# Doporučené postupy zabezpečení služby Active Directory

netwrix.com/active-directory-best-practices.html

Ochrana Active Directory (AD) je pro bezpečnostní týmy kritickým cílem kvůli její ústřední roli v mnoha zranitelných funkcích, včetně ověřování, autorizace a přístupu k síti. Pokaždé, když uživatelé, aplikace, služby a zařízení IoT přistupují k podnikovým systémům, spoléhají na Active Directory.

Při nedávném bezpečnostním incidentu utrpěla platforma pro správu identit Okta průnik do svého systému zákaznické podpory a odhalila citlivá data, jako jsou jména a e-mailové adresy všech uživatelů. Tato událost vyvolává obavy ohledně potenciálních bezpečnostních chyb, které by mohly být zneužity k manipulaci nebo ohrožení ověřování uživatelů a řízení přístupu. Organizace závislé na Okta z hlediska bezproblémové integrace s Active Directory se mohou potýkat s problémy při udržování zabezpečení jejich prostředí AD, protože ohrožené přihlašovací údaje nebo autentizační mechanismy by mohly být potenciálně využity pro přístup ke zdrojům AD.

Protivníci využívají slabiny v zabezpečení AD nejen k získání přístupu k síti, ale také k eskalaci svých privilegií, laterálnímu přesunu mezi koncovými body a jinými systémy, nasazení malwaru a dalším.

Chcete-li zabránit útočníkům v každém kroku, použijte následující kontrolní seznam doporučených postupů zabezpečení služby Active Directory.

## Zabezpečte své  řadiče domény

Řadič domény (DC) je server, který ověřuje uživatele kontrolou jejich přihlašovacích údajů proti uloženým datům a také autorizuje (nebo zamítá) požadavky na přístup k různým IT zdrojům. Tato funkce dělá z DC primární cíl pro kyberzločince.

Osvědčené postupy pro zabezpečení řadičů domény Active Directory zahrnují následující:

Nasazení

- Mějte alespoň dva řadiče domény v každé doméně služby Active Directory kvůli odolnosti proti chybám a vysoké dostupnosti.
- Zvažte nasazení řadičů domény jen pro čtení v pobočkách nebo na jiných místech s omezenou konektivitou k hlavnímu datovému centru, abyste zlepšili zabezpečení a výkon.
- Umístěte řadiče domény na různá fyzická umístění, abyste zajistili, že všechny nebudou ovlivněny jediným bodem selhání, jako je například výpadek napájení nebo přírodní katastrofa.

Řízení přístupu a dopravy

- Omezte fyzický přístup k DC pomocí opatření, jako jsou uzamčené serverové místnosti a systémy řízení přístupu.
- Pomocí segmentace sítě izolujte DC od ostatních částí sítě a omezte přístup pouze na autorizované systémy a správce.
- Implementujte brány firewall, abyste omezili příchozí a odchozí provoz na řadiče domény a umožnili pouze nezbytnou komunikaci mezi řadiči domény a dalšími síťovými prostředky.
- Izolujte DC od internetu konfigurací firewallů a směrovačů tak, aby blokovaly odchozí provoz z DC na internet. Pokud je pro řadič domény vyžadován přístup k internetu, použijte k řízení přístupu proxy server; nakonfigurujte proxy server tak, aby povoloval pouze nezbytný provoz a blokoval veškerý další provoz, a implementujte filtrování DNS, abyste zabránili komunikaci se známými škodlivými doménami.

Konfigurace a aktualizace

- Standardizujte konfiguraci DC. Použijte například automatizaci sestavení prostřednictvím nástrojů pro nasazení, jako je System Center Configuration Manager.

- Neinstalujte na řadiče domény další role serveru ani software, protože to může vést ke sporům o zdroje, nestabilitě a snížení výkonu. Pokud je vyžadován další software nebo role serveru, nasaďte samostatné členské servery nebo aplikační servery pro spouštění aplikací nebo hostování dalších služeb.
- Pravidelně aktualizujte řadiče domény nejnovějšími bezpečnostními záplatami a aktualizacemi, abyste je chránili před slabými místy zabezpečení.
- Pravidelně upgradujte operační systémy svých řadičů domény. Proces upgradu však důkladně naplánujte a otestujte v neprodukčním prostředí, abyste identifikovali a zmírnili potenciální problémy.

