ipswitch

Secure. Control. Perform.

EIN WHITEPAPER VON IPSWITCH

Überlegungen zum Thema Sicherheit und Compliance für Banken und Finanzdienstleister

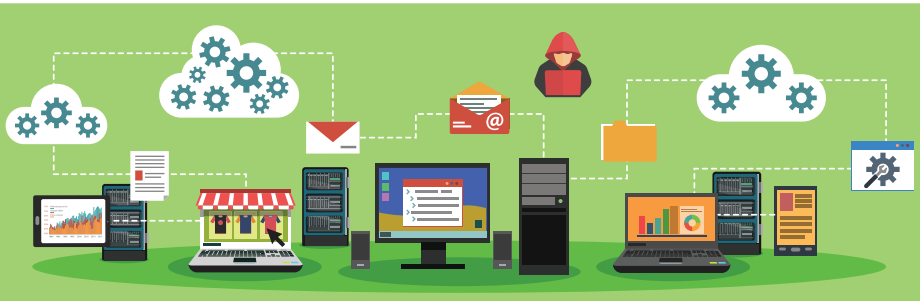
ipswitch

Einführung

In einer Zeit, in der Cyberkriminelle und Nationalstaaten gleichermaßen nach Schwachstellen in den Sicherheitssystemen von Unternehmen suchen, werden Datenschutzvorkehrungen zu einer zwingenden Notwendigkeit. Der Großteil der Daten, die Banken und Finanzdienstleister erfassen und speichern, erzielen auf dem Schwarzmarkt Höchstpreise. Das macht Ihr Unternehmen zu einem beliebten Ziel für Cyberangriffe.

Deshalb muss Ihr Unternehmen Richtlinien und Technologielösungen implementieren, die vertrauliche Finanzinformationen ebenso wie personenbezogene Daten von Kunden und Mitarbeitern schützen. Daten wie Sozialversicherungsnummern, Kontodaten, Adressen, Kreditinformationen und Kartennummern sind vertraulich und werden durch eine Reihe von Datenschutzbestimmungen geschützt. Das Fehlen von entsprechenden Sicherheitskontrollen, die eine Einhaltung von regionalen oder nationalen Bestimmungen (oder Branchenstandards) gewährleisten, kann für Finanzinstitutionen nicht nur erhebliche Geldbußen nach sich ziehen, sondern auch das Ansehen des Unternehmens beeinträchtigen.

Große Teile der Daten, mit denen Ihr Unternehmen jeden Tag arbeitet, werden gegebenenfalls auch in Bereiche übertragen, die sich außerhalb Ihres gesicherten Netzwerks befinden. Aktuelle Geschäftsmodelle sehen vielfach vor, dass Daten regelmäßig an externe Dienstleister übermittelt werden, die zentrale Aspekte der Finanzdienstleistungen bereitstellen, die Sie Ihren Kunden anbieten. Während dieser Informationsaustausch Ihrem Unternehmen ermöglicht, ein umfangreicheres Dienstleistungsangebot bereitzustellen und neue Wachstumschancen zu nutzen, macht er es auch anfällig für Sicherheitslücken und den Diebstahl, Verlust oder Missbrauch von Daten.



Außerhalb der Firewall steigt für vertrauliche Daten das Risiko eines möglichen Diebstahls oder Missbrauchs.

ipswitch

Um die nationale Wirtschaft zu schützen, haben Regierungen auf der ganzen Welt Gesetze erlassen, die die Sicherheit von Finanzinformationen kontrollieren. Angesichts von 6 Milliarden gestohlenen Datensätzen weltweit allein in den letzten drei Jahren wurden zudem immer striktere Regulierungen in Bezug auf die Erfassung, Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten eingeführt.

Banken, die in den USA tätig sind, müssen zahlreiche Richtlinien beachten, die Datenschutzbestimmungen oder -vorkehrungen beinhalten. Der Gramm-Leach-Bliley Act (GLB) reguliert die Erfassung und Offenlegung der persönlichen Finanzdaten von Kunden und verpflichtet Finanzinstitute zur Entwicklung, Implementierung und Verwaltung von Schutzvorrichtungen zum Schutz dieser Informationen. Für Börsenunternehmen verlangt der Sarbanes-Oxley Act eine Prüfbarkeit interner Kontrollen und Prozesse sowie die Vorhaltung von detaillierten Prüfprotokollen aller Zugriffe und Aktivitäten im Zusammenhang mit vertraulichen Geschäftsinformationen.

