clearswift
by HelpSystems

LEITFADEN *(Cybersicherheit)*

PCI-Compliance:

Die Notwendigkeit einer adaptiven Lösung

PCI-Compliance im Rahmen der DSGVO

Der Payment Card Industry Data Security Standard (PCI-DSS) gilt seit 2004 und wurde im April 2016 zum letzten Mal überarbeitet. Sein Ziel ist einfach: der Schutz von Zahlungskartendaten. Vor dem Inkrafttreten der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) im Mai 2018 haben sich Unternehmen erneut mit dem PCI-DSS befasst und ermittelt, was erforderlich ist, um diesen unter allen Umständen einzuhalten. Datenbankprobleme und deren Lösungen sind weitgehend bekannt – die wahre Herausforderung sind unstrukturierte Daten. Wenn Kreditkarteninformationen in E-Mails und Dokumente eingefügt werden, können diese dann innerhalb des Unternehmens oder auch an externe Empfänger verschickt werden, und dadurch ein unnötiges Risiko verursachen.

Risiken und Konsequenzen bei einem PCI-Verstoß

PCI-DSS war einer der ersten globalen Standards für ein breites Spektrum von Unternehmen. Im Wesentlichen besagt er, dass bei der Abwicklung von Kreditkartenzahlungen entweder Sie oder Ihr Geschäftspartner diesen Standard erfüllen müssen.

Bei einem Verstoß drohen Bußgelder zwischen 50 und 90 USD pro gefährdetem Karteninhaber. Bis zur Einhaltung des Standards fallen zudem weitere Strafgebühren an. Diese können zwischen 10.000 und 100.000 USD pro Monat betragen, sind also nicht unerheblich. Die größte Gefahr ist jedoch, dass Sie keine Daten mehr verarbeiten dürfen, d. h. Sie können keine Kreditkartenzahlungen mehr annehmen. In vielen Unternehmen kommt dadurch das Geschäft zum Erliegen.

Weitere Konsequenzen eines Verstoßes bleiben ebenfalls bestehen: von der Rufschädigung über den Verlust von Kunden, Partnern und Zulieferern bis hin zu erhöhten Prüfungshonoraren sowie die Kosten für Sanierungsmaßnahmen und möglicherweise eines Gerichtsverfahrens.

Unter der DSGVO drohen eventuell noch höhere Strafen: die Obergrenze beträgt 20 Millionen Euro oder 4 % des weltweiten Umsatzes (was immer höher ist).

Eingehende und ausgehende Kreditkarten – und Kundendaten

In vielen Unternehmen ist der Erhalt von E-Mails mit Kreditkartendaten alltäglich. Zwei mögliche Ursachen sind Kunden, die es bevorzugen Ihre Daten lieber schriftlich statt mündlich zu übermitteln, und Personen, die sich mit Online-Portalen schwer tun. Die natürliche Reaktion beim Erhalt einer E-Mail ist, darauf zu direkt zu antworten. Dies kann jedoch Probleme verursachen, weil das Unternehmen somit PCI-Daten über einen offenen Kanal verschickt. Und das bewirkt eine Datenpanne, selbst wenn die Daten zurück an den ursprünglichen Absender geschickt werden. Bei herkömmlichen Data Loss Prevention (DLP)-Lösungen wird die Kreditkartennummer erkannt und die komplette E-Mail gesperrt. Dieses Vorgehen sorgt jedoch für Frust: beim Kunden, der nicht weiß, ob seine Nachricht angekommen ist, beim Mitarbeiter, der keine Antwort schicken kann, und bei der IT- oder Compliance-Abteilung, die dem Problem nachgehen und eine entsprechende Lösung finden muss.

Datenverlust kann verheerende Auswirkungen für den Ruf des Unternehmens haben, doch jetzt gibt es auch noch ein Gebot für eingehende Informationen. Der Erhalt unerwünschter Daten kann nämlich genau so viele Probleme bereiten, wie Daten, die das Unternehmen verlassen. In diesem Zusammenhang sind einige Szenarien zu berücksichtigen.

PCI-Daten in einem Netzwerk, das dem PCI-DSS nicht gerecht wird

In vielen Unternehmen wird die Verarbeitung von Kreditkartendaten an Dritte vergeben, denn dadurch müssen die Unternehmen selbst den PCI-DSS nicht erfüllen. Selbst bei Banken gibt es Netzwerksegmente, die den PCI-DSS nicht erfüllen, weil dies theoretisch nicht erforderlich ist. Natürlich ist Theorie nicht gleich Praxis, und sie erhalten teilweise doch solche Daten. In dieser Situation werden Prüf- und Compliance-Beauftragte eingeschaltet, um dem Problem auf den Grund zu gehen und es dann zu beheben.

