IT-Sicherheit

E-Mail-Verschlüsselung und andere Sicherheitsrisiken

Wie eine Studie zeigt, sind nach wie vor ausgerechnet Topmanager für Sicherheitsthemen oft nicht richtig sensibilisiert und versenden vertrauliche Daten noch unverschlüsselt. Doch selbst wenn Anwender auf vermeintlich sichere Kommunikationswege wie die E-Mail-Verschlüsselung setzen, lauern noch versteckte Gefahren.

› Gabriel Gabriel

Cyberangriffe sind für Industrieunternehmen längst Alltag. Mit steigender Tendenz werden immer mehr Schweizer Firmen Opfer von Sabotage, Datendiebstahl oder Industriespionage. Im Jahr 2018 machten laut der Konferenz der kantonalen Polizeikommandanten (KKPKS) in der Schweiz Vermögensdelikte mit zwei Dritteln den grössten Anteil der erfassten Straftaten aus. Dabei sei die Zahl der Delikte im Zusammenhang mit dem Internet am meisten angestiegen. 13 Prozent mehr Straftaten gab es laut der KKPKS auch beim Missbrauch von Datenverarbeitungsanlagen.

Lesbar wie eine Postkarte

Reihum fordern Gesetzgeber und Experten deshalb die Verschlüsselung von Daten – beispielsweise in der EU-Datenschutzgrundverordnung, von der auch Schweizer Unternehmen betroffen sind. Allerdings gehört nach wie vor gerade der unverschlüsselte E-Mail-Versand in den Vorstandsabteilungen vieler Firmen zum Arbeitsalltag – auch für vertrauliche Dokumente. Dieser bietet jedoch viel Angriffsfläche für Cyberkriminelle, da die Nachrichten meist zwischen den verschiedensten Servern hin- und hergeroutet werden, die sich darüber hinaus meist in unterschiedlichen Ländern befinden. Das stellt ein perfektes Szenario für sogenannte «Man in the middle»-Angriffe dar, bei denen sich Hacker in die Kommunikationswege einklinken und unbemerkt Daten abgreifen können.

kurz & bündig

- Im Jahr 2018 machten Vermögensdelikte in der Schweiz den grössten Anteil erfasster Straftaten aus. Dabei sind Delikte im Zusammenhang mit dem Internet am meisten angestiegen.
- Nach wie vor gehört der unverschlüsselte E-Mail-Versand zum Arbeitsalltag, dies betrifft auch vertrauliche Dokumente.
- Allerdings bringt auch das Verfahren der Verschlüsselung einige Nachteile mit sich.
- Eine zusätzliche Absicherung sind virtuelle Datenräume, also Plattformen zum kontrollierten Informationsaustausch. Innerhalb dieser können Daten gespeichert, ausgetauscht, bearbeitet und je nach Bedarf für weitere ausgewählte Personen freigegeben werden.

Doch selbst ohne ausgeklügelte Angriffsstrategie können beim unverschlüsselten Mail-Verkehr leicht Informationen in falsche Hände geraten. Denn grundsätzlich können diese Nachrichten von jedem mitgelesen werden, man muss nur wissen, wonach man sucht. Sie sind also nicht sicherer als Postkarten, die ebenfalls jederzeit vom Postboten gelesen werden können. Um diese Risiken zu minimieren, hat sich in den letzten Jahren die E-Mail-Verschlüsselung immer mehr durchgesetzt.

Anfällige Verschlüsselungen

Wie die Studie «Boardkommunikation und -digitalisierung» von Brainloop zeigt, sind jedoch noch immer ausgerechnet Topmanager für Sicherheitsthemen oft nicht richtig sensibilisiert und versenden vertrauliche Daten noch unverschlüsselt. Gleichzeitig allerdings bringt auch das Verfahren der Verschlüsselung einige

Nachteile mit sich – und teilweise sogar massive Sicherheitslücken.

Leider sind die aktuell gängigsten Verfahren zur «Mail-Encryption», «Open PGP» und «S/MIME» (Secure/Multipurpose Internet Mail Extensions), nicht vollständig gegen die bereits erwähnten «Man in the middle»-Angriffe geschützt. Das hat die im Mai 2018 bekannt gewordene «Efail»-Sicherheitslücke gezeigt. Denn diese ermöglicht es Cyberkriminellen, eine E-Mail auf dem Versandweg abzufangen und zu manipulieren. Dabei kann nämlich die Verschlüsselung ganz einfach umgangen werden, indem die Anhänge verändert und so der Inhalt der Nachrichten im Klartext ausgelesen werden kann. Von Efail sind aktuell die Verschlüsselungs-Plug-ins nahezu aller gängiger Mailprogramme betroffen, also beispielsweise Thunderbird, Apple Mail oder Outlook.

