16. 6. 2021

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Deset ověřených pravidel, jak se bránit kyberútokům

Českou advokacii nedávno vystrašily zprávy o úspěšných hackerských útocích, které se nevyhnuly ani elitním kancelářím. Společnost SingleCase klade tématu kybernetické bezpečnosti velkou pozornost, a tak ve spolupráci s jedním z největších tuzemských odborníků Tomášem Honzákem připravila deset kroků, jak se bránit před útoky ransomware.

Technologie i hrozby se neustále vyvíjejí, ale základní pravidla zůstávají stejná. Je důležité mít na paměti, že neexistuje žádný zaručený způsob, jak se vyvarovat napadení. Ne náhodou se pro zákeřný software vžil termín "počítačový virus" – paralela s Covidem je téměř dokonalá. Dokud nejsem naočkovaný (nemám aktualizovaný software s posledními bezpečnostními záplatami), riziko nákazy rapidně narůstá a je třeba používat doplňující opatření. V reálném světě to jsou roušky a respirátory, ve virtuálním třeba systémy schované za VPNkou. Místo PCR testů scanujeme soubory antiviry (výhoda pro počítače – napadený soubor lze ihned izolovat). A stejně jako v lidském světě, i zde jsou zásadní hrozbou nové mutace, které umí uniknout počítačovým antivirům.

Pojďme si nyní představit deset prověřených pravidel, jak si vybudovat solidní imunitu a odolnost, aby ani případné úspěšné napadení nenechalo ve vaší síti víc škody, než drobná rýmička nebo banální viróza. Jak už to tak bývá, jejich dodržování není úplně zadarmo, nějaké to úsilí nebo i peníze budete muset vynaložit, ale v porovnání s milionovými škodami, jaké může způsobit ransomware, se to rozhodně vyplatí.

1. Používejte antiviry a antimalware.

Jak Windows, tak i stále častěji používaný MacOs, nabízejí základní ochranu proti virům zdarma, a pro zkušené uživatele a domácí prostředí může takováto ochrana stačit. Ve firmě byste ale měli sáhnout po komerčním řešení, nejlépe s centrální správou a reportingem. Ransomware se neustále vyvíjí a mění, a komerční firmy, které se výrobou antivirů živí, budou mít k dispozici detekci i nástroje na zachycení a zneškodnění malware tak rychle, jak to jenom jde. Spoustu dobrých tipů pro viry i antiviry najdete na serveru 365 tipů publicisty Daniela Dočekala.

2. Pozor na přílohy – nejen od neznámých odesílatelů!

Zavirovaný soubor v příloze mailu je suverénně nejčastější způsob, jakým se ransomware dostane do vaší sítě. Neotevírat přílohy od neznámých odesílatelů, zejména pokud mail neočekáváte, je základní poučka, ale ransomware můžete chytit i od kolegy, nebo někoho, kdo se za něj vydává. Pokud si nejste jisti, důvěryhodnost přílohy si ověřte napřímo s odesílatelem, nejlépe jiným kanálem, anebo podezřelý mail prostě vymažte. Jestli byl opravdu důležitý, odesílatel se vám ozve.

3. Zapněte zobrazení skrytých přípon souborů

Skrývání přípon u známých typů souborů je na první pohled šikovná "vychytávka", která technicky méně zdatným uživatelům zjednodušuje používání systému a zabraňuje riziku, že si člověk "zablokuje" soubor tím, že příponu pozmění nebo odstraní, ale pro útočníka je to vítaný způsob, jak podstrčit spustitelný soubor se škodlivým kódem namísto dokumentu Wordu anebo obrázku.

Nastavení je jednoduché, poučení uživatelů může zabrat více času, ale vyplatí se oboje.

4. Instalujte pouze důvěryhodné programy

Přibalit malware k instalaci legitimního programu je jednouché a účinné, ale o to jednodušší je prevence: software stahujte ideálně z oficiálních "App Store" nebo přímo od výrobce. Nelegální software představuje rizika nejen právní, ale i bezpečnostní. Samostatnou kapitolou jsou rozšíření prohlížečů – tady platí, že méně je více. Rozšíření si totiž často vyžádají přístup ke všem stránkám, a díky tomu mohou nejen odposlouchávat vaše přístupové údaje, ale i spouštět v kontextu webových aplikací škodlivý kód – ať už k dolování kryptoměn nebo k coby ransomware k šifrování souborů, které do cloudové služby ukládáte.

5. Udržujte systém aktuální a zabezpečený.

Sofistikovaný ransomware (jako byl třeba WannaCry) se může šířit i přímo po síti, k čemuž obvykle využívá zranitelnosti v software, který "poslouchá" po síti – sem patří například poštovní servery, databáze, síťové disky apod. Výrobci pravidelně vydávají aktualizace, které zranitelnosti odstraňují, ale neméně důležité je služby, které nepotřebuji, úplně vypnout a přístup k ostatním omezit podle potřeby. Server pro sdílení dokumentů v lokální síti by totiž neměl "poslouchat" po internetu.

