netwrix

Leitfaden zum Thema Insider-Bedrohungen:

Vermeiden von Datendiebstahl durch ausscheidende Mitarbeiter

Inhalt

Einführung

Stellen Sie sich Ihre IT-Infrastruktur als Burg vor, in der Ihre besonders kritischen Daten residieren. Noch vor wenigen Jahren mussten Sie zur Verteidigung dieser „Kronjuwelen“ lediglich einen Graben um die Burg herum ziehen, um Angreifer abzuwehren. Doch die Zeiten haben sich geändert. Noch immer investieren Unternehmen jedes Jahr viele Milliarden in Firewalls und Angriffserkennungssysteme, um ihre Daten vor Hackern zu schützen. Die eigentliche Gefahr lauert jedoch häufig innerhalb der Burgmauern: die Mitarbeiter.

Welche Konsequenzen hätte für Sie Datendiebstahl durch Mitarbeiter, die das Unternehmen verlassen? In der digitalen Welt von heute geht das Problem von Datendiebstahl durch ausscheidende Mitarbeiter weit über die Mitnahme einiger Kundennamen oder Produktdesignentwürfe hinaus. Ein solcher Datendiebstahl kann den Verlust vieler Gigabyte wichtiger Unternehmensdaten und rechtlich geschützter Informationen wie Kreditkartendaten von Kunden bedeuten. Ehemaligen Mitarbeitern stehen darüber hinaus heute wesentlich mehr Möglichkeiten zur Nutzung gestohlener Daten zur Verfügung: Sie können die Daten gegen ihren früheren Arbeitgeber verwenden, an Konkurrenten weitergeben, meistbietend verkaufen oder einfach im Internet veröffentlichen.

Dass Mitarbeiter bei ihrem Ausscheiden aus dem Unternehmen sensible Geschäftsdaten „mitnehmen“, mag sich wie ein Albtraum anhören, ist aber leider oft traurige Realität. So hat eine Umfrage von Biscom ergeben, dass ein Viertel der Mitarbeiter Daten mitnehmen, wenn sie ein Unternehmen verlassen. Auch in den Medien wird häufig über solche Fälle berichtet, wie die jüngsten Beispiele von Uber und Gucci zeigen.

Viele Unternehmen haben diese Gefahr bereits erkannt: Laut einer Umfrage zu IT-Sicherheitsrisiken, die Kaspersky im Jahr 2017 durchgeführt hat, sehen 52 % der Unternehmen in ihren Mitarbeitern das größte Risiko für die IT-Sicherheit. Insbesondere durch fahrlässiges Handeln gefährden sie die Umsetzung der Unternehmensstrategie. Wenn Sie noch nicht zu diesen 52 % gehören, ist es höchste Zeit, dass auch Sie sich der Gefahren bewusst werden, die von ausscheidenden Mitarbeitern ausgehen.

In diesem E-Book zeigen wir auf, weshalb ausscheidende Mitarbeiter zum Albtraum für die Sicherheit Ihres Unternehmen werden können, und beleuchten die Motive für Datendiebstahl. Wir erläutern, wie es zu Datendiebstahl kommen kann, und geben Ihnen Tipps an die Hand, wie Sie dieses Risiko mindern können.

Gründe, warum ausscheidende Mitarbeiter ein Sicherheitsrisiko darstellen können

Befassen wir uns zunächst mit den fünf häufigsten Gründen, warum Mitarbeiter zu „Bösewichten“ werden können:

1. HR und IT: zwei unterschiedliche Planeten

In vielen Unternehmen gestaltet sich die Kommunikation zwischen der Personalabteilung und der IT-Abteilung schwierig und findet folglich so selten statt, dass man den Eindruck hat, sie lebten auf zwei verschiedenen Planeten. Dieser Mangel an Kommunikation ist ein idealer Nährboden für ausscheidende Mitarbeiter mit unlauteren Absichten. Wenn das IT-Team nicht umgehend über Kündigungen informiert wird, haben böswillige Insider genügend Zeit, ihre Rechte zu missbrauchen und sensible Daten zu kopieren oder wichtige Daten zu löschen, damit auch andere keinen Zugriff mehr darauf haben. Natürlich ist eine unzureichende Kommunikation nicht der einzige Grund, warum Mitarbeiter auch nach ihrem Ausscheiden aus dem Unternehmen weiterhin über Zugriffsrechte verfügen können. Mitunter ist auch das IT-Team so überlastet und personell unterbesetzt, dass es schlicht nicht in der Lage ist, Konten zu deaktivieren – auch wenn bekannt ist, dass ein Mitarbeiter das Unternehmen verlassen hat. Das Ergebnis ist in beiden Fällen dasselbe: Es entsteht eine Sicherheitslücke.

2. Mitarbeiter werden oft nur unzureichend geschult

Werden Mitarbeiter nicht ausreichend geschult, was erlaubt ist und was nicht, kann es schnell zu Cybersicherheitsvorfällen kommen. So hat die Umfrage von Kaspersky zu IT-Sicherheitsrisiken ergeben, dass nachlässige oder unwissende Mitarbeiter mit 46 % nach Schadsoftware die zweithäufigste Ursache für schwerwiegende Sicherheitsverletzungen sind. Angesichts der Tatsache, dass für HR-Abteilungen die Schulung von Mitarbeitern zu zulässigen und unzulässigen Verhaltensweisen häufig nicht die höchste Priorität hat, überrascht es nicht, dass ausscheidende Mitarbeiter sich ihres Fehlverhaltens mitunter einfach nicht bewusst sind, wenn sie Dokumente oder eine Liste mit Kontaktdaten zu ihrem neuen Arbeitgeber mitnehmen.

