

Ransomware v Česku

Ohrožuje ransomware český veřejný sektor?

Aleš Hok



Ještě před rokem, když jsme se bavili se svými zákazníky, jsme vždy uváděli odstrašující příklady ze Spojených států, západní Evropy a různých vyspělých regionů. Bohužel, letos již při kontaktu se zákazníky můžeme uvádět i lokální příklady, zejména poté, co došlo k útoku na nemocnici v Benešově.

Další incidenty jsou jen otázkou času

Dnes již víme, že v případě útoku na nemocnici v Benešově nešlo o konkrétně cílený útok, že původcem byl malware Emotet a o zašifrování se postaral ransomware Ryuk. Celkové škody se podle posledních údajů vyšplhaly na 60 milionů korun. V mediálním stínu tohoto útoku došlo nedávno i k napadení magistrátu v Kladně, kde rovněž byly zaznamenány nezanedbatelné škody, a již dříve se oběti staly i některé české školy.



Samotné útoky ale nejsou tou nejhorší zprávou, větší obavy panují o celkový stav zabezpečení českého veřejného sektoru. Hejtmanství Středočeského kraje totiž v reakci na benešovský útok uvedlo, že „zabezpečení nemocnice bylo na standardní úrovni srovnatelné s ostatními nemocnicemi“. Jinými slovy, další incidenty jsou jen otázkou času.

Nejvíce ohrožená jsou právě zdravotnická zařízení, kde v případě zašifrování dat jde sice o významné finanční ztráty, ale mnohem vážnější jsou přímé následky na zdravotní stav pacientů. Nemocnice

jsou v tomto ohledu extrémně zranitelné a v situaci, kdy jde doslova o minuty, jsou k zaplacení výkupného přístupnější. Právě proto vzbudil případ benešovské nemocnice takový ohlas a zájem o celkový stav zdravotnického sektoru.

Nový ransomware je zákeřný a napadá i zálohy

Chování ransomwaru je stále zákeřnější. Již neplatí to, že po zašifrování živých dat lze snadno a automaticky obnovit vše ze zálohy. Dnešní kmeny ransomwaru se nejprve snaží napadat samotné zálohy nebo se snaží vypínat ochrany a zálohovací software tak, aby organizace po spuštění záloh zjistila, že vlastně žádné použitelné nemá a že jediná šance je zaplatit výkupné.

A jako třešnička na dortu přicházejí nejnovější verze, které v případě nezaplacení výkupného navíc vyhrožují zveřejněním citlivých dat. Což je velmi nepříjemné jak pro komerční firmy s cenným duševním vlastnictvím a patenty, tak také pro veřejné organizace, kterým hrozí vysoké pokuty za nedostatečnou ochranu osobních údajů dle GDPR.

Nejčastější vstupní branou, kterou ransomware proniká do sítí firem a organizací, je s využitím mailového phishingu či spear



Jedním z poučných případů kybernetického útoku ve veřejném sektoru byl například loňský ransomwarový útok na floridské město Miami, které v reakci na prodělané napadení vyhlásilo 14. října za „Miami CyberFit Day“, tedy jakýmsi dnem kybernetické ochrany. Tento den si všechny úřady v Miami připomínají důležitost kybernetické bezpečnosti a ochrany svých systémů, bez kterých by nemohly fungovat. Na snímku je Francis Suarez, starosta města Miami (uprostřed), se Sergejem Belousovem (vlevo), zakladatelem a ředitelem společnosti Acronis, která je partnerem města v oblasti kyberbezpečnosti. Vpravo je Gajdar Magdanurov, COO Acronisu.

phishingu, který je postaven na znalosti daného prostředí a je přesně cílený na typ organizace a pracovníka (nejčastěji managementu) s danou rolí a pravomocemi. Tento člověk pak spíše považuje takový e-mail za důvěryhodný a kliknutím na jeho přílohu otevře ransomwaru cestu do celé organizace.

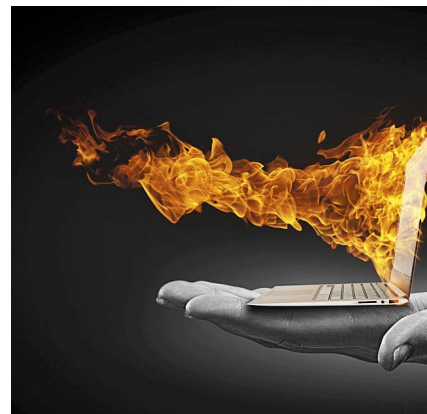
Rentgen s Windows 7

Na otázku z titulku tedy odpovídáme: ano, český veřejný sektor je ohrožen. Nabízí se pak další otázka, co s tím. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) uvádí 47 doporučení – na všechna v tomto článku nemáme prostor, tak připomeňme alespoň ta nejdůležitější:

- **Členit síť na menší segmenty a i mezi nimi používat firewall** – absence tohoto opatření byla jedním z důvodů, proč například nemocnice v Benešově přestala fungovat jako celek a nikoliv jen na několika málo odděleních.
- **Využívat antispamové řešení a nastavit přísné filtrování** – to by mělo být automatické u všech organizací. I když není samospasitelné, protože žádné antispamové řešení nedokáže 100% odchytilit

všechny podezřelé adresy. Proto pokud možno doplňte o selský rozum a školení uživatelů na podezřelé e-maily.

- **Omezit uživatelům práva na nutné minimum** – i management organizace a i správci sítě by měli pro běžnou práci využívat účty s omezenými právy. Přístup s plnými právy využívat jen ve výjimečných případech.
- **Používat aktualizované operační systémy a aplikace** – naprostá většina malwaru se v sítích šíří s pomocí již známých zranitelností. To je problém právě nemocnic, které používají nezabezpečená zařízení, typicky rentgen napojený na PC s nepodporovanými Windows XP či 7. V tomto případě platí pravidlo odpojit vše, co nemusí být nutně připojeno k internetu.
- **Dobře schované zálohy s aktivní ochranou proti ransomwaru** – zajistit, že jsou zálohy absolutně nedobytné, buď střídavým vypínáním úložišť, využíváním pásek anebo striktním dodržováním pravidla 3-2-1 (ukládáním záloh offsite). A pokud již dojde k nejhoršímu, pak s pomocí aktivní ochrany zabránit šifrování dat v samém zárodku. ■



Aleš Hok



Autor článku je Sales Manager ve společnosti Zebra systems, kde odpovídá za prodej řešení Acronis.