WHITE PAPER | Juli 2013

Irgendjemandem muss ich doch vertrauen. Oder?

Über den Umgang mit Bedrohungen der Cybersicherheit durch Insider

Russell Miller

Merritt Maxim

CA Technologies, Security Management

ca technologies

Inhaltsverzeichnis

Kurzfassung

„Wenn man Positionen mit privilegierten Zugriffsberechtigungen innehat, wie etwa ein Systemadministrator für diese Art von Nachrichtendienst, hat man auf breiter Ebene Zugang zu weitaus mehr Informationen als ein durchschnittlicher Mitarbeiter."

– Edward Snowden

Ausgangssituation

Viele Unternehmen konzentrieren sich bei ihren Sicherheitsvorkehrungen auf ihre Netzwerkgrenze; dabei sind es oft die Insider, die die Cybersicherheit am meisten gefährden können. Von Managern über IT-Administratoren bis hin zu Partnern haben viele Personen Zugriff auf sensible Daten, die, sollten sie an die Öffentlichkeit gelangen, erhebliche Auswirkungen auf die Geschäfte des Unternehmens oder sogar seine Existenz haben könnten.

Cybersicherheit gilt im Allgemeinen als technischer Bereich, in dem bestens ausgebildete Mitarbeiter versuchen, die Angreifer in puncto Intellekt und Ausdauer zu übertreffen. Obwohl diese Beschreibung nicht ganz von der Hand zu weisen ist, vernachlässigt sie doch den vermutlich wichtigsten Aspekt in Sachen Sicherheit: den Menschen. Menschen neigen dazu, ihnen bekannten Personen zu vertrauen, was dazu führt, dass sie Passwörter oder sonstige vertrauliche Informationen weitergeben.

Vertrauen ist in jeder Art von Unternehmen ein grundlegendes Element. Die Menschen benötigen aus vielen Gründen Zugriff auf sensible Daten und kritische Systeme, und mit diesem Zugriff muss ein gewisses Maß an Vertrauen verbunden sein. Der Umgang mit diesem Vertrauen stellt die wichtigste und schwierigste Aufgabe im Hinblick auf die Abwehr von Insiderbedrohungen dar.

Chancen

„Vertrauen" bedeutet nicht, dass Mitarbeiter einen uneingeschränkten und unnötigen Zugriff auf Daten bekommen. Mit den richtigen Sicherheitsvorkehrungen können Unternehmen die Gefahr von Insiderbedrohungen maßgeblich verringern. Wichtig dabei ist es, das richtige Gleichgewicht zwischen Handlungsmöglichkeiten der Mitarbeiter und Kontrolle zu finden, während die Mitarbeiter gleichzeitig die Verantwortung für ihr Handeln tragen. Das erfordert eine breite Palette von Maßnahmen, damit ein Unternehmen die Identitäten, den Zugriff und die Daten sorgfältig verwalten kann – von Identity Management über Governance und Privileged Identity Management bis hin zu Datensicherung.

Insiderbetrug ist kein Einzelfall.

Durchschnittlich verzeichneten Unternehmen in den vergangenen zwölf Monaten rund 55 von Mitarbeitern verursachte Betrugsfälle.[1]

– Ponemon Institute

Nutzen

Strenge Sicherheitsvorkehrungen senken nicht nur das Risiko, sondern können auch die Informationsweitergabe in einem Unternehmen unterstützen. Der Zugriff auf hochsensible Daten wird häufig aus Angst, dass die Daten öffentlich gemacht werden könnten, stark eingeschränkt. Mit den entsprechenden Sicherheitsvorkehrungen können die Daten jedoch einer größeren Gruppe von Personen zugänglich gemacht werden, die dann effizienter und innovativer arbeiten können.

„In der Welt von heute ist Technologie das wertvollste Gut, das man besitzen kann. Das Wichtigste, was dieses Land tun kann, ist den Schutz der Betriebsgeheimnisse sicherzustellen.“[3]

– U.S. District Judge Ruben Castillo

Abschnitt 1:

Ausgangssituation

Insider können sensible Daten aus unterschiedlichen Gründen vorsätzlich oder unabsichtlich stehlen, löschen oder offenlegen. Gleichzeitig benötigen Insider ein gewisses Maß an Zugriff, damit das Unternehmen funktionieren oder eine Organisation ihren Aufgaben nachkommen kann. Deshalb gilt es, Insiderbedrohungen auf mehreren Ebenen zu verstehen, von der Motivation über negative Beispiele bis hin zur Frage, wie die Bedrohung entstanden ist, um intelligente Risikominderungsstrategien einführen zu können.

Arten von Insiderbedrohungen

Insiderbedrohungen zeigen sich in unterschiedlicher Form. Demzufolge gibt es drei Arten von Insiderbedrohungen: böswillige Insider, die bewusst Informationen stehlen oder Schaden anrichten, Insider, die unwissentlich von Dritten ausgenutzt werden, und Insider, die unvorsichtig agieren und unbeabsichtigt Fehler begehen.

