Co nikdo neví, jako by se nedělo

Marian Němec, BA(Hons), AEC a.s.

Souhrn

Oblast kybernetické bezpečnosti se mění velmi dynamicky. Musí reagovat na vzniklé hrozby, musí být schopna reagovat na probíhající i budoucí kybernetické útoky. Položme si však otázku, je to však skutečně možné? Lze se účelně chránit před kybernetickými útoky?

Proč se kyber útoky týkají všech?

Pro kybernetickou bezpečnost se hodí použít Sokratovo známé „Scio me nihil scire“ tedy „Vím, že nic nevím“. Možná tato představa někomu může přijít absurdní, ale faktem zůstává, že kybernetičtí útočníci mají vždy náskok. Bezpečnostní technologie obvykle účinně fungují na známé hrozby, jejich slabým místem jsou nově vzniklé zranitelnosti a hrozby. Tím „obvykle“ je myšleno, že to platí v případě správné konfigurace a použití jednotlivých bezpečnostních prvků. Firmy mají nasazené firewally, IPS sondy, implementována data leak řešení, monitoringy uživatelů i aktivit v síti, ukládají a korelují logy, antispamovou i antivirovou ochranu. Ale riziko napadení kybernetickým útokem je vždy přítomné, protože bezpečnost není a nikdy nebude stoprocentní a k útokům přesto dochází a docházet bude. Je to nikdy nekončící souboj.

S takovým postojem je třeba přistupovat k návrhům bezpečnostní architektury a souvisejících opatření. Bohužel, nezřídka se naráží na odmítavý postoj ze strany managementu a často i odpovědných pracovníků za správu informační a komunikačních technologií. Nejčastějším argumentem bývá tvrzení: „…takové zabezpečení nepotřebujeme, nejsme přece banka….“. V takovém případě bývají veškeré návrhy na kvalitní a efektivní řešení kybernetické bezpečnosti odmítány a jen těžko lze takového člověka přesvědčit, že realita je trochu jiná, že prevence je v konečném účtování to nejlevnější řešení. Stále častější se stává situace, kdy je klient napaden, v lepším případě má pouze paralyzovanou informační infrastrukturu, v tom horším případě přichází o data, případně je jeho vybavení zneužíváno k útokům na jiné, více atraktivní cíle. Tak či tak, stal se obětí útoku a často volá o pomoc u odborných firem a ptá se, co má právě udělat, jak se má ochránit, co si má zakoupit. V takový okamžik by bylo správné říci: „Teď už nic, už je pozdě.“ nebo oblíbené „Já jsem vám to říkal.“ Ale to samozřejmě není možné, i v kybernetickém prostoru je možné se chybami poučit, odstranit akutní problém a důkladně se připravit na další možný útok. Smutným mementem jsou pak firmy, které se staly obětí kybernetické kriminality, přesto se nepoučily a doufají, že blesk neudeří 2x na stejné místo.

Takový riskantní přístup zpravidla vede ke špatným koncům. Obchodníci a manažeři se učí, že předpokládat znamená nevědět nic. Předpokládáme-li, že nejsme zajímavý subjekt pro útočníka z kyberprostoru a proto neřešíme bezpečnost důsledně, je již docela možné, že útok právě probíhá.

Kyber svět je nebezpečné místo

Přítomnost rizika je v celém kyberprostoru trvalá, respektive velikost takového rizika stále roste. Důvodem jsou příčiny kybernetických útoků. Každá činnost je nějak motivovaná, stejně tak kyberútoky. Tou motivací jsou zpravidla peníze, tedy kyber kriminalita, dále pak „dobré úmysly“, na vzestupu však je špionáž a nově s ní související i cyberwar. Za rok 2016 průměrně přes 70% všech útoků bylo způsobeno kriminálními původci. Kyberkriminalita je velmi výnosný byznys, který se však nezaměřuje jen na velké cíle. Jednak proto, že ani útočníci nejsou jen velké organizované skupiny, ale i jednotlivci, kteří si chtějí „přivydělat“. To vše je možné i proto, že rovněž existuje trh s nástroji a službami na kyber útoky. A to nejen na slavném Darknetu. Zajímavé služby pod hlavičkou kybernetické bezpečnosti nabízí například projekt Zerodium. Hodnotit na kolik riziková taková aktivita je, by bylo pouhou spekulací. Zájem jistě existuje, protože za poslední rok se ceny za některé služby ztrojnásobily.

Typické současné útoky lze rozdělit na dva typy. Ty, které při úspěšném útoku o sobě dají vědět a ty, které pokud proniknou do prostředí oběti, dále skrytě působí a šíří se. Jedním z hlavních představitelů prvního typu je ransomware, v současné době zastoupený zejména různými verzemi Cryptolockeru a jeho mutacemi. Když pronikne na počítač, nepozorovaně zašifruje data či uzamkne systém. Následně

požádá o platbu za jejich zpřístupnění. V lepším případě má napadený uživatel možnost systém a data obnovit ze zálohy, v tomu druhém má možnost zaplatit a doufat, že data získá zpět. Varianta s obnovou ze zálohy je však často utopií, zejména u fyzických osob, ale ani firemní prostředí neoplývá vždy kvalitním fungujícím zálohováním. Většinou to skončí dilematem, zda se rozloučit s daty, nebo zaplatit a věřit.