Monitorování a obnova

- Pomocí monitorovacích nástrojů můžete sledovat výkon řadičů domény a zajistit, aby fungovaly optimálně.
- Pravidelně zálohujte data na řadičích domény, abyste umožnili obnovu v případě selhání hardwaru nebo jiného problému.

## Vytvořte robustní zásady pro hesla

Služba Active Directory vám umožňuje definovat jemné zásady hesel pomocí faktorů, jako je délka hesla a požadavky na složitost. Postupujte podle následujících pokynů pro hesla NIST :

- Hesla by měla obsahovat alespoň osm znaků, když je nastavuje člověk, a šest znaků, když je nastavuje automatizovaný systém nebo služba.
- Použití jednoho silného hesla je efektivnější než pravidelná aktualizace slabých hesel.

- Vyhněte se požadavkům na složitost, které nejsou uživatelsky přívětivé, protože mohou vést k tomu, že uživatelé budou vytvářet slabá hesla nebo svá hesla ukládat nezabezpečeným způsobem (například na lístek na stole). Místo toho vyzvěte uživatele, aby volili dlouhé přístupové fráze, které jsou snadno zapamatovatelné.
- Sledujte resetování hesla správce. Neobvyklá aktivita resetování hesla může signalizovat kompromitaci účtu správce.
- Zkalibrujte nastavení uzamčení účtu a použijte přísnější nastavení na účty, které mají přístup k cenným datům a kritickým aplikacím. Tímto způsobem bude útočník, který se pokusí kompromitovat účet správce, uzamčen již po několika neúspěšných pokusech, ale běžný uživatel, který několikrát zadá své heslo špatně, nebude uzamčen a bude muset své heslo resetovat, než se bude moci vrátit. pracovat.
- Zvažte investici do správce hesel, který uživatelům usnadní používání silných a jedinečných hesel, aniž by zvyšoval zátěž vašeho helpdesku častým zamykáním účtů.

### Na každém počítači použijte jiné heslo místního správce

Organizace až příliš často vytvářejí obecné uživatelské ID místního správce se stejným heslem na každém počítači, což umožňuje špatnému herci, který kompromituje jeden stroj, kompromitovat i ostatní. Pomocí správných nástrojů můžete na každém zařízení snadno nastavit jiné heslo místního správce.

Zejména řešení hesla místního správce (LAPS) automaticky generuje a spravuje jedinečná, složitá hesla pro účty místních správců. Tato hesla jsou bezpečně uložena ve službě Active Directory a mohou je získat pouze oprávnění uživatelé nebo systémy. LAP nabízí následující další výhody:

- LAPS podporuje automatickou rotaci hesel místního správce v pravidelných intervalech, čímž zkracuje životnost prolomeného hesla.

- Správci mohou delegovat oprávnění pro získávání hesel místního správce na základě rolí a odpovědností uživatelů.
- LAPS se hladce integruje se službou Active Directory a využívá její funkce zabezpečení a řízení přístupu ke správě ukládání a získávání hesel místního správce.
- LAPS udržuje revizní záznam činností získávání hesel pro usnadnění vyšetřování a odpovědnosti.
- LAPS lze konfigurovat a spravovat pomocí zásad skupiny, které poskytují centralizovaný a škálovatelný přístup k nasazení a správě hesel místních správců v celé organizaci.

