White Paper

Change Guardian
Directory und Resource Administrator
Sentinel

Überwachung der Dateiintegrität schützt vor Datenmissbrauch und sorgt für PCI-DSS-Compliance

Zu den grundlegenden Funktionen eines Informationssicherheitsprogramms zählen das rasche Erkennen von Sicherheitsverstößen sowie die Einleitung entsprechender Gegenmaßnahmen. Und dennoch greifen Unbefugte Tag für Tag unbemerkt auf vertrauliche Unternehmensdaten zu. Dabei spielt es keine Rolle, ob dieser Verstoß auf einen gezielten Angriff von Cyberkriminellen zurückzuführen ist oder darauf, dass ein privilegierter Benutzer diese Daten aus Versehen aufruft: Die Folgen sind oft ausgesprochen unangenehm. Bleibt dieser unberechtigte Zugriff dann auch noch für längere Zeit unbemerkt, ist das Ergebnis meist fatal.

NetIQ

Inhaltsverzeichnis

Seite

Einleitung

Thema dieses White Papers ist die Überwachung der Dateiintegrität (FIM, File Integrity Monitoring) und welchen Stellenwert sie dabei einnimmt, Angriffe von Cyberkriminellen als auch von Unternehmensangehörigen schneller zu erkennen und einem Datenmissbrauch mit kostspieligen Folgen vorzubeugen. Zudem wird erläutert, warum die Überwachung der Dateiintegrität eine Grundvoraussetzung zur Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) ist und wie sich diese Sicherheits- und Compliance-Herausforderungen mit der NetIQ Produktfamilie für das Identity and Security Management bewältigen lassen.

Vorsicht ist besser als Nachsicht. Noch nie erschien diese Warnung angebrachter als in der heutigen Zeit. Obwohl sich immer mehr Unternehmen der ihnen drohenden Gefahren bewusst sind und entsprechende Schutzmaßnahmen ergreifen, dominieren Sicherheitsverstöße nach wie vor die Schlagzeilen. Die Zahlen sind immens: Über einen Zeitraum von neun Jahren hat der „Data Breach Investigations Report (DBIR)“ des Verizon Business RISK Teams über 2.500 Sicherheitsverstöße und 1,1 Milliarden geschädigte Datensätze festgestellt[1]. Noch alarmierender ist die Tatsache, dass diese Verstöße direkt vor der Nase von Informationssicherheitsteams stattfanden, wie am Beispiel Heartland Payment Systems deutlich wird, in dem der unerlaubte Zugriff auf 100 Millionen Kreditkartenkonten während 18 Monaten unentdeckt blieb[2].

1 Verizon Business RISK Team, „2013 DBIR“, Verizon Business, April 2013, **www.verizonenterprise.com/DBIR/2013/**

2 John Kindervag, „PCI X-Ray: File Integrity Monitoring“, Forrester Research, Inc., 26. Oktober 2009, **www.forrester.com/rb/research**

Überwachung der Dateiintegrität: eine kritische Sicherheitskomponente

Die Überwachung der Dateiintegrität ist zu einer kritischen Sicherheitskomponente geworden, insbesondere angesichts der steigenden Gefahren im Hinblick auf vertrauliche Unternehmensdaten. Heutzutage haben wir es mit einer neuen Art von Angreifern zu tun: Organisierte Gruppen verschaffen sich systematisch Zugriff auf Unternehmenssysteme, wobei sie meist für einen längeren Zeitraum unbemerkt bleiben. Auf diese Weise können sie bestimmte Ziele verfolgen, die meist über einen direkten finanziellen Gewinn hinausgehen. Bei diesem – auf Englisch auch als Advanced Persistent Threat (APT) bezeichnetem – Szenario erfolgen Verstöße meist durch Ausnutzung von Vertrauensstellungen, wobei der Angriff auf die Systeme über legitime Konten stattfindet. Aus diesem Grund sind zusätzliche Schutzmaßnahmen, darunter die Überwachung der Dateiintegrität notwendig, um vertrauliche Unternehmensdaten vor dieser Art von Bedrohung zu schützen.

An der Verwendung von individuell programmierter Malware hat sich in den letzten Jahren nicht viel geändert, der Unterschied ist jedoch, dass neuartige Malware viel schwerer zu entdecken ist und daher immer häufiger von standardmäßigen Schutzmechanismen nicht erfasst wird.

