WHITE PAPER | APRIL 2016

Wie Sie alle Hintertüren zu Ihrem Netzwerk schließen

Die fünf wichtigsten Best Practices zur Bewältigung der Risiken durch Drittanbieter

Dale R. Gardner
CA Security Management

ca technologies

Inhaltsverzeichnis

Kurzfassung

Ausgangssituation

Die gravierenden Sicherheitsverletzungen bei Target, Home Depot, eBay, dem US-amerikanischen Office of Personnel Management und anderen Unternehmen wurden durch gestohlene oder kompromittierte Anwenderberechtigungen ermöglicht, die einem privilegierten Anwender mit weitreichenden Zugriffsrechten auf sensible Systeme gehörten. In nahezu zwei Drittel der Fälle wurde der ursprüngliche Verstoß durch zu lockere Sicherheitspraktiken eines Drittanbieters begünstigt, d. h. einem Lieferanten oder Geschäftspartner, der Zugang zu einem internen Netzwerk hatte. Mit den gestohlenen Partneranmeldedaten konnten die Angreifer dann die gehackte IT-Infrastruktur auskundschaften und sich auf die Suche nach privilegierten Accounts machen, um sich darüber unbefugten Zugriff auf kritische Systeme zu verschaffen und den Unternehmen verheerenden Schaden zuzufügen.

Chance

Auch viele andere Unternehmen arbeiten mit einer bunten Mischung aus Drittanbietern, Subunternehmern und Geschäftspartnern zusammen, die Netzwerkzugriff auf ihre IT-Infrastruktur und verschiedene privilegierte Accounts haben, um unternehmenskritische Anwendungen auszuführen. In der vernetzten Welt von heute kann der Zugriff natürlich nicht komplett blockiert werden, ebensowenig ist es realistisch, die privilegierten Accounts abzuschaffen. Deshalb ist die einzige Möglichkeit, privilegierte Accounts besser vor unbefugten Anwendern zu schützen, die sensiblen Informationsressourcen besser zu schützen.

Nutzen

Kosteneinsparungen, eine höhere Qualität und mehr Effizienz durch Outsourcing werden erst durch das vernetzte Unternehmen möglich. Inzwischen ist es keine Option mehr, den Netzwerkzugriff an der Firewall einzuschränken. Um geschäftliche Vorteile zu erlangen, müssen die benötigten Ressourcen für die Geschäftspartner zugriffsbereit sein. Folglich bedarf es Best Practices für die Informationssicherheit, um Sicherheitsverletzungen zu verhindern, aber legitime Geschäftsaktivitäten zuzulassen.

Abschnitt 1

Risiken durch den Zugriff von Drittanbietern

Die meisten Unternehmen arbeiten heute mit externen Personen zusammen, die über gewisse privilegierte Zugriffsrechte für interne Netzwerke und Systeme verfügen. Oft weiß das für Informationssicherheit zuständige Team wenig bis gar nichts über diese Personen, es sei denn, sie arbeiten für Lieferanten, ausgegliederte Service Provider oder Geschäftspartner des Unternehmens. In der Regel stellen diese Anwender für das Unternehmen das größte Risiko dar, da ihre Accounts oft der einfachste Weg sind, das Unternehmen zu kompromittieren. Als Beispiel für solche Verstöße seien die jüngsten Geschehnisse bei Target, Home Depot usw. genannt. Der kompromittierte Anwenderzugriff eines relativ kleinen Drittanbieters kann leicht missbraucht werden, um sich weitreichenderen Zugang zu den Netzwerken und Systemen eines Unternehmens zu verschaffen – mit durchaus verheerenden Folgen. Und dies sind keine Einzelfälle. Laut Troy Leach von PCI Council lassen sich 65 % der Sicherheitsverstöße auf einen Drittanbieter zurückführen.

Die Behörden sind sich dieser Risiken wohl bewusst und arbeiten gemeinsam mit der Industrie an der Entwicklung geeigneter Kontrollen und Vorschriften für dieses Problem. So wurden z. B. mit PCI Version 3 des Data Security Standard neue Kontrollen eingeführt, um speziell die Risiken durch Drittanbieter anzugehen. Gemäß Benjamin Lawsky, Superintendent of Financial Services für den Staat New York, ist **„die Cyber-Security einer Bank zumeist nur so gut wie die Cyber-Security seiner Lieferanten. Leider bieten diese Drittfirmen Hackern, die an sensible Bankkundendaten kommen möchten, durch die Hintertür Zugang zu diesen Daten.“** Folglich sind Finanzdienstleister, Regulierungsbehörden im Gesundheitswesen oder in anderen Branchen dabei, neue Compliance-Anforderungen zu erarbeiten, um die Risiken zu minimieren und die Security zu verbessern.

> „Die Cyber-Security einer Bank ist zumeist nur so gut wie die Cyber-Security seiner Lieferanten. Leider bieten diese Drittfirmen Hackern, die an sensible Bankkundendaten kommen möchten, durch die Hintertür Zugang zu diesen Daten.“
>
> – Benjamin Lawsky, Superintendent of Financial Services, Bundesstaat New York

---

Abschnitt 2

Die fünf wichtigsten Best Practices zur Bewältigung der Risiken durch Drittanbieter

In der Zukunft wird die Kontrolle und das Management des Zugriffs durch Drittanbieter auf Netzwerke und Systeme zu einer immer wichtigeren Anforderung, was das Risikomanagement im Bereich Informationssicherheit wie auch die Einhaltung von Vorschriften anbelangt.

