ipswitch

Secure. Control. Perform.

EIN EBOOK VON IPSWITCH

Insider-Bedrohungen und deren Auswirkung auf Ihr Unternehmen

Einführung

Unternehmen sind sich weltweit nur allzu gut der mit Sicherheitslücken verbundenen Folgen bewusst. Vertrauliche Daten, die in falsche Hände gelangen, werden leicht zu Identitätsdiebstählen genutzt oder manipuliert und auf dem Schwarzmarkt verkauft. Um Sicherheitslücken zu vermeiden, treffen Unternehmen in der Regel Sicherheitsvorkehrungen, die verhindern sollen, dass Hacker und andere externe Bedrohungen in ihr Netzwerk eindringen und sich Zugriff zu diesen Daten verschaffen. Obgleich dies ein guter Ansatz ist, übersehen sie dabei häufig die Gefahren, die von Datendiebstählen durch Insider ausgehen.

Insiderbedrohungen entstehen, wenn sich vertrauensvolle Insider (aktuelle oder ehemalige Mitarbeiter, Auftragnehmer oder Geschäftspartner) mit offizieller Zugriffserlaubnis für sensible Unternehmensdaten unwissentlich oder absichtlich an Aktivitäten beteiligen, die den Schutz und die Sicherheit dieser Informationen gefährden.

Laut dem jüngsten Clearswift Insider Threat Index-Bericht (CITI) haben 74 % der Sicherheitslücken ihren Ursprung im erweiterten globalen Unternehmen.

In einer eingehenderen Analyse gaben 72 % der befragten globalen Sicherheitsexperten an, dass ihr Unternehmensvorstand ihrer Meinung nach internen Sicherheitsbedrohungen nicht dieselbe Bedeutung wie externen Bedrohungen beimisst. Diese Statistiken sind alarmierend. Die nachfolgende Abbildung zeigt die gängigsten internen Sicherheitsbedrohungen, denen Unternehmen heute gegenüberstehen.

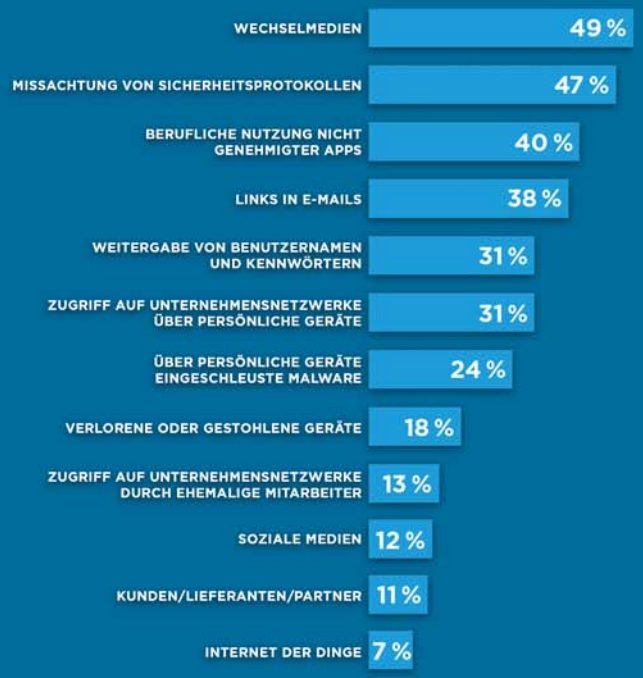


Abbildung 1: Größte interne Sicherheitsbedrohungen für Unternehmen
Quelle: 2015 Clearswift Insider Threat Index

Abbildung 2: Mr. Robot
Quelle: USA Networks (http://www.usanetwork.com/mrrobot)

MR. ROBOT

Kennen Sie Mr. Robot auf USA Networks? Mr. Robot steht für den Inbegriff einer Insiderbedrohung in Elliot Aldreson.

