WHITE PAPER | NOVEMBER 2015

Durchbrechen der Kill Chain

Verhindern von Datenmissbrauch mit Privileged Access Management

ca technologies

Kurzfassung

Ausgangssituation

Es vergeht kein Tag, ohne dass wir Nachrichten von einer neuen Datenkompromittierung hören, samt Verlust von Geschäftsgeheimnissen, Finanzdaten oder personenbezogenen Informationen. Diese Vorfälle betreffen alle Bereiche der Wirtschaft: Handel, Bildung und öffentlichen Sektor. Durch Cyberkriminalität entstehen der Wirtschaft weltweit schon heute jährliche Kosten von Hunderten Milliarden Dollar.[1] Es wird prognostiziert, dass diese Kosten ohne sofortige, aggressive Gegenmaßnahmen in weniger als zehn Jahren bei Billionen liegen werden.[2] Nicht in Zahlen angebbar sind die katastrophalen Auswirkungen auf Personen, deren persönlichste und privateste Daten bekannt geworden sind.

Securityspezialisten haben sich bisher bemüht, Perimeter-basierte Verteidigungsmechanismen einzurichten, die – einfach gesagt – die Bösen draußen halten und die Guten reinlassen sollten. Die nicht enden wollende Abfolge von Kompromittierungen, die wir heute sehen, zeigt deutlich, dass diese Perimeter ihren Hauptzweck nicht erfüllen. Durch solche Vorfälle wird Unternehmen immer stärker bewusst, dass eine im Wesentlichen neue Securityschicht, deren Schwerpunkt speziell auf Schutz und Management von Identitäten liegt, inzwischen unbedingt erforderlich ist, um die Flut der Kompromittierungen aufzuhalten. Die wichtigsten dieser Identitäten sind die der privilegierten Anwender. Da diese Anmeldeinformationen den „Generalschlüssel“ darstellen, werden sie zunehmend gestohlen und als Hauptangriffsvektor benutzt.

Chance

Securityteams können eine Anzahl ausgereifter Technologien und Prozesse nutzen, die allgemein als „Privileged Access Management“ bezeichnet werden. Sie ermöglichen es, Angreifer abzuwehren und abzuschrecken. Böswillige interne und externe Anwender verwenden eine vorhersagbare, logische Abfolge von Schritten, um erfolgreiche Angriffe durchzuführen. Diese Abfolgen, die ursprünglich von Cybersecurity-Teams bei Lockheed Martin identifiziert und beschrieben wurden,[3] werden als „Kill Chains“ (Angriffsabläufe) bezeichnet. Wenn die Abfolge der Schritte an irgendeinem Punkt aufgehalten werden kann, kann verhindert werden, dass der Angriff erfolgreich ist, oder er kann immerhin abgemildert werden. Das Privileged Access Management bietet die Mittel, um Angreifer bei mehreren Schritten im Angriffslebenszyklus abzuwehren. In diesem White Paper untersuchen wir eine etwas vereinfachte Version eines Angriffsablaufs und stellen an einem Beispiel dar, wie das Privileged Access Management dazu beitragen kann, Angriffe abzuwehren und Unternehmen vor Kompromittierungen zu schützen.

Nutzen

Der finanzielle Nutzen, den die Verhinderung dieser Kompromittierungen bedeutet, ist offensichtlich. Schwerer zu messen, aber häufig noch wichtiger, ist die Vermeidung der „immateriellen“ Kosten für Schäden an Marke und gutem Ruf, Vertrauensverluste bei Partnern und Kunden sowie Auswirkungen auf die Börsenbewertung des Unternehmens. Auch wenn diese Kosten sehr wichtig sind, sind das Schlimmste die katastrophalen Auswirkungen, die der Diebstahl detaillierter persönlicher Informationen auf arglose Personen haben kann, die dem Unternehmen vertraut hatten. Es ist offensichtlich, dass ein Privileged Access Management mit der Möglichkeit, diese weitreichenden Schäden zu mindern, sehr wichtig ist.

Herausforderung Datenkompromittierungen: eskalierende Risiken und unkalkulierbare Schäden

Wenn wir uns die aktuelle Flut von Securityvorfällen ansehen, fällt besonders der Vorfall bei Target auf, der Ende 2013 begann. Hierbei wurden um die 70 Millionen Zahlungskarten-Datensätze gestohlen. Dies war nicht die erste – und auch nicht die größte – Datenkompromittierung der Geschichte, nicht einmal des Jahres 2013. Eine Reihe von Faktoren führte jedoch dazu, dass der Sicherheitsvorfall bei Target das Interesse zahlreicher wichtiger Gruppen auf die hohen Schäden lenkte, die diese fortwährenden Angriffe verursachen. Seit der Kompromittierung bei Target gab es zahllose kleinere, weniger publik gewordenen Fälle sowie eine stetige Abfolge größerer Vorfälle, wie bei Home Depot und JP Morgan Chase etwa ein Jahr später, und den zum Zeitpunkt der Erstellung dieses White Papers aktuellsten Fall, die Kompromittierung der extrem sensiblen persönlichen Daten von ca. 15 Millionen T-Mobile-Kunden bei Experian.

> „Für digitale Unternehmen wird das Privileged Identity Management sehr wichtig, aber zugleich auch eine große Herausforderung. Es ist wichtig, weil ein einziger Administrator mit böser Absicht oder ein Diebstahl von Administratoranmeldeinformationen verheerende Auswirkungen auf Ihre Kunden, Umsätze und Ihren langfristigen guten Ruf haben kann."
>
> – Forrester Research[4]

Die Kosten für derartige Cyberkriminalität im Jahr 2014 wurden anhand von Daten von Intel Security und dem Center for Strategic and International Studies auf ca. 400 Mrd. US-Dollar geschätzt. Es kann schwierig sein, sich solche riesigen Zahlen vorzustellen. Vergleichen Sie daher die Kosten von 400 Mrd. USD mit dem geschätzten Gewinn aus dem weltweiten Drogenhandel, der „nur" geschätzte 300 Mrd. USD jährlich ausmacht. Die Auswirkungen der Cyberkriminalität sind sogar größer als das Bruttoinlandsprodukt vieler reicher Länder, wie beispielsweise Singapur mit ebenfalls ca. 300 Mrd. USD jährlich. Dies ist also offensichtlich ein großes finanzielles Problem, und die Daten legen nahe, dass es ohne schnelle Gegenmaßnahmen nur noch schlimmer werden wird. McKinsey prognostiziert weltweite jährliche Auswirkungen der Cyberkriminalität von 3 Billionen US-Dollar in 10 Jahren. Dies ist um Größenordnungen mehr als die heutigen Kosten.