- **Böswillige Insider** gibt es nur selten, doch gerade sie haben das Potenzial, beachtlichen Schaden anzurichten. Administratoren mit privilegierten Identitäten sind besonders risikoreich. Laut Ponemon Institute sind „Datenschutzverletzungen infolge von vorsätzlichen Angriffen die kostspieligsten“[2].
- **Ausgenutzte Insider** können von externen Parteien dazu überlistet werden, Daten oder Passwörter unberechtigterweise preiszugeben.
- **Unvorsichtige Insider** können versehentlich die falsche Taste drücken und damit kritische Informationen löschen oder ändern.

Insiderbedrohungen können auch von privilegierten Anwendern (Administratoren) oder regulären Anwendern mit Zugriff auf sensible Daten ausgehen. Administratoren besitzen häufig umfassende Berechtigungen für quasi alle Vorgänge auf vielen kritischen Systemen. Personen in allen Funktionen haben oft mehr Berechtigungen angehäuft, als sie für ihre derzeitige Position benötigen, was zu einem absolut vermeidbaren Anstieg des Risikos führt.

Was hat sich geändert?

Der Einsatz. Da sich die Wirtschaft zu einem immer stärker informationsbasierten System entwickelt, sind geistiges Eigentum und Betriebsgeheimnisse kritischer als je zuvor, wenn es darum geht, das Überleben eines Unternehmens zu sichern. Die Zunahme von Big Data-Analysen hat das Problem zusätzlich verschärft. Unternehmen speichern heute riesige Datenmengen, um Muster zu erkennen und Erkenntnisse zu gewinnen, die vor wenigen Jahren noch undenkbar gewesen wären. Obwohl diese Daten möglicherweise ein kritisches Unterscheidungsmerkmal darstellen können, handelt es sich dabei manchmal um hoch sensible Daten, die Informationen wie etwa persönliche Angaben der Kunden, Kreditkartennummern, Transaktionen, Kommunikation und sogar Ortsangaben beinhalten. Eine Sicherheitsverletzung in Bezug auf die Speicherung von Kundendaten kann einen Verstoß gegen das Datenschutzgesetz, Sammelklagen und eine Rufschädigung zur Folge haben, was das Ende des Unternehmens bedeuten kann.

Das Computer Emergency Response Team (CERT) der Carnegie Mellon University definiert einen böswilligen Insider wie folgt: „Ein böswilliger Insider ist ein aktueller oder ehemaliger Mitarbeiter, Subunternehmer oder Geschäftspartner, der Zugriffsrechte auf das Netzwerk, System oder die Daten eines Unternehmens besitzt bzw. besaß und diese Rechte auf eine Weise überschreitet bzw. missbraucht, dass die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen oder Informationssysteme des Unternehmens gefährdet wird.“[4] In der Vergangenheit handelte es sich bei einem Insider zumeist um einen Mitarbeiter. Das CERT hat allerdings festgestellt, dass die Insiderangriffe inzwischen über die interne Belegschaft hinausgehen und nun auch von vermeintlich vertrauenswürdigen Dritten wie z. B. Geschäftspartnern begangen werden. Diese Entwicklung sowie die Tatsache, dass die Mitarbeiter heute geografisch weit verstreut und überaus mobil sind, bedeutet, dass die Bedrohungen durch Insider so groß sind wie nie zuvor.

Risikofaktoren für Insiderbedrohungen

Alle Unternehmen stehen vor ähnlichen Herausforderungen, wenn es darum geht, das Risiko von Sicherheitsverstößen durch Insider zu senken:

Ineffektives Management privilegierter Anwender. In jeder IT-Umgebung gibt es privilegierte Anwender (Admin, Root), die auf wichtige Systeme, Anwendungen und Informationen uneingeschränkten Zugriff haben. Dies stellt nicht nur ein Sicherheitsrisiko dar, sondern kann auch die Einhaltung von Vorschriften erschweren. Die Weitergabe von Administratorpasswörtern ist ein weiteres häufiges Problem, das zu unberechtigten Zugriffen auf Ihre Systeme und Informationen führen kann und es letztendlich unmöglich macht festzustellen, wer genau welche Aktion in einem System durchgeführt hat.

Ungeeignete Zuweisung von Rollen und Berechtigungen. Das Management von Anwenderrollen und -berechtigungen ist eine der größten Herausforderungen vieler IT-Abteilungen. Rollen, die sich überschneiden, und doppelt vergebene oder inkonsistente Berechtigungen gehören zu den Problemen, die nicht selten unbefugte Zugriffe und eine unberechtigte Verwendung vertraulicher Informationen nach sich ziehen können. Wenn zudem keine automatisierte Deprovisionierung erfolgt, kann dies übermäßige Berechtigungen oder verwaiste Anwenderkonten zur Folge haben – beides Möglichkeiten für verärgerte Insider, einen Angriff zu starten.

Mangelhafte Identity Governance. Ein wirkungsvoller Schutz vor unbefugtem Zugriff auf Informationen oder deren Gebrauch erfordert umfassende Kontrollen der Anwenderidentitäten, des Zugriffs auf die Informationen sowie deren Verwendung. Die meisten Unternehmen verfügen in diesen Bereichen zwar bereits über einige Kontrollmechanismen, haben aber keinen einheitlichen und zuverlässigen Ansatz, mit dem sie ihre Informationen wirklich schützen könnten.