Weltweit müssen Finanzdienstleister, die Zahlungsinformationen mit den Logos von beispielsweise Visa, Mastercard, American Express oder Discover erfassen oder speichern, außerdem den Payment Card Industry Data Security Standard (PCI DSS) einhalten. Mehr als 32 Länder auf der ganzen Welt haben ein Datenschutzgesetz wie das Bundesdatenschutzgesetz (BDSG) erlassen, das die Sicherheit von personenbezogenen Daten regelt.

In den USA und anderen Ländern müssen Banken und Finanzdienstleister außerdem staatliche und regionale Richtlinien einhalten. Jedes Unternehmen, das personenbezogene Daten von Einwohnern der Europäischen Union erfasst, speichert oder übermittelt ist zudem an die Europäische Datenschutzgrundverordnung gebunden.

Viele dieser Regulierungen beinhalten zentrale Bestimmungen, die fordern, dass vertrauliche Daten nicht nur von den Institutionen geschützt werden, die diese erfassen und speichern, sondern auch von externen Parteien, die diese Informationen erhalten oder verarbeiten. Das bedeutet, dass das Lieferanten- und Partnermanagement ein wichtiger Bestandteil Ihrer Compliance-Strategie sein muss. Eine umfassende Risikobeurteilung erfordert, dass Sie den Sicherheits- und Compliance-Status Ihrer Lieferanten und Partner ebenso gut kennen müssen, wie Ihren eigenen.

Entscheidend ist, dass die Nichteinhaltung dieser Richtlinien und Gesetze mit erheblichen Geldstrafen geahndet werden kann.

Finanzdienstleister sollten der Nutzung ungesicherter File-Sharing-Technologien wie z. B. unverschlüsselte FTP-, E-Mail- und herkömmliche Cloud-Dienste durch Mitarbeiter und externe Partner besondere Aufmerksamkeit schenken.

ipswitch

Gewährleisten von Data Governance

In einem kürzlichen E-Mail-Spoofing-Angriff wurden Mitarbeiter eines nicht genannten Unternehmens gebeten, mit ihrem EFSS-Benutzernamen und -Kennwort zu antworten – **60 % sind dieser Bitte nachgekommen.**

Unternehmen, die auf Methoden wie z. B. Enterprise File Sync & Share (EFSS) und E-Mail setzen, um Daten mit Partnern, Niederlassungen und Kunden auszutauschen, verstoßen dabei möglicherweise konkret gegen Datenschutzbestimmungen. Diese Methoden sind zwar praktisch, doch fehlen ihnen üblicherweise die für eine Einhaltung der gesetzlichen Auflagen notwendigen Funktionen wie Verschlüsselung, Zugriffskontrolle und Prüfpfade. Unternehmen sollten sich außerdem bewusst sein, dass sie bei einem Missbrauch oder Datendiebstahl auch dann nicht aus der Verantwortung genommen sind, wenn ein Anbieter eines cloudbasierten Services behauptet, das angebotene Produkt oder der Service würden bestimmten Datenschutzbestimmungen entsprechen.

Viele nutzen mehrere FTP-Server und plattformabhängige Automatisierungsskripte für die Verwaltung von Dateiübertragungen. Je mehr unterschiedliche Systeme Sie für die Übertragung von Dateien nutzen, desto höher ist das Risiko von Angriffen. Die Reduzierung von möglichen Angriffspunkten und die Vereinfachung der Prüfprozesse zählen zu den wichtigsten Gründen für eine Konsolidierung verschiedener Systeme in einem Dateiübertragungssystem.

Richtlinien und Gesetze zum Datenschutz verlangen üblicherweise strenge Zugriffskontrollen, eine Datenverschlüsselung bei der Übertragung und Speicherung sowie protokollbasierte Prüfpfade. Interne Sicherheitskontrollen sollten außerdem Anforderungen für standardisierte Workflows beinhalten, um den Schutz der Daten zu gewährleisten. Um eine Einhaltung der gesetzlichen Auflagen sicherzustellen, sollten Banken nicht kontrollierte Datenübertragungsmethoden durch sichere, verlässliche und gesetzeskonforme Prozesse für den Informationsaustausch ersetzen, die Datensicherheit und -integrität gewährleisten.

