

MATURITNÍ OPAKOVACÍ TÉMATA: Informační technologie 18-20-M/01**KYBERNETICKÁ BEZPEČNOST****Komponenty osobního počítače a jejich role v kybernetické bezpečnosti**

- komponenty podílející se na kyberbezpečnosti, vysvětlíte jejich význam
- BIOS, EFI/UEFI, TPM, Secure Boot ad.

Právní rámec kybernetické bezpečnosti v ČR

- ZoKB + prováděcí předpisy, trestní zákoník, směrnice a nařízení EU,
- instituce a organizace v ČR řídící a zajišťující kybernetickou bezpečnost v ČR, CERT, CSIRT

Autentizace a autorizace, problematika hesel, jako základ kybernetické bezpečnosti

- pravidla pro tvorbu, používání a ukládání hesel
- autentizace, autorizace, 2FA, MFA

Zajištění kontinuity provozu informačních systémů a jejich obnova po výpadku provozu

- zálohování a obnova dat
- DRP, BCP, zajištění SLA

Kybernetická bezpečnost webových a komunikačních aplikací

- základní principy zabezpečení webových a komunikačních aplikací
- průběh a principy Vámi vybraného útoku na webovou či komunikační aplikaci
- uveďte základní principy obrany proti Vámi vybranému typu útoku

Kybernetická bezpečnost digitální identity

- principy fungování digitální identity
- různé druhy a typy digitální identity
- význam a využití digitální identity
- legislativní normy upravující používání digitální identity

Souborové systémy a jejich význam při zajišťování kybernetické a informační bezpečnosti

- přehled používaných souborových systémů a jejich možnosti a vlastnosti pro zajištění kybernetické a informační bezpečnosti
- spolehlivost, žurnálování, ACL, šifrování ad.

Jádro operačního systému a jeho vliv na spolehlivost a bezpečnost celého systému

- typy jader a jejich vlastnosti
- jednotlivé moduly jádra a jejich funkce
- Secure Boot

- srovnajte jádra Windows a Linux
- IPC a její význam pro bezpečnost operačního systému a aplikací

Kryptografie a její využití při zajištění informační a kybernetické bezpečnosti dat na paměťových médiích

- symetrická a asymetrická kryptografie
- význam a vliv jednotlivých souborových systémů
- FAT, NTFS, ad.
- šifrování paměťových médií – Bitlocker, LUKS, VeraCrypt ad.

Kryptografie a její využití při zajištění informační a kybernetické bezpečnosti v počítačových a komunikačních sítích

- symetrická a asymetrická kryptografie
- TL
- HTTPS, šifrování komunikace na koncových zařízeních
- VPN

Kryptografie a její využití při zajištění digitální autentizace

- symetrická a asymetrická kryptografie
- digitální podpis
- certifikáty
- certifikační autority

Bezpečnost v datových a komunikačních sítích – útočné modely

- CIA, PAM
- RECON, STRIDE, Kill Chain
- význam jednotlivých modelů
- indikátory kompromitace
- jednotlivé fáze útočných modelů

Bezpečnost v datových a komunikačních sítích – síťové hrozby

- Network Threats na jednotlivých síťových vrstvách
- indikátory kompromitace jednotlivých hrozeb a útoků
- obrana a mitigace

Bezpečnost v datových a komunikačních sítích – aktivní síťové prvky

- jak je možné využít aktivní síťové prvky ke zvýšení bezpečnosti a odolnosti datové sítě
- bezpečnostní funkce aktivních síťových prvků – switch, router
- typy portů na switchi
- segmentace sítě, VLAN
- DHCP Snooping, DAI

Bitlocker

- použité šifrování
- šifrovací klíče
- využití TPM
- klíče pro obnovu a jejich uložení
- srovnání s jinými nástroji (VeraCrypt apod.)