Laut dem DBIR 2013 waren an 14 Prozent der Verstöße Insider beteiligt[3]. In den meisten Fällen wiesen die Indizien darauf hin, dass ein Missbrauch von Zugriffsrechten den Datenmissbrauch überhaupt erst möglich machte. Das Ausmaß der Bedrohungen durch Unternehmensangehörige wächst schnell ins Unermessliche, wenn man sich vor Augen führt, dass ein Angreifer, der sich beispielsweise mithilfe von Malware Zugang verschafft hat, im Prinzip nicht von einem Mitarbeiter unterschieden werden kann.

Laut dem Verizon-Bericht laufen viele Angriffe nach demselben Schema ab: Der Angreifer schleust sich in das System des Opfers ein, beispielsweise mithilfe gestohlener oder unsicherer Zugriffsdaten, und installiert anschließend Malware zur Erfassung der dort gespeicherten Daten. An der Verwendung von individuell programmierter Malware hat sich in den letzten Jahren nicht viel geändert, der Unterschied ist jedoch, dass neuartige Malware viel schwerer zu entdecken ist und daher immer häufiger von standardmäßigen Schutzmechanismen nicht erfasst wird. Malware wurde zum Beispiel im oben genannten Heartland-Fall sowie bei anderen groß angelegten Diebstählen von Kreditkartendaten eingesetzt. Forrester Research[4] ist der Meinung, dass die beste Möglichkeit zur Senkung des Risikos derartiger Angriffe darin besteht, Tools zur Überwachung der Dateiintegrität einzusetzen, die unmittelbare Warnmeldungen ausgeben, wenn nicht autorisierte Software installiert wird oder kritische Dateien von einem privilegierten Benutzer geändert oder aufgerufen werden.

Die Implementierung einer FIM-Software ist nicht nur eine Best Practice zum Schutz vor Sicherheitsverstößen, sondern auch eine Voraussetzung im Rahmen des Payment Card Industry Data Security Standard (PCI DSS). Insbesondere der PCI-DSS-Standard erfordert den Einsatz von FIM-Software, um Mitarbeiter auf unbefugte Änderungen an kritischen Systemdateien, Konfigurationsdateien oder Daten hinzuweisen. Eine Überwachung der Dateiintegrität ermöglicht die Erfassung von unberechtigtem Zugriff und Änderungen an Systemdateien und senkt dadurch folgende Risiken:

3 *Verizon Business RISK Team, „2013 DBIR“*
4 *John Kindervag, „PCI X-Ray: File Integrity Monitoring“*

Die den größten Schaden verursachenden Datenmissbrauchsfälle wurden erwiesenermaßen von autorisierten Benutzern verübt, die nicht ausreichend überwacht oder deren Zugriffsrechte im Verlauf ihres Identitäts-Lebenszyklus nicht ausreichend angepasst wurden.

- **Datenmissbrauch** – *insbesondere beim Missbrauch eines privilegierten Zugriffs*
- **Systemausfall** – *verursacht von ungeplanten oder unbefugten Änderungen an Dateien, Systemen und Anwendungen*
- **Compliance-Verstöße** – *die aufgrund fehlenden Überblicks über Zugriff und Änderungen an sensiblen Daten auftreten. Die Überwachung der Dateiintegrität ist eine grundlegende Komponente eines wirkungsvollen Informationssicherheitsprogramms.*

Angriffe durch Unternehmensangehörige unter der Lupe

Man kann grundsätzlich zwischen zwei Arten von Bedrohungen durch Unternehmensangehörige unterscheiden: böswillige und nicht böswillige. Nicht böswillig ist beispielsweise die Offenlegung kritischer Systeme und Daten durch Fehler oder Fehleinschätzungen bzw. aus Versehen. Dies erfolgt unter Umständen durch E-Mail- oder andere Anwendungen oder dadurch, dass Notebooks und Smartphones verloren gehen oder gestohlen werden. Angesichts der steigenden Zahl unternehmenseigener wie auch privater Mobilgeräte am Arbeitsplatz sind die bisherigen Sicherheitskontrollen und Schutzmaßnahmen nicht mehr ausreichend, um das Risiko durch diese Geräte abzudecken. Nicht böswillige Sicherheitsverstöße durch Unternehmensangehörige werden somit zu einem immer größeren Problem.