> „Hacker verschafften sich über Anmeldeinformationen, die sie vom Subunternehmen KeyPoint Government Solutions gestohlen hatten, Zugriff auf die Netzwerke des OPM.“
>
> Exklusiv: Neue Details zur Sicherheitsverletzung beim OPM, 21. August 2015

Best Practice 1: Implementierung unterstützender Prozesse und Kontrollen

Ähnlich wie bei den meisten Problemen mit der Informationssicherheit ist ein guter erster Schritt, Prozesse und Kontrollen für das Risikomanagement zu definieren. Dies ist besonders wichtig zur Bewältigung der Risiken durch Drittanbieter, da die meisten Aktivitäten hier außerhalb der Reichweite und Kontrolle des Informationssicherheitsteams erfolgen. Da ohne Kenntnis bzw. Prüfung dieses Teams Geschäftsbeziehungen geknüpft und Zugriffsrechte gewährt werden können, sollte es zu den Vertragsverhandlungen hinzugezogen werden, sodass im Rahmen des allgemeinen Identity and Access Management entsprechende Richtlinien aufgestellt und durchgesetzt werden können.

Der einfache Teil des Prozesses besteht in der Provisionierung, Deprovisionierung und Definition geeigneter Richtlinien für privilegierte Anwender, die keine Mitarbeiter sind. Ähnlich wie bei anderen privilegierten Anwendern sind auch hier folgende Aspekte zu klären:

- Anwenderdefinition und -schulung
- Systeme und Ressourcen, auf die Zugriff erforderlich ist
- Maß an Berechtigungen, die für die jeweiligen Arbeiten benötigt werden
- Sämtliche zu erzwingenden Beschränkungen
- Monitoring, Aufzeichnung von Sessions, Abgabe von Warnungen und Häufigkeit der Überprüfung von Sessions

Die meisten Unternehmen setzen solche Richtlinien für privilegierte Anwender bereits um. Wenn es diese Richtlinien noch nicht gibt, ist es höchste Zeit, sie aufzustellen. Die gleichen Prozesse und Kontrollen, die auf angestellte privilegierte Anwender angewendet werden, müssen auch für Nicht-Mitarbeiter gelten. Je nach Organisationsstruktur und Größe des Unternehmens werden diese Prozesse von der IT-Abteilung, den Verantwortlichen für das Identity Management oder einem Vertragsunternehmen betreut. Darüber hinaus müssen Prozesse für Schulungen, Provisionierung, Monitoring und Deprovisionierung der privilegierten Anwender von Drittanbietern definiert werden.

Security-Standards

Grundsätzlich ist Security immer nur so stark wie das schwächste Glied. Durch den privilegierten Anwender eines Partners werden auch die Infrastruktur und Prozesse dieses Partners Teil der eigenen IT-Infrastruktur des Unternehmens. Nur ein einziger Partner mit unzureichenden Kontrollen oder mangelhafter Security kann sich schon als Schlupfloch erweisen, über das Hacker die Schutzmaßnahmen eines Unternehmens überlisten können. Beispiel hierfür ist das US-amerikanische Office of Personnel Management, auf das ein Angriff mit Anmeldeinformationen unternommen wurde, die die Hacker von seinem Subunternehmen KeyPoint Government Solutions gestohlen hatten. Aus Sicht des Risikomanagements ist eine Bewertung der Security-Maßnahmen jedes Geschäftspartners entsprechend den etablierten Standards des Unternehmens ein absolutes Muss. In immer mehr Fällen fordern PCI, HIPAA und andere Compliance-Vorgaben eine Überprüfung von Drittanbietern und sehen dafür spezifische Anforderungen vor.

Die meisten Unternehmen haben bereits Standards für die Informationssicherheit eingeführt. Es gilt aber, diese Standards auch auf Drittanbieter anzuwenden. Für die Entwicklung neuer Informationssicherheitsstandards stehen mehrere Quellen zur Verfügung:

- Shared Assessments veröffentlicht ein Dokument zu „Standard Information Gathering (SIG)“, das Unterstützung bei der Standardisierung der Erfassung im Bereich Informationssicherheit und der entsprechenden Beurteilungen bietet
- Das Office of the Comptroller of the Currency (OCC) gibt einen umfassenden Leitfaden für das Risikomanagement heraus, der hilfreiche IT-spezifische Kapitel enthält
- Der Federal Financial Institutions Examination Council (FFIEC) veröffentlicht Dokumente mit relevanten Standards
- Security Risk Assessment Tool des US-Gesundheitsministeriums (Department of Health and Human Services)
- NIST 800-53 Security and Privacy Controls for Federal Information Systems

- Staatliche Regulierungsbehörden
- COBIT- oder ISO 27002-Richtlinien und -Kontrollen

Auch können branchenspezifische Vorgaben Anforderungen für die Zusammenarbeit mit Drittparteien enthalten:

- PCI Data Security Standard
- HIPAA HITECH

Implementierung, Schulung und Erzwingung

Bewertungsmethoden und Prozesse müssen implementiert und durch die IT-, Finanz- oder Rechtsabteilung bzw. die zuständigen Fachabteilungen durchgesetzt werden. Grundsätzlich sollte dies selbstverständlicher Bestandteil der Vertragsdefinition und -umsetzung mit Dritten sein. Unten stehend finden Sie einige grundlegende Elemente, die in jedem Vertrag mit Dritten enthalten sein sollten:

- Garantien: Verweise auf die geltenden Richtlinien und Verfahren, zu deren Umsetzung sich der Lieferant verpflichtet, z. B. Hintergrundprüfungen und Schulung der Mitarbeiter, die auf die Systeme des Unternehmens zugreifen
- Rechtsmittel: Strafen bei Verstößen gegen diese Vereinbarungen und entsprechende Problembehebungsverfahren
- Audit-Bestimmungen: Kontrollmechanismen zur Überprüfung der Einhaltung von Vorschriften und der Häufigkeit von Audits

Diese fundamentalen Bestimmungen in Bezug auf das Risikomanagement müssen in den entsprechenden Phasen des Vertrags- und Umsetzungsprozesses berücksichtigt werden. Wie die Richtlinien und deren Erzwingung im Detail aussehen, hängt von den Geschäftsbereichen und der Abwägung zwischen Risiken und Kosten ab.

