Útoky po napadení Microsoft Exchange budou pokračovat

Připravte se, dokud je čas!

Maroš Barabas, Tomáš Sláma

Nedávno odhalená vlna útoků tvrdě zasáhla tisíce uživatelů poštovních serverů po celém světě. Rozsáhlý incident, využívající zranitelnosti jednoho z nejrozšířenějších softwarových produktů společnosti Microsoft, postihl jednotlivce, firmy a úřady i v České republice. Všichni teď stojí před výzvou, jak minimalizovat škody a jak se chránit před nebezpečím dalšího napadení.

Zahájení útoku na Microsoft Exchange Server, který slouží k výměně e-mailových zpráv a sdílení zdrojů, se datuje ke 3. lednu 2021. Než došlo k jeho odhalení, měli útočníci více než dva měsíce času kompromitovat systémy uživatelů po celém světě, především v Evropě a Americe. Jen v tuzemsku byly napadeny tisíce firem a institucí, řada z nich přišla o data, další se toho musí obávat.

Nejde o to, zda, ale kdy dojde ke zneužití odcizených dat

Útočníkům se podařilo zneužít až čtyř zero-day zranitelností a za pomoci spuštěného kódu získat přístup k bezprecedentnímu množství e-mailových účtů na serveru. Microsoft sice záhy vydal příkaz k záplatování, ale okolnost, že se podařilo zabránit v dalším přístupu útočníků k serveru, rozhodně nemůže být důvodem ke klidu.

Firmy si dnes nemohou být ani přes relativně brzkou instalaci záplat jisté, že z jejich systémů neunikla prostřednictvím odcizených e-mailů řada důvěrných informací – kontakty, adresy, částky, faktury, projekty, rodná čísla, jména zaměstnanců, investice, smlouvy… Experti na kybernetickou bezpečnost doporučují i nadále maximální míru obezřetnosti.

Uživatelé napadeného serveru, a to i ti, kteří nebyli přímo kompromitováni (nebo si to alespoň myslí), by měli mít na paměti, že hackeři si mohli – s pravděpodobností hraničící s jistotou – vytvořit v některých napadených systémech zadní vrátka a v budoucnosti je bezpochyby využijí k dalším útokům za použití těch nejsofistikovanějších postupů.

Zkušenosti odborníků ze společností, které poskytují firmám a institucím kybernetickou ochranu, ukazují, že útočníci, kteří již získali přístup k citlivým informacím, se následně pokoušejí ukradená data efektivně zpeněžit, prodat na černém trhu nebo využít k dalším útokům, především pomocí metod sociálního inženýrství.

I bez důkazů je rozumné předpokládat, že ke kompromitaci došlo

Počet útoků a jejich hrozba stále roste. Představa, že by tomu mohlo být v dohledné budoucnosti jinak, se míjí s realitou. Důvodem je pokračující digitalizace, s níž jde ruku v ruce narůstající složitost systémů, které jsou pro fungování společnosti stále důležitější. Oblast kybernetické bezpečnosti se přitom v České republice dlouhodobě potýká jak s nedostatkem zkušených IT expertů, tak s přetrvávajícím přístupem řady společností v duchu „nám se tohle stát nemůže“.

Nedávný masivní útok názorně ukázal, na jak tenké hraně takové přesvědčení balancuje. V případě incidentu s napadením Microsoft Exchange Serveru byly společnosti, které využívají jeho služeb, náhle a bez varování postaveny před zcela konkrétní a neodkladné výzvy: prověřit, zda mohly být kompromitovány, rozhodnout, jak omezit škody, ale hlavně – ujasnit si, jak se chránit před reálnou hrozbou dalšího útoku.

Minimalizace dopadů incidentu počítá s okamžitou aktualizací Microsoft Exchange Serveru a aplikací bezpečnostních záplat, včetně následné detekce pohybů dat v síti. Samozřejmostí by mělo být i pravidelné zálohování dat, a to tak, aby k nim měly zajištěný přístup všechny klíčové osoby, a to vždy a za každých okolností.

Výše uvedené povinné kroky však neřeší tu nejpalčivější otázku: co když se to bude opakovat? Co když si útočník, který kompromitoval systém, stihnul stáhnout naši poštu? Nyní už sice nemá přístup k Exchange serveru, resp. naší aktuální konverzaci, ale přesto nám bude kupříkladu schopen na základě získaných informací zaslat e-mail, který bude, ač podvržený, působit naprosto věrohodně.

