SEPPMAIL

DATEVNET:
SICHERE E-MAILS FÜR RUND 50.000 NUTZER

DATEV eG setzt auf verschlüsselte E-Mail-Kommunikation mit SEPPmail

Wer heute noch Wirtschaftsdaten unverschlüsselt per E-Mail versendet, der handelt grob fahrlässig. Nicht nur aufgrund der Europäischen Datenschutz-Grundverordnung (EU-DSGVO), sondern weil es folgende Szenarien begünstigt: Unternehmen, die seit Jahren unverschlüsselt kommunizieren, bieten Kriminellen ihre sensiblen Informationen auf dem Präsentierteller an. Die Folgen können enorme finanzielle Schäden sowie Imageverluste durch Insidergeschäfte, Erpressungen und Nachteile gegenüber Wettbewerbern sein.

Aus diesem Grund legt die DATEV eG als Softwarehersteller und IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten höchsten Wert auf Datenschutz. Eine Lösung zur sicheren E-Mail-Kommunikation ist daher ein unverzichtbarer Teil der Sicherheitslösung DATEVnet.

Zugegeben, die oben beschriebenen Fälle sind rein hypothetisch. Unwahrscheinlich sind sie aber nicht, denn eine unverschlüsselte E-Mail hat den gleichen Sicherheitsstatus wie eine Postkarte. Gerade Branchen, die hochsensible Daten versenden und verarbeiten oder in denen Vertrauen eine zentrale Rolle spielt, setzen bereits auf E-Mail-Verschlüsselung und verlangen dies auch von ihren Partnern und Dienstleistern. In Zeiten digitaler Kommunikation ist für sie eine IT-Sicherheitslösung ohne zuverlässige E-Mail-Verschlüsselung nicht mehr ausreichend. Zudem kommt für alle Unternehmen eine weitere rechtliche Anforderung ins Spiel: Die DSGVO verlangt, alle personenbezogenen Daten nach dem Stand der Technik zu schützen. Für Unternehmen führt also kein Weg mehr an der Verschlüsselung vorbei.

Steigende Nachfrage erwartet

Damit die Sicherheitslösung DATEVnet stets auf dem aktuellen Stand der Technik ist und um Kunden und Mitgliedern aktuelle und interessante Dienstleistungen anbieten zu können, führt die DATEV regelmäßige Marktbeobachtungen durch. „Wir gehen davon aus, dass unsere Kunden aufgrund der EU-DSGVO vermehrt verschlüsselte Kommunikation nutzen werden“, sagt Christian Bachhuber von der Abteilung Kommunikationsprodukte bei der DATEV. Er ist dort für DATEVnet und die reguläre Aktualisierung verantwortlich. „Aus diesem Grund ist es für uns sehr wichtig, dass DATEVnet zum einen die standardisierten Verschlüsselungsverfahren wie S/MIME und OpenPGP unterstützt. Da Verschlüsselungsverfahren immer noch nicht im Mainstream angekommen sind, ist es für uns ebenfalls sehr wichtig, dass bereits die erste Kommunikation verschlüsselt ablaufen kann und die Lösung leicht zu bedienen ist. Wir suchten also eine benutzerfreundliche Lösung, die automatisch aus verschiedenen Verschlüsselungsverfahren das jeweils Beste auswählt.

Auf der CeBit in Hannover fiel uns SEPPmail mit seiner integrierten GINA-Technologie ins Auge.“ Die Lösung beherrscht alle gängigen Verschlüsselungsverfahren. GINA kommt dabei immer dann zum Einsatz, wenn zwischen zwei Parteien zuvor noch keine verschlüsselte Kommunikation etabliert werden konnte.

„Bereits auf der Messe haben wir beschlossen, die GINA-Technologe bei der nächsten Modernisierung in die Evaluation mitaufzunehmen“, sagt Bachhuber. „Tatsächlich konnten wir nichts Vergleichbares finden und haben uns für eine Kooperation entschieden.

E-Mail-Verschlüsselung leichtgemacht

Doch wie funktioniert die Verschlüsselung von E-Mails im Alltag? Bevor eine Nachricht das System des Absenders verlässt, durchläuft sie in jedem Fall die Appliance. Hat der externe Empfänger früher schon einmal eine E-Mail mit einem offiziellen S/MIME-Zertifikat gesendet, wurde der öffentliche Schlüssel oder „Public-Key“ automatisch ausgelesen und kann bei der nun anstehenden Verschlüsselung verwendet werden. Ist dies nicht der Fall, prüft die Appliance, ob ein PGP-Key eingeliefert und als vertrauenswürdig eingestuft wurde. Ist beides nicht der Fall, greift sie auf die sogenannte Domain- oder TLS-Verschlüsselung zurück.