## Kontrola přístupových práv

Skupiny zabezpečení jsou doporučeným způsobem řízení přístupu ke zdrojům . Namísto přímého přidělování přístupových práv uživatelským účtům jeden po druhém přidělujete oprávnění skupinám zabezpečení a poté učiníte každého uživatele členem příslušných skupin. Postupujte podle těchto doporučených postupů:

- Důsledně dodržujte model nejmenších oprávnění, který každému uživateli poskytne pouze minimální oprávnění, která potřebuje k dokončení svých úkolů.
- Vytvářejte účty hostů s minimálními oprávněními.
- Nechte vlastníky dat pravidelně kontrolovat členství ve skupinách zabezpečení, aby bylo zajištěno, že členy každé skupiny jsou pouze ti správní uživatelé.
- Vytvořte model delegování AD podle osvědčených postupů .
- Pečlivě sledujte změny členství v bezpečnostních skupinách , zejména těch, které mají oprávnění k přístupu, úpravě nebo odstranění citlivých dat.
- Sledujte podezřelé úpravy účtů AD.
- Okamžitě deaktivujte účty zaměstnancům, kteří opustí organizaci.
- Sledujte neaktivní účty a v případě potřeby je deaktivujte.

## Zvláštní pozornost věnujte privilegovaným účtům

Útočníci se přirozeně zajímají zejména o získání přístupu k účtům, které mají oprávnění správce nebo přístup k citlivým údajům, jako jsou záznamy o zákaznících nebo duševní vlastnictví. Proto je důležité, abyste byli ohledně těchto výkonných účtů obzvláště ostražití. Mezi osvědčené postupy patří následující:

- Přísně omezte členství v Domain Admins a dalších privilegovaných skupinách v souladu se zásadou nejmenších oprávnění.
- Vyškolte administrátory, aby používali své administrátorské účty pouze tehdy, je-li to nezbytně nutné, aby se snížilo riziko krádeže přihlašovacích údajů.
- V ideálním případě implementujte řešení pro správu privilegovaných účtů (PAM). Pokud to není možné, ponechte ve skupinách, jako jsou Domain Admins, pouze výchozí účet a ostatní účty umístěte do této skupiny pouze dočasně, dokud svou práci nedokončí.
- Pravidelně kontrolujte používání privilegovaných účtů, abyste se ujistili, že jsou používány pouze pro autorizované účely a že přístup je udělen na základě potřeby vědět.
- Implementujte zásady silných hesel a postupy správy pro privilegované účty, včetně pravidelných změn hesel a používání složitých hesel.
- Vyžadujte, aby uživatelé s oprávněními používali k provádění administrativních úloh zabezpečenou pracovní stanici správce (SAW). SAW zvyšují zabezpečení pomocí funkcí, jako je silná autentizace, šifrování a monitorování. Omezte přístup k SAW na oprávněné pracovníky s administrativní odpovědností a zaveďte přísné kontroly přístupu, abyste zabránili neoprávněnému použití. Fyzicky a logicky izolujte SAW od standardních uživatelských pracovních stanic a sítí, abyste snížili riziko infekce malwarem a neoprávněného přístupu.

## Sledujte Active Directory, zda nevykazuje známky ohrožení

Active Directory je rušné místo. K rozpoznání útoků je nezbytné vědět, co hledat ve všech datech událostí. Zde je pět nejdůležitějších věcí, které je třeba sledovat:

Změny uživatelského účtu

Dávejte pozor na neobvyklé úpravy uživatelského účtu AD. Zvažte investici do nástroje, který vám pomůže odpovědět na následující otázky:

- Jaké změny byly provedeny u kterých uživatelských účtů?
- Kdo provedl jednotlivé změny?
- Kdy ke změně došlo?
- Odkud byla změna provedena?

Obnovení hesla administrátory

Správci by měli při resetování uživatelských pověření vždy dodržovat zavedené osvědčené postupy. Robustní monitorovací nástroj pomáhá zodpovědět otázky jako:

- U kterých uživatelských účtů byla resetována hesla?
- Kdo resetoval každé heslo?
- Kdy došlo k resetování?
- Kde admin resetoval heslo?

Změny členství ve skupinách zabezpečení

Neočekávané změny členství ve skupině zabezpečení mohou naznačovat škodlivou aktivitu, jako je eskalace oprávnění nebo jiné vnitřní hrozby. Potřebujete vědět:

- Kdo byl přidán nebo odebrán?
- Kdo provedl změnu?
- Kdy ke změně došlo?
- Kde byla provedena změna bezpečnostní skupiny?

