DREI WEGE, WIE PRIVILEGIERTE BENUTZER IHR ACTIVE DIRECTORY LAHMLEGEN KÖNNEN

Und acht Möglichkeiten, Risiken zu minimieren und Ihre Wiederherstellungsmöglichkeiten zu verbessern

Quest

Einführung

EIN ABSCHRECKENDES BEISPIEL

Weil er unzufrieden mit seinem Bonus war, schrieb Roger Duronio, IT-Administrator bei UBS Paine Webber, 50 Zeilen Code und stellte diesen auf Tausenden Systemen im Unternehmensnetzwerk bereit – unter Verwendung derselben standardmäßigen Unix Admintools, die für die Bereitstellung von legitimen Dateien auf den Systemen genutzt werden.

Dann kündigte er.

Die von ihm platzierte Code-Bombe jedoch blieb im Unternehmen. Sie zählte zuverlässig die Wochen herunter, sodass Duronio genug Zeit hatte, 20.000 USD in den Leerverkauf von UBS/PW-Aktien zu investieren. Eines morgens dann platzte die Bombe. Berichten zufolge lautete der Payload „rm -rf /“, was soviel bedeutet wie ALLES löschen.

Es herrschte pures Chaos. UBS/PW musste auf Stift und Papier zurückgreifen, um Geschäfte abzuschließen. 3 Millionen USD musste das Unternehmen allein in Beratungsdienstleistungen von IBM investieren, um die Systeme von Sicherungen wiederherzustellen. Über die Gesamtkosten können wir nur Vermutungen aufstellen.

ÜBER DIESES DOKUMENT

Das ist nur ein Beispiel dafür, wie ein verärgerter oder nachlässiger privilegierter Benutzer Chaos anrichten kann.

In einer Windows Umgebung ist dies tatsächlich ziemlich einfach, da alles von Active Directory (AD) abhängt. Wenn Active Directory ausfällt, fällt auch Ihr gesamtes Netzwerk aus – auch wenn keine Probleme mit Ihren Servern und Anwendungen bestehen.

Wie einfach ist es? Dieses E-Book beschreibt nur drei der vielen Möglichkeiten, wie privilegierte Benutzer – oder Angreifer mit gestohlenen privilegierten Anmeldedaten – Ihr AD und gleichzeitig Ihr gesamtes Netzwerk außer Kraft setzen können.

Anschließend besprechen wir acht wichtige Best Practices, mit denen Sie die Risiken reduzieren und Ihre Möglichkeiten zur Wiederherstellung verbessern können, falls der schlimmste Fall eintritt.

Drei Wege, wie privilegierte Benutzer Ihr AD lahmlegen können

METHODE 1: ANMELDERECHTE VERWEIGERN

Benutzer haben fünf verschiedene Möglichkeiten, sich bei Windows anzumelden: lokal, über das Netzwerk, als Batchauftrag, als Service und über Remotedesktopdienste. Für jede dieser Anmeldemethoden gibt es zwei Anmeldeberechtigungen, eine zum Gewähren der Anmeldung und eine zum Verweigern der Anmeldung.

Durch eine entsprechende Zuweisung der fünf Berechtigungen zum Verweigern der Anmeldung können privilegierte Benutzer den Betrieb zum Stillstand bringen:

- Benutzer können sich nicht bei ihren Workstations anmelden.
- Administratoren erhalten auch bei Verwendung der lokalen Tastatur und des Bildschirms an der Konsole keinen Zugriff auf die Domänencontroller.
- Es ist keine Anmeldung bei Dienstkonten möglich.
- Anwendungen können nicht gestartet werden.

Dies ist ein doppeltes Dilemma: Da Sie sich nicht mit einem Domänenkonto anmelden können, können Sie das Problem auch nicht remote beheben. Stattdessen benötigen Sie physischen Zugriff auf Ihre DCs, damit Sie einen Neustart in den DSRM durchführen und den Betrieb aus diesem wiederherstellen können.

Durch eine entsprechende Zuweisung der Berechtigungen zum Verweigern der Anmeldung können privilegierte Benutzer den Betrieb zum Stillstand bringen.