Dies sind offensichtlich schädigende Vorfälle. Die Unternehmen, die die Kompromittierungen erlitten, und andere ähnliche Fälle, verloren Marktkapitalisierung, Abschlüsse, Kundenvertrauen und Profite. Hinzu kommen die finanziellen und emotionalen Schäden der Personen, die unter diesen Kompromittierungen leiden, als Konsequenzen von Verbrechen wie Identitätsdiebstahl. Als wenn dies nicht schon bedrückend genug wäre, gibt es noch schlimmere Nachrichten hinsichtlich anderer Vorfälle, die in jüngster Zeit auftreten.

Erstens sehen wir neuerdings Angriffe, die offensichtlich darauf abzielen, den Betrieb der betreffenden Unternehmen wesentlich zu behindern. Möglicherweise haben Sie noch nie von Code Spaces gehört – dies war ein kleineres Unternehmen in Großbritannien, das Cloud-basierte Versionssteuerungs- und Backupservices für Entwickler anbot. Im Juni 2014 konnte ein Angreifer Administratoranmeldeinformationen von Code Spaces für die Managementkonsole von Amazon Web Services (AWS) erlangen. Der Angreifer erstellte mehrere Accounts und Backdoors und forderte dann ein Lösegeld von Code Spaces. Als autorisierte Administratoren versuchten, den Angreifer aus ihrem System zu entfernen, war es schon zu spät. Der Angreifer verfügte über vollständigen Administratorzugriff auf das gesamte Managementsystem von Code Spaces und begann, als Gegenschlag die gesamte IT-Infrastruktur des Unternehmens schnell zu zerstören – Server, Anwendungen und vor allem System- und Datenbackups. Der Angriff dauerte nur wenige Stunden. Das Unternehmen musste nach wenigen

Tagen seine Geschäftstätigkeit einstellen.[5] Die Code Spaces-Kompromittierung ist ein drastisches Beispiel, aber es gibt eine Reihe weiterer Beispiele (wie die Vorfälle bei Sony Pictures Entertainment und Saudi Aramco), die diesen Trend veranschaulichen.

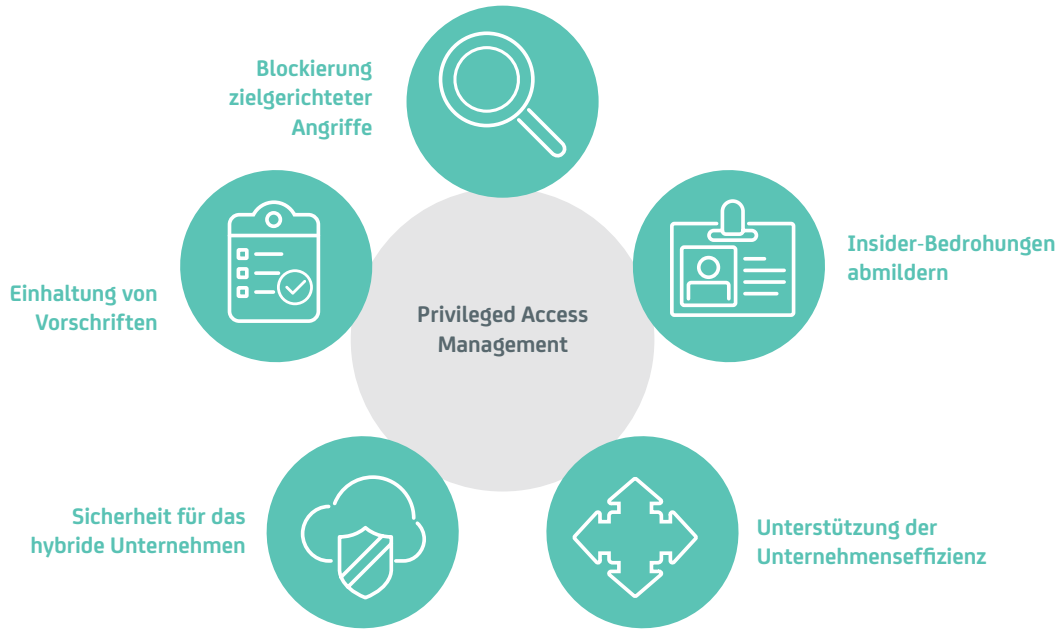
Von hier aus ist es nur ein kleiner Schritt zum aktuellsten Trend, der offenbar die Cyberspionage ist. Zu den ersten Anzeichen dieser Angriffe gehörten Kompromittierungen bei Versicherungen wie Anthem, Premera und CareFirst Anfang 2015. Während nie formell Staaten hierfür verantwortlich gemacht wurden, wird weithin vermutet, dass der Diebstahl von Millionen Datensätzen persönlicher Informationen Teil einer größeren Kampagne war, Unterlagen zu Personen zusammenzustellen, die kritische Positionen in Behörden, Rüstungsunternehmen, Finanzen und Telekommunikation innehatten, zusammen mit geopolitischen Entscheidungsträgern und anderen. Der Zeitraum der Kompromittierungen fiel mit dem Versand einer vertraulichen Warnung des FBI zusammen, dass chinesische Hacker personenbezogene Informationen aus Netzwerken von Unternehmen und Behörden in den USA zu stehlen versuchten.[6] Inzwischen haben wir von der Kompromittierung beim Office of Personnel Management (OPM) in den USA erfahren, bei der persönliche Daten gestohlen wurden, einschließlich der umfangreichen biografischen, finanziellen, beruflichen und persönlichen Vorgeschichten von Personen, für die Sicherheitsüberprüfungen anstanden.

