Tisková zpráva - 27. červen 2022

Podvodníkům na internetu jdou lidé sami naproti
Policisté prověřují denně případy podvodných jednání v kyberprostoru

KRAJ VYSOČINA - Policisté Krajského ředitelství policie kraje Vysočina prověřují v poslední době téměř denně případy různých podvodných jednání ve virtuálním prostoru. Vliv na to nepochybně má využívání internetového prostředí k platbě za zboží. Za této situace využívají pachatelé ten nejslabší článek v řetězci, a to důvěryhodnosti občanů a mnohdy bohužel také jejich neopatrnosti a naivity.

„Stále více dynamický rozvoj informačních technologií s sebou také přináší další a nová rizika, která nás mohou v kybernetickém prostředí potkat. Setkáváme se s případy společensky škodlivého jednání, s podvody na internetu, kybernetickými útoky a dalšími hrozbami, proto je kybernetické kriminalitě věnována stále větší pozornost,“ uvádí plk. PhDr. Aleš Indra, ředitel územního odboru Třebíč. Kybernetická kriminalita je definována jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.

A jaké jsou nejčastější cesty pachatelů? Prodáváte zboží v elektronickém bazaru (Bazoš, Winted….) Kupující vám napíše, že má zájem o přepravu předmětu prodeje prostřednictvím přepravce (DPD, GLS,…). Pokud souhlasíte, kupující vám sdělí, že vámi požadovanou částku složil na účet přepravce a vy máte do tabulky na zaslaném odkazu vypsat pouze přístupové údaje k vašemu elektronickém bankovnictví a současně požaduje sdělit také autorizační kód přístupu. Poté vám budou prostředky vloženy přímo na váš účet. Odkaz se na první pohled tváří jako odkaz přepravce a od oficiální adresy se liší nepatrně jen některým chybějícím, přidaným či změněným znakem oproti odkazu na skutečné stránky. Tímto krokem má ale pachatel možnost vstoupit do vašeho elektronického bankovnictví, doplnit svůj autorizační telefon, a pokud opět zašlete autorizační kód operace, ovládá již zcela váš účet. V některých variantách dokonce na váš účet peníze skutečně přijdou, ale později zase „odejdou“ i s vašimi zde uloženými finančními prostředky!

Velmi podobná je varianta s platbou platební kartou, kdy pachatel po získání údajů o platební kartě obdobným způsobem (vyplnění údajů do „podstrčené“ tabulky) má k dispozici údaje platební kartě a dále požaduje, a to i opakovaně pod různým legendami, zaslaní autorizačních kódů. Stejné metody se dají použít i při nákupu zboží, kdy falešný prodávající požaduje zaplacení tím způsobem, že vyplníte na jím zaslaném odkazu údaje k přístupu do elektronického bankovnictví/údaje o platební kartě. Bankovnictví ovládne a postupuje stejně. U platební karty se snaží o vylákání

Adresa
Vrchlického 46
587 24 Jihlava

Tel.: +420 974 261 207
Fax: +420 970 266 700
Email: dana.cirtkova@pcr.cz

autorizačních kódů nebo nakupuje zboží v obchodech, které nepodporují 3Dsekurity (není třeba autorizačního kódu).

A přinášíme další praktický případ: Ozve se vám pracovník banky, přijde vám textová zpráva „volejte na toto krizové číslo banky“, nebo volá policista, - někdy všechno dohromady. Legenda zní, že nastala důležitá změna při fungování vašeho elektronického bankovnictví, které je napadeno, vaše peníze jsou vyváděny. Jste nabádáni, abyste ihned provedli nutné kroky, které spočívají v převedení prostředků na tzv. bezpečný účet nebo k okamžitému výběru veškeré hotovosti a její převod na Bitcoin prostřednictvím Bitcoimatu. Obojí ale končí stejně - peníze jsou podvodníkem vyvedeny pryč mimo váš dosah. Žádná banka ani policie tento postup nepoužívá, tyto instituce mají jiné postupy, které nevyžadují vaší součinnost.

Další variantou je, že pracovník banky/policista po vás požaduje instalaci software pro ovládání plochy vašeho počítače, nejčastěji jde o AnyDesk, aby mohl nutné operace provést správně sám. Požaduje, aby se člověk přihlásil do elektronického bankovnictví, a protože váš počítač nyní ovládá, tak dokáže vyvádět pryč vaše peněžní prostředky, a to i za vašeho dohledu. Za pomoci stejného nástroje lze připravit nic netušícího klienta o peněžní prostředky pod legendou nabídky sjednání půjčky či výhodné investice, většinou virtuálních měn, nejčastěji do Bitcoin. Tito pachatelé na vás dokáží „tlačit“ i velmi tvrdě, opakovaně několik hodin i dnů. Tedy pozor na AnyDesk!

