11. Bezpečnost IT

Autentizace

- Proces ověřování identity uživatele, aby se zjistilo, zda má oprávnění k přístupu ke zdrojům.
- Může být prováděna pomocí jména a hesla, certifikátů, biometrických údajů atd.

Softwarová zranitelnost a vhodná opatření

- Zranitelnosti v softwaru mohou umožnit útoku hackerů na počítačovou síť nebo na samotný počítač.
- Je nutné vhodně opatření jako aktualizace softwaru, použití bezpečnostního softwaru atd.
- Je taky dobré rozdělit síť na více části, a tak omezit velikost útoku
- Další dobré opatření je zálohovat data, kdyby při útoku došlo ke ztrátě dat

Zero day Attack

- Využití zranitelnosti softwaru, která ještě není obecně známá a neexistuje pro ni zatím žádná obrana (Např. žádná aktualizace která chybu řeší.)
- K útoku využívá takzvaný exploit což je využití programátorské chyby, která způsobuje zranitelnost

Antivirová ochrana

- Antivirový program (zkráceně antivir) je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se používají dvě odlišné techniky:
    - Prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi
    - Detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.
- Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Aktuální virové databáze se dnes nejčastěji stahují z internetu.

Zabezpečení komunikace

Šifrování

- Šifrování dat je proces, kterým se nezabezpečená elektronická data převádí za pomoci kryptografie na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče.
- Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou.

VPN (Virtual Private Network)

- Je to technologie, která umožňuje uživateli připojit se k síti pomocí internetu tak, že se vytváří šifrovaný tunel mezi uživatelem a vzdáleným serverem.
- To poskytuje uživateli bezpečnější přístup ke síťovým zdrojům a umožňuje mu skrýt svou online aktivitu před náhodnými pozorovateli.
- Používá se hlavně když jsme připojeni na veřejných sítí

TLS (Transport Layer Security)

- Předchůdce SSL
- Protokol(y) TLS umožňují aplikacím komunikovat po síti způsobem, který zabraňuje odposlouchávání či falšování zpráv.
- Pomocí kryptografie poskytuje TLS svým koncovým bodům autentizaci a soukromí při komunikaci Internetem.

Zabezpečení lokální bezdrátové sítě

- Je nutné je zabezpečit silným heslem třeba domácí wifi router.
- Kdyby se jednalo o velmi jednoduché heslo tak pomocí bruteforce attacku se útočník do sítě dostane hned
- Využití WPA, který využívá šifrovací klíč
- Aktualizovat firmware zařízeních který nám poskytují bezdrátovou síť
- Můžeme síť ještě lépe zabezpečit třeba whitelistem nebo blokovat zařízení pomocí blacklistu
- Bezpečnost také můžeme zlepšit nainstalování bezpečnostního softwaru na jednotlivé zařízení které se k síti připojují

Funkce a zabezpečení perimetru sítě

Firewall

- Bezpečnostní software nebo hardware, který monitoruje a kontroluje příchozí a odchozí síťový provoz.
- Brána firewall pomáhá zabránit hackerům a škodlivému softwaru (například červům) v získání přístupu k počítači prostřednictvím sítě nebo internetu. Brána firewall může rovněž zabránit tomu, aby počítač odesílal škodlivý software do jiných počítačů.
- Funguje jako bariéra mezi veřejnou sítí a lokálním počítačem nebo sítí, a slouží k ochraně proti nežádoucímu nebo škodlivému provozu.
- Firewall může filtrovat provoz na základě IP adresy, protokolu, portu a dalších kritérií.

Proxy

- Proxy server, který slouží jako prostředník mezi klientem (jako je váš počítač nebo mobilní zařízení) a vzdáleným serverem, například webovým serverem.
- Když se připojíte k internetu prostřednictvím proxy serveru, všechny vaše požadavky na přístup k webovým stránkám, obrázkům a dalším online obsahu se vysílají přes proxy server, namísto přímého připojení k webovému serveru.
- Proxy servery se často používají k:
    - Ochraně soukromí: proxy server může maskovat vaši IP adresu, takže webové stránky a jiné online služby nemohou identifikovat váš počítač.
    - Filtrování obsahu: některé organizace používají proxy servery k filtrování nežádoucího nebo nevhodného obsahu, jako jsou pornografické stránky, sociální sítě a další.
    - Zrychlení přístupu: proxy server může ukládat vyrovnávací paměť kopie webových stránek a dalšího obsahu, takže při opakovaném použití je může zobrazit rychleji, aniž by se musel stahovat znovu.
    - Zkrátka, proxy server představuje vrstvu mezi vaším počítačem a internetem, která může sloužit k ochraně soukromí, filtrování obsahu a zrychlení přístupu k internetu.

IDS – Intrusion Detection System

- je bezpečnostní technologie, která slouží k detekci nežádoucích aktivit v síti.
- IDS kontroluje provoz síti aby detekoval podezřelou aktivitu.
- Pokud je detekována podezřelá aktivita, IDS může generovat varování, blokovat nežádoucí aktivity nebo zaznamenat údaje o aktivitách pro další analýzu.
- Tyto informace mohou být použity k identifikaci a řešení bezpečnostních problémů v síti a k posílení celkového zabezpečení.

DMZ (Demilitarizovaná zóna):

- DMZ je oddělená část sítě.
- Tyto sítě jsou nastaveny tak, aby bylo možné bezpečně hostovat veřejně přístupné služby, jako je například webový server, bez ohrožení zabezpečení vnitřní sítě.

Systém řízení bezpečnosti informace

ISMS (Information Security Management System)

- Je dokumentovaný systém, který řídí a spravuje bezpečnost informací.
- Cílem ISMS je identifikovat, analyzovat a řešit rizika bezpečnosti informací a zajistit, aby byly informace chráněny proti neoprávněnému přístupu, zneužití, ztrátě nebo poškození.
- ISMS vychází ze standardů ISO 27001 a je vytvořen tak, aby vyhovoval specifickým potřebám daného podniku nebo organizace.
- ISMS zahrnuje řadu opatření jako školení zaměstnanců, zavedení zásad zabezpečení, používání firewalle, pravidel pro hesla a dalších opatření, které zajišťují bezpečnost informací.