Chance: privilegierte Accounts – die neue vorderste Front

Fassen wir kurz zusammen. Datenkompromittierungen sind ein großes Problem, das immer größer wird. Es geht um immer mehr, und wir sehen uns immer intelligenteren – und immer finanzstärkeren – Gegnern gegenüber. Auch der optimistischste Leser kann hier zu Recht zumindest eine Spur von Pessimismus empfinden. Was können wir tun, um derartige Herausforderungen zu bewältigen?

Abbildung A

Privileged Access Management hilft Unternehmen, fünf allgemeine Ziele zu erreichen



Die gute Nachricht ist: Es gibt guten Grund zur Hoffnung, weil bei praktisch allen diesen Angriffen eine Gemeinsamkeit beobachtet wird. Diese Gemeinsamkeit sind privilegierte Anwender, und genauer die privilegierten Accounts und Anmeldeinformationen, mit denen diese Personen unsere IT-Infrastruktur konfigurieren, warten und betreiben. Diejenigen Anmeldeinformationen zu stehlen und auszunutzen, die privilegierten Zugriff auf IT-Infrastruktur bieten, hat sich als kritischer Erfolgsfaktor und primärer Angriffsvektor bei allen bisher erörterten Kompromittierungen erwiesen.

> „Schon 2018 wird die mangelnde Fähigkeit von Unternehmen, den richtigen Umfang und die richtigen Grenzen für den privilegierten Zugriff festzulegen, für bis zu 60 % des Missbrauchs durch Insider und der Datendiebstähle verantwortlich sein, gegenüber mehr als 40 % heute."
>
> – Gartner[7]

Bevor wir uns die zentrale Rolle des privilegierten Zugriffs in erfolgreichen Kompromittierungen ansehen, ist es hilfreich, kurz zu untersuchen, wer diese privilegierten Anwender sind, denn die Anzahl der Personen mit privilegiertem Zugriff sowie die Anzahl der Accounts und Anmeldeinformationen, die tatsächlich für diesen Zugriff verwendet werden, sind viel größer als allgemein angenommen.

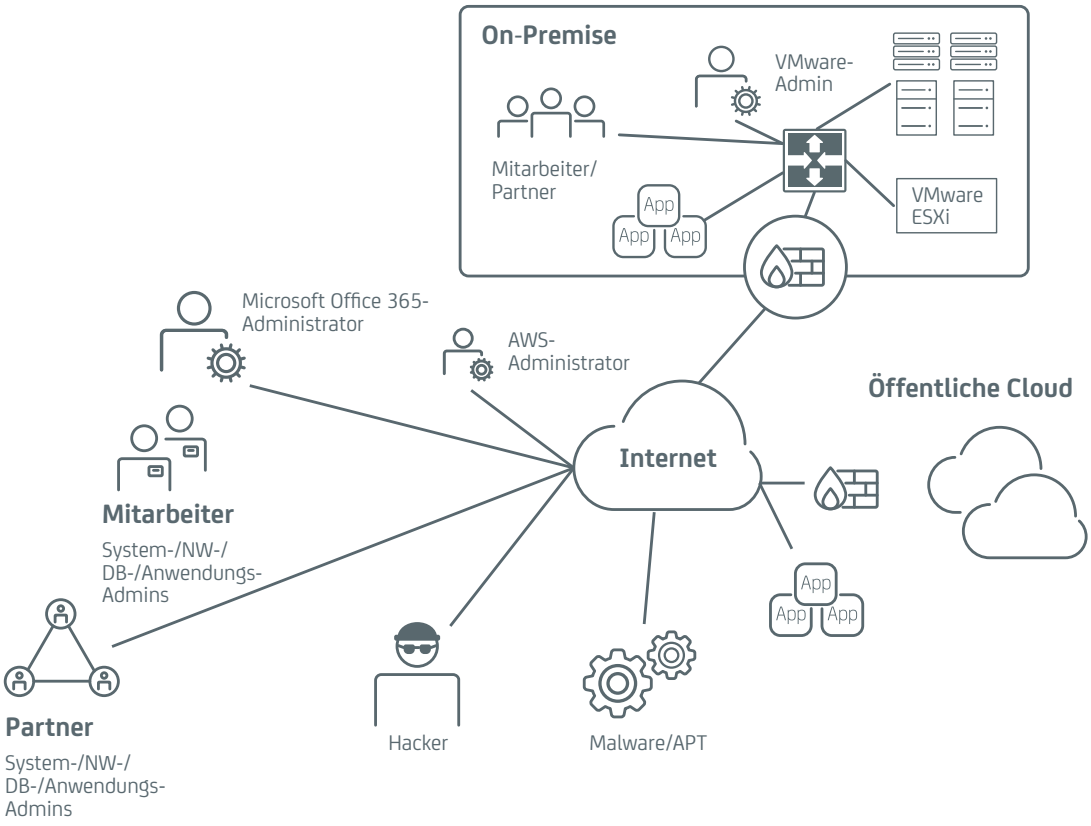


Abbildung B

Privilegierte Accounts: die neue vorderste Front

Jahrelang haben wir als privilegierte Anwender im Allgemeinen nur die Personen betrachtet, die innerhalb des Unternehmens direkte, praktische Verantwortung für die System- und Netzwerkadministration haben. Dies führt dazu, das Risiko zu unterschätzen und die Herausforderung des Privileged Access Management als die Aufgabe anzusehen, die so genannte „Bedrohung durch Insider" unter Kontrolle zu halten. Zwar ist es wahr, dass böswillige Insider riesige Schäden verursachen können, aber solche Vorfälle sind relativ selten und machen nur eine kleine Anzahl der Kompromittierungen aus.

