SEPPMAIL

UNIVERSITÄT FÜHRT SECUREMAIL EIN

SEPPmail an TU Dresden genutzt

Die E-Mail ist als Kommunikationsmittel Nr. 1 aus dem Geschäfts- und Verwaltungsalltag nicht mehr wegzudenken. Dennoch schenken ihr viele Nutzer nicht ihr volles Vertrauen. So verschickt laut einer Studie des Digitalverbands Bitkom rund jeder Zweite (56 Prozent) keine vertraulichen und persönlichen Informationen oder wichtigen Dokumente per E-Mail. Die Nutzer sind skeptisch: Ist die E-Mail von einem vertrauenswürdigen Absender? Werden meine Informationen vielleicht mitgelesen? Auch die Angst vor Viren oder Trojanern, die ganze IT-Systeme lahmlegen, ist groß. Diese und weitere Gründe haben die Technische Universität Dresden dazu veranlasst, die Verschlüsselungslösung SEPPmail einzuführen.

Die Technische Universität Dresden ist eine der traditionsreichsten und dynamischsten Universitäten Deutschlands. Seit 2012 gehört sie zum Kreis der elf deutschen Exzellenz-Universitäten und zählt über 8.000 Beschäftigte sowie 35.000 Studierende aus 125 unterschiedlichen Nationen. Täglich machen sich an der Universität tausende E-Mails auf die Reise. Ein universitärer Alltag ohne E-Mail? Heutzutage kaum vorstellbar. Doch wie steht es um den sicheren Versand bei der täglichen E-Mail-Flut?

Gesetzliche Regelungen wie die EU-DSGVO sehen die E-Mail-Verschlüsselung bereits vor. Zusätzlich verpflichtet das Sächsische E-Government-Gesetz Organisationen „[f]ür die elektronische Kommunikation [...] Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden“ (§ 2 Abs. 1 Satz 3). Diese Vorgaben verstärkten den Wunsch der TU Dresden nach einem einfachen und vor allem sicheren E-Mail-Versand. Verschlüsselung ist hier das wirksamste Mittel, die elektronische Kommunikation zu schützen. Aus diesem Grund hatte die TU Dresden das Thema E-Mail-Sicherheit auf die Tagesordnung gesetzt und das Projekt „CrypTUD“ ins Leben gerufen.

Verschlüsselt kommunizieren – ein absolutes Muss

Im Rahmen des Projekts wurde nach einem Anbieter gesucht, der eine einfache und verschlüsselte Kommunikation per E-Mail mit Dritten ermöglicht. „Bei mehr als 40.000 Personen an der TUD, die täglich per E-Mail kommunizieren, war uns vor allem wichtig, dass die Lösung besonders benutzerfreundlich und einfach zu bedienen ist“, sagt Matthias Rack, Mitarbeiter im Sachgebiet Informationssicherheit und Koordinator des Projekts ‚CrypTUD‘. „Zudem sollte sie unabhängig vom Mailserver und -client und auch auf mobilen Geräten genutzt werden können.“

Die Entscheidung fiel schließlich auf den Secure Messaging-Experten SEPPmail. „Die Verschlüsselungslösung konnte sich im Rahmen einer produktneutralen Ausschreibung durchsetzen und überzeugte zudem mit der integrierten GINA-Technologie“, so Rack. Bei einer Installation in dieser Größenordnung durfte der laufende universitäre Betrieb auf keinen Fall gestört werden.

E-Mail-Verschlüsselung leichtgemacht

Die SEPPmail-Lösung ist jetzt seit einigen Monaten an der TU Dresden im Einsatz. Dank der Software ‚SecureMail‘ ist das Versenden und Empfangen verschlüsselter E-Mails komfortabler denn je.
„Weder der Absender noch der Empfänger müssen die Software auf ihrem Rechner installieren“, sagt Rack. „Der externe Absender benötigt dabei kein digitales Zertifikat. Er muss sich lediglich beim SecureMail-Portal registrieren und seine E-Mail mit dem gewohnten Browser über dieses Portal versenden.“ Der Sender schreibt in seinem Standard E-Mail-Client eine vertrauliche Mail, markiert diese mit dem ‚Vertraulichkeits-Flag‘ oder vermerkt im Betreff „[+securemail]“. Die Appliance prüft bei jedem Versand, ob ein Schlüssel oder eine Domainverschlüsselung für die Sendestrecke vorhanden ist. Wenn beim Empfänger keine der genannten Technologien verfügbar und die Mail als vertraulich gekennzeichnet ist, kommt die GINA-Technologie zum Einsatz.
Wurde eine Appliance installiert, die teilweise im Clusterverbund betrieben werden kann. Die Cluster gewährleisten den stabilen Betrieb der Verschlüsselungslösung.

„Die GINA-Technologie ermöglicht uns eine einfache verschlüsselte E-Mail-Kommunikation mit Dritten, die kein digitales Schlüsselmaterial besitzen, wie es z.B. bei Forschungs- und Kooperationspartnern oder bei Stellenausschreibungen häufig der Fall ist“, sagt Rack.

Der Empfänger der Mail erhält auf einem zweiten sicheren Weg ein Initialpasswort – meistens per SMS, möglich ist aber auch die Zustellung per Fax oder Telefon. Mit diesem Kennwort registriert er sich einmalig am SecureMail-Portal und wird aufgefordert, das Initialpasswort in ein eigenes zu ändern. Zur weiteren Absicherung und zum späteren Zurücksetzen des Passworts muss er außerdem eine Sicherheitsfrage auswählen und seine Antwort hinterlegen. Die E-Mail wird als entschlüsselter HTML-Anhang im SecureMail-Portal angezeigt. Der Empfänger kann Anhänge abspeichern, E-Mails archivieren, eigenes Schlüsselmaterial hochladen und seine bevorzugte Verschlüsselungsform einstellen. Diese kommt dann bei der nächsten Mail automatisch zum Einsatz. Im SecureMail-Portal kann er anschließend sofort auf die Mail antworten.

Seine Antwort wird TLS-verschlüsselt und sicher an den ursprünglichen Sender ausgeliefert. „Besonders wichtig ist diese Technologie für Forschungs- und Kooperationspartner der TUD oder für das onlinegestützte Bewerbungsverfahren. Diese Art der Datenübermittlung, bei der die E-Mail immer vollständig ausgeliefert und nicht auf der Appliance gespeichert wird, stellt eine bequeme und vor allem sichere Alternative zu sonst wesentlich aufwändigeren Verfahren dar. Für die TU Dresden war dieses Produktmerkmal ein sehr wichtiges Kriterium“, so Matthias Rack. Auch künftige Anforderungen der Universität, wie die Anbindung an die Public-Key-Infrastruktur (PKI) des Deutschen Forschungsnetzes (DFN-Verein), wurden bereits berücksichtigt.