Zwei verbreitete Sicherheitsprotokolle, die für eine sicherere und verlässlichere Datenübertragung sorgen, sind Secure Sockets Layer (SSL) und Secure Shell (SSH). Beide wurden gezielt für die Verschlüsselung von Dateiübertragungen und der zugehörigen Authentifizierungsdaten entwickelt. SSL und SSH verbessern mithilfe einer Verschlüsselung, die hochgradig gefährdete Daten bei der Übertragung in offenen Netzwerken wie dem Internet vor nicht autorisiertem Zugriff und Modifikationen schützt, die Sicherheit und Verlässlichkeit der Dateiübertragung.

Daten sollten außerdem sowohl bei der Übertragung als auch bei der Speicherung (z. B. in einem zeitweiligen Speicher, bevor sie vom Empfänger geöffnet oder heruntergeladen werden) geschützt werden. Finanzinstitute sollten für die Speicherung und Übertragung von Daten die stärkste im Handel erhältliche Verschlüsselungstechnologie einsetzen. Eine Kombination von SSL und SSH mit OpenPGP bietet eine zusätzliche Sicherheitsstufe für gespeicherte Daten. OpenPGP verschlüsselt gespeicherte Dateien mithilfe von kryptografischen Schlüsselpaaren, die Benutzer und Daten authentifizieren. Empfänger müssen einen zugehörigen privaten Schlüssel verwenden, um eine Datei zu entschlüsseln.

ipswitch

Sichere verwaltete Dateiübertragung

Systeme für eine sichere verwaltete Dateiübertragung ermöglichen externe Dateiübertragungen auf sichere, präzise, kontrollierte und dokumentierte Art und Weise und decken damit das volle Spektrum aktueller und in der Entwicklung befindlicher rechtlicher Bestimmungen und Richtlinien ab. Solche Systeme ermöglichen Finanzinstituten das Versenden von Daten mit Empfangsbestätigungen und umfangreiche Nachverfolgungs- und Auditing-Funktionen, um die Einhaltung von Datenschutzbestimmungen wie GLB, PCI DSS, SOX, der EU-Datenschutzgrundverordnung und anderer nationaler und regionaler Auflagen zu gewährleisten.

Beim Vergleich von Systemen für eine sichere verwaltete Dateiübertragung mit möglichen Alternativen sollten Sie darauf achten, wie diese Anwendungen die Compliance von Funktionen in den folgenden vier Kategorien sicherstellen: ***Vertraulichkeit, Integrität, Verfügbarkeit und Prüffähigkeit***.

1

Die ***Vertraulichkeit*** sorgt dafür, dass Informationen ausschließlich von autorisierten Personen und nur für genehmigte Zwecke genutzt werden. Die Vertraulichkeit beginnt bei der Authentifizierung von Anmeldeinformationen und einer strengen Kennwortrichtlinie mit Funktionen wie zeitlich beschränkten Konten und einer Kennwortverwaltung. Die Zugriffskontrolle stellt sicher, dass eine SSL-Verschlüsselung mit 256-Bit AES und TLS für alle Verbindungen erforderlich ist. Diese Zugriffsanforderungen sollten für alle Clients, die sich mit Ihrer Netzwerkinfrastruktur verbinden, vorgeschrieben sein.

2

Integrität bedeutet, dass Sie dank umfassender SHA-Unterstützung eine zuverlässige Zustellung aller korrekten Daten gewährleisten können. Eine sichere, verschlüsselte Zustellung der Daten ist eine wichtige Voraussetzung für die Business Continuity. Sichere Hash-Algorithmen sorgen dafür, dass Dateien während der Übertragung nicht manipuliert wurden und dass die Ausgangs- und Zieldateien genau übereinstimmen. Die Nicht-Zurückweisung bietet durch die Verwaltung von digitalen Zertifikaten zur Sicherung der Übertragung und Datenverschlüsselung die höchste derzeit verfügbare Datensicherheitsstufe.

3

Die ***Verfügbarkeit*** wird durch Lastenausgleich und Architektur-Cluster erreicht, die automatisches Failover und eine zentralisierte Speicherung von Konfigurationsdaten unterstützen, um das Risiko von Sicherheitslücken zu minimieren. Dies bietet auch Schutz vor Distributed-Denial-of-Service-Angriffen. Eine hohe Verfügbarkeit kann auch durch die Integration von automatischen Neustartfunktionen am Kontrollpunkt und Systemrobustheit erreicht werden, die helfen, Hardwareausfälle oder Unterbrechungen der Internetkonnektivität zu überwinden.

