Když volají z banky, měli by vás o správné identitě přesvědčit oni, říká expert

idnes.cz/zpravy/domaci/rozhovor-jakub-olexa-mailkit-kyberbezpecnost.A230613_100316_domaci_nema

25. června 2023

E-maily, SMS zprávy, WhatsApp i klasické volání. Kyberútočníci využívají ke krádeži peněz či identity veškeré dostupné platformy. „Útoky jsou sofistikované, napadají i datové schránky," říká v rozhovoru pro iDNES.cz zakladatel a CEO e-mailingové platformy Mailkit Jakub Olexa, který se tématem internetové bezpečnosti dlouhodobě zabývá.

Zakladatel a CEO e-mailingové platformy Mailkit Jakub Olexa. | foto: Mailkit

Heslem nedávného Deliverability Summitu, který jste organizoval, bylo „Hlavní je bezpečnost". Je pro vás nyní zabezpečení e-mailových schránek a celkově online komunikačních platforem větší prioritou než dříve?
Určitě ano. Z pohledu odesílatele je pro nás důležité se věnovat

bezpečnosti nejen kvůli ochraně zneužití našich systémů, což by nás mohlo stát peníze, ale samozřejmě i v rámci ochrany prostředků našich klientů.

Téma bezpečnosti je u každé služby tohoto typu trochu odlišné, u nás například – na rozdíl od jiných společností – děláme se zákazníky nejdříve „vetting“ neboli proces prověřování. Bezpečnost je ale také často otázkou toho, že už někde existuje převzatý přístupový účet, kteří útočníci zneužijí.

Třeba k phishingu.
My už potom řešíme jeho následky. Jsou to ale nejrůznější nežádoucí aktivity, a nemusí být ani moc viditelné. Jako třeba spam, který jsme asi každý z nás někdy dostali, i plošný phishingový útok, například na banku, bývá medializovaný a tedy je vidět. Co už tak vidět není, je takzvaný „spear phishing“, což je vysoce cílený útok, kdy se sice mail pošle jen jeden, ale je připravovaný třeba i několik měsíců.

Já přece nic neposílal

Jakub Olexa

Patří mezi první Čechy, kteří se u nás v devadesátých letech připojili k internetu přes speciální linku vedenou z Vídně na ČVUT v Praze. V dalších letech se podílel na projektech jako například Xchat.cz či Mobil.cz.

Před 15 lety stál u zrodu společnosti Mailkit, kde dnes udává strategii vývoje a specializuje se na problematiku doručitelnosti, spamu a phishingu. Své letité zkušenosti uplatňuje také ve vzdělávání dalších odborníků působících v oblasti e-mailingu.

V červnu v Praze poprvé organizoval Deliverability summit, kde novinky ze světa e-mailingu představovali mimo jiné zástupci Yahoo, Mailkitu, Mailchimpu nebo Seznamu.

To mi přijde až neuvěřitelně dlouho. Vyplatí se to útočníkům?
Jsou v tom obrovské částky. U jednoho našeho klienta došlo ke spear phishingovému útoku, který byl koncipovaný tak, že generální ředitel firmy reaguje na e-mail finančnímu řediteli, kde schvaluje proplacení faktury v příloze. Provedení bylo od A do Z zcela perfektně udělané, e-maily byly autentifikované, vypadaly jako od správných lidí, byly správně napsané a dokonce i v tom stejném stylu, jak mezi sebou komunikují lidé uvnitř firmy.

Šlo o stovky tisíc eur. Jediný důvod, proč útok neuspěl, byla skutečnost, že jakmile přišel e-mail, byli finanční a generální ředitel spolu na telefonu.

To muselo být překvapení.
Když končili konverzaci, finanční ředitel řekl generálnímu, že fakturu hned vyřeší a proplatí. Ten se ho zeptal jakou fakturu myslí, že mu nic neposílal. A najednou se začalo pátrat. Zjistilo se, že útočníci museli ukrást nějakému zaměstnanci přístupové údaje měsíce předtím, než to na vedení firmy zkusili.