In Wirklichkeit sind viele privilegierte Anwender nicht Insider, sondern Zulieferer, Auftragnehmer, Geschäftspartner und andere, denen privilegierter Zugriff auf Systeme im Unternehmen gewährt wurde. In vielen Unternehmen ist die Anzahl solcher Drittanwender wahrscheinlich größer als die Anzahl herkömmlicher privilegierter „Insider". Außerdem hat die Erfahrung gezeigt, dass diese Dritten ein größeres Risiko darstellen. Betrachten wir die erwähnten Kompromittierungen – wie die Vorfälle bei Target, Home Depot, dem OPM und anderen – bei denen die Anmeldeinformationen eines autorisierten Dritten kompromittiert und dann für den unerlaubten Zugriff auf das Netzwerk und seine Ressourcen verwendet wurden.

Außerdem steigt die Anzahl privilegierter Anwender beim Übergang zur Cloud und zu Technologien wie der Virtualisierung. Vor allem, was die Cloud angeht, sind viele dieser privilegierten Anwender oft keine herkömmlichen IT-Mitarbeiter. Betrachten Sie beispielsweise den Fall von Mitarbeitern aus Geschäftsbereichen, die servicebasierte Angebote erwerben, wobei im schlimmsten Fall die herkömmliche IT- und Securityabteilung von dem Risiko gar nichts wissen.

Und vergessen wir nicht, dass immer mehr privilegierte Anwender gar keine Anwender sind – oder jedenfalls keine Menschen. In Cloud- und Virtualisierungsumgebungen hat das Aufkommen automatisierter Konfigurations- und Provisionierungstools, die von Scripts und Programmen gesteuert werden, sogar noch mehr „Anwender" mit umfangreichen Zugriffsrechten und Befugnissen für große Bereiche der Infrastruktur mit sich gebracht. Ein Ergebnis dieser automatisierten Systeme ist die oft unbekannte Anzahl der Scripts und Programme, die sich in jahrelangem Betrieb angesammelt haben, die Administratorzugriff oder sensiblen Zugriff auf Ressourcen wie Datenbanken oder andere Anwendungen und Systeme erfordern. In beiden Fällen werden dieser Zugriff und diese Transaktionen ordnungsgemäß durch Authentifizierung gesteuert. Allerdings sind die erforderlichen Anmeldeinformationen im Allgemeinen in Anwendungen oder Konfigurationsdateien hartcodiert. Dort sind sie ein leichtes Ziel für böswillige Anwender – ganz gleich, ob Insider oder Outsider.

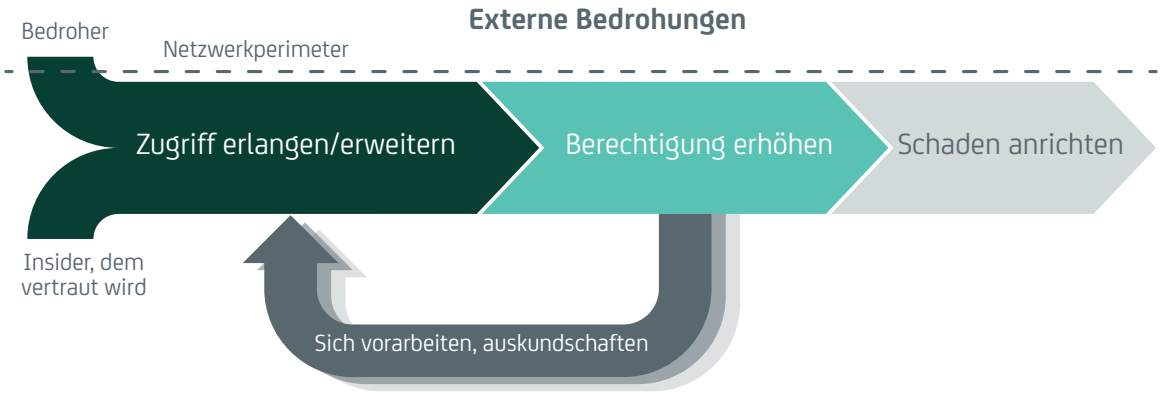
Und was vielleicht am Wichtigsten ist: Wir müssen bedenken, dass wir nicht nur über privilegierte Anwender sprechen, sondern über alle privilegierten Accounts und ihre Anmeldeinformationen in einem typischen Unternehmen. Diese Anmeldeinformationen stellen die wichtigste Bedrohung dar, da Angreifer sie ausnutzen müssen, um erfolgreich zu sein.

Der Angriffsablauf (Kill Chain) - und warum er funktioniert

Der Angriffsablauf besteht aus einer konsistenten und vorhersagbaren Reihe von Schritten, die ein Angreifer ausführen muss, um sein Ziel erfolgreich zu erreichen. Auch wenn einige Angriffsabläufe ziemlich komplex sein können, können die wichtigsten Schritte des typischen Angriffsablaufs einer Datenkompromittierung vereinfacht dargestellt werden.

Abbildung C

Ein Beispiel für einen vereinfachten Angriffsablauf



Es handelt sich um vier Schritte:

- **Zugriff erlangen:** Zuerst muss der Zugriff auf das Netzwerk erlangt werden. Für einen echten Insider oder vielleicht einen Dritten, der als vertrauenswürdig erachtet wird, ist das leicht – es müssen nur die vorhandenen Anmeldeinformationen und Zugriffsrechte ausgenutzt werden. Für einen Angreifer ist es jedoch nicht viel schwieriger, das Gleiche zu tun. Die wachsende Beliebtheit von Social Media-Websites wie LinkedIn führt dazu, dass es relativ leicht ist, spezifische Personen in einem Unternehmen zu identifizieren und anzugreifen, die wahrscheinlich über privilegierten Zugriff auf Systeme verfügen. Spearphishing wird immer ausgeklügelter. Dies bedeutet, dass es für einen Angreifer leichter ist als je zuvor, auch die erfahrensten und kenntnisreichsten Personen dazu zu verleiten, dass sie Anmeldeinformationen mitteilen – vor allem relativ einfache wie Anwender-IDs und Passwörter.
- **Berechtigungen erhöhen:** Nachdem ein Angreifer Zugriff erlangt hat, besteht einer der ersten Schritte darin, die Berechtigungen zu erhöhen, im Allgemeinen durch Kompromittierung anderer privilegierter Anmeldeinformationen. Dieser Schritt unterstützt zwei wichtige Maßnahmen. Erstens ermöglicht er dem Angreifer Schritte, wie die Protokollierung zu manipulieren oder zu deaktivieren, die verhindern, dass seine Existenz und Aktivität erkannt wird. Zweitens schafft er die Voraussetzungen für den nächsten Schritt im Angriffsablauf: auszukundschaften und sich vorzuarbeiten.
- **Sich vorarbeiten und auskundschaften:** Außer wenn ein Angreifer sehr viel Glück hat, ist das erste System, auf das der Zugriff erschlichen wurde, nicht das eigentliche Ziel. Das Ziel – Zahlungskarten-Verarbeitungssysteme, proprietäre Daten, persönliche Datensätze u. ä. – befindet sich fast immer anderswo im Netzwerk auf anderen Systemen. Der nächste Schritt im Angriffsablauf besteht darin, das Netzwerk auszukundschaften und auf Systeme und Server zu gelangen, die näher am eigentlichen Ziel sind.
- **Prozess bei Bedarf wiederholen:** Von hier an ist es einfach – es genügt, den Prozess zu wiederholen, bis das eigentliche Ziel erreicht ist. Die Erfahrung hat gezeigt, dass Angreifer auffallend geduldig sein können und sich die Zeit nehmen, Netzwerke zu erforschen und zu durchqueren, um ihr Ziel zu erreichen. Öffentliche Berichte zu Kompromittierungen erwähnen häufig, dass Angreifer monate- oder manchmal sogar jahrelang im Netzwerk eines Opfers aktiv waren. Wenn der Angreifer schließlich sein Ziel erreicht hat, folgt die eigentliche Aktion – Systeme zu stören, Daten zu stehlen usw.

Unternehmen erleichtern Angreifern häufig die Durchführung dieses Angriffsablaufs, vor allem, wenn ihnen sogar rudimentäre Prozesse und Tools des Privileged Access Management fehlen. Häufige Fehler sind:

- **Verwendung unzureichender Authentifizierungmethoden** für den Zugriff auf das Netzwerk oder auf spezifische Ressourcen. Dazu gehört, standardmäßige Administratoraccounts und -passwörter nicht zu löschen sowie zu einfache Anmeldeinformationen zu verwenden, wie einfache Kombinationen aus Anwender-ID und Passwort, die leicht gestohlen oder kompromittiert werden können.
- **Unzulängliches Management von Passwörtern und Schlüsseln**, bei dem Anmeldeinformationen nicht häufig und regelmäßig geändert werden. In Unternehmen mit Tausenden von Ressourcen kann dies sehr problematisch sein, weil es verlockend ist, betriebliche Probleme zu vermeiden und den Aufwand zu senken, indem schlechte Praktiken wie die Wiederverwendung von Anmeldeinformationen und das Fehlen regelmäßiger Änderungen angewendet werden.
- **Zulassen der gemeinsamen Nutzung von Accounts**, vor allem mächtigen Accounts wie „root“ oder „admin“. Dieses Vorgehen bedeutet mehrere Risiken, da ein Anwender leicht eine Berechtigung an andere weitergeben kann. Wenn viele Personen auf eine Berechtigung zugreifen können, ist es außerdem praktisch unmöglich, nachzuweisen, wer eine bestimmte Aufgabe auf einem System durchgeführt hat. Dies erschwert forensische Nachforschungen und die Problembehebung.
- **Gleichsetzen von Authentifizierung mit Access Control.** Viele Netzwerke sind schlecht segmentiert. Wenn eine Person sich erst einmal im Netzwerk befindet, kann sie daher viel mehr Ressourcen sehen, als notwendig oder sinnvoll ist. Dies erleichtert es Angreifern, auszukundschaften und sich vorzuarbeiten, sodass sie ihr eigentliches Ziel leichter erreichen können.
- **Fehlende Überwachung und Analyse von Aktivitäten privilegierter Anwender** können mehrere Probleme begünstigen. Wenn Aktivitäten nicht überwacht oder regelmäßig analysiert werden, kann verdächtiges Verhalten übersehen werden, sodass Angreifer freie Hand haben. Es liegt in der Natur des Menschen, Regeln zu dehnen oder zu brechen, wenn sie wissen, dass dies mit hoher Wahrscheinlichkeit unerkannt bleibt.

Empfehlungen: Durchbrechen des Angriffsablaufs

In drei wichtigen Schritten bietet das Privileged Access Management zahlreiche Möglichkeiten, den Angriffsablauf zu durchbrechen, Angreifer aufzuhalten und Kompromittierungen zu verhindern.

Schritt 1: Verhindern unbefugter Zugriffe

Vorzuschreiben, dass der privilegierte Zugriff auf Ressourcen über ein netzwerkbasiertes Gateway erfolgt, ist eine einfache Möglichkeit, die strenge Authentifizierung zu erzwingen. Natürlich sollte ein solches System in die vorhandene Identity Management-Infrastruktur integriert werden. Das System sollte daher Verknüpfungen mit vorhandenen Identitätsspeichern unterstützen, wie Active Directory oder LDAP-Verzeichnissen oder in einigen Umgebungen auch RADIUS oder TACACS+. Während das System die lokale Authentifizierung unterstützen kann und soll, besitzt Ihr Unternehmen meist bereits einen gut eingeführten Identitätsspeicher. Da diese Systeme bereits sowohl autorisierte Anwender als auch Rollen und Berechtigungen definieren, sollten Sie diese Daten als die Grundlage für privilegierte Zugriffe nutzen.