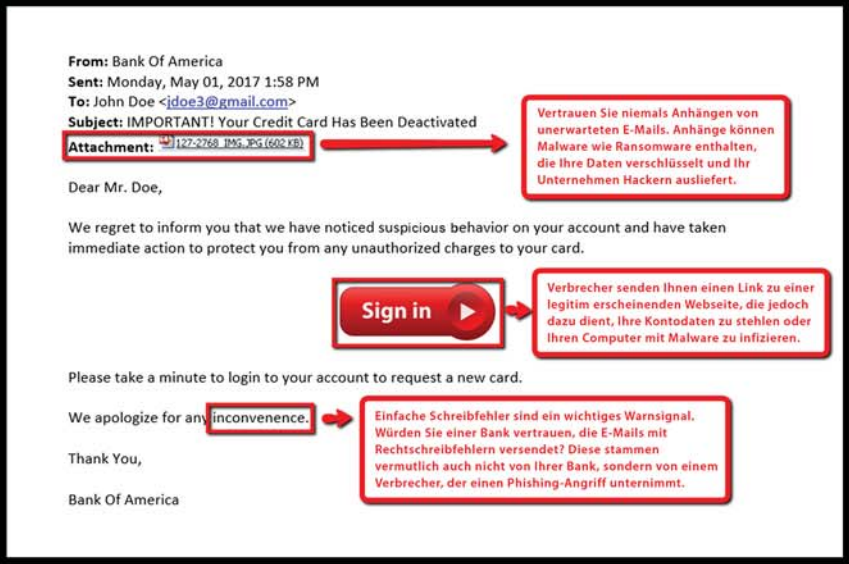
Elliot wird von einer anonymen Gruppe von Hacktivisten rekrutiert, deren Anführer ein Mann namens „Mr. Robot“ ist.

Tagsüber arbeitet Elliot als Sicherheitstechniker des Cybersicherheitsunternehmens Allsafe. Elliot nutzt sein Insiderwissen des Unternehmens, um seine Freunde, die Hacktivisten, bei Cyberverbrechen in seinem Unternehmen zu unterstützen. Sie verwenden die Informationen, um Kundendaten zu stehlen und Unternehmensgeheimnisse offenzulegen.

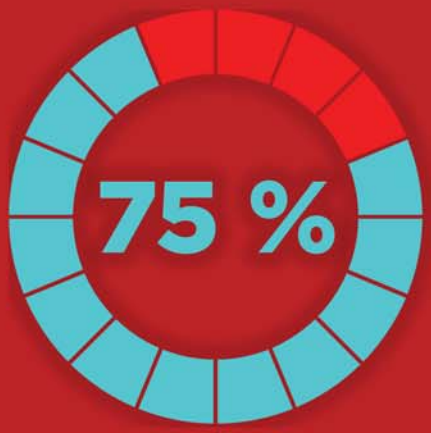
Während Mr. Robot natürlich ein extremes Beispiel einer Insiderbedrohung ist, veranschaulicht die Serie dennoch sehr echte Sicherheitslücken in heutigen Unternehmensnetzwerken. Obgleich zahlreiche interne Sicherheitslücken durch bösartige Insider verursacht werden, entstehen die meisten Insiderbedrohungen tatsächlich unbeabsichtigt durch Mitarbeiter, die vertraulich Informationen ungewollt offenlegen. Unbeabsichtigte Insiderbedrohungen resultieren in der Regel aus mangelhaften Sicherheitspraktiken wie etwa unbeaufsichtigten IT-Systemen oder der Missachtung von Sicherheitsprotokollen etwa durch die Weitergabe von Systemkennwörtern an Kollegen. Diese Bedrohungen lassen sich durch die Implementierung robuster Sicherheitsstandards und -protokolle einfach vermeiden.

Klar ist, dass IT-Teams bestehende Datenschutzstandards erweitern sollten, um sowohl externe als auch interne Sicherheitsbedrohungen abzuwehren und die Datenintegrität eines Unternehmens bestmöglich zu schützen. Die nachfolgenden Beispiele zeigen gängige Sicherheitsbedrohungen, auf die IT-Teams achten sollten.

