vedecká konferencia s medzinárodnou účasťou

AKTUÁLNE VÝZVY PREVENCIE POČÍTAČOVEJ KRIMINALITY

(spojená s praktickými ukážkami)

konaná pod záštitou rektorky ***Dr. h. c. doc. JUDr. Lucie KURILOVSKEJ, PhD.***

a s finančnou podporou ***Rady vlády SR pre prevenciu kriminality***
ako súčasť projektu prevencie počítačovej kriminality „Buď bezpečný!“

TERMÍN KONANIA: **21. 3. 2018**

MIESTO KONANIA: **aula Akadémie PZ v Bratislave, Sklabinská 1**

CIELE A TEMATICKÉ ZAMERANIE KONFERENCIE

Konferencia bola organizovaná ako súčasť projektu „Buď bezpečný!“, ktorý je prioritne zameraný na prevenciu páchania počítačovej kriminality. Preto hlavným cieľom konferencie bolo vymedzenie a analyzovanie základných problémov týkajúcich sa počítačovej kriminality, vytvorenie predpokladu pre systematický prístup k oblasti prevencie počítačovej kriminality zo strany zúčastnených subjektov nielen na národnej ale aj medzinárodnej úrovni, prepojenie teórie s aplikačnou praxou prostredníctvom workshopu zameraného na zvýšenie úrovne kybernetickej bezpečnosti.

V zmysle vytýčených cieľov a obsahového zamerania vedeckej konferencie boli jednotlivé prezentované príspevky koncentrované najmä na nasledovné okruhy:

- vedecké základy vzťahu ľudského faktora a kybernetickej kriminality,
- teoretické východiská riešenia prevencie kybernetickej kriminality,
- východiská skvalitňovania spolupráce Akadémie PZ v Bratislave s ostatnými vysokými škola doma i zahraničí, ako aj s inými inštitúciami v oblasti kybernetickej bezpečnosti s jej dopadom na systém odborného vzdelávania nielen študentov ale aj zamestnancov štátnej a verejnej správy.

PROGRAM KONFERENCIE

08.00 – 08.30 – **prezentácia účastníkov**

08.30 – 08.45 – **otvorenie konferencie, úvodné slovo**
Dr. h. c. doc. JUDr. Lucia Kurilovská, PhD., rektorka A PZ v Bratislave
Ing. Jozef Halcin, riaditeľ odboru prevencie kriminality MV SR

08.45 – 09.10 – **Projekt „Buď bezpečný!“ a jeho realizácia v praxi**
JUDr. Miroslav Brvnišťan, PhD., BMSEC s.r.o. Bratislava

09.10 – 09.25 – **Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky**
JUDr. Veronika Marková, PhD., vedúca KTP A PZ v Bratislave

09.25 – 09.45 – **Počítačová kriminalita z pohľadu policajnej praxe**
Mgr. Stanislav Španko, riaditeľ odboru počítačovej kriminality UKP PPZ

09.45 – 10.05 – **Rola polície pri boji s kriminalitou v kybernetickom prostredí – pohľad nezávislej odbornej spoločnosti na možnosti vyšetrovania a dokumentovania kybernetickej kriminality**
Corpus Solution, a.s. Praha

10.05 – 10.25 – **Riziká a nevýhody sociálnych sietí**
Michal Dragan, odborník na sociálne siete

10.25 – 10.40 – **prestávka, občerstvenie**

10.40 – 11.00 – **Zákon o kybernetickej bezpečnosti**
Mgr. Rastislav Janota, zástupca riaditeľa SK-CERT a predseda výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR

11.00 – 11.20 – **Budovanie proaktívneho bezpečnostného dohľadu na úrovni štátnej inštitúcie**
Fidelis Cybersecurity s.r.o. Praha

11.20 – 11.40 – **Digitálna identita v kontexte počítačovej kriminality**
Ing. Marek Laššák, vedúci oddelenia analýzy dát OPSKA KEÚ PZ P PZ MV SR

11.40 – 11.50 – **Možnosti stanovenia výšky škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov**
doc. JUDr. Peter Polák, PhD., Mgr. Bc. Tomáš Trúsik, ProtoWay s.r.o., Fakulta práva Paneurópskej vysokej školy n.o.

11.50 – 12.00 – **Etický hacking v organizácii v zmysle smernice o kybernetickej bezpečnosti**
PhDr. Peter Veselý, PhD. MBA, Mgr. Vincent Karovič, PhD., Fakulta manažmentu Univerzity Komenského v Bratislave

12.00 – 12.30 – **diskusia a prijaté závery**

12.30 – 13.30 – **obed**

13.30 – 15.00 – **workshop zameraný na praktické ukážky**
„Najlepší pomocník experta Security Operations Center alebo ako spoľahlivo detekovať, efektívne vyšetrovať a účinne eliminovať množstvo bezpečnostných incidentov."
Cieľ workshopu: Na konkrétnych praktických ukážkach predstaviť unikátne nástroje určené na detekciu a prevenciu pred sofistikovanými kybernetickými útokmi, ktoré vďaka svojim jedinečným vlastnostiam umožňujú veľmi hlbokú okamžitú aj retrospektívnu analýzu na sieti i koncových bodoch. Vysoká miera automatizácie detekčných, vyšetrovacích a remediačných postupov prináša významnú úsporu času i zefektívnenie činností vyšetrovateľov bezpečnostných incidentov. Názornú časť prezentácie bude tvoriť praktická živá ukážka stopovania útočníka a vyšetrenie incidentu.

