

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **43** ze dne **13.8.2023**

Nejčastější kybernetické hrozby na letních festivalech

Letní festivaly se vyznačují několika znaky, které mohou hrát (nejen) kyberútočníkům do karet. Obecně je při těchto událostech na jednom místě opravdu velké množství lidí, hlavním cílem jejich návštěvy je zábava a fanoušci mají dnes prakticky neustále v ruce svůj chytrý mobilní telefon. Jaké jsou nejčastější kybernetické hrozby na letních festivalech a jak se jim vyhnout?

Phishing a sociální inženýrství

Jedním z kybernetických rizik mohou být phishingové e-mailové zprávy, ve kterých se podvodníci budou vydávat například za prodejce vstupenek.

Vždy je proto důležité věnovat pozornost celému e-mailu – sedí adresa odesílatele s oficiální adresou poskytovatele vstupenek? Obsahuje e-mail nějaké odkazy na platební brány nebo přílohy? Pokud máte s prodejcem vstupenek nebo s pořadatelem festivalu zkušenosti již z minulých let, vyplatí se také všimnout si, zda se nějak nezměnil tón komunikace. Vždy je také bezpečnější neotevírat přílohy a neklikat na odkazy v e-mailu, který vám byl doručen nevyžádaný. Navštivte raději oficiální webové stránky pořadatele.

S podvody se můžete setkat také v okamžiku, kdy dáváte přednost nákupu vstupenek na různých fórech. Podvodník se může vydávat za prodejce vstupenek, ale takové vstupenky nemusí být platné nebo je po zaplacení vůbec neobdržíte. I v tomto případě je lepší vsadit na jistotu a nakupovat vstupenky jen na renomovaných portálech.

Falešné aplikace

Během festivalu se vám může v chytrém telefonu hodit celá řada aplikací. Některé z nich může poskytovat přímo pořadatel, některé využijete pro hledání ubytování a některé i k úpravě fotek nebo videí, které během festivalu chcete pořídit.

Aplikace stahujte ale vždy jen z oficiálních obchodů s aplikacemi, jako je například služba Google Play. Vyhněte se naopak úplně neznámým obchodům třetích stran nebo internetovým úložištím, kde můžete sice narazit na zajímavé nabídky a některé aplikace tam pořídit zcela zdarma, jako bonus si ale v naprosté většině případů stáhnete škodlivý kód nebo adware. Ten pak v zařízení zobrazuje agresivní reklamu a pokud na nějakou z nich kliknete, můžete být přesměrováni na podvodné stránky, přihlášení k placeným prémiovým službám nebo do svého telefonu stáhnout další škodlivý kód.

Veřejná Wi-Fi síť

Veřejná Wi-Fi síť v areálu festivalu šetří na několikadenní akci vaše data. Ale i přes ní mohou útočníci sledovat vaši aktivitu v online prostoru nebo ukrást vaše přihlašovací údaje.

Pokud potřebujete využít veřejnou festivalovou Wi-Fi síť, procházejte přes ní jen nedůležité weby, na kterých nezadávejte své přihlašovací údaje. Naopak pro přístup do e-mailu, přihlášení na sociální sítě a určitě do internetového bankovníctví využijte vždy pouze data od svého operátora.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **43** ze dne **13.8.2023**

Juice jacking

Doplňkem mnoha fanoušků na festivalech bývá dnes chytrý telefon. Pokud ale trávíte na akci několik dnů pod stanem, je vaší starostí také dobíjení. Pokud s sebou nevozíte powerbanky, třeba využíváte k tomuto účely různé nabíjecí kiosky a k tomu určená veřejná místa.

Problémem v takovém případě může být dobíjecí kabel vašeho telefonu. Kromě toho, že doplní šťávu, dokáže přenášet mezi telefonem a dalším zařízením také data. A toho mohou velmi dobře zneužít útočníci – buď vám odcizí touto cestou citlivá data, nebo doručí do zařízení škodlivý kód. A to i v okamžiku, kdy na svém telefonu odkliknete, že chce jenom nabíjet – útočníka může do zařízení vpustit třeba nějaká skrytá zranitelnost v operačním systému nebo aplikaci.

Jak se juice jackingu vyhnout? V případě, že opravdu potřebujete dobít telefon z veřejného zdroje, vždy používejte k dobíjení pouze svůj kabel. Před odjezdem na festival se také ujistěte, že máte nainstalované všechny aktualizace operačního systému telefonu i aplikací, které mohou obsahovat opravy různých chyb. Šikovným pomocníkem může být také takzvaný USB data blocker, který připojíte ke svému USB kabelu – zabráňuje přenosu dat a vy tak máte jistotu, že svůj telefon opravdu jen nabijete.

Krádež mobilního telefonu

Na festivalech se můžete setkat ještě s jedním tradičním rizikem, který spolu s kybernetickou bezpečností souvisí – s krádeží nebo ztrátou chytrého telefonu. Ve svých telefonech dnes nosíme celou řadu citlivých údajů, dokumentů a fotografií, které rozhodně nepatří do nepovolaných rukou. Před tím, než vyrazíte, tak pro jistotu proveďte zálohu svého telefonu a nastavte spolehlivý zámek telefonu, ideálně pomocí biometrických údajů.

Mějte také po celou dobu zapnuté zjišťování polohy a aktivity. Někaká zařízení touto funkcí disponují již v základní výbavě. Pokud ne, je možné využít software třetích stran. Například funkce Anti-Theft, která je součástí aplikace ESET Mobile Security, vám umožní sledovat používání zařízení a lokalizovat ho pomocí GPS. V případě ztráty či krádeže může funkce pomoci získat zařízení zpět a ochránit vaše citlivá data.

Zdroj: AVcentrumCZ