NetIQ

Flash Point-Paper

Einrichten effektiverer Zugriffskontrollen

Privilegierte Benutzer richtig verwalten

Vertrauen ist gut, Überwachung ist besser

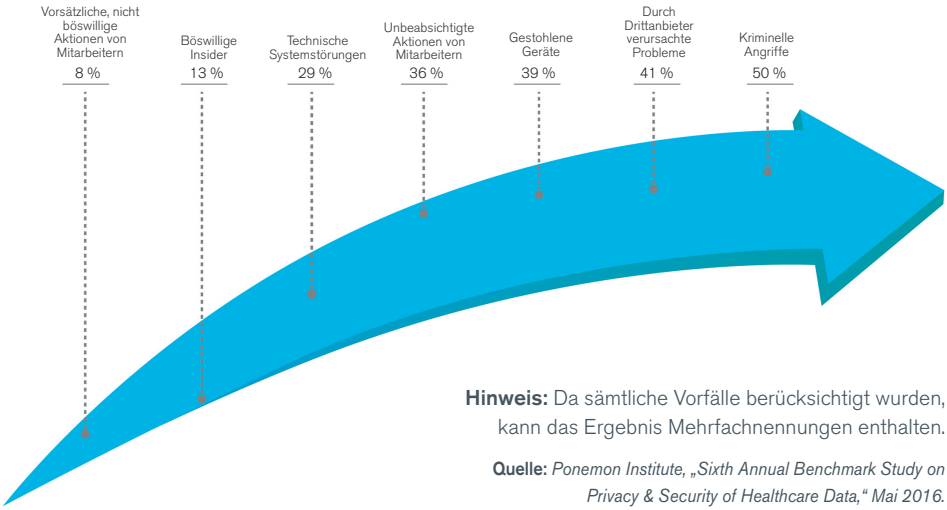
Zur Erledigung ihrer Aufgaben benötigen Mitarbeiter heute jederzeit und überall Zugriff auf Informationen und Dienste. Weil die dazu erforderlichen Technologien immer komplexer werden, muss ihr ordnungsgemäßes Funktionieren von Fachkräften sichergestellt werden. Diese Administratoren bzw. Superuser müssen permanent unmittelbaren und „privilegierten“ Zugriff auf sämtliche Bereiche der Systeme haben, um Fehler zu beheben und Probleme zu lösen.

Dieser privilegierte Zugriff ist zwar notwendig, birgt aber auch Risiken. Für die Verwaltung der immer komplexeren IT-Umgebungen werden nämlich zahlreiche Administratoren gleichzeitig benötigt, deren Zugang von der Root-Ebene über die Schlüsselsysteme bis zum Active Directory (AD) reicht. Die meisten Unternehmen verfügen über mehr solcher privilegierten Benutzer, als sie sich bewusst sind.

Wie erkennen Sie **beim Login eines privilegierten Benutzers,** dass es sich nicht um einen Hacker mit gestohlenen Zugriffsdaten handelt?

Vier Schritte, um Ihr Risiko von Sicherheitsverstößen zu senken:

- *Begrenzen Sie den Umfang der Zugriffsrechte und reduzieren Sie die Anzahl der berechtigten Benutzer*
- *Überwachen Sie Modifikationen an und Zugriffe auf Ihre wichtigsten Systeme und Daten*
- *Nutzen Sie identitätsbasierte Informationen, um festzustellen, ob Benutzeraktivitäten angemessen sind*
- *Legen Sie einen Maßstab für „normales“ Benutzerverhalten fest*



Hinweis: Da sämtliche Vorfälle berücksichtigt wurden, kann das Ergebnis Mehrfachnennungen enthalten.