Best Practice 2: bessere Authentifizierung der Anwender

Die beste Möglichkeit, bei geringstmöglichem Arbeits- und Kostenaufwand eine weitestgehende Risikominimierung zu erreichen, besteht in der Identifizierung und Authentifizierung der Anwender. Wie oben bereits erwähnt, lassen sich rund zwei Drittel der Sicherheitsverstöße auf eine mangelhafte Identifizierung und Authentifizierung der Anwender beim Drittanbieter zurückführen. Hierzu gehört auch das Management von Anmeldeinformationen (bzw. dessen Fehlen). Drittanbieter sind in der Regel kleinere Firmen, die in puncto Security nicht so ausgestattet und erfahren sind wie größere Unternehmen. Dies führt oft zu Problemen. Die Anmeldeinformationen der Anwender sind auf zweierlei Weise kompromittierbar: entweder durch nicht ausreichend sichere und verwaltete Anmeldeinformationen oder durch die versehentliche Offenlegung der Anmeldeinformationen gegenüber den falschen Personen.

- **Unsichere Anmeldeinformationen:** Selbst wenn ein sicheres Passwort gewählt wird, kann die Durchsetzung von Passwortregeln wie für ablaufende Passwörter sehr aufwendig sein. Insbesondere bei kleineren Anbietern wird dies nicht wirklich praktiziert. So verwendete ein Drittanbieter beispielsweise die gleiche Anwender-ID und das gleiche Passwort für alle Kunden. Nachdem die Angreifer diese eine Anmeldeinformation für einen Kunden abgefangen hatten, brauchten sie einfach nur die Kundenliste des Anbieters durchzugehen (die gewissenhaft auf dessen Website veröffentlicht war) und sich dann den Rest der Firmen vorzunehmen, um diese zu kompromittieren.
- **Versehentliche Offenlegung:** Laut den neuesten Statistiken liegt die Erfolgsrate bei wiederholten Phishing-Angriffen bei nahezu 100 % (nach nur fünf bis sieben Versuchen). Dies zeigt, wie raffiniert diese Angriffe geworden sind und wie schwierig es auch für die intelligentesten und erfahrensten Anwender ist, sie zu erkennen. Nur ein einziger Fehler kann zum Missbrauch führen, wie beim Sicherheitsvorfall eines ukrainischen Kraftwerks im Dezember 2015. Dies heißt, dass selbst qualifiziertere Geschäftspartner anfällig für Phishing-Angriffe sein können.

Die beste Möglichkeit zum Schutz von Anmeldeinformationen ist deren proaktive Verwaltung und Kontrolle durch die Definition und Erzwingung von Richtlinien. Dazu gehören z. B. folgende Aspekte:

- Komplexität
- Häufigkeit von Änderungen
- Mehrstufige Authentifizierung

Eine Best Practice für das Management von Anmeldeinformationen ist die mehrstufige Authentifizierung, durchgeführt für alle Drittparteien (und internen privilegierten Anwender). Nachdem ein Unternehmen Ziel eines Angriffs geworden ist, ist es nur eine Frage der Zeit, bis die von Drittanbietern verwendeten Anmeldeinformationen kompromittiert werden. Beim ukrainischen Kraftwerk scheint es beispielsweise so gewesen zu sein, dass die BlackEnergy-Malware an einen nichtsahnenden privilegierten Anwender über einen infizierten Microsoft Office-Anhang zugestellt und dann als initialer Zugang zur Erlangung legitimer Anmeldeinformationen genutzt wurde. Dies lässt sich am besten verhindern, indem man einen weiteren Faktor in den Authentifizierungsprozess hinzunimmt. Für die mehrstufige Authentifizierung stehen mehrere Optionen zur Verfügung. Welche Option am effektivsten ist, hängt von der Wirtschaftlichkeit und den jeweiligen Vorschriften oder Compliance-Vorgaben ab. So sieht die US-Regierung z. B. spezifische Anforderungen für den Einsatz von PIV/CAC-Karten für privilegierte und administrative Anwender vor. In anderen Umgebungen sind andere Optionen verfügbar, z. B. Zertifikate, hard- und sogar softwarebasierte Token oder Verifizierungsverfahren über das Mobiltelefon einer Person. Was die Wirtschaftlichkeit anbelangt, so schneidet die mehrstufige Authentifizierung sehr gut ab, denn der Business Case lässt sich einfach erstellen.

