

## E-Mail-Versand

### So finden Sie die für Ihr Unternehmen passende Verschlüsselungsstrategie

Über das Internet verschickte E-Mails sind wie Postkarten: Jeder, der den E-Mail-Verkehr einsieht, kann die Inhalte mitlesen. Aus diesem Grund verbietet sich der unverschlüsselte Versand von personenbezogenen Daten oder gar besonderer Arten personenbezogener Daten nach §3 Abs. 9 Bundesdatenschutzgesetz. Diese Grundregel wird leider in der Praxis häufig nicht befolgt. Der einzige Ausweg, der sich aus diesem Dilemma bietet, ist die konsequente Nutzung von E-Mail-Verschlüsselung.

Lesen Sie in diesem Artikel, welche Möglichkeiten der E-Mail-Verschlüsselung es gibt und welche Infrastruktur hier notwendig wird.

#### Diese Strategien gibt es

Für die Nutzung der Verschlüsselung muss in ihrem Unternehmen eine Verschlüsselungsarchitektur etabliert werden. Hier bieten sich grundsätzlich 2 Strategien an: End-to-End und zentral.

Beim **End-to-End-Ansatz** werden die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails sowie deren Verifikation auf dem lokalen Anwenderrechner durchgeführt. Jeder PC muss hierfür mit einem sicheren E-Mail-Client mit Verschlüsselungsfunktion ausgestattet werden. Die Fähigkeit zur Verschlüsselung bringt die Mail-Software entweder von Haus aus mit – wie etwa Microsoft Outlook – oder sie wird über Plug-ins nachgerüstet. In der Regel werden alle Mitarbeiter über eine zentrale Public-Key-Infrastruktur (PKI) mit eigenen und fremden Schlüsseln versorgt, die sie auf ihren PCs dezentral verwalten. Auf diese Weise ist es möglich, dass E-Mails durchgängig vom Sender zum Empfänger in geschützter Form versendet werden können – daher der Name „End-to-End“.

Bei einer **zentralen Lösung**, einem Secure-E-Mail-Gateway werden alle kryptografischen Vorgänge wie Verschlüsseln und Signieren vom individuellen Desktop-PC in ein dediziertes „E-Mail-Gateway“ verlagert. Dieses befindet sich dabei an zentraler Stelle im Unternehmensnetzwerk und wird entweder als eigenständiger Server oder als Aufsatz für vorhandene E-Mail-Server eingesetzt. Im Gegensatz zu einer End-to-End-Lösung nimmt ein sicheres E-Mail-Gateway alle wichtigen kryptografischen Vorgänge für Mitarbeiter und bestimmte Nutzergruppen vor: Es verschlüsselt und signiert ausgehende E-Mails und entschlüsselt und verifiziert den eingehenden E-Mail-Verkehr. Das alles erfolgt automatisch und einheitlich gemäß den Unternehmensrichtlinien.

#### End-to-End hat wichtige Nachteile

Bei der End-to-End-Verschlüsselung wird die notwendige Software auf jedem Client installiert. Daraus entsteht erheblicher Aufwand für Installation und Wartung. Außerdem müssen die betroffenen Mitarbeiter in der Nutzung der Software und über den Einsatz der

Verschlüsselungsverfahren geschult werden. Des Weiteren optimal arbeiten, da dieser nicht in die verschlüsselten E-Mails „hineinschauen“ kann.

Entscheidender Nachteil der End-to-End-Verschlüsselung ist sicherlich, dass die Unternehmensrichtlinien zur E-Mail-Verschlüsselung nur schwer umzusetzen sind, da jeder Benutzer eigenverantwortlich über den Einsatz der Verschlüsselung entscheiden kann. Eine unternehmensweite Sicherheitspolitik lässt sich so nur schwer umsetzen.

### **Diese Vorteile bietet ein zentrales E-Mail-Gateway**

Über die zentrale Steuerung und Umsetzung der Unternehmensrichtlinien in einem E-Mail-Gateway wird dem einzelnen Benutzer die Entscheidung abgenommen, welche E-Mails nun zu verschlüsseln sind. Disziplinlosigkeit einzelner Mitarbeiter, Flüchtigkeitsfehler und Unachtsamkeiten beim Verschicken von vertraulichen Informationen werden somit ausgeschlossen. Des Weiteren reduziert sich durch die zentrale Verwaltung der Administratorkosten erheblich, auch weil eine Installation jeglicher Clientsoftware entfällt.

### **Welche Lösung ist die Richtige für Ihr Unternehmen?**

E-Mail-Gateways bieten sich vor allen Dingen bei größeren Unternehmen an, da hier der Installations- und Konfigurationsaufwand bei einer Vielzahl von Clients bei einer End-to-End-Lösung die Mehrkosten, die durch ein E-Mail-Gateway entstehen, schnell aufwiegt. Aber auch in Unternehmen, die aufgrund ihrer Tätigkeit häufig E-Mails mit vertraulichem Inhalt versenden, bietet sich eine solche Lösung an.

Gerade kleinere Unternehmen, bei denen nur von wenigen Arbeitsplätzen zu schützende Informationen versendet werden, sollten eine End-to-End-Lösung ins Auge fassen. Sprechen Sie mit Ihrer IT-Abteilung das Thema E-Mail-Verschlüsselung an und unterstützen Sie sie bei der Beschaffung eine adäquaten Lösung.

Die Firma PC KLINIK MOSEL, Traben-Trarbach bietet Ihnen eine fertige Lösung zur Implementierung in Microsoft Outlook. Lassen Sie sich unverbindlich beraten - [ehilgers@pcklinik-mosel.de](mailto:ehilgers@pcklinik-mosel.de)