Quelle: *Ponemon Institute, „Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," Mai 2016.*

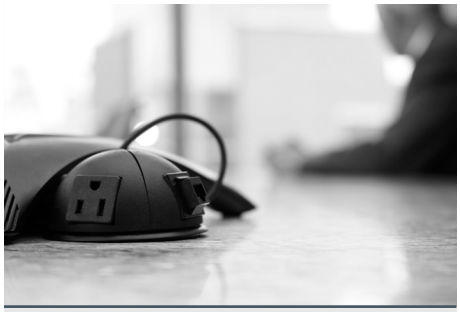
Laut dem Ponemon Institut beruhen die meisten Sicherheitsverstöße und -vorfälle heute auf Aktivitäten von Insidern. Die Problematik besteht in der Regel nicht darin, dass die privilegierten Benutzer böswillige Absichten verfolgen. Aber auch versehentliche oder unbeabsichtigte Aktionen dieser privilegierten Benutzer können aufgrund ihres umfassenden Zugriffs erhebliche Risiken für Ihr Unternehmen bergen. Die Anzahl der durch „tatsächliche" Insider verursachten Sicherheitsverstöße und -vorfälle ist signifikant. Das Ausmaß an „Insiderangriffen" nimmt jedoch noch einmal erheblich zu, wenn in die Betrachtung auch böswillige Angreifer einbezogen werden, die sich über privilegierte Konten Zugriff verschaffen. Diese Angreifer sehen zwar wie Insider aus, sie sind es aber nicht.

Es liegt auf der Hand, warum Hacker es heute insbesondere auf die Konten privilegierter Benutzer (oder anderer Benutzer mit weitreichenden Zugriffsrechten) abgesehen haben: Daten – ganz gleich, ob personenbezogene Informationen, Kreditkartendaten, Unternehmensgeheimnisse oder zwischen Unternehmen ausgetauschte Zugriffsrechte – sind ein kostbares und begehrtes Gut. Die Hacker nutzen ausgefeilte Methoden, um in den Besitz von Zugriffsdaten der privilegierten Benutzer zu kommen und Systeme zu infiltrieren. Ist dies einmal geschehen, geht es nicht mehr darum, „ob" sie sich Zugang zum gesamten System verschaffen können, sondern „wann" dies geschehen wird.

Die Frage ist letztendlich: Wie können Sie beim Login eines privilegierten Benutzers feststellen, ob es sich nicht doch um einen Hacker mit gestohlenen Zugriffsdaten handelt?

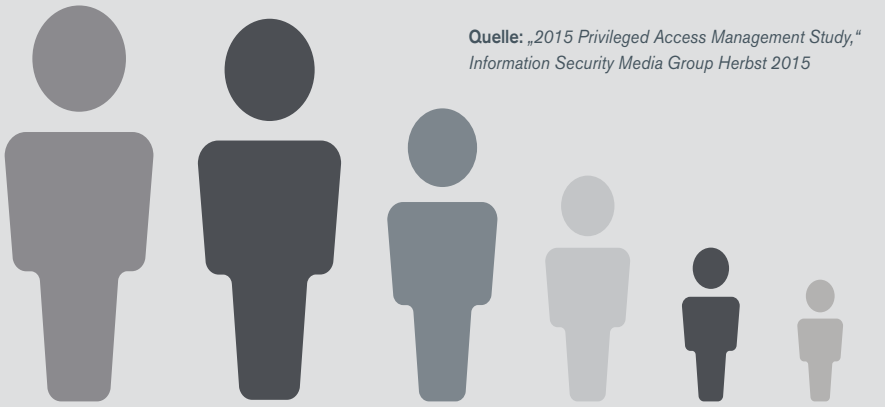
Auf privilegierte Benutzer können Sie nicht verzichten – aber Ihr Risiko mindern

Die Antwort ist eigentlich ganz einfach: Nutzen Sie einen risikobasierten Ansatz. Dazu sollten Sie zunächst sämtliche Projekte identifizieren, die für Ihr Geschäft Priorität haben, und Ihre Ressourcen entsprechend einteilen. Zudem sollten Sie bei diesen Schlüsselprojekten den höchstmöglichen Schutz für Daten und Systeme gewährleisten. Überwachen Sie anschließend genauestens, was mit den projektbezogenen Daten geschieht. Das Problem besteht nämlich nicht darin, dass Hacker Zugang zu vertraulichen Daten haben, sondern dass sie die Daten auf unerwünschte Weise nutzen werden.



Ist der Hackerangriff geschehen, geht es nicht mehr darum, „ob" sie sich Zugang zum gesamten System verschaffen können, sondern „wann" dies geschehen wird.