Wenn der Empfänger überhaupt keine Verschlüsselung nutzt oder es sich um die erste sichere Kommunikation handelt, kommt die GINA-Technologie ins Spiel: Sie verschlüsselt die Nachricht und versendet sie als html-Anhang mit einer Träger-E-Mail.

Somit ist die E-Mail ausgeliefert und liegt vollständig auf dem Empfängersystem vor. Bei der DATEV wurde das Verfahren so implementiert, dass der Empfänger – nachdem er den Anhang geöffnet hat – einmalig dazu aufgefordert wird, sein Passwort festzulegen. Damit kann er auch künftige html-Anhänge auf jedem internetfähigen Gerät öffnen, das über einen Browser verfügt. Im GINA-Webportal wird seine Nachricht über eine sichere Verbindung im Hintergrund hochgeladen und entschlüsselt. So kann er die Nachricht samt Anhängen lesen und auch sofort verschlüsselt antworten. Die SEPPmail-Appliance wählt immer die bestmögliche Verschlüsselungstechnologie aus, weder Absender noch Empfänger nehmen diesen Vorgang bewusst wahr.

„Die Funktionen der neuen Lösung decken sich exakt mit unseren Anforderungen“, sagt Bachhuber. „Der besondere Vorteil ist, dass nicht beide Kommunikationspartner die gleiche Lösung einsetzen müssen. Ein weiteres wichtiges Kriterium für uns war ein deutschsprachiger und schneller Support, der flexibel auf Wünsche und Anfragen reagieren kann.“

Implementierung mit tatkräftiger Unterstützung

Die DATEV betreibt für DATEVnet mehrere Rechenzentren. In diesen entschied man sich, SEPPmail auf virtuellen Maschinen zu betreiben. In anderen Standorten sollten Hardware-Appliances eingesetzt werden. Die Implementierung wurde von lokalen IT-Teams der DATEV eigenständig in Kooperation mit dem Support durchgeführt. Ein neues IT-System in eine komplexe IT-Infrastruktur an verteilten Standorten zu integrieren, ist kompliziert. So gab es zunächst Performance-Einbußen: Das Portal war für den Anwender in der Implementierungsphase nur eingeschränkt zu bedienen. „Die Experten aus dem Support verstehen ihr Handwerk“, sagt Bachhuber. „Sie haben die Performance-Einbußen genau unter die Lupe genommen, die Ursache lokalisiert und eine schnelle Lösung dafür entwickelt. Mit einer Code-Anpassung war das Problem dann behoben.“

Geschützte E-Mail-Kommunikation von 50.000 Nutzern

Bereits heute haben rund 50.000 Nutzer von DATEVnet Zugang zu sicherer E-Mail-Kommunikation. In den Rechenzentren setzt DATEV auf virtuelle Maschinen, an anderen Standorten schonen die Hardware-Appliances die IT-Ressourcen vor Ort. Die Lösung ist sowohl für die Mitarbeiter von DATEV als auch für die Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten einfach zu bedienen. Die Lösung ist mit Blick auf eine steigende Bedeutung der E-Mail-Verschlüsselung im Zuge der EU-DSGVO so implementiert worden, dass sie leicht und flexibel skaliert werden kann. Die ersten Rückmeldungen von Kunden, die an der Pilotierung des Projekts teilgenommen haben, fallen allesamt positiv aus. „Aufgrund der positiven Rückmeldungen und der guten Erfahrung mit dem technischen Support denken wir bereits über erste Erweiterungen nach“, kommentiert Bachhuber das abgeschlossene Projekt.

FAZIT

Unverschlüsselte E-Mails machen es Kriminellen viel zu leicht, Unternehmen und Privatpersonen immensen Schaden zuzufügen. Die DATEV leistet mit DATEVnet einen Beitrag zum Schutz sensibler Daten. Tausende Nutzer von DATEVnet haben nun eine einfache Möglichkeit, verschlüsselt per E-Mail zu kommunizieren. Empfänger, die selbst nicht verschlüsseln, können mit der GINA-Technologie E-Mails auf sicherem Weg erhalten und auch ihrerseits verschlüsselt antworten. Die Auswahl der jeweils besten Methode übernimmt die benutzerfreundliche Lösung von SEPPmail vollautomatisch.
Sie lässt sich mit Blick auf die verschärfte Gesetzgebung durch die EU-DSGVO flexibel skalieren. Auch der Versand von vertraulichen Dateianhängen ist zu realisieren.