Solution Brief

IDpendant
Secure your identity

Secure E-Mail

Vorteile

- Garantie der Authentizität und Integrität von E-Mails
- Entlastung der Mitarbeiter durch transparente Lösung
- Ende-zu-Ende-Sicherheit garantiert
- Keine Schulung der Mitarbeiter erforderlich
- Keine Software Installation notwendig
- Einfache Integration in Outlook, Lotus Notes, Mozilla usw.
- Kurze Integrationszeit
- Basierend auf Standards
- Anwender können individuell entscheiden, welche E-Mail signiert und/oder verschlüsselt werden soll
- Geringer Administrationsbedarf

Elektronische Kommunikation als strategischer Erfolgsfaktor

E-Mail ist heutzutage die mit Abstand am häufigsten verwendete Anwendung im Internet. Dabei lösen E-Mails die herkömmliche Kommunikation per Briefpost und Telefon mehr und mehr ab. Auch der Einsatz von Faxgeräten ist stark rückläufig. 107 Billionen E-Mails wurden Schätzungen zufolge im Jahr 2010 weltweit verschickt. Der Nachteil dabei ist, dass es bei E-Mails kein Briefgeheimnis und somit keine Vertraulichkeit bei der Kommunikation gibt.
E-Mails müssen auf ihrem Weg durch das weltweite Internet viele Stationen passieren, an denen sie abgefangen, von Unbefugten gelesen oder auch verändert werden können. An diesen Stationen und auf Servern werden alle E-Mails, darunter auch geschäftsrelevante, vertrauliche und somit schützenswerte Informationen, verarbeitet. Sensible Informationen können dadurch rasch in unbefugte Hände gelangen, wenn sie ungeschützt – das heißt ohne Mechanismen zur Absicherung – übermittelt werden. Wer eine E-Mail erhält, kann zudem nicht sicher sein, dass der Inhalt des elektronischen Briefes so empfangen wird, wie er vom Sender abgeschickt wurde. Wer sich unbefugten Zugang zu fremden Servern verschafft und E-Mails lesen kann, der kann auch deren Inhalt verändern und verfälschen. Dabei kann nicht nur der Text einer E-Mail verfälscht werden, sondern auch die Absenderangaben. Dadurch können falsche Identitäten vorgetäuscht werden, was verheerende Folgen haben kann.

Jedes Unternehmen ist ein potentielles Spionageopfer!

Hacker und Wirtschaftsspione haben es auf Internetverbindungen und auf lokale firmeneigene Netzwerke abgesehen. Da Geschäftsprozesse zunehmend elektronisch abgewickelt werden, ist es für Unternehmen und Institutionen essentiell, sensible Daten bei der Übertragung vor unbefugten Mitlesern und unerkannter Manipulation zu schützen.
Laut einer Studie zu Industriespionage von 2012 entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Im Vergleich zum Jahr 2007 entspricht dies einem Anstieg von 50 Prozent. Betroffen sind der Studie zufolge nicht nur Großkonzerne, sondern auch mittelständische Unternehmen. Das heißt: Jedes innovative und erfolgreiche Unternehmen, ob groß oder klein, ist ein mögliches Spionageopfer! So könnten etwa Ihre Mitbewerber ohne großen Aufwand die Kommunikation zwischen Ihnen und einer von Ihnen mit Patentanmeldungen beauftragten Person oder Institution abfangen. Dadurch geraten Ihre Unternehmensgeheimnisse und Ihr

IDpendant
Secure your identity

intellektuelles Eigentum in höchste Gefahr, wie der Fall Enercon zeigte.

Gesetzliche Anforderungen

Verstöße gegen Bestimmungen des Datenschutzes und des Steuerrechts sowie strafrechtlich relevante Verfehlungen können mit drastischen Bußgeldern sanktioniert werden. Für das Unternehmen verantwortliche Personen wie Geschäftsführer, Vorstände oder IT-Chefs können für Schäden persönlich haftbar gemacht werden. Bei besonders gravierenden Verstößen drohen im Extremfall sogar Haftstrafen. Darüber hinaus führt unzureichende IT-Sicherheit natürlich auch zu direkten Schäden wie Datenverlust oder Produktionsausfällen und nicht zuletzt zu Imageschäden, etwa wenn Sicherheitslücken in der Öffentlichkeit bekannt werden.

Sichere E-Mail-Kommunikation

Zur lückenlosen Ende-zu-Ende E-Mail-Sicherheit haben sich Client-basierte E-Mail-Verschlüsselung und Signatur in zahlreichen Unternehmen bewährt und helfen Organisationen, jederzeit den Schutz personenbezogener Daten zu gewährleisten. Unter Ende-zu-Ende-Sicherheit versteht man das digitale Signieren und Verschlüsseln der elektronischen Post am Arbeitsplatz: Einerseits kann durch eine digitale Signatur der Verfasser einer E-Mail zweifelsfrei festgestellt werden. Andererseits kann der Empfänger überprüfen, ob die Daten auf ihrem Weg verändert wurden. Die Verschlüsselung sorgt dafür, dass nur der ausgewählte Empfängerkreis die Dokumente entschlüsseln und somit einsehen kann. Klassische Geschäftsprozesse im Internet werden dadurch verbindlich und vertraulich.

Secure Mail bietet:

- **Vertraulichkeit**
  Die Verschlüsselung mit bewährten und sicheren Kryptoalgorithmen sorgt für Vertraulichkeit der E-Mails.
- **Interoperabilität**
  Durch die Verwendung von Standards bei den Secure Mail-Lösungen (S/MIME, OpenPGP) wird die Interoperabilität der geschützten E-Mail-Kommunikation mit den jeweiligen Geschäftspartnern gewährleistet.
- **Manipulationsschutz**
  Anhand der digitalen Signatur kann der Empfänger einer E-Mail deren Integrität (Unverfälschtheit) überprüfen.
- **Identität**
  Die unbestreitbare und eindeutige Identifizierbarkeit des Absenders einer E-Mail gewährleistet die notwendige Verbindlichkeit im geschäftlichen Umfeld.
- **Benutzerakzeptanz**
  Zur Steuerung der gesamten Anwendung sind nur 2 Buttons in Outlook – Signieren und/oder Verschlüsseln – notwendig.

Die Lösung

IDpendant bietet mit Secure Email eine umfangreiche Komplettlösung inklusive Support für die Absicherung Ihrer E-Mail-Kommunikation. Die Lösung von IDpendant ist der einfachste Weg zur Implementierung einer organisationsweiten, einheitlichen E-Mail-Sicherheitsrichtlinie (Security Policy). Der Einsatz von Signatur und Verschlüsselung wird zuverlässig und konform mit den Unternehmensrichtlinien integriert und umgesetzt.

IDpendant GmbH
Edisonstraße 3
D-85716 Unterschleißheim

Telefon +49 89 3700 110-0
Fax +49 89 3700 110-10
info@idpendant.com