Kybernetická kriminalita v ČR z kriminologické perspektivy

Podklady pro zasedání Republikového výboru pro prevenci kriminality 27. května 2021

Institut pro kriminologii a sociální prevenci

Mgr. Kateřina Kudrlová, Ph.D.

Dnešní společnost si lze jen stěží představit bez digitálních technologií (dále jen „ICT“). Prostupují každodenním životem běžných občanů s jednoduchou samozřejmostí: mobilní telefon, e-mail, sociální sítě, zpravodajství a nakupování online, od chytré domácnosti po chytré město. Používání internetu pomalu, ale jistě proniká všemi věkovými kategoriemi. V souvislosti s vývojem technologií a kyberprostoru se objevuje i kyberkriminalita, a to jak „tradiční kriminalita v novém kabátě“, tak nové formy kriminality (typicky malware). Její definice i členění se různí, můžeme se však spokojit s jejím označením za kriminalitu využívající informační a komunikační technologie.

Na kyberkriminalitu dopadá řada skutkových podstat (např. podvod), především však tzv. počítačové trestné činy (§ 230-232 TZ, dříve § 257a sTZ). Od samého počátku jejich kriminalizace roste počet detekovaných útoků, nemluvě o značné latenci, přičemž objasněnost v posledních letech klesla z necelé třetiny na pětinu v roce 2019 (zejména pro větší nápad) a v pandemicky neobvyklém roce 2020 pak na 12 %. Vzhledem k rostoucímu významu, počtu uživatelů i šíři aktivit online se na toto prostředí zaměřil i jeden z předchozích výzkumných úkolů IKSP, který se věnoval právě registrovaným počítačovým trestným činům.

Byly tak analyzovány trestní spisy zahrnující řízení o počítačových trestných činech, v nichž byla podána obžaloba a trestní řízení pravomocně skončilo v roce 2015 – šlo o 66 trestních spisů (z celkového počtu 71 věcí, včetně 27 řízení vedených pro spáchání výlučně počítačového trestného činu) zahrnujících 68 obviněných.[1] Sledované proměnné zahrnovaly zejména údaje o skutcích, pachatelích a o trestním řízení (např. způsob jednání, věk pachatele nebo délka trestního řízení).

[1] Kromě analýzy trestních spisů byly součástí projektu i polostrukturované rozhovory s vybranými odborníky a především realizace rozsáhlého dotazníkového šetření (viz dále).

V aktuálně probíhajícím projektu IKSP (Posouzení trendů kyberkriminality, 2021-2023) se pozornost zaměřuje zejména na analýzu poznatků získaných dotazníkovým šetřením realizovaným v listopadu 2020 prostřednictvím agentury ppm factum. Byly získány údaje od reprezentativního vzorku 6.811 českých uživatelů internetu ve věku 16-74 let. Respondenti vypovídali o svých zkušenostech za uplynulý rok v několika oblastech online: používaná zařízení, aplikace (obchodování online, internetové bankovnictví, e-mailové účty, sociální sítě, herní účty) a bezpečnostní návyky s nimi spojené, a to v roli oběti i pachatele.

Následující text předkládá vybrané poznatky získané analýzou trestních spisů a údajů z dotazníkového šetření, uváděné hodnoty jsou částečně zaokrouhleny.

Vybrané výsledky analýzy trestních spisů (§ 230-232 TZ, 2015)

Nejpočetněji jsou zastoupeni obvinění ve věku do 24 let (v rozmezí 17-58 let), téměř polovina jich je mladší 30 let (průměrný věk 34 let). Mezi obviněnými mladšími 30 let šlo pouze zhruba ve třetině o recidivisty, mezi staršími obviněnými pak jen o pětinu recidivistů (oproti zhruba polovině pachatelů-recidivistů v rámci kriminality celkové). Zdá se proto, že kyberkriminalita je doménou spíše prvopachatelů. Deset obviněných se dopustilo svého jednání v souvislosti se svým postavením úřední osoby, včetně pěti příslušníků Policie ČR.

Pětinu obviněných tvořily ženy, z nichž polovina byla ve věku 35-49 let (v rozmezí 19-56 let průměrný věk 38 let) a pouze 13 % recidivistek. Odsouzeno bylo menší procento žen oproti mužům, nicméně uložené tresty byly v průměru delší.