Problém tedy je, že se k někomu, kdo s námi nemá dobré úmysly, mohlo dostat množství důvěrných informací, které si firma někdy s někým přeposílala. A nejen to – pokud si hacker informace stáhnul, tak nyní ví, jak daná společnost s okolím komunikuje, a může na tuto komunikaci navázat. Následný útok je pak o to sofistikovanější a jeho následky mohou být fatální.

Každá firma využívající poštu od Microsoftu by měla zcela rozumně předpokládat, že jejich Exchange server byl kompromitován. A to i kdyby pro to zatím nebyly jasné důkazy. Musí počítat s tím, že útočník má jejich citlivá data a kontakty a zná veškeré podrobnosti o tématech, o nichž se v e-mailech píše. A co je ještě důležitější, nikdy nelze mít jistotu, že útok nezasáhl některého z partnerů, s nímž nadále komunikujeme.

Je možné, že Microsoft časem zveřejní instrukce, na jejichž základě budeme schopni zjistit, zda se hackeři dostali právě k našim citlivým informacím. Útočníkům jde proto o čas a je pravděpodobné, že mnozí z nich zaútočí co nejdříve, aby se pokusili odcizené informace zpeněžit. Jiní se naopak chovají tak, že si raději v tichosti počkají, často i několik měsíců, a udeří později, až bude relativní klid a ostražitost uživatelů opadne.

Neposkytujte žádné informace lidem, o nichž nic nevíte

Pokud tedy hrozí, že jsme mohli být kompromitováni, bezodkladně tuto zprávu poskytněme svým zaměstnancům, dodavatelům,

upozorněme každého, koho se to může týkat: Dávejte si prosím následující dny, týdny a měsíce velký pozor na to, kam klikáte, jaké přílohy otevíráte, s kým komunikujete. Hlaste jakoukoli podezřelou aktivitu.

Pokud je v tu chvíli správně nastavený Exchange s jasně definovanými pravidly přicházející pošty, měl by odhalit, který e-mail nepřichází z domény, již obsluhuje, a měl by ho označit jako nevyžádanou poštu. Na to však nelze spoléhat, protože útočník může kombinovat phishing, tedy v tomto případě podvodný e-mail, s vishingem, falešným telefonátem, a zavolat: Zdravím vás, poslal jsem vám ten e-mail, můžete se podívat, jestli vám to omylem nespadlo do nevyžádané pošty?

Právě toto riziko představuje pádný důvod pro to být apriori obezřetný. Neposkytujte informace lidem, kteří s naprostou samozřejmostí tvrdí, že jsou ti a ti, ale vy o nich přitom nic nevíte. Všechno si ověřujte, především v případě finančních transakcí. U obdržených faktur si jejich relevanci vždy ještě pro jistotu potvrďte u partnera telefonicky.

Nejlepší způsob ochrany firmy je vyškolit zaměstnance

Z dosud uvedených náznaků doporučované ochrany před pokračujícími útoky metodami sociálního inženýrství vyplývá jedna klíčová věc. Pokud chcete zabezpečit svoji společnost, můžete vystavět sebedokonalejší hradbu, ale najde-li útočník její nejslabší místo a překoná ho, je vám to na nic. A první věc, na niž se zkušený útočník vždy zaměřuje, je lidský faktor.

Dříve či později, často právě pod vlivem událostí, jako byl útok na Microsoft Exchange Server, dojde každé zodpovědné vedení firmy k poznání, že nejlepší způsob ochrany je vyškolit své lidi. Stačí jediné nevinné kliknutí unaveného, roztržitého nebo nepoučeného zaměstnance, jediný neověřený e-mail a veškeré nákladné technologické bariéry jsou náhle na vedlejší koleji.

Bezkonkurenčně nejefektivnější prevencí proti útokům jsou dobře proškolení zaměstnanci. Dobře proškolení však neznamená, že ti lidé jednou za čas někde v zasedačce „odzívají“ klasickou přednášku o možném nebezpečí otevírání nevyžádané pošty v podobném duchu, v jakém se dnes pracovníci běžně školí při BOZP.

