Název předmětu: Kybernetická bezpečnost

Téma: 1. Úvod do kybernetické bezpečnosti - základní pojetí

Cíl: Cílem je seznámit studenty se základním pojetím významu kybernetické bezpečnosti. Student se naučí rozlišovat obsah základních definic z oblasti kybernetické bezpečnosti a kybernetické obrany. Bude znát základní pravidla při zavádění kybernetické bezpečnosti v organizaci.

Úkoly pro samostatnou práci: naučit se a zopakovat si základní pojmy z oblasti kybernetické bezpečnosti, zopakovat si pravidla při zavádění kybernetické bezpečnosti v organizaci.

Studijní literatura:

1. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
2. HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav; PTÁČEK, Bohumil; SKORUŠA, Leopold; SLOŽIL, Richard. *Kybernetická bezpečnost: teorie a praxe.* Praha: Powerprint s.r.o., 2015, 250 s. ISBN 978-80-87994-72-6.
3. HRŮZA, Petr; PITAŠ, Jaromír; ŠANDA, Jaroslav; BRECHTA, Bohumil. *Kybernetická bezpečnost II.* Brno: Univerzita obrany, Brno, 2013, 100 s. ISBN 978-80-7231-931-2.
4. HRŮZA, Petr. *Kybernetická bezpečnost.* Brno: Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5.
5. Vydané normy ISO/ČSN řady 27000, platné zákony a vyhlášky z oblasti kybernetické bezpečnosti

Obsah:

Kybernetická bezpečnost je pro většinu lidí něco neuchopitelného. Pro manažery organizací je to jedna z nejtěžších úloh. Vědí, že jsou za ni odpovědní, ale nejsou si jisti, jak jí spolehlivě dosáhnout.

Kybernetická bezpečnost je doposud vnímána jako něco, co je ve výlučné kompetenci ICT oddělení. Vrcholový management se o tuto oblast často detailně nezajímá a iniciativu očekává od vedoucích ICT pracovníků. Tento přístup je ale v dnešní době naprosto nedostatečný a vede k situacím, kdy je oblast kybernetické bezpečnosti podceňována a systematicky neřešená.

Management organizací by měl pochopit a akceptovat, že řízení kybernetické bezpečnosti spadá mnohem více k dalším oblastem bezpečnosti a krizového managementu. Vždyť i dnešní sofistikované útoky jsou často multidisciplinární a kombinují v sobě oblasti ICT, sociálního inženýrství, personální a objektové bezpečnosti. Právě pro eliminaci takových hrozeb jsou kompetence ICT manažerů nedostatečné.

V praxi se také často setkáváme s tím, že vedení ICT, stejně jako celá společnost, je orientované a motivované na poskytování maximálního výkonu. Jejich úlohou je především zajištění fungování ICT infrastruktury a zvyšování efektivity procesů. Požadavky na kybernetickou ochranu organizace jsou přitom často v přímém rozporu s těmito požadavky, a navíc požadují zdroje a investice, jejichž uplatnění by vedení ICT radši vidělo v provozu.

Dne 1. ledna 2015 vstoupil v účinnost zákon o kybernetické bezpečnosti. Jedná se o vůbec první zákon ČR, který tuto sféru bezpečnosti řeší. Pro většinu lidí je však samotný pojem kybernetická bezpečnost poněkud mlhavý.

Definice základních pojmů

Zásadní součástí zákona je definice jednotlivých pojmů z oblasti kybernetické bezpečnosti, které lze jen obtížně pochopit intuitivně. Pro přesnost definice ponecháváme v plném znění.

- ***kybernetický prostor*** – digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací
- ***kybernetická bezpečnost*** - souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru
- ***kybernetický bezpečnostní incident*** - kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací
- ***stav kybernetického nebezpečí*** – stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací, a tím dojde nebo by mohlo dojít k porušení nebo ohrožení zájmu České republiky

Kybernetická bezpečnost (Cyber Security)

Kybernetická bezpečnost (Cyber Security) je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Termínem Bezpečnost informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením nebo kolapsem neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánované události. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

ICT oddělení tak pouze realizuje standardy a požadavky stanovené nezávislým bezpečnostním odborem. V opačném případě hrozí, že v organizaci převládne provozní aspekt (jenž je hlavní náplní IT oddělení) a bezpečnostní aspekty budou potlačeny.

Po etablování kompetentního a nezávislého bezpečnostního manažera je nezbytné vyhodnotit současný stav organizace a provést návrh vrcholových bezpečnostních směrnic, které stanoví

základní zodpovědnosti v organizaci (Bezpečnostní výbor). Následovat by měla analýza rizik, která zhodnotí všechna aktiva a podpůrná aktiva z hlediska důvěrnosti, dostupnosti a integrity. Výsledkem je přehled o všech rizicích, jejich dopadech a jednoznačné stanovení kompetencí za jednotlivá aktiva.

Vhodným doplněním z hlediska kybernetické ochrany je rovněž provedení testů zranitelnosti stávající technické infrastruktury, které může být vhodně doplněno rovněž testem odolnosti organizace vůči sociálnímu inženýrství (způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace). Následující analýza nápravných opatření stanoví přiměřená opatření pro eliminaci zjištěných rizik, dle jejich závažnosti a možných dopadů. Výsledkem je aktualizace bezpečnostní dokumentace a stanovení plánu realizace nápravných opatření, tedy realizace dílčích projektů, realizace nápravných opatření technické, personální nebo procesní povahy.

