Cryptshare
Making e-mail better

Presse-Information

Ein Ausblick auf 2019: Warum der europäische Datenschutz zum Exportschlager werden könnte

(Freiburg im Breisgau, 11.12.18) Aus astrologischer Sicht steht das Jahr 2019 ganz im Zeichen des Planeten Merkur, aus politischer Sicht werden Themen wie der Brexit die Agenda bestimmen. Und in der IT? Schon alleine wegen der Europäischen Datenschutz-Grundverordnung war 2018 ein bedeutendes Jahr. Im Zusammenhang damit wird 2019 von einigen Geldbußen die Rede sein. Vor dem Hintergrund der in diesem Jahr bekannt gewordenen Sicherheitsvorfälle hat Apple-CEO Tim Cook vor Kurzem die DS-GVO ausdrücklich gelobt, während die ersten US-Bundesstaaten bereits neue strenge Gesetze erlassen haben. Der Datenschutz nach Vorbild der DS-GVO wird 2019 zum Exportschlager.

Es war kein Geringerer als Tim Cook, der vor wenigen Wochen die DS-GVO als Basis für einen weltumspannenden Datenschutz lobte. Der Weg zu einem besseren Datenschutz sei wie eine Reise, sagte der Apple-Chef – und auch die längste Reise beginnt bekanntermaßen mit dem ersten Schritt, möchte man hinzufügen. Einen langen Weg noch vor sich haben da die Vereinigten Staaten, die beim Schutz der Privatsphäre schon geradezu traditionell hinter Europa herhinken.

Doch nun kommt Bewegung in die Sache, Politik und Unternehmen in den USA sind aufmerksam geworden und suchen nach Lösungen. Nach europäischem Vorbild haben die US-Bundesstaaten Kalifornien und Vermont bereits neue Datenschutzgesetze erlassen. Ich nehme an, dass die Bundesebene in den USA nachziehen wird – und dass diese Datenschutzgesetze die IT-Branche und ihre Kunden nachhaltig beeinflussen werden. Als die DS-GVO im Mai endgültig in Kraft trat, endete eine zweijährige Übergangszeit – und damit die Schonfrist für Unternehmen und Behörden. Von Geldbußen, die wegen vermeidbarer Datenverstöße verhängt werden, wird 2019 einiges zu hören sein.

Präzedenzfall geschaffen

Ein Präzedenzfall wurde mit Artikel 25 der DS-GVO bereits geschaffen. Hier sind die Rahmenbedingungen formuliert, wie Unternehmen Datenschutz durch Technikgestaltung und Voreinstellungen („Privacy-by-Design“ und „Privacy-by-Default“) umsetzen müssen. Diese Grundsätze erfordern es, Daten, wo immer es möglich ist, anonymisiert beziehungsweise pseudonymisiert zu erheben und verschlüsselt zu verarbeiten. Keine leichte Aufgabe…

Während die DS-GVO in vielen Fällen bewusst vage vom „Stand der Technik“ spricht, so auch in Artikel 32 („Sicherheit der Verarbeitung“), fordert sie dort explizit die „Verschlüsselung personenbezogener Daten“. Damit ist natürlich nicht gemeint, dass Unternehmen nur noch über verschlüsselte E-Mails kommunizieren dürfen. Wohl aber, dass Faktoren wie der Schutzbedarf der Daten zu berücksichtigen sind. Die Verordnung bezieht sich ausschließlich auf personenbezogene Daten, aber auch andere vertrauliche Daten sollten diesen Schutz erfahren.

Die E-Mail ist tot, lange lebe die E-Mail

Und dennoch haben Forscher in diesem Jahr geraten, vorerst auf Verschlüsselung in E-Mail-Clients zu verzichten. Sie hatten die Verschlüsselung von E-Mail-Systemen ausgehebelt und Details über Sicherheitslücken in den beiden Verschlüsselungsverfahren PGP und S/MIME veröffentlicht. Unter bestimmten Bedingungen lassen sich E-Mails entschlüsseln, auch nachträglich.

Die Folgerung der Forscher – E-Mail sei kein sicheres Kommunikationsmedium – ist nichts Neues. Was zugleich die gute und die schlechte Nachricht ist. Im Prinzip entspricht eine E-Mail einer Postkarte: Sie ist günstig und schnell zuzustellen, ihr Inhalt ist aber für jeden lesbar und auch modifizierbar, der sie transportiert. Was auf dem Transportweg der einzelnen E-Mails passiert, welche Stationen beteiligt sind, bleibt den Anwendern verborgen. Auf Verschlüsselung in E-Mail-Clients zu verzichten, wäre also in etwa so, als ob man grundsätzlich seine Haustüre offenstehen lässt, weil es ohnehin zu viele Einbruchsdelikte zu beklagen gibt. Auch 2019 werden wir also nicht das Ende der E-Mail-Verschlüsselung erleben, warum auch?

Die Chefmasche bleibt „attraktiv“

Ziel der „Business E-Mail Compromise“ (auch „Chefmasche“, „Chefbetrug“ oder „CEO Fraud“) genannten Methode ist es, ein Unternehmen – genauer gesagt: einen Mitarbeiter – so hereinzulegen, dass Geld auf das Konto der Angreifer fließt. Dafür nutzen die Cyber-Kriminellen ganz gezielt die „Schwachstelle Mensch“ aus: Sie schlüpfen in die Rolle eines Vorgesetzten oder wichtigen Kollegen und senden Social-Engineering-Mails direkt an ihr vorher identifiziertes Opfer, um es zur Überweisung zu veranlassen.

