Debata HN: Kyberbezpečnost

PROTI HACKERŮM SE DÁ BRÁNIT VZDĚLÁVÁNÍM LIDÍ

EXISTUJE VELKÉ NEBEZPEČÍ, ŽE ÚTOČNÍCI BUDOU VYHROŽOVAT ZVEŘEJNĚNÍM CITLIVÝCH DAT, NAPŘÍKLAD O PACIENTECH NEMOCNIC.

Zuzana Keményová
zuzana.kemenyova@economia.cz

Ať už je to volba amerického prezidenta, olympijské hry nebo pandemie koronaviru, významné celosvětové události vždy doprovází vlna hackerských útoků. Masy lidí tyto události sledují, reagují na ně a hackeři toho dokážou využít.

„Posílají zprávy, které s daným tématem souvisí, třeba informaci, kdy dostanete vakcínu nebo že nemocnice zjistila, že máte covid-19. Hackeři hledají vždy ten nejslabší článek. Hodně lidí se odstěhovalo na home office a ze soukromého počítače mají menší šanci se bránit, než je tomu v kanceláři, kde jsou technologie pod dohledem centrálního managementu. Hackeři tedy zranitelnosti na home officu využívají," řekl v on-line diskusi Hospodářských novin Ivan Svoboda, poradce pro kybernetickou bezpečnost společnosti Anect.

Další debatující odborník, Miloslav Lujka ze společnosti Check Point Software Technologies, potvrdil, že právě útoky pracující s tématem pandemie představují v současnosti nejsilnější proud v oblasti těch internetových. „Jsou to různé e-mailové phishingové kampaně využívající ukradených kontaktů z různých databází. (Phishing se obvykle provádí pomocí e-mailů, reklam či webů, které vypadají podobně jako stránky, jež už uživatel zná. Napodobuje e-mail od banky či nemocnice, pozn. red.) V takovém e-mailu vám napíší, že máte pozitivní testy, vy někam kliknete a stáhnete si třeba ransomware (program, který blokuje počítačový systém nebo šifruje data a pak požaduje výkupné za obnovení přístupu, pozn. red.)," popsal Lujka. Například banky se podle něj takovým útokům poměrně dobře brání, na phishing reagují rychle a snaží se své zákazníky před rizikem varovat.

KOMU HROZÍ NAPADENÍ

25,6 %
je podle červnové zprávy Avast Global PC Risk Report 2020 šance, že se běžný uživatel kdekoliv na světě setká s počítačovou hrozbou. Meziročně se toto riziko zvýšilo o více než pět procentních bodů.

15 %
firemních počítačů po celém světě je vystaveno riziku infekce malwarem.

4 %
je riziko napadení firemních počítačů v Česku pokročilým útokem.

Čína
Seznamu států, kde čelí domácí počítače vysokému riziku ohrožení, vévodí Čína, Afghánistán a Venezuela.

22 %
je pravděpodobnost, že uživatel v Česku narazí na jakýkoli druh hrozby. Minulý rok bylo takové riziko 17procentní.

5,6 %
je pravděpodobnost, že Češi budou čelit pokročilému útoku. Vloni míra rizika činila 4,1 procenta.

15 %
firemních počítačů v Česku je vystaveno riziku jakéhokoliv napadení.

Vietnam
Největší pravděpodobnost, že jejich počítače budou muset čelit kybernetickému útoku, mají firmy ve Vietnamu, Bangladéši a Indonésii.

Zdroj: Avast Global PC Risk Report 2020

Test ostražitosti

Všichni diskutující se shodli, že nejlepší prevencí před útoky hackerů je vzdělávání uživatelů, ať už jednotlivců u domácích počítačů, IT expertů či zaměstnanců ve firmách. „Vzdělávat lidi je to nelepší, co může firma udělat, a stojí to nejméně peněz. Bezpečnost by zaměstnanci neměli vnímat jako něco obtěžujícího nebo něco, co jim brání v práci, ale jako to, co je dokáže ochránit. Vedle bezpečnostních směrnic by firmy měly připravit jednoduché desatero, které svým lidem vštípí. Může to být například pomocí e-learningu, který je zakončen testem či kvízem," uvedl Miloslav Lujka.

