X-Force

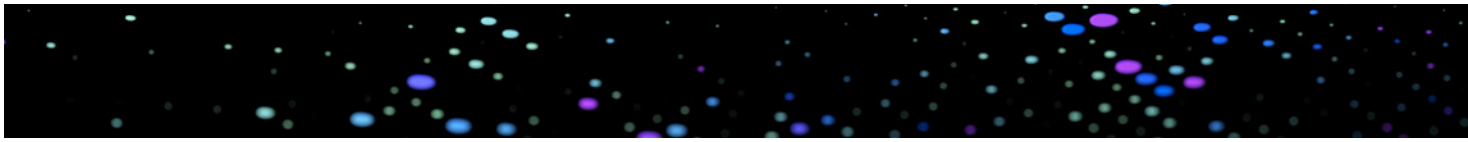
2021 IBM Security X-Force Bericht über Insider-Bedrohungen

IBM Security X-Force Threat Intelligence

Special Intelligence Report Q2 2021

IBM

Inhaltsverzeichnis



Einführung

Die Cyber-Bedrohungslandschaft verändert sich ständig, da sowohl Angreifer als auch Verteidiger bei neuen Technologien und Verfahren sehr innovativ agieren. Unternehmen geben insgesamt rund USD 60 Milliarden pro Jahr für den Schutz ihrer Anlagen und die Einstellung neuer Mitarbeiter aus, um Angriffe verhindern und auf diese reagieren zu können. Die Sicherheitsausgaben stiegen im Jahr 2021 um weitere 10 %.[1]

Während ein Großteil der Sicherheitsmaßnahmen und -ausgaben eines Unternehmens darauf ausgerichtet ist, Angriffe von außen abzuwehren, werden Insider-Bedrohungen oft übersehen: und zwar jene, die aus dem Unternehmen selbst kommen. Insider-Bedrohungen, von denen sich viele als nicht böswillig oder versehentlich herausstellen, haben das Potenzial, verheerende Schäden in Form von Datendiebstahl, finanziellen Verlusten, Diebstahl von geistigem Eigentum und Rufschädigung zu verursachen. In einer Umfrage aus dem Jahr 2020 schätzte das Ponemon Institute, dass Unternehmen im Durchschnitt USD 644.852 für die Erholung von einer Insider-Bedrohung ausgeben, unabhängig von der Ursache des Vorfalls.[2] Dazu gehören die Kosten für die Überwachung und Untersuchung mutmaßlicher Insider-Vorfälle als auch die Reaktion auf so einen Vorfall, die Eindämmung, Beseitigung und Behebung.

In diesem Paper definiert IBM Security X-Force einen „Insider“ wie folgt:

— Der fahrlässige Insider: ein unaufmerksamer Mitarbeiter oder ein anderer Lieferant/Auftragnehmer.[3]

— Der böswillige Insider: ein krimineller oder böswilliger Mitarbeiter oder ein anderer Lieferant/Auftragnehmer.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. Als ein fahrlässiger Insider wird eine Person definiert, die versehentlich einen Vorfall verursacht, der die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Systemen innerhalb eines Unternehmens beeinträchtigt. Dazu gehören keine Phishing-/Social-Engineering-Vorfälle.

Anhand von exklusiven, proprietären Daten aus tatsächlichen Untersuchungen zur Reaktion auf derartige Vorfälle analysierte X-Force mutmaßliche Insider-Bedrohungen – sowohl versehentliche als auch böswillige –, von denen Unternehmen zwischen 2018 und 2020 betroffen waren. In Verbindung mit Open-Source-Berichten über die bekanntesten Angriffe durch Insider-Bedrohungen werden in diesem Paper wichtige Erkenntnisse aus diesen Daten untersucht, darunter:

— Wie die meisten Insider-Angriffe festgestellt werden.

— Die Rolle, die die Zugriffsebene bei Insider-Angriffen spielt.

— Bewährte Verfahren zur Eindämmung von Insider-Bedrohungen.