Versehentlich verschickte Daten

Wie oft haben Sie schon aus Versehen Informationen verschickt oder erhalten? Wahrscheinlich ist das schon einmal vorgekommen, hoffentlich aber nicht zu oft. Wenn Sie diese Vorkommnisse jedoch mit der Anzahl Ihrer Mitarbeiter multiplizieren, treten sie häufiger auf, als Sie denken. In vielen Fällen bereiten die verschickten Informationen kein Compliance-Problem, manchmal aber schon. Ein weiteres

Risiko für eine Datenpanne sind „verborgene“ Informationen in Datenblättern oder Berichten. Bei der DSGVO sorgt ein neuer Grundsatz zur Verantwortungsteilung dafür, dass der Empfang unerlaubter Daten zu einem ernsthaften Problem wird.

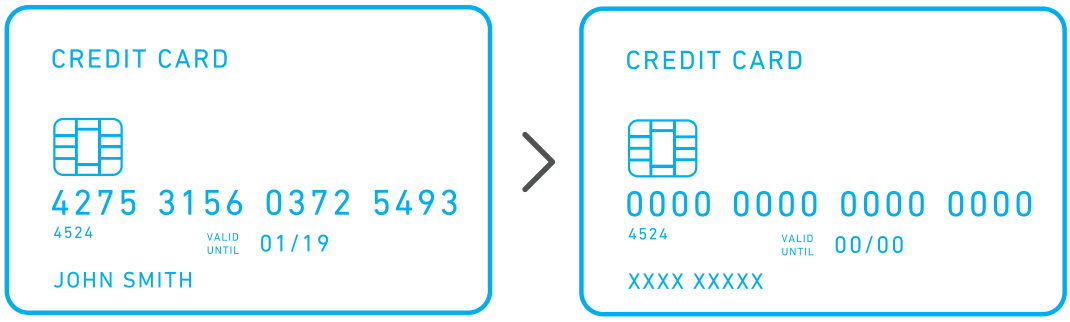
Weil elektronischer Informationsaustausch für den Erfolg von Unternehmen heute ausschlaggebend ist und traditionelle DLP aber die Kommunikation und somit die Zusammenarbeit unterbricht, wird sie nur selten eingesetzt. Das Risiko, dass dem Unternehmen Geschäfte entgehen, ist oft wichtiger, als das Problem zu beheben. Zum Glück gibt es aber noch eine andere Möglichkeit –bei der der Inhalt in Echtzeit adaptiert werden kann. Dadurch kann der Informationsaustausch fortgesetzt werden, und das Risiko, dass unerlaubte Daten gesendet oder empfangen werden, entfällt somit.

Eine adaptive Lösung

Clearswift gehört seit über 20 Jahren zu den führenden Unternehmen im Bereich E-Mail- und Internetsicherheit. Da uns die Probleme mit herkömmlicher DLP vertraut waren, haben wir versucht, eine Lösung zu finden. Das Ergebnis hieß Adaptive DLP. Das Konzept von Adaptive DLP ist relativ einfach: Informationen, die gegen die Richtlinie verstoßen, werden entfernt, der Rest erreicht ungehindert sein Ziel.

Adaptive Redaction besteht aus drei Komponenten:

1. Data Redaction: Hierbei werden Informationen entfernt, die sichtbar sind. Beispiel: Die Kreditkartennummer in einer E-Mail wird durch Nullen oder Sternchen ersetzt. Durch diese Funktion werden auch „unsichtbare“ Informationen entfernt, zum Beispiel ausgeblendete Zeilen und Spalten in Datenblättern, die PCI-Daten enthalten.

