Kybernetické útoky zneužívajúce identitu Slovenskej pošty

Národné centrum kybernetickej bezpečnosti SK-CERT **varuje** pred **pokračujúcou hackerskou kampaňou**, ktorá **zneužíva identitu Slovenskej pošty.** Kampaň momentálne prebieha prostredníctvom **SMS správ** (tzv. smishing). Útočník však môže zneužívať aj iné formy komunikácie (napr. e-mail).

Jedná sa o **rozsiahlu phishingovú kampaň**. Využíva tvrdenia, ktoré sa nezakladajú na pravde. Skutočným cieľom kampane je od vás **vylákať číslo platobnej karty** a aj osobné údaje.

Princíp kampane spočíva v tom, že útočník vám **pošle SMS**, v ktorej informuje o **doručenej zásielke**. Následne máte kliknúť na odkaz, ktorý vedie na podvodnú stránku. Tu musíte zadať informácie o svojej platobnej karte. Následne ste vyzvaný na **zadanie SMS tokenu**, ktorý vám príde obratom na vaše telefónne číslo. Útočník na druhej strane využije tieto informácie a platobnú kartu si priamo zadá do systémov na platenie prostredníctvom mobilných zariadení (Apple Pay, Google Pay, Garmin Pay a pod.). Následne tak útočník môže **platiť pomocou mobilu** aj bez, dnes už povinného, dodatočného overenia prostredníctvom vašej banky (3D Secure autentifikácia).

3D Secure autentifikácia je spôsob dodatočného overenia finančnej transakcie. Pri akejkoľvek platbe, pri ktorej neplatíte osobne kartou priamo v obchode alebo reštaurácii (ktorá neprebieha cez fyzický platobný terminál), ale napríklad cez internet (v e-shope, kde neprikladáte priamo kartu na terminál), je pri prevode používateľovi vystavené dočasné heslo, viazané na konkrétnu transakciu. To môže prísť napríklad SMS kódom alebo do špeciálnej aplikácie banky, ktorá okrem iného aj overuje takéto platby. Následne je používateľ počas transakcie vyzvaný, aby toto heslo zadal na jej potvrdenie. Overenie pomocou 3D secure je od 1. januára 2021 povinný postup, ktorý musia podporovať všetky banky a obchodníci.

Národné centrum kybernetickej bezpečnosti SK-CERT v súvislosti s touto, ale aj inými podvodnými - phishingovými kampaňami ODPORÚČA:

- v prvom rade – **neodpovedajte, nereagujte a neklikajte**
- ak vám takáto SMS alebo textová správa prišla, spomaľte a zamyslite sa. **Položte si jednoduché otázky** – naozaj som si objednal balík? Môže toto odo mňa niekto žiadať?
- nikdy **neposkytujte** cez SMS a textové správy alebo odkazy v nich svoje **osobné a finančné údaje**. Nikto okrem Vás na ne nemá nárok. Za **žiadnych okolností nevpisujte** svoje osobné/prihlasovacie údaje do webstránok, ktoré sú ľubovoľným spôsobom podozrivé alebo nemajú dôvod požadovať podobné informácie
- ak vám príde SMS správa s tokenom pre potvrdenie platby alebo potvrdenie inej aktivity, **nedávajte tento token nikomu**, ani ho nepíšte. Takéto SMS tokeny sú na potvrdzovanie len Vami iniciovaných aktivít
- neverte odosielateľovi, či už je to telefónne číslo alebo meno. Útočník sa môže maskovať za dôveryhodný názov alebo telefónne číslo. Preto si vždy takéto správy overte cez oficiálne kanály.

Ak vám prišla takáto podvodná správa prostredníctvom SMS, kontaktujte nás, alebo podvodnú SMS **nahláste priamo Národnému centrum kybernetickej bezpečnosti** . Môžete to spraviť dvoma spôsobmi:

- **preposlať** túto SMS spolu s uvedením telefónneho čísla odosielateľa aj prijímateľa (Vášho telefónneho čísla), na telefónne číslo **Národného centrum kybernetickej bezpečnosti: 0903 993 706**.
- skopírovať SMS správu spolu s telefónnym číslom odosielateľa a prijímateľa a zaslať ju na e-mail incident@nbu.gov.sk. Tento postup prosím použite aj pri textových službách ako Whatsapp a Facebook Messenger.