Mehrere Aspekte machen die Chefmasche für Angreifer so „attraktiv“. Sie lässt sich relativ unkompliziert handhaben und ist mit vergleichsweise geringen Kosten verbunden, weil eine aufwändige Infrastruktur nicht nötig ist. Zwar können die Kriminellen nicht wie bei herkömmlichen Online-Betrugsfällen nach dem Gießkannenprinzip vorgehen, sondern müssen zuerst den besten Weg auskundschaften, um eine für das Opfer glaubhafte E-Mail überhaupt erstellen zu können – aber das lässt sich häufig schon mit einer ausgeklügelten Suchabfrage in sozialen Medien bewerkstelligen.

Zumal den höheren Vorabinvestitionen auch größere Gewinne gegenüberstehen: Das FBI, das diese Angriffsart seit Oktober 2013 beobachtet, beziffert den weltweit seitdem entstandenen Schaden auf über zwölf Milliarden US-Dollar – das ist noch einmal mehr als eine Verdopplung über die vergangenen eineinhalb Jahre. Und schließlich sind die Angriffe sehr schwer zu entdecken, weil die E-Mails ja eben keinen Schadcode enthalten, bei dem IT-Sicherheitslösungen Alarm schlagen könnten.

Sind Unternehmen all dem schutzlos ausgeliefert? Keinesfalls. Voraussetzung ist, dass sie die Art ändern, in der die Anwender kommunizieren. Die bisher bekannt gewordenen Vorfälle – bis hin zur aktuellen Warnung des BSI im Fall „Emotet“ – zeigen, dass die Sensibilisierung von Mitarbeitern für das Thema Cyber-Sicherheit in Form von regelmäßigen Schulungen unabdingbar ist, aber nicht isoliert betrachtet werden sollte.

Passwort-Verwaltung wird einfacher

Das Internet ist seit langem aus unserem täglichen Leben nicht mehr wegzudenken, und stellt die Menschen doch vor große Herausforderungen. Man denke nur an die Verwendung von Passwörtern im Rahmen von Multi-Faktor-Authentifizierung.

Die gute Nachricht: Best-Practice-Methoden für Online-Sicherheit werden immer wichtiger. Die schlechte Nachricht: Das ist mit Aufwand verbunden, (zu) viele Benutzer leiden inzwischen an „Passwort-Ermüdung“. Sie müssen den Überblick über eine wachsende Anzahl von Online-Konten und Kennwörtern behalten. Die Folge sind unsichere Praktiken wie die Nutzung desselben Benutzernamens und Kennworts für mehrere Websites – oder das häufige Zurücksetzen von Passwörtern, was eine gern ausgenutzte Sicherheitslücke darstellt. In der Tat sind Passwort-Missbrauch und -Missmanagement die Ursache für die meisten Datenschutzverletzungen.

Ich glaube, dass neue Technologie-Ansätze künftig den Spagat schaffen und die Anwendung von Passwörtern beim Austausch verschlüsselter Nachrichten und Dateien deutlich vereinfachen werden.

Über Matthias Kess

Matthias Kess ist CTO der befine Solutions AG mit Sitz in Freiburg im Breisgau, die Kommunikationslösungen für Unternehmen entwickelt und vertreibt.

Über Cryptshare und Befine Solutions
Die inhabergeführte Befine Solutions AG entwickelt und vertreibt Softwarelösungen für Unternehmen, die damit ihre Prozesse unterstützen, optimieren und überwachen können. Hauptsitz und Entwicklungsstandort des im Jahr 2000 gegründeten Unternehmens mit über 50 Mitarbeitern ist Freiburg im Breisgau. Vertriebsstandorte gibt es in Großbritannien sowie den Niederlanden, eine Tochtergesellschaft in den USA.
Im Mittelpunkt steht Cryptshare, eine Kommunikationslösung für den sicheren Austausch von Informationen. Mit ihr lassen sich E-Mails und Dateien jeder Größe und Art ad-hoc austauschen – einfach und sicher, nachvollziehbar und kostengünstig. Sie ist in mehr als 1.400 Unternehmen in über 30 Ländern bei rund 3 Millionen Anwendern im Einsatz. Cryptshare wurde 2017 mit dem „Cybersecurity Excellence Award“ in der Kategorie „E-Mail Security“ ausgezeichnet.
Weitere Informationen finden sich unter www.cryptshare.com. Anwender können sich auch im Blog informieren.

Pressekontakt:
phronesis PR GmbH
Marcus Ehrenwirth, Marcus Wenning
Kobelweg 12 ¼
D-86156 Augsburg
Telefon: +49 821 444800
E-Mail: info@phronesis.de
Web: www.phronesis.de

Befine Solutions AG – The Cryptshare Company
Oliver Gäng – Chief Marketing Officer
Schwarzwaldstraße 151
D-79102 Freiburg im Breisgau
Telefon: +49 761 389130
E-Mail: oliver.gaeng@cryptshare.com
Web: www.cryptshare.com