Doporučené postupy zabezpečení služby Active Directory

semperis.com/blog/active-directory-security/active-directory-security-best-practices-checklist

October 13, 2023

Sean Deuby | Hlavní technolog

V rámci vaší IT infrastruktury je Active Directory (AD) centrálním centrem pro řízení přístupu ke zdrojům a udržení provozuschopnosti vašeho podniku. Důležitost služby Active Directory pro vaši organizaci ji však staví do hledáčku aktérů hrozeb. Pokud je služba Active Directory úspěšně narušena, útočníci mohou získat privilegovaná pověření a potenciálně ohrozit zabezpečení firemních dat nebo ovlivnit aplikace. Implementace osvědčených postupů zabezpečení služby Active Directory je proto důležitou součástí plánování politiky digitálního zabezpečení.

Jaké jsou doporučené postupy zabezpečení služby Active Directory?

Ochrana Active Directory znamená co nejvíce ztížit život kyberútočníkům. Těchto 12 osvědčených postupů zabezpečení služby Active Directory může pomoci snížit riziko narušení zabezpečení a zvýšit vaši kybernetickou odolnost. Cíl: **Zmenšit plochu útoku a chránit a posilovat prostředí služby Active Directory.**

1. Udržujte minimální počet privilegovaných uživatelů.
2. Použijte skupiny k přiřazení oprávnění.
3. Zabezpečené účty s oprávněními správce.
4. Prosazujte moderní zásady hesel.
5. Vynutit silná hesla na servisních účtech.
6. Provádějte pravidelná hodnocení, abyste odhalili porušení zásad hesel.
7. Vypněte službu Print Spooler.
8. Zakázat Server Message Block v1 (SMBv1) a omezit New Technology LAN Manager (NTLM).

9. Omezit přístup k řadičům domény (DC).
10. Plán obnovy služby Active Directory.
11. Použijte filtrování SID ve všech důvěryhodných doménových strukturách.
12. Monitorujte ve službě Active Directory podezřelou aktivitu a nezabezpečené konfigurace.

Jste připraveni začít?

1. Udržujte minimální počet privilegovaných uživatelů

Uživatelé s nadměrnými oprávněními přímo napadají požadavky na zabezpečení a dodržování předpisů. Pokud jsou tyto účty kompromitovány, umožňují útočníkům získat větší oporu ve vašem prostředí. Správa privilegovaných uživatelů je klíčovou součástí celkové správy služby Active Directory, ale může být také časově náročná. Velké podniky mohou mít stovky účtů v privilegovaných skupinách.

Některým účtům mohou být udělena nadměrná oprávnění k rychlému zprovoznění nových aplikací. Ostatní možná zdědili oprávnění, která již nepotřebují. Pokud jste odpovědní za udělování přístupu, řešení tohoto problému vyžaduje, abyste pochopili princip nejmenších oprávnění a použili jej k určení, jaká oprávnění každý uživatel nebo skupina potřebuje, aby mohl efektivně vykonávat svou práci.

Začněte kontrolou následujících skupin, abyste si ověřili, že každý člen má legitimní důvod být zahrnut:

- Enterprise Admins
- Správci schémat
- Správci domény
- Operátoři účtu (pokud existují)
- Operátoři serveru (pokud jsou k dispozici)
- Operátoři tisku (pokud jsou k dispozici)
- Správci DHCP

- DNSAdmins

2. Použijte skupiny k přiřazení oprávnění

Využití skupin zjednodušuje proces přidělování oprávnění uživatelům. Místo správy oprávnění jednotlivě (což může vést k chybám) uspořádejte uživatele do skupin a poté těmto skupinám přiřaďte příslušná oprávnění.

Kolekce uživatelů může představovat obchodní jednotku nebo interní tým, ve kterém mají uživatelé stejné potřeby ohledně přístupových práv. Určení toho, kdo by měl patřit do každé skupiny (např. kdo slouží jako správce domény nebo správce schématu) a jaká práva by tyto skupiny měly mít, vyžaduje komunikaci mezi týmem pro správu služby Active Directory a obchodními partnery.

3. Zabezpečte účty s oprávněními správce

Po vytvoření domény ve službě Active Directory se místní účet správce stane účtem domény správce a výchozím členem skupin Domain Admins a Administrators v doméně. Pokud je doménou kořenová doména doménové struktury, stane se účet také členem skupiny Enterprise Admins.

