Zabezpečení sítě client – server

1. Nastav server s unikátními přihlašovacími údaji.
2. Zapni šifrované spojení (např. TLS/SSL).
3. Definuj role a oprávnění pro klienty.
4. Nastav firewall na serveru i klientech.
5. Pravidelně aktualizuj software na obou stranách.

Detailní postup

**1. Nastav server s unikátními přihlašovacími údaji**

* **Na Windows Server**:
  + Otevři **Správce serveru > Místní uživatelé a skupiny** (nebo lusrmgr.msc).
  + Vytvoř nové uživatelské účty (např. „ServerAdmin“) s heslem minimálně 12 znaků (např. „Tr1ckyP@ssw0rd“).
  + Zakaž výchozí účet „Administrator“ (klikni pravým > Vlastnosti > Zaškrtni „Účet je zakázán“).
* **Cíl**: Zamezit použití snadno uhodnutelných účtů.

**2. Zapni šifrované spojení**

* **Na Windows Server**:
  + Pokud používáš vzdálenou plochu (RDP), zapni šifrování: **Ovládací panely > Systém > Vzdálené připojení > Povolit pouze připojení s NLA (Network Level Authentication)**.
  + Pro sdílení souborů aktivuj SMB šifrování: Otevři PowerShell jako admin a spusť Set-SmbServerConfiguration -EncryptData $true.
* **Na Windows 10**:
  + Při připojení k serveru (např. přes „Mapovat síťovou jednotku“) zkontroluj, že používáš šifrované SMB (automatické od Windows 10 verze 1709).
* **Cíl**: Chránit data při přenosu mezi serverem a klientem.

**3. Definuj role a oprávnění pro klienty**

* **Na Windows Server**:
  + Nainstaluj roli **Active Directory Domain Services** (Správce serveru > Přidat role a funkce).
  + Vytvoř doménu (např. „firma.local“) a přidej Windows 10 klienty do domény (Systém > Změnit nastavení > Připojit k doméně).
  + V **Active Directory – Uživatelé a počítače**:
    - Vytvoř organizační jednotky (OU), např. „Uživatelé“ a „Počítače“.
    - Přidej uživatele (např. „JanNovak“) a zařaď je do skupin (např. „Zaměstnanci“ – jen čtení, „Správci“ – plný přístup).
  + Nastav sdílenou složku (pravým na složku > Vlastnosti > Zabezpečení) a přiřaď práva skupinám.
* **Na Windows 10**:
  + Přihlas se k doméně pomocí účtu z AD a zkontroluj přístup k síťové složce.
* **Cíl**: Omezit, co kdo může na serveru dělat.

**4. Nastav firewall na serveru i klientech**

* **Na Windows Server**:
  + Otevři **Brána firewall s pokročilým zabezpečením** (Ovládací panely > Systém a zabezpečení).
  + Vytvoř pravidlo:
    - Příchozí pravidla > Nové pravidlo > Port > TCP 445 (SMB) > Povolit pouze pro lokální síť (např. 192.168.1.0/24).
    - Pokud používáš RDP, povol port 3389 stejným způsobem.
  + Blokuj vše ostatní (výchozí pravidlo: „Blokovat nepovolené připojení“).
* **Na Windows 10**:
  + V **Bráně firewall** povol připojení k serveru: Příchozí pravidla > Nové pravidlo > Program > Cesta k explorer.exe > Povolit pro serverovou IP (např. 192.168.1.10).
  + Zkontroluj, že „Veřejná síť“ je nastavena na blokování a „Soukromá“ na povolení jen pro důvěryhodné sítě.
* **Cíl**: Zamezit přístupu zvenčí a omezit provoz jen na potřebné služby.

**5. Pravidelně aktualizuj software na obou stranách**

* **Na Windows Server**:
  + Otevři **Windows Update** (Nastavení > Aktualizace a zabezpečení) a spusť kontrolu aktualizací.
  + Nastav automatické stahování záplat (Správce serveru > Konfigurace > Automatické aktualizace).
* **Na Windows 10**:
  + Stejně jako na serveru: Nastavení > Aktualizace a zabezpečení > Zkontrolovat aktualizace.
  + Zapni „Pokročilé možnosti“ a nastav automatické restarty mimo pracovní dobu (např. 3:00).
* **Cíl**: Odstranit známé zranitelnosti v systému a aplikacích.