METHODE 2: DNS AUSSER KRAFT SETZEN

Active Directory verwendet zur Lokalisierung von Domänencontrollern (DCs) DNS. Jede Windows Server 2003-basierte (oder später) Active Directory Domäne verfügt über einen DNS-Domänennamen und jeder Windows Server 2003 (oder später) Computer verfügt über einen DNS-Namen.

Um Ihr Active Directory lahmzulegen, muss alle DNS-Einträge auf einem DC löschen. Diese Änderungen werden dann unter Verwendung des zwischengespeicherten DNS in kürzester Zeit auf alle anderen DCs repliziert. Der DNS-Cache überschreitet das Zeitlimit und plötzlich ist nichts mehr auffindbar. Insbesondere können Workstations die Domänencontroller nicht mehr mithilfe von DNS finden. Sie greifen daher auf die NetBIOS-Namensauflösung zurück, was funktionieren kann, aber nicht zwangsläufig funktionieren muss.

Wenn DNS ausfällt, fällt auch alles andere aus.

Quest

METHODE 3: SCHWACHSTELLEN IM BETRIEBSSYSTEM AUSNUTZEN

Ein Unternehmen mit Windows Server 2008 stellte eines Tages fest, dass alle seine DCs sich in einem endlosen Neustartzyklus befanden. Es stellte sich heraus, dass ein privilegierter Benutzer eine IPv6-Einstellung in einem Subnetz zu einer ungültigen IP-Adresse geändert hatte. Als die ungültige Einstellung bei der Replikationseinrichtung über den Knowledge Consistency Checker (KCC) festgestellt wurde, schlug diese fehl. Dies führte zum Neustart des DC. Zuvor wurde die ungültige Einstellung jedoch auf alle anderen DCs in der gesamten Umgebung repliziert, sodass diese immer wieder neu gestartet wurden.

Durch unbekannte oder nicht behobene Schwachstellen kann Ihr AD lahmgelegt werden.

Microsoft hat bereits eine Fehlerbehebung für dieses Problem veröffentlicht, stellen Sie unter Windows 2008 oder 2008 R2 daher sicher, dass Sie alle aktuellen Patches installiert haben. Es besteht allerdings keine Garantie dafür, dass keine anderen Schwachstellen vorhanden sind, durch die privilegierte Benutzer vorsätzlich oder versehentlich ähnlich verheerende Konsequenzen hervorrufen.

Das Problem sind nicht nur verärgerte Insider

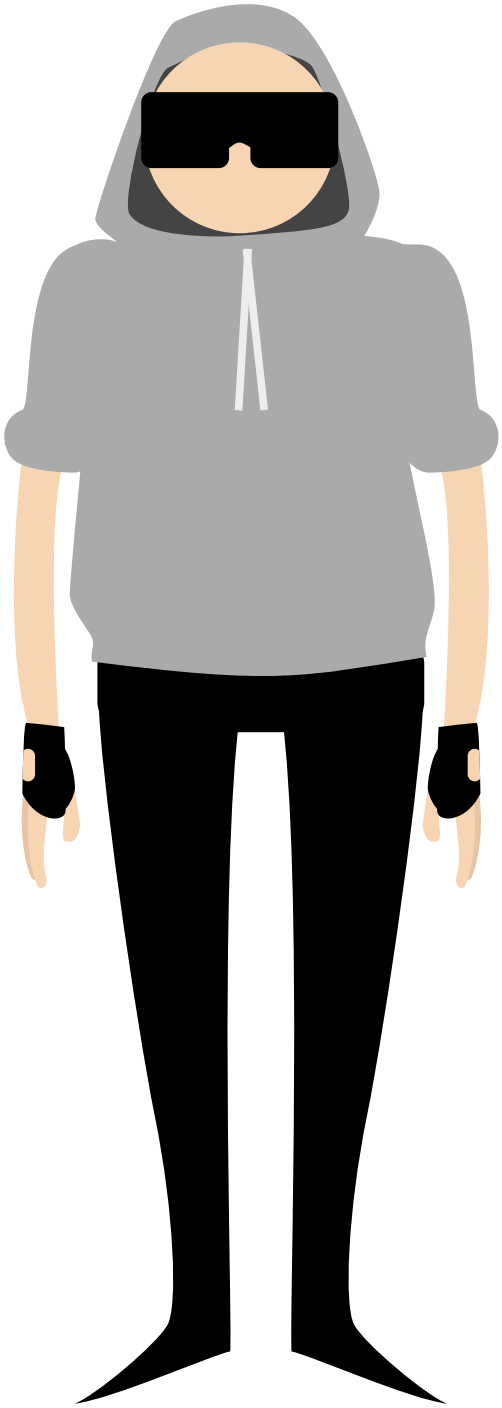
Zu viele Unternehmen versuchen, das Risiko solcher Szenarien mit der Behauptung zu verdrängen, dass es in ihrem Unternehmen keine verärgerten oder böswilligen privilegierten Benutzer gäbe, die zu Insider-Bedrohungen werden könnten. Selbst wenn es eine Möglichkeit gäbe, dies zum jetzigen Zeitpunkt und auch für die Zukunft zu garantieren, bestände aus zwei verschiedenen Gründen weiterhin ein gewisses Risiko. Zum einen machen auch die besten Administratoren Fehler – beispielsweise wie bei der soeben besprochenen, ungültigen IPv6-Einstellung. Darüber hinaus können privilegierte Anmeldedaten gestohlen und bei einem Cyber-Angriff missbräuchlich verwenden werden – und zwar durch Personen, die definitiv böswillige Absichten haben. Zu diesen zählen:

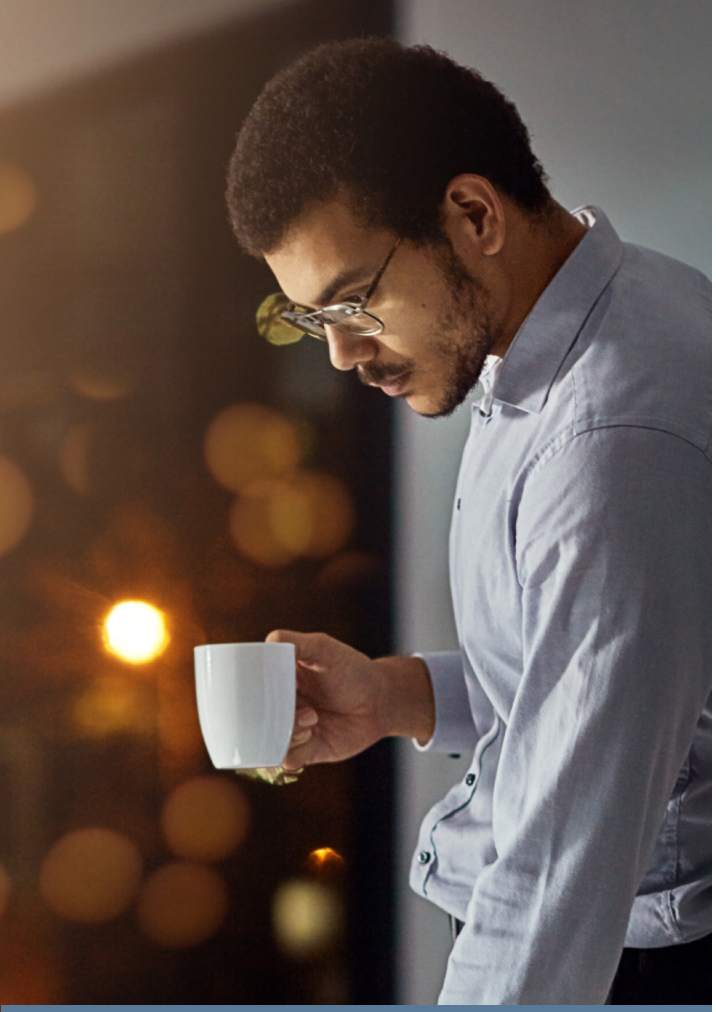
- Hacker
- Feindselige staatlich unterstützte Gruppen
- Wettbewerber
- Benachteiligte Parteien
- Nihilisten

Unternehmen sorgen sich gleichermaßen um Datensicherheitsverletzungen durch Nachlässigkeit, Fahrlässigkeit oder kompromittierte Anmeldedaten (51 %) wie um Datensicherheitsverletzungen durch böswillige Insider (47 %).

