

Na phishing může naletět každý. Služba Phishingator od sdružení CESNET nabízí bezpečný trénink

Datum 23.9.2026
Subjekt CESNET
Region Česká republika
Kategorie IT a komunikace, Technologie, Bezpečnost

Rozhovor s Alešem Padrtou, vedoucím Forenzní laboratoře CESNET.

CESNET se simulovanému phishingu věnuje od roku 2017. Z původních testů postupně vznikla služba Phishingator, která dnes organizacím umožňuje připravovat vlastní simulované kampaně a vzdělávat uživatele v bezpečném prostředí. S Alešem Padrtou jsme si povídali o tom, jak služba vznikala, co se za devět let změnilo, proč má smysl doplnit školení o praktickou zkušenost a proč může phishingu podlehnout kdokoli z nás.

Proč si myslíte, že je phishing tak účinný?

Phishing je navržený tak, aby v nás vyvolal rychlou, instinktivní reakci. Může pracovat se strachem, časovým tlakem, zvědavostí nebo třeba s vidinou něčeho, co bychom neradi propásli. Sám jsem to zažil ještě v době, kdy jsem pracoval na univerzitě. Opakovaně tam přicházely podvodné e-maily s tvrzením, že adresát dluží peníze a je proti němu vedeno exekuční řízení. Podrobnosti měl najít v příloze. Desítkám uživatelů jsem vysvětloval, že jde o podvod. A pak stejný e-mail přišel i mně.

Samozřejmě jsem věděl, že je falešný. Jenže v tu chvíli se mi hlavou začaly honit myšlenky: exekutor, přijdu o byt, co bude s kočkou... Člověk přesně ví, co se děje, a přesto ho instinkt nutí kliknout. Rozdíl mezi tím, když takovou zprávu posuzujete s odstupem, a tím, když přijde přímo vám, je obrovský.

Co nám pomůže se na takovou situaci připravit?

Teoretické školení nám pomůže phishing rozpoznat, ale úplně nás nepřipraví na situaci, kdy nám taková zpráva skutečně přistane ve schránce. Právě proto má smysl doplnit ho tzv. simulovaným phishingem. Můžeme si tak podobnou situaci vyzkoušet v bezpečném a kontrolovaném prostředí, kde naše případná chyba nemá žádné následky.

Kdo může naletět na simulovaný phishing?

Kdokoli z nás. Někdy zkrátka podlehneme tlaku okamžiku. Přijdete do práce unavení, řešíte nemocného domácího mazlíčka, myslíte na víkend nebo se jen snažíte rychle vyřídit administrativu před první kávou. A právě v takové chvíli přijde zpráva, která vás něčím zaujme nebo znepokojí.

Proto podle mě není správné dívat se na výsledky phishingové kampaně jako na seznam lidí, kteří udělali chybu. Důležité je, aby příště podvodnou zprávu dokázali rozpoznat.

Dokážou vás reakce na simulovaný phishing ještě překvapit?

Po těch letech už mě toho překvapí poměrně málo. Setkali jsme se s nejrůznějšími reakcemi. Jedna kampaň mi ale v paměti zůstala. Pro zákazníka jsme připravili zprávu, která nabízela možnost získat z evropského „fondu produktivity“ až 5 000 korun měsíčně navíc. Cílovou skupinu tvořilo zhruba 110 lidí. Své přihlašovací údaje postupně zadalo deset, dvacet, čtyřicet, osmdesát, sto lidí... Nakonec jich

bylo kolem 190. To nám samozřejmě nesedělo. Ukázalo se, že jedna sekretářka zprávu v dobré víře přeposlala všem zaměstnancům. Říkala si, že by přece byla škoda, kdyby o peníze přišli. A když vám podobný e-mail přepoše vaše sekretářka s doporučením, abyste na něj zareagovali, jeho důvěryhodnost výrazně vzroste.

Aby zprávy působily věrohodně, vycházíme při přípravě kampaní z prostředí konkrétní organizace, veřejně dostupných informací i aktuálního dění. V Plzni jsme například před svatým Martinem nabízeli prvním stovkám přihlášených svatomartinskou husu zdarma v univerzitní menze. U nás v CESNETu zase během čtyřicetistupňových veder přišel e-mail s výzvou, aby si zaměstnanci v personálním systému potvrdili nárok na „klimatické volno“.

