IKSP

Institut pro kriminologii
a sociální prevenci

Prosinec 2020

Kyberkriminalita v kriminologické perspektivě

HLAVNÍ ZJIŠTĚNÍ

↑ Pokračující trend růstu kyberkriminality je zjevný a její paleta pestrá. Zahrnuje celou řadu skutkových podstat jako podvod, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, poškození a ohrožení provozu obecně prospěšného zařízení aj., ale především tzv. počítačové trestné činy (§ 230-232 TZ, dříve § 257a sTZ). Od samého počátku jejich kriminalizace pozorujeme rapidní nárůst detekovaných útoků, nemluvě o značné latenci. Navzdory více či méně se zvyšujícímu počtu objasněných skutků se zdaleka nedaří pokrýt jejich nápad, a tak se objasněnost pohybuje v posledních letech zhruba na úrovni třetiny. Z hlediska justiční statistiky se situace zdá jen o málo lepší, když počet odsouzených oproti stíhaným osciluje v nadpolovičním množství, oproti obžalovaným pak kolem tří čtvrtin.

☑ Řadu zajímavých informací poskytla analýza trestních spisů vztahujících se k tzv. počítačovým trestným činům (§ 230-232 TZ), byť s výhradou omezené vypovídací hodnoty s ohledem na nízké četnosti a na předpokládanou vysokou latenci. O počítačových trestných činech rozhoduje obvykle okresní (obvodní) soud, zhruba ve dvou třetinách případů pachatel jednal v souběhu s dalším skutkem (především majetkového charakteru). Ve čtvrtině věcí soud obviněného zprostil obžaloby nebo řízení zastavil, odsouzeným pak uložil nejčastěji trest odnětí svobody, který podmíněně odložil.

Více než ve třetině kauz měli obvinění zneužít přístup k informační a komunikační technologii umožněný v souvislosti se zaměstnáním nebo díky důvěře poškozených. V téměř pětině případů měli obvinění zneužít cizích přihlašovacích údajů k různým účtům (sociální sítě, e-maily, internetové bankovnictví). Podobně často přihlašovací údaje někde nalezli (např. uložené v počítači, napsané na papíře). K využití technických prostředků došlo jen minimálně. K největším slabinám ochrany patří fyzické zabezpečení, dále ochrana e-mailových schránek, profilů na sociální síti Facebook a informačních systémů přístupných zaměstnancům. Z hlediska osobních údajů dochází v drtivé většině případů ke zneužití hesla.

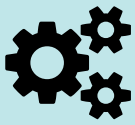
V rámci projektu byla část pozornosti věnována též specifické problematice kybergroomingu, tj. navazování kontaktů s dětmi v online prostředí za účelem jejich sexuálního zneužití. Takové jednání je od roku 2014 kriminalizováno (mimo jiné) coby navazování nedovolených kontaktů s dítětem (§ 193b TZ). Počet odsouzených případů (většinou prvopachatelé a častěji mladší 30 let) od té doby narůstal až po 45 odsouzených pachatelů v roce 2019, přičemž jejich charakteristiky a modus operandi zhruba odpovídal předpokladům uváděným v odborné literatuře.

DALŠÍ ZJIŠTĚNÍ

S vybranými odborníky byly realizovány polostrukturované rozhovory zaměřené na problematiku kyberkriminality, aktuální i možné budoucí hrozby, jakož i preventivní doporučení. Všichni hovořili o ransomwaru, většina se pak shodla na dalších tématech jako podvody v mezinárodním obchodě, dětská pornografie, slabiny infrastruktury, sociální inženýrství (mj. ve vztahu k zaměstnancům), shromažďování dat velkými korporacemi, rizika vyplývající ze zanedbávání aktualizací, využívání cloudů a samozřejmě také potenciální riziko v podobě zaměstnanců a především lidského faktoru vůbec. Shodně doporučovali zejména pravidelně aktualizovaný ochranný software a osvětu - zajistit typickým či aktuálním kauzám náležitou publicitu a školit v oblasti bezpečnosti informačních a komunikačních technologií zaměstnance i řadové uživatele (s důrazem na obezřetnost v oblasti přihlašovacích údajů).

ÚDAJE O VÝZKUMU

Výzkum byl realizován v letech 2016-2020. Analýza trestních spisů zahrnovala kauzy pravomocně skončené v roce 2015.



V rámci výzkumu byla provedena analýza trestních spisů zaměřená na tzv. počítačové trestné činy. Na jejím základě byla získána statisticky zpracovatelná a do budoucna srovnatelná data.

Realizováno bylo též dotazníkové šetření zaměřené na na zkušenosti obyvatel České republiky s vybranými jevy v on-line prostředí. Získané poznatky budou publikovány samostatně.

Cílem výzkumu bylo především získání, analýza a vyhodnocení nových poznatků o prevalenci vybraných forem kyberkriminality, pachatelích a jejich trestné činnosti.

TEORETICKÝ RÁMEC VÝZKUMU

V dnešní společnosti prostupují digitální technologie a zejména internet každodenním životem s jednoduchou samozřejmostí, od mobilního telefonu s e-mailem po chytré město. S tzv. internetem věcí a narůstající penetrací blížící se u některých věkových kategorií 100 % se objevuje i kriminalita s tím spojená - kyberkriminalita. Zahrnuje jak „tradiční kriminalitu v novém kabátě“, tak zcela nové formy kriminality nemyslitelné bez virtuálního prostředí (typicky malware). Protože jde o relativně novou, širokou a rychle se měnící oblast, výzkum se zaměřil na dvě hlavní části, a to počítačové trestné činy tak, jak je registrují orgány činné v trestním řízení, a na zkušenosti obyvatel ČR s některými jevy online. Proběhla analýza dostupných statistických údajů a vybraných trestních spisů, dále několik rozhovorů s experty a sběr dat v rámci dotazníkového šetření. Přetrvávající vzrůstající trend kyberkriminality je evidentní, a tedy i zájem o tuto problematiku z perspektivy kriminologického výzkumu.

Celý výzkum je k dispozici zde