Complimenten van:

ManageEngine

Interne bedreigingen en aanvallen detecteren

Aanvallen in realtime bewaken/melden

Vals-positieve meldingen verminderen

Analyses van gebruikersgedrag toepassen

Speciale editie van ManageEngine

Derek Melber, MVP

Over ManageEngine

ManageEngine biedt de hulpmiddelen voor realtime IT-beheer waarmee een IT-team de benodigde realtimediensten en ondersteuning kan leveren aan organisaties. Wereldwijd vertrouwen meer dan 60.000 gevestigde en nieuwe bedrijven, waarvan meer dan 60 procent in de Fortune 500-lijst voorkomt, op ManageEngine-producten om te verzekeren dat hun essentiële IT-infrastructuur zoals netwerken, servers, toepassingen, desktops en meer optimale prestaties levert. ManageEngine is een onderdeel van Zoho Corp. en heeft kantoren over de hele wereld, waaronder de Verenigde Staten, het Verenigd Koninkrijk, India, Japan en China.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Interne bedreigingen en aanvallen detecteren

Speciale editie van ManageEngine

door Derek Melber, MVP

for dummies®
A Wiley Brand

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Detecting Insider Threats & Attacks For Dummies®, (interne bedreigingen en aanvallen detecteren voor beginners) speciale editie van ManageEngine

Gepubliceerd door
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774 (VS)
www.wiley.com
Auteursrecht © 2020 door John Wiley & Sons, Inc., Hoboken, New Jersey (VS)
Geen enkel deel van deze publicatie mag worden gereproduceerd, opgeslagen in een ophaalsysteem of verzonden in welke vorm of op welke manier dan ook, elektronisch, mechanisch, door kopiëren met foto's, opnames, scannen of anderszins, behalve zoals toegestaan onder secties 107 of 108 van de 1976 United States Copyright Act zonder de voorafgaande schriftelijke toestemming van de uitgever. Verzoeken om toestemming aan de uitgever moeten worden gericht aan de Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030 (VS), (201) 748-6011, fax (201) 748-6008, of online via http://www.wiley.com/go/permissions.
Handelsmerken: Wiley, For Dummies, het Dummies Man-logo, Dummies.com en gerelateerde handelskleding zijn handelsmerken of gedeponeerde handelsmerken van John Wiley & Sons, Inc. en/of diens dochterondernemingen in de Verenigde Staten en andere landen, en mogen niet worden gebruikt zonder schriftelijke toestemming. ManageEngine en het ManageEngine-logo zijn handelsmerken of gedeponeerde handelsmerken van Zoho Corp. Alle andere handelsmerken zijn eigendom van hun respectievelijke eigenaren. John Wiley & Sons, Inc.is niet geassocieerd met enig product of leverancier genoemd in dit boek.

AANSPRAKELIJKHEIDSBEPERKING/AFWIJZING VAN GARANTIE: DE UITGEVER EN DE AUTEUR GEVEN GEEN VERKLARINGEN OF GARANTIES MET BETREKKING TOT DE NAUWKEURIGHEID OF VOLLEDIGHEID VAN DE INHOUD VAN DIT WERK EN WIJZEN IN HET BIJZONDER ALLE GARANTIES AF, MET INBEGRIP VAN ZONDER BEPERKINGSGARANTIES VOOR EEN BEPAALD DOEL. GEEN GARANTIE KAN WORDEN GEMAAKT OF VERLENGD DOOR VERKOOP OF PROMOTIEMATERIAAL. HET ADVIES EN DE STRATEGIEËN DIE HIER ZIJN OPGENOMEN, ZIJN MOGELIJK NIET GESCHIKT VOOR ELKE SITUATIE. DIT WERK WORDT VERKOCHT MET HET BEGRIP DAT DE UITGEVER NIET BETROKKEN IS BIJ WETTELIJKE, BOEKHOUDENDE OF ANDERE PROFESSIONELE DIENSTEN. ALS PROFESSIONELE BIJSTAND VEREIST IS, MOETEN DE DIENSTEN VAN EEN BEVOEGDE PROFESSIONELE PERSOON WORDEN INGESCHAKELD. DE UITGEVER EN DE AUTEUR ZIJN NIET AANSPRAKELIJK VOOR SCHADE DIE HIERUIT ONSTAAT. HET FEIT DAT EEN ORGANISATIE OF WEBSITE IN DIT WERK IS OPGENOMEN ALS CITAAT EN/OF EEN POTENTIËLE BRON VAN VERDERE INFORMATIE BETEKENT NIET DAT DE AUTEUR OF DE UITGEVER DE INFORMATIE DIE DE ORGANISATIE OF WEBSITE KAN AANBIEDEN OF AANBEVELINGEN KAN AANBRENGEN. VERDER MOETEN LEZERS DAT DE WEBSITES KUNNEN ZIJN GEWIJZIGD OF OPGEHEVEN DIE IN DIT WERK WORDEN VERMELD, TUSSEN WANNEER DIT WERK GESCHREVEN IS EN WANNEER HET WORDT GELEZEN.