Ve fázi realizace nápravných opatření dojde k realizaci jednotlivých procesů a technologií, kdy bezpečnostní manažer je interním zadavatelem pro ICT oddělení, případně jiná oddělení, která se podílejí na realizaci těchto opatření. Po provedení realizace nápravných opatření je nutné provést audit stavu kybernetické bezpečnosti, který ověří jejich účinnost, provede aktualizaci rizikové analýzy. Vedle celkového auditu je vhodné periodicky provádět testy zranitelnosti infrastruktury, a to jak vnější (ochrana perimetru), tak i v interní síti.

Zavádění kybernetické bezpečnosti

Zavádění kybernetické bezpečnosti by mělo být v souladu s celkovou bezpečnostní politikou organizace. Jako klíčové se jeví zakotvení silného postavení nástrojů bezpečnosti v organizaci. Základním aktem je ustanovení bezpečnostního manažera do první linie řízení organice, kdy přímo podléhá generálnímu řediteli. Jeho cílem je stanovení bezpečnostní politiky organizace, ideálně v podobě systému řízení bezpečnosti (ISMS – ISO27000) a jeho následné zavedení v organizaci.

Zavádění kybernetické bezpečnosti je nutné provádět v návaznosti na další oblasti bezpečnosti (zejména objektová bezpečnost a personální politika). V opačném případě je organizace velmi náchylná na rizika spojená např. se sociálním inženýrstvím. Velmi vhodné je rovněž zorganizovat školení kybernetické bezpečnosti, které přinese jednotlivým typům pracovních pozic pochopení problematiky kybernetické ochrany a návod bezpečného chování v prostředí internetu a informačních systémů.

Kybernetické hrozby jsou již reálné. Nejčastější důvody vedoucí management organizací k rozhodnutí o zavádění či vylepšování kybernetické ochrany organizace:

- *Ekonomický* – mezi nejvýznamnější rizika patří zastavení produkce a z toho přímo vzniklé ztráty z hlediska ušlé fakturace nebo odškodnění klientům.
- *Kybernetická kriminalita* – organizace se může stát snadno obětí kriminálních činů, jako je vydírání či zcizení dat o klientech konkurencí nebo nespokojeným zaměstnancem.

- *Průmyslová špionáž* – pro organizace je v dnešní době extrémně důležité dokázat si udržet svoje know-how, strategické záměry, obchodní nabídky, výsledky interního výzkumu a vývoje.

- *Ztráta kredibility* – podvržení internetových stránek organizace, zastavení výroby nebo zneužití dat klientů mohou mít velmi negativní dopad na spokojenost stávajících zákazníků nebo odrazení nových.

- *Legislativní důvody* – vedle stávající legislativy (ZoKB – Zákon o kybernetické bezpečnosti 181/2014 sb.), která vymezuje především prvky kritické infrastruktury, je to i postupné zavádění evropské legislativy, která stanovuje odpovědnosti i na další veřejné a soukromé subjekty.

Standardy kybernetické bezpečnosti

Standardy kybernetické bezpečnosti byly vytvořeny relativně nedávno, neboť teprve v posledních letech přibývá citlivých informací uložených v počítačích, které jsou připojeny k Internetu. Také mnoho úkolů, které byly původně zpracovávány v papírové podobě, jsou nyní prováděny na počítačích. Proto se zvyšuje potřeba pro informační věrohodnost a bezpečnost. Důležitým aspektem kybernetické bezpečnosti je ochrana před krádeží identity. Instituce a firmy mají zvýšenou potřebu k zajištění informační (počítačové) bezpečnosti, neboť potřebují chránit své obchodní tajemství, důvěrné informace a osobní údaje o jejich partnerech, zákaznících anebo zaměstnancích. Vláda má rovněž potřebu chránit své informace. Jedním z nejpoužívanější bezpečnostních standardů je ISO / IEC 27002.

Kybernetická bezpečnost v ČR

Vláda České republiky dne 15. března 2010 schválila usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a ustanovila Ministerstvo vnitra České republiky gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

Dne 24. května 2010 Vláda České republiky přijala usnesení č. 380, kterým zřídila Meziresortní koordinační radu pro oblast kybernetické bezpečnosti.

Dne 9. prosince 2010 podepsalo Ministerstvo vnitra České republiky se sdružením CZ.NIC Memorandum, kterým byl zřízen Národní CSIRT.

Dne 20. července 2011 Vláda České republika přijala usnesení č. 564 jímž mimo jiné schválila Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015.

Dne 19. října 2011 Vláda České republiky přijala usnesení č. 781 jímž ustavila Národní bezpečnostní úřad gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

Dne 13. května 2014 Národní bezpečnostní úřad (NBÚ ČR) za účasti premiéra České republiky a ředitele NBÚ ČR otevřel v Brně Národní centrum kybernetické bezpečnosti (Vládní CERT).

Dne 13. srpna 2014 prezident České republiky podepsal zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákon o kybernetické bezpečnosti je účinný od 1. ledna 2015.

Dne 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se novelizoval zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB) vznikl **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB).