Konference o kyberbezpečnosti na JU představila reálné incidenty, jejich řešení i možnosti ochrany

16.10.2025 - | Jihočeská univerzita v Českých Budějovicích

Říjen je evropským měsícem kybernetické bezpečnosti. Národní úřad pro kybernetickou a informační bezpečnost pravidelně pořádá "Festival bezpečného internetu", který nabízí sérii akcí realizovaných s cílem šíření osvěty o bezpečnosti v online prostoru. Na Přírodovědecké fakultě Jihočeské univerzity v Českých Budějovicích se uskutečnila dvoudenní konference ve spolupráci s organizací CZ.NIC. Akce byla určena především studentům a veřejnosti a jejím cílem bylo představit široké spektrum témat z oblasti kybernetické bezpečnosti – od reálných incidentů a jejich následků a poučení přes technologická řešení a ukázky digitální ochrany. Úvodní slovo pronesl prorektor pro vědu a výzkum Jihočeské univerzity, pan doc. Ing. Luděk Berec, Dr., který zdůraznil důležitost vzdělávání v oblasti bezpečnosti v digitálním prostoru.

Jedním z úvodních bloků byla analýza bezpečnostního incidentu, který se odehrál v roce 2024 ve finských Helsinkách. Matias Mesiä ze společnosti Traficom detailně rozebral průběh útoku, jeho dopady na infrastrukturu a následná opatření, která byla přijata. Poukázáno bylo i na aktuální trend zneužívaných zranitelností s porovnáním Finska s Českou republikou, kde hodnoty a trendy byly téměř totožné.

Další část programu se věnovala různým typům kybernetických incidentů, jejich řešení a poučením z praxe. Účastníci se seznámili s příklady útoků, způsoby reakce na incidenty a postupy, které vedou k efektivnímu zvládnutí krizových situací. Diskutovalo se i o tom, jak organizace analyzují incidenty, jaké nástroje využívají a jak se z nich poučit pro budoucnost.

Blok věnovaný organizaci CZ.NIC se zaměřil na několik témat. Jako první vystoupila Věra Mikušová, která studenty seznámila s fungováním CSIRT týmů v České republice, Evropské unii i ve světě, jejich rolí při řešení incidentů a způsoby mezinárodní spolupráce. Následně Oto Stefan představil fungování registru domén v České republice, systém FRED a principy správy DNS. Účastníci se dozvěděli, jak systém FRED funguje, kdo ho ve světě využívá a jak je technologicky zajištěn. Nakonec Jaromír Talíř předvedl téma bezpečných digitálních identit, které lze využít pro ochranu v kyberprostoru. Představeny byly jak jednotlivé světově využívané technologie a standardy, tak i vývoj řešení v ČR a budoucí plány EU v této oblasti.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) představil také několik témat. Jako první přiblížil Jakub Maděránek průběh útoku – od phishingu přes kompromitaci až po vyjednávání s ransomware skupinami. Ukázal, jak se z těchto skupin stávají téměř „firmy“, které řeší nejen technické aspekty útoků, ale i „spokojenost zákazníka“ – tedy obětí. Dále Jakub Onderka představil blok o postkvantové kryptografii, který nabídl pohled do aktuální problematiky standardů dnešních šifer a nastupujících postkvantových algoritmů, které mnozí z nás již využívají, aniž bychom si to uvědomovali. Na závěr dne představila Lenka Ondrysková webový portál NÚKIB a jeho postupnou transformaci v průběhu let, včetně sběru zpětné vazby od uživatelů a jejího využití pro další vývoj.

Druhý den konference zahájila čtveřice zaměstnanců společnosti ČEZ a. s. Účastníkům bylo představeno fungování jejich Integračního centra bezpečnosti (iSOC), které kombinuje klasický

bezpečnostní operační dohled (SOC) s prvky fyzické bezpečnosti, které zahrnují docházkové systémy pro kritické i běžné sekce budov ČEZ, technická a organizační opatření, nebo i systémy poplachů, čidla a další prvky fyzické ochrany. Všechny tyto informace zaměstnanci iSOC řeší v systému C4 Enterprise, který slouží jako centrální platforma pro řízení bezpečnostních procesů a integraci různých technologií v rámci bezpečnostního ekosystému ČEZ.

Další blok byl věnován Pavlu Gistingerovi z Policie ČR, konkrétně z NCTEKK. Ten představil postupy, jak policie odhaluje internetové podvodníky. Zaměřil se na případy, kdy útočníci cílí na méně technicky nebo finančně gramotné jedince prostřednictvím podvodných inzerátů a reklam, často s tématem investic. Účastníci tak získali přehled o tom, jak probíhá vyšetřování těchto případů, jak se provádějí zásahy proti mezinárodním podvodníkům a jaké techniky NCTEKK využívá.

Účastníci se dále seznámili s průběhem ransomware útoku, způsobem komunikace s útočníky a tím, jak se po takovém útoku mění fungování celé firmy. Přednášející sdílel zkušenosti z praxe, které ukazují, jak zásadní dopad může mít kybernetický útok na vnitřní procesy, firemní kulturu i bezpečnostní politiku organizace. Během přednášky zaznělo motto, kterým by se měla řídit každá firma v oblasti kybernetické bezpečnosti: ***„Neptejte se zda, ale kdy.“***

Závěrečný blok druhého dne patřil odborníkům z CESNET, kteří představili řadu svých služeb a open-source nástrojů. Pavel Kácha nejprve přiblížil historii vývoje sběru síťového provozu a bezpečnostních dat na CESNET a aktuálně používané technologie jako MENTAT, FTAS, NERD, PassiveDNS, WARDEN a mnohé další. Martin Šebela následně představil službu Phishingator, včetně ukázek cvičných phishingových kampaní, rozesílání podvodných e-mailů a výsledků testování. Cílem služby Phishingator je poučit uživatele, že phishing může přijít v libovolné podobě – což si někteří na JU již prakticky vyzkoušeli. Jakub Judiny poté ukázal, jak CESNET snižuje množství reportů a tím i zátěž na incident handlery pomocí agregace, třídění, tresholdingu a filtrace událostí ve službě MENTAT, kterou využívá i Jihočeská univerzita. Jaroslav Svoboda účastníkům představil metody skenování serverů a webů pomocí služeb SNER a AUROR, včetně využití TARANIS-NG od slovenského CERT týmu. Veškerá data z těchto služeb následně putují do systému WARDEN, ze kterého MENTAT vytváří přehledné reporty. Na závěr Pavel Kácha ukázal, jak CESNET využívá a poskytuje ostatním honeypot službu HUGO pro detekci anomálií a útočníků v počítačové síti.

https://www.jcu.cz/cz/univerzita/aktualne/konference-o-kyberbezpecnosti-na-ju-predstavila-realne-incidenty-jejich-reseni-i-moznosti-ochrany