Pokusy o přihlášení jednoho uživatele z více koncových bodů

Pokusy jednoho uživatele o přihlášení z různých koncových bodů jsou často známkou toho, že někdo převzal kontrolu nad jejich účtem nebo se o to pokouší. Je důležité označit a prozkoumat tuto aktivitu, abyste zjistili:

- Který účet se pokusil přihlásit z více koncových bodů?
- Jaké byly tyto koncové body?
- Kolik pokusů bylo provedeno z každého koncového bodu?
- Kdy začala podezřelá aktivita?

Změny zásad skupiny

Jediná nesprávná změna zásad skupiny může dramaticky zvýšit vaše riziko narušení nebo jiného bezpečnostního incidentu. Použití nástroje ke sledování této aktivity usnadní zodpovězení naléhavých otázek, jako jsou:

- Jaké změny byly provedeny v zásadách skupiny?
- Kdo provedl jednotlivé změny?
- Kdy byla provedena každá změna?

## Zakažte SMBv1 a omezte NTLM

Zařízení se systémem Microsoft Windows primárně používají komunikační protokol SMB (Server Message Block). Výzkum však ukazuje, že SMB se používá k narušení vzdáleným spuštěním kódu, takže se doporučuje zakázat SMBv1 a používat pouze nejnovější verze SMB.

Podobně NTLM je starý ověřovací protokol, který útočníci používají ke krádeži pověření. Pokud je to možné, nahraďte NTLM zcela novějším protokolem Kerberos. Minimálně odstraňte použití NTLMv1.

## Chraňte LSASS

LSASS (Local Security Authority Subsystem Service) je proces Windows, který zodpovídá za několik úkolů souvisejících se zabezpečením: ověřování přihlašovacích údajů uživatele během přihlašování; prosazování složitosti hesel, vypršení platnosti a zásad uzamčení; správa bezpečnostních tokenů, které poskytují přístup ke zdrojům; a implementaci autentizačního protokolu Kerberos. Osvědčené postupy pro ochranu LASAA zahrnují následující:

- Pravidelně aplikujte aktualizace zabezpečení a záplaty na operační systém, abyste řešili zranitelnosti, které by mohly být zneužity ke kompromitaci LSASS.
- Nasaďte na všechny systémy renomovaná antivirová a antimalwarová řešení, abyste detekovali a zabránili škodlivému softwaru zacílit na LSASS.
- Aktivujte Windows Credential Guard, bezpečnostní funkci ve Windows, která pomáhá chránit LSASS a přihlašovací údaje před krádeží malwarem.

### Spouštějte pouze podporované operační systémy a udržujte je aktualizované

Je důležité používat pouze podporované operační systémy, které dostávají pravidelné bezpečnostní aktualizace a opravy, abyste snížili riziko zranitelnosti zabezpečení a zajistili přístup k technické pomoci a pokynům pro problémy související se zabezpečením.

Kromě toho zajistěte, aby byly všechny operační systémy ve vašem prostředí pravidelně aktualizovány nejnovějšími bezpečnostními záplatami a aktualizacemi od dodavatele.

### Vyčistěte Active Directory

Osvědčené postupy zabezpečení služby Active Directory pro čištění zahrnují následující:

- Identifikujte a odstraňte všechny zastaralé nebo nepoužívané uživatelské účty a účty počítačů ze služby Active Directory, abyste zabránili protivníkům v jejich zneužití a zabránili odhalení.
- Vytvořte procesy, které zajistí, že uživatelský účet bude okamžitě deaktivován, když opustí organizaci.
- Odeberte všechny nepotřebné skupiny zabezpečení, abyste zmařili pokusy o eskalaci oprávnění.
- Zdokumentujte procesy čištění a stanovte pravidelné plány kontroly a údržby služby Active Directory, abyste zajistili trvalou bezpečnost a efektivitu.

