Kybernetická bezpečnost

Jiří Sedláček

Dne 21. 7. 2020 uspořádal SOVAK ČR ve spolupráci s Network Security Monitoring Cluster (NSMC) seminář Kybernetická bezpečnost – jak optimálně nastavit procesy a technická opatření, aby se minimalizovalo riziko škody při kybernetickém útoku.

NSMC se zaměřuje na osvětu v oblasti informační a kybernetické bezpečnosti a zvyšování povědomí o problémech a řešeních bezpečnostních aspektů počítačových sítí. Na semináři vystoupili zástupci tohoto uskupení Ing. Jiří Sedláček, Jiří Knápek, Ing. Robert Schindler, MSc., a Ing. Lukáš Přibyl.

Velice často se při mých osvětových/evangelizačních přednáškách o informační a kybernetické bezpečnosti stává, že jsem tázán, ať už v rámci následné diskuse, či ve foyer, jestli se tato problematika týká opravdu každého, bez ohledu na jeho profesi. K překvapení či nelibosti mnohých tazatelů ale musím konstatovat, že tato problematika se týká každého, a to jak v profesním, tak i soukromém životě. Důležité je se s tímto faktem vyrovnat a naučit se čelit novým hrozbám, vycházejícím z kybernetického prostoru. Náš reálný svět – ten hmotný kolem nás – se s tím kybernetickým totiž velice intenzivně prolíná. Víte například, že organizace v České republice čelí cca 530 kybernetickým útokům týdně?

V dnešní dynamické době jsme stále častěji konfrontováni s pojmy IoT, IoS, IoP, průmysl 4.0, chytré domy, chytrá města, cloudové služby, eGovernment, ale také kyberválka, kyberzločin, kyberšikana, kyberšpionáž, kybersabotáž, atd. Závislost dnešní společnosti na elektronických technologiích je stále vyšší a vyšší, stejně tak jako rizika z toho plynoucí. Stále častěji je zmiňována otázka tzv. kontinuity činnosti organizace (Business Continuity), která je v úzké vazbě a provázanosti s ICT. V případě narušení funkce informační infrastruktury, informačních technologií, řídicích systémů, průmyslových technologií, mohou být následky pro danou organizaci takového rozsahu, že řádově převyšují náklady na implementaci informační bezpečnosti. Pokud naše společnost nezmění přístup k této problematice, budou finanční ztráty narůstat. Základem pro změnu myšlení není nic jednoduššího než vzdělávání. Změna přístupů a chování, která spadá pod bezpečnost lidských zdrojů, je naprosto klíčová. A to od řídících struktur organizací až po řadové zaměstnance.

Pro nikoho z vás není zvláštní chránit se před povodněmi, před zloději, před ztrátou napájení, před kapsáři na ulici. Jelikož je ale kybernetický prostor těžko uchopitelným, hrozby z něj plynoucí mají mnozí z nás často tendenci zlehčovat, či zcela ignorovat. To nemluvím o velice rozšířeném pocitu absolutního bezpečí kdekoli a kdykoli mimo naše domácnosti. Až moc jsme si totiž zvykli mnohé delegovat na stát, včetně odpovědnosti za naši osobní bezpečnost, prevenci v této oblasti nevyjímaje. Ale vraťme se ke kybernetickému prostoru. Následky neoprávněné manipulace s osobními údaji (krásně zpracováno např. ve filmu The Net z roku 1995) mohou být fatálními ve vašem osobním životě. Následky/dopady například díky ransomware útoku na vaši organizaci stejně tak. Události v nemocnici Benešov, v OKD, ve FN Brno ukazují, jak jsme na informačních technologiích závislí. Zároveň nám bylo nastaveno zrcadlo. Ukázalo se, jak je otázka informační a kybernetické bezpečnosti podceňována a nedostatečně řešena a jaké fatální dopady z toho plynou. Kde jsou péče a odpovědnost řádného hospodáře?

Dne 1. 1. 2015 vešel v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále ZoKB), ve znění pozdějších předpisů. To je v naší legislativě významným milníkem, díky němuž se začal měnit přístup ke kybernetické bezpečnosti nejen z pohledu organizačních a technických opatření, ale i v právní rovině (povinné subjekty mají zákonnou povinnost řešit kybernetickou bezpečnost) a v oblasti vzdělávání a osvěty.

Každá organizace sestává ze tří pilířů. Jsou jimi lidé, procesy, technologie. Posluchače semináře jsme uvedli do problematiky kybernetické bezpečnosti a vysvětlili jsme jim význam lidského faktoru, který má podíl na cca 60 % kybernetických bezpečnostních incidentů. V rámci prezentace zaznělo, že důležitá je prezenční forma školení a že nedílnou součástí vzdělávání je i trénink. Byl prezentován kybernetický polygon Masarykovy univerzity v Brně, KYPO. Informační a kybernetická bezpečnost se implementuje zaváděním organizačních a technických opatření. Posluchače jsme seznámili s bezpečnostními politikami, analýzou rizik a analýzou aktiv. Pokud chci něco chránit, musím si nejdříve ujasnit, s jakými typy informací pracuji, co má pro mě jakou hodnotu, co jakou mírou souvisí s předmětem činnosti mé organizace a jaká musím zavádět opatření, abych zajistil nejen adekvátní ochranu, ale taktéž zajistil adekvátní a přiměřené finanční zdroje. Po zavedení organizačních opatření se implementují opatření technická.

Na semináři dále bylo představeno kybernetické dohledové centrum SOC (Security Operations Centera) a také se posluchači seznámili s posouzením kybernetické bezpečnosti podle doporučení NÚKIB.

Ing. Jiří Sedláček
Network Security Monitoring Cluster