Böswillige Angriffe von Seiten gewinn- oder rachsüchtiger Mitarbeiter können über einen längeren Zeitraum hinweg einen erheblichen finanziellen Schaden verursachen und dazu führen, dass Unternehmensgeheimnisse nach außen weitergegeben werden. Die den größten Schaden verursachenden Datenmissbrauchsfälle wurden erwiesenermaßen von autorisierten Benutzern verübt, die nicht ausreichend überwacht oder deren Zugriffsrechte im Verlauf ihres Identitäts-Lebenszyklus nicht ausreichend angepasst wurden. Laut Verizon Business machen Fälle verärgerter Mitarbeiter, die weiterhin aktive Anmeldedaten nutzen, jedes Jahr erneut einen gewissen Anteil der Sicherheitsverstöße aus.

Cyberangriffe aus Profitgründen

Einige der Sicherheitsverstöße, die den größten finanziellen Schaden angerichtet haben, gehen auf gezielte und technisch hoch entwickelte Hackerangriffe zurück. Eines der berüchtigtsten Beispiele dafür ist der bereits erwähnte Angriff auf Heartland Payment Systems. Sicherheitsexperten gehen davon aus, dass bei diesem Angriff gigantischen Ausmaßes 100 Mio. Kreditkarten von 650 verschiedenen Ausstellern offengelegt wurden. Der finanzielle Schaden war verheerend: Der Börsenwert von Heartland fiel um 300 Mio. US-Dollar, und es entstanden direkte Verluste von über 30 Mio. US-Dollar[5].

Ein weiteres prominentes Beispiel für einen ausgefeilten Multi-Vektor-Angriff ist der Stuxnet-Wurm. Bruce Schneier[6] zufolge ist der Stuxnet-Wurm „eine völlig neuartige Malware, die auf derart heimtückische und vielfältige Weise ungepatchte Sicherheitslücken ausnutzt, dass Sicherheitsexperten nach Untersuchung des Wurms davon ausgehen, dass er das Werk von professionellen Hackern ist, die auf der Gehaltsliste der Vereinigten Staaten stehen.“ Bis dato scheint das Programm bisher rund ein Fünftel der Zentrifugen in einer

5 *ibd.*
6 *Bruce Schneier, „Schneier on Security: The Stuxnet Worm“,* **www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html** *(Stand: 10. Februar 2011)*

iranischen Uran-Anreicherungsanlage schachmatt gesetzt zu haben. Der Bau der ersten iranischen Atomwaffen wurde dadurch zwar nicht unterbunden, aber zumindest verzögert[7]. Experten warnen jedoch davor, dass der zur Infiltration industrieller Kontrollsysteme konzipierte Wurm als Vorlage verwendet werden könnte, um Maschinen in Kraftwerken, Stromnetzen oder anderen Infrastrukturen zu sabotieren.

Cyberkriminellen das Handwerk legen

Die Angriffstaktiken haben sich in den letzten Jahren stark geändert und sind mittlerweile so raffiniert, dass sie von ihren Opfern kaum noch bemerkt werden. Auf diese Weise bleiben sie lange Zeit unentdeckt, und die Angreifer können die Zielsysteme in aller Ruhe ausnutzen. Um auf das Beispiel von Heartland Payment Systems zurückzukommen: Dieser Angriff blieb 18 Monate lang unentdeckt und wurde letzten Endes nicht vom internen Sicherheitsteam von Heartland, sondern von Außenstehenden aufgedeckt.

Diese tückischen Angriffe treten in mehreren Formen auf, wobei sich die Kriminellen verschiedene Vektoren zunutze machen. Nichtsdestotrotz gibt es verschiedene Merkmale, die allen Online-Angriffen gemein sind. In den meisten Fällen gab es zumindest ein Anzeichen für die Aufklärung vor dem eigentlichen Angriff, meist Foot-Printing, Scans oder das Zählen der Systemkomponenten. Sobald die Netzwerkgrenzen des angegriffenen Unternehmens einmal überwunden worden waren, konnten über 60 Prozent der Hacker das System binnen Minuten oder Stunden kompromittieren.

Verizon zufolge dauerte es in rund 66 Prozent aller Fälle mehrere Monate oder länger, bis den betroffenen Unternehmen der Angriff auffiel. Wird der Datenmissbrauch dann tatsächlich aufgedeckt, erfolgt dies meist über eine Backend-Überwachung von Kreditkartenunternehmen, die sich dabei einer als Common Point of Purchase (CPP) bezeichneten Methode bedienen, die normalerweise zur Aufdeckung betrügerischer Aktivitäten herangezogen wird.

