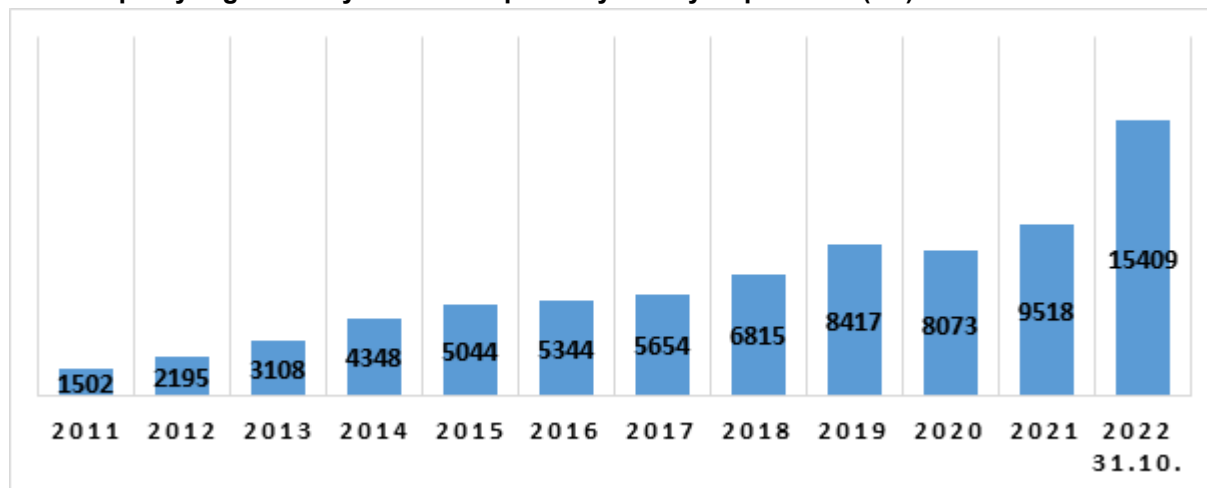


Policie ČR s ČSOB varují před zvýšenou aktivitou kybernetických zločinců

MĚLNICKO - Statistiky lámou rekordy.

Jen do října evidují policisté víc než 15 tisíc kyberzločinů. Na aktivity kybernetických podvodníků upozorňuje nová preventivní kampaň **Volač a Klikáč**.

Celkové počty registrovaných skutků spáchaných v kyberprostoru (TČ)



Policie ČR registruje do konce letošního října 15 409 trestných činů spáchaných v kyberprostoru, zatímco za celý rok 2021 to bylo 9518 a před deseti lety pouze 2195 případů. Nejčastěji se jedná o skutky motivované ziskuchtivostí. Okradených jsou desetitisíce a škody jsou ve stovkách milionů korun. Podle České bankovní asociace připadá na jednoho poškozeného klienta škoda v průměru 161 500 korun. „Počty online podvodů neustále narůstají a je tedy daleko větší pravděpodobnost, že se s nějakou hrozbou setká každý z nás a je jenom na nás, jak na to budeme připraveni. Navíc značně roste i kvalita a sofistikovanost těchto útoků. V posledních letech u online podvodů zaznamenáváme prvky organizovaného zločinu s mezinárodním přesahem. Odhalování je zde velmi složité a zdoluhavé, a proto je potřeba, aby se každý choval obezřetně a nenechal se natchytat,“ doplňuje **Tomáš Kubík, náměstek policejního prezidenta pro Službu kriminální policie a vyšetřování**.

ČSOB a Policie ČR společně v rámci dlouholeté spolupráce připravili preventivní kampaň s názvem Volač a Klikáč, aby zvýšili povědomí o této problematice, varovali před kyberpodvodníky a ukázali na co si dát pozor.

Podvodné navolávání (Volač)

Podvodníci se často vydávají za pracovníky bank a dokonce i policisty. Zneužívají neznalost a důvěřivost občanů a snaží se klienty bank vystrašit a zmanipulovat. Cílem pachatelů je vylákat z poškozeného citlivé údaje či ho donutit k bankovním převodům, nebo dokonce výběrům hotovosti a následnému nákupu kryptoměny. Nepodceňujeme pachatele. Jejich jednání je nesmírně manipulativní a přesvědčivé. Za poslední dva roky, co se tímto projevem ve větší míře setkáváme, jsme zaznamenali více jak 1000 případů. V některých jednotlivých případech jdou škody až do milionů korun.

Pachatelé se také snaží pod různými legendami vylákat i vzdálený přístup do našeho počítače, či mobilního telefonu. Mohou se vydávat za pracovníky bank, investiční poradce, nebo třeba pracovníky technické podpory.