3. Untätigkeit hat Folgen

Laut dem Bericht von Biscom gaben 90 % der Umfrageteilnehmer als Hauptgrund für die Mitnahme von Daten bei ihrem Ausscheiden aus dem Unternehmen an, dass ihr Arbeitgeber keine Richtlinien oder Technologien zur Verhinderung von Datendiebstahl implementiert hatte. Selbst wenn böswillige Absichten gegenüber dem Arbeitgeber nicht das primäre Motiv sind, nehmen Mitarbeiter vertrauliche Informationen mit, die an ihrem neuen Arbeitsplatz von Nutzen für sie sein könnten. Die Umfrage von Biscom hat ergeben, dass 85 % der Mitarbeiter, die Datendiebstahl begangen hatten, nur von ihnen selbst erstellte Dokumente mitgenommen hatten – frei nach dem Motto „was ich erstellt habe, gehört auch mir“. Lediglich 25 % der Befragten hatten auch Daten mitgenommen, die sie nicht selbst erzeugt hatten.

Wenn es keine Richtlinien mit klaren Regelungen dazu gibt, welche Maßnahmen beim Ausscheiden von Mitarbeitern zu ergreifen sind, ist es für IT-Teams nahezu unmöglich nachzuvollziehen, welche Daten kopiert oder gelöscht wurden, bevor es zu spät ist. Verschärft wird das Problem durch die zunehmende Beliebtheit von BYOD, insbesondere wenn die privaten Geräte der Mitarbeiter unzureichend verwaltet werden. Wird ein Beschäftigungsverhältnis beendet, bittet die IT-Abteilung den Mitarbeiter nur in den seltensten Fällen, seine persönlichen Geräte vorzuzeigen, um sicherzustellen, dass kritische Daten gelöscht wurden und nicht weiterhin auf dem privaten Gerät genutzt werden können.

4. Eine Verquickung unglücklicher Konten

Nur zu oft kennt ein ausscheidender Mitarbeiter die Kennwörter für Teamkonten, die den Zugriff auf wichtige Systeme oder Anwendungen wie CloudShare oder Dropbox ermöglichen. Er kann mit diesen Anmeldedaten aus persönlichen Gründen oder auf Aufforderung seines neuen Arbeitgebers auf Ihre Daten zugreifen und diese für seine Zwecke nutzen. Wenn die Kennwörter für gemeinsam genutzte Konten regelmäßig und insbesondere beim Ausscheiden von Mitarbeitern geändert werden, lässt sich das Risiko von unerlaubten Zugriffen auf kritische Daten deutlich mindern. Doch nur wenige Unternehmen beherzigen diese relativ einfache Best Practice.

5. Keine Verschwörungstheorie: Diebstahl von Betriebsgeheimnissen

Das schlimmste Szenario sind Mitarbeiter konkurrierender Unternehmen, die sich mit ausscheidenden Mitarbeitern Ihres Unternehmens verbünden, um Zugriff auf Betriebsgeheimnisse zu erlangen, die für sie von Vorteil sind. Solche Fälle können langwierige und kostspielige Gerichtsverfahren nach sich ziehen oder sogar das endgültige Aus für ein Unternehmen bedeuten.

Die Motive für Datendiebstahl durch ausscheidende Mitarbeiter

Nahezu alle sensiblen Daten werden heutzutage elektronisch gespeichert – von vertraulichen Betriebsgeheimnissen über Kundendaten bis hin zu Mitarbeiterinformationen. Zur Erledigung ihrer Aufgaben müssen Mitarbeiter auf bestimmte Daten zugreifen können. Leider sind manche der Auffassung, dass ihnen diese Daten auch gehören, wenn sie täglich damit arbeiten – und dass sie diese Daten folglich einfach mitnehmen können, wenn sie das Unternehmen verlassen. Andere wissen durchaus, dass dies Datendiebstahl ist, lassen sich aber dennoch nicht davon abhalten.

Die Motive für Datendiebstahl können sehr unterschiedlich sein: Ausscheidende Mitarbeiter möchten die Daten beispielsweise nutzen, um eigene, konkurrierende Unternehmen aufzubauen, die Informationen auf dem Schwarzmarkt verkaufen oder sich an ihrem ehemaligen Arbeitgeber rächen. Alle Fälle von Datendiebstahl lassen sich jedoch in folgende Kategorien unterteilen:

- **Datendiebstahl mit böswilliger Absicht:** Mitarbeiter mit unlauteren Absichten legen oft ein ungewöhnliches Verhalten an den Tag. Sie greifen beispielsweise auf Dateien zu, die sie noch nie zuvor abgerufen haben, kopieren sehr viele Dateien oder leiten wichtige E-Mails an ihr persönliches Postfach weiter. Administratoren mit privilegierten Rechten nehmen unerlaubt oder ohne Genehmigung kritische Änderungen vor, um weitere Berechtigungen zu erlangen. Solche Aktivitäten können ein Hinweis auf den Missbrauch von Berechtigungen sein, der zu Datendiebstahl führt.

