Kyberkriminalita pod lupou!

21.8.2024 - Tomáš Frolík | Policie ČR

Také kyberprostor vyžaduje smysl pro orientaci!

Stejně jako je tomu na celém území České republiky, tak také v Ústeckém kraji došlo ke zhodnocení vývoje bezpečnostní situace v oblasti kybernetické kriminality a ostatní kriminality páchané v kyberprostoru. Oproti roku 2023 došlo k mírnému nárůstu této kriminality o 5,1%. Potvrzuje se trend posledních let a kontinuální nárůst kybernetické kriminality, která tvoří za první pololetí roku 2024 9,8% z celkové kriminality. Pachatelé této trestné činnosti používají důmyslné techniky sociálního inženýrství, phishingu, využívají anonymitu internetového prostoru, důvěřivost a naivnost poškozených. Nejčastější trestní jednání jsou majetkového charakteru. V mnoha případech se jedná o sériové trestné činy, kdy dokumentace, prověřování a objasňování tohoto druhu kriminality je časově náročná a vyžaduje specifickou kvalifikaci a vybavení policistů. Vyšetřování má mezinárodní přesah, narůstá analytická činnost a forenzní zkoumání nosičů dat.

Něco málo ze statistických údajů. V prvním pololetí roku 2024 byl zaznamenán další nárůst podvodných online útoků o 11%. Pokud jde o útoky na online platební prostředky, došlo k mírnému poklesu, a to o 5,9%. Naopak neoprávněných přístupů do počítačových systémů a útoků na ně ubývá, konkrétně o 22%. Mravnostní kriminalita v online prostoru zůstává bohužel na shodné úrovni, nicméně v roce 2024 dochází k poklesu u porušení autorského práva o 30,8%, což možná souvisí i s ukončením činnosti známého webu „ulozto.cz„. Stoupající tendenci zaznamenává násilná kriminalita v prostředí internetu, konkrétně trestné činy vydírání +50%, nebezpečné pronásledování +75% a nebezpečné vyhrožování +66%. Pozadu nezůstávají ani pachatelé, kteří legalizují výnosy z trestné činnosti, kdy tato trestná činnost vzrostla o 38%.

Nejčastější odvětví, se kterými se prakticky denně v online prostoru setkáváme:

a) Kybernetická kriminalita
Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230)

Ransomware - neznámý pachatel prostřednictvím škodlivého software cíleně zašifruje data uložená v interních počítačových sítí různých obchodních korporací, subjektů veřejné správy, či kritické infrastruktury, čímž znemožní činnost takového subjektu, kdy za obnovu dat požaduje výkupné v kryptoměně Bitcoin, případně Monero.

b) Ostatní kriminalita páchaná v kyberprostoru
Podvody § 209 - mírný nárůst podvodných jednání. V roce 2023 evidováno 400 skutků, v roce 2024 je to již 443 registrovaných skutků v rámci KŘP Ústeckého kraje.

Podvodný investiční makléř - *p*achatel vyvěsí na internet inzerát (reklamu) s nabídkou lákavé investice do kryptoměny, akcií, nebo jiných komodit, spolu s registračním formulářem.

Falešný bankéř - pachatel telefonicky kontaktuje poškozeného a představí se jako pracovník banky s tím, že banka detekuje pokus o napadení bankovního účtu poškozeného a je nutno co nejdříve všechny peníze z účtu vybrat a uložit na jiný „bezpečný účet“. *Falešný bankéř*

Podvodný dopravce - pachatel reaguje na inzerát poškozeného umístěného na portálech „Bazoš, Vinted a pod s tím, že chce koupit jeho nabízené zboží. Navrhne, že zaplatí přepravní službou PPL, DPD (a jiné), kdy poškozenému zašle prostřednictvím WhatsApp komunikace (či emailu) podvodný odkaz na internetové stránky, které vypadají jako stránky skutečného dopravce, či banky.

Podvodný prodej zboží - pachatel nabízí na různých inzertních portálech k prodeji různé zboží za lákavé ceny, požaduje platbu předem, či na dobírku, kdy však na místo přislíbeného zboží dodá jiné, neznačkové, bezcenné.

Podvodná nabídka brigády v prostředí internetu - pachatel v rámci sítě internet nabídne přivýdělek. Nabídka práce spočívá v tom, že zájemce má prohlížet a tzv. „lajkovat" různé weby, aby zvýšil jejich rating a tím cenu umístěné reklamy.

Podvodné seznámení - pachatel kontaktuje poškozené prostřednictvím některé sociální sítě, nebo komunikační online platformy, vydává se za „amerického vojáka, lékaře, zaměstnance ropné plošiny, námořní lodi apod., naváže citový vztah, slibuje společnou budoucnost, přičemž pod různými legendami vyláká z oběti finančními prostředky na zahraniční bankovní účty, např. k uhrazení poplatků za převod majetku do ČR, vyřízení dědictví, vyvázání se služby, podplacení úředníků za účelem vycestování do ČR, opravy lodi, operace apod.

Sociální sítě - sociální sítě se stále více stávají prostředkem k vydírání, vyhrožování, obtěžování, či projevům extremismu. Řada takových případů je prozatím řešena jako přestupky, vzestup je však vidět i na poli trestního řízení.

Čím dál tím větším trendem je to, že pachatelé tzv. investičních podvodů používají ke spáchání trestných činů umělou inteligenci. Za její pomoci nasimulují videoreklamu na podvodný investiční produkt, který prezentuje umělou inteligencí vytvořená známá osobnost, např. premiér, prezident apod.

V rámci pohybu v kyberprostoru je dobré řídit se těmito základními pravidly:
Používejte kvalitně zabezpečený počítač, notebook, telefon!
Nedůvěřujte všem informacím, které naleznete na internetu - nejedná se vždy o pravdivé informace!
Vždy si chraňte soukromí a nikdy nesdělujte žádné PIN kódy, bezpečnostní kódy, ověřovací kódy!
Nikdy neodesílejte fotografie své platební karty či osobních dokladů. Nikomu! Ani nikomu, kdo tvrdí, že je z Vaší banky!
Bankovní instituce takové informace po svých klientech NIKDY nepožadují!
Nenechte se oklamat sliby virtuálních útočníků (dárky, peníze, vztah, láska apod.)!
Nikdy nevybírejte veškeré své úspory z účtu a nevkládejte je na neznámý účet!
Telefonické hrozby informující o napadení vašeho účtu a nutící vás k nelogickým finančním transakcím jsou vždy podvodem!
Nebojte se nevhodnou komunikaci ukončit a říci jasné NE!

A nezapomínejte na to, že prevence byla, je a bude klíčem k Vašemu bezpečí!!!

https://www.policie.cz/clanek/kyberkriminalita-pod-lupou.aspx