Voor algemene informatie over onze andere producten en diensten, of hoe u een aangepast *For Dummies*-boek kunt maken voor uw bedrijf of organisatie, kunt u contact opnemen met onze afdeling Business Development in de VS via 877-409-4177, info@dummies.biz of bezoek www.wiley. com/go/custompub. Neem voor informatie over licenties voor het merk *For Dummies* voor producten en diensten contact op met BrandedRights&Licenses@Wiley.com.
ISBN 978-1-119-65686-9 (pbk); ISBN 978-1-119-65685-2 (ebk)
Geproduceerd in de Verenigde Staten
10 9 8 7 6 5 4 3 2 1

Erkenningen van de uitgever

We zijn trots op dit boek en op de mensen die eraan hebben gewerkt. Enkele van de mensen die hebben geholpen dit boek op de markt te brengen:

Project Editor: Martin V. Minner

Acquisitions Editor: Ashley Coffey

Business Development Representative: Karen Hattan

Editorial Manager: Rev Mengle

Production Editor: Mohammed Zafar Ali

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Inleiding

Onderzoeken, rapporten en resultaten tonen aan dat interne dreigingen en aanvallen nog steeds groter zijn dan aanvallen van buiten de organisatie. De voor de hand liggende reden is dat interne medewerkers onmiddellijk toegang hebben tot het netwerk, met aanmeldingsgegevens voor toegang tot het netwerk. Beide zijn vereisten om een aanval uit te voeren, en interne personen hebben deze allebei standaard.

Waarom kunnen interne personen dan niet worden gedetecteerd bij het uitvoeren van een aanval? Het antwoord ligt in de standaard toegang. Als een gebruiker aanmeldgegevens en toegang tot het netwerk heeft, hoe kan dan een onderscheid worden gemaakt tussen goed en slecht gedrag? Beveiligingsprofessionals en beheerders proberen dit dilemma al jaren op te lossen.

Het goede nieuws is dat sommige afzonderlijke aanvallen in realtime kunnen worden bewaakt en gemeld. Deze aanvalsdetecties zijn 100 procent nauwkeurig en kunnen organisaties helpen tegen interne aanvallen. Zonder aanvullende technologieën kunnen de meeste aanvallen echter niet 100 procent worden geverifieerd. Veel organisaties gebruiken oplossingen voor beveiligingsinformatie en bewaking van gebeurtenissen (Security Information and Event Monitoring, SIEM), die technologieën bieden zoals drempelwaarden, regels en correlatie. Maar deze detecteren niet altijd 100 procent nauwkeurig.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Over dit boek

Veel organisaties wenden zich tot gebruikers- en entiteitsgedragsanalyses (User and Entity Behavior Analytics, UEBA) en gebruikersgedragsanalyses (User Behavior Analytics, UBA) om hun SIEM-technologie te helpen aanvallen nauwkeuriger en breder te detecteren. UEBA/UBA kunnen detecteren wat een traditionele SIEM niet kan door te zoeken naar vreemd gedrag van gebruikers, *anomalieën* genoemd. Deze kunnen wijzen op duidelijke aanvallen.

In dit korte boek bekijk ik gebruiksvoorbeelden over hoe u met 100 procent nauwkeurigheid interne dreigingen en aanvallen kunt detecteren met traditionele SIEM-technologieën, evenals UEBA/UBA-technologieën en -concepten.

Symbolen gebruikt in dit boek

Ik gebruik soms symbolen om de aandacht te vestigen op belangrijk materiaal. Dit kunt u verwachten:


TIP

Dit symbool verwijst naar advies en andere nuttige weetjes.


ONTHOUD

Als u dit symbool ziet, geef ik een vriendelijke verwijzing naar nuttige informatie.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

IN DIT HOOFDSTUK

- **De basis voor aanvallen leren**
- **Gebruikersaccounts bewaken**
- **Veranderingen die aanvallen aangeven**

Hoofdstuk **1**

Aanmeldingsaanval len detecteren

Veel organisaties traceren mislukt aanmeldingen. Het volgen van mislukte aanmeldingen kan helpen bij forensisch onderzoek en bij het detecteren van een aanval met grof geweld. Ik merk echter dat de meeste organisaties een van de krachtigste indicatoren van een interne aanval missen.

Voordat u de aanval kunt detecteren, moet u de basis voor deze aanval begrijpen. Ik richt me op Microsoft Active Directory (AD), omdat dit wereldwijd het meest gebruikte netwerkbesturingssysteem is voor identiteits- en toegangsbeheer.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Elke werknemer met een Active Directory-gebruikersaccount kan een lijst met alle andere gebruikersaccounts in de database ophalen. Op dezelfde manier kan elke werknemer een lijst verkrijgen van elke AD-groep en de bijhorende leden. Dit omvat domeinbeheerders, bedrijfsbeheerders, schemabeheerders en beheerdersgroepen.


TIP

Elk oproep door Lightweight Directory Access Protocol (LDAP) en PowerShell kan de lijst met gebruikers en groepsleden verkrijgen.

Aanvallen detecteren op accounts

In het ideale geval willen aanvallers als bevoorrechte gebruikersaccount toegang krijgen tot het netwerk. Het is logisch dat de aanvaller in dit scenario zal proberen zich aan te melden als een van de gebruikersaccounts die zich in de bevoorrechte groepen bevinden.

Nu u de basis voor de aanval begrijpt, volgen hier enkele manieren om de aanval te detecteren.

Beheerdersaccounts

Beheerders willen graag weten waar ze zijn en wanneer ze zich aanmelden. Dus simpelweg controleren wanneer diens eigen gebruikersaccount zich niet kan aanmelden, geeft een beheerder een duidelijke indicatie dat deze wordt aangevallen.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Hier volgen aanwijzingen dat een beheerdersaccount wordt aangevallen:

- Als een beheerder een e-mail typt en een melding ontvangt dat diens gebruikersaccount zich niet kan aanmelden.
- Als een beheerder niet op kantoor is om een evenement bij te wonen en een melding ontvangt dat diens gebruikersaccount zich niet kan aanmelden.

Bevoorrechte accounts

Bevoorrechte accounts zijn die accounts die meer kunnen dan een standaard gebruikersaccount. Deze accounts worden meestal gebruikt voor databasebeheer, e-mailbeheer, serverbeheer, enz. Deze accounts zijn geen beheerders op het niveau van 'admin', maar hebben duidelijk de mogelijkheid om de belangrijkste aspecten van het netwerk te beheren.