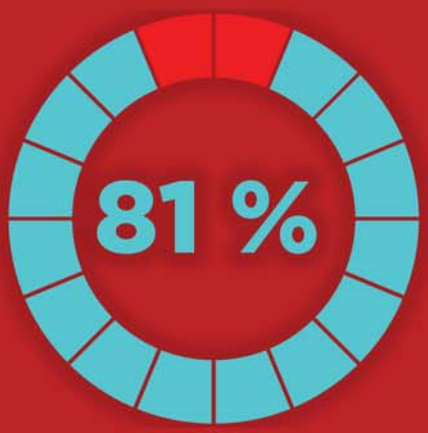
Notizen mit Anmeldeinformationen stellen ganz offensichtlich ein Problem dar. Für Verbrecher ist es ein Leichtes, diese zu fotografieren oder sich einfach so zu merken. Auffällig ist auch die schwache Kennwortwahl.



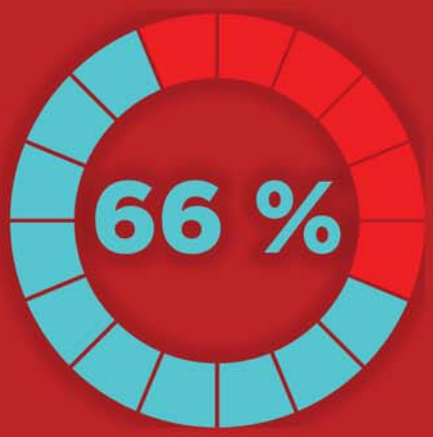
E-Mails sind kein sicheres Medium. Sorgen Sie dafür, dass Ihre Benutzer die neusten Phishing-Scams kennen. Schulungen sind mitunter die beste Abwehrmaßnahme gegenüber potenziellen Angriffen.



75 % der Sicherheitslücken entstehen durch externe Akteure und 25 % interne Benutzer.



81 % der Hackerangriffe erfolgen aufgrund von schwachen Kennwörtern.



66 % der Malware wird über schädliche E-Mail-Anhänge installiert.

Abbildung 3: 2017 Data Breach Investigation Report: 10. Auflage
Quelle: Verizon Enterprise (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)

Die meisten externen Angriffe resultieren aus internen Bedrohungen

Wie an den obigen Angaben zu erkennen ist, entstehen die meisten Sicherheitslücken durch externe Akteure. Warum sind also die internen Bedrohungen am auffälligsten? Um dies zu verstehen, muss der Bezug verdeutlicht werden.

Obgleich die meisten Sicherheitslücken durch externe Hacker entstehen, sind es die Mitarbeiter eines Unternehmens, die Verbrechern unbeabsichtigt den Zugang zum Netzwerk ermöglichen. Schwache Kennwörter und schädliche E-Mails sind die Hauptvektoren externer Angriffe. Aber nur, wenn Ihre Benutzer empfänglich dafür sind. In diesen Fällen sind Ihre Benutzer die Bedrohung.

E-Mails stellen aber nicht nur aufgrund von schädlichen E-Mail-Anhängen eine Gefahr dar. Auch wenn sie auf Ihrem Server möglicherweise verschlüsselt werden, können Dritte diese E-Mails nach dem Verlassen Ihres Unternehmensnetzwerks abfangen. Dies ist ein weiterer Vektor für Datenverluste.

E-Mail ist nicht Ihr Verbündeter

Die US-Wahlen 2016 sind uns allen noch in Erinnerung. Schlagzeilen machte dabei unter anderem Hillary Clintons privater E-Mail-Server, den sie zum Senden und Empfangen klassifizierter Informationen nutzte.

Ungeachtet von Politik und Spionage besteht das größte Problem hinsichtlich E-Mails darin, dass diese ohne das Wissen des Senders oder Empfängers von Dritten abgefangen werden können. Dies geschah auch mit Hillarys Clintons E-Mails. Selbst der sicherste E-Mail-Server der Welt nützt Ihnen nichts, sobald vertrauliche Daten Ihre durch Firewalls geschützte Unternehmensumgebung verlassen. Wenn der Empfänger es mit der Sicherheit nicht so ernst nimmt, wie Sie, ist der zuverlässige Schutz Ihrer E-Mails nicht mehr gegeben.

