STŘEDNÍ PRŮMYSLOVÁ ŠKOLA A VYŠŠÍ ODBORNÁ ŠKOLA, PÍSEK, KARLA ČAPKA 402

Maturitní témata 2025/2026

Kybernetická bezpečnost informačních systémů. Pracovní podklady pro ústní maturitní odpověď přibližně na 15 minut ke každému tématu.

Jak s podklady pracovat

Odpovědi kombinují počítačové sítě, aplikační software, informační systémy a kybernetickou bezpečnost. U síťových témat se vyplatí kreslit vrstvy, rámec, paket nebo jednoduchou topologii. U bezpečnosti je dobré vždy říct: hrozba, zranitelnost, dopad, protiopatření a příklad z praxe.

Text je záměrně stavěný jako mluvená osnova. Neuč se jednotlivé věty nazpaměť; nauč se pořadí pojmů, vztahy mezi nimi a ke každému tématu si připrav jeden praktický příklad.

Doporučené časování odpovědi

- **1 minuta:** vymezení tématu a základní pojmy.
- **4 minuty:** členění, model nebo schéma.
- **6 minut:** principy, protokoly, metody nebo procesy.
- **3 minuty:** bezpečnostní dopady, příklady a srovnání.
- **1 minuta:** shrnutí a návaznost na praxi.

Obsah

6. Přepínače, LAN architektura a redundance
7. Ethernet, rámce a MAC adresa
8. IPv4 adresy a subnetting
9. ARP, DHCP, NAT a PAT
10. IPv4, IPv6, IGMP a ICMP
11. Směrovače a směrovací protokoly
12. TCP, UDP, porty a TCP spojení
13. VLAN, VTP a směrování mezi VLAN
14. Aplikační protokoly
15. Zabezpečení sítí, ACL, firewally a DMZ
16. IS: zavádění a testování
17. Rozhodovací techniky a analýzy
18. Biometrie a bezpečnostní politika
19. Základy kyberbezpečnosti
20. Elektronické dokumenty a podpis
21. Licence SW a právo
22. Cloud a outsourcing
23. Kryptografie, šifrování a kódování
24. Hesla, bezpečnost a rizika
25. ITIL, COBIT, CSF a SLA
26. Základní pojmy IS
27. Životní cyklus IS a projektu
28. Metriky a projektový management
29. Práce s informacemi a mediální gramotnost
30. Business Intelligence

---

1. Historie sítí, rozdělení sítí, referenční model ISO/OSI

historie LAN WAN ISO/OSI vrstvy

Osnova odpovědi

1. Vysvětli, proč počítačové sítě vznikly: sdílení dat, tiskáren, výkonu a komunikace.
2. Stručně projdi vývoj od sálových počítačů, ARPANETu, Ethernetu a TCP/IP až po internet a mobilní sítě.
3. Rozděl sítě podle rozsahu: PAN, LAN, MAN, WAN, internet.
4. Rozděl sítě podle vlastnictví a účelu: privátní, veřejné, podnikové, školní, průmyslové.
5. Popiš referenční model ISO/OSI a smysl vrstvení.
6. Ke každé vrstvě uveď typické úlohy, zařízení nebo protokol.

Výkladové body

Síť je soustava zařízení, která si vyměňují data podle dohodnutých pravidel. Historicky šlo nejdříve o terminály připojené k centrálním počítačům, později o lokální sítě v budovách a nakonec o globální internet. Důležitý byl ARPANET, vznik TCP/IP, rozšíření Ethernetu a později webu.

Model ISO/OSI rozděluje komunikaci do sedmi vrstev: fyzická, linková, síťová, transportní, relační, prezentační a aplikační. Vrstvení pomáhá návrhu, výuce i diagnostice, protože každá vrstva řeší svůj úkol a používá služby vrstvy pod sebou.

Vrstvy OSI

- **1 fyzická:** signál, kabely, konektory, rádiový přenos.
- **2 linková:** rámce, MAC adresy, Ethernet, WiFi.
- **3 síťová:** IP adresy a směrování.
- **4 transportní:** TCP, UDP, porty.
- **5 až 7:** relace, formát dat, aplikace a služby.

> Dobrá věta: model OSI není přesný popis internetu, ale výborný referenční model pro pochopení, kde vzniká problém.

2. Logické a fyzické topologie sítí, přístupové metody, metalické kabely, útlum, ztráta a přeslech signálu

topologie UTP STP CSMA signál

Osnova odpovědi

1. Rozliš fyzickou a logickou topologii.
2. Popiš sběrnici, hvězdu, kruh, strom, mesh a hybridní topologie.
3. Vysvětli přístupové metody ke sdílenému médiu.
4. Popiš koaxiální kabel, UTP, ScTP a STP.
5. Uveď funkční dělení kabeláže: horizontální rozvody, páteřní rozvody, patch kabely.
6. Vysvětli zakončení, kategorie kabelů, útlum, ztrátu a přeslech.

Výkladové body

Fyzická topologie popisuje skutečné propojení kabely nebo rádiovým dosahem. Logická topologie popisuje, jak data sítí skutečně proudí. Moderní Ethernet je fyzicky často hvězda přes switch, ale provoz je řízen přepínáním podle MAC adres.

Metalické kabely přenášejí elektrický signál. UTP je nestíněná kroucená dvojlinka, STP je stíněná, ScTP má společné stínění. Kroucení párů snižuje rušení a přeslech. Kabely se zakončují konektory, typicky RJ-45 podle zapojení T568A nebo T568B.

Signál a kabeláž

- **Útlum:** zeslabení signálu se vzdáleností.
- **Ztráta:** obecně pokles kvality nebo energie signálu.
- **Přeslech:** rušení mezi páry ve stejném nebo sousedním kabelu.
- **Kategorie:** Cat5e, Cat6, Cat6A a vyšší určují podporované parametry.
- **Maximální délka:** běžný měděný Ethernet má typicky 100 m pro jeden segment.

> Nepopleť fyzickou hvězdu se sdíleným médiem starého hubu. Hub šíří provoz všem, switch provoz přepíná cíleně.