Pro ochranu tohoto účtu společnost Microsoft doporučuje nastavit příznak „Účet je citlivý a nelze jej delegovat“. Ověřte také, že objekty zásad skupiny (GPO) jsou nakonfigurovány tak, aby omezovaly použití účtů správce domény a vestavěných účtů správce v systémech připojených k doméně. Konkrétně zablokujte tyto účty z:

- Přístup k serverům a pracovním stanicím členů
- Přihlášení jako dávková úloha
- Přihlášení jako služba
- Přístup k členským serverům a pracovním stanicím pomocí Služby vzdálené plochy

4. Prosadit moderní zásady hesel

V centru každého podnikového útoku nebo narušení bezpečnosti je často ukradené heslo. Kromě použití těchto přihlašovacích údajů pro počáteční přístup mohou aktéři hrozeb použít přihlašovací údaje k laterálnímu pohybu v kompromitovaném prostředí.

Z tohoto důvodu je zabezpečení heslem prvořadé. Zkušenosti u velkých poskytovatelů cloudových služeb však ukázaly, že tradiční zásady hesel jsou proti moderním útokům nedostatečné. NIST a další velké organizace aktualizovaly své zásady hesel, aby tuto realitu uznaly.

Útoky hrubou silou proti internetovým službám ustoupily. Nahradily je útoky sprejem hesel, při kterých jsou známá běžná hesla pokoušena proti mnoha uživatelům v organizaci. Takové útoky jsou nyní běžné – a často úspěšné. Útoky sprejem hesel využívají tendenci uživatelů vytvářet hesla, která jsou snadno zapamatovatelná a snadno uhodnutelná.

Lepší strategií je nejprve se zaměřit na odstranění běžných hesel z Active Directory. Toho lze dosáhnout pomocí filtrů hesel třetích stran nebo pomocí ochrany heslem Microsoft Azure AD.

Druhým krokem k zásadě silných hesel je uznat, že vynucování složitosti může vést k heslům, která si uživatelé nepamatují, a snadno rozpoznatelným vzorům, které mohou útočníci rychle prolomit. Místo toho podpořte délku hesla nebo přístupové fráze s přidáním čísel a speciálních znaků, které umožňují vytvořit hesla, která si uživatelé snadno zapamatují, ale útočníci je obtížně uhodnou.

Například heslo **Implicate-Research1-Uncooked** lze snadno zapamatovat, ale (podle nástroje Bitwarden pro posílení hesel) by trvalo staletí, než by bylo prolomeno. Jak online zdroje, tak hlavní správci hesel obsahují nástroje pro generování přístupových frází. Uživatel může jednoduše pokračovat ve generování, dokud nenajde heslo, které si pamatuje.

Nakonec se nedoporučuje vyžadovat vypršení platnosti hesla. Zkušenosti ukázaly, že rotace nutí uživatele k snadno prolomitelným vzorům hesel. Pokud došlo k prolomení organizace nebo prolomení přihlašovacích údajů uživatele, hesla by měla být aktualizována. Jinak je nechte na pokoji.

Implementujte současně všechny tyto ovládací prvky: zákaz běžných hesel, snížení složitosti, prodloužení délky a zakázání vypršení platnosti hesla. Jinak riskujete vytvoření snadno prolomitelných hesel.

Další osvědčený postup: Využijte funkci jemně zrnitých zásad hesel. Ačkoli správci mohou použít výchozí zásady domény k nastavení jedné zásady hesla pro všechny členy domény, jemně zpracované zásady hesel správcům umožňují nastavit přísnější hesla pro jednotlivé uživatele a globální skupiny.

5. Prosadit silná hesla na servisních účtech

Kerberoasting je nejběžnějším způsobem kompromitace privilegovaného účtu a získání kontroly nad serverem Active Directory. Útoky Kerberoasting jsou na vzestupu, podle některých odhadů se od začátku roku 2022 zvýšily o 500+ %.

V této technice aktér hrozby začíná získáním běžného uživatelského přístupu prostřednictvím phishingu nebo jiné metody. Díky tomuto přístupu může útočník snadno získat seznam účtů služeb výčtem hlavních názvů služeb (SPN) ve službě Active Directory.

Poté útočník spojí tyto účty s členstvím v privilegovaných skupinách, aby získal seznam účtů privilegovaných služeb. Aktér hrozby si pak vyžádá lístek služby Kerberos z jednoho z těchto privilegovaných účtů. Tento lístek je zašifrován pomocí hash hesla servisního účtu, který útočník obvykle dokáže prolomit offline.

S prolomeným hashem hesla účtu služby může aktér hrozby rychle získat kontrolu nad Active Directory. Úspěšný útok Kerberoasting může ohrozit doménovou strukturu Active Directory během několika minut.

Jediný způsob, jak bojovat proti útoku Kerberoasting, je extrémně ztížit prolomení hesel servisních účtů:

- Použijte minimálně 25 znaků.
- Pomocí generátoru hesel vytvořte dlouhé, složité, vysoce entropické heslo a uložte je do trezoru hesel.
- Zvažte použití skupinově spravovaného servisního účtu (gMSA), který automaticky střídá složitá hesla. (Nejprve se však ujistěte, že jste obeznámeni s potenciálními zranitelnostmi souvisejícími s gMSA .)