Die wichtigsten Forschungsergebnisse

40 % der Vorfälle wurden durch Warnungen entdeckt, die über ein internes Überwachungstool ausgelöst wurden.

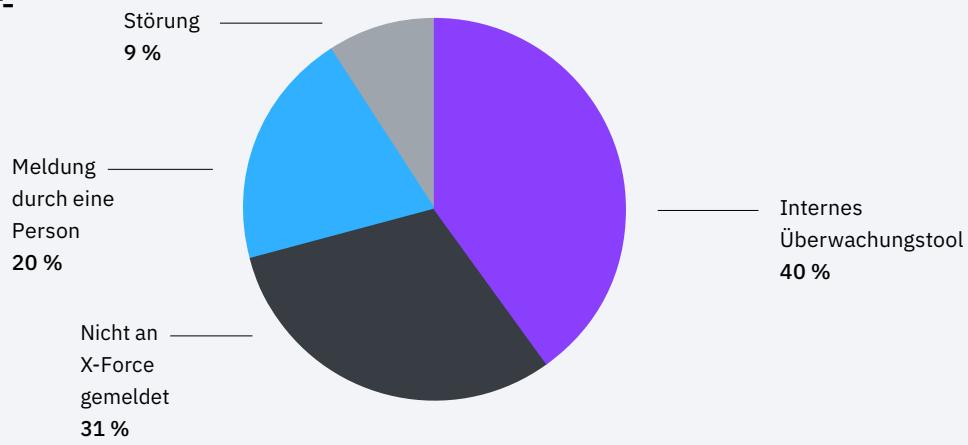
40 % der Vorfälle standen in Zusammenhang mit einem Mitarbeiter mit privilegiertem Zugriff auf Unternehmensressourcen.

Bei 100 % der Vorfälle, in denen der Insider nachweislich oder wahrscheinlich über einen administrativen Zugriff verfügte, spielte dieser erweiterte Zugriff eine Rolle bei dem Vorfall selbst.

Wie Insider-Angriffe erkannt werden

Als Insider-Bedrohungen werden im Allgemeinen Angriffe definiert, bei denen rechtmäßige Benutzer, die in gewissem Umfang Zugriff auf Unternehmensressourcen haben, diesen Zugriff entweder böswillig oder versehentlich nutzen und dem Unternehmen dadurch letztlich Schaden zufügen. Diese Bedrohung kann von einem aktuellen oder ehemaligen Mitarbeiter oder von einem anderen Auftragnehmer/Lieferanten ausgehen, der Zugriff auf die Daten hat, um damit bestimmte geschäftliche Aufgaben zu erfüllen.

Wie der Insider-Angriff erkannt wurde



Eine Analyse der Insider-Bedrohungen, auf die X-Force seit 2018 reagiert hat, zeigt, dass 40 % dieser Vorfälle durch Warnungen entdeckt wurden, die durch ein internes Überwachungstool gemeldet wurden. Meldungen durch Personen – z. B. Mitarbeiter, die ihr Unternehmen auf ungewöhnliche Aktivitäten aufmerksam machen – machten 20 % der ermittelten Fälle aus. In 9 % der Fälle wurden die Sicherheitsteams durch Systemstörungen gewarnt.

Der Cost of Insider Threats: Global Report 2020 des Ponemon Institute, unterstützt durch ObserveIT und IBM, schätzt, dass Unternehmen mithilfe von Tools wie User Behavior Analytics (UBA), Privileged Access Management (PAM), Security Information and Event Management (SIEM) und Programme wie Threat Intelligence Sharing und zur Schulung und Sensibilisierung der Benutzer im Durchschnitt USD 3 Millionen einsparen können, da durch ihren Einsatz Insider-Risiken von vornherein verringert oder sogar vollständig ausgeräumt werden.[4]

Kosteneinsparungen von USD 3 Millionen

Tools wie UBA, PAM, SIEMs und Programme wie Threat Intelligence Sharing und zur Schulung und Sensibilisierung der Benutzer verhelfen den Unternehmen zur Einsparung von schätzungsweise durchschnittlich USD 3 Millionen bei der Reduzierung oder Beseitigung von Insider-Risiken.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Mangelnder Nachweis und unbekannte Variablen in der X-Force-Forschungsstudie

