E-Bezpečí 2020, 5(1): Page 86-91. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1840

ZA KYBERNETICKÉ ÚTOKY ČASTO NEMOHOU "HACKEŘI", ALE OBYČEJNÉ LIDSKÉ CHYBY. PREVENCI KYBERNETICKÉ BEZPEČNOSTI V KRITICKÉ INFRASTRUKTUŘE NESMÍME PODCEŇOVAT!

Kamil KOPECKÝ

Hackerské útoky, útoky na kritické prvky infrastruktury, nemocnice, bankovní sektor, dokonce i útoky na počítač pana prezidenta, to vše plní pravidelně stránky online i offline masmédií a v běžném čtenáři budí často mylnou představu, že jsme pod neustálým kyberútokem neznámých hackerů a hackerských skupin, které se snaží zlikvidovat naši zemi. To však docela dobře zvládáme sami, velká část útoků je totiž způsobena nezodpovědným lidským chováním samotných zaměstnanců, kteří moderní IT technologie používají. Často pak při odhalování příčin bezpečnostních problémů vidíme především podcenění prevence, než sofistikovaný útok.

Na úvod je třeba říci, že samozřejmě **k cíleným útokům na konkrétní internetové uzly čas od času dochází**. Útoky pak probíhají např. tak, že konkrétní uzel či vrstvu (webovou stránku, mailový server, databázový server apod.) přetížíme velkým množstvím požadavků z různých zdrojů (tzv. botnetů či zombie počítačů), které daný internetový bod nezvládne zpracovat a zasekne se (tzv. DDoS útok - distributed denial of service). Poté nefungují ani systémy, které na daném uzlu závisí - třeba se nám nenačtou webové stránky, nefunguje pošta, nedostaneme se k

datům, přestane fungovat online bankovnictví, databáze úřadů apod. Technologickým nadšencům určitě doporučuji přečíst si např. tento článek, ve kterém jsou tyto typy útoků popsány poměrně detailně.

Pozor, to, že webové stránky nefungují, nemusí být vůbec způsobeno tím, že by k DDoS útoku docházelo, problém může být třeba v tom, že poskytovatel webových služeb jednoduše neodhadl, jak budou stránky zatěžovány přístupy běžných uživatelů!

Další možností útoku "hackera" je **využití různých druhů chyb, které se vyskytují v podstatě u všech druhů operačních systémů a obecně u software jako takového**, proto je velmi důležité pravidelně veškerý software aktualizovat. Díky využití chyb se totiž útočník dostane třeba do míst na disku, kam by běžně neměl mít přístup, která infikuje svým vlastním kódem - díky chybám získá např. administrátorská práva a začne systém kontrolovat, dostane se do databáze, získá zašifrovaná (ale často i nezašifrovaná) hesla, privátní soubory, účetnictví, osobní údaje o zaměstnancích, informace podléhající obchodnímu tajemství apod. S příchodem velkého množství zařízení připojitelných k internetu (IoT zařízení) se objevil další problém - útočník může do počítačové sítě proniknout nejenom prostřednictvím běžného počítače, ale také prostřednictvím veřejně přístupné IP kamery (třeba v rámci dětské chůvičky), nezabezpečného routeru, chytré ledničky či chytré televize apod. Nemluvě o tom, že často není nutné hledat v těchto zařízeních chyby v software, ale stačí využít běžného defaultního hesla pro vstup do administrativního rozhraní, které velká část uživatelů nemění a nechá ho přednastaveno od výrobce (typicky 0000, 1111, 12345, admin, root apod.). S pravidelností pak média informují o tom, jak "hacker" pronikl do domácí sítě a např. pořídil fotografie dítěte - jenže onen průnik do sítě bylo prostě jenom připojení k nezabezpečenému zařízení.

Nyní se dostáváme k lidským chybám. Těch je celá řada a často také stojí u celé řady incidentů, které dokázaly odstavit velkou část instituce. Klasickou **lidskou chybou je infikováním počítače různými druhy malware** (škodlivý software, ke kterému patří např. keyloggery, viry, červi, spyware, trojské koně, různé

backdoory apod.) - a to **prostřednictvím otvírání neověřených příloh emailů či dalších online souborů**. S malwarem se setkáme jak u běžných desktopových počítačů, tak u tabletů a smartphonů - např. při instalaci různých druhů neprověřených aplikací. Běžný malware jde ve většině případů z počítače odstranit, aniž by napáchal větší škody - v případě pravidelných záloh (např. v cloudu) pak máme jistotu, že většina našich dat virový útok přežije.

K problematickým druhům malware pak patří tzv. **ransomware, který funguje trochu jinak a je více nebezpečný** - kromě toho, že napadne náš operační systém a znemožní nám např. počítač standardně nastartovat (což zas tak velký problém není), rovněž v některých případech začne šifrovat naše osobní soubory velmi silnou šifrou, kterou často nelze překonat (používá např. dva šifrovací klíče, jeden statický a jeden vytvořený dynamicky - např. v závislosti na čase a hardware našeho počítače). Po odvirování počítače pak sice nemáme v počítači ransomware a operační systém funguje, ale naše soubory jsou znehodnoceny a nejdou používat. Za rozšifrování a odblokování počítače pak tvůrci ransomware požadují výkupné (odtud název ransomware - ransom = výkupné), které je třeba uhradit např. pomocí kryptoměn, nebo špatně sledovatelných transakcí. Pokud nezálohujeme a nemáme k dispozici velké finanční obnosy (výpalné na rozšifrování souborů např. dosahuje desítek až stovek tisíc korun, samotné odblokování pak obvykle několik tisíc korun), naše data už nezískáme. Řešením jsou samozřejmě pravidelné zálohy.