V jeho firmě například probíhá etický hacking, kdy jedno jejich IT oddělení testuje zaměstnance a tu a tam jim posílá e-mail, který vypadá jako běžná pracovní pošta, ale ve skutečnosti je to test ostražitosti. „Samozřejmě že za to nejsou žádné postihy, ale ten, kdo se nachytá, musí projít dalším školením nebo testem," přiblížil Lujka.

Ve firmě Ivana Svobody zase generální ředitel obchází kanceláře, a když někdo nechá na stole otevřený počítač, přiskočí k němu a jeho jménem pošle žertovný e-mail, například že daný člověk žádá o snížení platu. „Ten zaměstnanec to už podruhé neudělá," podotkl Svoboda.

Zdeněk Bínek, ředitel společnosti Zebra Systems, zase připomněl, že z preventivních opatření často pomáhají i drobnosti, například že se e-mail, který nepochází z firmy, výrazně označí jako externí. „Viděl jsem to na příkladu jedné nemocnice a myslím, že je to krásné a jednoduché opatření, které může mít vysokou účinnost."

Nikdy neplaťte výkupné

Diskutující také přiblížili, kdo jsou vlastně internetoví hackeři. Doby, kdy to byli „týpci v černé kapuci", už jsou dávno pryč, řekl Josef Javora, jednatel společnosti TIS Partners a tvůrce projektu Antihacker.

„Dnes se práce hackerů velmi systematizuje a mají až korporátní chování se vším všudy. Útoky nejsou jedním malwarem (program určený k poškození nebo vniknutí do počítačového systému, pozn. red.), ale je to celá sada útoků, které nejdříve dostanou útočníka do prostředí počítače a pak se snaží získat v něm nějaká privilegovaná práva. Samotný ransomware už může být finále útočné akce a celý útok může trvat třeba rok," upozornil Javora. Stejně tak virus může v počítači dlouhou dobu přebývat, aniž by o něm někdo věděl.

Častým jevem také bývá, že dochází ke kombinaci útoků. Nejen že útočníci zakryptují části počítače, ale zároveň mají ukradená data. A když majitel počítače řekne, že nic platit nebude, protože má data zálohovaná, stejně to nepomůže, protože útočníci mohou majitele vydírat zveřejněním jeho citlivých dat. Josef Javora rovněž zmínil loňský výzkum dánské společnosti CSIS Security Group, zaměřené na kybernetickou bezpečnost, podle nějž 46 procent obětí kyberútoků zaplatilo výkupné.

„Není moc dobrý nápad výkupné platit, protože i když ho zaplatíte, neznamená to, že se útočník z akce stáhne. Je to často skupina lidí, kteří sedí v kancelářích, na dálku spolu komunikují a často si jednotlivé fáze útoků předávají," uvedl Javora. Navíc ten, kdo získal takzvané backdoors, tedy možnost se do systému dostat znovu, má přístup stále a útok může zopakovat.

Zdeněk Bínek dodal, že zvlášť v poslední době existuje velké nebezpečí, že hackeři budou vyhrožovat zveřejněním citlivých dat, například o pacientech nemocnic. „Řešili jsme rovněž situaci jedné italské nápojové firmy, která měla veškeré systémy zálohované a vše by bylo možné obnovit. Ovšem útočníci zcizili osobní data, kvůli této krádeži hrozil postih za porušení GDPR, a tak firma výkupné zaplatila," popsal ředitel Zebra Systems.

Partnery debaty byly:
ANECT
Check Point SOFTWARE TECHNOLOGIES LTD
TISPARTNERS TRUSTED INFORMATION SECURITY
ZEBRA SYSTEMS