Die Angriffstaktiken haben sich in den letzten Jahren stark geändert und sind mittlerweile so raffiniert, dass sie von ihren Opfern kaum noch bemerkt werden. Auf diese Weise bleiben sie lange Zeit unentdeckt, und die Angreifer können die Zielsysteme in aller Ruhe ausnutzen.

7 *William J. Broad, John Markoff und David E. Sanger, „Israeli Test on Worm Called Crucial in Iran Nuclear Delay“,* New York Times, *15. Januar 2011,* **www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html** *(Stand: 10. Februar 2011)*

Mitarbeiter erhalten häufig mehr Zugriffsrechte, als sie zur Ausübung ihrer Tätigkeit benötigen. Zudem werden die Aktivitäten privilegierter Benutzer häufig nicht ausreichend überwacht. Die einfache Lösung besteht darin, privilegierte Benutzer in Echtzeit zu überwachen, um somit nicht autorisierte oder ungewöhnliche Aktivitäten umgehend zu erfassen.

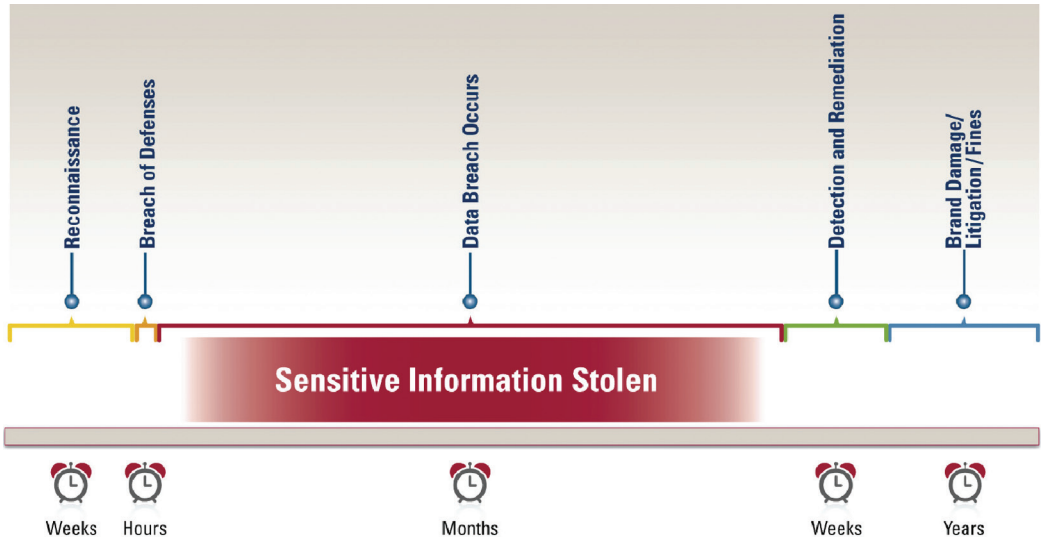

Abb. 1

Zeitverlauf eines typischen Datenmissbrauchs

Schutz vor Bedrohungen von innen und außen

Die Steigerung der Zahlen für Verstöße unter Beteiligung von Insidern im Jahresvergleich führt zu der Frage, ob Insider-Angriffe eine zunehmende Tendenz aufweisen. Doch unabhängig von der Ursache dieses Trends gibt es einfache Strategien, mit denen vertrauliche Unternehmensdaten zuverlässig geschützt werden können. Aus dem Verizon-Bericht geht klar hervor, dass Mitarbeiter häufig mehr Zugriffsrechte erhalten, als sie zur Ausübung ihrer Tätigkeit benötigen. Zudem werden die Aktivitäten privilegierter Benutzer häufig nicht ausreichend überwacht. Die einfache Lösung besteht darin, privilegierte Benutzer in Echtzeit zu überwachen, um somit nicht autorisierte oder ungewöhnliche Aktivitäten umgehend zu erfassen. Da privilegierte Benutzer häufig Zugriff auf vertrauliche oder kritische System- und Datendateien haben, lässt sich mithilfe von Technologien zur Überwachung der Dateiintegrität nachverfolgen, ob kritische Systemdateien, Sicherheitsprotokolle, vertrauliche Daten oder freigegebene Laufwerke aufgerufen und geändert wurden. Im Fall von Systemdateien auf geschäftskritischen Systemen oder vertraulichen Daten können Echtzeitwarnungen bei Änderungen ausgegeben werden, sodass Probleme umgehend erkannt werden.

