BEZ – BI-WSI-SI-01

Informační bezpečnost, architektura bezpečnosti v modelu OSI.

Obsah

1 Komponenty informační bezpečnosti

Komponenty lze rozdělit takto:

1. Informační technologie (IT): Technologie na zpracování informací.
2. Informační a komunikační technologie (ICT): technologie zahrnující jak počítačové systémy tak také telekomunikační sítě pro zpracovaní informací.

Kvůli zpracovaní a přenosu informací je potřeba řešit bezpečnost IT a ICT systémů. Bezpečnost dělíme na 2 úrovně:

1. Počítačová bezpečnost (computer security) Představuje souhrn prostředků zabezpečující bezpečný provoz počítačů a ochranu dat zpracovaných a uchovávaných na počítači.
2. Síťová bezpečnost (network security) Představuje souhrn prostředků zabezpečující ochranu dat po dobu jeich přenosu komunikačním prostředím a ochranu počítačů projených do počítačové sítě.

Hranice mezi tímto dělením ovšem není jednoznačná, například počítačové viry míří na počítačové systémy, ale mohou narušit celou počítačovou síť.

2 Informační bezpečnost

Definice: Souhrn prostředků a postupů na zabezpečení důvěrnosti, integrity a dostupnosti informací.

Tyto prostředky mají za učel definovat postupy pro ochranu uživatelských dat, také řízení uživatelského přistupu, tak aby pouze ověření uživatelé měli přístup k datům a to pouze k datům, kte kterým mají mít přístup.

- Důvěrnost (confidentiality) Vlastnost, která zaručuje ochranu dat před neautorizovaným přístupem.
- Integrita (integrity) Zaručuje ucelenost a nepoškozenost informace.
- Dostupnost (availability) Dostupnost zaručuje přístup k informacím pro autorizované subjekty.

U informačního systému (IS) je potřeba myslet vždy na systém jako na celek a celá jeho bezpečnost je stejně dobrá jako jeho nejslabší článek.

2.1 Užitková hodnota (asset)

Každý informační systém se skládá z užitkovž hodnot, což je vše co představuje určitou hodnotu pro organizaci, firmu nebo kterýkoliv ekonomický subjekt.

Tyto hodnoty dělíme do tří kategorií:

1. Hmotné užitkové hodnoty (physical assets): Jedná se hlavně o technické prostředky jako například počítače a další hardware, ale také budovy.
2. Nehmotné užitkové hodnoty (nonphysical assets): Software, informace (data) a možnost poskytování informací a služeb.
3. Lidské zdroje (human resources): Personál s přítupem k informacím či správci IS.

Užitkové hodnoty jsou vystavené různým hrozbám (threats), které představují potenciální narušení bezpečnosti IS a možnému úniku dat, jejich ztráty či poškození.

Hrozby můžeme taky rozdělit na dva typy a to úmyslná, která jsou prováděna za účelem získání dat nebo jejich poškození. Poté je zde neúmyslná hrozba, která pramení z možnosti že uživatel udělá chybu, například nesprávným zacházením s IS. Hrozby také mohou být přírodního charakteru. U charakteristiky hrozeb musíme nahlížet na:

- zdroj
- motivaci
- možnou početnost výskytů
- jejich pravděpodobnost
- a následné dopady

Hrozby z hlediska IS:

- Softwarová hrozba Jedná se hlavně o počítačové malware, které se zaměřují na napedení komunikace mezi jednotlivými částmi IS. Do systému se mohou dostat skrze paměťová média nebo přes síť, do které je daná komponenta připojená.
- Hrozba neautorizovaným subjektem (útočníkem) Potencionální možnost pro neověřeného uživatele dostat se do našeho systému za použití jiných nástrojů než již zmíněného malwaru.

Hrozby je tedy třeba ohodnit a na základě nich definovat jednotlivé zranitelnosti (vulnerability), které ukazují na slabá místa v IS a na základě, kterých můžeme určit jejich dopady a také možná opatření jak jim předejít. Zranitelnost můžeme stejně jako hrozbu ohodnotit (například: nízká, střední a vysoká). Samotná zranitelnost nezpůsobuje žádné škody pouze vytváří pro ně vytváří podmínky.

Při neočekávané či nežádoucí situaci mluvíme o incidentu infomační bezpečnosti. V návaznosti na incidenty můžeme mluvit o jejich dopadu (impact). Dopad může být but přímý (ztráta data či integrity IS) nebo nepřímý (finanční ztráty, ztráta konkurence schopnosti). Posouzení dopadu je pak založeno na poměru mezi cenou za ztrátu či narušené bezpečnosti a nástrojům, které zajistí, aby se situace neopakovala.

3 Rizika

Definice: Představuje potencionální možnost vzniku ztráty nebo poškození dat v IS tím, že bude využito zranitelnosti části IS. Riziko je dále charakterizováno jeho pravděpodobností vzniku incidentu a poté jeho dopadem. Jakákoliv změna v rámci assetů a bezpečnostních částí IS může ovlivnit rizika.

Rizika nelze nikdy úplně eliminovat, ovšem aplikací bezpečnostních prvků lze tyto rizika snížit na akceptovatelnou úroveň. Riziku, které je zde po aplikaci prvků nazýváme reziduální/zbytkové riziko.

- Analýza rizik (risk analysis) Systematický proces odhadu velikosti rizika.
- Posouzení rizika (risk assessment) Proces identifikace a analýzy rizika.
- Management rizika (risk management) Proces identifikace, řízení, eliminace a minimalizace rizika.

Pro limitování ohrožení, snížení zranitelnosti a omezení dopadů incidentu informační bezpečnosti definujeme mechanizmy bezpečnosti (safeguards). Jedná se procedury a procesy, kterých je možné využít i několik, jako například prevence a detekce útoků, obnova a další. Tyto mechanizmy mají ovšem také svá omezení (constraints), limitující a omezující účinnost mechanizmů (organizační, technická, personální a další).

4 Architektura informační bezpečnosti v modelu OSI

Model OSI (Open System Interconnection) je vázaný na doporučení od ITU-T a označuje se jako standard X.800.