Dodatečné tipy

* **Testování**: Po nastavení zkus z Windows 10 přistoupit k serveru (např. \\192.168.1.10\slozka) a ověř, že šifrování a oprávnění fungují.
* **Zálohování**: Nastav na serveru zálohu klíčových dat (Správce serveru > Zálohování Windows Serveru) na externí disk.

**Monitoring**: Použij **Monitor prostředků** (Správce úloh > Výkon > Otevřít monitor prostředků) na serveru a sleduj podezřelý síťový provoz.

Zabezpečení emailového klienta a serveru

1. Nastav silné heslo pro emailové účty.
2. Zapni šifrování komunikace (např. SSL/TLS pro SMTP/IMAP).
3. Použij dvoufaktorové ověření (2FA).
4. Nastav antispamový filtr na serveru.
5. Zálohuj emaily a kontroluj logy přístupu.

## Detailní postup

#### 1. Nastav silné heslo pro emailové účty

* **Na Kerio Mail Server**:
  + Přihlas se do administrace Kerio Connect (webový prohlížeč, např. https://tvuj-server:4040/admin).
  + Jdi do **Uživatelé > Uživatelé**, vyber uživatele (např. „jan.novak“), klikni na **Upravit**.
  + V sekci **Heslo** změň heslo na minimálně 12 znaků (např. „H3sl0Kerio2025!“) a zaškrtni „Uživatel musí změnit heslo při příštím přihlášení“.
* **Na Thunderbird**:
  + Otevři Thunderbird, jdi do **Nástroje > Nastavení účtů > Správa hesel** (nebo „Nastavení > Soukromí a zabezpečení > Uložená hesla“).
  + Najdi svůj účet (např. „imap://tvuj-server“), klikni na „Upravit“ a aktualizuj heslo podle serveru.
* **Cíl**: Zabránit snadnému prolomení slabých hesel.

#### 2. Zapni šifrování komunikace

* **Na Kerio Mail Server**:
  + V administraci jdi do **Konfigurace > Zabezpečení > SSL/TLS**.
  + Ujisti se, že máš platný SSL certifikát (ideálně od CA, např. Let’s Encrypt; pokud ne, vygeneruj self-signed: **Certifikáty > Nový certifikát**).
  + V **Služby > SMTP, IMAP, POP3** zaškrtni „Vyžadovat zabezpečené připojení (SSL/TLS)“ pro všechny protokoly.
  + Porty: SMTP – 587 (TLS), IMAP – 993 (SSL), POP3 – 995 (SSL).
* **Na Thunderbird**:
  + Jdi do **Nástroje > Nastavení účtů > Nastavení serveru** (pro IMAP/POP3).
  + Nastav:
    - **IMAP**: Server: tvuj-server, Port: 993, Zabezpečení spojení: SSL/TLS, Autentizace: Normální heslo.
    - **SMTP**: Server: tvuj-server, Port: 587, Zabezpečení spojení: STARTTLS, Autentizace: Normální heslo.
  + Pokud máte self-signed certifikát, Thunderbird zobrazí varování – klikni na „Přidat výjimku“ a potvrď.
* **Cíl**: Chránit emaily před odposlechem v síti.

#### 3. Použij dvoufaktorové ověření (2FA)

* **Na Kerio Mail Server**:
  + Jdi do **Konfigurace > Zabezpečení > Dvoufaktorová autentizace**.
  + Zapni 2FA (Kerio podporuje Google Authenticator nebo TOTP).
  + Uživatelé si v **Kerio Connect Client** (webmail) nastaví 2FA: přihlásí se, kliknou na svůj profil > „Nastavení 2FA“ a naskenují QR kód do aplikace (např. Google Authenticator).
* **Na Thunderbird**:
  + Thunderbird 2FA přímo nepodporuje, takže použij **aplikační heslo**:
    - V Kerio administraci u uživatele povol „Aplikační hesla“ (Uživatelé > Upravit > Zabezpečení).
    - Uživatel si vygeneruje heslo v Kerio Connect Clientu a použije ho v Thunderbirdu místo běžného hesla.
* **Cíl**: Zvýšit bezpečnost účtu i při úniku hesla.