Mangelhafte Klassifizierung von Informationen und Erzwingung von Richtlinien. Viele Unternehmen wissen nicht einmal, wo all ihre sensiblen Daten abgelegt sind. Oftmals sind nur unzureichend definierte und kommunizierte Richtlinien darüber vorhanden, wie mit vertraulichen Informationen umzugehen ist. Am schwerwiegendsten ist jedoch, dass viele Unternehmen keine Kontrollen implementiert haben, die die unbefugte Übertragung oder Offenlegung sensibler Daten erkennen und verhindern.

Unzureichendes Auditing und Analysen. Viele Unternehmen verfügen über keine Möglichkeit, den Zugriff kontinuierlich zu überprüfen, um sicherzustellen, dass nur Personen mit entsprechender Autorisierung Zugriff erhalten und dass die Art und Weise, wie diese die Informationen nutzen, den Richtlinien entspricht. Und selbst wenn sie Auditingtools im Einsatz haben, macht es die große Menge protokollierter Daten äußerst schwierig, die ganzen Daten zu sichten und Verstöße oder Bedrohungen auszumachen.

Komplexität von Auditprotokollen. Die große Menge an Audit- und Protokolldaten erschwert juristische Ermittlungen und Untersuchungen. Die Protokollierung sämtlicher IT-Aktivitäten ist bei der Bekämpfung von Insiderangriffen ein wichtiger erster Schritt. In den heutzutage hochgradig verteilten und komplexen IT-Umgebungen jedoch werden Unmengen an Protokolldaten generiert – und allein das Volumen dieser Daten ist kaum beherrschbar.

Reaktive Ansätze. Die meisten der heute verfolgten Ansätze zur Bekämpfung von Insiderbedrohungen sind reaktiv und nicht proaktiv. Dies hilft zwar bei juristischen Untersuchungen, der Angriff oder Diebstahl hat dann aber bereits stattgefunden. Deshalb sollten sich Unternehmen nach Lösungen umsehen, die mehr analytische und vorausschauende Leistungsmerkmale bieten, die – wenn sie schon nicht in der Lage sind, Insiderangriffe von vornherein zu verhindern – die Insider, von denen eine Gefährdung ausgehen könnte, identifizieren und für diese Personen dann ausführlichere Protokolle erstellen.

Keine umfassenden schriftlichen Richtlinien zur akzeptablen Nutzung. Jedes Unternehmen sollte über ausführliche Richtlinien zur akzeptablen Nutzung von Informationen verfügen, die für alle seine Mitarbeiter gelten. Es muss dann auch dafür sorgen, dass diese Richtlinien jedes Jahr von den Mitarbeitern durchgelesen und unterzeichnet werden. Dies ist ein wichtiger Schritt, der oft vernachlässigt wird. Eine schriftliche Sicherheitsrichtlinie allein wird Insiderangriffe nicht unbedingt komplett verhindern können, sie kann aber hilfreich sein, um das gesamte Unternehmen grundlegend darüber zu informieren, was unter „akzeptabler Nutzung“ zu verstehen ist und wie vertrauliche Daten zu handhaben sind.

Rund 65 Prozent der Mitarbeiter, die einen Insider-IP-Diebstahl begehen, hatten zum Zeitpunkt des Diebstahls bereits eine vergleichbare Position bei einem Mitbewerber angenommen oder ihr eigenes Unternehmen gegründet. Etwa 20 Prozent wurden von einem Outsider angeworben, der es auf die Daten abgesehen hatte. Mehr als die Hälfte der Personen stehlen die Daten innerhalb eines Monats vor dem Ausscheiden aus dem Unternehmen.

Behavioral Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall,

– Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D.

Die Schwierigkeit dabei: Risikosenkung vs. Unterstützung des gesamten Unternehmens

Vertrauen ist eine Grundvoraussetzung für die Geschäftstätigkeit jedes Unternehmens. Damit ein Unternehmen von sensiblen Daten profitieren kann, benötigen die richtigen Personen und Systeme Zugriff darauf, und übermäßig strenge Bestimmungen behindern ein Unternehmen in seiner Fähigkeit, rasch zu reagieren, Innovationsgeist zu beweisen und in seiner gesamten Tätigkeit zu bestehen. Gleichzeitig führt unnötiges Vertrauen zu unnötigen Risiken. So etwa können jene Personen, denen das meiste Vertrauen entgegengebracht wird, auch den größten Schaden anrichten: Dabei handelt es sich um die privilegierten Anwender in einem Unternehmen. Diese Administratoren besitzen nicht selten uneingeschränkte Rechte, mit denen sie in kritischen Systemen praktisch jede Aktion durchführen können. Und Anwender haben oft mehr Berechtigungen angesammelt, als sie für die Ausübung ihrer aktuellen Tätigkeit benötigen. Ein weiteres unnötiges Risiko in Verbindung mit privilegierten Identitäten sind gemeinsam genutzte Accounts. Wenn mehrere Personen Zugriff auf denselben Account haben, sind die Verantwortlichkeiten nicht mehr eindeutig.

Der Umgang mit dem menschlichen Element ist der schwierigste Aspekt in Bezug auf Insiderbedrohungen. Viele Menschen brauchen das Gefühl, dass ihr Unternehmen ihnen vertraut, und sind persönlich gekränkt, wenn neue Regelungen ihren Zugang zu Daten beschränken, die ihnen zuvor zur Verfügung standen. Zudem gelten Zugriffsberechtigungen insbesondere bei IT-Administratoren oft als Statussymbol, und jegliche Einschränkungen stoßen auf Widerstand.