Pozorujete při opakovaných kampaních posun v tom, jak lidé na phishing reagují?

Ano, a poměrně výrazný. V první kampani našemu simulovanému phishingu obvykle podlehně zhruba 20 % příjemců. Když ji například po půl roce zopakujeme, dostáváme se už jen na 2-5 %. Pozitivní vliv je tak vidět na první pohled. Zajímavé je také to, že některé kampaně v organizacích žijí vlastním životem ještě dlouho po skončení. Příběh se svatomartinskou husou si například lidé vyprávějí už řadu let. I taková historka pak funguje jako připomínka, že phishing existuje a že je potřeba být obezřetný.

Co simulované kampaně přinášejí organizaci a jak může jejich výsledky využít v praxi?

Osobní zkušenost pomáhá uživatelům lépe se phishingu bránit. Odolnější zaměstnanci pak přispívají k bezpečnosti celé organizace. Kampaň zároveň organizaci ukáže, jak na tom v danou chvíli je. Výsledky může využít při analýze rizik a rozhodování, jestli je současná míra rizika přijatelná, nebo jestli je potřeba přijmout další opatření, například další vzdělávání uživatelů. Důležitá je také pravidelnost. Pozornost časem přirozeně klesá, takže má smysl se k simulovanému phishingu vracet, třeba jednou ročně.

Když porovnáte phishingové zprávy z roku 2017 s těmi dnešními, v čem se nejvíc změnily? Je dnes pro běžného uživatele těžší phishing poznat?

Když se budeme bavit o těch skutečných phishingových e-mailech, tak se změnily výrazně. Už nás před světem nechrání náš poměrně komplikovaný jazyk, takže pryč jsou doby mizerné češtiny a oslovení „miláček zákazník“. Dnes už pomocí překladačů a umělé inteligence lze dosáhnout dokonalého překladu. Také je možné získat o cílových adresátech informace na internetu, např. na sociálních sítích nebo z webové prezentace firmy, a snadno tak připravit lépe cílený e-mail. Takže uživatelé to mají zase o kousek těžší, než mívají. Nicméně stále lze podvod rozpoznat, pokud se nenechají příliš vystresovat.

Jak jste se ve sdružení CESNET k simulovanému phishingu vlastně dostali?

V té době jsme poskytovali penetrační testy zaměřené především na prověření technického stavu IT infrastruktury. Jenže zákazníci za námi začali chodit s logickou otázkou: „Dobře, technické vybavení máme prověřené, ale co jeho obsluha? Dokážou naši ajťáci, správci a uživatelé odolat manipulaci?“ Na základě jejich podnětu jsme proto připravili službu Phishingové testy. Už názvem jsme chtěli dát najevo, že jde o obdobu penetračních testů, jen tentokrát zaměřenou na lidi.

Postupně se ukázalo, že poslat uživatelům jeden cvičný phishingový e-mail bez kontextu nestačí. Přidali jsme proto úvodní školení o tom, co phishing je a jak ho poznat. Vznikl tak ucelený blok: teoretická příprava, cvičný phishing odeslaný přímo do schránek uživatelů a následné vyhodnocení se závěrečnou zprávou pro zákazníka.

Používali jste už při těchto kampaních Phishingator?

Ještě ne. Ale už tehdy jsme potřebovali nějaké technické řešení, které by nám umožnilo rozesílat cvičné zprávy a vyhodnocovat výsledky. Používali jsme proto interní systém poskládaný z různých

komponent. Sledovali jsme, komu zpráva odešla a zda se nevrátila jako nedoručitelná. Zaznamenávali jsme také, jestli na ni uživatel odpověděl, navštívil odkazovanou stránku nebo na ní něco zadal. Dokázali jsme přitom rozlišit, zda šlo o platné přihlašovací údaje, nebo třeba jen o vtipný vzkaz domnělým kyberzločincům.

Pro naše potřeby to fungovalo. Rozhodně to ale nebyl nástroj, který bychom mohli dát zákazníkům, aby ho používali sami.

Co vás tedy přivedlo k vývoji samotného Phishingatoru?

