25 nejlepších osvědčených postupů zabezpečení služby Active Directory

activedirectorypro.com/active-directory-security-best-practices

27. dubna 2024

Toto je nejobsáhlejší seznam doporučených postupů zabezpečení služby Active Directory online.

V této příručce se podělím o svá doporučení pro zabezpečení služby Active Directory a o tom, jak můžete zlepšit zabezpečení prostředí vaší domény Windows.

Za zlepšení zabezpečení nemusíte utrácet jmění, existuje mnoho bezplatných a nízkonákladových řešení, která vám ukážu v této příručce.

Témata zabezpečení AD pokrytá v této příručce:

Proč je zabezpečení Active Directory nezbytné

V mnoha organizacích je Active Directory centralizovaným systémem, který ověřuje a autorizuje přístup k síti. Dokonce i v cloudovém nebo hybridním prostředí to stále může být centralizovaný systém, který uděluje přístup ke zdrojům. Při přístupu k dokumentu v síti, OneDrive, tisku na síťové tiskárně, přístupu k internetu, kontrole e-mailu a tak dále všechny tyto prostředky často procházejí přes Active Directory, aby vám udělily přístup.

Služba Active Directory existuje již dlouhou dobu a v průběhu let objevili zlomyslní aktéři zranitelná místa v systému a způsoby, jak je zneužít. Kromě zranitelností je pro hackery velmi snadné jednoduše ukrást nebo získat uživatelské přihlašovací údaje, které jim pak umožní přístup k vašim datům. Pokud mohou získat přístup k vašemu počítači nebo k vašemu přihlášení, mohou potenciálně získat úplný přístup k Active Directory a vlastnit vaši síť.

Nyní se ponoříme do seznamu doporučených postupů zabezpečení služby Active Directory.

1. Omezte používání správců domény a dalších privilegovaných skupin

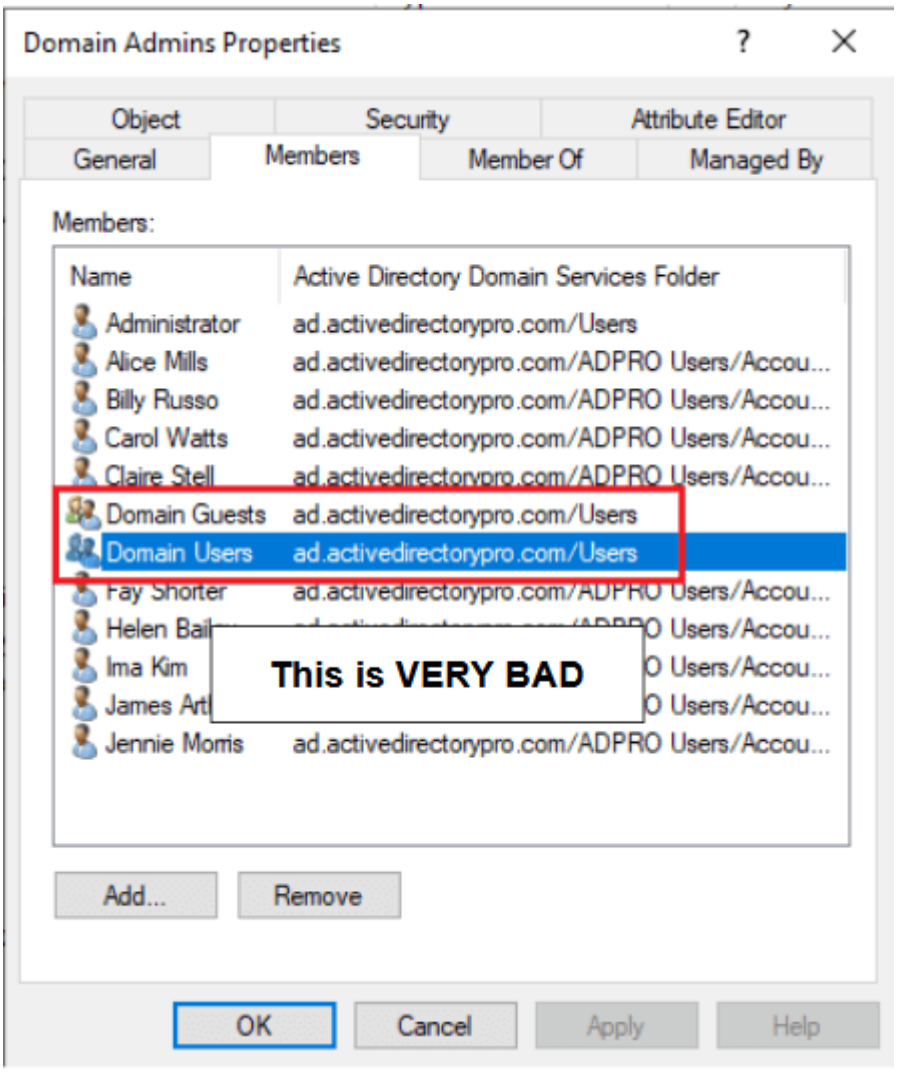
Členové doménových správců a dalších privilegovaných skupin jsou velmi výkonní. Mohou mít přístup k celé doméně, všem systémům, všem datům, počítačům, notebookům a tak dále.

Je doporučeno nemít žádné každodenní uživatelské účty ve skupině Domain Admins, jedinou výjimkou je výchozí účet Domain Administrator.

Správci domén jsou to, co se ti padouši snaží hledat.

Společnost Microsoft doporučuje, abyste v případě potřeby přístupu DA dočasně umístili účet do skupiny DA. Po dokončení práce byste měli odebrat účet ze skupiny DA.

Tento proces se také doporučuje pro skupiny Enterprise Admins, Backup Admins a Schema Admin.



O co jde?

Pro útočníky je příliš snadné získat nebo prolomit přihlašovací údaje.

Jakmile útočníci získají přístup k jednomu systému, mohou se v rámci sítě pohybovat laterálně a hledat vyšší oprávnění (administrátoři domény).

Jedna metoda, jak toho dosáhnout, se nazývá předat hash.

Předat hash umožňuje útočníkovi použít hash hesla k autentizaci do vzdálených systémů místo běžného hesla. Tyto hodnoty hash lze získat z počítačů koncových uživatelů.

Strašidelné, že?

Útočníkovi stačí jeden kompromitovaný počítač nebo uživatelský účet ke kompromitaci sítě.

Vyčištění skupiny Domain Admins je skvělým prvním krokem ke zvýšení zabezpečení vaší sítě. To může útočníka vzdorovitě zpomalit.

Proces odebrání účtů ze skupiny DA není snadný. Vím to z první ruky, protože jsem nedávno prošel tímto procesem. Je velmi běžné mít příliš mnoho účtů ve skupině DA.

Věci se zlomí, takže buďte připraveni.

2. Použijte dva nebo více účtů (běžný účet a účet správce)

Neměli byste se každý den přihlašovat pomocí účtu, který je místním správcem nebo má privilegovaný přístup (administrátor domény).

Místo toho vytvořte dva účty, běžný účet bez práv správce a privilegovaný účet, který se používá pouze pro administrativní úkoly.

ALE

Nevkládejte svůj sekundární účet do skupiny Domain Admins, alespoň trvale.

Místo toho se řiďte **nejméně privilegovaným administrativním modelem** . V zásadě to znamená, že by se všichni uživatelé měli přihlásit pomocí účtu, který má minimální oprávnění k dokončení své práce.

Můžete si přečíst další články a fóra a přidat svůj sekundární účet do skupiny Domain Admins.

Toto není osvědčený postup společnosti Microsoft a nedoporučoval bych to. Opět dočasné je v pořádku, ale musí být odstraněno, jakmile je práce hotová.

Díky tomu Microsoft neusnadňuje zbavit se práv správce domény. Neexistuje žádný snadný proces, jak delegovat práva na všechny systémy, jako je DNS, DHCP, skupinové zásady a tak dále. To je často důvod, proč má tolik lidí práva správce domény.

Měli byste používat běžný účet bez administrátora pro každodenní úkoly, jako je kontrola e-mailů, procházení internetu, lístkový systém a tak dále. Privilegovaný účet byste použili pouze tehdy, když potřebujete provádět úkoly správce, jako je vytvoření uživatele v Active Directory, přihlášení k serveru, přidání záznamu DNS atd.

Podívejte se na tyto dva scénáře.