Minimieren von Insiderbedrohungen bei Datenübertragungen außerhalb der Firewall

In den heutigen „grenzenlosen“ Unternehmen müssen vertrauliche Informationen sicher und auf regulärer Basis mit Dritten austauschbar sein. Sobald sich vertrauliche Daten außerhalb der Firewall eines Unternehmens befinden, können sie abgefangen oder gestohlen werden. Eine sichere und zuverlässige verwaltete Datenübertragungslösung (Managed File Transfer, MFT) stellt mitunter eine außerordentlich wertvolle Investition dar, um die rechtzeitige Übertragung an autorisierte Empfänger sicherzustellen. Gleichzeitig bietet es dem IT-Team die Möglichkeit, sämtliche Dateiübertragungsaktivitäten zu überwachen und zu erfassen.

Kontozugriff

Der unzulässige Zugriff auf vertrauliche Daten stellt eindeutig eine Sicherheitslücke für die Informationen in Ihrem Netzwerk dar. Sie können den Zugriff von Benutzern auf ein System auf einfache und konsistente Weise steuern, indem Sie in die Active Directory (AD)-Datenbank Zugriffsberechtigungen für Konten integrieren. Dem IT-Team ermöglicht dies die Steuerung und Überwachung der Zugriffsrechte von Mitarbeitern auf Systeme mit vertraulichen Informationen. Wenn verdächtige Verhaltensweisen festgestellt werden oder Mitarbeiter aus dem Unternehmen ausscheiden, lässt sich der Zugriff auf Benutzerkonten zudem schnell deaktivieren oder beschränken.

Warnungen, Dashboards und Berichte

Bei verwalteten Dateiübertragungssystemen ist ausschlaggebend, dass sich damit sämtliche Dateiübertragungsaktivitäten protokollieren und Alarme auslösen lassen, um die IT frühzeitig bezüglich schädlicher Verhaltensweisen von Benutzern zu warnen. Durch die Steuerung und Transparenz von Kontozugriffen und Dateiübertragungen lassen sich potenzielle Schäden infolge von Insiderbedrohungen minimieren. Gesicherte Prüfprotokolle gewährleisten, dass die Ereignisse auch bei einem erfolgreichen Angriff aufgezeichnet und zum Verursacher zurückverfolgt werden können.

Integration in Virenschutzsoftware

Angreifer infiltrieren ein System gerne, indem sie Malware in das Unternehmensnetzwerk einschleusen. Sobald ein Softwarevirus freigesetzt ist, kann er umfangreichen Schaden anrichten und Ihre vertraulichsten Daten offenlegen, bevor es der IT möglich ist, die Situation unter Kontrolle zu bringen. IT-Teams benötigen eine Virenschutzsoftware, die stets auf dem neuesten Stand ist, um die Gefahr derartiger Angriffe zu minimieren. Indem Sie sicherstellen, dass sich Ihr verwaltetes Dateiübertragungssystem in die Virenschutzsoftware Ihres Netzwerks integrieren lässt, können Sie verhindern, dass in Ihr Netzwerk eingeschleuste Malware Ihre FTP-Server und die darauf gespeicherten Daten infiziert.

Datenverschlüsselung

Die Datenverschlüsselung spielt bei der Übertragung von Daten aus einem Unternehmen eine äußerst wichtige Rolle. Auch wenn die IT den Zugriff autorisierter Benutzer auf Datenbanken mit vertraulichen Informationen beschränken kann, ist es ebenso wichtig, dass außerhalb des Unternehmens weitergeleitete Daten weder gelesen noch modifiziert werden können. Dieser Prozess kann auch durch Insider gefährdet werden, die versuchen, geschützte Informationen böswillig abzufangen oder zu missbrauchen, was sicherheitstechnisch jedoch häufig übersehen wird. IT-Teams sollten unbedingt über einen verwalteten Dateiübertragungs-Workflow verfügen, der sicherstellt, dass Daten sowohl während der Speicherung als auch der Übertragung verschlüsselt sind. Die Datenverschlüsselung verhindert den Missbrauch wichtiger Daten durch nicht autorisierte Benutzer, selbst wenn sich diese Zugriff auf den zugrundeliegenden Dateispeicher verschaffen. Darüber hinaus stellt sie die konsequente Integrität der Daten sicher.