Velmi vysoké škody zaznamenáváme také u případů, kdy lidem falešní investiční poradci přes telefonáty nabízejí možnost výhodné investice bez rizika, ale vše může být jen fikce a následky jsou často fatální. Nenechte se zlákat na přehnaně výhodné nabídky. Investujte s rozumem a raději u zavedených společností.

Podvodné odkazy (Klikáč)

Pachatelé se snaží pod různými legendami nalákat poškozené na webové stránky, které jsou prakticky k nerozeznání od těch pravých. Vždy proto dávejme pozor, kam zadáváme své citlivé a přihlašovací údaje.

Zde je velmi důležité být obezřetný a vše raději ověřit jinou cestou.

„Digitální bezpečnost patří k prioritám skupiny ČSOB v péči o klienty. Na investice do bezpečnosti a prevence vynakládáme ročně stamilióny korun, ale před zákeřnými kyberpodvodníky se nemůže bohužel ukrýt nikdo. Jsou organizovaní, stále profesionálnější a naprosto bez zábran, takže lze čekat jejich útoky ve zvýšené míře zejména před Vánocemi. Nejlepší prevencí jsou obezřetnost, informovanost a nebát se zeptat. Cílem naší nové společné kampaně s Policií ČR je zvýšit úroveň znalostí a naučit lidi základní pravidla efektivní obrany,“ říká Petr Hutla, člen představenstva ČSOB.

Znamé typické případy:

- Podvody spojené s inzercemi. Útočníci v současnosti cílí převážně na prodávající. Zareagují na vámi nabízené zboží na inzertním portálu a snaží se vás nalákat na platební bránu, kde máte zadat citlivé bankovní informace, včetně pinu k vaší platební kartě. S tím, že vám pak zašlou peníze. Je to nesmysl. Když něco prodáváte, tak kupujícímu pro zaslání platby stačí pouze číslo vašeho bankovního účtu. Těchto útoků registrujeme jen v letošním roce takřka 2000.
- Podvodné SMS zprávy. Útočníci zasílají velké množství SMS zpráv, které se vás pod různými legendami snaží přinutit ke kliknutí na přiložený odkaz, který zpravidla vede na webovou stránku, která je k nerozeznání od pravé. V současnosti se pachatelé vydávají například za banku či přepravní společnost a snaží se z obětí vylákat citlivé údaje a přístupová hesla k bankovníctví. V poslední době zaznamenáváme velké množství SMS zpráv s fiktivními státními sociálními příspěvky. Toto je velmi nebezpečné, protože velké množství lidí nějaké příspěvky očekávají. Pravděpodobnost kliknutí na přiložený odkaz je u SMS zpráv až 8x větší než u podvodného e-mailu.
- Topované odkazy na bankovníctví. V případě, že do internetového vyhledávače zadáte jméno vaší banky, tak je možné, že první výsledek, který vám prohlížeč nabídne, bude podvodná stránka, která bude k nerozeznání od webové stránky vaší banky. Zde je nutné pečlivě kontrolovat správnost webové adresy.
- Klasický phishing, neboli podvodné e-maily. Pachatelé rozesílají čím dále větší množství podvodných e-mailů, přes které se snaží vylákat citlivé údaje, provedení platby, nebo rozesílají viry. V období před Vánocemi očekáváme velký nárůst zpráv, které se budou tvářit jako zprávy od přepravních společností. Pachatelé tak využívají toho, že ztrácíte přehled o objednaném zboží. Pozor! Velké množství podvodných zpráv registrujeme i na sociálních sítích. Nikdy nevíte, s kým si píšete.

A proto Klikač a Volač dostali reálnou podobu. Aby si je lidé dokázali představit v běžném životě a dokázali se na ně připravit v podobě dodržování osvědčených postupů.

„Základní pravidla jsou velmi jednoduchá. Chceme naučit lidi, aby si před každým kliknutím na odkaz v SMS zprávě nebo v emailu či před zodpovězením otázky volajícímu sami položili dotaz: Nechce mě náhodou okrást? Není to náhodou Volač nebo Klikač? Banky totiž nepožadují citlivé osobní informace nebo data o účtech nebo kartách, protože své klienty znají nejlépe,“ vysvětluje Petr Vosála, manažer bezpečnosti digitálních kanálů ČSOB. Podle něho je v případě nejistoty a pochybností je nejlepší vždy kontaktovat přímo klientská centra bank, která fungují nonstop.

Odkaz na video PČR Volač a Klikač: <https://youtu.be/dn0tVxolFcE>

plk. Mgr. Zuzana Pidrmanová
vedoucí oddělení prevence