Scénář 1 – IT zaměstnanci s doménovými právy

Steve se přihlásí do svého počítače pomocí privilegovaného účtu, zkontroluje svůj e-mail a neúmyslně si stáhne virus. Vzhledem k tomu, že Steve je členem skupiny DA, má virus plná práva k jeho počítači, všem serverům, všem souborům a celé doméně. To by mohlo způsobit vážné poškození a vést k selhání kritických systémů.

Nyní vezměte stejný scénář, ale tentokrát je Steve přihlášen se svým běžným neadministrátorským účtem.

Scénář 2 – IT zaměstnanci s běžnými právy

Steve zkontroluje svůj e-mail a nechtěně stáhne virus. Virus má omezený přístup k počítači a nemá přístup k doméně nebo jiným serverům. Způsobilo by to minimální škody a zabránilo by se šíření viru po síti.

Pouhým používáním běžného účtu můžete zvýšit bezpečnost a vyhnout se vážným škodám.

Zde jsou některé běžné úkoly, které lze delegovat na sekundární účet správce.

- Práva pro uživatele a počítače služby Active Directory
- DNS
- DHCP
- Práva místního správce na serverech
- Zásady skupiny
- Výměna
- Práva místního správce na pracovních stanicích
- Vsphere nebo Hyper-v Administration

Některé organizace používají více než dva účty a používají víceúrovňový přístup. To je rozhodně bezpečnější, ale pro některé to může být nepříjemnost.

- Běžný účet
- Účet pro správu serveru
- Účet pro správu sítě
- Účet pro správu pracovní stanice

3. Zabezpečte účet správce domény

Každá doména obsahuje účet Administrator, tento účet je ve výchozím nastavení členem skupiny Domain Admins.

Vestavěný účet správce by se měl používat pouze pro nastavení domény a obnovu po havárii (obnovu Active Directory).

Každý, kdo vyžaduje přístup na úrovni správce k serverům nebo službě Active Directory, by měl používat svůj vlastní individuální účet.

Nikdo by neměl znát heslo účtu správce domény. Nastavte si opravdu dlouhé heslo o délce 20 znaků a zamkněte ho v trezoru. Opět je to potřeba pouze pro účely obnovy.

Kromě toho má společnost Microsoft několik doporučení pro zabezpečení vestavěného účtu správce. Tato nastavení lze použít na zásady skupiny a použít na všechny počítače.

- Povolit Účet je citlivý a nelze jej delegovat.
- Pro interaktivní přihlášení je vyžadováno povolení karty Smart Card
- Odepřít přístup k tomuto počítači ze sítě
- Odepřít přihlášení jako dávkovou úlohu
- Odepřít přihlášení jako službu
- Odepřít přihlášení přes RDP

Další podrobnosti o zabezpečení účtu správce domény naleznete v tomto článku společnosti Microsoft Zabezpečení vestavěných účtů správce ve službě Active Directory

4. Zakažte účet místního správce (na všech počítačích)

Účet místního správce je dobře známý účet v prostředí domény a není potřeba.

Není potřeba, je to pravda?

Ano

Měli byste používat individuální účet, který má potřebná práva k provádění úkolů.

Jaký je problém s účtem místního správce?

Dva problémy.

1. Je to dobře známý účet, i když jej přejmenujete, SID je stejné a útočníci jej dobře znají.
2. Často je konfigurován se stejným heslem na každém počítači v doméně.

Útočníci stačí kompromitovat jeden systém a nyní mají práva místního správce na každém počítači připojeném k doméně. Poté by mohli tento účet použít k převedení do jiného systému s cílem najít přístup správce domény.

Pokud potřebujete na počítači provádět úkoly správce (instalovat software, mazat soubory atd.), měli byste to dělat pomocí svého individuálního účtu, nikoli účtu místního správce.

I když je účet deaktivován, můžete zavést systém do nouzového režimu a použít účet místního správce.

Jako správce vím, že tyto osvědčené postupy nejsou vždy praktické nebo představují obrovské nepříjemnosti.

Co když je síť mimo provoz nebo karta NIC zanikla, co když ji potřebujete vyjmout z domény a znovu ji přidat? Existují způsoby, jak to obejít, ale může vás to opravdu zpomalit.

Pokud nemůžete účet deaktivovat, zde jsou doporučení pro zabezpečení účtu. **Lepší alternativou je použití nástroje Microsoft LAPS (popsáno níže v tipu #5)**

- Odepřít přístup k tomuto počítači ze sítě
- Odepřít přihlášení jako dávková úloha
- Odepřít přihlášení jako službu
- Odepřít přihlášení přes RDP

Další podrobnosti naleznete v následujícím článku Zabezpečení účtů a skupin místních správců

5. Použijte řešení hesla místního správce (LDAPS)

Řešení hesla místního správce (LAPS) se stává oblíbeným nástrojem pro zpracování hesla místního správce na všech počítačích.

LAPS je nástroj společnosti Microsoft, který poskytuje správu hesel místních účtů počítačů připojených k doméně. Nastaví jedinečné heslo pro každý účet místního správce a uloží jej do Active Directory pro snadný přístup.

Toto je jedna z nejlepších bezplatných možností pro zmírnění předávání hašovacích útoků a bočního pohybu z počítače do počítače.

Je velmi běžné, že organizace nasazují Windows pomocí systému založeného na bitové kopii. To umožňuje rychlé nasazení standardní konfigurace do všech zařízení.

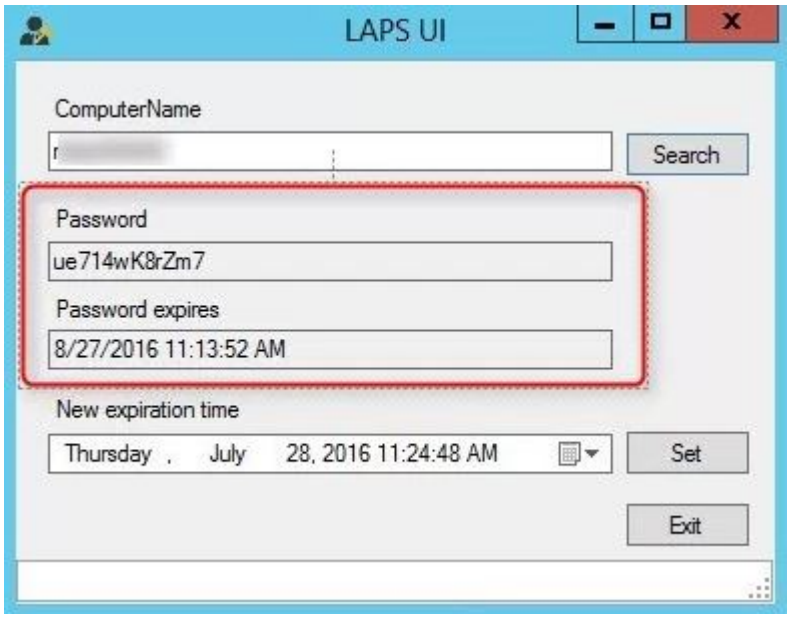
Ale..

To často znamená, že účet místního správce bude na každém počítači stejný. Vzhledem k tomu, že místní účet správce má plná práva ke všemu v počítači, stačí, aby byl jeden z nich kompromitován, a pak má hacker přístup ke všem systémům.

LAPS je postaven na infrastruktuře Active Directory, takže není potřeba instalovat další servery.

Řešení využívá rozšíření na straně klienta se zásadami skupiny k provádění všech úloh správy na pracovních stanicích. Je podporován na Active Directory 2003 SP1 a vyšší a klient Vista Service Pack 2 a vyšší.

Pokud potřebujete na počítači použít účet místního správce, heslo byste získali ze služby Active Directory a bylo by jedinečné pro tento jediný počítač.



Podrobné pokyny k instalaci LAPS naleznete v tomto článku Jak nainstalovat řešení hesla místního správce (LAPS)

6. Použijte zabezpečenou Admin Workstation (SAW)

Zabezpečená pracovní stanice správce je vyhrazený systém, který by se měl používat pouze k provádění administrativních úloh s vaším privilegovaným účtem.

Nemělo by se používat pro kontrolu e-mailů nebo procházení internetu. Ve skutečnosti by neměl mít ani přístup k internetu.

Jaké úkoly byste dělali na SAW?

- Administrace Active Directory
- Zásady skupiny
- Správa serverů DNS a DHCP
- Jakákoli úloha, která vyžaduje administrátorská práva na serverech
- Administrátorská práva k systémům pro správu, jako jsou VMware, Hyper-v, Citrix
- Správa Office 365

Dostanete nápad.