3. Model TCP/IP, podobnosti a odlišnosti ISO/OSI a TCP/IP, implementace vrstev, zařízení a protokoly, zapouzdření dat

TCP/IP encapsulation protokoly vrstvy

Osnova odpovědi

1. Definuj TCP/IP jako praktickou sadu protokolů internetu.
2. Porovnej čtyřvrstvý TCP/IP model se sedmivrstvým OSI modelem.
3. Popiš aplikační, transportní, internetovou a síťově přístupovou vrstvu.
4. Uveď protokoly a zařízení na jednotlivých vrstvách.
5. Vysvětli zapouzdření dat a názvy PDU: data, segment, paket, rámec, bity.
6. Uveď příklad průchodu požadavku HTTP sítí.

Výkladové body

TCP/IP model je bližší skutečné implementaci internetu než ISO/OSI. Aplikační vrstva zahrnuje funkce aplikační, prezentační i relační vrstvy OSI. Transportní vrstva řeší komunikaci mezi procesy pomocí portů. Internetová vrstva používá IP adresy a směrování. Vrstva síťového přístupu řeší konkrétní médium, například Ethernet nebo WiFi.

Zapouzdření znamená, že každá vrstva přidá k datům svou hlavičku, případně patičku. Aplikační data se vloží do TCP segmentu nebo UDP datagramu, ten do IP paketu, ten do ethernetového rámce a nakonec se převede na signál.

Příklady vrstev

- **Aplikace:** HTTP, DNS, SMTP, SSH.
- **Transport:** TCP, UDP, porty.
- **Internet:** IPv4, IPv6, ICMP, router.
- **Síťový přístup:** Ethernet, WiFi, switch, síťová karta.

> Při diagnostice postupuj podle vrstev: kabel a linka, IP adresa a routa, port a služba, aplikace.

4. Optická přenosová média v LAN, optická vlákna a kabely, zdroje a detektory, numerická apertura, útlum

optika SM MM LED laser útlum

Osnova odpovědi

1. Vysvětli, proč se v sítích používá optické vlákno.
2. Popiš konstrukci vlákna: jádro, plášť, ochranné vrstvy.
3. Rozliš single-mode a multi-mode vlákna.
4. Vysvětli princip přenosu světla úplným odrazem.
5. Popiš zdroje a detektory: LED, laserová dioda, fotodioda.
6. Vysvětli numerickou aperturu a typy útlumu.

Výkladové body

Optické vlákno přenáší data pomocí světla, proto je odolné proti elektromagnetickému rušení, umožňuje velké vzdálenosti a vysoké rychlosti. Single-mode vlákno má malé jádro a používá se pro delší vzdálenosti. Multi-mode má větší jádro a používá se často v budovách a datových centrech.

Světlo se ve vlákně šíří díky rozdílnému indexu lomu jádra a pláště. Numerická apertura vyjadřuje schopnost vlákna přijímat světlo pod určitým úhlem. Čím vhodněji je světlo navázáno do vlákna, tím menší jsou ztráty.

Útlum a praxe

- **Absorpční útlum:** část energie se pohltí v materiálu.
- **Rozptyl:** světlo se rozptyluje na nehomogenitách.
- **Ohybový útlum:** příliš ostrý ohyb vlákna zvyšuje ztráty.
- **Konektory:** LC, SC, ST; důležitá je čistota a přesné zakončení.
- **Moduly:** SFP/SFP+ umožňují vložit vhodný optický transceiver do switche.

5. Bezdrátové sítě, bezdrátový přenos dat, WiFi, CSMA/CA, Bluetooth, IR spoje, komponenty bezdrátových sítí

WiFi CSMA/CA Bluetooth radio

Osnova odpovědi

1. Definuj bezdrátovou síť a její výhody i omezení.
2. Popiš rádiový přenos, frekvenční pásma a rušení.
3. Vysvětli standardy WiFi z rodiny IEEE 802.11.
4. Popiš CSMA/CA a rozdíl proti CSMA/CD.
5. Uveď Bluetooth a infračervené spoje.
6. Popiš komponenty: AP, klient, antény, řadič, repeater, bridge.

Výkladové body

Bezdrátová síť používá k přenosu elektromagnetické vlny. U WiFi se běžně používají pásma 2,4 GHz, 5 GHz a 6 GHz. Výhodou je mobilita a snadné připojení, nevýhodou sdílené médium, rušení, menší stabilita a nutnost dobře řešit zabezpečení.

CSMA/CA znamená carrier sense multiple access with collision avoidance. Zařízení se snaží zabránit kolizím tím, že naslouchá médiu, čeká náhodnou dobu a používá potvrzování rámců. U bezdrátové sítě nelze kolize detekovat tak jednoduše jako u starého sdíleného Ethernetu.

Bezpečnost a provoz

- Aktuálně preferuj WPA2 nebo WPA3, silné heslo a oddělenou hostovskou síť.
- SSID je název sítě; BSSID je MAC adresa konkrétního AP.
- Kanály se nesmí zbytečně překrývat, jinak roste rušení.
- Bluetooth je vhodný pro krátké vzdálenosti a periferie.
- IR spoj vyžaduje přímou viditelnost a dnes se používá spíše okrajově.

6. Přepínače, architektura LAN, segmentace a mikrosegmentace, kolizní a broadcast doména, redundance, STP, EtherChannel, VRRP/HSRP

switch STP EtherChannel VRRP

Osnova odpovědi

1. Popiš roli switche v LAN a jeho práci s MAC tabulkou.
2. Vysvětli segmentaci a mikrosegmentaci.
3. Rozliš kolizní a broadcast doménu.
4. Popiš hierarchický návrh LAN: access, distribution, core.
5. Vysvětli redundanci a riziko smyček.
6. Popiš STP, EtherChannel a VRRP/HSRP.

Výkladové body

Switch pracuje hlavně na linkové vrstvě. Učí se zdrojové MAC adresy a ukládá je do tabulky, aby mohl rámce posílat jen na správný port. Každý port switche je samostatná kolizní doména, což je mikrosegmentace. Broadcast doména zůstává společná v rámci VLAN.

Redundance zvyšuje dostupnost, ale v ethernetové síti může vytvořit smyčky. STP blokuje některé redundantní cesty, aby vznikl strom bez smyček. EtherChannel spojuje více fyzických linek do jednoho logického kanálu. VRRP nebo HSRP zajišťuje redundantní výchozí bránu.