Welche ist die größte Herausforderung Ihres Unternehmens bei der Verwaltung privilegierter Benutzer?



Quelle: *„2015 Privileged Access Management Study," Information Security Media Group Herbst 2015*

Ermitteln Sie anhand von drei Fragen die Bedrohungen bei der Verwaltung und Verhaltensüberwachung privilegierter Benutzer:

1. Sind die Daten vertraulich? (Ja/Nein)

2. Darf der Benutzer aufgrund seiner Rolle auf die Daten zugreifen? (Ja/Nein)

3. Darf er mit den Daten so umgehen, wie er es tut? (Ja/Nein)

Wodurch zeichnet sich ein risikobasierter Ansatz aus?

1. Im ersten Schritt geht es darum, den Zugriff für privilegierte Benutzer unter Berücksichtigung des Lebenszyklus eines Mitarbeiterkontos zu begrenzen. In vielen Unternehmen verfügen privilegierte Benutzer nicht nur über Administratorrechte, ihre Rechte sind auch zu weitreichend. Dazu kommt, dass einmal erteilte Benutzerrechte oftmals nicht zeitnah wieder entzogen werden. Dies liegt daran, dass es schwierig und zeitaufwendig ist, detaillierte Zugriffsrechte zuzuweisen, und das zuständige Personal entweder nicht die Zeit hat, überflüssige Zugriffsrechte zu widerrufen, oder dies schlichtweg vergisst.

2. Im zweiten Schritt sollten Sie die Daten und Systeme betrachten, die für Ihr Unternehmen am wichtigsten sind. Stellen Sie sicher, dass Ihre Lösung Sie warnt, sobald kritische Daten oder bestimmte Systeme aufgerufen oder modifiziert werden. Im Idealfall sollten Sie nachvollziehen können, durch wen, wann und wo diese Änderungen erfolgt sind. Es reicht nicht aus, lediglich zu erfahren, wer für die Änderungen verantwortlich ist – Änderungen werden permanent durchgeführt, und die Wahrscheinlichkeit von Fehlalarmen wäre dementsprechend hoch. Leider ist dies der übliche Stand, auf dem sich die meisten Sicherheitsteams heute befinden.

3. Im dritten Schritt der Verwaltung von privilegierten Benutzern kommt ein zentraler Aspekt ins Spiel: die Identität des Benutzers. Die Identität geht über die Zugriffsdaten des Benutzers hinaus und beinhaltet weiteren Kontext wie seine Rolle und seinen Standort innerhalb des Unternehmens. Wenn Sie diesen identitätsbasierten Kontext in Ihre Überwachungsdaten einbinden, erhalten Sie ein Sicherheitssystem, mit dem Sie besser nachvollziehen können, wann eine Benutzeraktivität angemessen ist (z. B.: Ja, Herr Müller darf von unserem Standort aus um 15:00 Uhr auf den Server zugreifen) und wann sie verdächtig ist und untersucht werden sollte (z. B.: Nein, Herr Müller sollte um 03:00 Uhr nachts nicht vom anderen Ende der Welt auf unseren Server zugreifen).

Dies führt uns zum letzten Gesichtspunkt der Verwaltung privilegierter Benutzer: der Verhaltensüberwachung. Sie müssen in der Lage sein, das Benutzerverhalten zu überwachen und es mit der Identität hinter dem Benutzerkonto in Bezug zu setzen. Um das Benutzerverhalten auf wirkungsvolle Weise zu überwachen, müssen Sie einen Maßstab für „normales" Verhalten festlegen, anhand dessen ein Abgleich vorgenommen wird. Dies ist auch dann von Bedeutung, wenn unbeabsichtigte Fehler passieren. Root-Ebenen-Benutzer könnten z. B. versehentlich Systemeinstellungen ändern und damit den Zusammenbruch des Netzwerks herbeiführen. Wenn Sie nicht feststellen können, wodurch das Problem verursacht worden ist, werden Sie große Schwierigkeiten bei seiner Behebung haben. Sind Sie aber in der Lage, die Schritte Ihrer Benutzer nachzuvollziehen, können Sie herausfinden, wo das Problem entstanden ist, und es beheben.