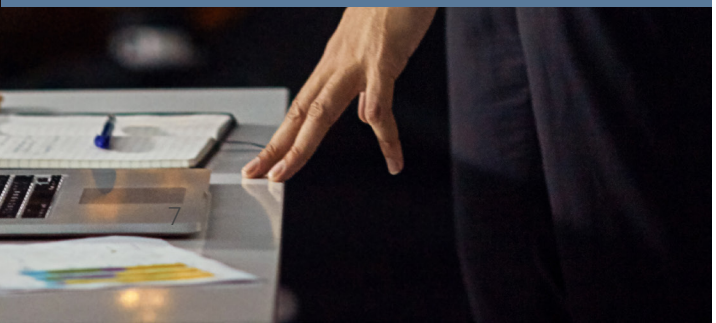
Quelle:** 2018 Insider Threat Report, **Cybersecurity Insiders

Beachten Sie, dass nicht alle diese Angreifer die Zeit und den Aufwand zum Stehlen Ihrer Daten investieren möchten. Einige möchten ganz einfach Ihre Dienste lahmlegen und Ihr Unternehmen schädigen, was deutlich einfacher ist.





Es ist unerlässlich, die Mitgliedschaft in privilegierten Benutzergruppen genau zu steuern.



Acht Best Practices für AD Sicherheit

Selbstverständlich stellen privilegierte Konten ein reales und erstes Risiko dar. Natürlich können Sie sie aber nicht einfach abschaffen, da sie für den Betrieb Ihrer Systeme unerlässlich sind. Glücklicherweise gibt es einige bewährte Schritte, die Sie ergreifen können, um das Risiko einer vorsätzlichen oder versehentlichen missbräuchlichen Verwendung zu reduzieren und sicherzustellen, dass Sie den Betrieb so schnell wie möglich wiederaufnehmen können, sollten diese vorbeugenden Maßnahmen fehlschlagen. Im Folgenden finden Sie acht wichtige Best Practices, die Sie implementieren sollten.

1. PRIVILEGIERTEN ZUGRIFF BESCHRÄNKEN.

Es ist unerlässlich, die Mitgliedschaft in privilegierten Benutzergruppen, wie den folgenden, genau zu steuern:

- Domänenadministratoren
- Unternehmensadministratoren
- Schemaadministratoren
- Administratoren
- DHCP-Administratoren
- Richtlinien-Ersteller-Besitzer
- Domänencontroller
- Netzwerkkonfigurations-Operatoren
- Server-Operatoren
- Sicherungs-Operatoren

Außerdem sollten Sie auch alle Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) genauestens steuern, die Auswirkungen auf Ihre Domänencontroller haben, sowie sämtliche Software, die auf den DCs installiert ist. Wenn beispielsweise ein Agent installiert ist, können Personen mit Zugriff auf diesen Agenten durchaus auch Domänenadministratoren sein.

Die beste Möglichkeit zur Steuerung von privilegiertem Zugriff ist die Verwendung einer vollwertigen Privilege Account Management (PAM)- und Privilege Session Management (PSM)-Lösung – mit von Personen erteilten Genehmigungen und Live-Überwachung von Zugriffsebenen, die Auswirkungen auf Ihre gesamte Domäne hätten. Da für Domänencontroller in der Regel keine tägliche Interaktion erforderlich sein sollte, ist es praktikabel, dass für sämtliche Aktionen zwei Personen anwesend sein müssen: eine Person, die die Aufgabe ausführt, und eine andere, die die Ausführung überwacht. Auch wenn die Überwachung remote durch einen Kollegen erfolgt, lässt sich dadurch das Risiko reduzieren, dass eine Einzelperson Ihrem Unternehmen schadet. Außerdem führen eine bessere Verantwortlichkeit und das Zwei-Augen-Prinzip zu einer Senkung des Risikos für kostspielige Fehler.

Quest

2. PRIVILEGIERTE KONTEN IN EINEM „RED FORREST“ SICHERN.

Es kann sehr schwierig sein, Produktionsgesamtstrukturen so zu härten, dass auch die wichtigsten privilegierten Administratorkonten ausreichend geschützt sind, ohne dass die Funktionalität in der Domäne leidet. Daher bietet Microsoft nun eine Möglichkeit, diese Konten in einer dedizierten administrativen Gesamtstruktur zu verwalten. Diese wird offiziell als Enhanced Security Admin Environment (ESAE) bezeichnet, trägt aber aufgrund der Wichtigkeit der Anmeldedaten inoffiziell den Namen „Red Forrest“.

