INSPO – informační a komunikační technologie pro osoby se specifickými potřebami
30. března 2019, Kongresové centrum Praha

NEJČASTĚJŠÍ HROZBY NA INTERNETU

Pavel Bašta
CZ.NIC, zájmové sdružení právnických osob
Milešovská 1136/5, Praha 3, 130 00, pavel.basta@nic.cz

Anotace: *Kybernetická kriminalita je dnes velmi často diskutovaným tématem. Pro firmy, ale i pro jednotlivce může znamenat nemalé finanční ztráty a přitom nelze říci, že by někdo byl proti těmto útokům zcela imunní. Kyberzločin si nevybírá, a proto by se o něj měli zajímat všichni, kdo s informačními technologiemi běžně pracují. Hrozby však nemusí přicházet pouze od anonymního kyberzločince. Jeho metody mohou proti nám použít i lidé, kteří jsou motivováni jiným než zištným způsobem. Ať už se jedná o osobní zášť, žárlivost, nenávist vůči odlišné skupině (hate crime) nebo třeba voyerismus. Každý by tedy měl znát hrozby, které na něj v on-line světě číhají, být schopen je rozpoznat a adekvátně zareagovat, pokud to situace vyžaduje. Jako provozovatelé CSIRT.CZ, tedy národního CSIRT (Computer Security Incident Response Team) České republiky, máme s těmito hrozbami bohaté zkušenosti.*

Nejčastější hrozby

S příchodem Internetu se svět velmi změnil. Jsme stále více závislí na informačních technologiích a řada z nás tráví jejich využíváním, ať už v práci nebo v soukromí, často i větší část dne. Proto není překvapením, že se do tohoto prostředí přesouvá i část zločinnosti, která byla dříve možná pouze v reálném světě. Jedná se o celou plejádu negativních jevů. Od zneužívání nezletilých, přes nebezpečné pronásledování, vydírání, podvody až po krádeže. Stejně jako v reálném světě, tak i v kybersvětě platí, že v některých případech můžeme ovlivnit míru pravděpodobnosti, že se staneme obětí útoku, nebo můžeme toto riziko dokonce úplně eliminovat.

Ovšem k tomu, abychom mohli hrozbám předcházet, potřebujeme vědět, čemu máme čelit a jakou podobu na sebe kyberzločin může brát. Mezi nejběžnější hrozby řadíme krádeže a zneužití přihlašovacích údajů, malware, napadení sítě a síťových zařízení nebo DoS a DDoS útoky.

Krádeže a zneužití přihlašovacích údajů jsou jedním z nejčastějších problémů. Na síti lze nalézt soubory obsahující seznamy uživatelských e-mailů nebo jmen s příslušnými hesly. K únikům těchto údajů ze serverů dochází celkem často a jako uživatelé je nemáme šanci ovlivnit. Můžeme však ovlivnit, zda takto uniklé údaje bude moci útočník dále zneužít.

Nicméně k únikům uživatelských údajů může dojít i jinými způsoby, jako jsou krádež s pomocí keyloggeru, hádání hesla, sociální inženýrství nebo třeba jejich odchycení na síti. Takto získané přihlašovací údaje pak může útočník zneužít k dalším útokům. Může se jednat o neoprávněný převod finančních prostředků z on-line bankovnictví, nejrůznější podvody, útoky na soukromí, kyberšikana, stalking, krádeže identity, ale třeba i získání nějaké jiné výhody, jako je třeba zlepšení prospěchu žáka, kterému se úspěšně podařilo proniknout do informačního systému školy.

Důležité je mít nejen dobré heslo, tedy ideálně náhodný řetězec znaků, písmen a čísel, ale také správné nakládání s hesly. Nepoužívat stejné heslo pro více služeb, heslo nikdy nikomu nesdělovat, dávat pozor kde heslo zadávám a tam, kde to služba umožňuje, využívat dvoufaktorové ověření.

Další velkou skupinou útoků, které je potřeba se věnovat, jsou ty, které využívají nějakou formu škodlivého kódu. Malware (malicious software) má dokonce svou taxonomii a rozeznáváme tak viry, rootkity, červy, trojské koně, rasnomwary a řadu dalších. Z pohledu běžného uživatele je však podstatné, že nechce žádný z těchto kódů ve svém počítači mít, a že by tedy měl mít představu, jak napadení svého počítače předejít. K tomu je opět potřeba vědět, jakým způsobem může dojít k útoku na uživatele.