Net als de beheerders uit het vorige voorbeeld hebben deze gebruikersaccounts een beperkte tijd waarop ze zich aanmelden. Dit geldt vooral wanneer ze mislukte aanmeldingen ervaren. In navolging van de aanpak van de voorgaande casus, zijn hier enkele voorbeelden van wanneer een van deze accounts duidelijk wordt aangevallen:

- Wanneer de SQL-databasebeheerder met verlof is en er wordt een waarschuwing geactiveerd dat diens gebruikersaccount een mislukte aanmelding heeft.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

» Wanneer een beheerder op het kantoor in New York werkt en een mislukte aanmelding zich voordoet op een pc in het kantoor in Londen.

Service-accounts

Service-accounts vormen een ander type gebruikersaccount dat duidelijke aanwijzingen voor aanvallen kan vertonen. *Service-accounts* zijn gebruikersaccounts die worden gebruikt om diensten te helpen verifiëren bij toegang tot het netwerk, andere servers en zelfs andere diensten. Voor de meeste netwerkdiensten zijn service-accounts vereist, zoals SQL, Exchange, SharePoint, enz.

Beste werkwijzen voor het beschermen van accounts

Hier zijn een paar beste werkwijzen voor service-accounts:

» Service-accounts zijn niet menselijk en kunnen hun eigen wachtwoorden dus niet wijzigen. Idealiter zou u de service-account zodanig moeten instellen dat deze het bijhorende wachtwoord niet kan wijzigen.

» Service-accounts zijn geconfigureerd om binnen de dienst zelf te functioneren. Daarom kan de service-account zich niet interactief aanmelden (vanaf het toetsenbord). Configureer idealiter de service-account zodanig dat deze zich niet interactief kan aanmelden.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

- Gebruik de ingebouwde beheerdersaccount niet.

Zelfs als u deze beste werkwijzen niet heeft gebruikt bij de configuratie, kunt u nog steeds duidelijke aanwijzingen krijgen dat een service-account wordt aangevallen. Hieronder volgen duidelijke aanwijzingen dat uw service-account wordt aangevallen:

- U heeft de aanmelding door de service-account beperkt tot server10, maar er wordt een mislukte aanmelding geregistreerd op werkstation100.
- U krijgt een melding dat een fout in de service-account is geregistreerd vanaf werkstation9.
- De service-account is geconfigureerd voor de dienst ACME. Deze wordt uitgevoerd op server50 in het kantoor in New York, maar er wordt een aanmeldingsfout geregistreerd op een werkstation in Londen.

Bewaking van gebruikersaccounts zonder beheerdersmachtigingen voor mislukte aanmeldingen

Idealiter wilt u zoveel mogelijk gebruikersaccounts controleren op mislukte aanmeldingen.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

De kernvereiste is dat er enige kennis moet zijn van de parameters voor de aanmeldingen bij gebruikersaccounts. Als u alle aanmeldingsfouten van gebruikersaccounts controleert en probeert een waarschuwing te ontvangen voor een mislukte aanmelding, resulteert dit in te veel waarschuwingen die geen duidelijke indicatie van een aanval geven.

Als de gebruikersaccount van Sally bijvoorbeeld maandagochtend om 8.00 uur een aanmeldingsfout aangeeft, wat geeft dan aan of dit Sally is die haar wachtwoord onjuist typt of een daadwerkelijke aanval? Zonder betere informatie over de gebruikersaccount van Sally is de waarschuwing mogelijk een vals-positieve indicatie van een aanval.

In dit geval is het voor gebruikersaccounts zonder beheerdersrechten misschien beter om drempelwaarden te gebruiken om een aanval aan te geven. Als een gebruiker bijvoorbeeld binnen 15 seconden vier mislukte aanmeldingspogingen doet, willen de meeste beheerders een melding ontvangen over deze activiteit.

TIP

Zorg ervoor dat uw drempelwaarde voor aanmeldingsfouten onder uw drempelwaarde voor accountvergrendeling ligt. Als uw drempelwaarde voor vergrendeling is ingesteld op drie en uw drempelwaarde voor mislukte aanmeldingspogingen op vier, zult u nooit een melding ontvangen over vier mislukte aanmeldingspogingen op de gebruikersaccount, omdat de account eerst wordt geblokkeerd.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Veranderingen aan groepen in domeinen met rechten detecteren

Een ander gebied binnen een Windows Active Directory waar het gemakkelijk is om aanvallen te herkennen, is gerelateerd aan groepen met rechten. Elke AD-installatie heeft dezelfde groepen met rechten die direct (OOB, Out Of the Box) worden geïnstalleerd. Zo weten aanvallers waar ze zich op moeten richten. Organisaties moeten echter verder kijken dan deze OOB-groepen met rechten om er zeker van te zijn dat ze alle groepen met rechten controleren die mogelijk zijn aangevallen.

Groepen met rechten kunnen worden onderverdeeld in drie categorieën: ingebouwd, dienst/toepassing en aangepast.

