což pravděpodobně způsobila válka na Ukrajině, rozprášení několika hackerských skupin a pokračující trend, kdy se tyto vyděračské gangy zaměřují spíše na velké cíle místo běžných uživatelů prostřednictvím metody „spray and pray". Jenže čerstvá data antivirové společnosti Avast z druhého kvartálu odhalila opět výrazný nárůst, a to o 24 procent oproti předchozímu čtvrtletí.

Z evropského srovnání Češi nevycházejí moc příznivě – patříme mezi pět zemí nejčastěji napadaných kyberútoky. Zatímco v Evropské unii mělo loni podle studie společnosti Soitron zkušenost s některým typem počítačové kriminality 28 procent malých a středních podniků, u nás šlo o 38 procent. Nejhůře na tom jsou Portugalci (48 procent) a nejlépe Švédové (15 procent).

O tom, že Česko je čím dál častějším terčem, svědčí i Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, kterou Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) předal vládě k projednání. Uvádí se v ní, že narostl počet škodlivých aktivit: NÚKIB eviduje 476 hlášení incidentů, z nichž jich řešil 157. V kolonce trestných činů kybernetické kriminality uvádí téměř deset tisíc případů, přičemž ransomware řadí mezi nejzávažnější hrozby.

Jak upozornil server Lupa.cz, velká část z nich je vedena jako RaaS, tedy ransomware-as-a-service, kdy se útok typicky vede jako tzv. double extortion (dvojí vydírání): útočník zašifruje soubory a zároveň vyhrožuje jejich zveřejněním nebo prodejem. Tzv. triple extortion přidává do vydírání ještě DDoS útok, tedy zahlcení serverů obrovským množstvím požadavků. „Kyberkriminalita je obrovský byznys. Relativně malé vstupní náklady a relativně obří potenciální zisky. Jednu věc můžete snadno replikovat x-krát a e-mail pošlete zadarmo. Sice tam je malá úspěšnost, ale pořád z jednoho zásahu mohou být obrovské peníze," říká Vladimír Rohel, kyberbezpečnostní expert z Národní agentury pro komunikační a informační technologie.

Zaplatit, nebo nezaplatit?

I když v branži léta platí pořekadlo, že s vyděrači se nevyjednává, realita není tak černobílá. „Příklady ze života ukázaly, že mnohdy zaplatit je jedinou cestou, jak se dostat ke svým datům zpět. Cena výpalného se raketově zvyšuje a dnes se pohybuje v milionech korun," popisuje Stachník z Cisca. „Navíc nedávný průzkum ukázal, že 80 procent organizací, které zaplatily výkupné, bylo krátce poté znovu napadeno."

Zaplatit, nebo nezaplatit? To je podle odborníků vysoce individuální otázka, při jejímž zodpovídání mají volnější ruce zástupci soukromých firem. Oproti tomu představitelé státních institucí a úřadů – a to ve svých vyjádřeních připomínal i šéf ŘSD Radek Mátl – by v případě zaplacení riskovali, že je takové rozhodnutí může přivést za mříže.

Pokud se firma rozhodne zaplatit, vyvstává otázka, jak tuto položku vpravit do účetnictví. Komora daňových poradců si k tomu nechala udělat i analýzu od KPMG a snažila se prosadit, aby výpalné finanční úřady braly jako daňově uznatelný náklad. Ty to odmítly s tím, že by to mohlo vést k daňovým podvodům – firmy by si placení výkupného mohly vymýšlet. „Chápali jsme jejich obavu ze zneužití a snažili se argumentovat, že by to měli uznat, pokud bude posudek z IT firmy, že ta data není schopná odblokovat a jediným řešením je výpalné zaplatit. Ale přesto to odmítli," uvedl Jiří Nesrovnal z prezidia Komory daňových poradců ČR.

Jednou z firem, které útočníkům výkupné zaplatily, je advokátní kancelář Michala Žižlavského. Ten patří k nejvýznamnějším hráčům v insolvenčním byznysu a spravuje přes 4000 insolvenčních případů. Jeho kancelář po akci kybernetických vyděračů na podmínky výpalného přistoupila a zaplatila. „Ačkoliv máme robustní IT infrastrukturu, do které průběžně investujeme miliony korun, samo o sobě to nestačilo," přiznal Žižlavský, ovšem vyloučil, že by došlo ke ztrátě klientských dat. K tomu, kolik za klíč k dešifrování disků jeho kancelář zaplatila, se vyjádřit odmítl. Připustil ale, že vznikla škoda nejméně v řádu stovek tisíc korun.

Opačné řešení po napadení zvolilo Centrum pro regionální rozvoj České republiky. Státní příspěvková organizace, řízená ministerstvem pro místní rozvoj, útok přiznala i ve své výroční zprávě za rok 2021. Hackeři shodili servery a zašifrovali všechna data ve vnitřní síti. Zároveň zanechali na serveru jeden přístupný textový soubor, který v angličtině popisoval způsob, jak soubory odkódovat.