Eine der wichtigsten Funktionen des Red Forest-Modells besteht darin, dass Administratorkonten in drei Sicherheitsebenen unterteilt werden:

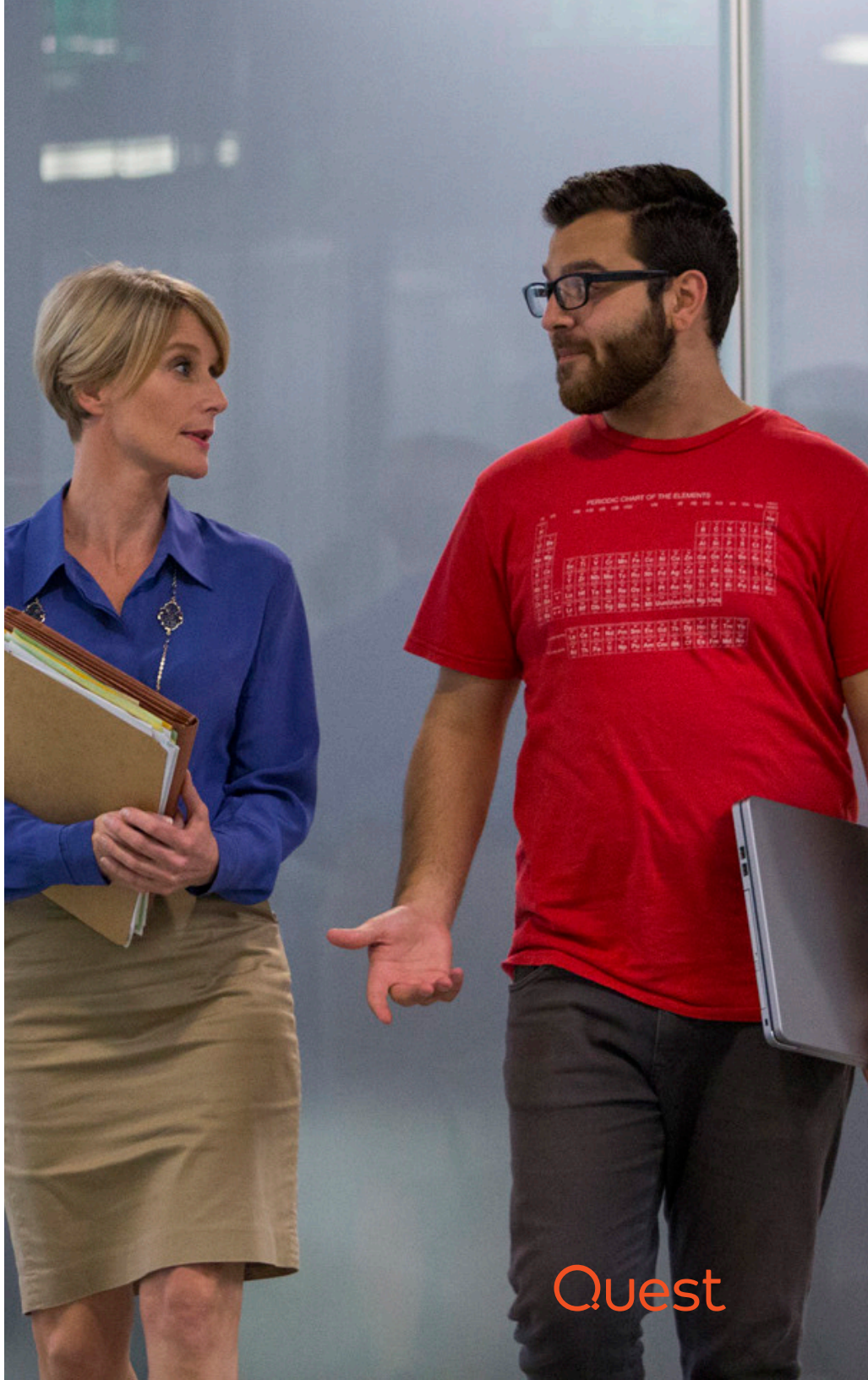
- **Ebene 0 –** Administratorrechte auf Gesamtstrukturebene (Unternehmensadministratoren)
- **Ebene 1 –** Administratorrechte für Server, Anwendungen und Cloud
- **Ebene 2 –** Administrative Steuerung von Workstations und Geräten