6. Provádějte pravidelná hodnocení, abyste odhalili porušení zásad hesel

Pravidelné kontroly zásad a nastavení hesel mohou pomoci odhalit problémy, které mohou Active Directory vystavit útoku. Například prozkoumejte jakýkoli účet s nastaveným příznakem PASSWD_NOTREQD. Kromě toho prozkoumejte účty, které jsou nastaveny tak, aby umožňovaly anonymní přístup ke službě Active Directory, což umožňuje neověřeným uživatelům dotazovat se na službu Active Directory.

7. Vypněte službu Print Spooler

Služba Print Spooler spravuje tiskové procesy a je standardně spuštěna na klientech a serverech Windows. Ačkoli se to na první pohled zdá v pořádku, každý ověřený uživatel se může vzdáleně připojit ke službě, požádat o aktualizaci nových úloh a sdělit DC, aby odeslalo oznámení do systému s neomezeným delegováním. A to odhaluje přihlašovací údaje k počítačovému účtu DC. Kvůli riziku je nejlepším postupem zakázat službu na všech DC.

8. Zakažte SMBv1 a omezte NTLM

V ohrožení jsou také řadiče domény, které povolují protokol SMBv1. Společnost Microsoft v roce 2014 ukončila podporu protokolu SMBv1, který je zranitelný vůči více útokům, a doporučuje jej zakázat.

Podobně omezte používání NTLM. Mnoho organizací pomalu deaktivuje NTLM kvůli dopadu, který tato akce může mít. IT lídři by však měli zvážit co největší omezení jeho používání .

9. Omezte přístup k řadičům domény

Organizace by měly omezit přístup k řadičům domény , aby omezily hrozbu ohrožení DC malwarem:

- Na DC by nemělo být povoleno žádné procházení webu.
- Objekty GPO propojené se všemi organizačními jednotkami DC v doménové struktuře by měly být nastaveny pouze tak, aby umožňovaly připojení protokolu RDP (Remote Desktop Protocol) od autorizovaných uživatelů a systémů.

10. Naplánujte obnovu služby Active Directory

Vytvoření komplexního a podrobného plánu obnovy služby Active Directory je klíčovou součástí budování kybernetické odolnosti. Organizace by měly zálohovat alespoň dva řadiče domény na doménu, včetně kořenové domény. Tyto zálohy by měly být uchovávány offline, aby se zabránilo jejich napadení malwarem.

11. Použijte filtrování SID ve všech důvěryhodných doménových strukturách

Chcete-li pochopit důležitost zabezpečení filtrování SID, zvažte, jak je spravováno řízení přístupu ke službě Active Directory mezi doménovými strukturami.

Vztah důvěryhodnosti doménové struktury spojuje dvě doménové struktury služby Active Directory, aby uživatelům v jedné doménové struktuře umožnil přístup k prostředkům ve druhé. Trusty doménových struktur jsou nezbytné pro zachování přístupu v organizaci s více doménovými strukturami. V jednom běžném scénáři mají uživatelé v centralizované doménové struktuře účtů přístup k aplikacím (jako jsou souborové servery nebo servery SharePoint) v jedné nebo více doménových strukturách prostředků.

Každý uživatel, skupina nebo počítač (známý jako objekty zabezpečení) v doméně a doménové struktuře služby Active Directory má jedinečný identifikátor zabezpečení (SID). Tento identifikátor se používá v přístupovém tokenu uživatele k udělení přístupu k prostředkům v celé doménové struktuře pomocí seznamů řízení přístupu (ACL).

Při testování beta verzí Active Directory jsem v Intelu narazil na problém související s SID: Když jsme migrovali uživatele do nové doménové struktury Active Directory, uživatel ztratil přístup ke zdrojům své zdrojové doménové struktury. K tomu došlo, protože SID, které bylo uživateli uděleno v nové doménové struktuře, se lišilo od původního SID uživatele. Ztratili tak oprávnění k přístupu ke zdroji.

Steve Grobman (nyní CTO McAfee) navrhl Microsoftu myšlenku atributu, který by obsahoval původní SID ze zdrojové doménové struktury, čímž by byl zachován přístup k původním zdrojům. Společnost Microsoft přijala tento požadavek na změnu návrhu a atribut **historie** sid byl na světě. Během jakéhokoli projektu migrace nebo konsolidace služby Active Directory je **historie sID** nezbytná pro zachování přístupu uživatelů k prostředkům ve zdrojové doménové struktuře, když uživatel migroval do cílové doménové struktury, ale prostředky nikoli.