V zásadě, když potřebujete používat svůj privilegovaný účet k provádění úkolů správce, měli byste to dělat ze SAW. Denně používané pracovní stanice jsou zranitelnější vůči kompromitaci z předávání hash, phishingových útoků, falešných webových stránek, keyloggerů a dalších.

Použití zabezpečené pracovní stanice pro váš zvýšený účet poskytuje mnohem větší ochranu před těmito vektory útoků. Vzhledem k tomu, že útoky mohou pocházet zevnitř i zvenčí, je nejlepší přijmout předpokládané porušení bezpečnostní pozice.

Vzhledem k neustálým hrozbám a změnám technologie se metodika nasazení SAW neustále mění. Existují také PAW a skokové servery, aby to bylo ještě více matoucí.

Zde je několik tipů, které vám pomohou začít:

- Použijte čistou instalaci OS (použijte nejnovější OS Windows)
- Aplikujte základní bezpečnostní linii tuhnutí (viz tip č. 25)
- Povolit úplné šifrování disku
- Omezit porty USB
- Povolte bránu Windows Firewall
- Blokovat internet
- Použijte virtuální počítač – terminálový server funguje dobře
- Nainstalovaný minimální software
- Pro přístup použijte dvoufaktorovou nebo čipovou kartu
- Omezte systémy tak, aby přijímaly pouze připojení ze SAW

Zde je můj typický pracovní postup pomocí SAW:

1. Přihlaste se do mého počítače pomocí svého běžného účtu, abyste mohli zkontrolovat e-maily a zobrazit nové žádosti o podporu.
2. Pokud mám nějaké administrativní úkoly, přihlásím se do svého SAW pomocí svého privilegovaného účtu, který má práva upravovat členství ve skupině AD a přidat uživatele do potřebné skupiny zabezpečení AD.

Docela přímočaré, že?

Může se to zdát jako problém, ale ve skutečnosti mi to takto vyhovuje. Mohu se vzdáleně připojit, když jsem mimo síť, a mít server, který má všechny nástroje, které potřebuji. Také se nemusím starat o přeinstalaci veškerého podpůrného softwaru, pokud potřebuji znovu vytvořit bitovou kopii svého počítače.

Další informace o tomto tématu najdete v dokumentaci k zařízením s privilegovaným přístupem společnosti Microsoft .

7. Povolte nastavení zásad auditu pomocí zásad skupiny

Ujistěte se, že jsou v zásadách skupiny nakonfigurována následující nastavení zásad auditu a použita na všechny počítače a servery.

Konfigurace počítače -> Zásady - Nastavení systému Windows -> Nastavení zabezpečení -> Rozšířená konfigurace zásad auditu

Přihlášení k účtu

Ujistěte se, že je „Ověření pověření auditu“ nastaveno na „Úspěch a neúspěch“

Správa účtu

Audit „Správa aplikační skupiny“ je nastaven na „Úspěch a neúspěch“
Audit „Správa účtu počítače“ je nastaven na „Úspěch a neúspěch“
Audit „Další události správy účtu“ je nastaven na „Úspěch a neúspěch“

Audit „Správa skupiny zabezpečení“ je nastaveno na „Úspěch a neúspěch“
Audit „Správa uživatelských účtů“ je nastaveno na „Úspěch a neúspěch“

Podrobné sledování

Audit 'PNP Activity' je nastaven na 'Success'
Audit 'Process Creation' je nastaven na 'Success'

Přihlášení/Odhlášení

Audit „Uzamčení účtu“ je nastaven na „Úspěch a neúspěch“
Audit „Členství ve skupině“ je nastaven na „Úspěch“
Audit „Odhlášení“ je nastaven na „Úspěch“
Audit „Přihlášení“ je nastaven na „Úspěch a neúspěch“
Audit „Jiné přihlášení“ /Události odhlášení' je nastaveno na 'Úspěch a neúspěch'
Audit 'Speciální přihlášení' je nastaveno na 'Úspěch'

Přístup k objektu

Audit „Vyměnitelné úložiště“ je nastaven na „Úspěch a selhání“

Změna zásad

Audit 'Změna zásad auditu' je nastavena na 'Úspěch a neúspěch'
Audit 'Změna zásad ověřování' je nastavena na 'Úspěch'
Audit 'Změna zásad autorizace' je nastavena na 'Úspěch'

Privilegované použití

Audit 'Sensitive Privilege Use' je nastaven na 'Success and Failure'

Systém

Audit „Ovladač IPsec“ je nastaven na „Úspěch a neúspěch“
Audit“ Jiné systémové události“ je nastaven na „Úspěch a neúspěch“
Audit „Změna stavu zabezpečení“ je nastaven na „Úspěch“
Audit „Rozšíření systému zabezpečení“ je nastaven na „Úspěch“ and Failure'
Audit 'Integrita systému je nastavena na 'Success and Failure'

Škodlivá aktivita často začíná na pracovních stanicích, pokud nemonitorujete všechny systémy, můžete přehlédnout první známky útoku.

V další části se budu zabývat tím, jaké události byste měli sledovat.

8. Monitorujte Active Directory, zda nevykazuje známky kompromisu

Měli byste sledovat následující události služby Active Directory, abyste pomohli zjistit ohrožení a abnormální chování v síti.

Zde jsou některé události, které byste měli každý týden sledovat a kontrolovat.

- Změny privilegovaných skupin, jako jsou Správci domén, Správci podniků a Správci schémat
- Nárůst pokusů o špatné heslo
- Nárůst uzamčených účtů
- Uzamčení účtu
- Zakázáno nebo odebrání antivirového softwaru
- Všechny aktivy prováděné privilegovanými účty
- Události přihlášení/odhlášení
- Použití účtů místního správce

Jak monitorujete události v Active Directory?

Nejlepším způsobem je shromáždit všechny protokoly na centralizovaném serveru a poté použít software pro analýzu protokolů ke generování zpráv.

Některé analyzátory protokolů jsou předpřipraveny se zprávami zabezpečení služby Active Directory a jiné si budete muset vytvořit sami.

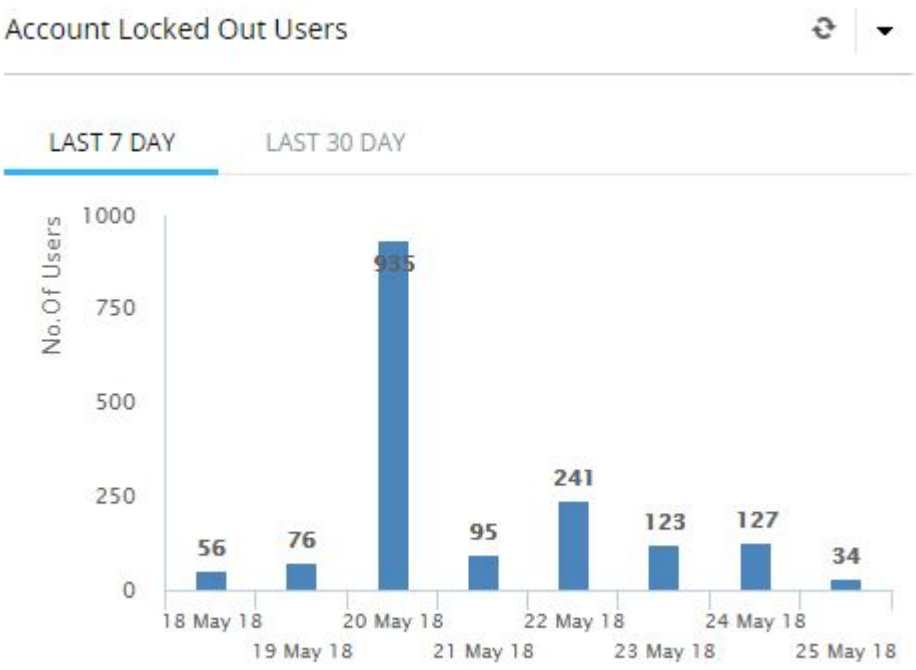
Zde jsou některé z nejpopulárnějších analyzátorů protokolů.