Beispiele für Sicherheitsverstöße durch Insider

Viele von Insidern begangene Sicherheitsverstöße werden niemals publik gemacht. Die Unternehmen möchten diese Verstöße lieber für sich behalten, statt eine Rufschädigung in Kauf zu nehmen oder sich mit möglichen Sicherheitsbedenken der Kunden auseinandersetzen zu müssen. Dennoch sind zahlreiche und in hohem Maß schädliche Insiderverstöße bekannt geworden. Im Folgenden sind einige der bekanntesten Beispiele aufgeführt:

Bekannte Sicherheitsverstöße durch Insider

National Security Agency	San Francisco	Motorola
Edward Snowden, der für Booz Allen Hamilton als Auftragnehmer für die NSA arbeitete, lieferte Journalisten brisante Dokumente über Programme mit den Namen „Prism“ und „Boundless Informant“. Snowdens Informationen enthüllten Details über die Speicherung und Verarbeitung von Kommunikation durch die NSA, darunter auch Telefongespräche und E-Mails.[5]	Ein verärgerter Mitarbeiter in San Francisco sperrte die Stadt aus ihrem eigenen FiberWAN-Netzwerk aus, das vertrauliche Dokumente, darunter auch Polizeiberichte, enthielt. Noch schlimmer war jedoch, dass auf E-Mails nicht zugegriffen werden konnte und keine Gehaltszahlungen veranlasst werden konnten. Die Stadt gab im Bemühen, den Netzwerkzugriff wiederherzustellen, mehr als eine Million Dollar aus – umsonst.[6]	Hanjuan Jin, der neun Jahre lang als Softwaretechniker bei Motorola tätig war, wurde von den US-amerikanischen Zollbeamten erwischt, als er gerade mit 30.000 USD Bargeld sowie mehr als 1.000 als „vertraulich und urheberrechtlich geschützt“ gekennzeichneten Dokumenten im Wert von 10-15 Millionen USD an Betriebsgeheimnissen in ein Flugzeug nach Peking steigen wollte. Hanjuan Jin wurde von einem US-amerikanischen Bundesgericht für schuldig befunden, Betriebsgeheimnisse gestohlen zu haben, und zu vier Jahren Haft verurteilt.[7]

Abschnitt 2:

Chancen

Unternehmen müssen sich der Realität stellen, dass Angriffe durch Insider eine immense Bedrohung darstellen und immer weiter an Komplexität zunehmen. Da so viele Assets und Informationen eines Unternehmens inzwischen online zugänglich sind, müssen diese proaktive Maßnahmen ergreifen, um sich vor Insiderangriffen zu schützen. Diese Maßnahmen sollten eine Reihe von Lösungen beinhalten, die sich dem Identity and Access Management und dem Schutz der Daten annehmen. Es gibt keine Lösung, die alle Insiderangriffe komplett verhindern kann. Lösungen aber, die einen offensiven proaktiven Ansatz verfolgen, können zur Senkung der Risiken und zur verbesserten Einhaltung von Vorschriften beitragen und der IT dabei helfen, die Unternehmensziele besser zu unterstützen.

Das Gleichgewicht finden

Mit Tools für das Management von Identitäten, Berechtigungen und Daten können Unternehmen das richtige Gleichgewicht zwischen Handlungsmöglichkeiten – und der Weitergabe sensibler Daten – und den Kontrollmechanismen finden, die nötig sind, um die Risiken von Sicherheitsverstößen durch Insider zu verringern. Unternehmen können das Risiko aller drei Arten von Insiderbedrohungen (böswillig, unwissentlich ausgenutzt von Dritten und unvorsichtig) reduzieren, indem sie die Verantwortlichkeiten klar regeln, minimale Zugriffsrechte implementieren und sensible Daten kontrollieren. Verantwortlichkeit veranlasst böswillige Insider dazu, es sich zweimal zu überlegen, bevor sie aktiv werden, hilft bei der Ermittlung von ausgenutzten Insidern und sorgt dafür, dass Anwender achtsamer werden. Mithilfe von minimalen Zugriffsrechten können Aktionen verhindert und die durch Insiderangriffe jeglicher Art entstandenen Schäden, einschließlich unbeabsichtigter Fehler, begrenzt werden. Durch eine direkte Kontrolle sensibler Daten können Unternehmen verhindern, dass diese Daten über Tools wie USB-Laufwerke oder sogar E-Mails außerhalb des Netzwerks gelangen.

„Vertrauen“ bedeutet nicht, dass die Mitarbeiter einen uneingeschränkten Zugriff auf Daten bekommen, die für ihren Job irrelevant sind. Unternehmen übertragen allen Mitarbeitern, die auf sensible Daten oder Systeme zugreifen, ein gewisses Maß an Vertrauen. Doch mehr Zugriffsrechte als notwendig bedeuten ein unnötiges Risiko, was nicht heißt, dass das Unternehmen seinen Mitarbeitern nicht vertraut. Es ist einfach eine kluge Vorgehensweise.