Jakmile je však projekt migrace nebo konsolidace dokončen, **historie sID** by měla být odstraněna. Aktér hrozby se zvýšenými právy by mohl využít **historii sID** ke zkopírování SID z důvěřující domény (například SID člena skupiny Domain Admins) a přidat jej do atributu historie sID hlavního objektu zabezpečení v důvěryhodné doméně – a tím udělit práva správce útočníka v důvěřující doméně.

Zde přichází na řadu filtrování SID. Odebere všechna cizí (tj. nikoli místní doménová) SID z přístupového tokenu uživatele, čímž se zabrání tomuto eskalačnímu útoku. **Filtrování SID by mělo být povoleno u všech důvěryhodných doménových struktur, pokud neprobíhá proces migrace nebo konsolidace.**

Bohužel, podle mých zkušeností většina migračních a konsolidačních projektů ve skutečnosti nikdy nekončí. Prostě mizí během obtížnější fáze migrace aplikací a historie SID je ponechána povolená, takže uživatelé mohou nadále přistupovat ke svým původním zdrojům.

Uvědomte si, že určité chyby konfigurace mohou snížit účinnost filtrování SID. Například:

- Odchozí důvěryhodnosti doménové struktury, které mají příznak **TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL** nastavený na hodnotu true, považují důvěryhodnost mezi doménami vůči doméně jako externí důvěryhodnost, čímž se uvolní přísnější filtrování prováděné na důvěryhodnosti mezi doménovými strukturami.
- Důvěryhodnosti s nastaveným atributem **TRUST_ATTRIBUTE_ CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION** nebo **TRUST_ATTRIBUTE_ PIM_TRUST** umožňují delegování lístku Kerberos, čímž se snižuje ochrana, kterou nabízí filtrování SID.

12. Sledujte ve službě Active Directory podezřelou aktivitu a nezabezpečené konfigurace

Útočníci často využívají konfigurace, které jim umožňují rychle eskalovat oprávnění a zůstat ve vašem prostředí nedetekováni. Pravidelně proto kontrolujte a sledujte přístupová práva, zda nenaznačují, že probíhá útok nebo že je vaše organizace vůči útoku zranitelná.

Některé objekty, jako je například objekt **AdminSDHolder** , se zřídka legitimně mění. Objekt **AdminSDHolder** slouží jako šablona oprávnění pro chráněné skupiny a účty v doméně. Pokud je povoleno dědění, útočník se může pokoušet změnit oprávnění u privilegovaných objektů řízených **AdminSDHolder** .

Správci by měli vědět, že byla provedena změna, a měli by být schopni formulovat důvod změny. Pokud byla úprava neúmyslná, pravděpodobnost kompromisu je vysoká. Monitorování tohoto typu aktivity je zásadní pro rychlé zachycení útoků a pro zabránění zneužití nastavení.

Jak vám Semperis může pomoci zabezpečit Active Directory

Semperis poskytuje řešení pro hodnocení a obnovu zabezpečení služby Active Directory, která vám pomohou zaměřit vaše úsilí.

- Bezplatný nástroj pro hodnocení zabezpečení Purple Knight skenuje prostředí Active Directory, Entra ID (dříve Azure AD) a Okta, aby rychle identifikoval zranitelnosti v prostředích hybridních identit a poskytl prioritní odborné pokyny k nápravě.
- Directory Services Protector (DSP) obsahuje hodnocení zabezpečení služby Active Directory, automatické vrácení podezřelých změn do služby Active Directory a další.
- Active Directory Forest Recovery (ADFR) urychluje obnovu Active Directory o 90 % ve srovnání s manuální obnovou.
- Náš nástroj Migrator for AD a služby migrace odborníků podporují tři kritické fáze jakéhokoli projektu konsolidace, migrace nebo modernizace služby Active Directory: příprava, provádění a monitorování po migraci.

- Odborníci Semperis na Breach Preparedness & Response Services vám mohou pomoci zkontrolovat a analyzovat vaši bezpečnostní architekturu a konfigurace, provozní postupy a potenciální cesty k útokům. Můžeme poskytnout plán doporučených vylepšení zabezpečení a také plány nápravy a obnovy.

Ochrana Active Directory se může zdát jako monumentální úkol. Přijetím osvědčených postupů pro zabezpečení služby Active Directory můžete zvýšit úroveň obtížnosti pro útočníky a zlepšit celkovou pozici zabezpečení vašeho prostředí.

Další informace o doporučených postupech zabezpečení služby Active Directory

- Zabezpečení Active Directory: Nejvyšší rizika a doporučené postupy
- Nejlepší tipy pro ochranu Active Directory
- Základní průvodce zabezpečením služby Active Directory
- AD Security 101: Zabezpečení řadiče domény