Jak to u této firmy dopadlo? Zvýšili nějak svoje zabezpečení?
Nakonec začali používat mechanismus DMARC *(Domain-based Message Authentication, Reporting and Conformance, slouží k validaci e-mailových zpráv a umožňuje majiteli domény zabezpečit elektronickou komunikaci tím, že pomůže lépe zachytávat nevyžádanou poštu zneužívající jeho doménu, pozn. red.)*, aby byli proti tomuto typu útoku chránění.

Jaké jsou další příklady spear phishingu, na co si mají lidé dávat největší pozor?
Dnes jsou to zřejmě podvodné SMS zprávy. Nedávno jsem takovou dostal, od „mé banky“. Podvodníci se v ní snažili vypadat důvěryhodně, dávali mi najevo, že jim mám věřit. Lidé na falešné esemesky ještě nejsou zvyklí, proto je to tak nebezpečné.

Banky jsou pro nás symbolem zabezpečení. Je to důvod, proč je útočníci tak rádi zneužívají?
Ano, i mně relativně často z mojí banky volají a ptají se, jestli jsem spokojený, a jestli nechci nějaký nový produkt. Už jsem se naučil automaticky reagovat „ne, díky“ a to i z toho důvodu, že se oni mě v telefonu ptají na různé osobní otázky a chtějí si ověřit mou totožnost. Podle mého názoru musí nejdříve oni přesvědčit klienta o tom, že jsou banka.

Mně volá neznámé českolipské nebo liberecké číslo, není to můj osobní bankéř a chce po mně osobní údaje? S použitím AI není problém udělat umělý hlas, který se klidně může vydávat za kohokoliv.

Nebrat AI jako kanón na vrabce

AI je tedy ve vašem odvětví hrozbou?
Umělá inteligence není nic nového. Není to otázka posledního roku, kdy se začalo mluvit o ChatGPT, které je samozřejmě unikátní. Stejně se ale třeba před pěti lety mluvilo o nahrazení tvorby obsahu strojovým učením. Obava toho, že AI způsobí zázračnou revoluci, je mylná. ChatGPT není o moc dál, než to, co tady bylo v oblasti e-mailů už dříve, kdy se třeba firma Phrasee specializovala na generování alternativních předmětů v e-mailech.

Nahrazujeme rutinní práci bez lidské přidané hodnoty, říká šéf AI startupu

Stejně tak je to v oblasti překladů. To, co umí Google překladač, je také strojové učení, k tomu nepotřebujete ChatGPT. Na první pohled může tento nový model vypadat báječně, chcete-li od něj ale něco relevantního a unikátního, nebude vám rozumět. A pak začnou vyplouvat na povrch problémy, což si většina lidí neuvědomuje.

Kvalitní novinový článek tedy jazykový model sám nenapíše?
Ne. Uvedu vám příklad. Vy umíte napsat článek, aby byl čtivý, já bych zřejmě uměl napsat článek, který je faktický a technicky přesný, ale neumím ho správně upravit pro cílové publikum. Když vezmu ten můj a požádám ChatGPT, aby ho přepracoval lépe, to on dokáže.

Takže mi jen pomáhá, nenahradí mě. Nedokáže interpretovat informaci, jen skládá slova. Za pár let se možná dostaneme k tomu, že bude umět pojmout i konkrétní témata. Nesmíme ale AI brát jako kanón na vrabce, musíme ji správně využívat.

AI „odpálila“ Pentagon. Odhalit podvod už skoro nejde, varují experti

Revoluci tedy nepředvídáte?
Když lidé vymysleli šicí stroj, švadleny také panikařily. Bezpochyby dojde ke zvýšení produktivity, překladové agentury už nyní používají jazykové agentury. To se ale projevuje na kvalitě přeložených textů. Technické termíny, odbornost, tam AI zatím selhává.

Spam je i v datových schránkách

Na začátku letošního roku zřídil stát živnostníkům, spolkům a nadacím v Česku automatické datové schránky. Jak moc jsou chráněné?
Garance není nikdy, už i v datových schránkách byl spam, protože je to placená služba. Úroveň bezpečnosti je daná mnoha faktory, ze své podstaty jsou datové schránky důvěryhodné a bezpečné. Nicméně to s sebou nese rizika, všechny vstupy musí být ověřované.