Ingebouwde groepen met rechten

Dit zijn groepen die worden geïnstalleerd op het moment dat AD voor het eerst wordt geïnstalleerd. De lijst met ingebouwde groepen met rechten die moeten worden bewaakt, omvat:

- Beheerders
- Domeinbeheerders
- Afdelingsbeheerders
- Eigenaren van aanmakers groepsbeleid

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Diensten- en toepassingengroepen

Diensten- en toepassingengroepen kunnen van organisatie tot organisatie sterk verschillen. Dit komt doordat sommige organisaties meer diensten en toepassingen binnen hun bedrijf nodig hebben dan andere organisaties. De sleutel is echter dat de groepen die zijn gemaakt om de geïnstalleerde diensten en toepassingen te kunnen beheren, moeten worden gedocumenteerd en gecontroleerd op wijzigingen. Voorbeelden van deze groepen kunnen zijn:

- Exchange-beheerders
- SQL-beheerders
- SharePoint-beheerders

Aangepaste groepen

Beheerders vertrouwen vaak op groepen die ze handmatig maken om machtigingen in te stellen en om toegang voor beheer te beperken of toe te staan. Ja, ingebouwde groepen bestaan voor dit doel. Maar bijna alle organisaties maken aangepaste groepen die gerelateerd zijn aan hun bedrijf in plaats van alleen te vertrouwen op de Microsoft-groepen. In bijna alle gevallen zijn deze aangepaste groepen lid van de ingebouwde groepen. De aangepaste groepen worden door de beheerders echter gebruikt om machtigingen en rechten te verlenen. Deze groepen moeten ook worden gedocumenteerd en gecontroleerd op wijzigingen.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Aanvallen op groepen in domeinen met rechten detecteren

Nu u de verschillende soorten groepen met rechten begrijpt, hoeft u de groepen alleen maar te controleren op wijzigingen. Ja, u moet het groepslidmaatschap ook kennen om er zeker van te zijn dat een onbekende wijziging een aanval is. Maar dat zou elke beheerder moeten willen. Als de huidige groepsleden niet bekend zijn, kunnen deze stappen u helpen de groepsleden te verifiëren en ervoor te zorgen dat ze correct zijn:

1. **Verkrijg een lijst van de leden van elke groep, tot op gebruikersniveau.**
2. **Geef de lijst aan de groepseigenaar, zodat deze de juiste leden kan verifiëren.**
3. **Werk de groep bij met de juiste leden.**


TIP

Om een lijst van elke groep op gebruikersniveau te ontvangen, kunt u een opdrachtregelprogramma, zoals PowerShell, of een grafisch hulpmiddel, zoals ADManager Plus, gebruiken.

Als het groepslidmaatschap correct is, is uw volgende stap om te controleren op veranderingen en het ontvangen van waarschuwingen te worden wanneer er een verandering optreedt, zoals weergegeven in Figuur 1-1. Hier zijn enkele praktijkgevallen die duidelijk op een aanval duiden:

» Uw organisatie heeft slechts drie domeinbeheerders en u krijgt een melding dat zojuist een gebruikersaccount van Financiën is toegevoegd aan de groep domeinbeheerders.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

- Er is een groep gemaakt die alleen service-accounts bevat en vervolgens wordt een waarschuwing gegenereerd dat het hoofd van het gebruikersaccount van HR zojuist aan deze groep is toegevoegd.
- Het bedrijf heeft besloten dat slechts twee gebruikers Exchange beheren. Vervolgens geeft een waarschuwing aan dat een gebruikersaccount van het verkoopteam is toegevoegd aan de groep Exchange-beheerders.

WHEN	WHERE	ACCOUNT NAME	ACCOUNT DOMAIN	CALLER USER NAME	MESSAGE
Jun 28 2019 11:44:37 AM	WINDOWS7	Administrators	ADSOLUTIONS.DEMO	daniel	Member 'Domain Admins' was added to Domain Local Security Group 'Administrators' by 'ADSOLUTIONS\daniel'.

FIGUUR 1-1: Een lokale groepswijziging.

Veranderingen detecteren aan lokale beheerdersgroep

Een lokale groep met rechten, beheerders, bevindt zich, net als domeingroepen met rechten, op elk werkstation en elke server die geen domeincontroller is in de Windows-omgeving. De lokale beheerdersgroep is een standaardgroep. Alle leden van deze groep kunnen de computer waarop deze groep zich bevindt bedienen. Ze hebben dan ook volledige controle over elk aspect van de computer.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Net als bij groepen met rechten, moet het lidmaatschap van de lokale beheerdersgroep op elke computer bekend zijn. Als het lidmaatschap bekend is en de beste werkwijzen voor lidmaatschappen worden gevolgd, dan helpt elke wijziging in deze groep een aanval aan te geven.

Hier volgen enkele beste werkwijzen voor de lokale beheerdersgroep op elke computer:

- Het lidmaatschap mag alleen domeinbeheerders en de lokale beheerdersaccount omvatten.
- Geen enkele gebruikersaccount, lokaal of domein, mag lid zijn van deze groep.
- In zeldzame gevallen, als een bedrijfstoepassing wordt gebruikt om computers te beheren, kan een service-account voor deze toepassing lid zijn van deze groep.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

IN DIT HOOFDSTUK

- **SIEM-regels, -drempelwaarden en correlaties herzien**
- **Weten wat SIEM niet zal detecteren**
- **Praktische UBA-gevallen doornemen**

Hoofdstuk **2**

Benutten en uitbreiden van SIEM-technologieën

Nu de lokale beheerdersgroep beperkt is tot domeinbeheerders, andere service-accounts en de lokale beheerdersaccount (zie hoofdstuk 1), mag het lidmaatschap van deze groepen niet veranderen, tenzij een 'admin' de wijziging aanbrengt. Als een waarschuwing wordt geactiveerd bij het controleren van wijzigingen aan een lokale beheerdersgroep op een Windows-computer, wijst dit duidelijk op een aanval.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

In deze context omvat *Windows-computer* alle domeinen: aangesloten Windows-computers, minus domeincontrollers. Dit omvat al uw lidservers en werkstations. Omdat het lidmaatschap van de lokale beheerdersgroep niet mag veranderen, zijn waarschuwingen zeldzaam. Als waarschuwingen optreden, onderscheiden deze zich van andere waarschuwingen en kan het IT-personeel onmiddellijk actie ondernemen.

