

Sylabus VYT-4 – MS

Základní téma předmětu: Počítačová bezpečnost v prostředí decizní sféry

Bližší tematické dělení:

1. Úvod do problematiky bezpečnosti
 2. Největší rizika a ohrožení ICT/IS v organizaci
 3. Zabezpečení a ochrana ICT/IS
 4. Shrnutí
-

Časové rozdělení lekcí

2 jednotky, tzn. 90 min. Cca 60 min přednáška k probíranému tématu. Následná diskuze, praktické ukázky, dotazy. Předpokládají se 4 lekce.

Rozpis abstraktů pro jednotlivé lekce

1. Úvod do problematiky bezpečnosti

Bezpečnost IT v organizaci z pohledu manažera. Proč se zabývat bezpečností, co to bezpečnost je. Bezpečnost z perspektivy administrace, dodavatelů infrastruktury. Bezpečnost infrastruktury vs. bezpečnost dat v infrastruktuře. Bezpečnost jako faktor spolehlivosti a faktor funkce organizace.

2. největší ohrožení

Definice rizika. Klasifikace rizik podle původce, podle možných dopadů na funkci organizace, podle závažnosti. Ohrožení IT necílené (šíření škodlivých kódů) vs. cílené (útoky). Úloha uživatele v zabezpečení IT a rizika vyplývající z činnosti uživatele. Úloha správce a manažera – rizika spojená s managementem. Typy útoků na data a úniků dat. Typy selhání s důsledky na bezpečnost infrastruktury. Viry, červy, malware. Hackerské útoky a hackeři – hacking jako profesionální činnost. Identifikace rizik a útoků. Proaktivní ochrana.

3. Zabezpečení a ochrana ICT/IS

Základní kroky k zabezpečení infrastruktury prováděné v organizacích. Nastavování pravomocí, ochrana před škodlivými kódy, ochrana před útoky. Identifikace rizik. Identifikace průniků do infrastruktury (IDS). Ochrana dat, šifrování, vymezení rolí. Antivirové systémy (serverové a klientské), firewally. Bezpečnost využitím nestandardních systémů a bezpečnost v nestandardních systémech. Bezpečnost serverů, stanic, systémových prvků.

Ochrana dat na mobilních a přenosných zařízeních. Zálohování, archivace, zajištění před neoprávněným únikem. Spojení s infrastrukturou pomocí VPN, problematika práce v neznámých sítích a rizika s ní spojená. Uživatelská hygiena, předběžná opatrnost.

Úloha managementu v zajištění ochrany informačních systémů a dat. Kontrola administrace, určování priorit, ověřování výsledků činnosti administrace. Úloha školení uživatelů a personálu, rizika spojená s personálem. Bezpečnost, jako organická funkce infrastruktury.

4. Shrnutí

Shrnutí a zopakování informací z předchozích lekcí. Akcentace faktu, že za zabezpečení dat nemůže být odpovědná technika, ale vždy správci a uživatelé. Diskuze.

Základní zdroje

www.ictsecurity.cz Online magazín o bezpečnosti

www.securityworld.cz Časopis o bezpečnosti

www.secunia.com Server o bezpečnosti aplikací