



ZÁKLADNÍ METODIKA PRO PRÁCI S OBĚTÍ KYBERNETICKÉ KRIMINALITY PRO POLICISTY

Jak postupovat při přijetí oznámení v oblasti kyberkriminality,
jak pracovat s důkazy, kde vyhledat podporu?

POSTUP PŘIJETÍ OZNÁMENÍ

1. Co se stalo?

Podvod – elektronické nákupy, podvodné inzeráty a aukce, falešné e-shopy, nedodání objednaného zboží, dodání zboží, které neodpovídá objednanému, podvodné vylákání např. informací k bankovním účtům, platebním kartám, přístupům do e-mailu či do účtů na sociálních sítích (nebo jiných elektronických systémů).

Mravnostní trestná činnost – držení a šíření zakázané pornografie (především dětské), lákání dětí na schůzky, navazování kontaktů s dětmi.

Porušování autorských práv – sdílení nebo jiné šíření filmů, hudby, knih apod.

Neoprávněný přístup k nosiči informací – neautorizované vstupy do elektronických systémů jako je např. e-mail, účet na sociální síti, počítačový systém aj.

Vyhrožování, vydírání, urážení (hate speech) např. v diskuzních příspěvcích, propagace hnutí směřující k potlačování práv člověka a mnohé jiné.



POSTUP PŘIJETÍ OZNÁMENÍ

2. Pak je třeba ověřit

Zda **oznamovatel nezničil elektronické stopy** (blokace útočníka, vymazání komunikace atd.).

Zajistit **souhlas s přístupem do internetových služeb** (profil na sociální síti, e-mailová schránka apod.), u osoby mladší 18 let souhlas i zákonného zástupce.

Náležité **poučení poškozeného + sepsání protokolu** s uvedením veškerých identifikátorů a uvedení časového snímku + celá anabáze jednání.

Místo spáchání trestného činu - internetový prostor je dynamické prostředí, které se neustále mění. V případě kybernetických hrozeb je velmi nutné vědět, kde se oznamovaná věc stala či kde se projevil následek protiprávního jednání. Nejčastěji to znamená, že **oznamovatel by měl co nepřesněji určit místo na Internetu, kde se s útokem setkal**.

Nezapomenout v ETŘ (evidence trestního řízení) věc označit:
Sledovaná událost – IT kriminalita.



POSTUP PŘIJETÍ OZNÁMENÍ

3. Jak zajistit důkazy

U důkazních materiálů je velmi důležité jejich **včasné pořízení**.

Provedení **okamžité zálohy zájmových dat, případně převzetí takovýchto dat ze strany oznamovatele** (může je předložit) – sepsání ÚZ o zajištění, či zajištění dle trestního řádu (§ 78).

Na služebně nemusí být k dispozici všechny odpovídající programy a jejich různé verze. S vyhodnocením elektronických stop je proto vhodné **obracet se na specializovaná pracoviště kybernetické kriminality**.

Bude-li se jednat o specifické jednání pachatele a s tím užitý nástroje internetu a informačních technologií, které si vyžaduje jiný přístup a postup, je na místě okamžitá **konzultace u pracovníků kybernetické kriminality**.

Vydalo Centrum prevence rizikové virtuální komunikace
Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s Policií ČR. © 2019
Tento materiál vznikl v rámci projektu Oběť kybernetické kriminality s podporou
Ministerstva vnitra a Olomouckého kraje.
www.e-bezpeci.cz



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



Univerzita Palackého
v Olomouci