Mehrstufige Authentifizierung

Die mehrstufige bzw. Multi-Faktor-Authentifizierung (MFA) bietet eine weitere hervorragende Sicherheitsebene, die dazu beitragen kann, dass nur autorisierte Benutzer Zugriff auf vertrauliche Informationen erhalten. MFA ist ein mehrstufiger Überprüfungsprozess, der die Identität der Benutzer sicherstellt, indem er während ihrer Anmeldung bei einem Systemkonto einen zusätzlichen Nachweis in Form eines Sicherheitscodes fordert. Der Sicherheitscode wird an eine alternative Quelle (Telefon, E-Mail usw.) übermittelt, die direkt mit dem Benutzer verknüpft ist. Diese zusätzliche Sicherheitsschicht verhindert, dass Mitarbeiter Kennwörter von Kollegen nutzen oder nicht autorisierte Benutzer mit gestohlenen Anmeldeinformationen Zugriff auf vertrauliche Daten erlangen.

Cloud-Dienste

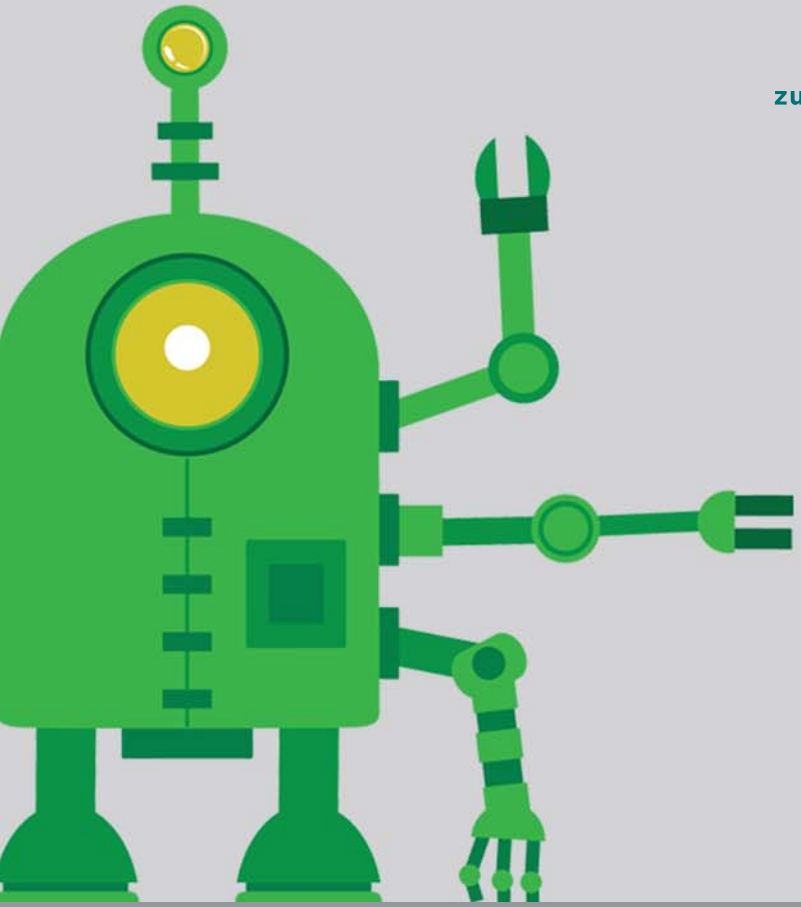
Mittlerweile werden immer mehr Anwendungen über die Cloud angeboten. Ein wesentlicher Vorteil der Implementierung einer Cloud-basierten SaaS-Lösung für Ihre Dateiübertragungsaktivitäten ist die zuverlässige Aktualität Ihrer Softwareprotokolle. Cloud-basierte SaaS-Lösung verkleinern das Angriffsfenster, über das sich Insider Zugriff auf vertrauliche Daten verschaffen können. Bei einer lokalen Implementierung besteht zwischen der Bereitstellung von Softwareaktualisierungen bzw. Patches und der tatsächlichen Planung und Anwendung innerhalb des Netzwerks durch die IT eine erhebliche zeitliche Sicherheitslücke.