Welke SIEM-regels goed werken en waar ze kunnen mislukken

SIEM-*regels* (Security Information and Event Management) weerspiegelen het meest elementaire van wat een SIEM-oplossing evalueert, bewaakt en meldt. SIEM-regels beschouwen doorgaans afzonderlijke gebeurtenissen om signalen te activeren die IT informeren over een mogelijk probleem.

Denk hierbij bijvoorbeeld aan mislukte aanmeldingen door gebruikers binnen uw Active Directory-domein (AD). Stel dat u een evenement bijwoont en niet op kantoor bent. Tijdens het evenement ontvangt u een e-mail van uw SIEM-oplossing. Hierin wordt aangegeven dat uw gebruikersaccount een mislukte aanmeldingspoging heeft ondervonden via een computer op uw bedrijfsnetwerk.

Deze aanmeldingsfout heeft slechts één mogelijke oorzaak: De realiteit is dat u wordt aangevallen.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

U kunt nu actie ondernemen door te kijken naar de details van de aanval, waar de aanval vandaan komt en of er andere aanmeldingsfouten zijn.

Alle accounts met rechten moeten worden gecontroleerd op aanmeldingsfouten. Elke aanmeldingsfout voor een account met rechten waarvoor geen reden is opgegeven, is duidelijk een aanval.

Deze regel voor mislukte aanmeldingen schiet tekort als u alle mislukte aanmeldingen controleert en de SIEM instelt om voor elke gebruikersaccount met een mislukte aanmelding waarschuwingen te verzenden. Gebruikers vergeten hun wachtwoord vaak een of meerdere keren. Dus het ontvangen van waarschuwingen voor mislukte aanmeldingen voor standaardgebruikers zou niet veel informatie opleveren.

Welke SIEM-drempelwaarden goed werken en wanneer kunnen ze mislukken

SIEM-oplossingen worden ook geleverd met *drempelwaarden.* Hiermee kunt u het systeem instellen om te zoeken naar een herhaalde gebeurtenis, die vervolgens een waarschuwing kan activeren. In veel gevallen betekent een enkele gebeurtenis in een typisch netwerk niet veel. Dezelfde gebeurtenis die in korte tijd meerdere keren wordt geactiveerd, kan echter duiden op een aanval.

Als ik het voorbeeld uit de vorige sectie over SIEM-regels gebruik en daarover uitweidt, kunt u zien hoe SIEM's drempelwaarden kunnen gebruiken. Het vorige voorbeeld met betrekking tot mislukte aanmeldingen kwam te kort toen u standaardgebruikers beschouwde.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Maar als er binnen 15 seconden vier mislukte aanmeldingen waren? Dit kan er zeker op wijzen dat de gebruikersaccount wordt aangevallen.

Als u een SIEM kunt instellen om te zoeken naar herhaalde gebeurtenissen voor dezelfde gebruikersaccount of hetzelfde apparaat, kunt u aanvullende informatie krijgen. Een standaardregel zou daar niet voor zorgen.


TIP

Stel de drempelwaarde niet zodanig laag in dat deze vals-positieve waarschuwingen veroorzaakt. Stel de drempelwaarde echter niet dusdanig hoog in dat de waarschuwing wordt gemist, omdat de drempelwaarde nooit wordt bereikt. Dit kan gebeuren als de drempelwaarde voor vergrendeling van het wachtwoordbeleid is ingesteld op vijf en u de drempelwaarde voor aanmeldingsfouten in uw SIEM instelt op zes.

Deze SIEM-functie mislukt als de gebruikersaccount wordt geopend met minder fouten dan de drempelwaarde. Als de account echt wordt aangevallen en de aanvaller met succes toegang krijgt tot de gebruikersaccount na slechts drie pogingen, maar de drempelwaarde is ingesteld op vier, wordt de waarschuwing nooit geactiveerd.

Welke SIEM-correlaties goed werken en waar ze kunnen mislukken

SIEM-oplossingen bieden nog een andere handige functie. *Correlatie* is een geavanceerde techniek die niet naar een enkele gebeurtenis kijkt, en zelfs niet naar herhaalde gebeurtenissen, zoals drempelwaarden.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

In plaats daarvan kan met correlatie gebeurtenissen op verschillende apparaten achter elkaar worden bekeken.

Correlatie is een “reverse-engineered” reeks gebeurtenissen die in de SIEM worden georganiseerd. Zo kan de SIEM zoeken naar het patroon van gebeurtenissen dat de aanval vertegenwoordigt.

Deze gebeurtenissen kunnen mislukte of gelukte aanmeldingen zijn, installatie van toepassingen, het starten van een dienst, het aanmaken van een gebruikersaccount, het wijzigen van toestemmingen, enz. Hier is een voorbeeld waarbij correlatie duidelijk op een aanval kan duiden:

1. Een standaard gebruikersaccount kent binnen 15 seconden vier mislukte aanmeldingen, gevolgd door een gelukte aanmelding binnen de volgende 15 seconden.
2. Binnen een minuut opent de gebruiker een bestandsserver om een dienst te installeren.
3. Na het installeren van de dienst wordt de gebruikersaccount toegevoegd aan een lokale groep met rechten. Vervolgens wordt de gebruiker toegevoegd als de service-account voor de nieuw geïnstalleerde dienst.
4. De laatste gebeurtenis is het starten van de dienst.

Als uw SIEM deze reeks gebeurtenissen meldt, heeft u een duidelijke indicatie van een mogelijke aanval die de dienst gebruikt om informatie te verzamelen en te verzenden.