Dies ist jedoch nur ein Grundverhalten. Da es relativ leicht ist, die Anmeldeinformationen eines Anwenders zu stehlen, kann der Weg durch ein solches Gateway für einen Angreifer ein relativ leichter Schritt sein. Um dies zu verhindern, ist es wichtig, die Verwendung der mehrstufigen Authentifizierung (Multi-Factor Authentication, MFA) für privilegierte Zugriffe erforderlich zu machen. Durch Hinzufügen der MFA wird es für einen Angreifer wesentlich schwieriger, sich Zugriff auf das Netzwerk zu verschaffen. Früher war die MFA eine teure Technologie mit hohem Administrationsaufwand. Technologische Fortschritte haben jedoch die wirtschaftlichen Aspekte der Implementierung der mehrstufigen Authentifizierung drastisch

verändert. Da privilegierte Zugriffe hohe Risiken mit sich bringen, zeigt sogar eine einfachste Kosten-Nutzen-Analyse, dass eine mehrstufige Authentifizierung notwendig ist.

Außerdem ist sie für die Einhaltung von Vorschriften und für Audits wichtig. Die US-Bundesregierung gehörte hier zu den Vorreitern. Sie richtete Standards ein, die die Verwendung so genannter PIV/CAC-Karten für den Administratorzugriff auf Systeme vorschrieben. „PIV" steht für „Privileged Identity Verification" (für zivile Behörden) und „CAC" für „Common Access Card" (ein ähnliches Hilfsmittel für das Militär). Diese Karten ermöglichen eine PKI-basierte Identifizierung einer Person. Zusammen mit einem Identitätsnachweisverfahren bietet dies hohe Sicherheit hinsichtlich der Identität eines Anwenders. Ähnliche Standards wurden auch zu einer Reihe von Compliance-Vorgaben hinzugefügt, darunter beispielsweise die aktuelle Revision des Payment Card Industry Data Security Standard (PCI-DSS).

Andere offensichtliche Maßnahmen, die ergriffen werden können, um das Risiko unbefugter Zugriffe zu mindern, sind Einschränkungen für den Systemzugriff, die auf der IP-Adresse des Anwenders bei der Anmeldung oder auf der Tageszeit basieren. Derartige Kontrollmechanismen können über ein Privileged Access Management-Gateway sowie agentenbasiert für bestimmte Server oder Ressourcen implementiert werden. Wenn ein bestimmter Anwender sich sowieso nur zu bestimmten Tageszeiten oder von bestimmten Orten anmeldet, können Sie den Zugriff entsprechend beschränken. Außerdem sollten Sie möglicherweise Anmeldungen von einer Reihe von IP-Adressen vollständig blockieren, von denen aus ein Zugriff niemals erwartet würde oder akzeptabel wäre.

Ein zweiter Aspekt dieses Problems besteht darin, die Anmeldeinformationen zu schützen, die für den tatsächlichen Zugriff auf verwaltete Systeme verwendet werden. Wie bereits umrissen, werden diese Anmeldeinformationen allzu häufig schlecht geschützt, wahllos weitergegeben oder schlecht verwaltet. Dies bedeutet offensichtliche Risiken. Idealerweise stellt ein Privileged Access Management-System einen „Safe" für Anmeldeinformationen bereit, in dem Passwörter und Schlüsselpaare verschlüsselt gespeichert werden können, sodass spähende oder böswillige Anwender sie nicht erhalten können. Dieser „Safe" muss es ermöglichen, Anmeldeinformationen aktiv zu verwalten und mit Systemen zu interagieren, um Passwörter anhand von Standards zu ändern, die dem Risikolevel des Unternehmens oder der Ressource angemessen sind. Diesen Prozess zu automatisieren, senkt sowohl Securityrisiken (da es möglich ist, Anmeldeinformationen auf Tausenden oder sogar Hunderttausenden Ressourcen regelmäßig zu aktualisieren und sie zugleich zu schützen) als auch betriebliche Risiken, da automatisierte Aktualisierungen von Passwörtern und Schlüsseln weniger fehleranfällig sind. In Kombination mit Single Sign-On für privilegierte Anwender kann ein hohes Securitylevel erreicht werden, da es möglich ist, einem Anwender Zugriff auf ein System zu bieten, ohne ihm zugleich Zugriff auf die entsprechenden Anmeldeinformationen zu geben. Und Anmeldeinformationen, die ein Anwender nicht kennt, kann dieser Anwender auch nicht stehlen, weitergeben oder versehentlich einem trickreichen Angreifer verraten.

Schritt 2: Begrenzen, wie sehr Anwender Berechtigungen erhöhen, Systeme ausforschen und sich vorarbeiten können

Dies bildet den Übergang zum nächsten Schritt für das Durchbrechen der Kill Chain: Begrenzen Sie die Möglichkeiten, die ein Anwender hat, um das Netzwerk auszuforschen und sich darin zu bewegen. In den meisten Netzwerken ist die Authentifizierung im Endeffekt dasselbe wie die Access Control: die Anmeldung am Netzwerk bedeutet häufig Zugriff auf Ressourcen im gesamten Netzwerk. Dies ist offensichtlich hervorragend für Angreifer: Sie haben die Zeit und häufig die Mittel, um sich von einem System zum anderen zu bewegen und ihrem Ziel näher zu kommen.

Funktionen wie ein Single Sign-On für privilegierte Anwender sind gegen alle diese Herausforderungen wirksam. Dieser Ansatz basiert auf dem Prinzip der minimalen Zugriffsberechtigungen, auch als Zero-Trust Access Control bezeichnet. Indem die Authentifizierung und der Zugriff auf das Privileged Access Management-System vom tatsächlichen Zugriff auf verwaltete Ressourcen getrennt werden, können Anwender nur die Systeme und Ressourcen sehen, die von der Richtlinie definiert und gestattet werden. Wenn die Arbeitsaufgaben eines Anwenders den Zugriff auf einen einzelnen Server oder eine Klasse von Ressourcen erfordern, sollte der Anwender auch nur genau dies im Netzwerk sehen. Indem Sessions per Proxy oder Broker zwischen dem Privileged Access Management-System und den verwalteten Ressourcen vermittelt werden, können Sie ihre Autorität über ein System begrenzen und steuern, welche Befehle sie ausgeben können. Dies begrenzt die Möglichkeit weiter, Berechtigungen zu erhöhen oder sich im Netzwerk vorzuarbeiten.