TPM čip a jeho význam pro kybernetickou bezpečnost

- umístění
- využití
- struktura
- konfigurace PC
- význam pro bezpečnost

Vícefaktorová autentizace

- autentizace a autorizace; rozdíl mezi jednofaktorovou, dvoufaktorovou (2FA) a vícefaktorovou autentizací
- autentizační faktory a jejich nezávislost
- používané metody – SMS kódy, jednorázová hesla HOTP/TOTP, autentizační aplikace, push potvrzení, hardwarové tokeny a bezpečnostní klíče FIDO2
- biometrie a passkeys
- bezpečnost, omezení a odolnost
- nasazení v organizaci – ochrana administrátorských účtů, vzdálený přístup, použitelnost pro uživatele.

Bezpečnostní konfigurace PC s operačním systémem Windows

- základní principy zabezpečení – PoLP, RBAC omezení dostupných služeb a více vrstev ochrany
- Windows Update a ochrana proti škodlivému software, Firewall
- uživatelské, správcovské a systémové účty, sudo, sudoers, root
- zabezpečení spouštění a hardwaru – UEFI, Secure Boot, TPM a ochrana před neoprávněným spuštěním z externích médií
- souborové systémy, LUKS
- audit a sledování událostí – protokoly událostí, audit přihlášení a změn oprávnění, rozpoznání podezřelých aktivit
- zálohování a obnova – pravidelné oddělené zálohy, ověřování obnovy dat a postup při bezpečnostním incidentu.

Bezpečnostní konfigurace PC s operačním systémem Linux

- základní principy zabezpečení – PoLP, RBAC omezení dostupných služeb a více vrstev ochrany
- aktualizace systému a aplikací, důvěryhodné instalační zdroje, ochrana proti škodlivému software
- uživatelské, správcovské a systémové účty a oprávnění, UAC
- zabezpečení přihlašování – hesla, Windows Hello
- zabezpečení spouštění a hardwaru – UEFI, Secure Boot, TPM a ochrana před neoprávněným spuštěním z externích médií
- audit a sledování událostí – protokoly událostí, audit přihlášení a změn oprávnění, rozpoznání podezřelých aktivit, journalctl

Elektronická pošta

- asynchronní komunikace, princip store-and-forward, e-mailová adresa a doména
- architektura e-mailového systému – klienta a server: MUA, MSA, MTA, MDA
- cesta zprávy od odesílatele k příjemci – odeslání, předávání mezi servery, doručení a načtení ze schránky
- DNS a elektronická pošta – MX záznamy, dohledání adres poštovních serverů a význam reverzního DNS
- struktura e-mailové zprávy – hlavička, tělo, Message-ID a rozdíl mezi SMTP obálkou a obsahem zprávy, adresování a příjemci – obálkový odesílatel a příjemce, pole From, To, Cc, Bcc a Reply-To
- MIME – textové a HTML zprávy, znakové sady, přílohy a vícedílné zprávy
- protokol SMTP – navázání spojení, základní příkazy a odpovědi, odesílání klientem versus přenos mezi servery.
- přístup ke schránce – principy a porovnání POP3, IMAP a JMAP; webmail
- zabezpečení přenosu a přístupu – TLS, STARTTLS, implicitní TLS, autentizace uživatele a používané porty, DKIM a DMARC, jejich spolupráce a omezení

Bezpečnostní konfigurace serverů

- hardening, PoLP, minimalizace útočné plochy a více vrstev ochrany
- role serveru a analýza rizik – poskytované služby, chráněná data, dostupnost a důsledky kompromitace, bezpečná instalace a aktualizace – důvěryhodné instalační zdroje, minimální instalace, bezpečnostní opravy a plánování restartů
- účty a administrátorská oprávnění – oddělené správcovské účty, servisní účty, MFA a pravidelné kontroly oprávnění, vzdálená správa, SSH, RDP
- síťové zabezpečení – firewall, povolené porty, segmentace sítě, DMZ a oddělení provozní a správcovské komunikace
- zabezpečení služeb a aplikací – odstranění nepotřebných služeb, bezpečné konfigurace, omezení oprávnění a izolace procesů
- ochrana OS – bezpečnostní zásady Windows Server, SELinux či AppArmor v Linuxu a řízení spouštění aplikací
- logování, audit a monitoring – centrální sběr protokolů, synchronizace času, sledování změn a upozornění na podezřelé události
- kontrola konfigurace a zranitelností – bezpečnostní standardy, skenování, kontrola změn a pravidelné přezkoumání nastavení.