K využití technických prostředků došlo jen minimálně. Více než ve třetině kauz šlo o zneužití přístupu k informační a komunikační technologii v souvislosti se zaměstnáním nebo díky důvěře poškozených, kteří usnadnili neoprávněný přístup tím, že dostatečně nezabezpečili svá hesla. Ta byla odhadnutelná, fyzicky přístupná, neměnná či pro pachatele snadno obnovitelná. V téměř pětině případů měli obvinění zneužít cizích přihlašovacích údajů k různým účtům (především k e-mailům,[2] které významně souvisely se čtvrtinou všech sledovaných řízení, dále k sociálním sítím a internetovému bankovnictví), podobně často přihlašovací údaje někde nalezli (např. uložené v počítači, napsané na papíře). K největším slabinám ochrany tak patří

[2] Zneužito např. za účelem pátrání po nevěře, komunikace jménem poškozeného nebo přeposílání e-mailů konkurenci.

fyzické zabezpečení, dále ochrana e-mailových schránek vůbec, profilů na sociální síti Facebook a informačních systémů přístupných zaměstnancům.

Sledovaná jednání lze rozdělit zhruba na polovinu na virtuální násilí[3] a majetkovou trestnou činnost, přičemž obdobné rozdělení prochází napříč různými kategoriemi, včetně např. věku nebo vzdělání.[4] Konkrétně šlo ve 40 % případů o snahu o finanční přilepšení a ve 30 % o důsledek komplikované vztahové situace, v obou kategoriích se také rýsují určité skupiny podobných pachatelů/jednání. U majetkových deliktů (v polovině případů šlo o zneužití přístupu k ICT) jsou to příslušníci Policie ČR (zneužití přístupu do policejních informačních systémů), „vynalézavé ženy" (zneužití postavení v zaměstnání při řešení své špatné finanční situace) a „datoví magnáti" (zneužití osobních údajů klientů z informačních systémů zaměstnavatele). Dále pak „geekové" (zneužití vlastních ICT schopností a přístupu ke konkrétnímu zařízení či informačnímu systému) a „online zloději" (zneužití přihlašovacích údajů k různým účtům obětí ze svého bezprostředního okolí). U virtuálního násilí (obviněný v 90 % kauz znal oběť a obvykle zneužil znalost hesla či přístup k zařízení v důsledku vztahu s obětí) jde o „mstitele" (zejména mladší bezúhonní muži škodící bývalým partnerkám) a „žárlivce" (škodí podobně jako „mstitelé", leč napadají i stávající partnerky a usilují o jejich kontrolu).

Mezi poškozenými byly fyzické i právnické osoby, ve třech čtvrtinách věcí šlo o 1 poškozeného, ve zbývajících věcech o 2-5 osob, pouze ve 4 řízeních figurovaly desítky až stovky poškozených. Pachatelé způsobili ve 40 % kauz finanční škodu (1.200 Kč - 27 milionů Kč), nemajetkovou újmu uváděli poškození v 70 % věcí. V téměř dvou třetinách věcí se obvinění s poškozenými osobně znali (ve třetině šlo o jejich stávající či bývalé partnery, v pětině o prosté známé, v desetině o příbuzné), ve třetině útočili na své zaměstnavatele (stávající či bývalé). Obvinění v zaměstnaneckém či služebním poměru s poškozeným subjektem byli o něco starší (průměrně ve věku 38 let, v rozmezí 21-56 let).

Trestní řízení trvala průměrně 1,5 roku, 90 % věcí bylo skončeno do 2,5 roku. Přípravné řízení zabralo průměrně 0,8 roku, řízení před soudem 0,7 roku. U většiny věcí vyřešených do 2 let převažovala doba přípravného řízení.

[3] Např. zveřejňování intimních fotografií poškozených, dehonestující komunikace jejich jménem atp.
[4] Liší se např. v závislosti na pohlaví, neboť pouze 30 % pachatelek se dopustilo virtuálního násilí, nebo při zohlednění postavení úřední osoby, které až na výjimku sledovaly majetkový zájem.

Vybrané výsledky analýzy údajů z dotazníkového šetření (2020)

Prvotní poznatky z dotazníkového šetření naznačují, že penetrace kyberkriminalitou se (přibližně) v uplynulém roce pohybovala převážně v řádu do 5 %. Výjimku představuje tzv. phishing požadující peníze, s nímž se setkala až téměř polovina respondentů.

Podobně jako vyplynulo z analýzy trestních spisů (viz výše), respondenti se nejčastěji setkali s napadením soukromé e-mailové schránky (5 %, 366 respondentů), a to ve třetině všech 64 případů se známým pachatelem ex-partnerem a ve třetině partnerem (31 a 27 %). Více než čtvrtina útoků spočívala v převzetí identity, pětina pak ve zjištění nějakých informací (28 a 22 %).[5] Naproti tomu se 3 % respondentů (169 osob) k napadení e-mailové schránky přiznalo, přičemž za oběť označili nejčastěji partnera a někoho z úzkého rodinného kruhu (v obou případech zhruba třetina napadených, 33 a 31 %) a za zdaleka nejčastější jednání zjištění informací (59 %).