Ein effektives Management der Anmeldeinformationen von Drittanbietern setzt voraus, dass die Anwender über individuelle Anmeldeinformationen verfügen. In vielen Unternehmen ist dies aber noch nicht gängige Praxis. In vielen Fällen wird kein Account für einen Anwender erstellt, sondern für einen Anbieter, weil man davon ausgeht, dass jeder Mitarbeiter des Anwenders den gleichen Account mit den gleichen Anmeldeinformationen verwenden kann. Dies ist zwar aus administrativer Sicht einfacher, wenn sich mehrere Personen aber einen Account teilen, ergeben sich folgende Probleme:

- Die mehrstufige Authentifizierung gestaltet sich komplizierter.
- Es ist schwieriger, den Zugriff und die Verwendung der Anmeldeinformationen zu kontrollieren, besonders dann, wenn jemand das Unternehmen verlässt oder intern die Position wechselt. Gemeinsam genutzte Anmeldeinformationen können sehr leicht abgefangen bzw. gestohlen werden.
- Es ist unmöglich festzustellen, welche Person eine bestimmte Aktion im Netzwerk ausgeführt hat. Wenn sich mehrere Personen einen Account teilen, besteht keine Möglichkeit zu wissen, welche von diesen Personen die problematische Aktion durchgeführt hat.

Durch einen Prozess, bei dem Anmeldeinformationen an einzelne Personen und nicht an einen Anbieter vergeben werden, lassen sich diese Probleme vermeiden. Zudem wird das On- und Offboarding von Anwendern vereinfacht. Wenn jemand damit beginnt, bei einem Geschäftspartner zu arbeiten, wird für diese Person ein Account angelegt und der Zugriff wird erteilt. Account und Zugriff können genauso einfach und schnell wieder deaktiviert werden, wenn die Person das Unternehmen verlässt oder die Stelle wechselt. Ob das Zugriffsmanagement und die Anwenderauthentifizierung erfolgreich sind, hängt nicht nur von der Technologie ab, sondern auch von den Menschen, Prozessen und Schulungsmaßnahmen. All diese Aspekte müssen bei der Verhandlung der Verträge mit den Anbietern und bei der Implementierung der Prozesse berücksichtigt werden. Personaländerungen müssen von den Anbietern sofort gemeldet werden (was für sie zusätzlichen Aufwand bedeutet). Deshalb sollten entsprechende Verfahren vorhanden sein, um dies den Anbietern zu erleichtern. Im Großen und Ganzen ist es den zusätzlichen administrativen Aufwand wert, denn es ist für mehr Security und Kontrolle gesorgt. Tatsächlich wird laut Vorschriften verlangt, dass die Authentifizierung und Access Control auf der Ebene einzelner Anwender erfolgt, weil dies am effektivsten ist.

Auch wenn sich dies in den Unternehmen noch nicht durchgesetzt hat, werden Hintergrund- und Identitätsprüfungen der Mitarbeiter von Drittanbietern gefordert, die auf die Systeme des Unternehmens zugreifen. Auch hier gilt: Dies ist ein Thema, das zum Risikomanagement gehört. Die anfallenden Kosten (sowohl finanzieller als auch administrativer Art) lassen sich im Allgemeinen gut rechtfertigen, besonders bei sensiblen Umgebungen.

Eine Technologie, die Regeln zur Passwortkomplexität, Passwortänderungen und die Integration von mehrstufigen Authentifizierungssystemen zentralisiert und automatisiert, ist ein Vault, in dem die Anmeldeinformationen gespeichert werden. Was sich nach dem Management der Anmeldeinformationen als Nächstes anbietet, ist die Trennung der Authentifizierung von der Access Control.

Best Practice 3: Trennung der Authentifizierung von der Access Control

In den meisten Netzwerken ist es so, dass wenn sich eine Person Zugriff auf das Netzwerk verschafft, sie Einblick in verschiedenste Geräte und Systeme hat – und potenziell auch darauf zugreifen kann. Aus einer solchen Netzwerkarchitektur können sich allerdings Sicherheitsrisiken ergeben, wie sie Target, Home Depot, dem ukrainischen Kraftwerk und vielen mehr zum Verhängnis wurden. Diese Art von Angriffen werden über die „Kill Chain“ ausgeführt. Bei der „Kill Chain“, also dem Angriffsablauf, führen die Angreifer eine Serie von Schritten aus, manchmal iterativ, um in das Netzwerk einzudringen. Zuerst verschafft sich der Angreifer einen ersten Zugang zum Netzwerk, oft durch kompromittierte Anmeldeinformationen eines Drittanbieters. Sobald er eingedrungen ist, kann er nach Schwachstellen oder zusätzlichen Anmeldeinformationen suchen, die er nutzen könnte, um weitreichenderen Zugriff mit noch mehr Privilegien zu erhalten, bis er schließlich sein Ziel erreicht – wie den Stromausfall in der Ukraine.

> „Alle drei Unternehmen gaben an, dass die Angreifer einige Systeme durch Ausführen der Malware KillDisk am Ende der Cyberattacke vollständig löschten. Die KillDisk-Malware entfernt ausgewählte Dateien auf den Zielsystemen und beschädigt den Master-Bootdatensatz, was die Systeme außer Betrieb setzt. Es wurde ferner berichtet, dass in mindestens einem Fall Windows-basierte Mensch-Maschine-Schnittstellen, die in dezentralen Terminaleinheiten eingebettet waren, ebenfalls durch KillDisk überschrieben wurden. Die Angreifer machten auch Seriell-zu-Ethernet-Geräte in Teilkraftwerken unbrauchbar, indem sie deren Firmware beschädigten. Den Berichten zufolge gelang es den Angreifern sogar, eine Trennung von den unterbrechungsfreien Stromversorgungen der Server über deren dezentrale Managementoberfläche zu terminieren. Das Team geht davon aus, dass mit diesen Aktionen versucht wurde, die bevorstehenden Sanierungsmaßnahmen zu stören.“
>
> Cyberangriff auf wichtige ukrainische Infrastruktur
> Erstveröffentlichung: 25. Februar 2016

Wie in Best Practice 2 erwähnt, lässt sich der Angriffsablauf durchbrechen, indem der Zugang zum Netzwerk durch die mehrstufige Authentifizierung kontrolliert und so das Eindringen für Angreifer erschwert wird. Eine zusätzliche Schutzoption ist, den Zugriff auf die Ressourcen im Netzwerk einzuschränken. Die meisten Anbieter brauchen nur Zugriff auf ganz bestimmte Systeme. Sie müssen nicht unbedingt auf das ganze Netzwerk bzw. nicht einmal auf ein Teilnetzwerk zugreifen.

