MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Společné výzvy v boji proti počítačové kriminalitě.

Zdroj: https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges

Autor: Europol a Eurojust

Cílem tohoto dokumentu je identifikovat a kategorizovat společné výzvy v boji proti počítačové kriminalitě a to jak z hlediska prosazování práva, tak i z hlediska soudního. Identifikované výzvy spadají do pěti hlavních oblastí:

- ztráta dat;
- ztráta místa (dislokace pachatele);
- výzvy spojené s vnitrostátními právními rámci;
- překážky mezinárodní spolupráce; a
- výzvy partnerství veřejného a soukromého sektoru.

Figure 1: Common Challenges in Combating Cybercrime

Tento dokument dále zkoumá některé praktické důsledky těchto výzev a navíc uvádí některé z nejdůležitějších probíhajících činností a otevřených otázek, týkajících se každé z identifikovaných výzev.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Ztráta dat

Jestliže v některých členských státech EU existuje povinnost poskytovatelů internetových služeb uchovávat informace pro potřeby vymáhání práva a v jiných ne, jde o závažnou překážku úspěšnému vyšetřování a stíhání závažných trestných činů, včetně rozmáhající se počítačové kriminality (kybernetické útoky, nadnárodní platební podvody, Dark Web, atd.). Otevřeným problémem proto zůstává potřeba nového legislativního rámce, upravujícího na úrovni EU uchovávání relevantních údajů pro potřeby prosazování práva.

Výzvy související s řízením internetu

Problém ztráty dat je také pociťován rozšířeným zaváděním technologií CGN (Carrier Grade Network Address Translation) společností ISP. Technologie CGN vedla k vážným nedostatkům v oblasti online v oblasti vynucování práva při vyšetřování a přičítání trestné činnosti. Vzhledem k vyčerpání IP adres v rámci IPv4 (Internet Protocol Version 4) využívají poskytovatelé služeb CGN technologie ke sdílení jedné veřejné IPv4 adresy mezi více účastníky (koncovými uživateli) ve stejnou dobu (možná několik tisíc).

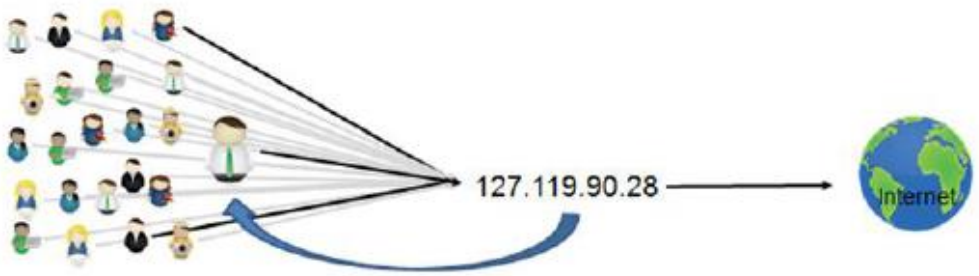

Figure 2 Carrier-Grade Network Address Translation (CGN)

Aby byli poskytovatelé internetových služeb technicky schopni identifikovat koncového uživatele za CGN na základě veřejného protokolu IPv4, je třeba, aby jim donucovací orgány poskytly adresu IPv4, přesný čas připojení a číslo zdrojového portu. Cyber vyšetřovatelé jsou pak konfrontováni se seznamy potenciálně stovky nebo dokonce tisíce koncových uživatelů spojených s určitou veřejnou adresou IPv4, jejíž vyšetřování vyžaduje mnoho zdrojů, způsobuje dlouhé zpoždění a generuje otázky soukromí pro mnoho nevinných zákazníků.

Řešení tohoto problému je dosud otevřené a dosud není stanoven pevný postup jeho řešení.