Co zdůraznit

- **Kolize:** u moderního plně duplexního switche prakticky nevznikají.
- **Broadcast:** šíří se v rámci VLAN a zatěžuje všechna zařízení v doméně.
- **STP:** chrání před broadcast stormem.
- **EtherChannel:** zvyšuje propustnost i odolnost.
- **VRRP/HSRP:** virtuální IP adresa brány pro koncová zařízení.

7. Ethernet: struktura rámce 802.3 a Ethernet II, MAC adresa, specifikace 802.3, CSMA/CD

Ethernet MAC 802.3 rámec

Osnova odpovědi

1. Definuj Ethernet jako nejrozšířenější technologii LAN.
2. Popiš MAC adresu a její formát.
3. Vysvětli rámec Ethernet II a IEEE 802.3.
4. Uveď pole rámce: preambule, cílová a zdrojová MAC, typ/délka, data, FCS.
5. Uveď příklady specifikací 802.3 podle rychlosti a média.
6. Vysvětli CSMA/CD a proč dnes ztratil význam.

Výkladové body

Ethernet přenáší data v rámcích na linkové vrstvě. MAC adresa je 48bitová fyzická adresa síťového rozhraní, zapisovaná obvykle hexadecimálně. Prvních 24 bitů často označuje výrobce, zbytek identifikuje konkrétní zařízení.

Ethernet II používá pole EtherType, které říká, jaký protokol vyšší vrstvy je v rámci nesen, například IPv4 nebo IPv6. IEEE 802.3 používá pole délky a navazující LLC/SNAP. Kontrolní součet FCS slouží k odhalení chyb v rámci.

Specifikace a CSMA/CD

- 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T pro metaliku.
- 1000BASE-SX/LX a další varianty pro optiku.
- CSMA/CD detekovalo kolize ve sdíleném poloduplexním médiu.
- Moderní switche používají full duplex, takže CSMA/CD se prakticky nepoužívá.

8. IP adresy IPv4: účel, třídy, rezervované adresy, veřejné a soukromé adresy, subnetting, supernetting, VLSM

IPv4 subnetting VLSM CIDR

Osnova odpovědi

1. Vysvětli účel IP adresy na síťové vrstvě.
2. Popiš strukturu IPv4 adresy a masky.
3. Uveď historické třídy A, B, C, D, E.
4. Rozliš veřejné, soukromé a rezervované adresy.
5. Vysvětli subnetting, supernetting a CIDR zápis.
6. Popiš VLSM a proč šetří adresy.

Výkladové body

IPv4 adresa má 32 bitů a zapisuje se čtyřmi desítkovými oktety. Maska určuje, která část adresy je síťová a která hostitelská. CIDR zápis například `/24` znamená, že prvních 24 bitů tvoří síťovou část.

Soukromé rozsahy jsou 10.0.0.0/8, 172.16.0.0/12 a 192.168.0.0/16. Nejsou přímo směrovatelné v internetu a běžně se kombinují s NAT. Subnetting dělí větší síť na menší podsítě. Supernetting spojuje sousední sítě do většího bloku. VLSM používá různé délky masek podle potřeby konkrétních podsítí.

Rezervované adresy

- **127.0.0.0/8:** loopback, typicky 127.0.0.1.
- **169.254.0.0/16:** link-local při selhání DHCP.
- **224.0.0.0/4:** multicast.
- **0.0.0.0:** neurčená adresa nebo default route podle kontextu.
- **255.255.255.255:** lokální broadcast.

> U subnettingu se vyplatí ukázat příklad: síť, maska, počet hostů, adresa sítě, broadcast a rozsah použitelných adres.

9. Protokoly pro správu adres: ARP, RARP, BootP, DHCP, NAT, PAT

ARP DHCP NAT PAT

Osnova odpovědi

1. Vysvětli, proč je potřeba mapovat adresy a přidělovat konfiguraci.
2. Popiš ARP jako překlad IPv4 adresy na MAC adresu.
3. Zmiň RARP jako historický opačný postup.
4. Popiš BootP jako předchůdce DHCP.
5. Vysvětli DHCP proces DORA.
6. Popiš NAT a PAT a jejich použití.

Výkladové body

ARP se používá v IPv4 síti k nalezení MAC adresy zařízení ve stejné lokální síti. Stanice pošle broadcastový ARP request a vlastník IP adresy odpoví ARP reply. Výsledky se ukládají do ARP cache.

DHCP automaticky přiděluje IP adresu, masku, bránu, DNS a další parametry. Proces se často popisuje jako DORA: Discover, Offer, Request, Acknowledge. NAT překládá adresy mezi vnitřní a vnější sítí, PAT navíc rozlišuje spojení podle portů, takže více klientů může sdílet jednu veřejnou adresu.

Bezpečnostní poznámky

- ARP nemá silné ověřování, proto existuje riziko ARP spoofingu.
- DHCP spoofing lze omezit funkcemi jako DHCP snooping na switchi.
- NAT není plnohodnotný firewall, jen mění adresy a často komplikuje přímá příchozí spojení.
- PAT se často označuje jako NAT overload.

10. Protokoly síťové vrstvy: IPv4, IPv6, IGMP, ICMP, ping a tracert

IPv6 ICMP IGMP diagnostika

Osnova odpovědi

1. Začni úlohou síťové vrstvy: adresace a směrování mezi sítěmi.
2. Porovnej IPv4 a IPv6.
3. Popiš základní vlastnosti IPv6 adres.
4. Vysvětli ICMP a jeho diagnostické použití.
5. Vysvětli ping a tracert/traceroute.
6. Popiš IGMP pro správu multicastových skupin v IPv4.

Výkladové body

IPv4 je 32bitový protokol, IPv6 používá 128bitové adresy a vznikl hlavně kvůli vyčerpání IPv4 adres. IPv6 má větší adresní prostor, jednodušší hlavičku, podporu autokonfigurace a místo broadcastu používá multicast a anycast.

ICMP slouží k chybovým a diagnostickým zprávám. Ping posílá ICMP echo request a čeká echo reply. Tracert nebo traceroute zjišťuje cestu k cíli pomocí postupně zvyšované hodnoty TTL nebo hop limit a odpovědí od mezilehlých směrovačů.

