Komentář ESET: Jak se vyhnout kybernetickým rizikům během letních festivalů

5.6.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Kyberbezpečnostní společnost ESET připravila souhrn doporučení, jak se vyhnout kyber rizikům v souvislosti s probíhajícími a chystanými letními festivaly. Právě bezstarostná atmosféra může přispívat k nárůstu rizik a online podvodů. Kromě škodlivých kódů mohou lidé narazit i na podvodné vstupenky, rizika plynoucí z nezabezpečených Wi-Fi sítí či ze ztráty mobilního telefonu. Důsledkem mohou být jak finanční škody, tak ztráta osobních a citlivých dat, se kterými mohou útočníci obchodovat na černém trhu.

Lidé se mohou během festivalové sezóny setkávat s phishingovými zprávami v e-mailech, chatovacích aplikacích nebo SMS zprávách. Zprávy se mohou tvářit jako oficiální komunikace pořadatele či prodejce vstupenek. Cílem podvodníků je vylákat peníze nebo přístupové údaje k důležitým účtům – například k těm do bankovnictví.

„Útočníci vědí, že když se lidé dobře baví, ztrácejí ostražitost. Opatrnost při nákupu vstupenek a při komunikaci s pořadateli je proto namístě, zvlášť, když je dnešní komunikace extrémně rychlá a vše máte dostupné na pár klinutí. Vždy proto pečlivě ověřujte adresu a profil odesílatele a v nevyžádaných zprávách neklikejte bez rozmyslu na odkazy ani neotvírejte přiložené soubory. Zvlášť opatrný bych byl u přeprodávání vstupenek. Ideální je zvolit si oficiální a prověřenou platformu, přes kterou i vstupenky z druhé ruky bezpečně zaplatím prověřenému prodejci," říká Vítězslav Pelc, tiskový mluvčí společnosti ESET v České republice.

Řada akcí může účastníkům poskytovat nápomocné mobilní aplikace. I zde je na místě opatrnost při jejich stahování a využívání.

„Festivalová aplikace může být skvělým pomocníkem, ať už pro orientaci v programu či účasti v různých výzvách a soutěžích. Pořadatel může také jejich prostřednictvím zasílat návštěvníkům důležité notifikace. Pokud je ale stáhneme mimo oficiální obchody, mohou obsahovat škodlivé kódy. Proto by si festivaloví návštěvníci měli pohlídat, odkud tuto aplikaci stáhnou. Útočníci mohou legitimní verze aplikací různě upravovat a maskovat jimi například adware. A i když jeho hlavní funkcí je zahltit vás dotěrnou reklamou, často slouží jako prostředník mezi vaším zařízením a daleko závažnějším škodlivým kódem, který dokáže stáhnout. Doporučuji také udělit festivalové aplikaci jen základní oprávnění pro přístup k vašim datům a po návratu zvážit její odinstalování," říká Pelc.

„Důležité je také zmínit riziko v podobě falešných QR kódů, kterými mohou útočníci jednoduše přelepit ty oficiální. Pokud je tak někde vyvěšen QR kód k zaplacení například parkování, nabití telefonu nebo stažení festivalové aplikace, je na místě určitě opatrnost. Před naskenováním QR kódu si zkontrolujte, zda nezakrývá jiný QR kód. Po naskenování se pečlivě podívejte na URL adresu a zkontrolujte, zda je legitimní," dodává Pelc.

Festivalové areály často nabízejí bezplatné Wi-Fi připojení. To sice šetří data, ale může být bezpečnostním rizikem – útočníci mohou odposlouchávat komunikaci nebo získat vaše přihlašovací údaje.

„Pokud mluvíme o riziku zneužití nezašifrované Wi-Fi sítě, používáme termín Man-in-the-Middle –

člověk uprostřed. Útočník se dokáže dostat do komunikace mezi námi a serverem, tedy cílovou stránkou, kterou si chceme na internetu zobrazit. Následně dokáže sledovat, co na internetu děláme. Pokud veřejnou Wi-Fi síť potřebujete používat, snažte se to dělat prostřednictvím sítě VPN. Přinejmenším se na veřejné Wi-Fi nepřihlašujte k žádným důležitým účtům, jako je ten bankovní či e-mailový, ani nezadávejte citlivé informace do formulářů na webu. To proveďte raději před data svého operátora," říká Pelc.

Kybernetická rizika se nemusejí objevit jen mezi jedničkami a nulami. Může k nim přispět i možnost, že telefon zkrátka ztratíte nebo vám jej někdo odcizí. Kvůli bezpečnosti by lidé měli také dávat pozor, když telefon nabíjejí na veřejných místech.

„I když existence powerbank nám trochu zjednodušila věčné hledání místa, kde telefon při celodenních aktivitách nebo pod stanem dobijeme, festivaly jsou typem akcí, kde ho máme pořád při ruce a vybijeme ho velmi rychle. Ani naše powerbanka tak nemusí stačit. Pokud se hudební fanoušci rozhodnou využít veřejné festivalové dobíjecí stanice, doporučil bych jim přibalit si tzv. USB Data blocker, který zamezí nechtěnému přenosu dat či škodlivého kódu. Vždy také mějte u sebe vlastní USB kabel," doporučuje Pelc.

„V neposlední řadě je pak vhodné udělat zálohu dat a ujistit se, že na svém telefonu používáte spolehlivé zámky a způsoby potvrzení – ideálně ověřením biometrických údajů jako je otisk prstu nebo snímek obličeje. Operační systém zařízení a všechny aplikace v něm také aktualizujte na nejnovější verze, hlavně kvůli opravám zranitelností a chyb, kterých by mohli útočníci využít. Zvažte i pořízení spolehlivého bezpečnostního programu, který dnes bývá už něčím víc než jen antivirem. Obsahuje i řadu šikovných funkcí, jako je například vzdálené uzamčení nebo smazání obsahu zařízení. Funkci, která vám v případě ztráty pomůže mobilní telefon najít, si můžete zapnout také v samotném telefonu," dodává Pelc z ESETu.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/komentar-eset-jak-se-vyhnout-kybernetickym-rizikum-behem-letnich-festivalu