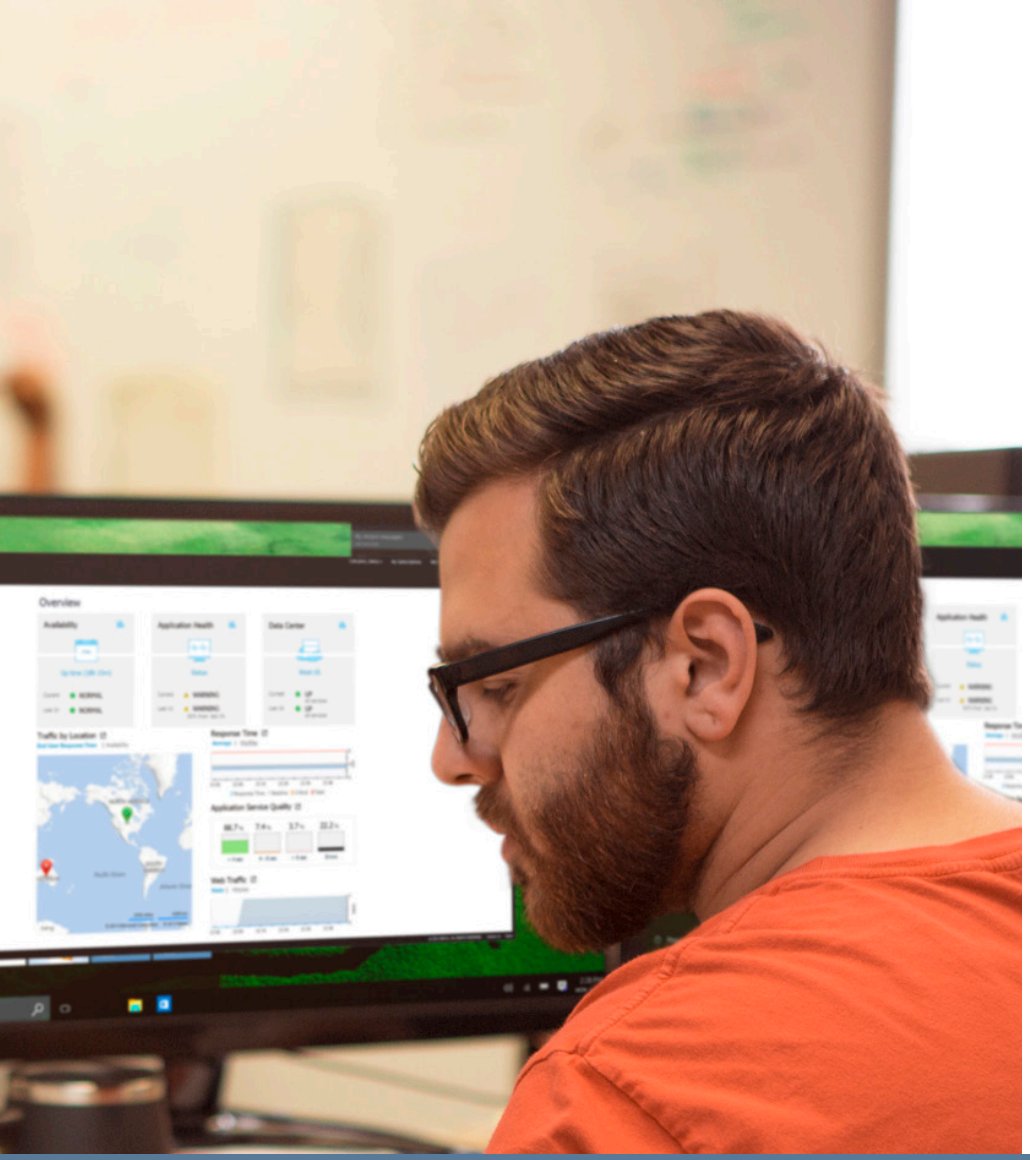
Indem Sie alle Konten der Ebene 0 in einer separaten Gesamtstruktur platzieren, können Sie sie genauer überwachen und einfacher zusätzliche Sicherheitsanforderungen anwenden. So können Sie zum Beispiel vorgeben, dass die Anmeldung über eine gehärtete Workstation erfolgen muss, oder Zwei-Faktor-Authentifizierung durchsetzen.