Příklady

- **IPv6 loopback:** `::1`.
- **Link-local IPv6:** typicky `fe80::/10`.
- **ICMP:** důležitý i pro fungování IPv6, nejde ho bezmyšlenkovitě zakázat.
- **IGMP:** používá se například u IPTV a multicastového provozu.

11. Směrovače, směrování a směrovací protokoly RIPv1, RIPv2, OSPF, EIGRP

router routing OSPF RIP

Osnova odpovědi

1. Definuj směrovač jako zařízení síťové vrstvy.
2. Vysvětli směrovací tabulku a výběr nejlepší cesty.
3. Rozliš statické a dynamické směrování.
4. Popiš základ RIPv1 a RIPv2.
5. Popiš OSPF jako link-state protokol.
6. Zmiň EIGRP a rozdíl proti otevřeným standardům.

Výkladové body

Router propojuje různé sítě a rozhoduje, kam poslat IP paket. Směrovací tabulka obsahuje cílové sítě, masky, next-hop adresy, rozhraní a metriku. Pokud neexistuje přesnější záznam, používá se default route.

RIP je jednodušší distance-vector protokol, používá počet hopů a má limit 15 hopů. RIPv1 je classful a neposílá masku, RIPv2 je classless a podporuje VLSM. OSPF je link-state protokol, vytváří mapu topologie oblasti a počítá nejkratší cestu. EIGRP je pokročilý protokol známý hlavně z prostředí Cisco.

Porovnání

- **Statická routa:** jednoduchá, předvídatelná, ale ručně spravovaná.
- **RIP:** jednoduchý, pomalejší konvergence, menší sítě.
- **OSPF:** škálovatelnější, oblasti, rychlejší reakce na změny.
- **Metrika:** kritérium pro výběr cesty, například počet hopů nebo cena linky.

12. Protokoly transportní vrstvy: TCP, UDP, port, sliding window, navázání a ukončení TCP spojení

TCP UDP porty 3-way handshake

Osnova odpovědi

1. Vysvětli úlohu transportní vrstvy.
2. Definuj port a socket.
3. Porovnej TCP a UDP.
4. Popiš navázání TCP spojení pomocí SYN, SYN-ACK, ACK.
5. Vysvětli spolehlivost TCP: pořadová čísla, potvrzování, retransmise.
6. Popiš sliding window a ukončení spojení.

Výkladové body

Transportní vrstva rozlišuje aplikace pomocí portů. Port spolu s IP adresou a protokolem tvoří socket. TCP je spojovaný a spolehlivý protokol. UDP je nespojovaný, jednodušší a bez záruky doručení, ale má menší režii a hodí se pro DNS, streaming, hry nebo VoIP.

TCP navazuje spojení třemi kroky: klient pošle SYN, server odpoví SYN-ACK a klient potvrdí ACK. Sliding window umožňuje poslat více dat bez čekání na potvrzení každého segmentu zvlášť a reguluje tok dat podle kapacity příjemce a sítě.

Příklady portů

- HTTP 80, HTTPS 443, SSH 22, DNS 53.
- SMTP 25/587, IMAP 143/993, FTP 20/21.
- Ukončení TCP typicky používá FIN/ACK, případně RST při násilném ukončení.
- Firewall často rozhoduje právě podle IP adres, protokolu a portů.

13. VLAN a VTP, nativní a tagované rámce, směrování mezi VLANy

VLAN 802.1Q trunk inter-VLAN

Osnova odpovědi

1. Vysvětli VLAN jako logické rozdělení sítě na broadcast domény.
2. Popiš access port a trunk port.
3. Vysvětli tagování rámců podle IEEE 802.1Q.
4. Popiš nativní VLAN a rizika jejího špatného nastavení.
5. Vysvětli VTP a jeho účel.
6. Popiš možnosti směrování mezi VLANami.

Výkladové body

VLAN umožňuje oddělit provoz podle oddělení, účelu nebo bezpečnostní úrovně, i když zařízení používají stejnou fyzickou infrastrukturu. Access port patří do jedné VLAN a používá se pro koncová zařízení. Trunk přenáší více VLAN mezi switchi nebo ke směrovači pomocí 802.1Q tagu.

Směrování mezi VLANami je nutné, protože každá VLAN je samostatná síť. Může ho dělat router-on-a-stick, kdy jeden router používá subrozhraní, nebo L3 switch pomocí SVI rozhraní. VTP distribuuje informace o VLANách mezi switchi, ale při špatném použití může způsobit nechtěné změny v celé síti.

Bezpečnost

- Nepoužívej výchozí VLAN 1 pro běžný provoz, pokud tomu lze předejít.
- Nativní VLAN na trunku nastav vědomě a stejně na obou stranách.
- Nepoužité porty vypnout nebo dát do izolované VLAN.
- VTP v menších sítích často raději transparent nebo vypnout podle zařízení.

14. Protokoly aplikační vrstvy: Telnet, SSH, FTP, TFTP, HTTP, SMTP, DNS, HTTPS, NTP

DNS HTTP SSH SMTP

Osnova odpovědi

1. Vysvětli, co řeší aplikační vrstva.
2. Rozděl protokoly podle účelu: správa, přenos souborů, web, pošta, jména, čas.
3. Porovnej Telnet a SSH.
4. Porovnej FTP a TFTP.
5. Vysvětli HTTP a HTTPS.
6. Popiš SMTP, DNS a NTP.

Výkladové body

Aplikační protokoly poskytují konkrétní služby uživatelům nebo aplikacím. Telnet slouží ke vzdálené textové správě, ale přenáší data nešifrovaně, proto se dnes používá SSH. SSH šifruje komunikaci a podporuje bezpečnou správu serverů i přenos souborů.

HTTP přenáší webové stránky a API, HTTPS je HTTP chráněné TLS. DNS překládá doménová jména na IP adresy a další záznamy. SMTP se používá pro odesílání e-mailů. NTP synchronizuje čas, což je důležité pro logy, certifikáty i bezpečnostní analýzu.

Porty a poznámky

- Telnet 23, SSH 22, FTP 20/21, TFTP 69.
- HTTP 80, HTTPS 443, DNS 53, NTP 123.
- FTP používá řídicí a datové spojení; TFTP je jednoduchý přes UDP.
- Nešifrované protokoly jsou rizikové v nedůvěryhodných sítích.