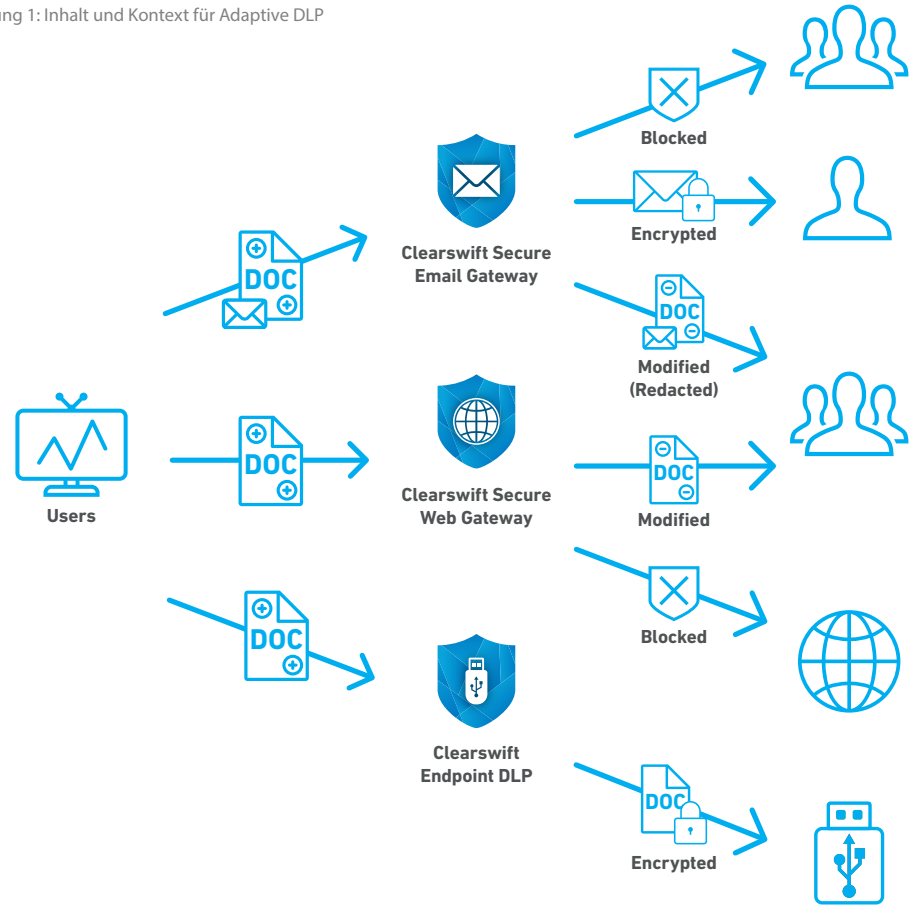


2. Document Sanitization: Hierbei werden verborgene Informationen wie Dokumenteigenschaften, Revisionsverlauf und Schnellspeicherdaten entfernt.
3. Structural Sanitization: Entfernt aktive Inhalte und somit die gängigste Methode für das Einschmuggeln von Ransomware in Unternehmen.

In der Sicherheitsbranche gilt der Leitsatz: „Man ist nur so stark wie das schwächste Glied“. In der Praxis heißt das, dass sämtliche Kommunikationskanäle berücksichtigt werden müssen. E-Mail, Internet oder Endgeräte, an denen Informationen auf einen USB-Stick oder andere Wechselmedien kopiert werden können – sie alle stellen ein Risiko dar.

Der adaptive Ansatz von Clearswift basiert auf einer allgemeinen DCI (Deep Content Inspection)-Engine. Dadurch lässt sich eine Richtlinie erstellen, die dann auf alle Kommunikationskanäle angewendet werden kann. Welche Maßnahmen getroffenen werden, hängt dann vom Kanal ab. Siehe Abbildung 1. Bei einer E-Mail werden möglicherweise Daten redigiert, während Inhalte, die auf ein Kollaborationsportal (z. B. Microsoft OneDrive) hochgeladen werden sollen, gesperrt werden und Daten beim Kopieren auf einen USB-Stick verschlüsselt werden.

Abbildung 1: Inhalt und Kontext für Adaptive DLP



Eine unbegrenzt flexible Richtlinie gewährleistet die nötige Granularität, um eine Entscheidung anhand des Inhalts, des Kontexts (wer versucht was) und des Kommunikationskanals zu ermöglichen.

Verteilte Verwaltung

Bei keiner DLP-Lösung sind Sicherheitsvorfälle jedoch ganz auszuschließen, selbst bei Adaptive DLP. Es kann passieren, dass die Richtlinie zu genau greift und geändert werden muss. Die Lösung von Clearswift kann problemlos zusammen mit Microsoft Active Directory (und allen anderen DLAP-Diensten) verwendet werden. Sie sorgt dafür, dass DLP-Ereignisse nicht einfach an irgendeine Person oder Abteilung weitergeleitet werden, sondern an den Vorgesetzten des Mitarbeiters, der den Verstoß verursacht hat.

Obwohl die Sicherheitsvorfälle auch an bestimmte Personen oder Abteilungen gemeldet werden können, haben wir festgestellt, dass die DLP-Lösung wesentlich weniger Aufwand verursacht, wenn Zwischenfälle an den Vorgesetzten geleitet werden. Dieser

weiß nämlich, in welchem Zusammenhang der Mitarbeiter gehandelt hat, und kann – sofern es die Umstände erlauben – die ursprüngliche E-Mail per Mausklick auf eine URL wieder freigeben. Siehe Abbildung 2.