## Audit Active Directory

Níže jsou uvedeny některé osvědčené postupy pro audit služby Active Directory:

- Ujistěte se, že je v Active Directory povoleno auditování pro sledování změn a přístup k objektům adresáře. To lze provést prostřednictvím nastavení zásad skupiny nebo přímo v konzole Uživatelé a počítače služby Active Directory.
- Nakonfigurujte zásady auditu na základě konkrétních požadavků na zabezpečení a shodu vaší organizace. Zejména auditování změn uživatelských účtů, členství ve skupinách, oprávnění a kritických objektů zásad skupiny.
- Pravidelně kontrolujte protokoly auditu generované službou Active Directory, abyste identifikovali jakékoli podezřelé změny nebo jinou neobvyklou aktivitu. Okamžitě prozkoumejte všechny potenciální bezpečnostní hrozby.
- Zvažte implementaci řešení monitorování v reálném čase, které poskytne okamžitá upozornění na kritické bezpečnostní události a automatickou reakci na hrozby na očekávané hrozby AD.
- Zvažte použití automatizovaných nástrojů pro generování pravidelných auditních zpráv, které mohou pomoci při sledování souladu, demonstraci náležité péče a identifikaci trendů nebo vzorců v činnosti adresářů.

### Proveďte správu oprav

Vytvořte proces pro rychlé přijímání a nasazování bezpečnostních záplat pro Active Directory a další kritické systémy. Upřednostněte nasazení oprav na základě závažnosti zranitelnosti a potenciálního dopadu na organizaci.

Před nasazením do produkčního prostředí otestujte opravy v neprodukčním prostředí, abyste se ujistili, že nezpůsobují žádné problémy s kompatibilitou nebo stabilitou.

### Proveďte skenování zranitelnosti a testování pera

Provádějte pravidelné kontroly zranitelnosti služby Active Directory a dalších kritických systémů, abyste identifikovali potenciální slabá místa zabezpečení. Upřednostňujte zranitelnosti podle závažnosti a potenciálního dopadu na vaši organizaci. Opravte zranitelná místa aplikací bezpečnostních záplat, implementací bezpečnostních kontrol nebo přijetím jiných opatření. Zvažte použití automatizovaných nástrojů k provádění skenování zranitelnosti, abyste zefektivnili proces a snížili riziko lidské chyby.

Provádějte také pravidelné penetrační testy, abyste identifikovali potenciální zranitelnosti a vyhodnotili efektivitu vašich bezpečnostních kontrol.

## Uzamkněte servisní účty

Účty služeb se používají ke spouštění služeb, naplánovaných úloh a aplikací. Chcete-li snížit bezpečnostní rizika, přidělte každému účtu služby minimální potřebná oprávnění k provádění jeho specifických funkcí. Kromě toho prosazujte zásady silných hesel, které zahrnují požadavky na složitost a omezení opakovaného použití hesel a vyžadují pravidelné změny hesla.

Účty služeb by měly být nakonfigurovány tak, aby zakazovaly interaktivní přihlášení. Neměly by se používat pro interaktivní relace nebo přihlášení ke konzole, protože jsou určeny pro spouštění

služeb a úloh na pozadí.

Kdykoli je to možné, používejte účty spravovaných služeb (MSA).

Účty spravovaných služeb (MSA) automaticky generují a spravují silná a složitá hesla, což eliminuje potřebu ruční správy hesel a snižuje riziko problémů se zabezpečením souvisejících s hesly. Heslo je automaticky spravováno a střídáno řadiči domény. MSA lze snadno nasadit a spravovat pomocí příkazů PowerShellu nebo zásad skupiny, což z nich činí škálovatelné a efektivní řešení.

### Implementujte vícefaktorové ověřování (MFA)

MFA zvyšuje zabezpečení tím, že vyžaduje, aby se uživatelé autentizovali pomocí dvou nebo více různých metod, jako je kód z hardwarového nebo softwarového tokenu nebo SMS zprávy, biometrie a push notifikace na mobilní zařízení. Zvažte faktory, jako je snadnost použití, škálovatelnost a kompatibilita s vaší stávající infrastrukturou, včetně Active Directory.