15. Zabezpečení sítí: útoky na datové sítě a strategie obrany, ACL, firewally, demilitarizované zóny

security ACL firewall DMZ

Osnova odpovědi

1. Začni cíli bezpečnosti: důvěrnost, integrita, dostupnost.
2. Uveď typické síťové hrozby: odposlech, spoofing, malware, DoS, špatná konfigurace.
3. Vysvětli princip obrany ve vrstvách.
4. Popiš ACL jako pravidla pro povolení nebo zákaz provozu.
5. Popiš firewall a rozdíl mezi packet filter, stateful a aplikační kontrolou.
6. Vysvětli DMZ a její praktické použití.

Výkladové body

Zabezpečení sítě stojí na prevenci, detekci a reakci. Nestačí jeden prvek; používá se segmentace, aktualizace, silné ověřování, šifrování, monitoring, zálohy a pravidelné testování konfigurace.

ACL filtruje provoz podle adres, protokolů a portů. Firewall je centrálnější bezpečnostní prvek, který může sledovat stav spojení, aplikace, uživatele nebo reputaci cíle. DMZ je oddělená zóna pro servery dostupné z internetu, například web nebo mail gateway, aby nebyly přímo v interní síti.

Strategie obrany

- Princip nejmenších oprávnění.
- Oddělení sítí podle rizika: uživatelé, servery, hosté, správa.
- Logování a alerting pro důležité události.
- Pravidelné zálohy a plán obnovy.
- Školení uživatelů proti sociálnímu inženýrství.

16. IS: zavádění a testování, úrovně řízení, druhy zavádění IS, typy testování SW

IS zavádění testování řízení

Osnova odpovědi

1. Definuj informační systém jako kombinaci lidí, procesů, dat, technologií a pravidel.
2. Rozděl IS podle úrovně řízení: operativní, taktická, strategická.
3. Popiš příklady systémů: TPS, MIS, DSS, EIS/ESS.
4. Vyjmenuj druhy zavádění: přímé, paralelní, pilotní, postupné.
5. Popiš výhody a rizika jednotlivých způsobů zavádění.
6. Vyjmenuj typy testování softwaru.

Výkladové body

Operativní úroveň řeší každodenní transakce, například objednávky, sklad nebo docházku. Taktická úroveň podporuje střední management a plánování. Strategická úroveň pomáhá vrcholovému vedení sledovat trendy, cíle a dlouhodobá rozhodnutí.

Přímé zavedení znamená rychlý přechod na nový systém, ale má vyšší riziko. Paralelní provoz je bezpečnější, protože starý i nový systém běží současně, ale je dražší. Pilotní zavedení testuje systém na menší části organizace. Postupné zavedení nasazuje systém po modulech nebo odděleních.

Testování

- Unit, integrační, systémové a akceptační testy.
- Funkční a nefunkční testy: výkon, bezpečnost, použitelnost, kompatibilita.
- Regresní testy ověřují, že nová změna nerozbila staré funkce.
- UAT testuje, zda systém splňuje potřeby uživatele.
- Penetrační test ověřuje odolnost proti bezpečnostním útokům v dohodnutém rozsahu.

17. Rozhodovací techniky a analýzy: SWOT, SMART, softwarové inženýrství, CSF, problémy IS, marketing 4P

SWOT SMART CSF 4P

Osnova odpovědi

1. Vysvětli, proč se při návrhu IS používají analýzy a rozhodovací techniky.
2. Popiš SWOT analýzu.
3. Popiš SMART cíle.
4. Vysvětli CSF jako kritické faktory úspěchu.
5. Uveď typické problémy IS.
6. Vysvětli marketingový pohled 4P a jeho vazbu na IS.

Výkladové body

SWOT hodnotí silné stránky, slabé stránky, příležitosti a hrozby. Silné a slabé stránky bývají vnitřní, příležitosti a hrozby vnější. SMART pomáhá formulovat cíle tak, aby byly specifické, měřitelné, dosažitelné, relevantní a časově ohraničené.

CSF jsou kritické faktory úspěchu, tedy oblasti, které musí dobře fungovat, aby projekt nebo IS splnil účel. U informačního systému to může být kvalita dat, podpora vedení, školení uživatelů, integrace s okolními systémy nebo bezpečnost.

Příklady

- **Problémy IS:** nejasné požadavky, odpor uživatelů, nekvalitní data, překročení rozpočtu, slabé zabezpečení.
- **4P:** product, price, place, promotion.
- IS může pomoci sledovat prodeje, zákazníky, kampaně, ceny a dostupnost produktu.
- Rozhodovací analýza má skončit konkrétním doporučením, ne jen tabulkou.

18. Biometrie a bezpečnostní politika: pojmy, druhy, hodnocení, využití, analýza rizik

biometrie rizika politika MFA

Osnova odpovědi

1. Definuj biometrickou autentizaci.
2. Rozliš fyziologické a behaviorální biometrické znaky.
3. Popiš proces registrace a ověření biometrie.
4. Vysvětli FAR, FRR a vyvážení přesnosti a použitelnosti.
5. Popiš bezpečnostní politiku organizace.
6. Vysvětli analýzu rizik: aktiva, hrozby, zranitelnosti, dopady, opatření.

Výkladové body

Biometrie ověřuje identitu podle tělesných nebo behaviorálních znaků. Patří sem otisk prstu, obličej, duhovka, hlas, způsob psaní nebo chůze. Výhodou je pohodlí a vazba na osobu, nevýhodou je citlivost biometrických dat: heslo lze změnit, otisk prstu ne.

Bezpečnostní politika definuje pravidla pro ochranu informací, přístupy, hesla, zařízení, incidenty, zálohy, školení a odpovědnosti. Analýza rizik určuje, co je cenné, co tomu hrozí, jaká je pravděpodobnost a dopad a jaká opatření jsou přiměřená.

Hodnocení biometrie

- **FAR:** false acceptance rate, neoprávněný uživatel je přijat.
- **FRR:** false rejection rate, oprávněný uživatel je odmítnut.
- **Liveness detection:** ověření, že jde o živou osobu, ne fotografii nebo kopii.
- Biometrie se často používá jako jeden faktor v MFA, ne jako jediná ochrana.