Man sollte sich vor Augen führen, dass das Verhalten eines Angreifers, der sich Zugang zu einem internen Benutzerkonto verschafft hat, häufig nicht von legitimen Aktivitäten unterschieden werden kann. Eine Überwachung der Dateiintegrität sorgt jedoch dafür, dass die typischerweise bei einem Advanced Persistent Threat auftretende Änderung von Dateien erfasst wird. Eine derartige Aktivität kann dann umgehend genauer untersucht werden, bevor es zu einem kostspieligen Datenmissbrauch kommt. Durch eine frühzeitige Erkennung eines solchen Verstoßes ist das Sicherheitsteam in der Lage, wesentlich schneller zu reagieren und eventuelle Schäden weitestgehend einzudämmen.

Mit der PCI-DSS-Anforderung 11.5 soll gewährleistet werden, dass Unternehmen über stabile Abwehrmaßnahmen vor der Ausnutzung kritischer Ressourcen (insbesondere Server) verfügen.

Ein Fall für unternehmensweite Compliance: PCI DSS

Die Überwachung der Dateiintegrität trägt nicht nur dazu bei, das Risiko eines Datenmissbrauchs zu verringern, sondern ist auch für Compliance unabdingbar. Der Payment Card Industry Data Security Standard ist eine vertraglich geregelte Vorgabe für Unternehmen, die Karteninhaberdaten von Visa, MasterCard, Discover, American Express und Diner's Club verwalten[8]. PCI DSS schreibt die Verwendung von FIM-Software in den Anforderungen 10 und 11 vor.

Anforderung 10.5: Schutz von Audit-Trails (Protokolldateien) vor Veränderungen

> *„Verwenden Sie Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle, damit bei der Änderung von bestehenden Protokolldaten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).“*

Die PCI-DSS-Anforderung 10.5 schreibt die Verwendung von Dateiintegritätsüberwachung oder Tools zur Erkennung von Änderungen an Protokolldateien vor. Außerdem muss bei Änderungen ein Alarm ausgelöst werden. Dies trägt dazu bei, die Sicherheit von Audit-Trails zu gewährleisten.

Anforderung 11.5: Zugriff auf und Änderungen an kritischen Inhalts- und Systemdateien

> *„Setzen Sie Tools zur Überwachung der Dateiintegrität ein, die das Personal über nicht autorisierte Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und konfigurieren Sie die Software so, dass sie mindestens wöchentlich Vergleiche wichtiger Dateien herstellt.“*

Mit der PCI-DSS-Anforderung 11.5 soll gewährleistet werden, dass Unternehmen über stabile Abwehrmaßnahmen vor der Ausnutzung kritischer Ressourcen (insbesondere Server) verfügen. Unternehmen können den Schutz ihrer kritischen Systeme jedoch erst dann gewährleisten, wenn sie auf Änderungen an Dateien und Dateisystemen aufmerksam gemacht werden und sie diese Änderungen dokumentieren. Sie müssen beispielsweise folgende Fragen beantworten können:

8 *PCI Security Standards Council, LLC, „About the PCI Data Security Standard (PCI DSS)“,* **www.pcisecuritystandards.org/security_standards/pci_dss.shtml** *(Stand: 29. März 2010).*

Doch unabhängig davon, ob die Gefahr nun in Malware oder dem nicht autorisierten Zugriff auf vertrauliche Informationen besteht, kann das Risiko für kritische Daten und Infrastrukturen mithilfe eines Systems zur Überwachung der Dateiintegrität drastisch verringert werden, da somit in Echtzeit überwacht wird, ob sensible Dateien und Systeme aufgerufen und geändert werden.

- *Wer hat die Änderung vorgenommen?*
- *Was genau wurde geändert – Dateien, die Registrierung oder Konfigurationseinstellungen?*
- *Wann fand die Änderung statt?*
- *Welchen Wert hatte die Einstellung vor der Änderung?*
- *Auf welchen neuen Wert wurde die Einstellung geändert?*
- *Wurde diese Änderung im Rahmen eines Änderungsmanagement-Prozesses genehmigt?*

Sicherheit und Compliance dank wirkungsvoller Überwachung der Dateiintegrität mit NetIQ Change Guardian

Sicherheitsexperten sind derzeit mit einer Vielfalt von Bedrohungen konfrontiert. Doch unabhängig davon, ob die Gefahr nun in Malware oder dem nicht autorisierten Zugriff auf vertrauliche Informationen besteht, kann das Risiko für kritische Daten und Infrastrukturen mithilfe eines Systems zur Überwachung der Dateiintegrität drastisch verringert werden, da somit in Echtzeit überwacht wird, ob sensible Dateien und Systeme aufgerufen und geändert werden.