Nejčastější cesty pro napadení počítače jsou stále přílohy podvodných e-mailů, odkazy zasílané přes on-line komunikační platformy, ale také útoky s využitím nejrůznějších zranitelností. To je také důvod, proč bychom měli věnovat nejprve pozornost samotné příloze a neotevírat a stahovat ty, o kterých si nejsme jistí, co obsahují. A dále, proč bychom měli pravidelně záplatovat veškerý používaný software, který máme v PC, ale i v dalších zařízeních. Malware pak může pro uživatele znamenat narušení soukromí, ztrátu dat nebo zapojení uživatelova zařízení do dalších útoků bez vědomí samotného uživatele.

Další častý problém, kterému mohou uživatelé čelit, je napadení sítě, či síťového zařízení. V případě běžných uživatelů se obvykle jedná o problém se špatně zabezpečenou WiFi sítí, nebo o napadení domácího routeru. Nejčastějším důvodem napadení bezdrátové sítě je buď úplná absence zabezpečení (tzv. otevřené sítě), použití nevhodného zabezpečení (WEP), nebo špatná konfigurace vybraného zabezpečení (WPA-PSK se slovníkovým heslem, ponechání výchozího nastavení).

Pokud jde o napadení samotného routeru, nejčastěji dochází buď k manipulaci s nastavením DNS a následně přesměrováním všech zařízení na falešné webové stránky, nebo k instalaci škodlivého kódu a následnému zneužití zařízení k dalším útokům. Tím, že útočník získá přístup k síti, může sledovat síťový provoz a v závislosti na dalších okolnostech může odposlouchávat hesla nebo třeba pozměnit obsah přenášených dat. Důležité je tedy používat i pro přístup k domácí bezdrátové síti neslovníkové heslo a využívat zabezpečení WPA2-PSK.

Napadení chytrých zařízení si zaslouží zvláštní pozornost. Často jsou trvale připojena k síti, přitom jejich zabezpečení bývá opomíjeno jak samotnými uživateli, tak bohužel někdy i výrobci. K samotnému napadení těchto zařízení dochází nejčastěji buď kvůli laxnímu přístupu uživatele, který nechá zařízení ve výchozím stavu a nezmění ani přihlašovací heslo, nebo kvůli neopraveným zranitelnostem.

Protože se jedná o relativně levné spotřební zboží, je zde patrná snaha výrobců každý rok oznámit nová a vylepšená zařízení, ovšem často se pak stane, že se o starší typy přestane zajímat a vytvářet pro ně bezpečnostní záplaty. Takové zařízení pak může být zneužito pro útoky proti soukromí uživatele nebo třeba pro další útoky. Známým příkladem je botnet Mirai. Ten dokázal převážně z kamer připojených k Internetu a domácích routerů vytvořit botnet, který se podílel na jedněch z největších DDoS útoků.

DoS a DDoS útoky jsou založeny na principu, kdy dojde k odepření služby uživateli. V případě DoS je obvykle cílem útoku nějaká chyba či zranitelnost, jejíž zneužití vede k výpadku služby. U DDoS, tedy distrbuovaného DoS, mluvíme o útoku z více zdrojů, kdy dojde obvykle k vyčerpání dostupných zdrojů díky zasílání stejného požadavku z mnoha různých zařízení ve stejném čase.

Tyto útoky se obvykle běžných uživatelů přímo nedotknou a jsou mířeny na firmy, které pak bývají vydírány s žádostí o poplatek za ukončení útoku. I běžný uživatel by však měl mít nějaké povědomí. Nejen proto, že se může stát, že se nějaká jím používaná služba stane cílem tohoto útoku a on tak třeba nebude schopen se dostat ke svým datům, ale i proto, že v praxi národního CSIRT jsme zaznamenali útok, směřující přímo na zákazníky internetového poskytovatele, kterým útočník na dálku stále dokola restartoval jejich modemy a tím je vlastně udržoval odpojené od Internetu.