Bei Insider-Vorfällen bei denen die Feststellungsmethode „nicht an X-Force gemeldet“ wurde oder ein „mangelnder Nachweis“ vorlag, erhielten die X-Force-Reaktionsteams nicht genügend Informationen, um eine Entscheidung über die Feststellungsart treffen zu können. Dies liegt oftmals daran, dass viele Unternehmen über geringe Einblicke in ihre Grundumgebung verfügen und nicht genau wissen, wie sie funktioniert. Um ungewöhnliche Aktivitäten innerhalb eines Systems zu erkennen, ist es wichtig zu wissen, wie normale Aktivitäten aussehen, damit Ausreißer leichter und sicherer erkannt werden können. 2019 gab IBM einen SANS-Bericht[5] in Auftrag, der sich mit der Umgebung erweiterter Bedrohungen für Unternehmen befasste. Diese Forschungsstudie ergab Folgendes:

- 48 % der Unternehmen erkannten die größte Sicherheitslücke in der mangelnden Transparenz ihrer Infrastruktur.
- 35 % waren der Ansicht, dass sie nicht in der Lage sind, einen Missbrauch durch Unternehmensinsider aufzudecken.
- 47 % der Unternehmen gaben zu, nicht in der Lage zu sind, zu verstehen, wie normale Grundaktivitäten in ihren Netzwerken aussehen.

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

Privilegierter versus administrativer Zugriff

X-Force hat bei der Analyse von Insider-Bedrohungen zwischen zwei Benutzertypen unterschieden.

Ein **privilegierter Benutzer** ist eine Person innerhalb eines Unternehmens, die Zugriff auf sensible Daten hat. Bei diesen Daten kann es sich um geistiges Eigentum, Kunden- oder Personaldaten handeln. Bei diesen Benutzern könnte es sich um Personen handeln, die über einen Zugriff auf sensible Geschäftsinformationen wie Fusions- und Übernahmedaten oder andere rechtliche Informationen verfügen.

Benutzer mit **administrativem Zugriff**, auch als Administratoren oder Admins bezeichnet, sind Personen mit erweiterten Zugriffsrechten auf IT-Systeme innerhalb des Netzwerks. Theoretisch sollte es bei dieser Art des Zugriffs keine Überschneidungen geben. X-Force hat jedoch festgestellt, dass die IT-Umgebungen von Endnutzern oft überdimensioniert sind.

Insider mit administrativem Zugriff unterscheiden sich von jenen mit sensiblem Zugriff auf eine Unternehmensumgebung. Dazu gehören Mitarbeiter und Auftragnehmer/Lieferanten mit Zugriff auf die IT-Umgebung des Unternehmens, die aufgrund ihrer erweiterten Netzwerkprivilegien ein besonderes Risiko für das Unternehmen darstellen.

Beispiele für Positionen mit privilegiertem Zugriff

- HR-Positionen
- Leitende Positionen
- Finanzpositionen
- Juristische Positionen
- Positionen in der Forschung
- Andere Positionen mit Zugriff auf geistiges Eigentum eines Unternehmens oder auf die „Kronjuwelen“ oder Kundendaten

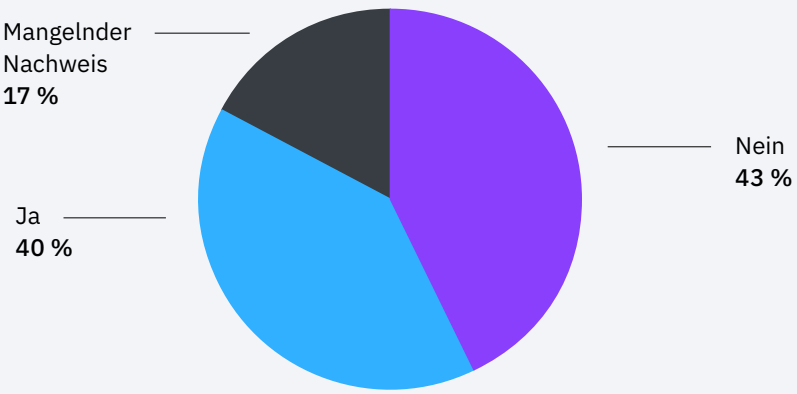
Beispiele für Positionen mit administrativem Zugriff

