Pizzu za korunu zaplatili svými daty. ČMIS varuje před QR kódy, mohou být branou pro kyberútoky

2.10.2025 - Komerční sdělení | ČTK

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. Denně je přitom rozesláno 3,4 miliardy phishingových e-mailů. Více než polovina však vzniká kvůli lidské chybě. 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 útočníkům 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 Svátek.

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, cloudovým úložištím nebo platebním údajům. Experiment zároveň potvrdil, že lidský faktor zůstává nejslabším článkem kybernetické bezpečnosti a pouhá technická opatření nestačí.

„Chtěli jsme ukázat, jak snadno lidé naletí atraktivní nabídce. 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: neskenujte neznámé QR kódy, vždy ověřte, kam vedou, a nikdy nezadávejte 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, generální ředitel společnosti ČMIS.

ČMIS zároveň upozorňuje, že prevence a připravenost jdou ruku v ruce. *„Kromě osvětových kampaní pomáháme firmám s praktickou ochranou. Zajišťujeme phishingové simulace, školení zaměstnanců, bezpečnostní audity, penetrační testy i nepřetržitý dohled a rychlou reakci při incidentech. Při ransomwarových útocích podporujeme firmy v rámci služby Ransomware pohotovost. Aktivujeme pohotovostní postupy, kde izolujeme napadené systémy, provádíme forenzní analýzu, obnovujeme data ze záloh a koordinujeme další kroky s právními a komunikačními týmy. Díky tomu lze dopad útoku omezit na minimum a provoz rychle obnovit,“* uvádí Svátek.

Těžko stravitelná čísla

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.

Nejde však jen o jednotlivce. Průzkumy 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.

Podle NÚKIB se počet hlášených kybernetických incidentů v Česku v roce 2023 zvýšil o 80 procent, z 146 na 262. V roce 2024 pak firmy a instituce čelily celkem 1699 útokům, které způsobily škody ve výši 632 milionů korun. Nejčastěji byly terčem e-shopy, školy, vzdělávací instituce a nebankovní společnosti. Specifická data k quishingu zatím v Česku dostupná nejsou, odborníci však očekávají, že vývoj bude kopírovat zahraniční trendy.

Více o ČMIS

Technologická společnost ČMIS, která patří k největším českým hráčům na poli hostingu, cloudových a serverových řešení, dokáže svým zákazníkům zajistit, že jejich e-shopy nespadnou a fungují hladce i během špičky, takže nepřijdou o své tržby kvůli výpadkům. Mezi hlavní služby patří hosting aplikačního prostředí pro účetní a obchodní systémy, dále hosting databází, úložišť a privátní cloud pro velké e-commerce hráče, jako jsou Rohlik Group či Shoptet. V neposlední řadě poskytuje jako Microsoft direct partner klientům MSSQL licence za nejvýhodnější cenu na českém trhu a také má nejvýhodnější cenové plány pro službu MS 365.

Zdroj: ČMIS

http://www.ceskenoviny.cz/tiskove/zpravy/-pizzu-za-korunu-zaplatili-svymi-daty-cmis-varuje-pred-qr-kody-mohou-byt-branou-pro-kyberutoky/2728620