Definujte zásady MFA na základě uživatelských rolí, skupin nebo specifických požadavků na zabezpečení. Můžete například chtít vynutit MFA pro všechny privilegované účty, žádosti o vzdálený přístup nebo konkrétní aplikace.

### Zabezpečené DNS

- Zabezpečení DNS pomocí zón DNS integrovaných se službou Active Directory. To poskytuje vylepšené zabezpečení prostřednictvím seznamů řízení přístupu (ACL) a zabezpečených dynamických aktualizací.
- Implementujte Domain Name System Security Extensions (DNSSEC) a přidejte do DNS další vrstvu zabezpečení. DNSSEC pomáhá chránit před útoky DNS spoofing a cache poisoning digitálním podepisováním DNS dat.

- Nakonfigurujte servery DNS tak, aby omezovaly přenosy zón na autorizované servery. Omezení zónových přenosů pomáhá zabránit neoprávněnému přístupu k datům zóny DNS.
- Využijte řešení filtrování a ochrany DNS k blokování škodlivých domén a zabránění přístupu ke známým škodlivým webům. To může pomoci chránit před malwarem, phishingem a dalšími bezpečnostními hrozbami.
- Nasaďte bránu firewall DNS k filtrování a blokování škodlivého provozu DNS. DNS firewally mohou pomoci chránit před útoky založenými na DNS a zmírnit riziko úniku dat.
- Udržujte servery DNS aktuální pomocí nejnovějších bezpečnostních záplat a aktualizací, abyste opravili zranitelnosti a chránili před známými zneužitími.

## Vynutit RDP k použití šifrování TLS

Remote Desktop Protocol (RDP) je populární protokol používaný pro vzdálený přístup k systémům založeným na Windows. Ve výchozím nastavení používá RDP k zabezpečení komunikace mezi klientem a serverem šifrování. Pro zvýšení bezpečnosti se však doporučuje vynutit použití šifrování Transport Layer Security (TLS) pro RDP. Nainstalujte a nakonfigurujte certifikát SSL/TLS na serveru Brána vzdálené plochy. Tento certifikát bude použit k šifrování komunikace mezi klientem a serverem.

## Implementujte plán zálohování a obnovy po havárii pro Active Directory

Katastrofa nebo výpadek, který postihne AD, může mít vážné důsledky pro provoz organizace. Implementace plánu obnovy po havárii pro AD může pomoci zajistit kontinuitu podnikání v případě havárie. Nezapomeňte zahrnout procedury zálohování a obnovy, procedury převzetí služeb při selhání a navrácení služeb při selhání, komunikační a oznamovací procedury. testování postupů zálohování a obnovy a ukládání zálohovaných dat mimo pracoviště.

Mezi další doporučené postupy AD související se zálohováním a obnovou patří následující:

- Zálohujte Active Directory podle pravidelného plánu. Windows Server obsahuje vestavěnou funkci zálohování, kterou lze použít k zálohování služby Active Directory. K provedení záloh stavu systému, které zahrnují data AD, můžete použít nástroj "Zálohování serveru Windows". Řešení zálohování od jiných výrobců speciálně navržená pro Active Directory však nabízejí další funkce a flexibilitu.
- Zejména se ujistěte, že zálohujete řadiče domény s rolemi FSMO, protože ty jsou pro operace AD kritické.
- Ujistěte se, že zálohovaná data jsou bezpečně uložena. To zahrnuje ochranu záložních médií před fyzickým poškozením, šifrování zálohovaných dat a omezení přístupu k záložním souborům na oprávněné osoby.
- Zdokumentujte postupy zálohování pro Active Directory, včetně plánu zálohování, požadavků na uchování a jakýchkoli specifických aspektů pro vaše prostředí.

### Povolte bránu Windows Firewall na všech systémech

Povolte bránu Windows Firewall na všech systémech, abyste se chránili před neoprávněným přístupem a síťovými hrozbami.