- **Datendiebstahl ohne böswillige Absicht:** Mitarbeiter können auch ohne böswillige Absicht durch ihr Verhalten die Sicherheit Ihrer Daten gefährden. Beispiele dafür sind Benutzer, die Dateien auf ihre persönlichen Geräte kopieren, um sie für ein Projekt zu verwenden – ohne zu wissen, dass dies nicht erlaubt und gefährlich ist. Selbst wenn diese Benutzer die kopierten Daten niemals missbrauchen würden, wird es dadurch für Personen mit unlauteren Absichten einfacher, sich Zugriff auf die Daten zu verschaffen. Das IT-Team muss deshalb sicherstellen, dass sich solche Aktivitäten nicht ihrer Kenntnis entziehen und somit die Datensicherheit gefährden können.

- **Datendiebstahl infolge von Datenmissbrauch:** Klassische Beispiele für Datenmissbrauch sind das versehentliche Anhängen der falschen sensiblen Daten an eine E-Mail und das Senden der richtigen sensiblen Daten an die falschen Empfänger. Ganz gleich, ob der Missbrauch durch Unaufmerksamkeit, Stress oder Unkenntnis der richtigen Workflows entsteht – er kann schnell ebenso große Schäden nach sich ziehen wie die anderen Arten von Datendiebstahl.

Die drei häufigsten Methoden, wie ausscheidende Mitarbeiter Daten abgreifen

Weshalb gehen Mitarbeiter ein Risiko ein und begehen Datendiebstahl? Laut dem Verizon Data Breach Investigations Report (DBIR) aus dem Jahr 2017 ist das primäre Motiv dabei der finanzielle Vorteil, der 2016 die Ursache für 60 % der Datenschutzverletzungen war. Dieses Ergebnis überrascht nicht. Personenbezogene Informationen werden auf dem Schwarzmarkt für hohe Summen gehandelt und mit dem Verkauf von gestohlenem geistigen Eigentum (Betriebsgeheimnisse, Verkaufsprognosen, Marketingpläne usw.) an Konkurrenten lassen sich Milliardenbeträge verdienen. Weniger häufige Motive für Datendiebstahl sind Cyberspionage, um die eigene Karriere voranzubringen, Rache, Whistleblowing und das Stehlen von Daten einfach zum Spaß. Doch auch diesen Motiven können finanzielle Überlegungen zugrunde liegen.

Wie genau also läuft ein Datendiebstahl aus diesen unterschiedlichen Motiven ab? Die folgenden drei Beispiele sollen dies veranschaulichen und dabei auch die Folgen für die betroffenen Unternehmen aufzeigen.

Fall 1: Datendiebstahl zur Verschaffung eines finanziellen Vorteils und zur Karriereförderung

Mitarbeiter mit unlauteren Absichten gefährdet die Strategie von Uber für autonomes Fahren (2017)

Dieses Beispiel zeigt, wie aus einem Traum schnell ein Albtraum werden kann. Uber ist eines der erfolgreichsten und meistbekannten Unternehmen weltweit. Um die Entwicklung selbstfahrender Autos voranzutreiben, übernahm Uber das Start-up-Unternehmen Otto und die von ihm entwickelte Technologie sowie das Entwicklungsteam rund um den Gründer Anthony Levandowski. Uber war auf dem besten Weg, die Marktführung im Bereich autonomes Fahren zu übernehmen.

Ein Jahr darauf reichte Waymo, ein weniger bekannter Konkurrent von Uber (und Tochterunternehmen des Konzerns Alphabet, zu dem auch Google gehört), Klage gegen Uber wegen des Diebstahls von Firmengeheimnissen ein.

Laut Waymo hatte Anthony Levandowski rund 14.000 vertrauliche technische Dokumente, Entwürfe, Designdokumente und weitere Dateien gestohlen, als er Waymo verließ, und dieses geistige Eigentum zur Gründung seines Start-ups genutzt, das später von Uber übernommen wurde. Uber befand sich in einer äußerst schwierigen Lage: Dem Unternehmen drohte ein Strafverfahren, weil es sowohl gestohlene Technologien bei der Produktion seiner selbstfahrenden Autos verwendet als auch den Diebstahl von Betriebsgeheimnissen gezielt vertuscht hatte.

Nach verschiedenen öffentlichen Anhörungen waren die Aussichten für Uber alles andere als rosig, insbesondere da gegen das Unternehmen auch wegen eines angeblichen Verstoßes gegen den Computer Fraud and Abuse Act (CFAA) ermittelt wurde. Es stand viel auf dem Spiel:

In dem Prozess ging es um nichts Geringeres als die Entwicklung einer Technologie, die für die Branche ähnlich große Bedeutung haben könnte wie die Erfindung des Autos selbst. Anfang 2018 einigten sich die Kontrahenten auf die Beilegung des Rechtsstreits und Waymo erhielt 0,34 Prozent Anteile an Uber.

Fall 2: Vorsätzlicher Datendiebstahl bzw. vorsätzliche Schädigung

Drama um einen Schönheitschirurgen in Beverly Hills (2017)

Für Patienten von Schönheitschirurgen ist es eine Horrorvorstellung, dass Fotos und Videos ihrer Eingriffe im Internet auftauchen könnten – insbesondere für einen Prominenten, dessen Gesicht Millionen von Zuschauern bekannt ist. Doch genau das passierte Patienten des berühmten Schönheitschirurgen Dr. Zain Kadri aus Beverly Hills.