#### 4. Nastav antispamový filtr na serveru

* **Na Kerio Mail Server**:
  + Jdi do **Konfigurace > Ochrana obsahu > Antispam**.
  + Zapni „SpamAssassin“ a nastav citlivost (např. skóre 5 pro označení spamu, 8 pro odmítnutí).
  + Přidej blacklist/whitelist (např. blokuj domény typu „@spamdomain.com“).
  + Aktivuj „Greylisting“ pro zpomalení spamu od neznámých odesílatelů.
* **Na Thunderbird**:
  + Jdi do **Nastavení účtů > Nevyžádaná pošta** a zapni „Adaptivní filtr nevyžádané pošty“.
  + Označuj spam ručně (klikni pravým > „Označit jako nevyžádané“), aby se filtr učil.
* **Cíl**: Snížit množství spamu a phishingu.

#### 5. Zálohuj emaily a kontroluj logy přístupu

* **Na Kerio Mail Server**:
  + Jdi do **Konfigurace > Archivace a zálohování**.
  + Nastav zálohování:
    - Cíl: externí disk nebo síťové úložiště (např. \\192.168.1.100\backup).
    - Harmonogram: denně v 2:00 (např. „Každý den, kompletní záloha“).
  + V **Protokoly > Bezpečnost** sleduj pokusy o přihlášení (filtruj „neúspěšné přihlášení“).
* **Na Thunderbird**:
  + Zálohuj lokální data: **Nástroje > Import/Export > Zálohovat profil** na USB/disk.
  + Pravidelně kontroluj složku „Místní složky“ – tam se ukládají emaily, pokud je stahujete offline.
* **Cíl**: Mít zálohu dat a odhalit podezřelou aktivitu.

## Dodatečné tipy

* **Testování**: Po nastavení odešli testovací email z Thunderbirdu a zkontroluj, že dorazí (např. na jiný účet).
* **Antivirus**: Na Kerio zapni vestavěný antivirus (Konfigurace > Ochrana obsahu > Antivirus) a na PC s Thunderbirdem měj aktualizovaný antivirus (např. Windows Defender).
* **Síť**: Ujisti se, že Kerio server není veřejně přístupný jako open relay – v **Konfigurace > SMTP Server > Řízení relé** nastav „Povolit pouze ověřeným uživatelům“.

Firemní politika

1. Vytvoř dokument s pravidly používání IT (např. hesla, internet).
2. Definuj role zaměstnanců a jejich přístupy.
3. Stanov postup pro hlášení bezpečnostních incidentů.
4. Zajisti školení zaměstnanců o bezpečnosti.
5. Pravidelně aktualizuj politiku podle potřeb firmy.

Návrh Active Directory

1. Nainstaluj AD na serveru (Windows Server).
2. Vytvoř doménu s názvem firmy (např. firma.local).
3. Přidej organizační jednotky (OU) pro oddělení.
4. Nastav uživatele a skupiny s přístupovými právy.
5. Otestuj přihlášení z klientského PC do domény.

Zabezpečení a zálohování dat

1. Zašifruj citlivá data na disku (např. BitLocker).
2. Nastav přístup jen pro oprávněné uživatele.
3. Vytvoř zálohovací plán (např. denně na externí disk).
4. Použij zálohovací software (např. Windows Backup).
5. Pravidelně testuj obnovu ze zálohy.

Zabezpečení webového serveru

1. Nainstaluj SSL certifikát pro HTTPS.
2. Nastav silné heslo pro administrátorský přístup.
3. Aktualizuj webový server (např. Apache, IIS).
4. Zapni firewall a povol jen potřebné porty (80, 443).
5. Pravidelně kontroluj logy a hledej podezřelou aktivitu.