- Serveradministratoren
- IT-Administratoren
- Help-Desk
- Andere IT-Anbieter
- Weitere Positionen, welche Änderungen an den Konfigurationen/Einstellungen auf IT-Systemen vornehmen können

Wer beobachtet die Beobachter?

Haben Insider, die die Zwischenfälle verursachen, in der Regel privilegierten Zugriff? Kurz gesagt: ja.

Hatte der Insider privilegierten Zugriff auf Daten?



Eine Analyse der X-Force-Daten zeigt, dass bei 40 % der von Insidern verursachten Vorfälle ein Mitarbeiter mit privilegiertem Zugriff auf sensible Unternehmensressourcen beteiligt war. Für diese Forschungsstudie klassifizierte X-Force den privilegierten Zugriff für Personen, die in Bereichen wie der IT-Abteilung, der Personalabteilung, dem Finanzwesen, der Sicherheit oder in Führungspositionen tätig sind.

Bei weiteren 17 % der Daten war unklar, ob der Insider privilegierten Zugriff auf sensible Daten hatte oder nicht. Die Zahl der von Benutzern mit privilegiertem Zugriff verursachten Vorfälle könnte also noch wesentlich höher liegen.

Personen mit erweitertem Zugriff auf kritische Ressourcen wie Netzwerkfreigaben, Sicherheitsanwendungen, E-Mail-Systemen, persönlich identifizierbaren Informationen von Mitarbeitern oder Kunden, geistigem Eigentum oder Finanzdaten können ein deutlich höheres Risiko darstellen als Personen mit eingeschränkten Rechten.

Demzufolge kosten Vorfälle, die versehentlich durch Insider mit privilegiertem Zugriff verursacht werden, Unternehmen mehr als solche, die versehentlich durch Insider mit geringeren Zugriffsrechten verursacht werden. Vorfälle, die durch böswillige Insider mit höheren Zugriffsrechten ausgelöst werden, sind noch kostspieliger, da diese Angriffe zu einer folgenschweren Datenpanne führen können. So wurde beispielsweise 2018 ein australischer Immobilienmakler für schuldig befunden, vor seinem Ausscheiden aus einem renommierten lokalen Maklerunternehmen auf dessen vertrauliche Datenbanken zugegriffen zu haben. Der Mitarbeiter manipulierte den Stand der Verkaufsaussichten im System durch eine Herabstufung des potenziellen Kundeninteresses. Außerdem gestand er die Mitnahme von mehr als 200 Kundendatensätzen, um mit diesen bei einer anderen Makleragentur neue Aufträge zu generieren. Dieser Insider-Angriff hat das betroffene Maklerunternehmen schätzungsweise USD 30 Millionen an potenziellen Immobilienverkäufen gekostet.[6]

Eine der wirkungsvollsten Möglichkeiten, Insider-Vorfälle mithilfe von Zugriffsrechten zu verhindern, ist das Prinzip der Minimalprivilegien. Hierbei wird sichergestellt, dass die Benutzer über die geringstmöglichen Berechtigungen zur Ausführung ihrer Aufgaben im Unternehmen verfügen. Dies kann in Form einer Privileged Access Management (PAM) Lösung erfolgen, die auf einem Zero-Trust-Modell aufbaut.[7,8] Bei diesem Modell erhalten Personen, die über ein Benutzerkonto verfügen, so wenige Berechtigungen wie möglich. Dadurch verringert sich die Wahrscheinlichkeit, dass ein Insider unbeabsichtigten Zugriff auf Daten oder andere Ressourcen erhält. Dieses Konzept ist in der Cloud noch wichtiger, wo weitere Daten gespeichert sind und sowohl menschliche als auch nichtmenschliche Zugriffe erfolgen.