Za představitele druhého typu útoku pak lze považovat tzv. APT (Advanced Persistant Threats) útoky. Tento typ kybernetického útoku je založen na využívání pokročilých, ale rovněž i ověřených technik případně nedostatečně zabezpečené ICT prostředí vybrané organizace. Kromě potřeby zůstat skryt se však APT útoky od ransomware liším ještě jedním zásadním prvkem. Zatímco ransomware v podstatě jen čeká, kdo ho spustí, svou oběť aktivně nehledá a cíleně nevybírá, APT jsou cílené útoky určené k napadení konkrétního cíle. K tomu útočník obvykle využívá postupy, pro které se používá termín „kill chain“. Tento termín poměrně přesně vystihuje princip postupného útoku, kdy útočník nejprve poznává svůj cíl, pak postupně zkouší různé, dle konkrétních potřeb vybrané techniky, a s nimi úspěšně zaútočí. Častým jevem je, že jeden typ známého útoku následně využije pro odvedení pozornosti, aby v okamžiku, kdy zaměstná cíl řešením jednoho problému, proniká do systému jinou cestou. Tím hlavním cílem je získat trvalý a utajený přístup do sítě cíle, kde nadále může vykonávat další činnosti. Od krádeží dat, přes podvrhnutí informací, až po využívání výpočetního výkonu cíle.

Je možné se ubránit?

Bylo by možné si položit otázku, jestli má cenu se bránit podobným útokům. Odpověď je poměrně jednoduchá, i když samotné řešení úplně snadné není. Vyžaduje si velmi profesionální přístup, nemalé finanční prostředky a mnoho investovaného času. Hlavní překážkou stále zůstává podcenění velikosti hrozby a toho plynou všechna další související rizika. Dokud se firma nedostane do situace, kdy se sama stane obětí, nepřipouští si tuto hrozbu. Neuvědomuje si, že takový útok může mít zásadní dopady na funkčnost infrastruktury a s tím související dopady na samotnou existenci firmy, na její byznys.

Je nezbytné pochopit, že samotné pořízení bezpečnostních technologií hrozbu neodstraní. Odborný způsob jejich implementace je zásadní pro správnou funkčnost kybernetické bezpečnosti. Je třeba si uvědomit, že je třeba přijmout určitá omezení z důvodu zabezpečení infrastruktury a související procesní opatření. I obyčejný Cryptolocker v posledních verzi Cryptowall 4.0 dokáže úspěšně proniknout ochranou, která se teoreticky jeví jako dostatečná, avšak IPS sonda je nakonfigurovaná pouze na monitoring, ne na blokování. Systém sice zachytí závadný kód, ale nezastaví ho. Ten tak proniká do vnitřní sítě, a pokud si specialista tohoto hlášení nevšimne včas, je zaděláno na problém. Jakmile je malware uvnitř může začít působit. Proto je důležité implementovat vícevrstvé zabezpečení, které umožní nejenom detekci známého malware, ale také detekci anomálií, které dokáže analyzovat a následně případně zablokovat. Se správně nastavenými procesy, které např. zajistí vhodnou reakci na případné bezpečnostní incidenty, je možné reagovat na útok včas a zejména adekvátně. Technologií, která může významně pomoci, je např. Sandbox, který patří k nejvíce efektivním řešením proti APT útokům a zero-day zranitelnostem.

Avšak nekvalitní implementace bezpečnostních technologií či nevhodná bezpečnostní architektura jsou jedinými nedostatky v bezpečnostním konceptu. Velmi často je opomíjen ten nejdůležitější prvek a tím je člověk. Nejsou tím myšleny jen nedostatečné personální kapacity bezpečnostních pracovníků, ale obecně lidský prvek. Nedostatečně vyškolení uživatelé představují pro kybernetickou bezpečnost stejné riziko jako nekvalitně implementované technologie. V rámci APT útoku lze využít například prvků sociálního inženýrství a proniknout tak do infrastruktury specializovaným malwarem, který umožní útočníkovi získat další možné přístupy, či rovnou celé prostředí získat pod kontrolu.

Ze všeho výše napsaného plyne jediné. Kybernetickou bezpečnost je třeba brát vážně a nepodléhat mylné představě, že právě my nejsme pro útočníky zajímavým cílem. Kyberkriminalita představuje výnosnou činnost a lze tak předpokládat, že dále poroste. Z toho důvodu musíme k řešení kybernetické bezpečnosti aplikovat komplexní přístup. Kromě technologií a jejich správné implementace nezapomínat i na využívání bezpečnostních specialistů, ale s tím musí jít ruku v ruce i nastavení správných bezpečnostních procesů a šíření bezpečnostního povědomí mezi uživateli. Pokud k tomu takto nepřistoupíme, zbyde nám maximálně se obrátit na reverendku Joey Tally z Kalifornie (čarodejnice

specializující na vyhánění zlých duchů a počítačových virů), která vám malware z infrastruktury vyžene pomocí zaříkání.