Der Netzwerkzugriff lässt sich durch die physische Netzwerksegmentierung einschränken. Häufig wird diese Netzwerksegmentierung angewendet, um behördliche Vorschriften zu erfüllen. Durch Segmentierung des Netzwerks und Steuerung des Zugriffs kann der Umfang verfügbarer Ressourcen eingegrenzt werden. Diese Methode kann zwar sehr effektiv sein, hat aber auch einige Nachteile:

- Hoher administrativer Aufwand für die Einrichtung und Wartung der Netzwerkarchitektur
- Schwachstellen bei den Verbindungen zwischen den verschiedenen Teilen des Netzwerks; so kann ein Angreifer Netzwerkverbindungen nutzen, um sich Zugriff auf sein Ziel zu verschaffen

Eine bessere Alternative ist die logische Segmentierung mit einer Privileged-Identity-Management-Lösung wie CA Privileged Access Manager, die den Zugriff auf die Ressourcen einschränkt. Diese Lösung funktioniert durch Implementierung eines „Drosselungspunktes", den ein Drittanbieteranwender passieren muss, um Zugriff auf geschützte Ressourcen zu erhalten. Dieser Ansatz bietet eine Reihe von Vorteilen:

- **Zero-Trust-Modell bei der Access Control:** Wer sich erfolgreich anmeldet, erhält keinen Zugang zum gesamten Netzwerk. Stattdessen werden vom System Richtlinien erzwungen, die angeben, welche Ressourcen einem Anwender zur Verfügung stehen. So kann eine Person nur auf die für sie bestimmten Systeme zugreifen. Dies ermöglicht eine sehr strikte Access Control, bei der Anwender nie die Ressourcen zu Gesicht bekommen, auf die sie nicht zugreifen dürfen. Sie sehen nur eine vordefinierte Liste mit den Systemen, für die sie Zugriff erhalten haben.
- **Verhinderung von „Leapfrog":** Um die Auskundschaftung von Netzwerken zu kontrollieren, fängt ein System verschiedene Netzwerkbefehle wie TELNET- oder SSH-Befehle ab und hindert sie an der Ausführung. So wird der Zugriff von Drittanbietern auf die vordefinierten Systeme beschränkt. Es besteht also keine Möglichkeit, in das restliche Netzwerk zu gelangen und sich Zugriff auf andere Systeme zu verschaffen.

Es ist wichtig, die Zugriffsmethoden mit einem „Drosselungspunkt" zu standardisieren und zu konsolidieren, entweder mit einer Privileged-Access-Management-Lösung, einem VPN oder einer anderen Lösung, die den Zugriff über bekannte Pfade kanalisiert. Eine Definition der akzeptierten Pfade für den externen Zugriff auf Ressourcen vereinfacht das Monitoring. Indem nicht genehmigte Protokolle minimiert und genehmigte Sessions an eine vordefinierte Route geleitet werden, können Anomalien einfacher erkannt und weiter untersucht werden. SIEM- und Protokollierungstools helfen bei der Kennzeichnung abnormaler Ereignisse.

Best Practice 4: Verhinderung von Fehlern und unbefugten Befehlen

Um den Zugriff auf die IT-Ressourcen einzuschränken, können Zugriffsrechte und -berechtigungen verwendet werden. Dieses Vorgehen bietet mitunter jedoch nicht das Maß an Genauigkeit, das es braucht, um die Aktivitäten von Anwendern in einem System wirklich zu kontrollieren. So muss sich ein Systemadministrator eines Drittanbieters oft bei einem Server mit einem „root"- oder „admin"-Account anmelden, also einem Superuser-Account mit weitreichenden Berechtigungen. Aus technischen oder administrativen Gründen mag dieser Ansatz gerechtfertigt sein, er ist jedoch mit vielerlei Risiken behaftet. Ausgestattet mit einer solchen Fülle an Befugnissen kann die Person alles Mögliche im System anstellen, es unter anderem auch vollkommen löschen. Dies ist für die meisten Unternehmen ein inakzeptables Risiko, auch wenn es sich bei dieser Person um einen Mitarbeiter handelt.

Besser geeignet ist ein anderer Ansatz, bei dem eine Privileged-Access-Management-Lösung zur Anwendung kommt, da hier die Berechtigungen auf spezifischere Weise kontrolliert werden, um diese Art von Anwender besser zu managen. Mithilfe einer Privileged-Access-Management-Lösung können Sie zulassen, dass Sessions für einen Anwender in dessen Namen auf verschiedene Zielsysteme mit verschiedenen Accounts (z. B. „root") vermittelt werden, jeweils mit unterschiedlichen Berechtigungsstufen.