Beispielsweise kann ein Anwender sich in einer Session mit Proxy mit einem Standardaccount anmelden, sogar mit einem mächtigen wie „root". Da das System Befehlsfilter erzwingen kann, ist es möglich, diese Person auf bestimmte Befehle zu beschränken oder nicht autorisierte zu verhindern. Beispielsweise hat ein Anwender die Aufgabe, Software auf einer Reihe von Servern zu aktualisieren, und es ist hierfür notwendig, als „root" angemeldet zu sein. Mit Befehlsfiltern ist es möglich, dass der Anwender sich anmeldet und nur genau die Befehle ausführen kann, die für die Aufgabe erforderlich sind. Andere Befehle, wie das Beenden eines Prozesses oder der Neustart eines Systems, können verhindert werden.

Zusätzliche Kontrollmechanismen ermöglichen variable Reaktionen auf Versuche, gegen die Richtlinien zu verstoßen. Angenommen, ein Anwender gibt einen nicht autorisierten Befehl aus. Ihre Richtlinien ergeben möglicherweise, dass dies wahrscheinlich das Ergebnis einer legitimen Notwendigkeit oder einfach ein Fehler war. In diesem Fall kann eine Warnung an den Anwender ausgegeben und die Befehlsausführung verhindert werden. Wiederholte Versuche oder schwerwiegendere Verstöße können dazu führen, dass die Session beendet wird oder sogar der Account des Anwenders deaktiviert wird, bis ein Administrator sich den Vorfall genauer angesehen hat.

Indem hostbasierte Agenten hinzugefügt werden, können ähnliche Funktionen erreicht werden, aber häufig mit weit spezifischeren Kontrollmechanismen, wie der Möglichkeit, den Zugriff auf Dateien und Verzeichnisse strikt zu beschränken oder Dateien auf Veränderungen zu überwachen. Außerdem kann verhindert werden, dass ein Anwender sich im Netzwerk vorarbeitet. Ein Angreifer, der Zugriff auf ein System erlangt hat, versucht beispielsweise, einen SSH- oder TELNET-Befehl auszugeben oder eine RDP-Remotesession mit einem Zielsystem zu eröffnen. Auch hier kann das Privileged Access Management-System Richtlinien untersuchen und ermitteln, ob die Aktivität zulässig ist. Wenn nicht, wird die Ausführung des Befehls verhindert, und der versuchte Verstoß wird protokolliert.

Schritt 3: Überwachen, Aufzeichnen und Auditing von Aktivitäten

Im Idealfall gelangt ein Angreifer nie an den Punkt, sein eigentliches Ziel erreichen zu können; die zahlreichen Kontrollmechanismen und Überprüfungen, die ein Privileged Access Management-System erzwingt, bieten genug Möglichkeiten, den Angriffsablauf zu durchbrechen. Der letzte Schritt der Überwachungs-, Aufzeichnungs- und Auditingaktivitäten dient als zusätzliche Abschreckung für Kompromittierungen und bietet wesentliche Vorteile, falls eine Kompromittierung im Endeffekt erfolgreich ist.

Wie gesagt, kann schon das Wissen, dass alle Aktivitäten aufgezeichnet und analysiert werden, böswilliges Verhalten oder scheinbar unschuldige, aber potenziell gefährliche Untersuchungen von Systemen wirksam abschrecken. Außerdem bieten umfangreiche Protokollierungs-, Warnungs-, Aufzeichnungs- und Reportingfunktionen ein „Frühwarnsystem", das andere Administratoren sowie Manager und Auditoren über verdächtiges oder ungewöhnliches Verhalten informiert. Warnungen und Ereignisse weisen sofort auf Richtlinienverstöße und Kompromittierungsversuche hin, sodass schnelle Reaktionen möglich sind. Protokolle können einzeln oder über ein Protokollmanagement- oder SIEM-System im Kontext anderer Systemaktivitäten analysiert werden, um weitere Indizien für verdächtige Ereignisse zu erhalten, sodass eine Untersuchung möglich ist, bevor eine Kompromittierung auftritt.

Da gemeinsam genutzte Administratorkonten so häufig sind, ist die Zurechenbarkeit von Aktionen mit einem solchen Account zu einer bestimmten Person eine wichtige Anforderung, um Vorschriften einhalten zu können.

Und schließlich bietet die Aufzeichnung von Sessions eine Reihe von Vorteilen. Manchmal machen Administratoren Fehler. Die Aufzeichnung von Sessions kann in solchen Fällen hilfreich sein, da sie es ermöglicht, im Nachhinein genau zu sehen, welche Maßnahmen bei einer Interaktion durchgeführt wurden. Dies kann die Problembehebung beschleunigen, wenn beispielsweise ein Problem bei einem System erkannt wird. Wenn in einer früheren Arbeitsschicht ein Update oder eine Konfigurationsänderung durchgeführt wurde, kann es schwierig und zeitaufwendig sein, genau zu ermitteln, was durchgeführt wurde. Sessionaufzeichnungen können unmittelbar wiedergegeben werden, um die Wiederherstellung zu beschleunigen. Außerdem können sie zu Schulungszwecken verwendet werden, sodass es leichter ist, vorzuführen, wo ein Fehler unterlaufen ist und welche Aktion richtig gewesen wäre.

Natürlich können solche Aufzeichnungen und Protokolle im schlimmsten Fall, bei einer erfolgreichen Kompromittierung, entscheidend sein, um genau zu ermitteln, welche Aktionen für ein System durchgeführt wurden, welche Informationen abgerufen wurden und wie die Ressource kompromittiert wurde. All dies beschleunigt forensische Nachforschungen, unterstützt die Schadensermittlung und bietet wertvolle Informationen, die verwendet werden können, um das Risiko zukünftiger Kompromittierungen zu verringern.