Obdobný problém existuje ve vztahu k databázi WHOIS. Databáze WHOIS je základním prvkem online odpovědnosti, protože je jediným místem na internetu, na kterém lze zjistit, kdo je zodpovědný za určité doménové jméno a kdo je zodpovědný za e-maily a webové stránky,

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

které tento název domény používají. Tyto otázky jsou výchozím bodem každého vyšetřování trestné činnosti založené na doméně.

Provozovatelé registrů a registrátoři mají povinnost redigovat všechny osobní údaje z veřejně dostupných záznamů WHOIS. Od registrů a registrátorů se vyžaduje, aby poskytovali „přiměřený přístup“ k osobním údajům v registračních údajích třetím stranám. Jedná se o roztříštěný systém pro poskytování přístupu, který se skládá z potenciálně tisíců různých politik v závislosti na zúčastněném registrátorovi. Tento nedostatek konzistentních politik pro přístup k neveřejným informacím způsobuje zpoždění při vyšetřování a má závažné provozní důsledky.

I řešení tohoto problému je dosud otevřené, přičemž cílem je konsensus na jednotné politice.

Šifrování

Stále větší počet poskytovatelů elektronických služeb implementuje ve svých službách standardně šifrování. Současně jsou široce dostupné a podporovány nástroje, které umožňují osobní šifrování anebo anonymizaci komunikací a dalších dat. V důsledku toho se stávající vyšetřovací techniky, jako je zákonné odposlechy komunikace, stávají méně účinnými nebo dokonce technicky nemožnými. Zvýšená implementace šifrování také negativně ovlivňuje digitální forenzní analýzu, což vede k situaci, kdy jsou zločinci schopni účinně a donekonečna skrývat kritické důkazy a jejich nezákonné činnosti před vymáháním práva.

Tento vývoj má vážné důsledky pro vyšetřování kyberkriminality, neboť narušuje schopnost orgánů činných v trestním řízení a soudních orgánů získat informace potřebné jako důkaz a trestně stíhat a odsoudit pachatele trestných činů.

Řešením problému by mělo být poskytování vymáhání práva s plným souborem nástrojů, technik a odborných znalostí potřebných k řešení trestného zneužívání šifrování.

Kryptoměny

Rozšiřování kriminálního využití decentralizovaných kryptoměn silně komplikuje možnosti odhalování a vymáhání majetku, jakož i předcházení podvodným transakcím. Nedostatek (minimálních) standardů pro due diligence a Know-Your-Customer (KYC) vytváří další výzvy pro vyšetřování počítačové kriminality.

Kryptoměny jsou nadále zneužívány kybernetickými zločinci, přičemž Bitcoin je měnou volby na trzích trestných činů a jako platbu za pokusy o vydírání vydávané v kybernetickém režimu, jako jsou ransomware a útoky Distributed Denial of Service (DDoS). Bitcoin je proto primárním krypto-měny, se kterou se setkávají orgány činné v trestním řízení v rámci vyšetřování trestných činů.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Zatímco znalosti a zkušenosti v tom, jak vyšetřovat, sledovat a využívat kryptoměny stále roste v oblasti prosazování práva a soudnictví, doplněné různými nástroji soukromého sektoru pro přidělení, jsou tyto znalosti často omezeny na Bitcoin, a nikoli na jiné kryptografické nástroje. na trhu trestných činů.

Řešení problému lze shrnout jako potřebu zásadního zvyšování příslušného typu odbornosti na úseku vymáhání práva.

Ztráta místa (dislokace pachatele)

Nedávné trendy, jako je rostoucí míra trestného zneužívání nástrojů pro šifrování anebo anonymizaci, kryptoměny a Dark Web, také vedly k situacím, kdy vymáhání práva již nemůže (rozumně) stanovit fyzické umístění pachatele, infrastruktury nebo elektronických důkazů. V těchto situacích je často nejasná země s jurisdikcí, stejně jako právní rámec, který upravuje (v reálném čase) shromažďování důkazů nebo využívání zvláštních vyšetřovacích pravomocí, jako je sledování trestné činnosti online a různá utajená opatření.