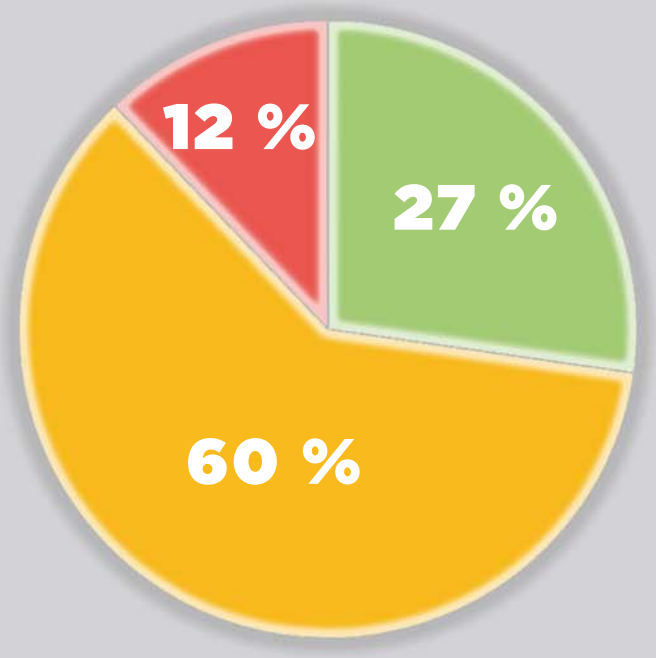
Automatisierung

Die Automatisierung bietet eine Datenübertragungsmethode ohne Benutzereingriffe, die verhindert, dass vertrauliche Dateien aufgrund von (absichtlichen oder unwissentlichen) Skriptfehlern in die falschen Hände gelangen. Ein robustes Automatisierungssystem ermöglicht es der IT, Dateiübertragungs-aktivitäten zu verwalten und zu verfolgen und bestimmte Übertragungen aufgrund von verdächtigen Aktivitäten schnell zu deaktivieren bzw. zu stoppen.

Abbildung 4: Intelligente Systeme in Aktion
Quelle: Ipswitch (www.ipswitch.de)