Současným interaktivním trendům ve školení proti útokům metodami sociálního inženýrství není nic vzdálenějšího než standardizovaná jednorázová sezení. Už i v České republice dnes najdeme společnosti, které poskytují služby v rámci security awareness na světové úrovni. Takové dlouhodobé řešení obnáší komplexní učení, které zahrnuje nejenom propracovaný e-learning a podrobné on-line školení, ale především řadu metod, jejichž účelem je školeného zaměstnance maximálně zaujmout.

Jedná se o sérii promyšlených a zajímavě podaných kroků, které mají za cíl v průběhu určitého období intenzivně a opakovaně atakovat pozornost zaměstnanců tak, aby se jim dané téma dostalo pod kůži. Aby považovali kybernetickou bezpečnost za poutavý námět k hovoru, řešili ji se svými kolegy, bavili se o ní při běžné konverzaci.

Nejmodernější metody školení jsou k dispozici i v ČR

K tomu, aby se téma kybernetické bezpečnosti stalo přirozenou součástí firemní kultury, se využívají nejrůznější propracované metody, postupy a technologické nástroje. Součástí takového školení je i intenzivní a specifické přezkušování zaměstnanců. Školitelé například dovedou v rámci služeb sociálního inženýrství vytvořit kontrolované phishingové nebo vishingové útoky, které nasměrují přímo na konkrétní pracovníky. Ti se tak učí správně reagovat a čelit jak falešným e-mailům, tak i podvodným telefonátům, ať už v češtině nebo angličtině.

Některé atraktivní platformy spojují zajímavým způsobem testování zaměstnanců s dalším učením. Příkladem může být špičková americká platforma KnowBe4, která umožňuje přesně zjistit, co dělá konkrétnímu zaměstnanci největší problém, a zaměřit se na individuální řešení jeho nedostatků.

Lektoři nabízejí svým klientům také workshopy určené pro větší skupiny lidí. Během nich jim – pokud s tím dotyční souhlasí – pouštějí falešné telefonáty, jimiž byli zaměstnanci v rámci testování oklamáni. Cílem není daného pracovníka vystavit pobavené reakci kolegů, ale zaujmout je, překvapit, vtáhnout do dané situace, a to i tím, že ji v případě potřeby záměrně odlehčí.

Nejde o nějaký frustrující rozbor chyb, smyslem je zájemcům vysvětlit nejčastější postupy útočníků, ukázat, jak snadno lze pod uměle vyvolaným tlakem udělat chybu a především pak, jak se takovému zákeřnému útoku bránit. Právě tyto názorné metody se ukazují jako nejlepší způsob, jak si lze vštípit správné reakce – zkušenost vlastním prožitkem je v tomto případě natolik intenzivní, že ji už nikdo z účastníků školení nezapomene. Více informací naleznete na www.socialing.cz. ■

Příklad obrany proti útoku metodou sociálního inženýrství

Ačkoli nevíme, zda jsme byli my nebo náš obchodní partner kompromitováni, nadále spolu komunikujeme. Jednáme o obchodních záležitostech, standardně si vyměňujeme e-maily, řešíme faktury.

A do toho se ve vhodnou chvíli vloží útočník s podvrženým e-mailem, který je úplně stejný jako všechny ostatní, které si s pracovníkem našeho obchodního partnera běžně posíláme. Jedná se o klasickou pokračující konverzaci s veškerou historií, se stejnými formulacemi, firemními logy, kontakty a podobně. A v takovém e-mailu se jednou může objevit i na první pohled zcela nevinná poznámka: Tak tady je ta faktura, o které se bavíme, jenom ještě pro jistotu upozorňujeme na změnu čísla našeho účtu...

Z takového e-mailu nepoznáme, že jde o podvrh, jediná šance je si to okamžitě telefonicky ověřit: Paní Nováková, dostal jsem teď od vás e-mail s fakturou na částku X za službu Y ze dne Z. Opravdu máte nový účet? Mohla byste mi prosím pro jistotu nadiktovat číslo účtu, na který mám ty peníze poslat?

Maroš Barabas

Autor článku působí ve společnosti AEC na pozici Head of Product Management.

Tomáš Sláma

Autor článku působí ve společnosti AEC na pozici Head of Security Assessment Division.