

## MITARBEITER KOMMUNIZIEREN MIT AUFTRAGGEBERN VERSCHLÜSSELT

### **TZM schützt Produktionsgeheimnisse mit sicherer E-Mail von SEPPmail**

Die Konstruktionen des Göppinger Engineering-Dienstleisters TZM sind entscheidend für den wirtschaftlichen Erfolg seiner Kunden. Vertraulichkeit spielt eine große Rolle und immer mehr Unternehmen fordern von ihren Dienstleistern, verschlüsselt zu kommunizieren. Sichere E-Mails sind daher für das Unternehmen kein Neuland. Seit 2017 setzt das Unternehmen auf die benutzerfreundliche Lösung von SEPPmail.



Der Engineering-Dienstleister TZM zählt zu den erfolgreichsten Unternehmen der Steinbeis-Gruppe. Die Kunden kommen vorrangig aus der Automobil-, Automatisierungs- oder Medizinbranche. Der Technologievorsprung, den TZM seinen Kunden bietet, ist für deren Erfolg in hart umkämpften Märkten essentiell. Daher kam es auch in der Vergangenheit immer wieder vor, dass Kunden zu bestimmten Themen nur verschlüsselten Datenaustausch akzeptierten.

Die Vorsicht ist verständlich, denn die Informationen in einer unverschlüsselten E-Mail sind ungefähr so sicher wie der Text auf einer Postkarte. „In diesen Fällen haben wir bisher auf eine TLS-Verschlüsselung gesetzt“, erklärt Sascha Hintz, Systemadministrator bei der TZM GmbH. „Das Protokoll ist sicher und kann von den meisten Verschlüsselungslösungen ohne großen Aufwand eingesetzt werden. In den letzten Jahren haben diese Anfragen allerdings zugenommen, so dass wir entschieden haben, unternehmensweit eine neue Lösung einzuführen.“

### **Arbeitsprozesse bitte nicht stören!**

Im Falle der TZM war vor allem wichtig, dass die neue Lösung einfach zu bedienen ist, denn nicht alle Mitarbeiter sind mit E-Mail-Verschlüsselung vertraut. Die Lösung muss sich also möglichst ohne steile Lernkurve in bestehende Arbeitsprozesse einfügen. Das gilt für die eigenen Mitarbeiter, aber auch die Kunden, mit denen vertrauliche Nachrichten ausgetauscht werden. Außerdem darf die Lösung den E-Mail-Verkehr mit Kunden, die gar keine Verschlüsselung einsetzen oder wünschen, nicht erschweren.

Aber auch mit diesen Kunden muss eine sichere Spontankommunikation möglich sein. Dabei sollte sichergestellt sein, dass sichere Kommunikation auch mit Kunden möglich ist, von denen bislang kein Schlüsselmaterial vorliegt. Ein weiterer wichtiger Punkt für die TZM: das Versenden von Anhängen. Zudem sollte die Lösung offizielle Zertifikate unterstützen. Diese Zertifikate bestätigen, dass der Absender einer E-Mail auch derjenige ist, als der er sich ausgibt, und dass der Inhalt der Nachricht nicht verändert wurde. Eine zertifizierte E-Mail beugt bestimmten Betrugsmaschen vor und sorgt beim Empfänger für Vertrauen.

### **E-Mail-Verschlüsselung ist Vertrauenssache**

„Mit diesen Anforderungen im Kopf haben wir uns dann die Aussteller auf der it-sa, der großen IT-Security-Messe in Nürnberg, angesehen“, sagt Sascha Hintz. „Von diesen Lösungen sagte uns die von SEPPmail am besten zu. Bereits am Messestand wurden konkrete Anforderungen der TZM besprochen und ein Proof of Concept erstellt.“

Mit einer sehr guten Vorbereitung kann die Implementierung der eigentlichen SEPPmail-Lösung schnell verlaufen: Vor der eigentlichen Installation hat TZM bei dem Schweizer Trust Service Provider (TSP) SwissSign 100 Zertifikate gekauft. Deren Vorteil: TZM kann diese Zertifikate über den eingebauten SwissSign Konnektor voll automatisch erstellen, erneuern und verwalten. Außerdem hatten die Administratoren von TZM bereits eine virtuelle Maschine für die SEPPmail-Lösung vorbereitet. Da SEPPmail seine Produkte über ein Partnernetzwerk vertreibt, kam ein qualifizierter SEPPmail Partner als Integrator zum Projekt hinzu. Sie erhielten einen Fernzugriff auf die bereits fertig eingerichtete virtuelle Maschine.