Deze SIEM-functie kan mislukken als de gemaakte acties allemaal correct zijn. Vaak worden in een klein bedrijf gebruikersaccounts voor werknemers geconfigureerd om als diensten uit te voeren.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

De gebruiker kan diens wachtwoord zijn vergeten en zich vervolgens hebben aangemeld om de dienst te installeren en configureren.


TIP

Dit is de reden waarom automatische acties, zoals het afsluiten van de server, vaak niet zijn geconfigureerd om de normale verwerking van een server niet te verstoren in gevallen waarin uw SIEM zou kunnen 'denken' dat er een aanval is omdat er correlatiegebeurtenissen zijn aangetroffen.

Een voorbeeld van wat een traditionele SIEM zou missen

Traditionele SIEM-oplossingen zoeken goed naar afzonderlijke gebeurtenissen, herhaalde gebeurtenissen en zelfs complexe reeksen gebeurtenissen om aanvallen te detecteren. In veel gevallen is een SIEM-oplossing echter niet ontworpen om te zoeken naar bepaalde gebeurtenissen en situaties die duidelijk op een aanval duiden.

Als een kwaadwillende gebruiker zich bijvoorbeeld op uw netwerk op elk standaard gebruikersaccount probeert aan te melden met slechts één wachtwoord, merken traditionele SIEM-oplossingen dit niet op.


ONTHOUD

Eenmalige aanmeldingsfouten voor standaard gebruikersaccounts treden voortdurend op. Dus de meeste SIEM's zijn niet geconfigureerd om hiernaar te zoeken.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Wat is UEBA/UBA?

User and entity behavior analytics (UEBA) is een technologie die automatisch leren gebruikt om omvangrijke hoeveelheden gegevens over beveiligingsgebeurtenissen te analyseren om abnormaal gedrag van een gebruiker of apparaat te detecteren.

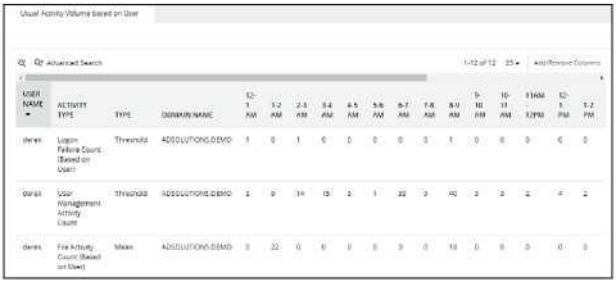
Met die definitie vraagt u zich misschien af hoe dit verschilt van andere SIEM-oplossingen. UEBA werkt met SIEM-oplossingen, maar analyseert de informatie op een ander niveau.

Traditionele SIEM-oplossingen en -regels beschouwen de binnenkomende gebeurtenissen als een unieke gebeurtenis of in correlatie met andere gebeurtenissen. Wanneer een gebeurtenis of reeks gebeurtenissen wordt bepaald, kan actie worden ondernomen. Natuurlijk kan de actie een script zijn, een toepassing activeren, een e-mail verzenden of een bericht op een computer achterlaten. Deze soort bewaking van gebeurtenissen is ideaal voor sommige situaties, zoals:

- Wijzigingen aan lidmaatschappen van beveiligingsgroepen
- Mislukte aanmeldingen door gebruikers met rechten
- Aanmeldingen bij service-accounts vanaf een niet-goedgekeurde computer
- Een beheerder dier zich probeert aan te melden op een non-Privileged Account Workstation (PAW, werkstation zonder accountrechten)

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Gebruikersgedragsanalyses (UBA, User Behavior Analytics) kijken niet afzonderlijk naar gebeurtenissen. In plaats daarvan kijkt UBA eerst naar elke gebruiker en talloze gedragingen om de basis te bepalen. Gedrag kan bijvoorbeeld mislukte aanmeldingen, aanmeldtijd, afmeldtijd, volume van binnen een dag geopende bestanden zijn, enz. Dit wordt weergegeven in Afbeelding 2-1. De basislijn wordt de 'normale activiteit' voor de gebruiker.



FIGUUR 2-1: Een basis bepalen voor normale activiteiten.


TIP

De meeste UBA-basisregels hebben 30 dagen nodig om geldig 'normaal gedrag' te ontwikkelen.


ONTHOUD

UBA is analyse van gebruikersgedrag, en UEBA staat voor analyse van gedrag door gebruikers en entiteiten. *Entiteit* kan een computer, switch, router, bestandsserver, enz., vertegenwoordigen. In dit boek kort ik UBA en UEBA af naar *UBA*.

Nadat u een basis heeft vastgesteld, worden alle aanvullende gebeurtenissen die onder deze basis vallen met de basis vergeleken. Elke nieuwe gebeurtenis die buiten het 'normale bereik' van de basis valt, wordt als *afwijking* beschouwd.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Afwijkingen zijn activeringen voor het uitvoeren van acties, het starten van toepassingen, het verzenden van e-mails, enz.

Praktische gevallen voor UBA onderzoeken

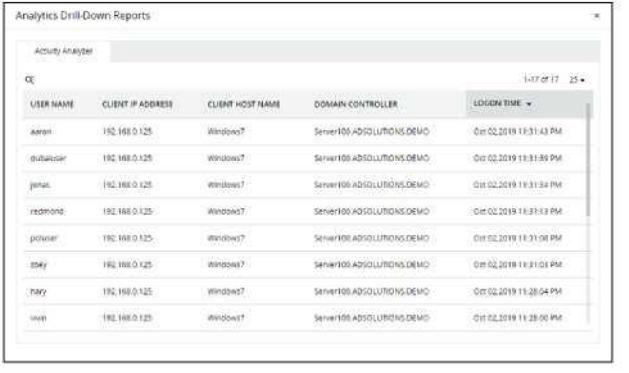
In eerdere delen van dit hoofdstuk wordt uitgelegd wat uw SIEM goed doet en waar uw SIEM de aanvallen die plaatsvinden mogelijk niet controleert. Door UBA aan uw SIEM toe te voegen, krijgt u meer diepgaande en wijd verspreide informatie over aanvallen wanneer deze zich voordoen. Sommige zijn, net als de vorige SIEM-voorbeelden, duidelijke indicatoren van een aanval en andere zijn slechts indicaties van een mogelijke aanval.