Die Implementierung eines solchen Systems ist jedoch nicht nur unverzichtbar zum Schutz von Daten, sondern auch zur Erfüllung von Vorschriften, die spezifisch Maßnahmen zur Überwachung der Dateiintegrität erforderlich machen. Auf diese Weise vermeiden Unternehmen empfindliche Strafen und andere negative Auswirkungen aufgrund eines Mangels an Compliance.

NetIQ Change Guardian umfasst eine Dateiintegritätsüberwachung in Echtzeit mit folgenden Eigenschaften:

- *Erkennung von Änderungen an kritischen Systemen und Dateien in Echtzeit*
- *Benachrichtigungen, auch wenn die Inhalte nur angezeigt und nicht geändert wurden*
- *Integration in führende SIEM-Lösungen (Security Information and Events Management) wie NetIQ Sentinel*
- *Bereitstellung umfassender Informationen im Rahmen der Benachrichtigung, beispielsweise Zeitpunkt der Änderung, Name der Person, die die Änderung vorgenommen hat, Umfang der Änderung und Status vor der Änderung*
- *Einhaltung der Compliance durch Überwachung des Zugriffs auf vertrauliche Daten*
- *Erkennung von Änderungen auf den wichtigsten Plattformen: Microsoft Windows, Active Directory (einschließlich Gruppenrichtlinienobjekten), UNIX und Linux*

Mit NetIQ Change Guardian können Ihre Sicherheitsteams in Echtzeit erfassen, ob auf kritische Dateien, Systemkonfigurationen oder Active Directory (inklusive Gruppenrichtlinienobjekten) ohne Autorisierung zugegriffen wurde oder diese geändert wurden. Somit werden Unternehmensinformationen und Kundendaten proaktiv vor böswilligen Angriffen und unbeabsichtigten Sicherheitsverstößen geschützt. Diese Lösungen stellen die für intelligente Entscheidungen nötigen Informationen bereit, verringern das Risiko des Verlusts von Unternehmensdaten und sorgen dafür, dass der Wert vorhandener Sicherheitssysteme voll ausgeschöpft wird.

Gemeinsam stark: NetIQ Identity and Security Management-Lösungen

Nicht autorisierte Änderungen der Konfiguration kritischer Systeme und Infrastrukturen stellen ein signifikantes steigendes Risiko für Unternehmensdaten, Kundeninformationen und die Systemstabilität dar. NetIQ Change Guardian versetzt Sie in die Lage, unbefugte Änderungen umgehend zu erfassen und entsprechend darauf zu reagieren. Das Ergebnis: eine drastische Senkung des Risikos schädlicher Aktivitäten sowie ein umfassender und zuverlässiger Schutz von Daten.

Mit der integrierten Lösung von NetIQ können Ihre Sicherheitsexperten eine umfassende und skalierbare Sicherheits- und Compliance-Infrastruktur aufbauen, die zudem mit einem geringeren Arbeitsaufwand verbunden ist. NetIQ Change Guardian lässt sich sowohl mit neuesten Tools zur Workflow-Automatisierung als auch mit NetIQ Directory and Resource Administrator einsetzen und ermöglicht eine detaillierte Kontrolle des administrativen Zugriffs. Daraus resultiert eine leistungsstarke, integrierte und automatisierte Lösung für das Identity and Security Management. NetIQ Change Guardian kann zudem nahtlos in SIEM-Lösungen wie den preisgekrönten NetIQ Sentinel integriert werden, um korrelierte, umfassende und relevante Informationen in Echtzeit an Sicherheits- und Compliance-Teams weiterzuleiten. Unternehmen profitieren beim gemeinsamen Einsatz dieser Produkte nicht nur von einem zuverlässigen Schutz ihrer Daten, sondern können auch Vorschriften wie beispielsweise PCI DSS ohne Probleme erfüllen.