6. Používejte důvěryhodné a spolehlivé cloudové (software-as-a-service) služby

SaaS neboli software jako služba může před ransomware pomoci nejen tím, že je logicky oddělena od vaší vlastní sítě, má své vlastní správce IT i bezpečnosti a obvykle je na ochranu před škodlivým software mnohem lépe připravena než téměř libovolná firma, pro kterou je IT "jen" pracovní nástroj, a ne zdroj obživy. Ransomware útočí tím, že "tupě" šifruje soubory na disku a je mu jedno, zda to je dokument Wordu, PDF soubor, tabulka nebo třeba lokální databáze MS Accessu. Cloudová služba typicky znamená webovou aplikaci, která se ovládá přes prohlížeč, s daty pracuje strukturovaně, má oddělenou logickou vrstvu od fyzického úložiště – a tato kombinace je pro ransomware tužší překážka než pro Covid roušky, rozestupy a desinfekce rukou.

7. Pravidelně zálohujte lokální data i samotné zálohy.

Zálohování je nejúčinnější způsob, jak minimalizovat škody, pokud se ransomware do vaší sítě dostane. Proces zálohování by měl být ideálně pravidelný, plně automatický a samotné zálohy je důležité oddělit do samostatné sítě či podsítě, aby se k nim ransomware nedostal. Použitím cloudové služby jako třeba AWS S3 navíc ještě zvýšíte odolnost společnosti proti selhání hardware. A nezapomeňte si zálohovací proces hlídat a občas zkontrolovat, že zálohy jdou obnovit.

8. Dělejte si průběžné audity kybernetické bezpečnosti

Jak už jsme si řekli v úvodu, technologie i hrozby se průběžně vyvíjí. Kromě toho, jsme všichni lidi a děláme chyby, a zkontrolovat, že jsme všechny systémy nastavili a zabezpečili správně, je to nejmenší, co můžeme pro vlastní bezpečnost udělat. Před auditem si projděte doporučení výrobců a odborníků, nebojte se použít mezinárodní standardy a doporučení, jako třeba CIS Controls (EN). Pokud máte větší síť a služby a aplikace si provozujete sami, pořiďte si skenery na detekci zranitelností nebo si nechte technickou bezpečnost pravidelně auditovat profesionální firmou.

9. Mějte plán, co dělat, až nastane malér

Říká se, že štěstí přeje připraveným, a o schopnosti úspěšně se zotavit z bezpečnostního incidentu to platí dvojnásob. Součástí vašich plánů kontinuity činností by měly být i postupy pro ransomware nebo jiný bezpečnostní útok. I když nemáte vlastní bezpečnostní techniky, měl by být ve firmě někdo

“na telefonu”, komu může každý zaměstnanec, zákazník či partner nahlásit podezření na útok. Konkrétní postupy pak budou záležet na velikosti firmy a kvalifikaci vašeho IT oddělení, ale jako úplné minimum by tento krizový manažer měl mít kontakty na profesionály, kteří se zotavením pomohou. Třeba firma, která vám dělá bezpečnostní audity.

10. Používejte selský rozum

S počítači a IT je to jako s ohněm; je to dobrý sluha, ale zlý pán. Často stačí málo – před tím, než člověk něco udělá, měl by se zamyslet. To, že jsou útoky ransomware čím dál úspěšnější, nesouvisí jen s rozšířením pronikání IT do všech částí našeho života nebo hromadným přesunem na práci z domova kvůli pandemii, důvody jsou psychologické. Může to být vytvoření dojmu urgence (důležitý email od šéfa v pátek těsně před koncem pracovní doby), vyvolání zájmu (Šok! na internetu lze zbohatnout anebo přijít o všechno!) nebo roztomilé video s koťátky…

Co říct závěrem? Naše pracovní a soukromé životy “online” jsou propojené čím dál tím víc, a chytrá firma toho umí využít nejen ke zvýšení efektivity a zisku, ale i k holistickému pohledu na bezpečnost. Zvyšováním povědomí vašich IT kolegů i zaměstnanců o tom, jaká rizika hrozí a jak se jim bránit, přispějete všem. A můžete začít třeba tím, že jim přepošlete toto desatero.

Další články:

- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- AML a diskriminace v realitní praxi: chyby, které mohou vyjít draho
- Souhrn významných událostí ze světa práva
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Evropská unie mění pravidla plateb: více odpovědnosti, intenzivnější zpracování dat, více kontrol
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Odpovědnost zaměstnavatele a zaměstnance v souvislosti s využitím umělé inteligence
- Nový návrh zákona o platformové práci – 2. díl: Redefinice závislé práce