Natürlich ist die Bereitstellung einer administrativen Gesamtstruktur keine triviale Aufgabe. Weitere Informationen erhalten Sie in diesem aufgezeichneten Webcast, in dem Sicherheitsexperte Randy Franklin Smith erklärt, warum sich der zusätzliche Aufwand lohnt, und welchen Einschränkungen das Red Forest-Modell unterliegt.

3. ÄNDERUNGEN TESTEN, BEVOR SIE AN PRODUKTIONSSYSTEMEN VORGENOMMEN WERDEN.

Um das Risiko von Fehlern zu reduzieren, die Ihr AD lahmlegen könnten, richten Sie ein Testszenario ein, damit Sie die Auswirkungen von Upgrades oder anderen Änderungen testen können, bevor Sie sie in der Produktionsumgebung vornehmen. Um so mehr das Testszenario der Produktionsumgebung entspricht, desto besser.





Überprüfen Sie alle geschäftskritischen Änderungen in Active Directory und geben Sie entsprechende Warnmeldungen aus.

4. ÜBERPRÜFEN.

Umfassende Überprüfung ist aus verschiedenen Gründen wichtig. Sie ermöglicht Verantwortlichkeit, wodurch böswillige Aktionen von Insidern vermieden werden können, und kann Benutzer mit wohlgemeinten Absichten dazu bringen, mit mehr Vorsicht vorzugehen. Dadurch lassen sich die Anzahl und der Schweregrad von Fehlern senken. Außerdem können Sie auf diese Weise schnell feststellen, was schief gelaufen ist, und korrigierende Maßnahmen ergreifen bzw. sicherstellen, dass dasselbe Problem nicht ein weiteres Mal auftritt.

Stellen Sie sicher, dass Ihr Prüfpfad systemeigene Ereignisse, Sicherheitsprotokolle von Anwendungssystemen, Verzeichnisdienstprotokolle und andere wichtige Daten einschließt, damit Sie die Daten schnell überprüfen, durchsuchen und analysieren können. Sorgen Sie außerdem dafür, dass Ihr Überprüfungssystem im Fall eines AD-Ausfalls weiterhin zugänglich bleibt.

5. WICHTIGE ÄNDERUNGEN ÜBERWACHEN UND WARNMELDUNGEN AUSGEBEN.

Stellen Sie sicher, dass Sie umgehend informiert werden, wenn Änderungen an geschäftskritischen Objekten vorgenommen werden, beispielsweise an einer privilegierten Gruppe oder einem GPO, das Auswirkungen auf Ihre Domänencontroller hat Da solche Änderungen selten vorkommen sollten, besteht kein Risiko dafür, dass Sie mit Warnmeldungen überflutet werden. Warnmeldungen zu legitimen Änderungen dienen als Bestätigung dafür, dass Ihr Überwachungssystem funktioniert, während Warnmeldungen zu nicht autorisierten Änderungen Ihnen ermöglichen, schnell zu reagieren – vielleicht auch schnell genug, um schwerwiegende Konsequenzen zu vermeiden.

6. AD STRUKTUR DOKUMENTIEREN.

Nehmen Sie sich die Zeit, Ihre AD zu dokumentieren. Halten Sie diese Informationen auf dem neuesten Stand und speichern Sie sie offline (zum Beispiel in Dropbox), damit Sie auch bei einem AD-Ausfall weiterhin darauf zugreifen können. Es sollten Informationen zu folgenden Aspekten enthalten sein:

- Gesamtstrukturen
- Domänen
- Vertrauensstellungen
- DNS
- Subnetze und Replikationslinks zwischen diesen
- Sämtliche Domänencontroller, einschließlich der IP-Adresse, des physischen Standorts, der gesteuerten Domänen, der enthaltenen flexiblen einfachen Mastervorgänge und Informationen dazu, ob es sich um einen globalen Katalog handelt

Quest

7. ACTIVE DIRECTORY SICHERN.

Sichern Sie Active Directory mit einer Sicherungslösung der Enterprise-Klasse. Verlassen Sie sich nicht ausschließlich auf die Wiederherstellung des Papierkorbs.

