

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **123** ze dne **4.11.2025**

Experiment ČMIS ukázal, jak ochotně se lidé podělí o údaje ze své platební karty

Quishing, tedy phishing prostřednictvím QR kódů, patří mezi nejrychleji rostoucí kybernetické hrozby. Meziročně vzrostl počet útoků o 21 procent, QR kód se objevil ve 22 procentech phishingových kampaní, které sloužily primárně k vylákání přihlašovacích údajů. Česká technologická společnost ČMIS na riziko upozornila kampaní ČMIZZA, která ukázala, jak snadno většina lidí podléhá lákavým nabídkám a nevědomky vystavují svá data riziku.

„Quishing má mnoho podob. Útočníci vylepují falešné QR kódy na parkovacích automatech nebo plakátech a oběti pak přesměrují na podvodné platební brány. V e-mailech se stále častěji objevují PDF přílohy s vloženým QR kódem, který vede na škodlivý web a dokáže obejít běžné bezpečnostní filtry. Kódy ale mohou směřovat i na stránky s falešnou reklamou nebo malwarem, případně na podvodné Wi-Fi sítě. Setkáváme se také s podvrženými aplikacemi pro čtení QR kódů, které útočnickům umožňují přístup k soukromí zařízení. Problém je, že QR kódy působí na uživatele důvěryhodněji než odkaz v e-mailu a zároveň je dokážou snadno maskovat i před technickými opatřeními. To z nich dělá atraktivní a velmi účinný nástroj pro útoky,“ upozorňuje Václav Svátek, generální ředitel společnosti ČMIS.

Česká technologická společnost ČMIS se rozhodla na toto riziko upozornit v rámci experimentu s názvem ČMIZZA. Vystoupila pod fiktivní značkou pizzerie a nabízela kolemjdoucím pizzu za jednu korunu. Stačilo naskenovat QR kód na krabici. Test odhalil, že téměř dvě třetiny lidí neváhaly a ochotně zadaly údaje ze své platební karty, protože nabídku vyhodnotili jako výhodnou příležitost. Celá akce ukázala, jak snadno lze uživatele nalákat na atraktivní nabídku a přimět je k zadání citlivých informací. Stejným způsobem útočníci získávají přístup k firemním e-mailům nebo cloudovým úložištím. Experiment zároveň potvrdil, že lidský faktor zůstává nejslabším článkem kybernetické bezpečnosti a pouhá technická opatření nestačí. Průzkumy totiž ukazují, že jen 27 procent zaměstnanců si věří, že dokážou rozpoznat cílený phishingový e-mail. Útočníci navíc často zneužívají skutečnou firemní komunikaci, což odhalení dále komplikuje. Vysoké riziko se týká i nových zaměstnanců, kteří v prvních 90 dnech ve firmě mají až o 44 procent vyšší pravděpodobnost, že útoku naletí. Celkově platí, že 95 procent kybernetických útoků má původ v lidské chybě.

„Chtěli jsme ukázat, jak snadno lidé naletí atraktivní nabídce. Naše akce „pizza za korunu“ byla neškodná, ale stejný scénář v reálném světě může znamenat, že útočníci získají přihlašovací údaje nebo otevřou přístup do firemní sítě. Obrana je přitom jednoduchá: pokud skenujete QR kódy, vždy ověřte, kam vedou, a nikdy nezasílejte citlivé údaje na podezřelých stránkách. Proto musejí firmy kromě technických opatření pravidelně školit své zaměstnance, protože lidská chyba zůstává hlavní vstupní branou útoků,“ vysvětluje Václav Svátek.

Statistiky hrozby potvrzují: každý den je po celém světě rozesláno přibližně 3,4 miliardy phishingových e-mailů, meziročně vzrostl počet útoků o 21 procent. QR kód se objevuje ve 22 procentech phishingových kampaní. V 90 procentech quishingových útoků jde o krádež přihlašovacích údajů a dalších citlivých dat, obvykle zaměřených na firemní e-mailové systémy, cloudové úložiště nebo nástroje pro vzdálený přístup. Experiment ČMIS ukázal, že více než 60 procent lidí bez rozmyslu načte QR kód a zadá platební údaje, aniž řeší potenciální riziko.

AV centrum ČR