Der Cost of Insider Threats: Global Report 2020 zeigte, dass nur 39 % der Unternehmen Privileged Access Management in irgendeiner Form einsetzen.[9] Außerdem machte er deutlich, dass die Einführung eines PAM zu Kosteneinsparungen in Höhe von USD 3,1 Millionen führte, was die Wirksamkeit dieser Maßnahme unterstreicht.

39 %

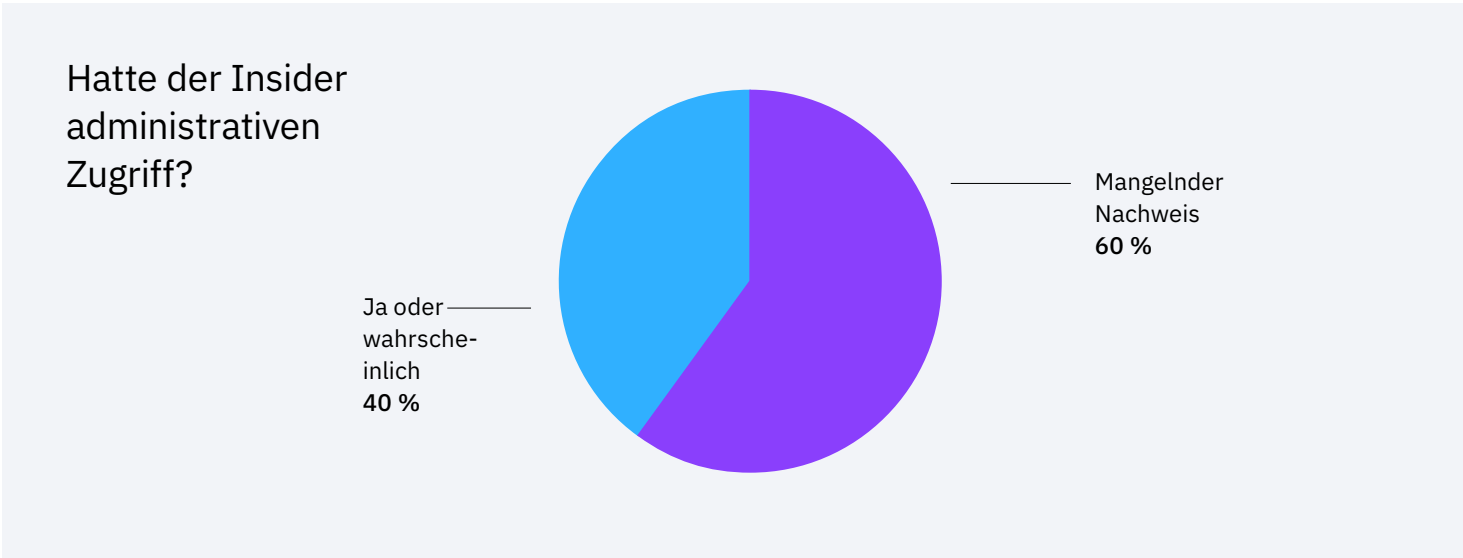
39 % der Unternehmen setzen Privileged Access Management in irgendeiner Form ein.[9] Dies hat zu Kosteneinsparungen in Höhe von USD 3,1 Millionen geführt.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