- Pomocí zásad skupiny můžete centrálně spravovat a vynucovat nastavení brány Windows Firewall ve všech systémech ve vaší síti.
- Vytvořte pravidla brány firewall pro povolení nebo blokování konkrétních typů provozu na základě zásad zabezpečení vaší organizace. Můžete například vytvořit pravidla pro povolení příchozího a odchozího provozu pro konkrétní aplikace, služby nebo porty a zároveň blokovat zbytečný nebo potenciálně rizikový provoz.

- Pomocí konzoly Brána firewall systému Windows s pokročilým zabezpečením můžete nakonfigurovat pokročilá nastavení, jako jsou pravidla zabezpečení připojení, výjimky z ověřování a vlastní pravidla brány firewall, která poskytují podrobnou kontrolu nad síťovým provozem.

### Nasaďte antivirové a antimalwarové nástroje a udržujte je aktualizované

Vyberte si spolehlivý antivirový a antimalwarový software, který je kompatibilní se službou Active Directory a splňuje bezpečnostní potřeby vaší organizace.

Nainstalujte antivirový a antimalwarový software na server v prostředí Active Directory. Ujistěte se, že je software nakonfigurován pro skenování a ochranu všech systémů a zařízení připojených k síti Active Directory.

Nastavte automatické aktualizace pro antivirový a antimalwarový software, abyste zajistili, že bude vždy aktuální s nejnovějšími definicemi virů a bezpečnostními záplatami.

### Bezpečná síťová komunikace

- Nakonfigurujte službu Active Directory tak, aby používala SSL/TLS pro komunikaci LDAP k šifrování dat přenášených mezi klienty a řadiči domény.
- Použijte Internet Protocol Security (IPsec) k zabezpečení síťového provozu mezi doménovými řadiči a zajistěte, aby byla data šifrována a ověřena.
- Povolte podepisování Server Message Block (SMB), abyste zajistili, že data přenášená přes síť budou podepsána a ověřena, čímž se zabrání neoprávněné manipulaci a neoprávněnému přístupu.
- Nakonfigurujte službu Active Directory tak, aby používala ověřování Kerberos, které poskytuje zabezpečené vzájemné ověřování mezi klienty a řadiči domény.

## Implementujte VPN

Implementujte virtuální privátní sítě (VPN) pro svůj intranet na základě potřeb vaší organizace, včetně počtu vzdálených uživatelů, typů aplikací, ke kterým přistupujete, a požadované úrovně zabezpečení. Při výběru řešení VPN myslete také na snadnou údržbu, bezpečnostní funkce a škálovatelnost. Nainstalujte a nakonfigurujte klientský software VPN na zařízeních vzdálených uživatelů a zajistěte, aby se mohli bezpečně připojit k serverům VPN v rámci intranetu.

## Izolujte starší systémy a aplikace

Fyzicky nebo logicky oddělte starší systémy a aplikace od zbytku sítě, abyste omezili bezpečnostní rizika. Vytvořte samostatné organizační jednotky (OU) v AD pro starší systémy a aplikace, abyste mohli snadno použít nastavení zásad skupiny a řízení přístupu přizpůsobené jejich požadavkům.

## Vyřaďte starší systémy a aplikace z provozu

Vyhodnoťte využití, obchodní dopad a bezpečnostní rizika starších systémů a aplikací a vytvořte plán na jejich vyřazení z provozu, pokud je to možné. Informujte uživatele a zúčastněné strany o podrobnostech, včetně časových plánů, alternativních řešení a potenciálních dopadů na jejich pracovní postupy. Nezapomeňte archivovat všechna data, která již nejsou potřeba, ale musí být uchována pro účely souladu nebo pro historické účely.

## Závěr

Zde uvedené osvědčené postupy zabezpečení služby Active Directory jsou nezbytné pro posílení vaší pozice zabezpečení. Pečlivá správa aktivit v celé síti, které ovlivňují zabezpečení AD, vám umožní snížit plochu povrchu útoku a rychle detekovat hrozby a reagovat na ně.