19. Základy kyberbezpečnosti: terminologie, hrozby, útočníci, útoky, ochrana, kyberkriminalita, social engineering, etika

CIA hrozby social engineering etika

Osnova odpovědi

1. Definuj kyberbezpečnost jako ochranu systémů, sítí, dat a uživatelů.
2. Vysvětli důvěrnost, integritu a dostupnost.
3. Rozliš hrozbu, zranitelnost, riziko, incident a dopad.
4. Uveď typy útočníků: jednotlivec, insider, organizovaná skupina, hacktivista, státní aktér.
5. Popiš běžné útoky na vysoké úrovni: phishing, malware, ransomware, DoS, zneužití slabých hesel.
6. Vysvětli ochranu, kyberkriminalitu a etiku.

Výkladové body

Kyberbezpečnost se netýká jen techniky, ale také lidí a procesů. Slabé heslo, nepozorný uživatel nebo špatný postup může být stejně rizikový jako technická chyba. Social engineering zneužívá psychologii, důvěru, autoritu, strach nebo časový tlak.

Ochrana zahrnuje aktualizace, zálohy, silné ověřování, segmentaci, monitoring, školení, šifrování, řízení přístupů a plán reakce na incident. Etika znamená respektovat zákon, soukromí a dohodnutý rozsah testování. Bez souhlasu se do cizích systémů nezasahuje.

Příklady obrany

- Správce hesel a MFA.
- Pravidelné zálohy ověřené obnovou.
- Princip nejmenších oprávnění.
- Bezpečnostní monitoring a logování.
- Školení proti phishingu a podvodným telefonátům.

20. Elektronické dokumenty, elektronický podpis, certifikáty a certifikační autority, ochrana dat před ztrátou a zneužitím

e-podpis certifikát CA zálohy

Osnova odpovědi

1. Definuj elektronický dokument a jeho vlastnosti.
2. Vysvětli integritu, autenticitu, nepopiratelnost a časové razítko.
3. Popiš elektronický podpis a jeho funkci.
4. Uveď úrovně elektronického podpisu podle běžné praxe: prostý, zaručený, kvalifikovaný.
5. Vysvětli certifikát, veřejný klíč a certifikační autoritu.
6. Popiš ochranu dat před ztrátou a zneužitím.

Výkladové body

Elektronický dokument je digitální obsah, který může být podepsán, šifrován, archivován a přenášen. Elektronický podpis pomáhá ověřit autora a integritu dokumentu. V praxi se používá asymetrická kryptografie: soukromý klíč podepisuje, veřejný klíč ověřuje.

Certifikát váže veřejný klíč na identitu. Certifikační autorita potvrzuje tuto vazbu a vydává certifikáty. Důvěra stojí na řetězci certifikátů, platnosti, revokaci a bezpečné správě soukromého klíče.

Ochrana dat

- **Před ztrátou:** zálohy, redundance, verzování, test obnovy.
- **Před zneužitím:** šifrování, přístupová práva, DLP, audit, školení.
- **3-2-1:** tři kopie, dvě různá média, jedna kopie mimo hlavní místo.
- **Časové razítko:** dokládá, že dokument existoval v určitém čase.

21. Licence SW a právo, Creative Commons, informační etika a právo, autorské právo osobní a majetkové

licence copyright CC etika

Osnova odpovědi

1. Vysvětli, co je softwarová licence.
2. Rozliš proprietární software, freeware, shareware, open source a svobodný software.
3. Uveď příklady licencí: GPL, MIT, Apache, komerční EULA.
4. Popiš licence Creative Commons a jejich značky.
5. Vysvětli rozdíl mezi informační etikou a informačním právem.
6. Popiš osobní a majetková autorská práva.

Výkladové body

Licence určuje, jak lze software používat, kopírovat, upravovat a šířit. Proprietární software má obvykle omezená práva uživatele. Open source licence umožňují přístup ke zdrojovému kódu, ale podmínky se liší. GPL vyžaduje zachování stejné licence u odvozených děl, MIT je velmi permisivní.

Creative Commons se používají hlavně pro obsah, například texty, fotografie nebo výukové materiály. Značky BY, SA, NC a ND určují povinnost uvést autora, zachovat licenci, nepoužívat komerčně nebo neupravovat dílo.

Autorské právo

- **Osobní práva:** autorství a ochrana osobního vztahu k dílu.
- **Majetková práva:** užití díla, rozmnožování, šíření, odměna.
- Etika může být přísnější než zákon: citování, férové užití zdrojů, respekt k soukromí.
- U školní práce je důležité uvádět zdroje a neodevzdávat cizí práci jako vlastní.

22. Cloud a outsourcing: definice, výhody a nevýhody, typy cloudových služeb, využití a zabezpečení

cloud | IaaS PaaS SaaS | outsourcing | SLA

Osnova odpovědi

1. Definuj cloud computing.
2. Uveď výhody: škálovatelnost, dostupnost, platba podle spotřeby, rychlé nasazení.
3. Uveď nevýhody: závislost na dodavateli, připojení, náklady při špatném řízení, compliance.
4. Popiš modely IaaS, PaaS, SaaS.
5. Popiš veřejný, privátní, hybridní a komunitní cloud.
6. Definuj outsourcing a jeho bezpečnostní dopady.

Výkladové body

Cloud poskytuje výpočetní prostředky jako službu přes síť. IaaS poskytuje virtuální servery, sítě a úložiště. PaaS poskytuje platformu pro běh aplikací bez správy celé infrastruktury. SaaS je hotová aplikace dostupná uživateli, například e-mail, CRM nebo kancelářský balík.

Outsourcing znamená předání části činností externímu dodavateli. Může jít o správu serverů, helpdesk, vývoj, bezpečnostní dohled nebo účetnictví. Přináší specializaci a úspory, ale také rizika závislosti, úniku dat a horší kontroly.

Zabezpečení

- Smluvně řešit SLA, odpovědnosti, umístění dat a audit.
- Šifrovat data při přenosu i uložení.
- Používat MFA a řízení identit.
- Rozumět modelu sdílené odpovědnosti mezi zákazníkem a poskytovatelem.
- Plánovat exit strategii při změně dodavatele.