*Im September 2015 erlitt **Facebook eine Reihe von drei weltweiten Ausfällen, die insgesamt über 2,5 Stunden andauerten.** Die Ausfälle waren nicht auf böswillige Angriffe zurückzuführen, sondern Fehler im Konfigurationssystem.*

Noch wichtiger ist, dass Sie bei der Überwachung des Benutzerverhaltens anhand von drei einfachen Fragen Bedrohungen ermitteln können: 1. Sind die Daten vertraulich? (Ja/Nein) 2. Darf der Benutzer aufgrund seiner Rolle auf die Daten zugreifen? (Ja/Nein) 3. Darf er mit den Daten so umgehen, wie er es tut? (Ja/Nein)

Sicherer Zugriff ohne Beeinträchtigung des Geschäftsbetriebs

Unbeabsichtigte Ausfälle können zu großen Herausforderungen führen, besonders, wenn Cloud-Services betroffen sind. Beispielsweise setzen Verbraucher auf den Social Networking-Giganten Facebook mit seinen monatlich 1,5 Milliarden Benutzern weltweit, um mit Familie und Freunden in Kontakt zu bleiben. Auch Unternehmen verlassen sich auf die Funktionsfähigkeit ihrer mit Facebook verbundenen Apps und Marketingaktivitäten im Social Media-Bereich. Im September 2015 erlitt Facebook eine Reihe von drei weltweiten Ausfällen, die insgesamt über 2,5 Stunden andauerten. Die Ausfälle waren nicht auf böswillige Angriffe zurückzuführen, sondern Fehler im Konfigurationssystem. Nur einige Monate zuvor kam es zu einem signifikanten weltweiten Ausfall, der, wie das Unternehmen zugab, daraus resultierte, dass Techniker auf kritische Konfigurationswerte zugriffen und mit diesen „herumspielten“. Der stündlich von Facebook erlittene Einnahmeverlust durch Werbeanzeigen belief sich auf ungefähr 0,8 bis 1,7 Millionen US-Dollar. Nach den Ausfällen im September 2015 fiel die Facebook-Aktie um fast 4 Prozent, was die Enttäuschung am Markt widerspiegelte.

Die einzige wirklich sichere Lösung bestünde darin, überhaupt keine Zugriffsrechte mehr zu erteilen – was natürlich nicht praktikabel ist. Sie können jedoch sicherstellen, dass Sie Ihren Benutzern eine adäquate Zugriffsstufe zuweisen, und dann überwachen, was Benutzer mit den an sie zugewiesenen Rechten tun.

So können Administratoren, die weitreichenden Zugriff haben müssen, ihre Aufgaben weiterhin ungehindert erledigen. Da sich die Reaktion auf überwachte Sicherheitsereignisse automatisieren lässt, muss Ihr Sicherheitspersonal zudem nicht jedes einzelne Vorgangsprotokoll manuell prüfen.

Des Weiteren können Sicherheitsteams dadurch, dass das Verhalten und die Identität von Benutzern in die Sicherheitsüberwachungsdaten mit eingeschlossen wird, potenzielle Bedrohungen noch schneller erkennen und auf sie reagieren.

Auswahl der richtigen Lösung zur Verwaltung privilegierter Benutzer

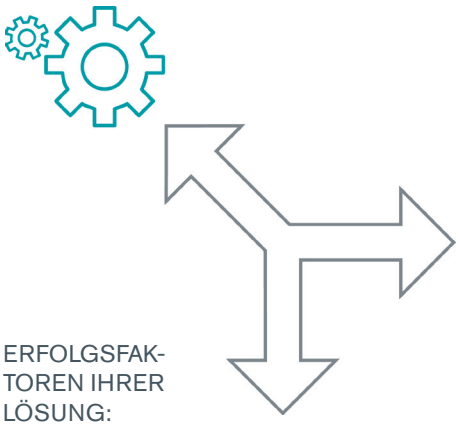
Es gibt viele Möglichkeiten, an die beschriebene Problematik heranzugehen – z. B. mithilfe diverser Security Information and Event Management (SIEM)-Produkte, Identity Management-Lösungen, Change-Management-Systeme und Automatisierungslösungen. Bei der Entscheidung für eine Lösung sollten Sie auf folgende Merkmale achten:

- **Nahtlose Zusammenarbeit der Komponenten.** Die einzelnen Systeme Ihrer Lösung erfüllen zwar unterschiedliche Aufgaben, ergänzen sich aber gegenseitig. Im Idealfall kommunizieren sie untereinander und tauschen Informationen aus. Ist dies nicht der Fall, ist die Lösung für Ihr Problem ungeeignet.
- **Hinlängliche Automatisierung.** Je höher der Grad der Automatisierung, umso weniger Arbeit haben Sie. Eine Lösung, die manuelle Eingriffe oder ein umfassendes Fachwissen erfordert, ist ungeeignet. Es geht letztendlich darum, Ihnen und Ihrem Team die Unterscheidung zwischen echten Bedrohungen und unbedeutenden Aktionen zu erleichtern.
- **Richtlinienbasierte Überwachung.** Die Erweiterung der Sicherheitsüberwachung durch den identitätsbasierten Kontext ist nur sinnvoll, wenn Sie für bestimmte Geschäftsszenarios Regeln und Richtlinien festlegen können. Diese Funktion ist für eine leistungsstarke Lösung unverzichtbar.
- **Langfristige Kosteneffektivität.** Denken Sie nicht nur an den Anschaffungspreis, sondern berücksichtigen Sie auch, welche langfristigen Kosten die Lösung verursacht. Ist sie benutzerfreundlich? Ist sie mit Ihren vorhandenen Systemen kombinierbar? Wie hoch ist die zusätzliche Verwaltungszeit? Wie hoch ist der zusätzliche Schulungsaufwand?

Bei der Auswahl einer geeigneten Lösung sollten Sie die identitätsbasierten Sicherheitslösungen von NetIQ in Betracht ziehen. Unsere Identity, Access and Security Management-Lösungen lassen sich nahtlos integrieren und ermöglichen Unternehmen, die Gesamtanzahl der Benutzer mit privilegierten Zugriffsrechten zu reduzieren und sicherzustellen, dass die richtigen Mitarbeiter den richtigen Zugriff erhalten, wenn sie ihn benötigen. Außerdem überwachen sie, was Benutzer, und zwar besonders diejenigen mit weitreichenden Zugriffsrechten, mit den ihnen gewährten Rechten tun. Die Nutzung identitätsbasierter Informationen auf diese Weise hilft Ihnen, den für die Produktivität nötigen Zugriff mit dem Bedarf, die Risiken unserer hyper-verbundenen Welt zu reduzieren, auszubalancieren.

- **NetIQ Change Guardian** bietet Ihnen Informationen dahingehend, wer wann und wo in Ihrem Unternehmen welche Aktionen durchführt – ganz gleich, ob es dabei um die Änderungen von Konfigurationen oder den Zugriff auf sensible Dateien (Überwachung der Dateiintegrität) geht. Dabei erhalten Sie die Sicherheitsinformationen, die Sie benötigen, um Aktivitäten von privilegierten Benutzern, die einen Sicherheitsverstoß darstellen oder zu Compliance-Lücken führen können, schnell erkennen und darauf reagieren zu können.
- **NetIQ Sentinel** ist eine funktionsreiche SIEM-Lösung. Sie erleichtert die Implementierung, die Verwaltung sowie die tägliche Verwendung von SIEM. NetIQ Sentinel kann problemlos an dynamische Unternehmensumgebungen angepasst werden und liefert genau die Daten, die Sicherheitsexperten benötigen, um den Bedrohungsstatus zu erkennen und die entsprechenden Reaktionen zu priorisieren.
- **NetIQ Identity Manager** ist eine umfassende und zugleich kostengünstige Lösung, mit der Sie unternehmensweit steuern, welche Benutzer auf welche Daten und Systeme zugreifen – sowohl innerhalb der Firewall als auch in der Cloud. Identity Manager bietet den Benutzern sicheren und bequemen Zugriff auf kritische Informationen und gewährleistet dabei Ihre Compliance.
- **NetIQ Directory and Resource Administrator** bietet clevere Active Directory (AD)-Verwaltungsfunktionen, darunter die detaillierte Delegierung von Administratorrechten und die Kontrolle des Administratorzugriffs. Die Lösung delegiert auf einfache Weise Administrationsrechte für auf Office 365 gehostete Active Directory-, Exchange Server- und Exchange Online-Dienste von Microsoft.
- **NetIQ Privileged Account Manager** erlaubt IT-Administratoren, an Systemen zu arbeiten, ohne dass dabei die Passwörter von Administratoren oder Supervisors oder die Anmeldedaten für Root-Konten mitgeteilt werden müssen. Die Lösung verwaltet, steuert und zeichnet Aktivitäten von privilegierten Benutzern für alle benutzerdatenbasierten Systeme auf, darunter Anwendungen, Datenbanken, Cloud-Services und virtuelle Server. Sie unterstützt zudem Multi-Faktor-Authentifizierung und Single Sign-on für eine verbesserte Zugriffssicherheit.