Nutzen

Datenkompromittierungen – mit allen zugehörigen Kosten und Schäden – werden unweigerlich immer wieder versucht. Wie hier gezeigt, folgen Angreifer hierbei jedoch normalerweise einem beschreibbaren, vorhersagbaren Verfahren. Das Privileged Access Management bietet zahlreiche Funktionen und Kontrollmechanismen, die Angreifer daran hindern, wichtige Schritte ihrer Angriffe durchzuführen, unterbricht also den Angriffsablauf. Außerdem unterstützt es bei einem erfolgreichen Angriff die Verringerung von Risiken, die Minimierung von Schäden und die Beschleunigung der Wiederherstellung. Die Implementierung einer umfassenden Lösung für das Privileged Access Management bietet folgende Vorteile:

- **Risikominderung:** Verhindern Sie unbefugte Zugriffe und beschränken Sie bei genehmigten Netzwerkzugriffen den Zugang zu Ressourcen. Schützen Sie Passwörter und andere Anmeldeinformationen vor unbefugten Zugriffen und vor Kompromittierung. Begrenzen Sie die Aktionen, die Anwender für Systeme durchführen können: Verhindern Sie, dass jemand unbefugte Befehle ausgibt oder sich in Ihrem Netzwerk vorarbeitet.
- **Erhöhung der Zurechenbarkeit:** Ordnen Sie jede Anwenderaktivität dem Urheber zu, auch bei Verwendung gemeinsam genutzter Accounts. Umfassende Protokollierung, Aufzeichnung von Sessions und Anwenderwarnungen erfassen Aktivitäten und schrecken unbefugtes Verhalten ab.
- **Verbesserung des Auditings und Vereinfachung der Einhaltung von Vorschriften:** Vereinfachen Sie die Einhaltung von Vorschriften, indem Sie neue Anforderungen an Authentifizierung und Access Control unterstützen, und begrenzen Sie die Tragweite von Compliance-Anforderungen, indem Sie das Netzwerk in logische Segmente aufteilen.
- **Senken der Komplexität und Erhöhen der Operatorproduktivität:** Ein Single Sign-On für privilegierte Accounts trägt nicht nur zur Risikobegrenzung bei, sondern kann die Produktivität einzelner Administratoren erhöhen, da sie leichter und schneller auf das System und die Ressourcen zugreifen können, die sie verwalten sollen. Zentrale Richtliniendefinitionen und -erzwingung vereinfachen die Erstellung und Erzwingung von Securitymechanismen.

Fazit

- Privilegierte Identitäten, Accounts und Zugriffe sind zentrale, kritische Assets für Unternehmen. Sie müssen mithilfe einer Kombination von Technologien und Prozessen auf der Grundlage des Privileged Access Management wirksam geschützt werden.
- Dieser Schutz dient dazu, den Angriffsablauf für Datenkompromittierungen zu durchbrechen, um Angriffe zu verhindern und die Auswirkungen erfolgreicher Angriffe zu verringern.
- Ein Modell der Zero-Trust Access Control ist für alle Arten privilegierter Zugriffe unerlässlich, sowohl durch Menschen als auch durch Programme.
- Während es sich gezeigt hat, dass perimeterbasierte Ansätze für die Security wesentliche Nachteile haben, ist eine mehrschichtige Verteidigung weiterhin eine wichtige Strategie für den Schutz von Ressourcen. Ein Privileged Access Management kann mehrere zusätzliche Verteidigungsebenen im Hinblick auf privilegierte Anwender, Accounts und Anmeldeinformationen bieten, sowohl auf Netzwerk- als auch auf Hostebene.
- Da Kompromittierungen so häufig und die Angreifer so gewieft sind, ist es sehr verlockend – und wird häufig empfohlen– sich nur auf die Erkennung von Kompromittierungen und auf Reaktionen darauf zu konzentrieren. Das ist ein Fehler. Diese Maßnahmen sind zwar wichtig, aber es muss auch bedacht werden, dass ein Privileged Access Management Unternehmen helfen kann, Kompromittierungen wesentlich besser von vornherein zu verhindern.

Informationen zum Autor

Dale R. Gardner verfügt über mehr als zwei Jahrzehnte Erfahrung mit Unternehmenssoftware für das Netzwerk- und Systemmanagement und mehrere Bereiche der Security, darunter Identity Management, Anwendungssecurity, Schwachstellenmanagement, Einhaltung von Vorschriften und Netzwerksecurity. Als früherer Marktforschungsanalytiker und -autor hat er mehrere Management- und Security-Lösungen definiert, aufgebaut und vermarktet, die den Betrieb verbessern und zur Integrität und Zuverlässigkeit der IT-Infrastruktur in Unternehmen beitragen. Zurzeit ist er für das weltweite Marketing des Privileged Access Management-Produktportfolios von CA Technologies verantwortlich.

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 in allen Branchen und in allen Unternehmen im Mittelpunkt. Ob Planung, Entwicklung, Management oder Security – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen abwickeln und kommunizieren, in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen neu zu gestalten. Weitere Informationen finden Sie unter **ca.com/de**.

1 Intel Security und das Center for Strategic and International Studies, „Net Losses: Estimating the Global Loss of Cybercrime, Economic Impact of Cybercrime II“, Juni 2014, http://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf

2 World Economic Forum und McKinsey & Company, „Risk and Responsibility in a Hyper-connected World“, Januar 2014, http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

3 Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D., Lockheed Martin Corporation, „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains“, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

4 Andras Cser, Forrester Research, „Critical Questions to Ask Your Privileged Identity Management Solution Provider“, 10. September 2014.

5 Ars Technica, „AWS console breach leads to demise of service with 'proven' backup plan“, 18. Juni 2014, http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/

6 Brian Krebs, „China To Blame in Anthem Hack?“, 15. Februar 2015, http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

7 Anmol Singh und Felix Gaehtgens, „Twelve Best Practices for Privileged Access Management, Gartner“, 8. Oktober 2015, G00277332

 CS200-162063_1115