Befehlsfilterung sowie Black- und Whitelists können ebenfalls verwendet werden, um die Befehle einzugrenzen, die von einem Anwender ausgeführt werden können. Eine Blacklist enthält alle Befehle, die nicht zulässig sind, während in einer Whitelist all jene Befehle aufgeführt sind, die ausgegeben werden können. Werden Black- und Whitelists zusammen eingesetzt, bieten sie ein hohes Maß an Kontrolle und Flexibilität. Der privilegierte Anwender kann so auf die Ressource zugreifen, ohne unakzeptablen Schaden anzurichten. Ein unverhoffter Vorteil der Befehlsfilterung ist, dass versehentliche Fehler vermieden werden. In dem Beispiel oben kann der Superuser zwar Dateien verschieben, aber nicht die Festplatte neu formatieren.

Befehlsfilter in Kombination mit Protokollfunktionen erleichtern das Monitoring und die Ausgabe von Warnungen, sodass das System auf angemessene Weise reagieren kann, wenn jemand versucht, einen der Filter zu umgehen. Es könnte z. B. eine Warnung ausgegeben oder eine verdächtige Session beendet werden. Eine Person könnte beispielsweise verschiedene Versuche starten, bevor sie die durch Befehlsfilter erzwungenen Limits erreicht. Wenn die Limits ausgelöst werden, kann das System eine Warnung generieren, die eine Untersuchung der Aktivitäten dieser Person anstößt. Hier einige der möglichen Reaktionen:

- Sperren und Warnen des Anwenders
- Beenden der Session
- Deaktivieren des Anwender-Accounts
- Generieren von SOC-Warnungen

Best Practice 5: Monitoring und Untersuchung

Ein gewisses Maß an Monitoring ist unerlässlich. Der Umfang dieser Überwachung hängt jedoch von den jeweiligen Anforderungen an das Risiko- und Compliance-Management ab.

Selbst wenn die Risiken eigentlich gering sind, hilft die Protokollierung bei der Problembehebung und der Untersuchung verdächtiger Aktivitäten. Bei einer Protokollierung werden die Ereignisse erfasst. Die Protokolle bieten dann Unterstützung bei der Prüfung unangemessener oder unbefugter Aktivitäten. Ein Protokoll umfasst:

- Anmelde- und Abmeldezeit
- Systeme, auf die zugegriffen wurde
- Ausgegebene Befehle
- Erhaltene Antworten

Bei sensiblen Vorgängen greift das Monitoring auf Protokolle zurück, um definierte Richtlinien für den Systemzugriff zu erzwingen, da jeglichen Versuchen, diese Richtlinien zu verletzen, nachgegangen werden sollte. Als Reaktion auf einen versuchten Richtlinienverstoß können verschiedene Maßnahmen ergriffen werden. Solche Versuche rechtfertigen auf jeden Fall eine Untersuchung, um herauszufinden, was passiert ist. Unter Umständen sind weitere Schulungen erforderlich, damit alle verstehen, was von ihnen erwartet wird. Ein Verstoß kann einfach nur einen Fehler als Ursache haben, oder er ist ein Hinweis auf böswilliges Verhalten. Das Monitoring hilft bei der Erfassung verdächtiger Ereignisse, damit diese untersucht werden können.

Und diese Untersuchungen sind sehr wichtig, wie der Fall von JPMorgan Chase zeigt, denn hier wurde ein Sicherheitsverstoß entdeckt, als die Mitarbeiter des Unternehmens einen seiner Anbieter überprüften.

„JPMorgan entdeckte die Hacker in seinen Systemen im August, nachdem das Unternehmen gerade erst herausgefunden hatte, dass die gleichen Hacker eine Website für einen Wohltätigkeitslauf, den die Bank sponserte, kompromittiert hatten ... Erst nachdem JPMorgan feststellte, dass die Website zu dem Firmenlauf gehackt wurde, erfuhr es, dass sein eigenes Netzwerk von den gleichen Hackern angegriffen wurde."

„Neglected Server Provided Entry for JPMorgan Hackers"
The New York Times, 22. Dezember 2014

In noch kritischeren Situationen kann es sich als notwendig erweisen, Sessions aufzuzeichnen, um umfassende Informationen darüber zu liefern, was in einer bestimmten Session passiert ist, und um Unterstützung bei künftigen Ermittlungen zu leisten. Ein gängiges Vorgehen ist, bei sensiblen Sessions den gesamten Bildschirm zu erfassen und aufzuzeichnen. Diese Aufzeichnungen können dann untersucht werden, wenn es zu Richtlinienverstößen kommt oder im Nachhinein Probleme mit einem System auftreten. So ist nachvollziehbar, was in der ursprünglichen Session passiert ist. Je nach Sensibilität der Umgebung sind möglicherweise stichprobenartige Überprüfungen wünschenswert. Eine der Herausforderungen bei der Aufzeichnung von Sessions ist in der Regel, dass dies ein beträchtliches Datenaufkommen (mit entsprechender Systembelastung) verursacht. Eine weitere Herausforderung ist der Aktionsplan für die Überprüfung der aufgezeichneten Sessions. Da bei der Session-Aufzeichnung die Kosten für Technologie und Aufwand steigen, können mithilfe von Kosten-Nutzen-Analysen die Fälle herausgefiltert werden, in denen diese Investitionen wirklich notwendig sind. Als Ausgangspunkt kann es helfen, sich folgende Fragen zu beantworten:

- Wann und wie lange soll etwas aufgezeichnet werden?
- Wann und wie oft sollten die Aufzeichnungen überprüft werden?
- Wie sieht die Richtlinie zur Aufbewahrung der Aufzeichnungen genau aus?