V rámci jednotlivých bodov programu konferencie išlo najmä o riešenie nasledovných otázok:

JUDr. Miroslav Brvnišťan, PhD. zo spoločnosti BMSEC ako manažér projektu „Buď bezpečný“ bližšie predstavil účastníkom konferencie uvedený projekt. Vysvetlil jeho ciele, ako aj prínos pre prax. Ide hlavne o vytváranie bezpečnostného povedomia prostredníctvom on-line vzdelávania, interaktívnych kurzov a výučbových aktivít dostupných pre každého. Vyzval prítomných na aktívne sa zapojenie do prieskumu, ktorý je súčasťou projektu. Pozri: www.budbezpecny.sk

JUDr. Veronika Marková, PhD., vedúca KTP A PZ v Bratislave sa vo svojom vystúpení venovala trestno-právnym aspektom počítačovej kriminality. Poukázala na nedostatočné a absentujúce ustanovenia týkajúce sa počítačovej/ kybernetickej kriminality a nutnosť ich doplnenia.

Mgr. Stanislav Španko, riaditeľ odboru počítačovej kriminality ÚKP PPZ venoval svoju pozornosť otázkam počítačovej kriminality v súvislosti s výkonom policajnej praxe, pričom poukázal na najčastejšie trestné činy, s ktorými sa stretávajú príslušníci PZ zaradení na tomto odbore.

Zástupca **spoločnosti Corpus Solutions** prezentoval pohľad nezávislej odbornej spoločnosti na možnosti vyšetrovania a dokumentovania kybernetickej kriminality orgánmi činnými v trestnom konaní s dôrazom na rolu príslušníkov Policajného zboru pri boji s kriminalitou v kybernetickom prostredí.

Iný pohľad na riešenú tému priniesol **Michal Dragan**, ktorý sa venoval sociálnym sieťam a rizikám prinášajúcich ich využívanie. Načrtol otázky krádeží kybernetických identít a zneužívania verejne dostupných dát, ako aj riziká spojené so zverejňovaním informácií o svojom súkromí vo virtuálnom priestore, pričom uviedol aj viaceré praktické príklady. Dôležitým bodom príspevku bolo prezentovanie vlastnej skúsenosti s týmto typom nelegálnej činnosti s dôrazom na pripomenutie skutočnosti, že útočníkovi stačí pár informácií, pretože ľudia si neuvedomujú riziká sociálnych sietí.

Mgr. Rastislav Janota, zástupca riaditeľa SK-CERT a predseda výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR účastníkom konferencie priblížil tvorbu a obsah Zákona o kybernetickej bezpečnosti, ktorého účinnosť je 1. 4. 2018.

Téme budovania proaktívneho bezpečnostného dohľadu na úrovni štátnej inštitúcie sa venoval zástupca **spoločnost Fidelis Cybersecurity** Jan Rydval, ktorý v nadväznosti na túto prednášku realizoval workshop .

Vystúpenie **Ing. Mareka Laššáka**, vedúceho oddelenia analýzy dát OPSKA KEÚ PZ P PZ MV SR zaujalo účastníkov tým, že mali možnosť viac sa dozvedieť o digitálnej identite v kontexte počítačovej kriminality.

Rokovanie konferencie svojim vystúpením obohatil **Mgr. Bc. Tomáš Trúsik** zo spoločnosti. ProtoWay, ktorý svoju pozornosť venoval problematike stanovenia výšky škody

spôsobenej neoprávnenými zásahmi do počítačových systémov a programov. Prínosom jeho príspevku bolo prezentovanie vlastného návrhu vzorca výpočtu škôd, ktorý doteraz v praxi absentuje.

PhDr. Peter Veselý, PhD. MBA vo svojom vystúpení dotvoril tému prevencie počítačovej kriminality prostredníctvom etického hackingu.

Praktický príklad testovania organizácie prostredníctvom phishingu ponúkol **Ing. Henrich Slezák.** Na tomto základe je možné overiť neopatrné až nezodpovedné správanie sa užívateľov v prostredí internetu, a tým následne upozorniť testovaných na nebezpečenstvo otvárania neoverených e-mailov a webových adries.

V poobedňajších hodinách sa uskutočnil workshop vedený odborníkmi zo spoločnosti Fidelis Cybersecurity, počas ktorého došlo k interaktívnej komunikácii s publikom a k praktickým ukážkam systému Security Operations Center na detekovanie, efektívne vyšetrovanie a eliminovanie bezpečnostných incidentov.

ZHODNOTENIE

Možno konštatovať, že vytýčené ciele vedeckej konferencie sa podarilo naplniť aj vzhľadom na rozličnosť prístupov venujúcich sa tejto problematike. Za prínos treba považovať skutočnosť, že bola prezentovaná tak z hľadiska trestnoprávneho, ako aj špecificky policajno-odborného, kriminalisticko-expertízneho, ale aj vyslovene technického, resp. technologického. Bolo zaujímavé sa na jednej strane pozrieť na predmetnú oblasť z týchto odlišných uhlov pohľadu, a na strane druhej dospieť k záveru, že aj napriek tomu sa väčšina účastníkov vedeckej konferencie zhodla na nutnosti legislatívnej úpravy, keďže v súčasnej dobe takáto úprava nie je komplexná. Následkom toho vzniká vysoká miera latencie, neochota občanov nahlasovať takúto formu kriminality (najmä z dôvodu nízkeho povedomia o spôsoboch oznamovania - komu a ako je potrebné takéto konanie oznámiť), čím vzhľadom na narastajúci počet používateľov počítačov v akejkoľvek forme narastá aj motivácia páchateľov dopúšťať sa kybernetickej kriminality. Konferencia priniesla mnohé zaujímavé pohľady na možnosti ochrany pred takýmito nelegálnym konaním, či už za pomoci využitia špeciálnych systémov, etického hackingu alebo testovania a školenia zamestnancov dotknutých organizácií. Vedecká konferencia tým priniesla mnoho nových a zaujímavých poznatkov uplatniteľných v praxi.