UBA kent beide niveaus van aanvalsindicatoren ook. In deze sectie behandel ik twee duidelijke indicaties dat er een aanval plaatsvindt. De mogelijkheid om aanvallen met UBA te detecteren, kan de manier veranderen waarop u uw omgeving beveiligt.

Een aanval op interne AD-gebruikersaccounts

Het eerste voorbeeld is een aanval op uw interne Active Directory-gebruikersaccounts. De aanval probeert één wachtwoord voor elk gebruikersaccount en wordt een *password spray attack* genoemd. Om de volledige breedte van de aanval en het onvermogen om deze aanval te detecteren aan te tonen, behandel ik alle aspecten van wat nodig is voor de aanval, hoe de aanval onopgemerkt kan blijven en hoe UBA deze aanval gemakkelijk in realtime detecteert. Dit wordt weergegeven in Figuur 2 -2.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.



FIGUUR 2-2: UBA gebruiken om een password spray attack te detecteren.

De password spray attack vereist eerst dat de aanvaller eerst de volledige lijst met namen van gebruikersaccounts uit Active Directory haalt.

TIP

Elke gebruiker met een AD-gebruikersaccount kan een volledige lijst met alle gebruikersaccounts uit Active Directory verkrijgen. Dit is mogelijk omdat alle gebruikers leestoegang hebben tot de map en daardoor deze informatie kunnen verkrijgen. De eenvoudige opdracht: net group/domein "domeingebruikers" geeft u een lijst van alle gebruikersnamen in het domein.

Zodra de volledige lijst met namen van gebruikersaccounts is verkregen, wordt een klein batchbestand gemaakt om elke gebruikersnaam met één wachtwoord te proberen.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Dit is een ideale aanval die de meeste SIEM's niet kunnen opvangen. Dit wordt veroorzaakt door de volgende redenen:

- Enkele mislukte aanmeldingen activeren geen waarschuwingen.
- Mislukte aanmeldingen op vele gebruikersaccounts worden niet gecontroleerd.
- Mislukte aanmeldingen worden niet per apparaat getraceerd.

Wanneer UBA wordt opgenomen in uw SIEM, wordt deze aanval echter snel gevonden en wordt een waarschuwing naar alle beheerders gestuurd om hen te informeren over de aanval, omdat UBA mislukte aanmeldingen zoekt voor een apparaat, die buiten de normale mislukte aanmeldingen vallen.

Een typisch werkstation ontvangt niet veel mislukte aanmeldingen op één dag, omdat de meeste gebruikers zich hoogstens een paar keer per dag aanmelden. Wanneer hetzelfde apparaat echter veel mislukte aanmeldingen kent tijdens de password spray attack, ziet UBA dat dit gedrag buiten de normale basis valt en wordt een waarschuwing geactiveerd.

Afwijkingen op UBA combineren

Een tweede voorbeeld is complexer, maar duidt ook op een duidelijke aanval. Deze UBA-techniek omvat het concept van het combineren van afwijkingen op UBA in een *over risk score*.

Het doel is niet om te kijken naar individuele afwijkingen, maar om te kijken naar dezelfde gebruiker of entiteit met veel afwijkingen in korte tijd.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Een enkele afwijking duidt mogelijk niet op een kwaadaardige bedoeling. Als zich in korte tijd veel afwijkingen voordoen door dezelfde gebruiker of entiteit, is de kans groot dat dit een aanval betreft.

Stel dat de gebruiker in het voorbeeld de volgende acties uitvoert, die allemaal afwijkingen veroorzaken in vergelijking met de basisregels:

- Vier mislukte externe aanmeldingen om 02:00 uur (dit veroorzaakt drie afwijkingen.)
- Een gelukte externe aanmelding om 02:00 uur (dit veroorzaakt twee afwijkingen.)
- Installatie van een dienst op het werkstation.
- De lokale dienst starten op het werkstation.
- Meer dan 1.000 bestanden openen op een bestandsserver.
- Wijzigingen aan registerinvoer op het lokale werkstation.

Elk van deze afwijkingen afzonderlijk zou geen problemen opleveren bij een traditionele SIEM. Als u echter naar het gedrag van de gebruiker kijkt, toegang tot het netwerk midden in de nacht, via een externe verbinding (wat zeldzaam is voor deze gebruiker) en vervolgens tien keer zoveel bestanden als normaal openen, zijn de acties niet normaal en vormen deze waarschijnlijk een aanval.

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

IN DIT HOOFDSTUK

» Schadelijk gedrag herkennen

» Interne aanvallen in de toekomst voorkomen

Hoofdstuk 3

Tien cruciale leerpunten

Incidenten als potentiële interne aanvallen identificeren is belangrijk om die aanvallen te stoppen en toekomstige aanvallen te kunnen voorkomen. Om aanvallen correct als zodanig te kunnen identificeren, moet u kunnen herkennen wat echt kwaadaardig gedrag is (wat wijst op een mogelijke aanval) en wat normaal zou kunnen zijn, zoals een gebruiker die zijn of haar wachtwoord vergeet.