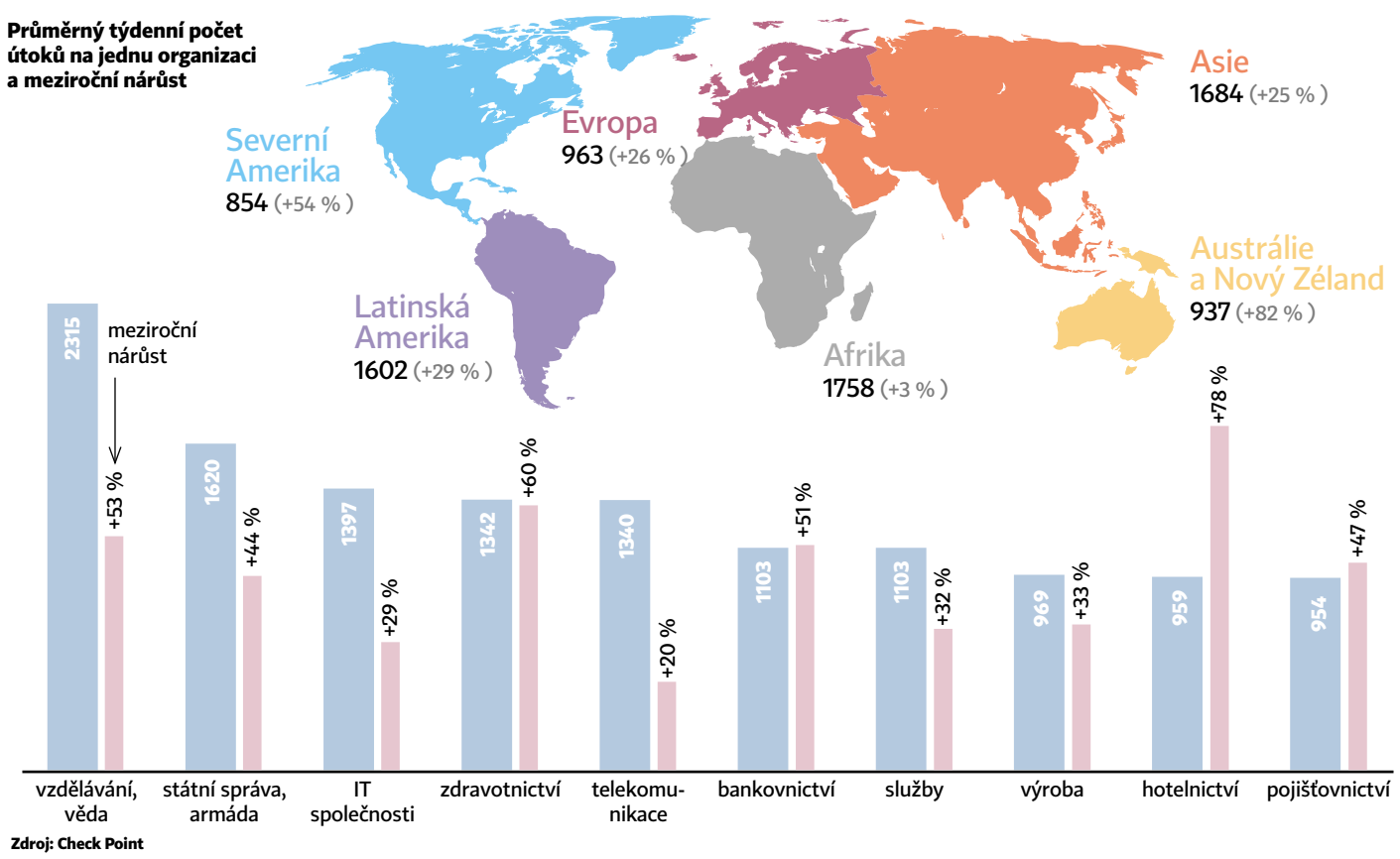
„Bylo v něm napsáno, že nemáme nikoho kontaktovat, a přiložené přihlašovací údaje se způsobem, jakým zaplatit v bitcoinech," popisuje ředitel centra Zdeněk Vašák s tím, že o zaplacení výkupného neuvažoval. „Měli jsme veškerá data zálohovaná, takže jsme udělali jednoduchou věc: servery jsme smazali a nahráli zálohy. V účetnictví a v personálním systému jsme ztratili data jen za šest hodin a během týdne vše opět fungovalo."

Ransomwarové útoky mají jednoduchý motiv: vydělat útočníkům peníze. Využívají k tomu i obchodní a prodejní taktiky známé z normálního byznysu. „Mají čím dál profesionálnější přístup. Nabízí slevy či splátkové kalendáře a zákaznickou podporu, prostě to, na co jsou lidé zvyklí z normálního života. Jen tady jde o kriminální činnost," říká Richard Brulík, šéf společnosti Safetica, která se specializuje na ochranu citlivých dat ve firmách. „Zapomeňte na obrázek hackera s kapucí v temné místnosti, jaký známe z fotobank. Často to jsou až absurdně moderní byznysové provozy."