2016 stellte Dr. Kadri eine Mitarbeiterin ein, die zunächst als Fahrerin und Übersetzerin für ihn arbeitete und später auch für die Eingabe von Patientendaten und Telefonate zuständig war. 2017 verließ sie die Praxis, nachdem ihr vorgeworfen wurde, dass sie Gelder veruntreut hatte. Offenbar hatte sie ihre Rechte als Mitarbeiterin jedoch auch noch auf andere Weise missbraucht. Laut einer Stellungnahme der Praxis hatte sie mit ihrem Firmenhandy Bilder von Patientenakten und Kreditkarteninformationen sowie unangemessene Fotos und Videos von Patienten vor und nach ihrer Operation gemacht.

Dr. Kadri geht davon aus, dass dieses Vorgehen vor allem durch Rache motiviert war. Mindestens ein Teil der Videos und Fotos wurde auf Snapchat und Instagram veröffentlicht – wohl wissend, dass dies die berühmte Klientel von Dr. Kadri verärgern und seiner Praxis Schaden zufügen würde. Es gab keinerlei Beweise dafür, dass die Mitarbeiterin aus finanziellen Motiven handelte oder von einem Konkurrenten angeheuert worden war.

Fall 3: Menschliches Versagen oder Fahrlässigkeit

Fehlverhalten einer Mitarbeiterin führt bei der FDIC zu Datenschutzverletzungen (2016)

Im Februar 2016 endete das Beschäftigungsverhältnis einer Mitarbeiterin der US-amerikanischen Federal Deposit Insurance Corporation (FDIC). An ihrem letzten Arbeitstag lud sie ihre persönlichen Dateien von ihrem Arbeitsrechner auf ein USB-Laufwerk herunter, das sie mit nach Hause nahm. Drei Tage später stellte die Datenschutzsoftware der FDIC fest, dass die Mitarbeiterin zusammen mit ihren persönlichen Daten versehentlich 44.000 Kundendatensätze, die auch personenbezogene Daten enthielten, kopiert hatte. Das Unternehmen setzte sich umgehend mit der ehemaligen Mitarbeiterin in Verbindung und bat sie, das Gerät zurückzugeben und eine eidesstattliche Versicherung zu unterzeichnen, dass sie die Informationen nicht verwenden oder weitergeben würde.

Dieser Fall war deshalb so besorgniserregend, weil es bei der FDIC bereits mindestens fünf ähnliche Sicherheitsvorfälle gegeben hatte, bei denen ausscheidende Mitarbeiter versehentlich Unternehmensdaten auf ihre persönlichen Speichergeräte übertragen hatten, darunter auch hochgradig sensible Daten wie Darlehens- und Bankinformationen. Im Gegensatz zu dem Vorfall im Februar 2016 hatte die FDIC nicht alle früheren Datenschutzverletzungen umgehend gemeldet und darauf reagiert, was eine Reihe von Anhörungen und Bußgelder der Aufsichtsbehörden nach sich zog.

Zwar hat die FDIC inzwischen offenbar begriffen, dass Sicherheitsvorfälle umgehend gemeldet werden müssen, doch sollte sich die Geschäftsführung zwei wichtige Fragen stellen: Wann bringt das Unternehmen seine Sicherheitsrichtlinien auf den neuesten Stand und stellt sicher, dass Mitarbeiter grundlegende Regeln zur Cybersicherheit befolgen? Und waren all diese Datenschutzverletzungen wirklich unbeabsichtigt?

Die geschilderten Beispiele haben eines gemeinsam: Die ehemaligen Mitarbeiter benötigten für das Abgreifen sensibler Daten weniger Zeit als das Unternehmen für die Erkennung und Untersuchung des Vorfalls. In der Tat dauert es nicht lange, Daten von einem Unternehmen zu stehlen – bis Sie einen böswilligen Insider im Netzwerk Ihres Unternehmens entdecken, können hingegen Monate oder gar Jahre vergehen.

Eindämmung des Risikos von Datendiebstahl durch ausscheidende Mitarbeiter

Sie sind nun vielleicht versucht, sofort eines oder mehrere der auf dem Markt erhältlichen Tools zur Erkennung von Bedrohungen zu kaufen. Zunächst sollten Sie sich jedoch ein genaueres Bild davon machen, worauf Sie achten müssen. Im Folgenden finden Sie einige Tipps und Best Practices:

- Gehen Sie nach dem von Gartner entwickelten Konzept CARTA (Continuous Adaptive Risk and Trust Assessment) vor. Wenn Sie die sich stetig ändernde Risikolandschaft kennen und Ihren Mitarbeitern nur so weit vertrauen, wie es zu einem bestimmten Zeitpunkt angemessen ist, können Sie Schäden infolge des Verhaltens Ihrer Benutzer begrenzen.
- Sie sollten sich bewusst sein, dass es keine pauschale Lösung gibt, mit der sich alle Bedrohungen für Ihre Daten abwehren lassen. Vielmehr benötigen Sie verschiedene zuverlässige Lösungen mit jeweils speziellen Funktionen.
- Sie sollten wissen, welche Daten Sie schützen müssen. Machen Sie eine Bestandsaufnahme Ihrer sensiblen Informationen und ihrer Speicherorte, sodass Sie Muster bei den Benutzeraktivitäten im Zusammenhang mit diesen Datenspeichern erkennen und ungewöhnliche Aktionen aufdecken können, die eine Bedrohung darstellen könnten.
- Implementieren Sie unternehmensweite Governance-Richtlinien für die Datensicherheit. Stellen Sie sicher, dass diese auf das Erkennen und Eindämmen von Risiken für die Datensicherheit abzielen, aber auch auf Ihre geschäftlichen Anforderungen abgestimmt sind.