Um neue Sicherheitsvorkehrungen zu unterstützen, ist es wichtig, minimale Zugriffsrechte als kulturelle Norm zu etablieren, indem standardmäßig im gesamten Unternehmen Kontrollen zur Anwendung kommen. Dadurch erleben die Mitarbeiter die Datensicherheit als Priorität im Unternehmen und nicht als mangelndes Vertrauen in eine bestimmte Person. Das führt dazu, dass eine sorgfältig kontrollierte Datenzugriffsstrategie weniger negativ erlebt wird.

Ein breiter Ansatz zur Verringerung der Insiderbedrohungen

Die Security-Lösungen von heute können den Schaden eines Sicherheitsverstoßes durch einen Insider verringern, einen Verstoß nach dem Vergehen identifizieren, um eine effektive Reaktion zu ermöglichen, oder einen Verstoß sogar verhindern. Zu den besonders kritischen Funktionen zählen dabei:

Privileged Identity Management

Privileged Identity Management ist das Kernstück jeder Cyberverteidigung gegen Insiderbedrohungen. Accounts mit besonderen Berechtigungen bieten den Zugriff, den eine Person benötigt, um die sensibelsten Daten eines Unternehmens anzuzeigen und zu stehlen oder kritischen IT-Systemen den meisten Schaden zuzufügen. Normalerweise handelt es sich dabei um gemeinsam genutzte Accounts, wobei mehrere Personen Zugriff auf dieselben Accounts und Passwörter haben, wodurch die Verantwortlichkeiten verschwimmen.

Das Management privilegierter Identitäten erfordert einen breit angelegten Ansatz. Neben dem Management gemeinsam genutzter Accounts regeln zusätzliche Kontrollen die Verantwortlichkeit von Insidern und können den durch einen externen Angreifer verursachten Schaden begrenzen, falls ein solcher Zugriff auf einen Administrator-Account bekommt.

56 % „Prozentsatz der Führungskräfte, die angaben, dass ihr schwerster Betrug durch einen privilegierten Anwender erfolgte.“[8]

– Pricewaterhouse Coopers

Schlüsselfunktion	Notwendigkeit	Beschreibung	Nutzen
Passwortmanagement für gemeinsam genutzte Accounts	Accounts mit besonderen Berechtigungen, wie z. B. „root“ unter UNIX und „Administrator“ unter Windows, werden häufig gemeinsam verwendet, wodurch Verantwortlichkeiten nicht mehr eindeutig sind.	Kontrolle des Zugriffs auf privilegierte Administrator-Accounts mit Passwort-Storage und automatischer Anmeldefunktion. Das ist der Ausgangspunkt für die meisten Privileged Identity Management-Lösungen.	Reduziert das Risiko, dass unberechtigte Anwender Zugriff auf privilegierte Accounts erhalten. Beugt einer gemeinsamen Passwortverwendung vor.
Spezifische Access Controls	Der Zugriff auf privilegierte Accounts basiert häufig auf einer Alles-oder-Nichts-Strategie. Diese stellt allerdings ein unnötiges Risiko dar, das dazu führt, dass Anwender mehr Berechtigungen bekommen, als sie tatsächlich benötigen.	Verwaltung des Zugriffs durch privilegierte Anwender nach der Anmeldung. Kontrolle über die Zugriffsrechte der Anwender basierend auf der jeweiligen Identität, selbst wenn ein gemeinsamer Administrator-Account verwendet wird.	Reduziert das Risiko, indem Administratoren nur mit den Berechtigungen ausgestattet werden, die sie für die Ausführung ihrer Tätigkeit benötigen.
Reporting der Anwenderaktivitäten/ Videoaufzeichnung von Sessions	Es ist wichtig, alle Anwenderaktionen zu verfolgen, um im Rahmen einer Untersuchung feststellen zu können, was passiert ist und wer was getan hat. Nicht alle Anwenderaktivitäten werden aufgezeichnet, und viele Anwendungen erzeugen keine Protokolle. Hierdurch werden Verantwortlichkeiten reduziert und juristische Untersuchungen erschwert.	Aufzeichnung aller Anwenderaktionen und Verfolgung aller Datensätze nach Person, auch wenn ein gemeinsamer Account verwendet wird. Im Idealfall wird ein IT-System in einem videoähnlichen Format verfolgt.	Anhand eines verständlichen Videos kann in einer juristischen Untersuchung leicht bestimmt werden, „wer welche Aufgaben ausgeführt hat“. Das Durchsuchen von unverständlichen Protokolldateien ist somit nicht mehr erforderlich. Regelt die Verantwortlichkeit für Anwender von IT-Systemen. Erstellt Protokolle für Anwendungen, die keine systemeigenen Protokolle generieren.
Virtualisierungssicherheit	Die Virtualisierung sorgt für eine neue Infrastrukturebene, die es zu sichern gilt – den Hypervisor.	Verwaltung privilegierter Anwender auf VMware, während gleichzeitig eine virtualisierungsorientierte Automatisierung von Sicherheitskontrollen auf virtuellen Maschinen erfolgt.	Reduziert die Risiken der Virtualisierung von VMware-Administratoren bis hin zu virtuellen Maschinen.
UNIX Authentication Bridging	Die Verwaltung von Anwender-Accounts und Berechtigungen auf einzelnen UNIX- und Linux-Servern geht mit einem hohen Aufwand einher und kann zu Fehlern führen.	Authentifizierung von Anwendern auf UNIX- und Linux-Systemen für Microsoft Active Directory.	Konsolidiert Authentifizierungs- und Account-Informationen in Active Directory statt einer lokalen Verwaltung der UNIX-Anmeldeinformationen auf jedem System. Reduziert den Verwaltungsaufwand.