Erfahren Sie mehr über die nächsten Schritte unter **www.netiq.com**



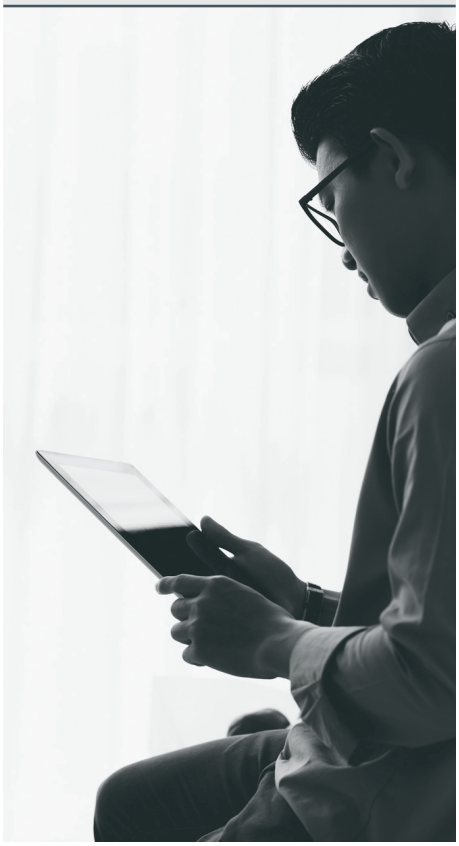
ERFOLGSFAKTOREN IHRER LÖSUNG:

- Nahtlose Zusammenarbeit der Komponenten
- Hinlängliche Automatisierung
- Richtlinienbasierte Überwachung
- Langfristige Kosteneffektivität

Systemautomatisierung kann Problemen vorbeugen:

1. Automatisiertes Provisioning/ De-Provisioning/ Re-Provisioning von Zugriffsrechten
2. Zentralisiertes Personalverwaltungssystem für das Erstellen, Widerrufen und Aktualisieren von Rechten

Dies ist besonders hilfreich, wenn große Gruppen von Benutzern mit privilegiertem Zugriff (z. B. Auftragnehmer oder befristete Angestellte) das Unternehmen verlassen. Lassen Sie hier kein Hintertürchen offen!



Unsere Lösungen zur Verwaltung privilegierter Benutzer ermöglichen Unternehmen, die Gesamtanzahl der Benutzer mit privilegierten Zugriffsrechten zu reduzieren und sicherzustellen, dass die richtigen Mitarbeiter den richtigen Zugriff erhalten, wenn sie ihn benötigen. Außerdem überwachen sie, was Benutzer, und zwar besonders diejenigen mit weitreichenden Zugriffsrechten, mit den ihnen gewährten Rechten tun.

www.netiq.com

NetIQ
Deutschland
Fraunhoferstr. 7
85737 Ismaning
Tel: +49 (0)89 420940
Email: infoDE@netiq.com

Schweiz
Flughafenstrasse 90
P.O. Box 253 8058 Zürich
Tel: +41 (0)43 456 2400
Email: infoCH@netiq.com

info@netiq.com
www.netiq.com/communities
www.netiq.com

Die vollständige Liste unserer Niederlassungen in Nordamerika, Europa, Nahost, Afrika, Lateinamerika sowie im asiatisch-pazifischen Raum finden Sie unter: www.netiq.com/contacts

www.netiq.com