Sobald Sie wissen, welche Schutzmaßnahmen erforderlich sind, benötigen Sie die richtigen Technologien zur Umsetzung Ihrer Strategie. Um Sie bei den ersten Schritten zu unterstützen, haben wir zwei Beispiel-Toolkits – ein grundlegendes und ein erweitertes Toolkit – für Sie zusammengestellt, mit denen Sie Routineaufgaben für die Überwachung und Verwaltung Ihrer IT-Landschaft durchführen sowie potenzielle Bedrohungen (beispielsweise Datendiebstahl durch Mitarbeiter) erkennen und mindern können. Das grundlegende Toolkit beinhaltet Technologien, mit denen Sie das Risiko von Datendiebstahl durch Mitarbeiter ganz einfach eindämmen können:

- Ihre wichtigste Abwehrmaßnahme sind grundlegende Regeln und Richtlinien. Sie können beispielsweise E-Mails isolieren, die an persönliche E-Mail-Konten gesendet wurden, die Nutzung von Speichergeräten wie USB-Sticks verbieten, das Prinzip der geringsten Rechte durchsetzen und alle Änderungen an der Mitgliedschaft in privilegierten Gruppen überwachen.
- Mit einem Prozess für das Widerrufen von Berechtigungen nach Beendigung des Beschäftigungsverhältnisses eines Mitarbeiters nach Best Practices (die natürlich unternehmensweit gewissenhaft befolgt werden sollten) können Sie sicherstellen, dass ausscheidende Mitarbeiter nicht weiterhin Zugriff auf Ihre IT-Infrastruktur haben.
- Um über alle Aktivitäten Ihrer Benutzer auf dem Laufenden zu bleiben, benötigen Sie Auditing-Tools mit Funktionen für die Protokollerfassung und Berichterstattung. Damit können Sie beispielsweise ermitteln, wer welche sensiblen Daten abgerufen hat oder wie oft ein bestimmter Benutzer versucht hat, auf ein freigegebenes Postfach zuzugreifen, und dann die Aktivitäten des Benutzers genauer analysieren. Wenn Sie über ausreichend Budget verfügen, empfiehlt sich der Einsatz einer SIEM-Lösung.
- Integrierte DLP-Lösungen unterstützen Sie dabei, sensible Daten zu ermitteln und sicherzustellen, dass diese das Unternehmen nicht unbemerkt verlassen. Ermöglicht wird dies durch die Sicherung von Web- und E-Mail-Gateways, die Verschlüsselung von E-Mails, die Gewährleistung eines sicheren Cloud-Zugriffs und weitere Sicherheitsvorkehrungen.

Das erweiterte Toolkit richtet sich an erfahrene Sicherheitsexperten, die Funktionen benötigen, die über den Umfang des grundlegenden Tookits hinausgehen:

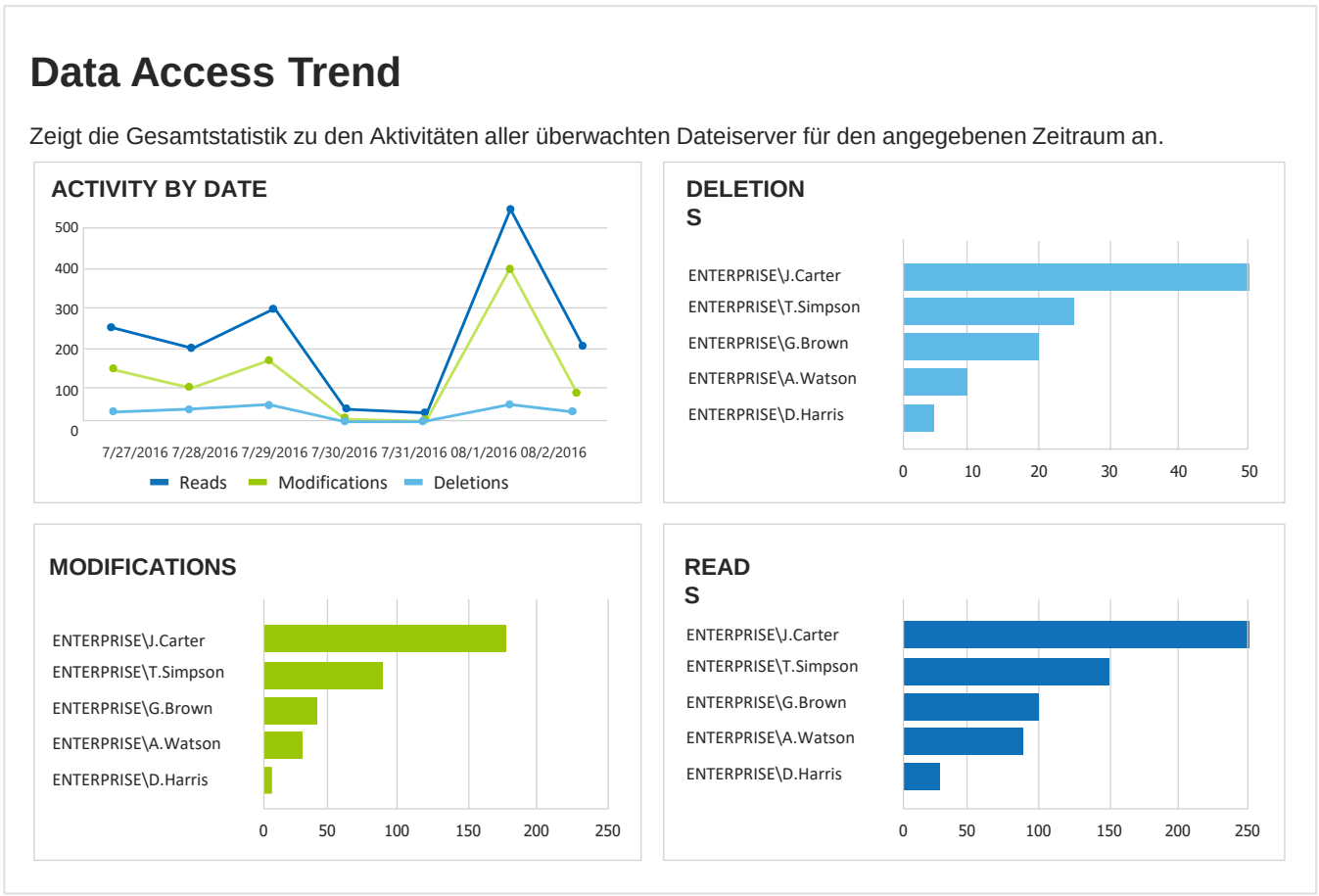
- Mit Technologien für die Identitäts- und Zugriffsverwaltung können Sie die Informationssicherheit verbessern, Workflows optimieren, Fehler vermeiden und die Compliance sicherstellen. Zugleich halten sie Lösungen für die meisten Probleme im Zusammenhang mit der Identitätsverwaltung parat, beispielsweise für kompromittierte Konten sowie Identitäts- und Datendiebstahl.
- Die Verwaltung des privilegierten Zugriffs sorgt dafür, dass Administratoren und andere privilegierte Benutzer nur über die Berechtigungen verfügen, die sie jeweils zur Erledigung ihrer Aufgaben benötigen. Mit den entsprechenden Tools können Sie die Aktivitäten dieser Benutzer überwachen.
- Cloud Access Security Broker (CASB) ermöglichen eine höhere Datensicherheit in der Cloud, indem sie Einblick in die Aktivitäten der Benutzer gewähren und Administratoren über verdächtige Aktionen benachrichtigen, die auf Datendiebstahl durch Insider oder einen externen Angriff hindeuten.
- Mit UEBA- oder SIEM-Lösungen, die Funktionen zur Analyse des Benutzerverhaltens bereitstellen, können Sie verdächtige Benutzeraktivitäten in Ihrer lokalen Umgebung aufdecken und geeignete Maßnahmen zur Risikoeindämmung ergreifen, bevor es zu Datendiebstahl kommt. In hybriden Umgebungen profitieren Sie durch die Kopplung einer UEBA- oder SIEM-Lösung mit einem CASB von umfassender Transparenz auf allen Ebenen.
- Die Überwachung von Mitarbeitern funktioniert ähnlich wie eine Überwachungskamera. Alle Mitarbeiteraktivitäten werden nachverfolgt: die von ihnen abgerufenen Daten, die von ihnen kopierten Dateien, die Empfänger von E-Mails mit kritischen Daten, ihre Gesprächspartner bei Telefonaten usw.
- Mit Lösungen zur Ermittlung und Klassifizierung von Daten können Sie feststellen, welche Daten auf Ihren Systemen gespeichert sind, bestimmen, welche dieser Daten sensibel sind, und analysieren, wie die Daten genutzt werden. So können Sie Risiken wie den Diebstahl von Daten durch Insider mindern.
- Sicherheitsservices wie Penetrationstests können Angreifer simulieren, die Schwachstellen in Ihrer Umgebung ausnutzen, und dann Maßnahmen zur Abwehr dieser Angriffe vorschlagen. Wenn Sie nicht über ein dediziertes Sicherheitsteam verfügen, können Sicherheitsservices von Drittanbietern eine wertvolle Hilfe sein.
- Mit DLP-Lösungen der Enterprise-Klasse können Sie ausgefeiltere Datenschutzverfahren implementieren und das Risiko von Datenverlust auf Ihren Endgeräten minimieren. Die Voraussetzungen dafür schaffen ein zentrales Management, Unterstützung für die Definition erweiterter Richtlinien sowie Workflows und Berichte für die Ereignisverwaltung.
- Die verwendeten Datenschutztechnologien können von einer bestimmten Funktion in einer einzelnen Lösung bis hin zu umfassenden Tools reichen, die Funktionen für Sperrung, Tokenisierung und Datenmaskierung enthalten.

Aufdecken von Datendiebstahlversuchen ausscheidender Mitarbeiter mit Netwrix Auditor

Um das geistige Eigentum, die Finanzdaten, personenbezogenen Informationen und andere wertvolle Daten Ihres Unternehmens vor Diebstahl zu schützen, stellt Netwrix Auditor vordefinierte Berichte und Dashboard-Übersichten bereit. Damit können Sie die erforderlichen Vorkehrungen treffen, damit Mitarbeiter bei ihrem Ausscheiden aus dem Unternehmen keine geschäftskritischen Daten mitnehmen.

1. Überwachen Sie den Datenzugriff

Durch das Identifizieren einer ungewöhnlich hohen Anzahl von Versuchen, Daten zu lesen, zu ändern und zu löschen, können Sie rechtzeitig auf verdächtige Benutzeraktivitäten reagieren und Datenschutzverletzungen vermeiden.