Hier zijn tien belangrijke tips om uw organisatie te beschermen tegen interne bedreigingen en aanvallen:

» **Standaard toegang misleidt detectie van aanvallen.**

» **Bewaking van accounts met rechten is essentieel.**

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

- **User and Entity Behavior Analytics (UEBA) en User Behavior Analytics (UBA) ontdekken afwijkingen die traditionele SIEM-technologieën niet detecteren.**
- **Mislukte aanmeldingen bij gebruikersaccounts moeten worden bewaakt.**
- **Aanvallers willen netwerktoegang via een gebruikersaccount met rechten.**
- **Beveilig service-accounts met beste werkwijzen.**
- **Groepen moeten worden gecontroleerd op wijzigingen.**
- **Beste werkwijzen voor lokale beheerdersgroepen moeten worden opgevolgd.**
- **Service-accounts moeten worden bewaakt.**
- **Niets doen opent het netwerk voor geslaagde aanvallen.**

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

D

Appendix

Gratis hulpmiddelen

De hoofdstukken in dit boek geven inzicht in het beveiligen en bewaken van accounts met rechten. Voordat u begint met traceren en beveiligen, moet u echter weten wie en wat toegang heeft in uw omgeving. De hulpmiddelen in deze appendix helpen u deze doelen te bereiken. De hier genoemde hulpmiddelen bieden een gratis 30-daagse proefversie:

- **ADAudit Plus**

  www.manageengine.com/products/active-directory- audit/

- **EventLog Analyzer**

  www.manageengine.com/products/eventlog/

- **Log360**

  www.manageengine.com/log-management/

- **ADManager Plus**

  www.manageengine.com/products/ad-manager/

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

» **ADSelfService Plus**

www.manageengine.com/products/self-service- password/

» **DataSecurity Plus**

www.manageengine.com/data-security/

» **Exchange Reporter Plus**

www.manageengine.com/products/exchange- reports/

» **RecoveryManager Plus**

www.manageengine.com/ad-recovery-manager/

» **O365 Manager Plus**

www.manageengine.com/office365-management- reporting/

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Uitgebreide UEBA-oplossing

ManageEngine Log360

ManageEngine Log360 is een UEBA-hulpmiddel dat strengere beveiligingsmaatregelen afdwingt door gedragsafwijkingen te detecteren en uw verdediging tegen interne bedreigingen en **gegevenslekken** te versterken.

Log360 bevat meer dan 1000 vooraf gedefinieerde rapport- en waarschuwingsprofielen en gebruikt automatisch leren om te verdedigen tegen:

- Interne bedreigingen
- Account Compromise
- Gegevens uitfilteren

Scan QR-code

Probeer Log360 nu!

bit.ly/ManageEngine-Log360

Oplossing voor Active Directory-beveiliging

ManageEngine ADAudit Plus

ADAudit Plus is het onderdeel van Log360 dat in realtime wijzigingen controleert en analyses samenstelt en helpt bij het beveiligen van uw Active Directory, Azure AD, bestandsservers en andere Windows-servers..

ADAuditPlus stemt automatisch leren af voor het leveren van meldingen aan beveiligingspersoneel in het geval van:

- Schadelijke aanmeldingen
- Afwijkende veranderingen in activiteiten
- Gegevenslekken

Scan QR Code

Start uw gratis 30-daagse proefperiode nu!

bit.ly/ADAuditPlus

Deze materialen zijn © 2020 John Wiley & Sons, Inc. Elke verspreiding, distributie of elk ongeoorloofd gebruik is ten strengste verboden.

Interne bedreigingen en aanvallen detecteren

Veel organisaties wenden zich tot gebruikers- en entiteitsgedragsanalyses (User and Entity Behavior Analytics, UEBA) en gebruikersgedragsanalyses (User Behavior Analytics, UBA) om hun oplossingen voor beveiligingsinformatie en bewaken van gebeurtenissen (Security Information and Event Monitoring, SIEM) te helpen bij het detecteren van aanvallen. UEBA/UBA kunnen detecteren wat een traditionele SIEM niet kan door te zoeken naar vreemd gedrag van gebruikers, *anomalieën* genoemd. Deze kunnen wijzen op duidelijke aanvallen. In dit boek kunt u lezen hoe u, met 100 procent nauwkeurigheid, interne dreigingen en aanvallen kunt detecteren met behulp van traditionele SIEM-technologieën en UEBA/UBA.

Hierin...

- Aanvallen detecteren op accounts
- Aanmeldingen door gebruikers met rechten bewaken en meldingen hierover
- Veranderingen aan groepen met rechten traceren
- SIEM-regels, -drempelwaarden en correlaties begrijpen
- Weten wat SIEM niet kan detecteren
- Analyses van gebruikersgedrag afstemmen

Go to Dummies.com™
for videos, step-by-step photos,
how-to articles, or to shop!

for dummies®
A Wiley Brand

ManageEngine

Derek Melber is een voormalige MVP voor Microsoft MVP en Chief Technical Evangelist bij ManageEngine. Hij richt zich op Active Directory, groepsbeleid en beveiliging voor bedrijfsnetwerken. Derek heeft meer dan 15 boeken geschreven en door de jaren heen duizenden artikelen en blogs gepubliceerd. Derek onderwijst en evangeliseert elk jaar Microsoft-technologieën aan duizenden beheerders over de hele wereld. U kunt hem bereiken via derek@manageengine.com.

9 781119 656869

LICENTIE-OVEREENKOMST VOOR EINDGEBRUIKERS VAN WILEY

Ga naar www.wiley.com/go/eula voor de licentie-overeenkomst voor eindgebruikers van Wiley voor e-boeken.