Pokud existuje možnost si od České pošty objednat posílání čehokoliv přes API *(aplikační programové rozhraní, slouží k předávání dat mezi softwarovými aplikacemi. Mnohé služby nabízejí*

veřejná API, díky nimž může kdokoli do služby předávat obsah nebo ho z ní odebírat, pozn. red.) za kredit, proč by to někdo nemohl udělat. Pokud tato možnost není hlídaná, může ji někdo snadno zneužít. Což se i mně mimochodem stalo, v pandemii mi do datovky někdo posílal nabídku na předražené roušky.

O kolik vede zabezpečení datové schránky k lepší vymahatelnosti v případě zneužití? Vždyť se přece vede evidence o tom, kdo ji používá.
Neumím to zcela posoudit, jsem ale přesvědčený, že datové schránky vyžadují plnou identifikaci klientů. Pokud tedy někdo někoho vyspamuje, proces vyšetřování by měl být přímočarý. U e-mailu je to dopátratelné jen těžko. Posílání hromadných datových zpráv by podle mě měly mít možnost jen ověřené instituce.

Jak moc velký nárůst kybernetických útoků jste zaznamenali po začátku ruské invaze na Ukrajinu?
Rusko bylo masivním zdrojem útoků vždycky, spamboti odtud byli a jsou masivním procentem z celkového počtu útoků. Co se změnilo, je směřování, obrovské množství útoků hrálo na ukrajinskou notu, v řetězových e-mailech stálo „podpořte Ukrajinu“. V pozadí ale stálo „pošlete bitcoiny do naší peněženky“.

Část z toho byli prostí oportunisti, viděli, že velká část lidí přispívá peníze na Ukrajinu a chtěli se toho chytit. Je tady i čistě ruská podpora, také se vydávající za podporu Ukrajiny. To je podle mě ještě nebezpečnější.

Dezinformátoři umějí dobře napodobit seriózní média, varuje expertka

Jak jsou na tom vlastně nyní řetězové e-maily? Dá se vypátrat jejich původce?
Rozdělil bych to na dva typy, před a po sociálních sítích. Ty dřívější se daly vypátrat, se sociálními sítěmi je to však mnohem těžší. Zdrojů už nejsou jednotky, ale desetitisíce. Lepší trollové mají v profilu i ukradenou nebo vygenerovanou fotku, což přidává na autenticitě. Na Twitteru je nyní i po zaplacení pár dolarů možné se „ověřit“, což může dezinformátorům také pomáhat.

K internetu jste si v České republice „čuchnul“ jako jeden z prvních, v Mailkitu se staráte o e-mailingové řešení firem už řadu let. Jaké trendy nyní ve svém oboru vidíte?
Hodně útoků se přenáší na jiné platformy, ať už jsou to SMS zprávy, iMessage, WhatsApp nebo třeba Telegram. Dalším trendem je propojení specifických e-mailových útoků a dezinformací. Mnohdy je to také subjektivní. Co já si myslím, že je jasná dezinformace, někdo jiný považuje za názor. Mnohem citlivější je to podle mých zkušeností ve Spojených státech, kde jinak vnímají právo na informace a svobodu slova.

Velcí hráči jako Google nebo Microsoft by mohli technicky docela snadno zasáhnout, kdyby to ale udělali, začaly by na ně platit antikartelové zákony. A stejné je to u sociálních sítích. Donalda Trumpa zablokovali na Twitteru, ale na Facebooku ne. Každá společnost se rozhoduje samostatně, hraje v tom velkou roli politika.

Autor: Matěj Nejedlý

Související

Češi nemají rádi příliš mnoho newsletterů

Proč používat e-mail na jedno použití

Premium Rozšíření Gmailu pomůže. Vylepšuje psaní zpráv či přináší kontrolu doručení

Dovolená 2023: Poplatky, ceny, trasy

Kudy jet, kam natankovat, kde vyměnit peníze? Portál iDNES.cz přináší před začátkem letních dovolených přehled aktuálních cestovních tipů včetně rad, jak ušetřit nebo se na prázdniny připravit tak, aby se ze zájezdu nestala noční můra.

- Ceny v Chorvatsku
- Trasy k moři
- Cesta do Chorvatska
- Kde jsou uzavírky
- Ceny benzínu a nafty v Evropě
- Pokuty v zahraničí
- Kde měnit peníze
- České léto

Témata: banka, Datová schránka, peníze, WhatsApp, Ukrajina