2. Behalten Sie die Aktivitäten Ihrer Benutzer außerhalb der Geschäftszeiten im Blick

Überwachen Sie, welche Benutzer außerhalb der Geschäftszeiten mit Firmendaten arbeiten, und sammeln Sie Beweise für die Untersuchung potenzieller Sicherheitsverletzungen.

Activity Outside Business Hours

Zeigt die Benutzer an, die außerhalb der üblichen Geschäftszeiten Aktionen durchgeführt haben. Mithilfe dieses Berichts können Sie verdächtige Benutzeraktivitäten aufdecken.

User Name	Actions
ENTERPRISE\D.Harris	663
ENTERPRISE\J.Carter	44
ENTERPRISE\T.Simpson	21
ENTERPRISE\A.Watson	15
ENTERPRISE\G.Brown	8

3. Überwachen Sie den Zugriff auf archivierte Daten

Rufen Sie regelmäßig eine Liste aller Benutzer ab, die auf Daten auf Ihren Archivspeichersystemen zugegriffen haben, und überprüfen Sie dabei auch, wann diese Zugriffe erfolgt sind und welche Dateien abgerufen wurden.

Access to Archive Data

Zeigt die Benutzer an, die auf Dateien auf Ihren Archivspeichersystemen zugegriffen haben. Eine hohe Anzahl von Lesezugriffen kann ein Hinweis auf böswillige Aktivitäten sein. Mithilfe dieses Berichts können Sie verdächtige Aktivitäten aufdecken und die Sicherheit Ihrer Daten kontrollieren.

User Name	Reads
PRECINCT34\D.Harris	118
PRECINCT34\G.Brown	5
PRECINCT34\T.Simpson	2
PRECINCT34\J.Carter	1
PRECINCT34\A.Watson	1

4. Decken Sie ungewöhnliche Zugriffe auf sensible Daten auf

Identifizieren Sie Benutzer, die auf Dateien mit sensiblen Informationen zugreifen, die sie normalerweise nicht benötigen. Gewährleisten Sie die Sicherheit Ihrer Daten, indem Sie verdächtige Datennutzungsmuster untersuchen.

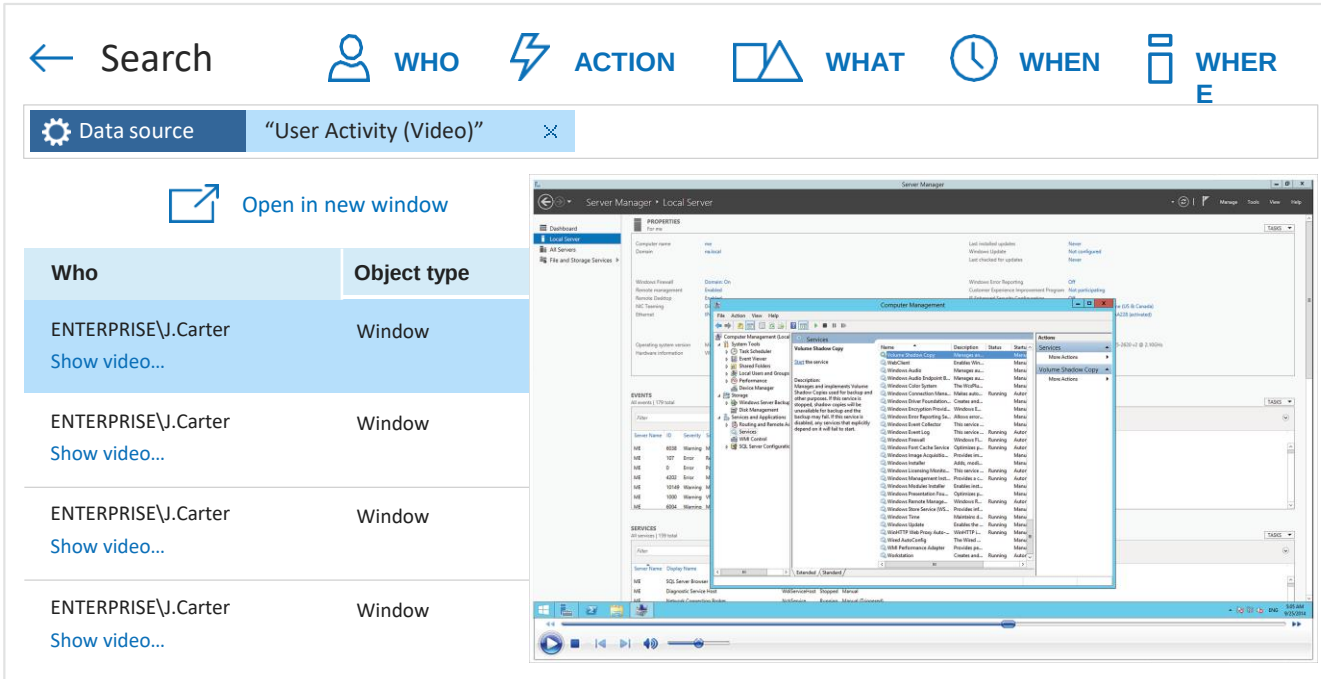
Data Access Surges

Zeigt die Benutzer an, die auf sensible Daten zugegriffen haben, die sie bislang fast noch nie abgerufen haben (der Schwellenwert für Inaktivität ist standardmäßig auf 2 eingestellt). Der Bericht listet zuvor inaktive Benutzer auf, die innerhalb eines kurzen Zeitraums (standardmäßig sieben Tage) mehr Aktionen durchgeführt haben als in einem deutlich längeren Zeitraum davor (standardmäßig 30 Tage).