Odkud ransomwaroví nájezdníci pocházejí? Experti se shodují, že nelze jednoduše ukázat jedním směrem. „Může to být západ i východ. Paradoxně hodně útoků k nám míří z USA," po-

Ransomware ve světě roste

Celosvětový průměrný týdenní počet ransomwarových útoků na jednu organizaci za 2. čtvrtletí 2022. Jde o globální data podle regionů a odvětví z analýzy americko-izraelské softwarové společnosti Check Point, která se specializuje na kybernetickou bezpečnost.



Zdroj: Check Point

pisuje Rohel. Většina kybergangů působí přes hranice a zametá stopy, takže je těžko dohledatelné místo původu. Přesto lze ale vysledovat aktivitu vyděračských skupin spjatých s režimem zemí, jako je Rusko, Čína či Pákistán.

„Velká část gangů je ruská, dá se to zjistit z analýzy protokolů a určitých chyb v angličtině. Navíc tam platí výjimka ze zákonů: stát vás nestíhá, pokud neděláte útoky proti Ruské federaci," popisuje Martin Rehák, zakladatel bezpečnostního start-upu Resistant AI. Podle jeho slov se cílení přesouvá ze západní Evropy dále na východ. „Už se to významně přelévá i do Česka. To, co některým gangům nefunguje na západních trzích, může ještě dobře fungovat u nás. Když už nejsem tak rychlý gepard, tak si najdu pomalejší gazelu," tvrdí.

„Vidím to 50 na 50. Jsou organizace, které jsou připravené, ale vím i o systémech, které by měly velký problém. Často jsou podfinancované nebo jsou připravené na staré hrozby, jelikož mají obrannou architekturu postavenou deset patnáct let nazpět," vysvětluje Rohel s tím, že nejslabší článek se většinou skrývá v konkrétním člověku – zaměstnanci, který nedodrží bezpečnostní standardy nebo se zachová naivně.

To potvrzuje i ředitel Vašák z napadeného Centra pro regionální rozvoj. „Vektor útoku nevíme jistě, ale nejpravděpodobnější je, že byl diskreditován účet našeho zaměstnance. Bylo to v době, kdy zaměstnanci pracovali z domu a měli vzdálený přístup," říká. Právě v době home officů se obranná linie firem často ztenčila, jelikož zaměstnanci do firemních systémů často přistupovali zvenčí a z jiných zařízení.

Dalším častým způsobem je napadení skrz dodavatele, například při posílání faktur. Útočníkům stačí věrně napodobit adresu a styl obvyklé komunikace a jsou „uvnitř".

„Přes dodavatele to je klasická metoda. Pošlou jakoby očekávanou fakturu, přibalí škodlivý program a je to," připomíná Rehák, že to byl nejspíš i způsob infiltrace do ŘSD. „Zaměstnanci, kteří otevírají větší množství e-mailů nebo faktury od dodavatelů, by neměli používat normální počítače ale chromebooky, iPady nebo tablety, jinými slovy zařízení s nižší hrozbou zranitelnosti, a každý večer je uvést do továrního nastavení nebo obnovit ze zálohy."

Firmy nejsou připravené

NÚKIB vydal manuál, jak se bránit útokům ransomwarem a bezpečně zacházet s počítačem a telefonem. Pořádá také školení, kterými loni prošlo téměř 34 tisíc lidí. Zdroj z úřadu ovšem anonymně HN přiznal, že spousta firem a organizací patřících do kritické infrastruktury státu není připravena. „I když je kontrolujeme a říkáme, jak mají zálohovat, nedělají to. Kašlou na to, poučí se až z vlastních chyb."

„Většina českých firem na sebe není dost přísná, co se týče bezpečnosti IT," potvrzuje Rehák s tím, že by měly dělat pravidelné průnikové testy a připravit se i na nečekané události, například požár serverovny. Citovaný průzkum společnosti Acromis popsal, že IT experti za nejdůležitější prvky ochrany považují nezaměnitelnost záloh, jejich aktivní obranu a také využívání cloudových služeb.

Podle Stachníka by si každá firma měla vybudovat vnitřní architekturu „nulové důvěry" a pořádat pravidelná kyberbezpečnostní „bojová cvičení". „Ta by neměla být jen na papíře, ale měla by se stejně jako požární cvičení každoročně procvičovat a vylepšovat, aby napadené organizaci nezbyly jen oči pro pláč a pokladna, v tom lepším případě, o pár milionů lehčí," říká šéf českého Cisca.

Česká projekční kancelář zmíněná na začátku textu se po zaplacení výkupného poučila. Do zabezpečení rychle nainvestovala 30 milionů korun. „Kompletně jsme předělali celou strukturu našeho IT. Máme všechno nové, od firewallů po servery," říká její šéf. I on však přiznává, že až při dalším velkém útoku se ukáže, jak robustní nová obrana doopravdy je.