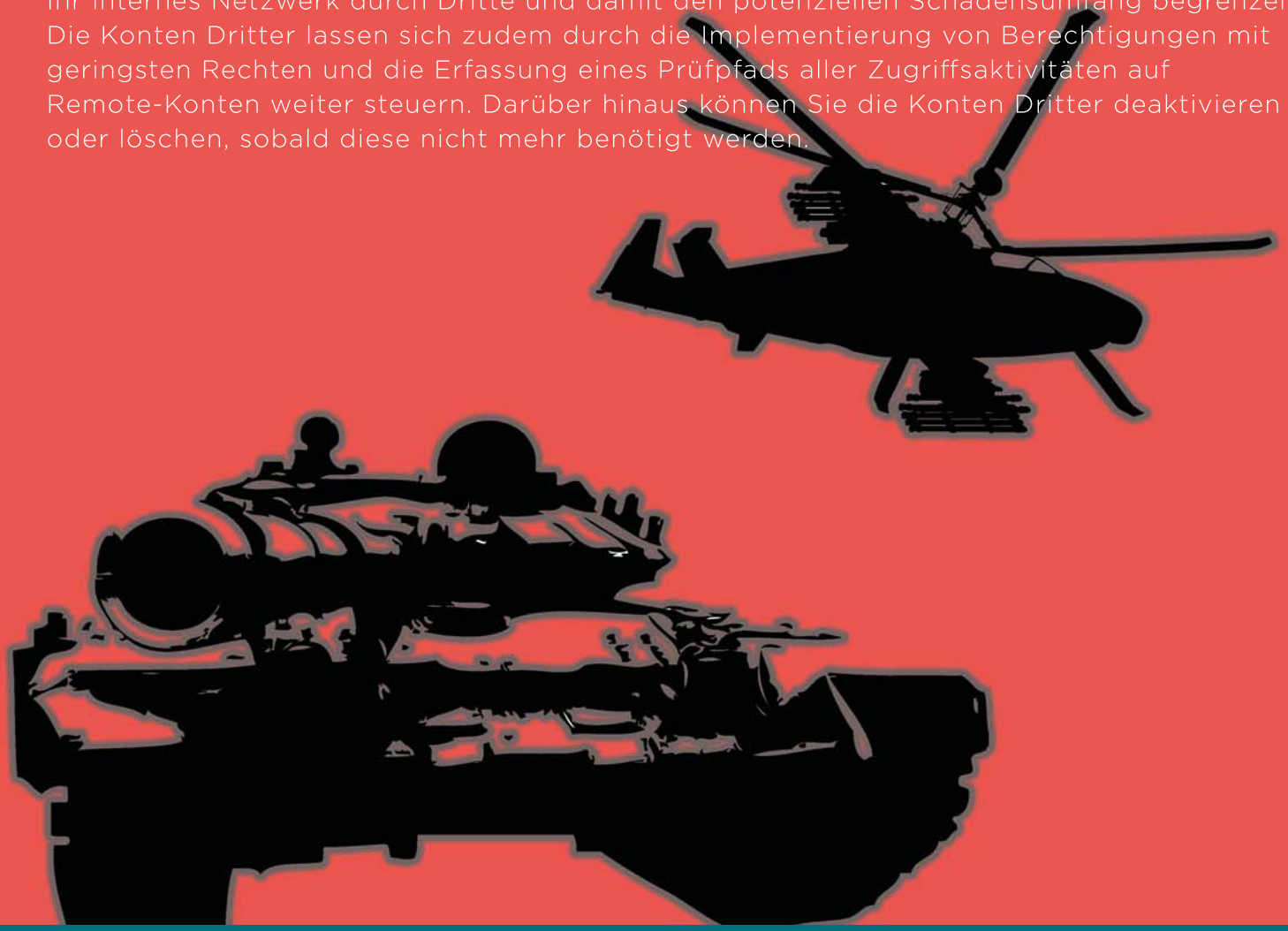
Wie schätzen Sie aktuell Ihre Verwaltungs- und Automatisierungsfähigkeiten für eine sichere Dateiübertragung ein?





Kontozugriff durch Dritte

Insiderbedrohungen beschränken sich nicht nur auf Mitarbeiter und Auftragnehmer. Unternehmen entwickeln heute häufig enge Beziehungen zu Drittanbietern und Partnern, denen sie privilegierten Zugriff auf Netzwerkbereiche gewähren. Wenn dieser Zugriff unter anderem dem Informationsaustausch dient, kann die Gefahr durch Insiderbedrohungen eingeschränkt werden. Die Implementierung eines verwalteten Dateiübertragungsservers, der sich außerhalb Ihrer Firewall in der DMZ befindet, können Sie den direkten Zugriff auf Ihr internes Netzwerk durch Dritte und damit den potenziellen Schadensumfang begrenzen. Die Konten Dritter lassen sich zudem durch die Implementierung von Berechtigungen mit geringsten Rechten und die Erfassung eines Prüfpfads aller Zugriffsaktivitäten auf Remote-Konten weiter steuern. Darüber hinaus können Sie die Konten Dritter deaktivieren oder löschen, sobald diese nicht mehr benötigt werden.



Erfahren Sie mehr über die verwaltete Dateiübertragung mit MOVEit:

www.ipswitch.de

ipswitch