Path	User Name	Attempts
\\fs1\Office\Finance\Cardholders.xlsx	ENTERPRISE\J.Smith	19
http://spenterprise/Documents/Legal/Social Security Numbers.xlsx	ENTERPRISE\G.Johnson	11
\\emcfs2\Office\Accounting\Budget2016.xlsx	ENTERPRISE\J.Rosenberg	6
\\nf1\Marketing\Backup\Passwords.txt	ENTERPRISE\D.Harris	2

5. Zeichnen Sie die Aktivitäten Ihrer Benutzer auf Video auf

Machen Sie mit Videoaufzeichnungen das Benutzerverhalten sichtbar und decken Sie potenziell schädliche Aktivitäten auf, beispielsweise die unerlaubte Verwendung von USB-Sticks, die Ausführung von nicht genehmigten Anwendungen und andere Ereignisse, die sich nicht protokollieren lassen.



Informationen zu Netwrix

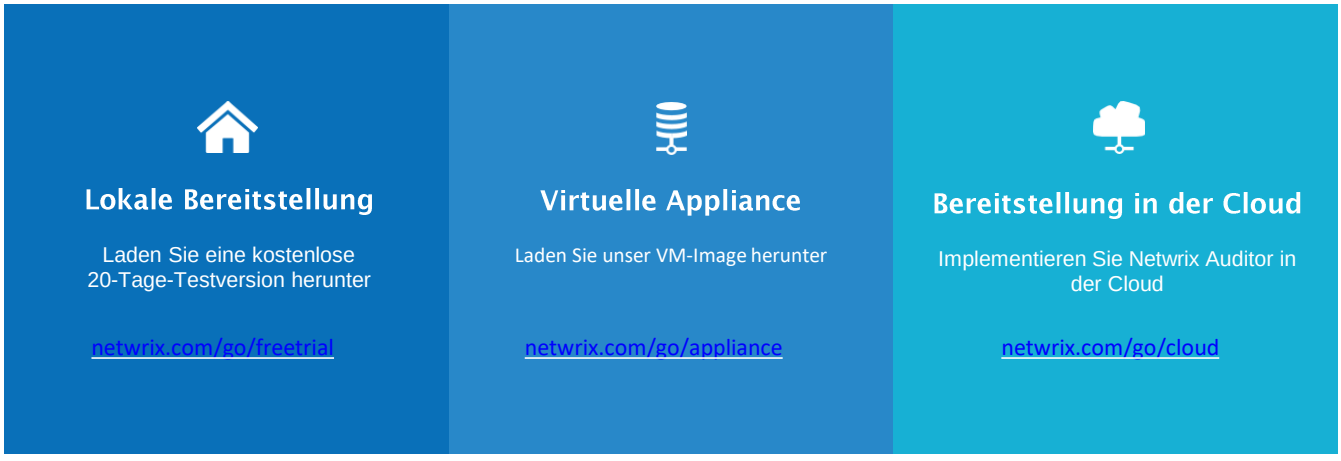
Mit den Lösungen von Netwrix haben Informationssicherheits- und Governance-Verantwortliche umfassende Kontrolle über sensible, regulierte und geschäftskritische Daten – unabhängig davon, wo diese gespeichert sind. Mehr als 10.000 Unternehmen weltweit nutzen die Lösungen von Netwrix, um sensible Daten zu schützen, mit ihren Daten Mehrwert zu schaffen, Compliance-Audits mit geringerem Zeit- und Kostenaufwand erfolgreich zu bestehen und die Produktivität ihrer IT-Teams und Anwender zu steigern.

Netwrix Auditor ist eine Plattform für Transparenz durch Analyse des Benutzerverhaltens und Eindämmung von Risiken, mit der Unternehmen Änderungen, Konfigurationen und Zugriffsrechte in hybriden IT-Umgebungen kontrollieren und Daten unabhängig vom Speicherort schützen können. Sicherheitsanalysen ermöglichen die Erkennung von ungewöhnlichem Benutzerverhalten und die Untersuchung von Bedrohungsmustern, noch bevor es zu Datenschutzverletzungen kommt.

Netwrix Auditor beinhaltet Anwendungen für Active Directory, Azure AD, Exchange, Office 365, Windows-Dateiserver, Dell EMC-Speichergeräte, NetApp Filer-Appliances, SharePoint, Oracle Database, SQL Server, VMware und Windows Server. Auf der Grundlage einer RESTful API und der Videoaufzeichnung von Benutzeraktivitäten bietet die Plattform einheitliche Transparenz und Kontrolle für sämtliche lokalen und cloudbasierten IT-Systeme.

Mehr als 160.000 IT-Abteilungen auf der ganzen Welt setzen auf Netwrix Auditor, um Insider-Bedrohungen in lokalen und Cloud-Infrastrukturen zu erkennen, Compliance-Audits ohne hohen Kostenaufwand zu bestehen und die Produktivität ihrer für IT-Sicherheit und IT-Betrieb zuständigen Teams zu steigern.

Weitere Informationen finden Sie unter www.netwrix.de.



Firmenzentrale:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618, USA
Hotline: DE: +49 711 899 89 187, **CH:** +41 43 508 34 72, **AT:** +43 72 077 58 72

netwrix.com/social