Wenn Sie sich für eine Session-Aufzeichnung entscheiden, achten Sie auf folgende Funktionen:

- Einfacher Zugriff auf die Metadaten zur Session (z. B. Beginn und Ende der Session)
- Möglichkeit, die Sessions schnell durchzugehen und zu einem bestimmten Punkt in einer Aufzeichnung zu springen
- Möglichkeit, „interessante" Aktivitäten hervorzuheben, z. B. Richtlinienverstöße und sensible Aktivitäten

Situationen mit besonders hohem Risiko rechtfertigen unter Umständen ein direktes Monitoring „über die Schulter" oder einen Zugriff in Anwesenheit von zwei Personen. Dazu muss eine weitere Person abgestellt werden, die in Echtzeit überwacht, was ein privilegierter Anwender tut. Situationen mit Extremrisiko, in denen ein solches Vorgehen angemessen wäre, gibt es normalerweise aber nicht bei Drittparteien oder anderen externen Anwendern. Das direkte Monitoring „über die Schulter" birgt gewisse technische Herausforderungen. Die Person, die diese Art von Monitoring durchführt, muss sehr erfahren sein, das heißt, sie muss die Aktivitäten und deren Folgen auf die ganze Umgebung nachvollziehen können. Aus Sicht des Risikomanagements ist diese Art der Überwachung nur für sehr wenige Situationen geeignet.

Für gewöhnlich umfasst das Monitoring zwei Schritte:

- **Echtzeitreaktion auf Richtlinienverstöße:** Es können mehrere Aktionen angestoßen werden – eine Warnung des Anwenders, eine Benachrichtigung an die zuständige Security-Abteilung, die Beendigung einer Session oder die Deaktivierung eines Accounts.
- **Untersuchung und Analyse nach dem Ereignis:** Es können Protokolle oder Session-Aufzeichnungen durchgegangen werden, die wichtige Informationen für die Problembehebung oder forensischen Ermittlungen bieten.

Untersuchungen und Analysen nach Eintreten des Ereignisses können Maßnahmen beinhalten wie die Korrelation von Protokollen und Warnungen, die bei unerwarteten Ereignissen durch ein Privileged-Access-Management-System mit anderen Netzwerk- und Security-Tools generiert wurden. In Unternehmen beispielsweise, in denen eine Privileged-Access-Management-Lösung implementiert wurde, sind alle administrativen Tätigkeiten im Privileged-Access-Management-System zentralisiert. Wenn SSH- oder TELNET-Session-Anforderungen von anderen Teilen des Netzwerks eingehen, werden diese als unmittelbare Warnungen betrachtet, dass etwas schiefläuft, und werden daraufhin untersucht. Wenn nicht autorisierte Verwaltungstools nicht mehr zugelassen werden, sind verdächtige Aktivitäten recht einfach identifizierbar. Eine Firewall der nächsten Generation bietet Unterstützung bei der Kennzeichnung von unzulässigen Anwendungen oder Protokollen. Weitere verdächtige Aktivitäten sind beispielsweise Zugriffe zu unerwarteten Zeiten oder ungewöhnliches Verhalten wie z. B. der Download von Dateien.

Im Laufe der Zeit lassen sich die Tools und Richtlinien durch kontinuierliche manuelle Audits und Prüfungen verfeinern, sodass Fehlalarme ignoriert und Trigger und Warnungen automatisiert und so effektiver werden.

Abschnitt 3:

Vorteile beim Management der Risiken durch Drittanbieter

Kein modernes Unternehmen kann es sich leisten, seine Internetverbindung gänzlich zu kappen. Die Geschäftsbeziehungen sind auf die elektronische Zusammenarbeit angewiesen, um sensible Informationen zwischen Partnern auszutauschen. Die Unternehmen greifen heute vermehrt auf Drittanbieter für Buchhaltungsdienste, die Kreditkartenverarbeitung, Rechtsberatung, Marketingservices, Fertigung und viele andere Aufgaben zurück. Die elektronische Zusammenarbeit zwischen Geschäftspartnern spart Zeit und Geld und ermöglicht automatisierte Prozesse und Systeme, die die Qualität, Effizienz und Genauigkeit verbessern. Den Netzwerkzugriff für Drittanbieter auf Ebene der Firewall zu beschränken, ist keine Option. Um geschäftliche Vorteile zu erlangen, müssen die benötigten Ressourcen für die Geschäftspartner zugriffsbereit sein. Dennoch stehen die Unternehmen vor realen Risiken, wenn sie über das Internet mit Drittanbietern verbunden sind.

Und Sicherheitsverletzungen sind teuer. Laut dem Fortune Magazine schätzte Target seine Kosten nach dem Diebstahl der Daten zu 40 Millionen Zahlungskarten und von 70 Millionen anderen Datensätzen Ende 2013 auf 162 Millionen US-Dollar – nach Abzug der Rückerstattung durch die Versicherung. Sony gab eigenen Angaben zufolge 35 Millionen US-Dollar für die „Wiederherstellung der Finanz- und IT-Systeme“ nach einem Angriff im Jahre 2014 aus. Home Depot kostete ein Sicherheitsverstoß 28 Millionen US-Dollar netto vor Steuern. Und in den oben genannten Kosten sind noch nicht einmal die Reputationsschäden und gestiegenen Versicherungsprämien enthalten. Was zu diesen Kosten noch hinzukommt, sind die persönlichen negativen Erfahrungen der Beteiligten. Viele verloren ihre Jobs, andere mussten rund um die Uhr arbeiten, um Untersuchungen anzustellen und die Folgen einzudämmen.