Mit der integrierten Lösung von NetIQ können Ihre Sicherheitsexperten eine umfassende und skalierbare Sicherheits- und Compliance-Infrastruktur aufbauen, die zudem mit einem geringeren Arbeitsaufwand verbunden ist.

Fazit

Durch die Überwachung der Dateiintegrität wird gewährleistet, dass ein nicht autorisierter Zugriff auf kritische Systeme umgehend erkannt wird. Sie ist somit ein grundlegendes Element zur Verhinderung von Datenmissbrauch, der auf Malware-Angriffe oder böswillige (bzw. unbeabsichtigte) Aktivitäten von Unternehmensangehörigen zurückzuführen ist. Des Weiteren ist die Überwachung der Dateiintegrität eine explizit in den Anforderungen 10.5 und 11.5 erwähnte Grundvoraussetzung für PCI-DSS-Compliance, die dafür sorgt, dass das Aufrufen und Ändern von kritischen Systemen erfasst und zuverlässig dokumentiert wird. Zur optimalen Aufrechterhaltung von Sicherheit und Compliance sollte Software zur Überwachung der Dateiintegrität mit SIEM-Lösungen verknüpft werden, um eine Korrelation mit anderen Sicherheitsereignissen zu erzielen und sicherzustellen, dass kritische Daten und Systeme optimal geschützt sind.

Unsere Kunden und Partner entscheiden sich für NetIQ, weil wir kostengünstige Lösungen für den Schutz von Daten und die Verwaltung dynamischer, hochgradig verteilter Anwendungsumgebungen bereitstellen.

NetIQ Change Guardian ermöglicht die Erfassung von unbefugtem Zugriff und Änderungen an kritischen Dateien und Systemkonfigurationen sowie Alarmierungen in Echtzeit. Dadurch verringern Sie nicht nur das Risiko eines Datenmissbrauchs oder Insider-Angriffs, sondern erfahren auch, wer wann und wo welche Änderungen an wichtigen Komponenten Ihrer Infrastruktur, wie z. B. Active Directory und Gruppenrichtlinienobjekte, vorgenommen hat.

Insbesondere in Verbindung mit herkömmlichen SIEM-Lösungen werden mit dieser Lösung auf umfassende und effektive Weise der Zeitaufwand zum Sammeln von Informationen verkürzt, das Fällen von Entscheidungen beschleunigt und das Risiko für Sicherheitsverstöße verringert.

Weitere Informationen zur Erfüllung Ihrer Anforderungen in Bezug auf die Überwachung der Dateiintegrität erhalten Sie unter **www.netiq.com** oder von Ihrem lokalen NetIQ Vertriebsmitarbeiter oder Partner.

Informationen zu NetIQ

NetIQ ist ein weltweiter Anbieter von IT-Lösungen und Unternehmenssoftware, für den der Erfolg seiner Kunden im Mittelpunkt steht. Unsere Kunden und Partner entscheiden sich für NetIQ, weil wir kostengünstige Lösungen für den Schutz von Daten und die Verwaltung dynamischer, hochgradig verteilter Anwendungsumgebungen bereitstellen.

Unser Portfolio umfasst skalierbare, automatisierte Lösungen für Identität, Sicherheit und Governance sowie IT-Operations-Management, mit denen Unternehmen ihre Computing-Services in klassischen Client-Server-, virtuellen und Cloud-Umgebungen zuverlässig bereitstellen, messen und verwalten können. In Kombination mit unserem praxisnahen, kundenorientierten Ansatz sorgen diese Lösungen dafür, dass Unternehmen selbst schwierigste Herausforderungen meistern und dabei gleichzeitig Kosten, Komplexität und Risiken minimieren.

Weitere Informationen zu unseren branchenweit anerkannten Softwarelösungen finden Sie unter **www.netiq.com**.

NetIQ
Deutschland
Fraunhoferstr. 7
85737 Ismaning
Tel: +49 (0)89 420940
Email: infoDE@netiq.com

Schweiz
Flughafenstrasse 90
P.O. Box 253 8058 Zürich
Tel: +41 (0)43 456 2400
Email: infoCH@netiq.com

info@netiq.com
www.netiq.com/communities
www.netiq.com

Die vollständige Liste unserer Niederlassungen
in Nordamerika, Europa, Nahost, Afrika, Lateinamerika sowie im asiatisch-pazifischen Raum finden Sie unter: www.netiq.com/contacts

www.netiq.com

www.netiq.com