Der Missbrauch des administrativen Zugriffs kann teuer werden

Es sind zahlreiche Fälle bekannt geworden, in denen Insider ihre Macht als Verwaltungsangestellte in Unternehmen für schädliche Zwecke missbraucht haben, z. B. aus Rache, Habgier oder aus anderen böswilligen Gründen. Im Februar 2020 wurde der ehemalige Microsoft-Ingenieur Volodymyr Kvashuk für schuldig befunden, seinen privilegierten Zugriff genutzt zu haben, um digitale Vermögenswerte des Unternehmens im Wert von über USD 10 Millionen zu stehlen.[10] Der Diebstahl wurde durch Kvashuks administrativen Zugriff auf die Einzelhandelsplattform ermöglicht, für die er verantwortlich war.[11] Konkret verwendete Kvashuk die E-Mail-Adressen seiner Kollegen und gültige Testkonten im System und verschleierte dadurch ihre Aktivitäten, einschließlich der Exfiltration von digitalen Geschenkkarten. Diese und andere gestohlene Wertsachen verkaufte er im Internet und erzielte daraus einen großen Gewinn, mit dem er später ein Haus im Wert von USD 1,6 Millionen sowie einen Tesla im Wert von USD 160.000 erwarb.[12]

Der Missbrauch des administrativen Zugriffs in Zahlen

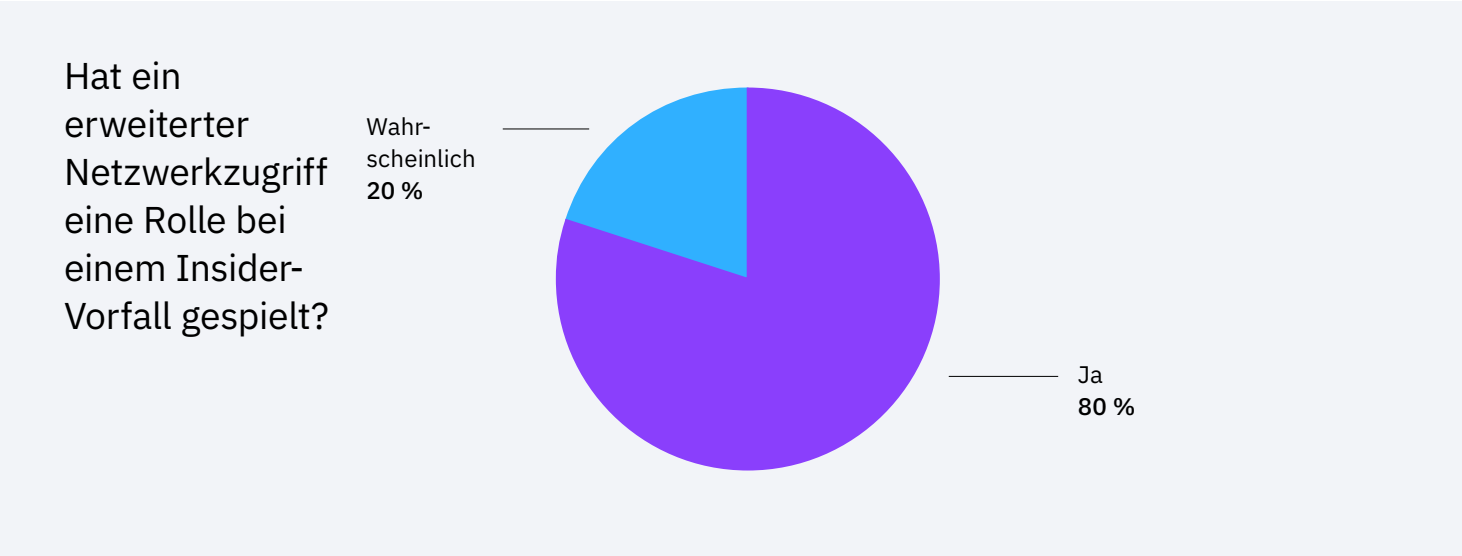


Bei 40 % der Vorfälle, auf die X-Force von 2018 bis 2020 reagierte, hatte ein Insider nachweislich oder wahrscheinlich administrativen Zugriff auf das betroffene Netzwerk. Die X-Force-Analysten bestimmten die Art des Insider-Zugriffs anhand der Einzelheiten zum Vorfall, sofern die spezifische Position des betreffenden Benutzers vom Kunden nicht angegeben wurde.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

Bei den Vorfällen kam es u. a. zur Datenexfiltration, zur Offenlegung und Löschung sensibler Daten und zur Installation nicht autorisierter Software. Einige Unternehmen verloren Petabytes an Protokollen, die von Servern gelöscht wurden, mussten absichtliche Quellcode-Lecks in Kauf nehmen oder hatten mit teuren Ausfällen zu kämpfen, die von einem Insider mit Administratorrechten verursacht wurden.