Partner figuroval i při zneužití internetového bankovnictví (zkušenost měla shodně 3 % obětí i útočníků). Oběti (199 respondentů) označovaly za pachatele kromě partnera (23 %) e-shop či poskytovatele nějaké služby (29 %, např. opakované strhávání plateb) nebo ex-partnera (14 %). Naproti tomu pachatelé (191 respondentů) označovali za majitele zneužitých účtů především své partnery a někoho z úzkého rodinného kruhu (41 a 38 %) a především zjišťovali finanční informace (49 %), ale také převáděli peníze (100 Kč – 900 tis. Kč, 36 %).

Respondenti měli zkušenosti i s ransomwarem a již zmíněným phishingem. S ransomwarem se setkala 4 % v roli oběti (290 osob, z toho 40 % opakovaně), 37 osob (0,4 %) pak v roli pachatele (70 % opakovaně), přičemž nejčastější požadovanou měnou byly postupně české koruny, bitcoiny, eura (33 %, 22 %, 17 %). S phishingem požadujícím peníze se setkalo 3.040 respondentů (45 %, včetně 315 pouze pravděpodobných útoků) a s phishingem požadujícím osobní údaje 1.695 osob (25 %, včetně 281 pouze pravděpodobných útoků). Za odesílatele phishingu se označilo pouhých 28 respondentů (0,4 %).

Poslední zde zmíněnou oblastí je zneužití soukromého účtu na sociální síti (převážně Facebook). Mezi oběti se zařadila 4 % respondentů (377 osob, z toho 26 % opakovaně), mezi útočníky 2 % (100 osob, z toho 14 % opakovaně). Mezi známé útočníky (59 případů) řadily oběti nejčastěji zcela cizí osoby bez vzájemného vztahu (20 %), dále partnery a ex-partnery

[5] U zaměstnaneckého e-mailu byl nejčastějším známým útočníkem spolubydlící (třetina případů) a nejčastějším jednáním stažení obsahu, zjištění informací a převzetí identity (shodně po čtvrtině věcí).

(shodně po 15 %) a osoby z úzkého rodinného kruhu (12 %). Tito respondenti hovořili zejména o převzetí identity a vkládání obsahu (26 a 25 %), dále o změně přihlašovacích údajů (16 %) a zjišťování informací (13 %). Útočníci označili za napadené naproti tomu především své partnery (44 %) a osoby z úzkého rodinného kruhu (18 %). Přiznali se nejčastěji ke zjišťování informací (64 %), výrazně méně často pak ke stažení nějakého obsahu (12 %) či k jinému jednání. Podobně jako u zneužití e-mailových schránek je tedy evidentní, že zneužití spočívá v řadě případů v „pouhém" zjištění informací, o kterém se napadený pravděpodobně nedozví.

Ve všech výše uvedených oblastech byli mimo jiné za účelem odhadnutí míry latence respondenti dotázáni, jakým způsobem řešili vlastní napadení/zneužití, včetně obrácení se na policii.[6] Oznamovaná jednání se rozdělila do dvou skupin: spíše jen sporadicky (do 5 %) se respondenti obrátili na policii při řešení phishingu (2-3 %), zneužití soukromé e-mailové schránky a soukromého účtu na sociální síti (obojí 5 % napadených). Výrazně častěji (kolem 15 %) však hledají pomoc policie respondenti, kteří se stali obětí zneužití internetového bankovnictví, ransomwaru či zneužití zaměstnaneckého e-mailu (14, 15 a 16 %). Pro úplnost je vhodné podotknout, že respondenti, kteří se na policii obrátili, s ní byli převážně spokojeni (56-82 % osob bylo zcela či spíše spokojeno).

Výše uvedené poznatky představují souhrn informací z ukončeného výzkumného úkolu IKSP, jehož podrobné výsledky jsou publikované a dostupné online na www.kriminologie.cz (J. Vlach, K. Kudrlová, V. Paloušová. Kyberkriminalita v kriminologické perspektivě. IKSP, 2020). Poznatky z dotazníkového šetření představují prvotní základní informace získané v rámci právě probíhajícího projektu. Výsledná zjištění budou postupně publikována a zahrnou podrobnější analýzy (např. vztah mezi věkem a pohlavím uživatelů a některými jejich bezpečnostními návyky), kromě oblastí stručně představených výše se budou věnovat mimo jiné také obchodování online a používání herních účtů.

[6] Záměrně bez rozlišení Policie ČR.