Access Control Lists

- účel a princip ACL, ACE, druhy ACL
- vyhodnocování pravidel – pořadí položek, shoda s pravidlem, výchozí chování a rozdíly mezi jednotlivými implementacemi
- souborové ACL ve Windows a v Linuxu
- síťové ACL – filtrování podle IP adres, protokolů a portů, příchozí a odchozí pravidla, volba rozhraní, dopad na provoz
- audit a diagnostika – ověřování efektivního přístupu, počítadla shod, logování a hledání příčin zamítnutí

Kybernetická bezpečnost bezdrátových sítí

- specifika bezdrátové komunikace – sdílené přenosové médium, dosah signálu mimo budovu a možnost odposlechu
- základní prvky architektury Wi-Fi, průběh připojení k síti
- zabezpečení Wi-Fi – vývoj WEP, WPA, WPA2 a WPA3; slabiny starších mechanismů, silná hesla, omezení WPS, aktualizace firmwaru a zabezpečení správy AP či radiče
- autentizace a šifrování – PSK, SAE, AES-CCMP a GCMP, režimy Personal a Enterprise, IEEE 802.1X, EAP a autentizační server RADIUS
- certifikáty a ověřování sítě – EAP-TLS, ověřování certifikátu serveru a rizika připojení k podvrženému přístupovému bodu
- typické útoky – odposlech, hádání hesel, rogue AP, evil twin, podvržené captive portály a útoky na dostupnost.
- segmentace a řízení přístupu – oddělení zaměstnanců, hostů a IoT zařízení; VLAN, firewall a izolace klientů, veřejné a otevřené Wi-Fi – rizika, význam HTTPS a VPN, možnosti OWE; captive portál jako prostředek řízení přístupu.
- zabezpečení klientských zařízení – aktualizace, automatické připojování, uložené profily a omezení sdílení.
- základní bezpečnostní rizika Bluetooth, NFC a bezdrátových sítí IoT.

Šifrování blokových zařízení – LUKS

- základní pojmy a architektura – blokové zařízení, oddíl, šifrovaný svazek, LUKS, dm-crypt a nástroj cryptsetup
- vrstvy úložiště – vztah fyzického zařízení, šifrování, LVM a souborového systému, možné pořadí těchto vrstev
- formát LUKS1 a LUKS2, hlavička, metadata a šifrovaná datová oblas.
- šifrování sektorů, AES-XTS, hierarchie klíčů, klíče svazku, uživatelské heslo, odvozený klíč a odemčení klíče svazku
- vytvoření a používání svazku – inicializace LUKS, otevření mapování, vytvoření souborového systému, připojení a bezpečné uzavření.
- integrace do systému – /etc/crypttab, /etc/fstab, initramfs a odemykání při startu.
- rozsah šifrování, zálohování hlavičky

Mobilní síť GSM

- princip buňkové sítě, rádiové rozhraní, frekvenční pásma, MIMO, Beam Forming
- architektura sítě – BTS, BSC, síťové subsystémy, MSC/GMSC, HLR, VLR, AuC, EIR.
- SIM, IMSI, TMSI, MSISDN a IMEI
- autentizace a zabezpečení
- sestavení a ukončení hovoru, mobilita, roaming, handover
- SMS a doplňkové služby, datové přenosy
- bezpečnostní slabiny GSM