Bei «Open PGP S/MIME» werden jeweils Schlüsselpaare samt Passwörtern für den jeweils verwendeten Mail-Account erstellt. Dabei gibt es jeweils einen privaten und einen öffentlichen Schlüssel, der auf einem Server abgelegt wird. Der Empfänger muss dabei ebenfalls ein Schlüsselpaar erstellen und einen öffentlichen Key hochladen. Das nennt sich dann asymmetrische Verschlüsselung. Dieser Vorgang muss mit jedem externen Kommunikationspartner separat durchgeführt werden.

Es wird also ein gewisses technisches Grundverständnis verlangt, das jedoch bei vielen Mitarbeitern nicht oder nur unzureichend gegeben ist – was in der Folge zu Nachlässigkeiten und dadurch Sicherheitslücken führen kann. Ausserdem ist das komplizierte Verfahren eher weniger geeignet, wenn nur einzelne E-Mails ausgetauscht werden sollen.

Ein weiterer Nachteil dieser Verschlüsselung ist, dass sich die Absicherung rein auf den Daten- und Informationsaustausch beschränkt. Sobald sich die Daten auf den jeweiligen Rechnern der Kommunikationspartner befinden, sind sie jedoch nicht mehr innerhalb der «sicheren Zone». Heisst: Jeder, der die Mails bekommt, hat die darin befindlichen Informationen für immer – und kann sie im Folgenden auch unverschlüsselt an Dritte weitergeben oder auf nicht abgesicherten Datenträgern abspeichern.

Der Kontrollverlust ist also vorprogrammiert. Ausserdem wird die Nachricht auf den jeweiligen Mail-Servern im Klartext abgelegt, ist also bei gezielten Cyberangriffen leichte Beute. Sämtliche Verfahren zur E-Mail-Verschlüsselung erfüllen demnach nicht die regulären Compliance-Anforderungen zum Schutz sensibler Daten und Informationen. Denn sie bieten weder eine volle Kontrolle über die Zugriffe, noch sind sie revisionssicher.

Virtuelle sichere Datenräume

Angesichts dieser Nachteile setzen daher immer mehr Unternehmen auf virtuelle Datenräume – hochsichere Plattformen zu einem kontrollierten Informationsaustausch. Innerhalb dieser Datenräume können Daten gespeichert, ausgetauscht, bearbeitet und je nach Bedarf für weitere ausgewählte Personen freigegeben werden. Als zentrale Funktion zur Informationssicherheit bieten diese Lösungen sehr umfangreiche Massnahmen, um vertrauliche Dokumente jederzeit zu kontrollieren, beispielsweise mit einem digitalen Wasserzeichen oder Information-Rights-Management, das die Dokumentenberechtigung so weit einschränken kann, dass ein Dokument zwar geöffnet, aber weder gedruckt noch gespeichert werden kann. Darüber hinaus werden alle Datenzugriffe revisionssicher dokumentiert, man sieht also zu jeder Zeit, wer Zugang zu welchen Informationen hat. So kann die Data Governance in Unternehmen effektiv umgesetzt werden.

Ein Unternehmen, das bereits auf diese Art des Informationsaustauschs setzt, ist die Schweizer Grossbank Credit Suisse. Diese hat sich zum Launch eines neuen Fonds-Produkts für einen virtuellen Datenraum von Brainloop entschieden, um vertrauliche Kundeninformationen sicher und vor allem Compliance-konform auszutauschen und zu bearbeiten. Um dabei sicherzustellen, dass auch wirklich nur die jeweils berechtigten Personen Zugang zu den vertraulichen Dokumenten haben, gibt es innerhalb des Systems einen separaten Datenraum für jede einzelne Transaktion – der darüber hinaus auch noch eigene Nutzerberechtigungen aufweist. Auf diese Weise ist ein sicherer und vor allem nachvollziehbarer Informationsaustausch sowohl mit internen als auch externen Mitarbeitern und Partnern gewährleistet – und erfüllt sämtliche gesetzlichen und internen Richtlinien. «

Porträt

Gabriel Gabriel
Managing Director, Brainloop Schweiz

Kontakt

gabriel.gabriel@brainloop.com
www.brainloop.com