4

Die ***Prüffähigkeit*** bezieht sich auf umfassende Protokollierungsfunktionen und eine Protokollanzeige mit Manipulationsschutz zur Sicherung der Integrität von Protokolldateien. Für Technologie-, Sicherheits- und andere Prüfzwecke sollten alle Interaktionen zwischen Client und Server sowie alle administrativen Vorgänge protokolliert werden.

ipswitch

Compliance-Funktionen von Ipswitch® MOVEit

MOVEit® ist ein System für die sichere verwaltete Dateiübertragung, mit dem Sie den Austausch vertraulicher Daten mit externen Parteien verwalten, anzeigen, sichern und kontrollieren können, um Compliance mit Datenschutzverordnungen sicherzustellen. In der Tabelle unten wird gezeigt, wie MOVEit die sieben zentralen Best Practices für Compliance mit Datenschutzverordnungen angeht.

Sicherheitsanforderung	MOVEit-Kontrolle
Compliance	MOVEit sorgt dafür, dass Dateiübertragungen gesichert, Daten jederzeit geschützt und Aufzeichnungen über Übertragungen in manipulationssicheren Prüfpfaden über einen gesetzlich vorgeschrieben Zeitraum hinweg gesichert sind, bevor sie garantiert vernichtet werden.
Kommunikationssicherheit	MOVEit ermöglicht zentrale Transparenz, Kontrolle und vorherige Autorisierung aller Dateiübertragungen sowie Verschlüsselung, Nachverfolgbarkeit und Nicht-Zurückweisung von Übertragungen einschließlich sicherer Prüfpfade für wichtige Ereignisse. Die MOVEit-Lösung ist so gestaltet, dass sie in bereits bestehende Sicherheitsinfrastrukturen, -richtlinien und -anwendungen integriert werden kann. Dadurch wird sichergestellt, dass sich keine unverschlüsselten Daten in der DMZ befinden, und Anforderungen für externen Zugriff werden eliminiert.
Informationssicherheitsrichtlinien	MOVEit verschlüsselt Dateien am Speicherort und während der Übertragung, bietet Nicht-Zurückweisung und Dateiintegritätsprüfungen. Ipswitch stellt E-Mail-, Web-, Mobilzugriff- und Desktop-Clients bereit, die bei Verwendung in Kombination mit MOVEit allen Benutzern vorschriftsgemäßen Dateiübertragungszugriff bieten.
Zugriffskontrolle	MOVEit bietet eine Auswahl an Authentifizierungsmechanismen, einschließlich Integration in bereits vorhandene Systeme, und umfangreiche Funktionen zur Unterstützung des Benutzerzugriffsmanagements, einschließlich Blacklists und Whitelists, sowie Tools, die Administratoren dabei helfen, die für die Einhaltung ihrer Sicherheitsrichtlinien geeignetsten Einstellungen auszuwählen.
Kryptografie	MOVEit setzt starke kryptographische Mechanismen und sichere Auswahl, Verteilung und Schutz von Ver- und Entschlüsselungsschlüsseln ein, die den internationalen gesetzlichen und behördlichen Anforderungen entsprechen.
Physische Umgebungssicherheit	MOVEit bietet Flexibilität bei der Implementierung, mit der Sie die Einhaltung der lokalen physischen Sicherheitsanforderungen sicherstellen können.
Business-Continuity-Sicherheit	MOVEit dient dem Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Dateiübertragungen über alle Fehler-, Notfall- oder Ausfallphasen hinweg. Ipswitch Failover sorgt für ununterbrochene Verarbeitung von Dateiübertragungen.

Über Ipswitch

Ipswitch unterstützt Sie mit einfachen Lösungen bei der Behebung komplexer IT-Probleme. Die Software des Unternehmens wird weltweit von Millionen Benutzern zur Übertragung von Dateien zwischen Systemen, Geschäftspartnern und Kunden sowie zur Überwachung von Netzwerken, Anwendungen und Servern verwendet. Ipswitch wurde 1991 gegründet und ist in Lexington im US-Bundesstaat Massachusetts ansässig. Das Unternehmen unterhält Niederlassungen in den USA, Europa und Asien.

Weitere Informationen finden Sie unter **www.ipswitch.com**.

ipswitch

Laden Sie Ihre KOSTENLOSE 30-TÄGIGE TESTVERSION unter Ipswitch MOVEit herunter! ›