Varování před podvody přes internet!

Kyberkriminalita zaznamenala nárůst v řádu několika set procent!

Policisté jsou v současné době zahlcení internetovou kriminalitou. Oddělení analytiky a kybernetické kriminality PČR od počátku roku 2022 zaznamenalo obrovský nárůst případů, a to v řádu několika set procent. To obnáší velké zvýšení počtu prověřovaných případů, zvýšení počtů poškozených a jim způsobené škody přesahující milionové částky.

Internetová kriminalita tu byla i v letech minulých, ale neměla tak silné zastoupení, jednalo se o jiné způsoby páchání této trestné činnosti a zaevidovaných případů bylo znatelně méně. Bohužel v současné době pachatelé zneužívají „volný trh" a jejich působení v kyberprostoru je markantní.

U internetové (kybernetické) kriminality se jedná o majetkovou trestnou činnost, hlavně o podvody. Již od počátku jejího nárůstu bylo evidentní, že za vším stojí organizované zločinecké skupiny, které se takto vcelku snadno obohacují o obrovské zisky. V republikovém měřítku se jedná o desítky podvodů denně a o miliardy korun ročně. Pachatelé nemají důvod přestat, naopak stále mění své způsoby trestné činnosti, vymýšlejí nové varianty komunikace, vylepšují své legendy a přizpůsobují se změnám na trhu.

U INTERNETOVÉ KRIMINALITY PŘEVAŽUJÍ ČTYŘI ZÁKLADNÍ ZPŮSOBY PÁCHÁNÍ PODVODŮ.

1 Falešní zájemci o inzerované zboží

Prvním jsou podvody s falešnými zájemci o inzerované zboží. Oběti inzerují na různých portálech, v poslední době často na Vinted.cz, Bazoš.cz, Marketplace apod., kde nabízejí své zboží k prodeji, přičemž portály s tím nemají nic společného. Zpravidla cestou WhatsAppu se ozve falešný zájemce o zboží s tím, že je z jiného města a má o zboží obrovský zájem. Podvodník nabídne, že zaplatí dopravu a platbu předem a přes Whatsapp podvrhne odkaz na podvodné stránky tvářící se jako stránky přepravce typu DPD, PPL či Zásilkovna. Pak z oběti vyláká přihlašovací údaje do bankovnictví nebo i kompletní údaje k platební kartě včetně CVC kódu, který je na její druhé straně. Toto je nesmyslný požadavek, k prodeji není třeba číslo vaší karty, její platnost či CVC kód. Stejně jako požadavek přihlášení se do svého internetového účtu a následná autorizace. Správně kupujícímu poskytněte maximálně své číslo účtu, kam má peníze zaslat.

Poskytnutí všech ostatních osobních údajů a citlivých informací připravují prodávajícího o peníze, často v řádech deseti tisíců až statisíců korun. V tomto tak zvaném Phishingu jsou podvodníci bohužel velice úspěšní a prodejci naivní.

Máme případy, kdy firmy přišly o finanční částku přesahující v jednom případě 10 milionů a v druhém 13 milionů korun.

U občanů jsme evidovali největší škodu při investování do akcií, a to přes 2 miliony korun v jednom případě a v dalším případě přesahující 1 milion korun.

2 Falešní bankéři a policisté

Druhým příkladem je tzv. „falešný bankéř nebo policista", kteří volají s následující legendou. Váš účet je v ohrožení, proto musíte zajít do své banky, ale zde nikomu nic neříkat, protože pracovník banky je v této akci rovněž zapletený. Nutné je tedy peníze vybrat a vložit je do bitcoinmatu podle instrukcí, které podvodník „ohroženému klientovi" dá. Při komunikaci používají pachatelé tzv. spoofované telefonní číslo, které může napodobit skutečné číslo banky či policie. Finanční prostředky převedené na kryptoměnu se okamžitě přesouvají jinam a stávají se nedobytné. Jakkoliv se může zdát legenda pachatelů úsměvná, evidujeme bohužel případy, kdy se pachatelé projevují jako zdatní manipulátoři a přivedou tak oběť k jednání, které s odstupem času sám nechápe.

3 Investování do kryptoměn a akcií

Třetím příkladem internetové kriminality je investování do kryptoměny či akcií známých firem. Oběť reaguje na reklamu, kterou mají pachatelé na sociálních sítích nebo zpravodajských serverech, ale oběť bývá často i přímo oslovena telefonicky. Když oběť zareaguje a projeví zájem o investování, pachatel ho manipulativními technikami přiměje vyplnit dotazník s osobními údaji a zaregistrovat se na podvržených stránkách. Následuje počáteční vklad v řádech tisíců korun jako ověření, že má oběť skutečný zájem. Následně ji přimějí k tomu, v rámci pomoci a zjednodušení, aby si do počítače nainstalovala software pro vzdálenou zprávu počítače, například program AnyDesk. Tím podvodníci získají správu počítače oběti a vidí vše, co na něm dělá, aniž to tuší. Dál už jejich trestná činnost funguje poměrně jednoduše. Přímo před obětí podvodníci zadávají vlastní platební příkaz, které jim oběť potvrzuje pomocí autorizace, které oběť obdrží od banky.