„Wenn Sie keine entsprechenden Kontrollen für privilegierte Anwender implementieren, laufen Sie Gefahr, dass sich die Service Levels verschlechtern, dass Kosten für Korrekturmaßnahmen aufgrund von Audits anfallen, Entwickler auf (sensible) Produktionsdaten zugreifen und verärgerte Mitarbeiter die Infrastruktur lahmlegen oder Sie in Geiselhaft nehmen.“[9]

– Forrester Research, Inc.

ca technologies

Identity Management und Governance

Eine der Hauptursachen für Sicherheitsverstöße sind unangemessene Berechtigungen. Dies kann durch falsche anfängliche Zugriffsberechtigungseinstellungen, eine Ansammlung von Berechtigungen über die Zeit oder sogar falsche Zugriffsberechtigungen für einen Anwender verursacht werden, die absichtlich von einem nicht loyalen Administrator festgelegt wurden. Die Ansammlung von Berechtigungen kann die Folge mangelnder Maintenance sein, wenn ein Mitarbeiter in eine andere Position wechselt und alle bisherigen Berechtigungen beibehält. Obwohl falsche Anwenderberechtigungen primär das Risiko von Insiderbedrohungen erhöhen, können auch Außenstehende Zugriff auf diese Accounts erhalten oder nicht benutzte Accounts finden, hinter denen sie ihre Aktivitäten verbergen können. Ein häufiger Fehler vieler Unternehmen besteht darin, dass die Accounts nicht unverzüglich deprovisioniert und nicht alle Zugriffsberechtigungen gelöscht werden, wenn Administratoren das Unternehmen verlassen.

Eine Best Practice-Lösung ist ein umfassender und kontinuierlicher Prozess, mit dem Sie verstehen können, welche Anwender Zugriff auf welche Ressourcen haben sollten. Sie können dann regelmäßig überprüfen, ob jeder Anwender über angemessene Zugriffsberechtigungen verfügt. Identity Governance, die auf hoher Ebene in Rollenmanagement und Identitäts-Compliance aufgeteilt wird, umfasst mehrere identitätsbezogene Prozesse, einschließlich der Bereinigung vorhandener Anwenderberechtigungen, der Einrichtung exakter Rollenmodelle und der Einführung von Richtlinien und Prozessen, mit denen Anwendern geeignete Berechtigungen erteilt werden können. Identity Governance-Lösungen bieten unter anderem folgende Vorteile:

- höhere Sicherheit durch die Automatisierung von Prozessen, die für den erfolgreichen Abschluss von Compliance-Audits erforderlich sind, und die Einrichtung von systemübergreifenden Sicherheitsrichtlinien für Identitäten
- reduzierte Kosten für das Identity Management durch eine Rationalisierung der in Projekten erforderlichen Schritte wie Rollenerkennung, Berechtigungsbereinigung und Zertifizierung
- schnellere IAM-Time-to-Value und bessere Einhaltung von Richtlinien durch schnellere Bereitstellung einer konsistenten, exakten Rollen- und Sicherheitsgrundlage

Datenkontrollen

Im Falle eines Cyberangriffs ist das letztliche Ziel des Angriffs der Diebstahl sensibler Daten oder die Verursachung eines Schadens. Daher sind Datenkontrollen ein wesentlicher Bestandteil einer erfolgreichen Verteidigungsstrategie. Ebenso sind viele Sicherheitsverstöße von Insidern die Folge davon, dass ein Mitarbeiter wertvolles geistiges Eigentum (wie etwa Quellcode) herunterlädt. Um sensible Daten zu schützen, sollte ein Unternehmen seine Daten in den folgenden vier Zuständen schützen und kontrollieren:

1. **Daten während des Zugriffs.** Sensible Informationen, auf die ein versuchter Zugriff über eine Person in einer unzulässigen Rolle erfolgt.
2. **Daten während der Verwendung.** Sensible Informationen, die auf einer lokalen Workstation oder einem Laptop verarbeitet werden.
3. **Daten während der Übertragung.** Sensible Informationen, die über das Netzwerk übertragen werden.
4. **Gespeicherte Daten.** Sensible Informationen, die in Repositories wie Datenbanken, Dateiservern oder Kooperationssystemen gespeichert sind.

Dazu müssen Unternehmen Richtlinien definieren, um die Zugriffssteuerung zu erzwingen, wenn unbefugte Zugriffe oder eine unzulässige Datennutzung erkannt werden. Sobald ein Richtlinienverstoß auftritt, beispielsweise der versuchte Zugriff auf geistiges Eigentum, das Kopieren der Daten auf einen USB-Stick oder der Versuch, die Daten per E-Mail weiterzuleiten, sollte die Lösung die Gefährdung eindämmen und gleichzeitig eine Warnung generieren.