Denken Sie immer daran: Der Papierkorb ist eine Annehmlichkeit und nichts anderes. Er unterliegt mehreren schwerwiegenden Einschränkungen, die im Whitepaper „The Windows Server 2016 and Azure AD Recycle Bins, and Quest Recovery Solutions“ beleuchtet werden. Denken Sie beispielsweise daran zurück, dass wir zuvor erwähnt haben, dass Ihr AD durch das Löschen all Ihrer DNS-Datensätze lahmgelegt werden kann. Anstatt die Datensätze zu löschen, könnte ein böswilliger Benutzer die Einstellungen auch durch ungültige IP-Adressen ersetzen. Über den Papierkorb können Sie diese Attribute nicht wiederherstellen.

8. SICHERUNGEN TESTEN.

Sie sollten Sicherungen unbedingt als fehlerhaft betrachten, bis das Gegenteil bewiesen ist. Überprüfen Sie die Funktionstüchtigkeit einer Sicherung, indem Sie sie laden und ein Objekt daraus auslesen. Bilden Sie Ihre Active Directory Gesamtstruktur außerdem regelmäßig in einer Testumgebung nach, um sicherzustellen, dass Sie nach einem schwerwiegenden Problem schnell eine Wiederherstellung durchführen können.

Sichern Sie Active Directory mit einer Sicherungslösung der Enterprise-Klasse und testen Sie die Sicherungen.

Fazit

Wenn Sie Anrufe erhalten und nichts funktioniert, wissen Sie zunächst nicht, was das Problem ist bzw. wie groß der Umfang dieses Problems ist. Es könnte sein, dass ein verärgerter Insider das Problem hervorgerufen hat. Oder Sie sind Opfer eines Malware-Angriffs. Es besteht außerdem auch die Möglichkeit, dass ein versehentlicher Fehler Ihr AD lahmgelegt hat.

Wenn Sie die hier beschriebenen Best Practices befolgen, können Sie das Risiko für diese unglücklichen Szenarien verringern. Vollständig ausräumen lässt sich das Risiko aber selbstverständlich nicht. Daher müssen Sie Maßnahmen ergreifen, um eine schnelle Active Directory Wiederherstellung zu vereinfachen, einschließlich der Beibehaltung eines strukturierten und umfassenden Prüfpfads und der Speicherung von zuverlässigen Sicherungen.

Sie haben wahrscheinlich bereits Horrorgeschichten darüber gehört, wie ein Versuch aussehen kann, AD über das Wochenende neu aufzusetzen. Die Wiederherstellung von AD ist nicht mit der Wiederherstellung von Dateien zu vergleichen, die gelöscht wurden. Und die Wiederherstellung lässt sich auch nicht einfach testen oder simulieren – zum Teil deshalb, weil das richtige Verfahren für die AD-Wiederherstellung vom entsprechenden Notfallszenario abhängt.

Doch mit der richtigen Lösung können Sie Ihre vollständige Active Directory Gesamtstruktur mit einem einzigen Klick wiederherstellen. Weitere Informationen finden Sie in unserem Whitepaper „That Dreaded Day: Active Directory Disasters & Solutions for Preventing Them“.

Mit der richtigen Lösung können Sie Ihre vollständige Active Directory Gesamtstruktur mit einem einzigen Klick wiederherstellen.

Quest

ÜBER QUEST

Bei Quest versuchen wir, komplexe Herausforderungen mit einfachen Lösungen zu bewältigen. Dies gelingt uns dank unserer speziellen Unternehmensphilosophie, bei der hervorragender Service und unser allgemeines Ziel – ein unkomplizierter Geschäftspartner zu sein – im Vordergrund stehen. Unsere Vision besteht darin, Technologien bereitzustellen, bei denen Sie sich nicht zwischen Effizienz und Effektivität entscheiden müssen. Dadurch müssen Sie und Ihre Organisation sich weniger um die IT-Verwaltung kümmern und haben mehr Zeit für Unternehmensinnovation.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:

Quest Software Inc.
Attn: LEGAL Dept

Informationen zu unseren regionalen und internationalen Standorten finden Sie auf unserer Website (www.quest.com/de).

Ebook-3WaysToHoseYourAD-US-GM-DE-WL-32410

Quest