- Elk Stack
- Lepid
- Splunk
- ManageEngine ADAudit Plus
- Předávání událostí systému Windows

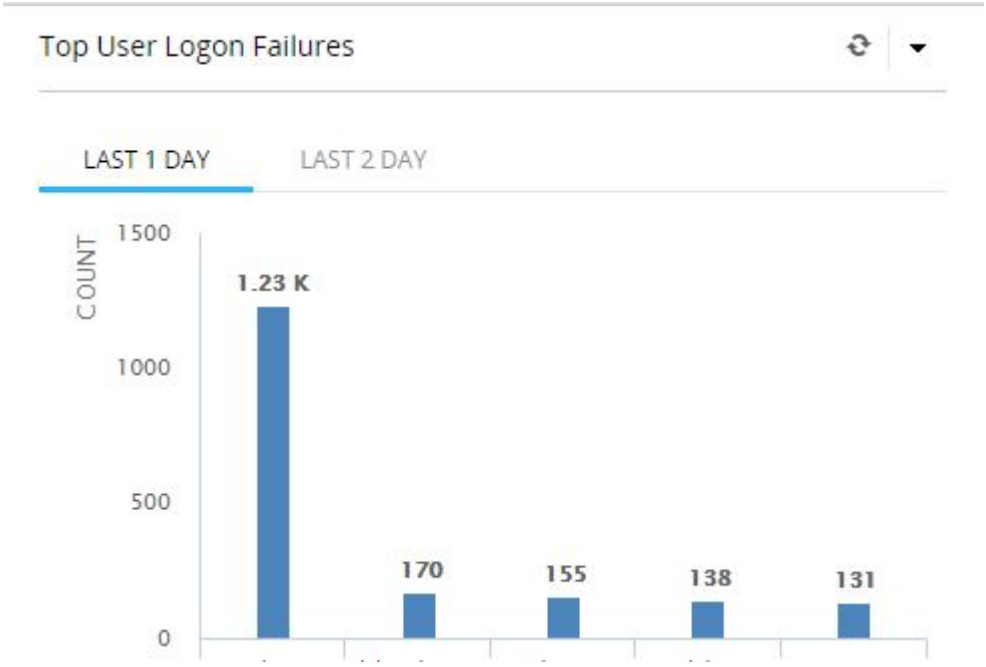
S dobrým analyzátorem protokolů budete schopni rychle odhalit podezřelou aktivitu ve vašem prostředí Active Directory.

Zde je několik snímků obrazovky z analyzátoru, který používám. První snímek obrazovky ukazuje prudký nárůst uzamčení účtů.

To rozhodně není normální.



Na tomto snímku obrazovky můžete vidět obrovský nárůst selhání přihlášení. Bez analyzátoru protokolů by tyto události bylo těžké zjistit.



9. Složitost hesla je na hovno (použijte přístupové fráze)

8 složitých znaků již není bezpečné heslo. Místo toho použijte minimálně 12 znaků a trénujte uživatele na přístupové fráze.

Čím delší heslo, tím lépe.

Přístupové fráze jsou jednoduše dvě nebo více náhodných slov spojených dohromady. Pokud chcete, můžete přidat čísla a znaky, ale nekladl bych to jako požadavek.

Studie ukázaly, že když požadujete složitost, používá se podobným způsobem a poté se opakuje. Hackeři se toho chytli a nyní existují obrovské seznamy hesel (volně dostupné), které obsahují miliony snadno uhodnutelných hesel.

Znáte někoho, kdo používá taková hesla?

S@mmer2018 nebo zima 2018! června 2018 $

Jsou to příšerná hesla a lze je snadno uhodnout.

Dlouhá hesla a používání techniky passphrase ztěžují softwaru pro prolomení hesel a hackerům uhodnutí.

Lepší zásady hesel

- Nastavte hesla o 12 znacích
- Zapamatujte si 10 historie hesel
- používat přístupové fráze
- Zásada uzamčení 5 pokusů

Klíčem k používání přístupových frází je být u každého slova zcela náhodný. Nechcete psát větu, kde lze uhodnout další slovo.

Dobrá hesla pomocí přístupových frází

Bucketguitartire22
Screenjugglered
RoadbluesaltCloud

Výše uvedené příklady jsou zcela náhodné. Ty by praskly velmi dlouho a s největší pravděpodobností by je nikdo neuhádl.

Příklady špatných přístupových frází

Ireallylikepizza22
Theskyisblue44

NIST nedávno aktualizovala své pokyny k zásadám hesel ve speciální publikaci 800-63, aby řešila nové požadavky na zásady hesel.

Pokud vaše organizace musí splňovat určité standardy, ujistěte se, že tyto standardy podporují tato doporučení hesel.

Nezapomeňte také aktualizovat písemné zásady vaší společnosti.

10. Použijte popisné názvy skupin zabezpečení

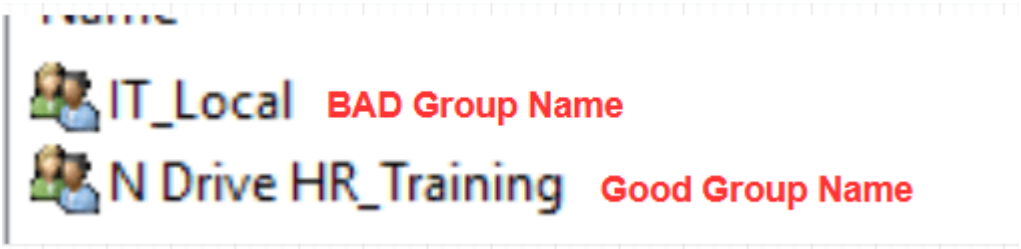
Nejprve se ujistěte, že používáte oprávnění ke zdrojům se skupinami zabezpečení, nikoli na jednotlivé účty, což značně usnadňuje správu zdrojů.

Dále nepojmenujte své bezpečnostní skupiny obecným názvem, jako je helpdesk nebo školení HR.

Když máte obecná jména, jako je tato, zvyknou si na všechny druhy zdrojů a vy ztratíte veškerou kontrolu nad bezpečností.

A neexistuje snadný způsob, jak zjistit, kde se skupiny zabezpečení používají. Ano, existují nástroje, které můžete spustit, ale pokud máte středně velké nebo velké prostředí, bude to obrovský úkol.

Zde je příklad



IT_Local je velmi obecné. Jen při pohledu na název nevím, k čemu se to používá. Ano, pravděpodobně to používá IT oddělení, ale kde?

Takto se oprávnění mohou vymknout kontrole a můžete skončit tím, že lidem zpřístupníte věci, ke kterým by neměli mít přístup. Některý správce systému může dostat žádost o přístup ke sdílené síťové složce IT oddělení a přidat uživatele do této skupiny. Ale neví, že skupina může být použita na jiných systémech. Nyní dal některým uživatelům plná oprávnění k jiným systémům.

Když použijete popisný název, jako je skupina „N Drive HR_Training“, můžete se na název podívat a mít dobrou představu o tom, k čemu slouží. V tomto příkladu je to pro jednotku N, je to pro HR a má něco společného s tréninkem. Váš IT personál by měl mít dobrou představu o tom, co to je, jen podle názvu.

Zde je reálný příklad toho, jak špatné názvy skupin mohou vést k problémům.

Pracoval jsem s klientem na vyčištění oprávnění k Active Directory. Existovalo několik skupin zabezpečení, které delegovaly oprávnění službě Active Directory.

Existovala skupina s názvem helpdesk, další skupina IS Support a další s názvem AD Modify.

Měl jsem dojem, že pouze zaměstnanci Helpdesku mají práva ke službě Active Directory resetovat hesla a odemknout účty.

Přijďte zjistit, že tyto skupiny byly použity pro jiné zdroje, jako je software helpdesku, síťové sdílení a tiskárny. Takže to zahrnovalo různé IT pracovníky.

Jakmile jsem tyto skupiny odstranil, dostal jsem telefonáty od programátorů a obchodních analytiků, kteří se ptali, proč už nemohou resetovat uživatelská hesla. Proč proboha programátoři resetují uživatelská hesla?

Vymazal bych přesný název skupiny zabezpečení, který by tomu zabránil.

Pokud nepojmenujete konkrétní skupinu zabezpečení, může to být úlovek pro oprávnění k mnoha dalším věcem.

Zde je několik dobrých příkladů, jak pojmenovat skupiny.

Příklad 1: Umožněte helpdesku resetovat hesla

Název skupiny zabezpečení: IT-Helpdesk-PW-Reset

Protože je název skupiny přesný, pomůže to zabránit jeho použití na jiných zdrojích, jako je tiskárna nebo sdílená síť.