Ve všech výše uvedených případech je zájmem pachatele stejný - vylákat pod různými legendami (a musíme počítat s tím, že vzniknou další a další) potřebné údaje nebo mechanismy pro ovládnuté vašeho elektronického bankovnictví či k možnosti nelegálně platit vaší platební kartou. Při správném standardním chování jste schopni eliminovat nebezpečí na minimum.

Proto musíte dodržovat základní zásady:

- Není žádnou ostudou, že nepoužíváte některý z mnoha platebních prostředků v prostředí internetu. Nikdo vás k tomu nemůže nutit. Pokud jej používáte, používejte pouze osvědčené a vám známé postupy. Všechny „nové“ a „moderní“ mohou být nelegálním způsobem, jak vás připravit o peníze. Všichni solidní prodejci nabízejí několik platebních metod, pokud si nejste nabízenou platební metodou jisti, klidně platbu neproveďte a požadujte pro vás důvěryhodnou metodu nebo prostě obchod neuskutečněte.
- Při platbě kartou si musíte velmi pečlivě hlídat, zde subjekt, který platbu provádí, byl vámi úspěšně v minulosti použit (gopay, comgate, payu, pays, global payments, platební brány bank…)
- Platba kartou se provádí výhradně na internetu v prostředí tzv. platební brány, nikdy nikam nic nepřeposílám ani nesděluji údaje mimo platební bránu, zejména autorizační kódy zaslané bankou ať je žádá kdokoliv, a to i opakovaně.
- Vždy je nutné zkontrolovat, zda autorizační kód přišel skutečně od vaší banky. Při běžném používání elektronického bankovnictví máte v telefonu před aktuální zprávou na konkrétním telefonním čísle zprávy o předchozích provedených platbách a zejména zkontroluji, zdůrazňujeme, zkontroluji částku a účet, na který platba odchází a zda souhlasí s mojí zamýšlenou platbou.
- K platbě kartou není nikdy potřeba sdělovat jakékoliv přístupové údaje k elektronickému bankovnímu účtu.
- Pokud vám někdo chce peníze poslat, potřebuje pouze jediný údaj, a tím je číslo vašeho účtu.
- Velmi pečlivě zvažujte, komu umožníte tzv. vzdálený přístup na plochu vašeho počítače (software např. AnyDesk,…) Musí to být opravdu člověk, jemuž velmi značně důvěřujete a vždy si jeho identitu ověřte jiným kanálem (např. telefonicky). Rozhodně v žádném případě

pro žádnou, zdůrazňujeme žádnou činnost prováděnou jakoukoliv osobou (bankéř, policista, servis PC) v citlivých programech, zejména v elektronickém bankovnictví.

- Pečlivě sledujte chování platebního systému a v případě nestandartního chování je nutné platbu přerušit, zkontrolovat přístup do elektronického bankovnictví, poslední provedené platby a autorizační telefon (pachatel po ovládnutí účtu přiloží svůj).
- Krizové stavy v bankovnictví nikdy neřeší banka ani policie přímo s klientem, vždy je nutné je ověřovat na prověřeném telefonním čísle banky.
- V případě nedostupnosti elektronického bankovnictví je nezbytné kontaktovat okamžitě svoji banku.

„Ve všech uvedených případech je zájmem pachatele jedno jediné - vylákat pod různými legendami - a vzniknou zcela určitě další a další - potřebné údaje nebo mechanismy pro ovládnuté vašeho elektronického bankovnictví či k možnosti nelegálně platit vaší platební kartou. Při vašem správném standardním chování jste sami schopni eliminovat takové nebezpečí na minimum,“ uzavírá plk. PhDr. Aleš Indra s tím, že pokud budou mít lidé jakékoliv podezření, že se stali obětí podvodníka, nesmí váhat a okamžitě se obrátit o pomoc na linku 158 nebo na nejbližší služebnu Policie České republiky.

Krajské ředitelství policie kraje Vysočina
oddělení tisku a prevence
mjr. JUDr. Dana Čírtková
tisková mluvčí
tel: 974 261 207
mobil: 725 375 094
e-mail: dana.cirtkova@pcr.cz