23. Kryptografie, šifrování, kódování, steganografie, kryptoanalýza, symetrické a asymetrické šifrování, klíč, hash

kryptografie hash symetrie asymetrie

Osnova odpovědi

1. Rozliš kryptografii, šifrování a kódování.
2. Vysvětli steganografii a kryptoanalýzu.
3. Popiš symetrické šifrování a jeho použití.
4. Popiš asymetrické šifrování, veřejný a soukromý klíč.
5. Vysvětli hashovací funkci a rozdíl proti šifrování.
6. Uveď praktické použití v HTTPS, podpisech, heslech a zálohách.

Výkladové body

Kódování mění reprezentaci dat podle známého pravidla, například Base64 nebo znakové sady. Není určeno k utajení. Šifrování chrání obsah pomocí klíče. Kryptografie je širší obor zabývající se šifrováním, podpisy, hashi, výměnou klíčů a dalšími metodami ochrany informací.

Symetrické šifrování používá stejný tajný klíč pro šifrování i dešifrování a je rychlé. Asymetrické používá pár klíčů: veřejný a soukromý. Je pomalejší, ale řeší výměnu klíčů a elektronické podpisy. Hash je jednosměrný otisk dat, používaný pro integritu a ukládání hesel.

Příklady použití

- TLS kombinuje asymetrické ověření s rychlým symetrickým šifrováním relace.
- Elektronický podpis chrání integritu a potvrzuje držitele soukromého klíče.
- Hash souboru umožňuje ověřit, že se soubor nezměnil.
- Steganografie skrývá existenci zprávy, například v obrázku.

24. Hesla a bezpečnost, bezpečnostní politika, matice a mapa rizik, hash, salt, pepper, iterace, prolomení hesla a obrana

hesla rizika salt MFA

Osnova odpovědi

1. Vysvětli roli hesel v autentizaci.
2. Popiš bezpečnostní politiku hesel v organizaci.
3. Vysvětli matici rizik: pravděpodobnost krát dopad.
4. Rozliš kódování, šifrování a hashování.
5. Vysvětli salt, pepper a iterace při ukládání hesel.
6. Uveď základní způsoby prolomení hesel na vysoké úrovni a obranu.

Výkladové body

Heslo je něco, co uživatel zná. Bezpečné heslo má být dlouhé, jedinečné a neuhodnutelné. Dnes je praktické používat správce hesel a vícefaktorové ověření. Organizace má pravidla pro délku hesel, zakázaná slabá hesla, MFA, reset hesel, správu privilegovaných účtů a školení.

Hesla se nemají ukládat v čitelné podobě ani běžně šifrovaná. Ukládá se pomalý kryptografický hash se saltem. Salt je náhodná hodnota unikátní pro heslo. Pepper je tajná hodnota uložená odděleně. Iterace nebo paměťově náročné algoritmy zpomalují hromadné hádání hesel.

Obrana

- Dlouhá hesla nebo passphrase, pro každý účet jiné.
- MFA pro důležité účty.
- Omezení počtu pokusů a detekce podezřelého přihlašování.
- Kontrola hesel proti známým únikům.
- Bezpečné algoritmy pro ukládání hesel, například Argon2, bcrypt nebo scrypt.

> U maturity stačí popsat principy a obranu. Praktické návody na prolomení cizích hesel sem nepatří.

25. Bezpečnostní politika, ITIL, COBIT, best practice, CSF a SLA

ITIL COBIT SLA governance

Osnova odpovědi

1. Definuj bezpečnostní politiku a best practice.
2. Vysvětli ITIL jako rámec pro řízení IT služeb.
3. Popiš základní myšlenky ITIL: hodnota služby, incident, problém, změna, katalog služeb.
4. Vysvětli COBIT jako rámec pro řízení a kontrolu IT.
5. Popiš rozdíl mezi ITIL a COBIT.
6. Definuj CSF a SLA a jejich význam.

Výkladové body

ITIL se zaměřuje na řízení IT služeb tak, aby IT dodávalo hodnotu uživatelům a organizaci. Řeší například incident management, problem management, change enablement, service desk, konfigurace a zlepšování služeb.

COBIT je rámec pro governance a management podnikového IT. Pomáhá sladit IT s cíli organizace, řídit rizika, kontrolu, měření a odpovědnosti. Zjednodušeně: ITIL je více provoz a služby, COBIT je více řízení, kontrola a governance.

Pojmy

- **CSF:** critical success factor, co musí vyjít, aby služba nebo projekt uspěl.
- **SLA:** dohoda o úrovni služby, například dostupnost, reakční doba, doba opravy.
- **KPI:** měřitelný ukazatel výkonu.
- Bezpečnostní politika musí být schválená, známá, vymahatelná a pravidelně aktualizovaná.

26. Základní pojmy IS: zpráva, symbol, znak, abeceda, signál, číselné soustavy, prostorová náročnost dat a technické vybavení

data informace binární úložiště

Osnova odpovědi

1. Rozliš data, informaci a znalost.
2. Definuj zprávu, symbol, znak, abecedu a signál.
3. Vysvětli digitální reprezentaci pomocí bitů a bajtů.
4. Uveď číselné soustavy: dvojková, desítková, šestnáctková.
5. Uveď jednotky velikosti dat a příklady objemů.
6. Přiřaď objemům vhodné technické vybavení.

Výkladové body

Data jsou zaznamenané hodnoty bez kontextu. Informace vzniká interpretací dat a má význam pro příjemce. Zpráva je přenášený obsah. Symbol je prvek používaný k reprezentaci informace, znak je konkrétní symbol z abecedy. Signál je fyzikální nosič informace, například napětí, světlo nebo rádiová vlna.

Počítače pracují binárně. Bit má hodnotu 0 nebo 1, bajt má 8 bitů. Hexadecimální soustava se hodí pro kompaktní zápis binárních hodnot, například adres, barev nebo strojových dat.

Příklady objemů

- Textový dokument: jednotky KB až MB.
- Fotografie: jednotky MB.
- Video: stovky MB až desítky GB podle kvality.
- Databáze firmy: GB až TB.
- Technika: RAM pro běh, SSD/HDD pro ukládání, NAS/SAN a cloud pro sdílená data.