Die Klassifizierung von Informationen ist ein wesentlicher Aspekt jeglicher Datensicherheitsinitiativen. Ohne Kontext und Kenntnisse darüber, um welche Informationen es sich handelt und wo sich die Informationen befinden, kann kein umfassendes Programm zur Datensicherung implementiert werden. Ein Unternehmen muss sensible Daten genau erkennen und klassifizieren können – und zwar basierend auf dem Grad ihrer Sensibilität. Dies schließt auch geistiges Eigentum ein, ebenso personenbezogene Daten, Patienteninformationen sowie andere nicht öffentliche Informationen.

Sobald die Informationen ordnungsgemäß klassifiziert, Richtlinien definiert und Zugriffssteuerungen implementiert wurden, kann ein Unternehmen den Zugriff und die Verarbeitung sämtlicher sensibler Informationen überwachen und kontrollieren. Dies umfasst unterschiedlichste Anwenderaktionen – vom simplen Versuch, auf sensible Daten zuzugreifen und sie zu lesen, bis hin zum Kopieren der Daten auf Wechselmedien, dem Weiterleiten per E-Mail an Dritte außerhalb des Netzwerks oder aber das Auffinden von Daten, die in Repositories wie SharePoint gespeichert sind.

„Nur Amateure greifen Maschinen an; Profis greifen Menschen an.“[10]

– Bruce Schneier

Erweiterte Authentifizierung

Obwohl die Authentifizierungsmethoden bei der Erörterung von Insiderbedrohungen normalerweise nicht berücksichtigt werden, sind diese für den Fall, dass ein Außenstehender einen Insider ausnutzt, um an seine Anmeldeinformationen heranzukommen, doch von großer Bedeutung. Passwörter bieten keine ausreichende Sicherheit für die heutigen kritischen Anwendungen und Informationen. Wenn sich Angreifer bei einem System authentifizieren, gibt es oft kontextbezogene Faktoren, die – wenn sie erkannt werden – eine Warnung hinsichtlich der Berechtigung der Authentifizierung darstellen. Wenn sich beispielsweise ein Mitarbeiter aus der Finanzabteilung in New York plötzlich aus Russland anmeldet oder wenn sich ein Mitarbeiter aus Rom anmeldet, der sich zwei Stunden zuvor aus New York abgemeldet hat, ist es offensichtlich, dass eine betrügerische Authentifizierung stattfindet.

Lösungen für eine risikobasierte Authentifizierung legen eine Risikobewertung für jede versuchte Authentifizierung fest, mit der zu erkennen ist, ob möglicherweise ein versuchter Sicherheitsverstoß vorliegt. In diesen Fällen kann eine zusätzliche, stärkere Authentifizierungsmethode („Step-up-Authentifizierung“) erforderlich gemacht werden, der Versuch kann einfach abgelehnt oder eine Warnmeldung ausgegeben werden.

Virtualisierungssicherheit

Das mit Insiderbedrohungen verbundene Schadenspotenzial ist in letzter Zeit größer geworden, da die Menge an sensiblen Daten explosionsartig angestiegen ist und leistungsstärkere Verwaltungstools verfügbar sind. Insbesondere der Trend zur Virtualisierung hat neue Risiken mit sich gebracht. Zunächst gibt es eine neue Klasse von Administratoren auf dem Hypervisor, die es zu verwalten, überwachen und steuern gilt. Zudem können diese Hypervisor-Administratoren unzählige virtuelle Maschinen mit wenigen Mausklicks ändern, kopieren oder löschen, was Diebstähle und Schäden einfacher, schneller und fataler sowie schwerer erkennbar macht als je zuvor.

Um Herausforderungen für die Sicherheit in einer virtualisierten Umgebung zu überwinden, benötigen Unternehmen einen proaktiven Ansatz statt eines reaktiven Ansatzes für den Umgang mit möglichen Bedrohungen und Fehlern. Als ersten Schritt können die Grundlagen der Sicherheit, die bereits in Ihrer herkömmlichen Infrastruktur berücksichtigt sind, auch auf Hypervisor-Ebene angewendet werden.

Diese Aktionen ermöglichen die Einrichtung einer soliden Sicherheitsbasis, doch allein genommen können sie sich nicht auf all die dynamischen Veränderungen auswirken, die virtuelle Server weniger sicher machen als physische Server. Die virtuelle Infrastruktur muss weiter gesichert werden, indem auch virtualisierungsspezifische Funktionen implementiert werden. Eine virtualisierungsbezogene Automatisierung bietet bahnbrechende Leistungsmerkmale für das Risikomanagement im Zusammenhang mit der Hypervisor-Sicherheit. In Verbindung mit grundlegenden Sicherheitsmaßnahmen schützt sie Ihre virtuelle Umgebung und unterstützt zugleich die schnell wachsenden Anforderungen Ihres Unternehmens.

Abschnitt 3:

Nutzen

Durch die Implementierung von identitäts- und datenbasierten Sicherheitsvorkehrungen reduzieren Unternehmen das Risiko von Verstößen durch Insider und verbessern gleichzeitig ihre Compliance-Programme. Automatisierte und zentral verwaltete Funktionen tragen zur Senkung der Kosten bei, während gleichzeitig die Steuerungsmechanismen für die IT-Sicherheit verstärkt werden. Umfassendes Auditing erleichtert die Einhaltung von Vorschriften, da Unternehmen Steuerungsmechanismen nachweisen und gegenüber Auditoren den effektiven Betrieb der von Ihnen eingesetzten Sicherheitsmechanismen darlegen können.

