Advokáti terčem kybernetických vyděračů. Za odšifrování spisů požadují výkupné

Martin Drtina
martin.drtina@economia.cz

Kybernetické útoky se v poslední době nevyhýbají ani velkým českým advokátním kancelářím. V nich je celkem standardem, že veškeré spisy jsou vedené pouze v elektronické podobě. Stačí pak, aby útočník pronikl do hůře zabezpečené vnitřní sítě a nechal na disku v centrálním úložišti zašifrovat data. Poté může požadovat výkupné výměnou za dešifrovací klíč.

Firma pak má na výběr ze dvou možností: buď má k dispozici čerstvou zálohu, ze které data obnoví, anebo raději výkupné zaplatí. Do té doby pro ni zůstávají data nepřístupná. Prakticky to znamená, že se advokáti po určitý čas nedostanou ani do práce, protože jim přestanou fungovat přístupové kartičky, ani k dokumentům, které nutně pro svoji práci potřebují.

Takzvaný ransomware neboli vyděračský software využívá nedostatky v zabezpečení elektronických systémů. Loni jimi byla v Česku podle studie The State of Ransomware 2021 zasažena téměř třetina středních a velkých organizací. Čtvrtina z nich požadované výkupné zaplatila. Tyto platby probíhají v bitcoinech, aby byly obtížně dohledatelné. Útočníci podle typu oběti požadují částky v přepočtu od desítek tisíc až po jednotky milionů korun.

Počtem ohlášených společníků patří advokátní kancelář Michala Žižlavského k nejvýznamnějším hráčům v insolvenčním byznysu. Spravuje přes 4100 insolvenčních případů a vedle toho vykonává i advokátní praxi. Její webová prezentace začíná nadpisem „bezpečná řešení“. Na konci května však podobný osud potkal i ji. Podle informací HN kancelář čelila útoku kybernetických vyděračů a nakonec na jejich podmínky přistoupila.

„Ačkoliv máme robustní IT infrastrukturu, do které průběžně investujeme miliony korun, samo o sobě to nestačilo,“ přiznal útok Michal Žižlavský, který současně vyloučil, že by došlo ke ztrátě klientských dat. K tomu, kolik za klíč k dešifrování disků jeho kancelář zaplatila, se s ohledem na probíhající vyšetřování vyjádřit odmítl. Připustil ale, že útokem vznikla škoda nejméně v řádu stovek tisíc korun.

Insolvenčním soudům útok Žižlavského kancelář neoznámila. „Obávali jsme se toho, že bychom mohli vyvolat paniku, která by narušila řádný průběh mnoha řízení,“ zdůvodnil Žižlavský. Oznámení však zaslal Úřadu pro ochranu osobních údajů a Národnímu úřadu pro kybernetickou a informační bezpečnost. Jeho mluvčí Jiří Táborský řekl, že u subjektů nespadajících pod zákon o kybernetické bezpečnosti jsou taková oznámení dobrovolná.

„Nahlášení incidentů i ze strany neregulovaných subjektů vítáme, protože se díky tomu dozvídáme další informace o aktuálních hrozbách,“ dodal Táborský s tím, že podle závažnosti útoku NÚKIB v takovém případě poskytne poradenství, jak konkrétní ransomware útok zvládnout a vrátit postižené systémy zpátky do provozu.

Vzhledem k tomu, že ve spisech advokátů jsou uložena i osobní data klientů, podléhá každý takový případ povinnému hlášení také strážcům osobních dat. Mluvčí ÚOOÚ Vojtěch Marcín potvrdil, že se případem úřad zabývá. Vzhledem k tomu, že jde o neukončené řízení, konkrétní být nechtěl. Z hlediska možného postihu je podle něj důležité, jaká opatření správce dat přijal před útokem a posléze ke zmírnění škod. „Uplatňujeme přístup, že když jsou správcem přijatá opatření adekvátní a incident nevznikl důsledkem systémového pochybení, sankce z naší strany zpravidla udělena není,“ uvedl Marcín.

Česká advokátní komora se podle mluvčí Ivy Chaloupkové s podobným případem, kdy by se advokát stal terčem hackerského útoku, dosud nesetkala. Na rozdíl od ztráty například podpisové knihy jí však členové bezpečnostní incidenty ve svých systémech ani hlásit nemusí. „Takovou povinnost právní ani stavovské předpisy advokátům výslovně neukládají,“ uvedla Chaloupková s tím, že v tomto konkrétním případě Žižlavského kancelář komoru informovala datovou zprávou o tom, že po dobu několika dnů musela z bezpečnostních důvodů své databázové systémy vyřadit z provozu.

V insolvenčních řízeních právě nedostupnost dat může být velkým problémem. Například v oddlužení je výplata mzdy dlužníka zasílána přímo na účet insolvenčnímu správci a ten odpovídá za to, že bude včas a podle rozvrhu splátek zaslána jednotlivým nezajištěným věřitelům na umoření jejich pohledávek.

Žižlavský připouští, že v ojedinělých případech k nedodržení příslušné lhůty dojít mohlo. „Pokud někde došlo k porušení lhůty, šlo o jednotky dní. Takové případy budeme řešit individuálně, jakmile je zjistíme,“ uvedl v odpovědi na otázky HN.

Výhodou insolvenčních správců oproti advokátům je, že celý obsah spisu je veřejně přístupný v insolvenčním rejstříku. Pokud tedy přijdou o data ve svých počítačích, mohou si příslušné dokumenty najít a stáhnout z webu spravovaného ministerstvem spravedlnosti.

U advokátních spisů však podobná možnost chybí. Když se ztratí data advokátům a nemají aktuální zálohu, ze které by je mohli obnovit, nezbývá jim než objíždět jednotlivé soudy, nahlížet do spisů a postupně si je rekonstruovat na základě pořízených fotokopií.

Hackeři útočí na firmy *Ransomware neboli vyděračský software loni v Česku zaútočil téměř na třetinu středních a velkých organizací.* **Foto: Shutterstock**