

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **71** ze dne **4.6.2024**

Antispam: jak poznat nebezpečnou komunikaci a škodlivé e-maily?

Když jde o spam, spoléháme se na filtry v e-mailových schránkách. Útočníci jsou však mistry nebezpečných e-mailů, a tak není od věci hledat spolehlivý antispam k ochraně naší online komunikace.

Mnozí z nás e-mailové bezpečnosti nevěnují příliš pozornosti, ale to by mohla být chyba. Komunikaci na internetu bereme jako neoddelitelnou součást našich online životů a leckdy se prostě spoléháme na to, že nevyžádaná zpráva skončí v příslušné složce, do které nikdy nenahlédneme. Jenže spam si i tak může najít cestu a namísto neškodného reklamního sdělení může být zpráva pokusem o phishingový útok nebo podvodnou nabídku. V dnešním světě může být nevyžádaná pošta také zdrojem dezinformací.

Zatímco ještě před pár lety byl spam k vidění především v e-mailech, dnes se s ním můžeme setkat i v SMS nebo chatovacích aplikacích. Útočníci navíc stále hledají nové cesty, jak k nám nebezpečnou zprávu doručit tak, aby ji e-mailové filtry a zabezpečení v naší elektronické poště nezachytily.

Spam versus phishing

Zatímco spam je souhrnné označení pro veškerou nevyžádanou komunikaci online, phishing pak představuje jednu z jeho variant, která je dnes zdrojem stejného nebezpečí, jako samotný malware.

Phishingové zprávy jsou silně manipulativní a mají nás donutit k okamžité akci, nad kterou nemáme přemýšlet. Často jsou tak hlavními příběhy této komunikace hacknutý bankovní účet, zděděné miliony nebo domnělý blízký v nesnázích. Takové zprávy v nás vyvolávají silné emoce, negativní i pozitivní, a vypínají nám tak racionální myšlení. To je ale zrovna k obraně před těmito útoky klíčové.

Útočníci se při phishingových útocích často také vydávají za nějakou známou instituci – typicky banku, přepravce nebo IT podporu. Nebo se mohou tvářit jako naši přátelé nebo kolegové z práce. V takových případech je důležité zachovat chladnou hlavu a v případě, že se jedná o nějakou naléhavou situaci k řešení, je na místě zbystřit: Z jaké adresy zpráva přišla? Nejsou v komunikaci nějaké chyby? Sedí tón komunikace, je příliš formální nebo naopak až příliš přátelský?

Pamatujte, není nic špatného na tom se protistrany doptat na další informace či zavolat na oficiální zákaznickou linku a požadavek si ověřit. Svým přátelům a kolegům můžete v případě pochybností také vždy zavolat.

Spam zacílený na elektronickou poštu

Kromě toho, že je e-mail stále jednou z nejpoužívanějších forem komunikace, je také úložištěm celé řady našich citlivých dat – využijeme ho při komunikaci s lékařem, právníkem nebo pojišťovnou. Útočníci to moc dobře vědí, a proto jsou naše e-mailové schránky tak často pod palbou spamu.

Jak už bylo řečeno výše, může se dnes na nás snést celá řada méně či více nebezpečných nevyžádaných zpráv. Když vezmeme stranou podvodné reklamní sdělení, může se jednat i o zprávy, které mohou sloužit k celé řadě dalších útoků:

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **71** ze dne **4.6.2024**

Přílohy e-mailů, které ukrývají spyware

Jakmile stáhneme a otevřeme nebezpečnou přílohu se spywarem, vpustíme tento škodlivý kód do zařízení a ten následně odcizí naše hesla a přihlašovací údaje.

Sociální inženýrství ve spamových kampaních

Jeden phishingový e-mail může vést k získání přístupů do našeho online bankovníctví, nebo k získání našich dat, která budou sloužit k dalším typům manipulativní komunikace – například smishingu nebo vishingu.

Credential stuffing

Díky získanému heslu, například s pomocí spywaru nebo phishingového útoku, mohou útočníci dále pokračovat tímto útokem. Spoléhají se při něm na to, že používáme stejné přihlašovací údaje i na jiných účtech. Ty se pomocí automatizovaného softwaru pokusí prolomit.

Převzetí kontroly nad e-mailovou schránkou

Jakmile budou mít útočníci volný vstup k přihlášení do e-mailu, mohou náš účet využít například k resetování našich dalších účtů a k jejich odcizení. To je bohužel častým případem při krádeži účtů na sociálních sítích. Většina webových stránek, kde máme zařízení svůj účet, umožňuje zasílat odkaz pro resetování. Po únosu našeho e-mailového účtu se útočník k tomuto odkazu snadno dostane a využije toho ke změně dalších hesel.

Jedno je dobré vědět – riziko může vznikat již při samotném otevření spamových zpráv. Ani nemusíme klikat na odkaz nebo stahovat a spustit přílohu. Už jen otevřením zprávy totiž dáváme jeho odesílateli vědět, že je náš e-mail aktivní a že ho používáme.

Spam v chatu nebo SMS

Také ve zprávách v chatovacích aplikacích nebo v SMS platí stejné triky kyberútočníků, ačkoli v těchto případech může být složitější nebezpečnou komunikaci poznat. Útočníci se totiž mohou vydávat za někoho, koho známe, pokud se zmocnili jeho profilu.

Podobně, jako u nevyžádaných e-mailů, i zde bychom měli mít na paměti bezpečnostní zásady. Měli bychom být skeptičtí ke každé zprávě z cizího čísla, nebo od lidí mimo okruh našich přátel. Vhodné je k této komunikaci vždy přistupovat tak, jakoby by byla od podvodníka.

Obezřetnost je ale namístě i u zpráv od našich přátel. Zbystřete u nečekaných žádostí, které běžně nedostáváte. Pokud po vás chtějí něco, co se vymyká vašim běžným pořádkům, není nic snazšího, než jim prostě zavolat a zeptat se jich na podrobnosti.

S obranou pomůže antispam i naše vlastní skepse

Nikdo z nás nemůže mít nikdy jistotu, že ve spěchu či ve chvílce nepozornosti neklikneme na nebezpečný odkaz v nevyžádané zprávě. Přesto existuje několik pravidel kybernetické bezpečnosti, na která bychom při komunikaci v online světě neměli zapomínat.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **71** ze dne **4.6.2024**

Protože žijeme v době, kdy nemůžeme mít jistotu, že to, co vidíme nebo slyšíme, je pravda, je naší nezbytnou výbavou i obyčejný selský rozum a zdravá dávka skepse. Pokud dostaneme nějakou senzační nebo naopak příliš dramatickou zprávu, mělo by to pro nás být upozorněním na to se zastavit a začít se ptát po více informacích.

Pravidlem tesařským do kamene pak také je neotvírat nikdy přílohy a neklikat na odkazy v nevyžádaných zprávách, od neznámých uživatelů, ale i od přátel, pokud takovou zprávu nedoplní nějakým podrobnějším vysvětlením.

A pak jsou tu také nástroje antispamové ochrany. Anti-spam obsahuje kombinaci několika bezpečnostních principů, které zajišťují tzv. nadřazené filtrování příchozí pošty v našich e-mailových schránkách – jinými slovy tento nástroj kontroluje náš mailbox a udržuje poštovní schránku čistou.

Zdroj: AVcentrum ČR