Rostoucí využívání úložišť a služeb založených na cloudu navíc znamená, že data uložená v cloudu mohou být fyzicky umístěna v různých jurisdikcích.

Ztráta místa může také vést k nejistotě ohledně soudní pravomoci týkající se výkonu procesních opatření, zdůrazňující potřebu včasného zapojení soudních orgánů prostřednictvím Eurojustu, přímých policejních kanálů pro spolupráci a komunikaci usnadněných Europolem a neustálé inovace v oblasti soudnictví. proces operativní spolupráce.

Otevřeným problémem je Mezinárodní právní rámec pro přímý přeshraniční přístup k údajům (včetně cloudstorage).

Výzvy spojené s vnitrostátními právními rámci

Problémem jsou rozdíly jednotlivých legislativ. Hlavní rozdíly se týkají kriminalizace chování a ustanovení pro vyšetřování počítačové kriminality a shromažďování elektronických důkazů. V členských státech existují například různá opatření a sankce, pokud jde o boj proti bezhotovostním platebním podvodům. Přizpůsobení a sladění právních rámců je často časově náročné a obtížné vzhledem k rychlému vývoji krajiny ohrožující počítačovou kriminalitu.

Právní předpisy by měly být harmonizovány na úrovni EU, což by umožnilo účinnější společné operativní akce. Konkrétně by bylo možné v rámci EU harmonizovat možnosti sledování

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

trestné činnosti online a zákonného shromažďování kritických důkazů na webových stránkách Deep Web a Dark Web, aby se umožnily účinné provozní činnosti a následné zavedení důkazů v soudním řízení.

Otevřeným problémem je rozvoj celoevropského právního rámce pro provádění on-line vyšetřování, konkrétně na webu Deep Web a Dark Web.

Překážky mezinárodní spolupráce

V mezinárodním kontextu neexistuje žádný společný právní rámec pro urychlené sdílení důkazů (stejně jako pro zachování důkazů). Tato situace znamená, že v praxi, i když jsou důkazy zachovány, může uplynout dlouhá doba, než budou důkazy dostupné pro vyšetřování trestného činu nebo soudní řízení v dožadující zemi. Sběr elektronických důkazů je však často otázkou citlivou na čas. Současný proces je odborníky vnímán jako příliš pomalý na to, aby mohl efektivně shromažďovat a sdílet elektronické důkazy.

Zřetelně je zapotřebí lepší mechanismus pro přeshraniční komunikaci a výměnu informací pro účely vyšetřování, prevence a ochrany, ale také zajistit, aby jakákoli následná žádost o právní pomoc byla v souladu se všemi příslušnými právními požadavky dožádané země.

Rozsáhlé kybernetické útoky představují specifickou výzvu pro mezinárodní spolupráci. Vzhledem k zásadní úloze, kterou donucovací orgány a soudnictví hrají při vyšetřování rozsáhlých incidentů kybernetické bezpečnosti nebo krizí podezřelé škodlivé povahy, je zásadní jejich včasné zapojení do plánovaných činností reakce zásadní. Důležitá je také jejich aktivní účast na kybernetických simulačních cvičeních, neboť tato činnost usnadňuje důvěru a spolupráci
s komunitou v oblasti bezpečnosti sítí a informací.

Výzvy partnersví veřejného a soukromého sektoru

Otevřené problémy se v tomto směru týkají právního rámce takové spolupráce, tj. nastolení legislativní rovnováhy mezi potřebami týkajícími se soukromí a přiměřenými opatřeními, která by soukromému sektoru umožnila nepřetržitě podporovat vymáhání práva v boji proti počítačové kriminalitě. Totéž se týká jasných a transparentních pravidel pro zapojení soukromých osob do shromažďování důkazů. Další problémy se týkají zneužívání hranic jednotlivých jurisdikcí a schopnosti zpracovávat enormní objemy dat při vyšetřování případů počítačové kriminality.