Příklad 2: Povolte práva HR ke sdílené složce

Název skupiny zabezpečení: N Drive HR-Training-Folder-RW

Opět to má velmi konkrétní název a pomáhá identifikovat, k čemu by měl být použit.

Můžete přijít s vlastní konvencí pojmenování, stačí se upřesnit jménem a vyhnout se obecným názvům jednoslovných skupin.

11. Najděte a odstraňte neaktivní účty uživatelů a počítačů

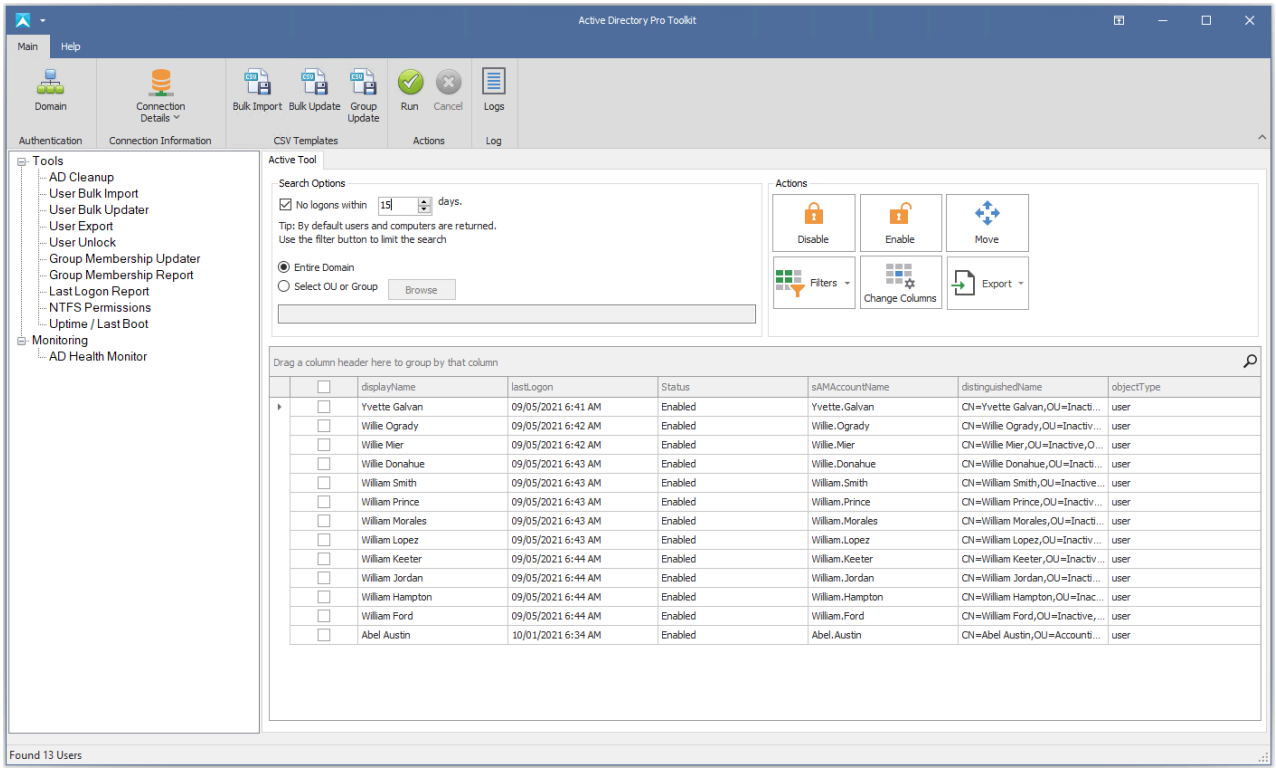
Musíte mít zaveden postup pro detekci neaktivních uživatelů a počítačových účtů ve službě Active Directory.

Nechcete, aby spousta nepoužívaných účtů seděla v Active Directory a čekala, až je útočník objeví a použije. To může také způsobit problémy s hlášením, opravami a zpomalením zásad skupiny.

CIS Critical Security Controls říká: „Existuje mnoho způsobů, jak skrytě získat přístup k uživatelským účtům, včetně slabých hesel, účtů stále platných poté, co uživatel opustí podnik, nečinných nebo přetrvávajících testovacích účtů“

CIS doporučuje smazat nebo deaktivovat spící účty po 45 dnech nečinnosti

Vytvořil jsem nástroj s názvem AD Cleanup Tool , který vám umožní rychle najít neaktivní uživatele a počítačové účty.



Pokud chcete další podrobnosti o hledání neaktivních uživatelů nebo o tom, jak to provést pomocí PowerShell, podívejte se na tento článek s názvem Hledání neaktivních uživatelů ve službě Active Directory

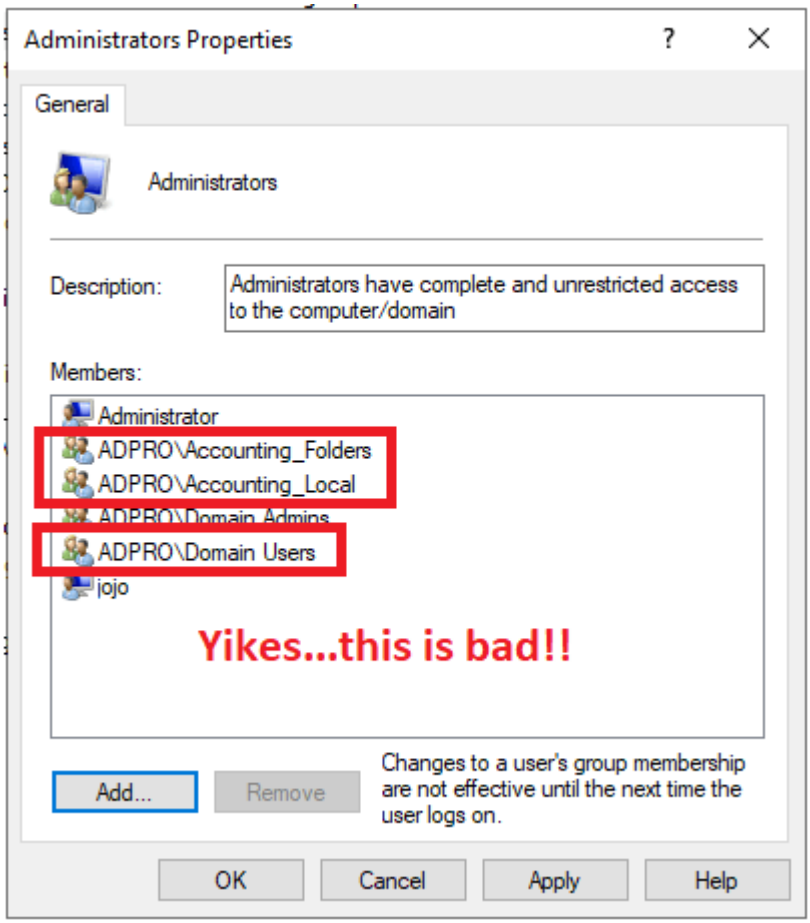
12. Odeberte uživatele z místní skupiny administrátorů

Běžný uživatel by neměl být v místní skupině správců na počítačích.

Uživatel s právy místního správce má plný přístup k celému operačnímu systému Windows. To může vést ke všem druhům bezpečnostních problémů, jako je instalace softwaru, deaktivace antiviru, stahování a instalace malwaru, krádež dat, hackování přihlašovacích údajů, přepínání na jiné počítače a tak dále.

Zpráva o zranitelnostech společnosti Microsoft říká:

„Ze všech zranitelností Windows objevených v roce 2018 bylo 169 z nich považováno za „kritické“. Odstranění administrátorských práv mohlo zmírnit 85 % těchto kritických zranitelností“



Odebráním uživatelů z místní skupiny správců výrazně omezíte možnosti útočníků získat přístup k vašemu počítači a síti.

Doporučuji ovládat skupinu místních správců pomocí zásad skupiny. Pokud je odeberete z počítače bez centralizovaného řízení, někdo práva jen přidá zpět. Tuto bitvu jsem vedl mnohokrát s helpdeskem. Odeberu práva a při řešení problému je prostě přidají zpět.

Použití skupinových zásad a omezených skupin zabrání vašim zaměstnancům opustit účty ve skupině.

Napsal jsem kompletního průvodce, podívejte se na to zde -> Odebrat uživatele ze skupiny místních správců pomocí zásad skupiny .