Nutno říci, že **v řadě útoků na kritické prvky infrastruktury stál za incidenty právě ransomware**, který se do počítačové sítě dostal buď pomocí bezpečnostní chyby (neaktuální software) nebo právě díky lidskému faktoru. Běžný uživatel online služeb je k otevření zavirované přílohy často donucen velmi sofistikovanými způsoby - např. v případě tzv. sextortion (scam) byli uživatelé přesvědčováni, že pachatelé pomocí webové kamery nahrávali jejich sexuální aktivity před monitorem a pokud nezaplatí výkupné, bude jejich záznam (např. z masturbace) zveřejněn na internetu. V příloze k emailu pak bylo “fiktivní video”, které v řadě případů obsahovalo virus. Cílem pak nebylo primárně infikovat počítač, ale hlavně vystrašit uživatele a přinutit je k ukvapené reakci. Podobně se pak choval tzv. policejní virus, který opět strašil uživatele tím, že

zachytil jejich nelegální aktivity v oblasti dětské pornografie a policie požaduje zaplacení “pokuty”. I zde však šlo o podvod.

{loadposition souvisejici}

Dalším typem **podvodu, který je postaven na lidské chybě, je scam**. Jeho cílem je vylákat z uživatelů peníze, a to pomocí nejrůznějších smyšlených příběhů. Sem patří např. podvodné loterie, scam419 (tzv. Nigerijské dopisy), stále častější romance scam (vojáci z afghánistánu apod.), investment scams (zaručené výdělky díky investicím) apod. Zde je však primárně poškozen důvěřivec, který na tento druh podvodu naletí - terčem bývají často např. senioři, kteří uvěří pohádce třeba o tom, že jejich předek byl nesmírně bohatý, zemřel v zahraničí a vy jste dědic, který zdědil neuvěřitelné bohatství. Stačí jediné, zaplatit bankovní poplatky za převod peněz ze zahraničí.

Velký **problém představuje phishing, který je opět postaven na lidské chybě** a který může ohrozit fungování celé instituce. V praxi jde o podvod postavený na tom, že je uživateli podsunuta napodobenina oficiálního oznámení (e-mailu) nějaké důležité autority (třeba banky), která obsahuje odkaz vedoucí na falešný web, který je klonem oficiálních stránek instituce. Odkaz a samotný web pak obsahuje drobné odchylky - třeba v názvu domény instituce, které však neznalý uživatel často přehlédne (míst www.csob.cz je např. www.cosb.cz). Cílem phishingu je získat od uživatele klíčové osobní a citlivé údaje, např. jméno a heslo, pod kterým se do systémů přihlašuje, a emailovou adresu, která je s účtem spojena. Samozřejmě přihlášení na podvodné stránky se nedaří a uživatel stále zadává a zadává své přihlašovací údaje, které předává tvůrcům tohoto podvodu. Díky získaným údajům jde pak např. proniknout na e-mail, na účet do sociálních sítí atd. Uživatelé velmi často (podle některých výzkumů až v 50 procentech případů) používají univerzální hesla - tj. stejné heslo pro přístup k různým službám - v řadě případů se takto útočník dostal třeba do firemního intranetu, firemních databázových systémů apod.

Čas od času se k testování firemních zabezpečení používají různé druhy “nástrah” v podobě volně ležících flash disků, které slouží jako návnady. Tímto způsobem pak mohou výzkumníci otestovat,

kolik pracovníků dané firmy/instituce do svého počítače bez přemýšlení připojí neznámý flash disk ponechaný na stole. Podle zjištění společnosti Servodata více než 60 procent zaměstnanců do svého počítače připojí neznámý flash disk ponechaný na stole. Tomuto způsobu testování bezpečnosti se říká **baiting** (USB baiting, dříve také CD baiting).

Na závěr je třeba říci, že odpovědnost za kybernetickou bezpečnost institucí nelze přehrávat pouze na firemní/institucionální ajťáky a další "nerdy" či "geeky". Je třeba začít u samotných zaměstnanců, vypěstovat v nich základní bezpečnostní návyky a pravidelně je s aktuálními hrozbami seznamovat. Samozřejmostí by pak měly být automatické aktualizace, zabezpečení aktivních síťových prvků (routery apod.), všech veřejně dostupných zařízení připojených do sítě a samozřejmě aktuální antivir. Až budete opět v médiích číst titulky o kybernetickém útoku na instituce, nezapomeňte, že v řadě incidentů je problém v lidském faktoru - samotných zaměstnancích.

Pro E-Bezpečí
Kamil Kopecký
Univerzita Palackého v Olomouci