Dank der Einführung der verteilten Verwaltung kann selbst in kleinen und mittleren Unternehmen eine kostengünstige DLP-Lösung eingesetzt werden, ohne dass zusätzliche IT-Mitarbeiter erforderlich sind.

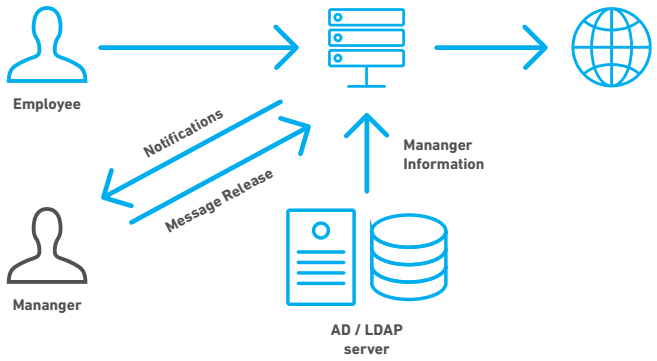


Abbildung 2: Verteilte Verwaltung senkt die Betriebskosten

Verbesserung bestehender Sicherheitslösungen

Die adaptive Lösung von Clearswift kann sowohl alleine verwendet werden als auch im Zusammenhang mit bereits bestehenden E-Mail- und Internetgateways oder anderen DLP-Lösungen. Somit müssen vorhandene Produkte nicht ausgetauscht werden. Und falls Sie sich doch entscheiden, auf einen Gateway von Clearswift zu wechseln, lässt sich eine adaptive DLP-Richtlinie schnell und einfach für den Gateway übernehmen – egal, ob er physisch vorhanden ist oder in der Cloud.

Altdaten

Auch wenn Sie sich um aktuelle Daten kümmern, können Altdaten immer noch ein Problem darstellen. So zum Beispiel Berichte oder anderen Dateien die im Unternehmen verbreitet worden sind. Clearswift bietet daher eine Funktion zum Scannen von ruhenden Daten (Data-At-Rest, DAR) auf Endgeräten und Servern. Dadurch werden Systeme, auf denen PCI-Daten gespeichert sind, im Handumdrehen erkannt. Diese Überprüfung kann auch auf Cloud-Laufwerke ausgeweitet werden, um sicherzustellen, dass keine kritischen Daten unerlaubt hochgeladen worden sind. Eventuell reichen ein einfacher Bericht oder eine automatische Maßnahme, bei der alle betroffenen Dateien auf einen sicheren Server verschoben werden. Abhängig von der Richtlinie lässt sich das Risiko von Altdaten auch granular beheben.

Zusammenfassung

In Sachen PCI kann mangelnde Compliance verheerend für Unternehmen sein. Zum einen aufgrund hoher Bußgelder und zum anderen, wenn das Unternehmen keine Kreditkarten verarbeiten kann, bis Compliance erreicht hat, kommt möglicherweise das gesamte Geschäft zum Erliegen. Selbst Unternehmen, die die Verarbeitung von Kreditkartendaten an Dritte abgegeben haben, laufen Gefahr, solche Daten aus Versehen zu erhalten.

Aus Sicht der Compliance ist es relativ egal, auf welche Weise Daten unerlaubt in fremde Hände gelangen – ob durch einen externen Hacker, einen Mitarbeiter mit unlauterer Absicht oder einen Fehler.

Herkömmliche DLP-Lösungen bringen einige wesentliche Nachteile mit sich, besonders für kleine und mittlere Unternehmen. A-DLP-Lösungen der nächsten Generation hingegen senken das Risiko, ohne unnötige Zusatzkosten zu verursachen. Mit Hilfe einer zentralen Richtlinie für sämtliche Kommunikationskanäle, die sowohl auf eingehende als auch auf ausgehende Daten angewendet wird, lässt sich jedoch sicherstellen, dass Kreditkarteninformationen stets geschützt bleiben.

clearswift
by HelpSystems

www.clearswift.de

Über HelpSystems

HelpSystems ist ein Softwareunternehmen, in dem die Menschen an erster Stelle stehen. Getreu unserem Motto Build a Better IT TM unterstützen wir außergewöhnliche Unternehmen bei ihrer Arbeit. Unsere ganzheitliche Produktsuite aus Sicherheits- und Automatisierungslösungen schafft eine einfachere, intelligentere und leistungsstarke IT. Kunden in über 100 Ländern und in den unterschiedlichsten Branchen vertrauen auf HelpSystems. Erfahren Sie mehr unter www.helpsystems.com/de.