Interessanterweise spielte bei 100 % der Vorfälle, bei denen der Insider nachweislich oder wahrscheinlich über administrativen Zugriff verfügte, dieser erweiterte Zugriff eine Rolle bei dem Vorfall selbst. (Siehe Diagramm unten)



Anders ausgedrückt: Hätte der Insider über keinen administrativen Zugriff verfügt, hätte der Vorfall wahrscheinlich weitaus geringere Folgen für das Unternehmen gehabt oder hätte sich in vielen Fällen gar nicht erst ereignet. X-Force reagierte auf mehrere Insider-Vorfälle, bei denen wichtige Datenbanken und Protokolle von Servern gelöscht wurden. Hätte der Insider über keinen administrativen Zugriff auf diese Systeme verfügt, wäre es erst gar nicht zu dem Vorfall gekommen.

Empfehlungen

X-Force ist der Ansicht, dass die Zahl der Insider-Vorfälle in den Daten von Dritten unterrepräsentiert ist. Wahrscheinlich existieren noch weitaus mehr Vorfälle dieser Art, die von Unternehmen intern abgewickelt und aus Angst vor Haftung oder Rufschädigung des Unternehmens nicht veröffentlicht werden.[13]

Die Forschungen und Daten von X-Force zeigen, dass potenzielle Insider-Bedrohungen aufgrund der Auswirkungen, die diese Vorfälle auf ein Unternehmen haben können, ein wichtiger Bestandteil eines Informationssicherheitsprogramms sein müssen. IBM Security empfiehlt bei Insider-Bedrohungen insbesondere Folgendes:

Defense-in-Depth-Strategien eignen sich gut zur Erkennung von Insider-Bedrohungen.

Viele gehen davon aus, dass ein mehrschichtiger Ansatz bei den von Unternehmen implementierten Technologien und Prozessen vor externen Bedrohungen schützen soll. Die X-Force-Forschungsstudie zeigt jedoch, dass viele dieser Tools, darunter SIEM-Lösungen (Security Information and Event Management), auch für die Erkennung von Insider-Bedrohungen entscheidend sind.

Sie müssen wissen, was in Ihrer Umgebung normal ist.

Die beste Möglichkeit, verdächtige Aktivitäten jeglicher Art von Angreifern zu erkennen, besteht in erster Linie darin, zu wissen, welche Aktivitäten innerhalb des eigenen Netzwerks als normal gelten. Ein solides Verständnis der Grundaktivitäten macht es einfacher, abweichendes Verhalten zu erkennen und umgehend und effektiv darauf zu reagieren. Eine robuste UBA-Lösung (User Behaviour Analytics) stellt diese Funktion bereit und passt sich im Laufe der Zeit an Änderungen in Ihrer Umgebung an.

Administrative Zugriffsrechte sind regelmäßig zu überprüfen.

X-Force stellte fest, dass mehrere Insider-Vorfälle, in welche Administratoren verwickelt waren, wahrscheinlich auf übermäßige Zugangsrechte der Benutzer zurückzuführen waren. Strenge Änderungs- und Prozesskontrollen sollten für den administrativen Zugriff eingeführt werden, insbesondere auf unternehmenskritischen Servern. Nutzen Sie ggf. Technologielösungen, die den administrativen Zugriff auf sensible Systeme und Funktionen protokollieren und nur vorübergehend gewähren.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Informationssicherheits- und IT-Verwaltungsteams müssen getrennt voneinander arbeiten.

Die Erfahrung von X-Force hat gezeigt, dass ein ausgewogener Ansatz zur Verwaltung der Unabhängigkeit und Governance von Sicherheits- und Verwaltungsteams zu mehr Sicherheit beiträgt. Er ermöglicht den Verwaltungsteams die nötige Flexibilität und Kreativität, um die Untersuchung und Feststellung von Bedrohungen zu optimieren und gleichzeitig dem Unternehmen eine ausreichende Überwachung und Kontrolle zu bieten, damit Risiken innerhalb des Teams minimiert werden können.