Die Verteidigung gegen jegliche Art von Insidern stellt grundsätzlich eine große Herausforderung dar. Der Informationsfluss ist für das Funktionieren eines Unternehmens von kritischer Bedeutung. Einschränkungen können operative Probleme zur Folge haben oder den Zugriff der Mitarbeiter auf jene Informationen verhindern, die sie für effizientes und innovatives Arbeiten benötigen.

Doch mit den ***richtigen*** Steuerungsmechanismen kann ein Unternehmen Informationen für eine Vielzahl von Personen freigeben. Diese Steuerungsmechanismen gestatten es einem Unternehmen, auf Basis eines ***begrenzten Vertrauens*** zu agieren. Wenn Unternehmen keine Alles-oder-Nichts-Lösung mehr wählen müssen, können sie bestimmte Informationen für Personen freigeben, denen ein Zugriff darauf früher nicht gestattet war. Unternehmen, die Steuerungsmechanismen auf diese Art einsetzen, machen die Sicherheit zu einem Tool, das die Geschäftstätigkeit unterstützt.

Zudem sollten Unternehmen auch bedenken, dass sie sich mit dem Schutz vor Insiderbedrohungen gleichzeitig auch vor externen Angriffen schützen. Identitäten, darunter auch privilegierte Identitäten, werden oft von Außenstehenden verwendet, nachdem der Angreifer den Netzwerkperimeter durchbrochen hat. Durch die Implementierung eines soliden Sets interner Sicherheitsvorkehrungen schafft ein Unternehmen eine stabile Basis zur Vermeidung von externen Angriffen oder Verringerung des dadurch entstehenden Schadens.

Abschnitt 4.

Schlussbemerkungen

Die Bedrohung durch Insider ist real und nimmt zu. Unternehmen müssen sich dieser Realität stellen und einsehen, dass diese Bedrohung keine abstrakte Vorstellung mehr ist, sondern etwas, das jederzeit eintreten kann. Anstatt sich jedoch vollkommen abzuschotten oder in Passivität zu verfallen und die Unausweichlichkeit solcher Insiderangriffe einfach hinzunehmen, sollten Unternehmen diese Bedrohungen offensiv angehen. Eine wesentliche Komponente bei diesem offensiven Ansatz sollte das Identity and Access Management sein – ergänzt um entsprechende Data Loss Prevention-Lösungen.

Die Bedrohung durch Insider lässt sich niemals komplett beseitigen. Die in diesem Dokument beschriebenen identitätsbezogenen Maßnahmen bilden jedoch das Grundgerüst für ein effektives Programm zum Schutz vor Insiderbedrohungen. Die Unternehmen, die es mit der Bekämpfung von Insiderbedrohungen ernst meinen, sollten einige oder alle diese Merkmale implementieren, da sie so über einen effizienten und bewährten Mechanismus verfügen, um Angriffe durch Insider unter Kontrolle zu halten.

Abschnitt 5:

Literaturhinweise

1 Ponemon Institute, „The Risk of Insider Fraud: Second Annual Study“, Februar 2013

2 Ponemon Institute, „The Risk of Insider Fraud: Second Annual Study“, Februar 2013

3 bigstory.ap.org/article/sentencing-set-corporate-espionage-suspect

4 cert.org/insider_threat

5 newyorker.com/online/blogs/closeread/2013/06/edward-snowden-the-nsa-leaker-comes-forward

6 slate.com/articles/technology/future_tense/2013/02/fiberwan_terry_childs_gavin_newsom_on_why_governments_should_outsource_technology.single

7 articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets

8 online.wsj.com/article/SB10001424052970203753704577255723326557672

9 Forrester Research Inc., „Assess Your Identity And Access Management Maturity“, 26. September 2012

10 schneier.com/crypto-gram-0010

Abschnitt 6:

Informationen über die Autoren

Russell Miller arbeitete über sechs Jahre in verschiedenen Positionen im Bereich der Netzwerksicherheit, von „Ethical Hacking“ bis Produktmarketing. Er ist derzeit Director of Solutions Marketing bei CA Technologies mit Schwerpunkt auf Privileged Identity Management und Virtualisierungssicherheit. Russell Miller hat einen B.A. in Computerwissenschaften vom Middlebury College und einen M.B.A. von der MIT Sloan School of Management.

Merritt Maxim blickt auf 15 Jahre Erfahrung im Produktmanagement und Produktmarketing in der Informationssicherheitsbranche zurück und war dabei für RSA Security, Netegrity und CA Technologies tätig. In seiner aktuellen Rolle bei CA Technologies betreut Merritt Maxim das Produktmarketing für Initiativen von CA in den Bereichen Identity Management und Cloud Security. Merritt Maxim, Co-Autor von „Wireless Security“, bloggt über zahlreiche IT-Sicherheitsthemen. Sie können ihm unter www.twitter.com/merrittmaxim folgen. Merritt Maxim ist BA cum laude der Colgate University und MBA der MIT Sloan School of Management.

Kontaktieren Sie CA Technologies unter ca.com/de.

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht im Mittelpunkt jedes Unternehmens in allen Branchen. Von der Planung über die Entwicklung bis zum Management und der Sicherheit – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, mit zu verändern, ganz gleich, ob in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.