13. Neinstalujte další software nebo role serveru na DC

Řadiče domény by měly mít nainstalovaný omezený software a role.

DC jsou pro podnik zásadní, nechcete zvyšovat bezpečnostní rizika tím, že na nich běží další software.

Windows Server Core je skvělá volba pro spuštění role DC a dalších rolí, jako je DHCP, DNS, tiskové servery a souborové servery. Server Core běží bez grafického uživatelského rozhraní a vyžaduje méně bezpečnostních záplat kvůli menším rozměrům.

Jádro serveru může mít své problémy, ačkoli některý software třetích stran není kompatibilní.

14. Správa oprav a skenování zranitelnosti

Útočníci rychle využívají známé zranitelnosti.

Pokud pravidelně nekontrolujete a neopravujete objevené zranitelnosti, vystavujete se mnohem většímu riziku.

K dispozici je velké množství nástrojů pro zranitelnost a skenování, viz můj seznam nejlepšího softwaru pro správu oprav .

Tipy pro pokračující správu zranitelnosti

- Prohledejte všechny systémy alespoň jednou měsíčně, abyste identifikovali všechny potenciální zranitelnosti. Pokud můžete skenovat častěji, je to ještě lepší.
- Upřednostněte nalezení skenů zranitelnosti a nejprve opravte ty, které mají ve volné přírodě známé zranitelnosti.
- Nasaďte automatické aktualizace softwaru do operačních systémů
- Nasaďte automatické aktualizace softwaru třetích stran
- Identifikujte zastaralý software, který již není podporován, a nechte jej aktualizovat.

15. Použijte zabezpečené služby DNS k blokování škodlivých domén

Blokováním škodlivých vyhledávání DNS můžete zabránit pronikání velkého množství škodlivého provozu do vaší sítě.

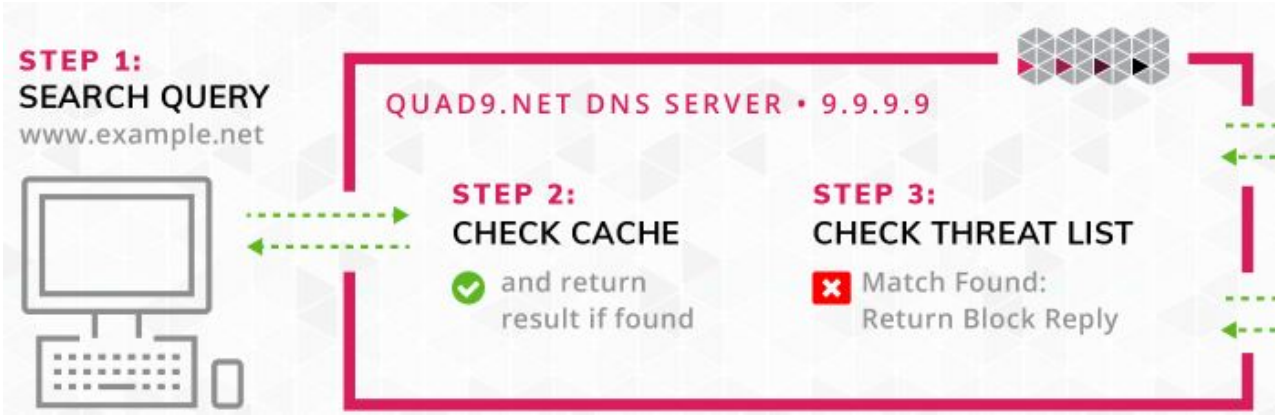
Kdykoli systém potřebuje přístup k internetu, ve většině případů použije název domény. Počítače spolu mluví pomocí IP adresy, takže počítače používají DNS k mapování názvu domény na IP adresu.

Existuje několik dostupných služeb, které kontrolují dotazy DNS na škodlivé domény a blokují je.

Jak to funguje?

Tyto služby DNS shromažďují informace o škodlivých doménách z různých veřejných a soukromých zdrojů. Když dostane dotaz na doménu, kterou označila jako škodlivou, zablokuje přístup, když se ji váš systém pokusí kontaktovat.

Zde je příklad:



Krok 1: Klient klikne na odkaz, který vede na example.net

Krok 2: Zkontroluje se místní mezipaměť

Krok 3: Služba DNS zkontroluje, zda je doména na seznamu hrozeb, takže vrátí odpověď blokování.

Ve výše uvedeném příkladu, protože dotaz DNS vrátil blok, do sítě nikdy nevstoupil žádný škodlivý provoz.

Zde jsou některé z nejoblíbenějších zabezpečených služeb DNS.

- Quad9
- OpenDNS
- Comodo Secure DNS

Momentálně používám Quad9, je zdarma a snadno se nastavuje.

Většina systémů IPS (Intrusion Prevention Systems) také podporuje možnost kontrolovat vyhledávání DNS proti seznamu škodlivých domén.

16. Spusťte podporované operační systémy

S každou novou verzí operačního systému Windows společnost Microsoft zahrnuje vestavěné funkce zabezpečení a vylepšení. A co je důležitější, získáte aktualizace zabezpečení.

Pouhé setrvání na nejnovějším operačním systému zvýší celkovou bezpečnost.

Nové funkce zabezpečení v Serveru 2022:

- Server se zabezpečeným jádrem
- Hardwarový kořen důvěry
- Firmwarová ochrana
- Zabezpečené spouštění UEFI
- Zabezpečení založené na virtualizaci

Zde je video od Roberta McMillena o funkcích zabezpečení na serveru 2002.

Watch Video At: https://youtu.be/nD7PTSYS5K8

17. Použijte dvoufaktorové ověřování pro Office 365 a vzdálený přístup

Kompromitované účty jsou velmi běžné a mohou útočníkům poskytnout vzdálený přístup k vašim systémům prostřednictvím VPN, Citrixu nebo jiných systémů vzdáleného přístupu.

Zkontrolujte své protokoly Office 365 nebo ADFS, budete překvapeni, kolik pokusů o přihlášení přichází z Číny a Ruska.

Jedním z nejlepších způsobů ochrany před napadenými účty je dvoufaktorové ověřování. To také pomůže proti útokům sprejování hesel.

Řekněme, že uživatel napadl pokus o phishing, který jej požádal o ověření uživatelského jména a hesla.

Nyní má útočník pověření služby Active Directory daného uživatele. Útočník by nyní mohl získat přístup k řadě systémů odkudkoli.

Pokud by měl uživatel povoleno dvoufaktorové nastavení, mohlo by to zabránit přístupu, i když byl účet kompromitován. Útočník by potřeboval druhou sadu přihlašovacích údajů, aby se mohl přihlásit.

Skutečně nic nezabrání tomu, aby byly účty kompromitovány, existuje příliš mnoho způsobů, jak mohou útočníci získat přihlašovací údaje.

Pokud používáte Office 365 a v závislosti na tom, jaký balíček máte, může být součástí MFA. Využijte této funkce.

Populární řešení dvoufaktorové autentizace

- DUO
- RSA
- Nastavení Office 365 MFA

18. Sledujte protokoly DHCP pro připojená zařízení

Pokud máte více míst se spoustou uživatelů a počítačů, měli byste vědět, co je připojeno k vaší síti, což může být náročné.

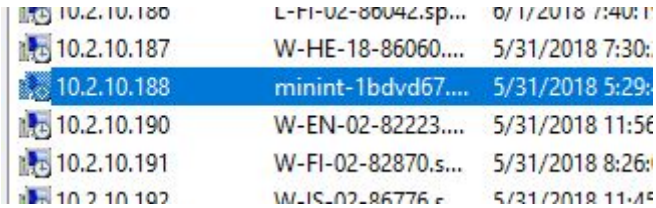
Existují způsoby, jak zabránit připojení pouze autorizovaných zařízení, ale to může být nákladné a může to být hodně práce na nastavení. Pokud máte prostředky, pak je to cesta.

Další metodou, kterou již máte k dispozici, je sledování protokolů DHCP pro připojená zařízení.

Měli byste mít všechna zařízení koncových uživatelů nastavena pro použití DHCP. Poté se můžete podívat do protokolů a zjistit, co se připojuje. Měli byste mít konvenci pojmenování pro vaše zařízení, což usnadní odhalení možných neautorizovaných zařízení.