Erstellen Sie Risikoprofile für sensible Unternehmenspositionen.

Da bei vielen Insider-Vorfällen, auf die X-Force reagierte, erweiterte Zugriffsrechte eine Rolle spielten, empfehlen wir Unternehmen, Risikoprofile für Positionen innerhalb des Unternehmens zu erstellen, die über einen sensiblen oder administrativen Zugriff auf Systeme oder Daten verfügen. Die Implementierung einer PAM-Lösung (Privileged Access Management), die auf einem Zero-Trust-Modell aufbaut, gewährt den Benutzern nur die minimal notwendigen Rechte und kann so die Folgen von Insider-Vorfällen minimieren.

Aktualisieren Sie das Incident Response Playbook, damit auch Insider-Bedrohungen berücksichtigt werden.

Eine generelle Schulung für diese Art von Vorfällen ist nicht ausreichend. Die meisten Incident Response Playbooks sind auf externe Angriffe ausgelegt, Unternehmen sollten aber auch Szenarien für versehentliche oder böswillige Insider-Bedrohungen in ihre Abläufe aufnehmen. Ziehen Sie die Zusammenarbeit mit einer Organisation in Erwägung, bei der Sie für die Entwicklung von Notfallplänen und angriffsspezifischen Playbooks Unterstützung erhalten, damit Sie sich besser auf einen Cyberangriff vorbereiten und darauf reagieren können.

Schulen Sie Ihre Mitarbeiter regelmäßig.

Ethische Geschäftspraktiken sind neben Social-Engineering-Schulungen Bestandteil der jährlichen Schulungsprogramme zahlreicher Unternehmen. Viele der Insider-Vorfälle, auf die X-Force reagiert hat, wurden von Mitarbeitern, nicht von technologischen Lösungen entdeckt. Unternehmen sollten die Meldung eines vermuteten Insider-Vorfalls in die jährlichen Schulungen zu Geschäftsethik oder Social Engineering aufnehmen. Außerdem tragen rollenbasierte Schulungen für Mitarbeiter mit privilegiertem Zugriff dazu bei, auf Anzeichen sensibilisiert zu werden, die darauf hindeuten, dass etwas in ihrer Umgebung nicht in Ordnung ist.

Nutzen Sie seriöse Threat Intelligence Services.

Oft stehen Kunden vor der Herausforderung, Bedrohungsdaten zu erstellen, zu verwalten und zu operationalisieren. Wählen Sie eine Lösung, die die Bündelung, Automatisierung und Integration unterstützt, die für eine umfassende Operationalisierung von Bedrohungsdaten erforderlich sind.

Managed Detection and Response Services bieten Schutz rund um die Uhr.

MDR-Sicherheitsservices (Managed Detection and Response) sind unerlässlich, um Insider-Bedrohungen vorzubeugen, sie zu erkennen und schnell darauf zu reagieren. Lösungen, die über die herkömmliche Prävention hinausgehen, indem sie AV der nächsten Generation für verhaltensbasierte Blockierungen, Untersuchungen und kontinuierliche Richtlinienverwaltung einsetzen, sind unverzichtbar.

Erfahren Sie, wie IBM Security Kunden dabei hilft, komplexe und kritische Umgebungen vor externen und internen Bedrohungen zu schützen.

Weitere Informationen zu IBM Security

IBM Security

© Copyright IBM Corporation 2021

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika
Mai 2021

IBM, das IBM Logo, ibm.com und X-Force sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der Marken von IBM finden Sie auf der Webseite „Copyright and trademark information“ unter ibm.com/legal/copytrade.html.

Das vorliegende Dokument ist mit Stand vom Datum der ersten Veröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist. DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN. Die Garantie für Produkte von IBM richtet sich nach den Bestimmungen und Bedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

IBM