> „Unabhängig von der Art und Weise, wie wir es messen oder ob wir nach vorne oder zurückschauen, sind wir uns in einem wichtigen Punkt einig – dass die Unternehmen in Informationssicherheit investieren müssen.“
>
> Benjamin Dean, Mitarbeiter der School of International and Public Affairs der Columbia University, Fortune Magazine, 27. März 2015

Kein Unternehmen möchte sich als Opfer eines weiteren Sicherheitsverstoßes auf der Titelseite des Wall Street Journal wiederfinden. Mit den fünf wichtigsten Best Practices für Informationssicherheit können Sie Sicherheitsverletzungen verhindern und die Informationsressourcen Ihres Unternehmens wie auch seinen Ruf schützen, legitime Geschäftsaktivitäten aber weiterhin zulassen.

Abschnitt 4:

Fazit

Verizon schätzt in seinem Data Breach Investigations Report (DBIR) von 2015 die finanziellen Verluste aus 700 Millionen kompromittierten Datensätzen auf 400 Millionen US-Dollar. Die 70 Unternehmen, die zu diesem Bericht beitrugen, dokumentierten 79.790 Security-Vorfälle, von denen 2.122 bestätigte Vorfälle in 61 Ländern waren. Zwei Drittel der Vorfälle fanden in den USA statt. Der Großteil der Bedrohungen geht zwar immer noch von externen Quellen aus, die Risiken durch interne Quellen und Partner haben zwischen 2013 und 2014 jedoch leicht zugenommen. Die Risiken sind real, wie auch die verheerende Sicherheitsverletzung beim US-amerikanischen Office of Personnel Management zeigte.

Die Methode des Angriffs beim OPM folgte einem bestimmten Muster: Greife einen Subunternehmer via Social Engineering an, und stehle dessen Anmeldeinformationen, um dir Zugriff auf das Netzwerk zu verschaffen. Platziere Malware in einem System, und schaffe dir ein Hintertürchen. Schaffe die Daten monatelang unerkannt nach außen.

Dieser Verstoß beim OPM offenbarte auch die Anfälligkeit der Unternehmen für Social-Engineering-Angriffe. Mitarbeiter und Subunternehmer von Behörden werden inzwischen geschult, um ihr Bewusstsein im Hinblick auf Security zu stärken und um zu lernen, welche Gefahren Phishing und andere Social-Media-Bedrohungen bergen.

> „Die innovativsten und verheerendsten Hacking-Angriffe 2015“,
> CSO Magazine, 28. Dezember 2015

Viele Risiken lassen sich mithilfe der in diesem Dokument beschriebenen fünf Best Practices abmildern, die zusammen ein wirksameres, mehrschichtiges und flexibleres Instrument für die Informationssicherheit bilden. Diese Best Practices sind:

- Implementierung unterstützender Prozesse und Kontrollen, die die Zugriffsrichtlinien für privilegierte Anwender bei Drittanbietern definieren und erzwingen
- Bessere Authentifizierung der Anwender durch den Einsatz einer Mehrfaktor-Authentifizierungstechnologie, damit die Anmeldeinformationen privilegierter Anwender schwerer kompromittiert werden können, auch bei Social-Engineering- und Phishing-Angriffen
- Trennung der Authentifizierung von der Access Control, sodass privilegierte Anwender nur begrenzt Einblicke in interne Netzwerke haben und der Schaden, den Anwender bzw. ihre gestohlenen Anmeldeinformationen anrichten können, minimiert wird
- Verhinderung von Fehlern und unbefugten Befehlen, indem als erstes Abwehrinstrument Trigger in Echtzeit ausgelöst werden, was die Infrastruktur vor Nachlässigkeiten und böswilligen Aktivitäten bewahrt
- Überwachung der Aktivitäten und Untersuchung verdächtiger Ereignisse, um Verstöße schnell zu erkennen, das Schulungsangebot bei Bedarf zu verbessern und die Automatisierung und andere Vorgänge kontinuierlich zu optimieren, um Fehlalarme zu eliminieren

Privileged-Access-Management-Systeme verfügen über automatisierte Leistungsmerkmale und Funktionen, die dabei helfen, die fünf beschriebenen Best Practices im gesamten Unternehmen für physische, virtuelle und Cloud-basierte Umgebungen zu definieren, zu automatisieren und zu erzwingen. So können die Unternehmen system-, anwendungs- und geräteübergreifend konsistente Prozesse implementieren.

Abschnitt 5

Literaturhinweise

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

Bericht des NYS Financial Services Department vom 9. April, „Update on Cyber Security in the Banking Sector: Third Party Service Providers“
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

„How Much do Data Breaches Cost Big Companies? Shockingly Little“
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ 27. März 2015

http://fortune.com/tag/data-breach 2. März 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh 27. Juli 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx August 21, 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Abschnitt 6:

Informationen zum Autor

Dale R. Gardner verfügt über mehr als zwei Jahrzehnte Erfahrung mit Unternehmenssoftware insbesondere für das Netzwerk- und Systemmanagement und mehrere Bereiche der Security, darunter Identity Management, Anwendungs-Security, Schwachstellenmanagement, Einhaltung von Vorschriften und Netzwerk-Security. 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. Von der Planung über die Entwicklung bis hin zu Management und Security arbeitet CA Technologies weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, neu zu gestalten – ob mobil, in der privaten oder öffentlichen Cloud oder in verteilten Systemen oder Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.

CS200_183401_0416