Na níže uvedeném snímku obrazovky snadno najdu zařízení, které nesplňuje konvenci pojmenování mého počítače.

minint-1bdvd67 není něco, co uznávám. Musím se na to podívat a zjistit, zda je to autorizované zařízení.



19. Sledujte protokoly DNS na přítomnost škodlivé síťové aktivity

Většina připojení začíná dotazem DNS. Všechny systémy připojené k doméně by měly být nastaveny tak, aby používaly váš místní server DNS systému Windows.

S tímto nastavením můžete protokolovat každé interní a externí vyhledávání DNS. Když se klientské zařízení připojí ke škodlivému webu, zaznamená název tohoto webu do protokolů DNS.

Tyto škodlivé domény jsou obvykle liché domény s náhodnými znaky, které nevypadají normálně.

Zde je několik snímků obrazovky podezřelých vyhledávání DNS z mých protokolů. Tyto se opakovaně zobrazují v mých protokolech pro několik zařízení.

Vážně pochybuji, že se uživatel pokouší přejít na tento web úmyslně. Tyto druhy vyhledávání je třeba prozkoumat, abyste zjistili, zda jsou škodlivé nebo ne.

```
(3)b-0(11)19-a7000008(1)0(4)170c(4)22c7(4)2f4a(3)410(1)0(26)5b574pzbk36prdvz9m3il96i4t(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a7000008(1)0(4)170c(4)22c7(4)2f4a(3)410(1)0(26)5b574pzbk36prdvz9m3il96i4t(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a3000008(1)1(4)170c(4)22c7(4)2f4a(3)410(1)0(26)srd2mzbvmsqv7dmlsar1nvuazq(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a3000008(1)1(4)170c(4)22c7(4)2f4a(3)410(1)0(26)srd2mzbvmsqv7dmlsar1nvuazq(4)avts(6)mcafee(3)com(0)
```

```
NOERROR] A      (55)c-6rtwjumjzx7877x24lttlqjfix789x2elx2eitzgqjhqnhpx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A      (55)c-6rtwjumjzx7877x24lttlqjfix789x2elx2eitzgqjhqnhpx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A      (38)c-6rtwjumjzx7877x24fix2efrnstufdx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A      (33)c-6rtwjumjzx7877x24ix2eflpsx2ehtr(3)g00(3)msn(3)com(0)
```

Chcete-li zobrazit vyhledávání DNS, musíte nejprve povolit protokoly ladění DNS na serverech Windows.

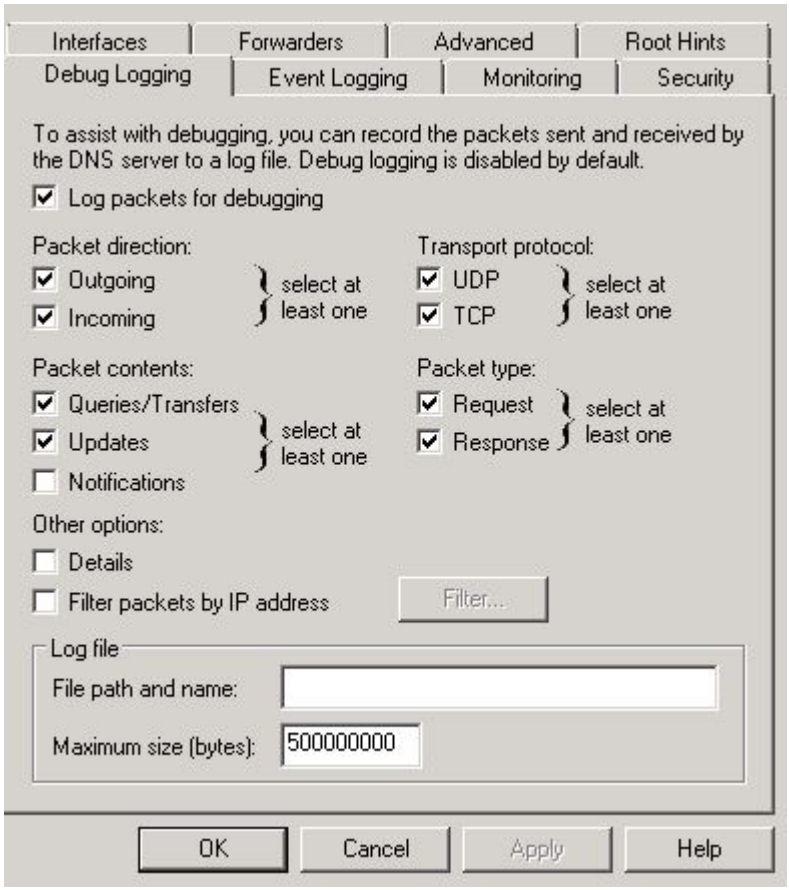
Kroky pro povolení protokolů ladění DNS na Windows Server

Krok 1: Otevřete konzolu pro správu DNS

Krok 2: Klikněte pravým tlačítkem a vyberte vlastnosti

Krok 3: Klepněte na kartu Protokolování ladění

Krok 4: Zaškrtněte políčko „Protokolovat pakety pro ladění



Jakmile budete mít nastavení protokolů ladění, můžete tyto protokoly importovat do analyzátoru, abyste rychle odhalili škodlivou aktivitu.

Soubor protokolu můžete také převést na CSV, aby bylo snazší číst a filtrovat.

20. Použijte nejnovější funkce ADFS a zabezpečení Azure

ADFS a Azure mají některé skvělé funkce zabezpečení. Tyto funkce pomohou se sprejováním hesel, kompromitací účtu, phishingem a tak dále.

Bez ohledu na to, na jaké úrovni Office 365 se nacházíte, existují některé funkce, na které byste se měli podívat.

Prémiové předplatné má samozřejmě nejlepší bezpečnostní funkce.

Ale

Microsoft vylepšuje a přidává nové funkce na každé úrovni (alespoň toho jsem si všiml od té doby, co jsem na Office 365).

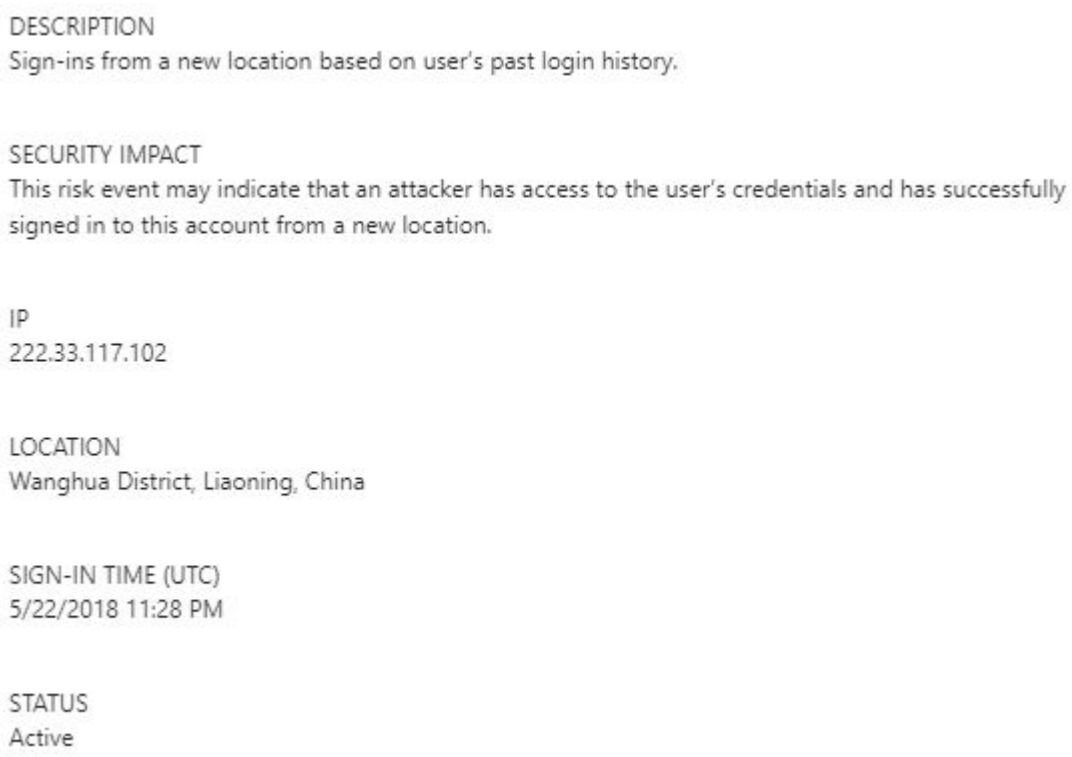
Zde je několik funkcí, které stojí za to prozkoumat:

- Inteligentní uzamčení – používá algoritmy k odhalení neobvyklé aktivity.
- IP Lockout – Používá databázi známých škodlivých IP adres společnosti Microsoft k blokování přihlášení.
- Simulace útoků – Měli byste provádět pravidelné testy phishingu, které vám pomohou vyškolit koncové uživatele. Microsoft velmi brzy uvolní software pro simulaci phish.
- MFA Authentication – dvoufaktorové řešení společnosti Microsoft
- Zakázaná hesla – Kontroluje hesla proti známému seznamu
- Azure AD Connect Health – poskytuje několik dobrých sestav
- Vlastní špatná hesla – Možnost přidat vlastní zakázaná hesla ke kontrole.