27. Životní cyklus IS a projektu, CSF jednotlivých stupňů, porovnání životního cyklu projektu a IS

SDLC projekt CSF provoz

Osnova odpovědi

1. Definuj životní cyklus informačního systému.
2. Popiš fáze: záměr, analýza, návrh, vývoj nebo pořízení, testování, nasazení, provoz, údržba, ukončení.
3. Ke každé fázi uveď kritické faktory úspěchu.
4. Definuj životní cyklus projektu.
5. Popiš například waterfall, agilní nebo hybridní přístup.
6. Porovnej cyklus projektu a cyklus IS.

Výkladové body

Životní cyklus IS trvá od nápadu až po vyřazení systému. Projektový životní cyklus je užší: řeší dočasnou organizovanou práci s cílem dodat změnu. IS pak může být v provozu mnoho let po skončení implementačního projektu.

U analýzy je CSF správné pochopení požadavků. U návrhu realistická architektura. U vývoje kvalita kódu a řízení změn. U testování dostatečné pokrytí rizik. U nasazení školení a plán přechodu. U provozu monitoring, podpora, bezpečnost a zálohy.

Porovnání

- **Projekt:** má začátek, konec, rozpočet, tým a výstup.
- **IS:** má dlouhodobý provoz, údržbu, rozvoj a ukončení.
- **Waterfall:** postupné fáze, vhodné pro stabilní požadavky.
- **Agile:** iterace, zpětná vazba, průběžné dodávky.

28. Ukazatele, metriky a projektový management: MTTR, MTBF, MD, CSF, ROI, TCO, TBO, TVO, TVOp, Ganttův diagram

metriky ROI TCO Gantt

Osnova odpovědi

1. Definuj metriku jako měřitelný ukazatel stavu, výkonu nebo kvality.
2. Rozliš tvrdé a měkké metriky.
3. Vysvětli MTTR, MTBF, MD a CSF.
4. Popiš ekonomické ukazatele ROI, TCO, TBO, TVO a TVOp.
5. Vysvětli Ganttův diagram.
6. Uveď atributy dobré metriky.

Výkladové body

MTTR je mean time to repair, tedy průměrná doba opravy nebo obnovy. MTBF je mean time between failures, průměrná doba mezi poruchami. MD, man day, je práce jednoho člověka za jeden den. CSF jsou kritické faktory úspěchu.

ROI vyjadřuje návratnost investice. TCO je total cost of ownership, tedy celkové náklady vlastnictví včetně pořízení, provozu, podpory, licencí a ukončení. TBO a TVO se používají pro pohled na přínosy a hodnotu technologií; důležité je vždy říct, co se do ukazatele započítává a proč.

Atributy metrik

- Jasná definice a jednotka.
- Měřitelnost a dostupný zdroj dat.
- Vazba na cíl nebo rozhodnutí.
- Pravidelné vyhodnocování a odpovědnost.
- Ganttův diagram ukazuje úkoly v čase, návaznosti a milníky projektu.

29. Práce s informacemi a komunikačními prostředky, informační etika, Thomasův teorém, mediální gramotnost, manipulace, hoaxy, propaganda

informace | mediální gramotnost | hoax | kritické myšlení

Osnova odpovědi

1. Vysvětli význam práce s informacemi v digitálním prostředí.
2. Definuj informační etiku a odpovědné sdílení informací.
3. Vysvětli Thomasův teorém.
4. Popiš mediální gramotnost a mediální manipulaci.
5. Uveď argumentační fauly a kritické myšlení.
6. Popiš hoaxy, propagandu a ověřování informací.

Výkladové body

Thomasův teorém říká, že pokud lidé definují situace jako reálné, jsou reálné ve svých důsledcích. V mediálním prostoru to znamená, že i nepravdivá informace může ovlivnit chování lidí, volby, bezpečnost nebo reputaci.

Mediální gramotnost je schopnost rozumět médiím, hodnotit zdroje, rozpoznat manipulaci a pracovat s informacemi odpovědně. Kritické myšlení znamená ověřovat tvrzení, hledat důkazy, rozlišovat fakta a názory a uvědomovat si vlastní zkreslení.

Ověřování informací

- Zkontrolovat autora, zdroj, datum a kontext.
- Porovnat více nezávislých důvěryhodných zdrojů.
- Pozor na silné emoce, falešnou autoritu a vytržené citace.
- U obrázků použít reverzní vyhledávání a kontrolu metadat, pokud jsou dostupná.
- Argumentační fauly: ad hominem, falešné dilema, slaměný panák, apel na strach.

30. Řešení Business Intelligence: vazby B-G-C-A, BI s DWH, datové sklady, tržiště, procesy a IS

BI DWH ETL reporting

Osnova odpovědi

1. Definuj Business Intelligence jako podporu rozhodování pomocí dat.
2. Vysvětli vazby mezi Business, Government, Citizen a Administration na příkladech.
3. Popiš schéma BI s datovým skladem.
4. Vysvětli ETL/ELT proces, datový sklad a datová tržiště.
5. Uveď výstupy BI: reporty, dashboardy, KPI, analýzy, predikce.
6. Uveď příklady procesů a informačních systémů, které BI využívají.

Výkladové body

BI převádí data z provozních systémů na informace pro rozhodování. Data se získávají z ERP, CRM, e-shopu, účetnictví, výroby, logů nebo externích zdrojů. ETL znamená extract, transform, load: data se načtou, očistí, sjednotí a uloží do datového skladu.

Datový sklad DWH je centrální historické úložiště optimalizované pro analýzu. Datové tržiště, data mart, je menší část dat pro konkrétní oblast, například finance, prodej nebo marketing. BI nad tím staví reporty a dashboardy, které ukazují KPI a trendy.

Příklady vazeb a systémů

- **B2G:** firma podává elektronické hlášení státu.
- **G2C:** stát poskytuje občanovi portál veřejné správy.
- **C2A:** občan komunikuje s administrací, například žádost nebo formulář.
- **BI systémy:** reporting prodejů, skladové obrátky, finanční plánování, zákaznické segmenty.
- Úspěch BI závisí na kvalitě dat, definici metrik a ochotě rozhodovat podle ověřených dat.

Závěrečná poznámka

Obsahem zkoušky jsou témata z počítačových sítí, aplikačního softwaru a kybernetické bezpečnosti systémů. Pro jistotu si ke každému síťovému tématu připrav jednoduché schéma a ke každému bezpečnostnímu tématu konkrétní příklad rizika a obrany.