Zeitgleich standen die Administratorenteams telefonisch in Kontakt. „Diese Kombination hat einwandfrei funktioniert“, sagt Sascha Hintz. „Für das Vorbereiten der virtuellen Maschine haben wir einen halben Tag benötigt. Die Installation durch den qualifizierten SEPPmail Partner hat ebenfalls einen halben Tag in Anspruch genommen. Insgesamt war die Lösung also nach einem Arbeitstag einsatzbereit.“

#### **E-Mailverschlüsselung – unbemerkt eingeführt**

Die Umgebung bei TZM ist überwiegend virtuell. Zwei physisch voneinander getrennte Server im HA (High Availability)-Verbund stellen sicher, dass, auch wenn ein Server einmal ausfallen sollte, die Dienste der TZM ungestört weiterlaufen können. Das gilt auch für die virtuelle Maschine, auf der die SEPPmail-Lösung läuft. „Es war zwar bekannt, dass wir eine E-Mail-Verschlüsselung einführen wollten, aber die meisten Kollegen haben überhaupt nicht gemerkt, dass sich etwas geändert hat“, sagt Sascha Hintz. „Mit den meisten unserer Kunden haben wir vollkommen problemlos eine Domain-Verschlüsselung eingeführt.“ Die dafür notwendigen Zertifikate sind direkt in die Lösung integriert und können von TZM selbst verwaltet werden. Auch der Austausch mit Partnern, die andere Zertifikate verwenden, ist kein Problem. Insgesamt haben die meisten Mitarbeiter die Lösung gut angenommen. Für die weitere Steigerung der Akzeptanz und die einheitliche Umsetzung des Sicherheitskonzeptes hat TZM Schulungen für Angestellte geplant.

#### **Large File Transfer – aber bitte verschlüsselt**

Für den Versand von großen Datenmenge nutzt TZM die GINA-Technologie, die auch sichere Spontankommunikation ermöglicht. GINA schickt in dem Fall eine ~~Empfänger~~-E-Mail mit dem verschlüsseltem Inhalt der eigentlichen Nachricht als HTML-Container. Parallel erhält der Adressat ein Initialpasswort (z.B. per SMS) zum Entschlüsseln der Nachricht. Er registriert sich per Multi-Faktor-Authentifizierung über den E-Mail-Account und mittels Passwort. Der Empfänger öffnet den HTML-Container gibt sein Passwort ein, und die Nachricht wird automatisch im Hintergrund ent-schlüsselt. Der Empfänger kann seinerseits unmittelbar mit einer verschlüsselten Nachricht antworten, ohne selbst eine Software installieren zu müssen. Die benötigten Schlüssel und Zugangspasswörter werden von GINA automatisch erstellt und verwaltet.

#### **FAZIT**

Geht es um den Versand großer Anhänge, Die TZM suchte nach einer einheitlichen funktioniert GINA ähnlich. Die Daten werden und leicht zu bedienenden Lösung für die dann allerdings für den Adressaten auf dem E-Mail-Verschlüsselung. SEPPmail konnte Server zum Download bereitgehalten. Die mit seiner Lösung und glaubwürdigen GINA-Technologie gilt als besonders sicher, Referenzen überzeugen. Nach rund einem denn sollte ein Angreifer eine Nachricht Arbeitstag für Installation und Einrichtung abfangen, so kann er ohne Passwörter versendete TZM E-Mails bereits standard-nichts damit anfangen. Gelangt er an die mäßig verschlüsselt und signiert. Für seine Passwörter, so hat er keine Nachricht, die 80 Mitarbeiter kann der Engineering-Dienst-er entschlüsseln könnte. Die Lösung hat für leister bis zu 100 Zertifikate des Trust TZM noch einen weiteren Vorteil: Im Paket Service Providers SwissSign in Eigenregie „Secure E-Mail Gateway“ sind weitgehende verwalten. Das Unternehmen kann so flexibel Sicherheitsfunktionen enthalten. Fortschritt- neue Mitarbeiter mit Zertifikaten versorgen. liche Spam-Erkennungs- und -Filtermaß- Mit den meisten Kunden konnte sofort eine nahmen sowie eine leistungsfähige Anti-Vi- Domain-Verschlüsselung etabliert werden. ren- und Anti-Phishing-Engine durchsuchen Für Dateianhänge oder sichere Spontankom-munikation kommt die GINA-Technologie zum Einsatz.