Momentálně používám hybridní nastavení Office 365. V azurové barvě vidím na hlášeních několik riskantních nápisů.

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE
High	Offline	Users with leaked credentials
Medium	Real-time	Sign-ins from anonymous IP addresses
Medium	Offline	Impossible travels to atypical locations
Medium	Real-time	Sign-ins from unfamiliar locations

Azure mě upozornil na přihlášení, které přišlo z Číny z jednoho z našich účtů.



Některé z těchto funkcí jsou dostupné v nejnovější verzi ADFS a některé jsou součástí předplatného Office 365.

Rozhodně se podívejte na všechny dostupné funkce zabezpečení v ADFS, Office 365 a Azure.

Zdroje:

Obrana proti útokům spreje hesel

21. Použijte Office 365 Secure Score

Skóre zabezpečení analyzuje zabezpečení vaší organizace Office 365 na základě aktivity a nastavení zabezpečení.

Secure Score zkontroluje vaše služby Office 365, poté zkontroluje vaše nastavení a aktivity a poskytne vám skóre zabezpečení.

Jakmile analyzuje vaše skóre, poskytne podrobný seznam toho, co bylo skórováno, a doporučené akce k vyřešení problémů.

Pro přístup k této funkci budete potřebovat předplatné Premium nebo Enterprise a navíc vám bude muset být přidělena role globálního správce nebo vlastní role.

Microsoft pokračuje v rozšiřování a přidávání dalších funkcí do Secure Score.

Pokud máte k této funkci přístup, využijte ji.

Další podrobnosti najdete v mém článku Doporučené postupy zabezpečení Office 365 .

22. Mějte plán obnovy

Pokud by byla vaše síť dnes ohrožena nebo zasažena RansomWare, co byste udělali?

- Máte zásady odezvy?
- Vyzkoušeli jste a proškolili personál, jak takovou akci zvládnout?
- Máte zálohu stavu systému aktivního adresáře ? Toto je nutnost pro případ, že potřebujete obnovit doménu ze zálohy.

Kybernetické útoky mohou vypnout systémy a zastavit obchodní operace.

Město Atlanta bylo uzavřeno kybernetickým útokem, který obyvatelům zabránil platit účty za služby online. Policisté navíc museli sepisovat hlášení ručně.

Naposledy jsem zkontroloval, že jejich zotavení z útoku stálo více než 5 milionů dolarů.

Dobrý plán reakce na incidenty by mohl omezit dopad a umožnit, aby byly služby online mnohem rychleji.

Zde je několik věcí, které je třeba zahrnout do plánu reakce na incidenty

- Vytvořte politiku a plán reakce na incidenty
- Vytvořte postupy pro provádění řešení a hlášení incidentů
- Stanovte postupy pro komunikaci s vnějšími stranami
- Vytvořte reakční týmy a vedoucí
- Upřednostňujte servery
- Návod a školení

NIST má skvělého průvodce řešením počítačových bezpečnostních incidentů , na který se doporučuji podívat.

23. Dokument Delegace do AD

Nejlepším způsobem, jak řídit přístup ke službě Active Directory a souvisejícím zdrojům, je použití skupin zabezpečení.

Pokud delegujete práva na jednotlivce, ztrácíte kontrolu nad tím, kdo má přístup.

Vytvářejte vlastní skupiny s velmi specifickými názvy, dokumentujte, kdo má práva, a procesem přidávání nových uživatelů. Nepovolujte pouze přidávání uživatelů do těchto vlastních skupin bez schvalovacího procesu. To je jen další způsob, jak se oprávnění mohou vymknout kontrole.

Zjistěte, jaké skupiny jsou delegovány na jaké zdroje, zdokumentujte to a ujistěte se, že váš tým je na stejné stránce.

24. Uzamčení servisních účtů

Účty služeb jsou účty, které spouštějí spustitelný soubor, úlohu nebo službu, ověřování AD atd.

Ty se hojně používají a často mají heslo nastavené tak, aby nikdy nevypršelo.

Tyto účty často skončí s příliš mnoha oprávněními a častěji jsou členy skupiny doménových administrátorů.

Špatné..velmi špatné

Někdy to navrhne prodejce.

Nedovolte, aby se to stalo, existují způsoby, jak to zajistit bez přístupu DA.

Zde je několik tipů pro uzamčení servisních účtů.

- Místo toho použijte účty spravovaných služeb
- Používejte dlouhá silná hesla
- Poskytněte přístup pouze tomu, co je potřeba
- Pokuste se vyhnout udělení práv místního správce
- Nevkládejte do Domain Admins
- Odmítnout přihlášení lokálně
- Odepřít přihlášení jako dávku
- Vyžadovat od dodavatelů, aby jejich software fungoval bez práv správce domény

25. Používejte základní linie zabezpečení a srovnávací testy

Výchozí instalace operačního systému Windows má mnoho funkcí, služeb, výchozích nastavení a povolených portů, které nejsou zabezpečené.

Tato výchozí nastavení by měla být porovnána se známými srovnávacími testy zabezpečení.

Zavedením bezpečné konfigurace na všech systémech lze snížit plochu útoku při zachování funkčnosti. Existuje několik zdrojů, které poskytují srovnávací testy zabezpečení.

Společnost Microsoft má sadu Security Compliance Toolkit , která vám umožňuje analyzovat a testovat podle doporučených zásad konfigurace zabezpečení společnosti Microsoft.

Dalším skvělým zdrojem je CIS SecureSuite

Poskytuje také základní linie konfigurace zabezpečení. Kromě toho poskytuje nástroje, které mohou skenovat systém a poskytovat zprávu o poruchách.

Většinu doporučených nastavení lze nastavit pomocí zásad skupiny a nasadit na všechny počítače.

Zde je snímek obrazovky nástroje CIS Securesuite. Provedl sken v mém počítači a vygeneroval zprávu o všech nastaveních, která prošla a selhala.

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	**5**	**4**	**0**	**0**	**5.0**	**9.0**	**56%**
1.1 Password Policy	2	4	0	0	2.0	6.0	33%
1.2 Account Lockout Policy	3	0	0	0	3.0	3.0	100%
2 Local Policies	**63**	**41**	**0**	**0**	**63.0**	**104.0**	**61%**
2.1 Audit Policy	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	12	0	0	27.0	39.0	69%
2.3 Security Options	36	29	0	0	36.0	65.0	55%
2.3.1 Accounts	2	4	0	0	2.0	6.0	33%
2.3.2 Audit	1	1	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	2	0	0	0.0	2.0	0%
2.3.5 Domain controller	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	5	3	0	0	5.0	8.0	62%
2.3.8 Microsoft network client	2	1	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	1	4	0	0	1.0	5.0	20%
2.3.10 Network access	8	4	0	0	8.0	12.0	67%
2.3.11 Network security	2	7	0	0	2.0	9.0	22%
2.3.12 Recovery console	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	1	0	0	0.0	1.0	0%
2.3.15 System objects	2	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	7	2	0	0	7.0	9.0	78%
3 Event Log	0	0	0	0	0.0	0.0	0%

CIS Securesuite může také skenovat proti jiným systémům, jako je Cisco, VMware, Linux a další.

Kontrolní seznam zabezpečení služby Active Directory

Stáhněte si tuto příručku ve formátu jednoduchého kontrolního seznamu. Obsahuje 3 bonusové bezpečnostní tipy.

Stáhnout kontrolní seznam ve formátu PDF

Doufám, že vám můj seznam osvědčených postupů zabezpečení služby Active Directory byl užitečný.

Máte-li dotaz nebo komentář, napište jej níže.