Znovu nás k tomu přivedli zákazníci. Říkali nám: „Teoretické školení si zvládneme udělat sami. Jsme na akademické půdě a pedagogických talentů máme dost. Ale rozesílat simulované phishingové zprávy a vyhodnocovat výsledky je technicky složité. Přitom bychom chtěli kampaně dělat častěji a nechceme pokaždé čekat, až na nás u vás přijde řada.“ A tehdy vznikla základní myšlenka: dejme organizacím nástroj, se kterým si budou moci simulované phishingové kampaně připravovat samy.

A jak se z myšlenky stal hotový nástroj?

Tady už přichází na scénu Martin Šebela. Tehdy jsem ještě částečně pracoval na univerzitě. Jednoho dne jsem seděl v kanceláři a odpovídal na e-maily, když někdo zaklepal. Ve dveřích se objevil student a povídá: „Dobrý den, já jsem Martin Šebela, zajímám se o phishing a na katedře mi řekli, že tady tomu nejvíc rozumíte. Mohl bych nějaký rozesílat v rámci semestrální práce?“ Slovo dalo slovo a po nějaké době vznikla bakalářská práce Phishingator, která na téhle myšlence stavěla.

Trvalo pak ještě přibližně dva roky, než se Martin stal zaměstnancem CESNETu a z bakalářské práce vznikl plnohodnotný open-source nástroj. Ten dnes nabízíme také jako službu, tedy Software as a Service.

Jak Phishingator funguje dnes?

V současnosti ho využívá 24 zákazníků (od vysokých škol až po výzkumné instituce). Každému ho na začátku nastavíme na míru. Nahrajeme například seznam uživatelů a připravíme cvičné přihlašovací stránky, které napodobují vzhled těch skutečných. Potom si už zákazníci mohou kampaně vytvářet sami. A důležité je, že je mohou dělat bez omezení. Ve sdružení CESNET nám jde především o vzdělávání uživatelů a šíření bezpečnostního povědomí. Proto nemáme licenční model typu „platíte za každý odeslaný e-mail“ nebo „platíte za každého uživatele“. Služba má pevný měsíční poplatek a organizace si pak může připravovat kampaně podle svých potřeb.

Vzpomenete si ještě na prvního zákazníka Phishingatoru?

Samozřejmě. Byl jím Výzkumný a zkušební letecký ústav. První nasazení vždycky přinese něco, s čím člověk přes veškerou snahu dopředu nepočítá. Díky nadšení na naší straně i na straně VZLÚ jsme ale všechny potíže zvládli a ústav Phishingator využívá dodnes.

Jaké novinky v Phishingatoru přibyly a co plánujete do budoucna?

Phishingator rozvíjíme průběžně. Od původní verze přibyla například možnost vkládat do zpráv parametry, jako jsou e-mailová adresa příjemce, jeho jméno a příjmení nebo aktuální datum. Máme také více možností, jak upravit podobu podvodného odkazu. A nezapomínejme ani na to, že vedle čistě textových e-mailů umí Phishingator posílat také zprávy v HTML. Můžeme tak používat tabulky, barvičky, odkazy typu „klikněte zde“ a všechno další, na co jsou uživatelé z běžných e-mailů zvyklí.

Martin teď pracuje na možnosti vkládat do zpráv QR kód místo odkazu, tedy na simulaci takzvaného quishingu. Do budoucna bychom chtěli, aby Phishingator uměl posílat také SMS zprávy a simulovat tak smishing. Rádi bychom se zaměřili i na další kanály elektronické komunikace. Taky uvidíme, co si budou přát uživatelé a kam se svět za pár let zase posune.

Kde se o Phishingatoru mohou zájemci dozvědět víc?

Stačí se nám ozvat. Rádi si s nimi domluvíme online schůzku. A 1. října se Phishingatoru budeme věnovat také na workshopu v rámci Konference e-infrastruktury CESNET. Budeme mluvit o tom, co nového se Phishingator za poslední rok naučil, o současných trendech v phishingu i o zkušenostech jeho uživatelů. Kapacita workshopu na místě už je naplněná, ale budeme ho vysílat také online, takže se může připojit každý.

Děkujeme za rozhovor.

<https://www.cesnet.cz/novinky/na-phishing-muze-naletet-kazdy-sluzba-phishingator-od-sdruzeni-cesnet-nabizi-bezpecny-trenink-318>