dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Sichere E-Mails

Dieses Merkblatt beschreibt die wichtigsten Massnahmen, um Informationen in E-Mails möglichst sicher zu versenden und zu empfangen. Ihre Daten schützen Sie am besten, wenn Sie die folgenden Punkte beachten:

1. Verhalten anpassen
2. Sicherheitsmassnahmen treffen
3. Vertraulichkeit gewährleisten

1 Verhalten anpassen

Das richtige Verhalten beim Bearbeiten von E-Mails minimiert Risiken wie Diebstahl von Identitätsdaten und deren Missbrauch sowie Malware-Befall. Mögliche Massnahmen sind:

- Sparsam mit der Bekanntgabe der eigenen Adresse umgehen
- Verschiedene Adressen für verschiedene Zwecke einrichten
- Keine Angaben über Benutzeridentifikationen, Passwörter, Konto- und Kreditkartennummern oder sonstige Zugangsdaten per E-Mail weitergeben
- Bei E-Mails mit unbekannten Absendern nie auf Links klicken oder Dateianhänge öffnen
- Sichere Passwörter wählen (Überprüfung mit dem Passwortcheck)
- Passwörter periodisch ändern

2 Sicherheitsmassnahmen treffen

Die Umsetzung der folgenden Sicherheitsmassnahmen erhöht den Schutz Ihrer Daten:

- Betriebssystem, E-Mail-Client und Drittanwendungen (zum Beispiel Adobe Reader, Browser, Flash Player und Java) regelmässig aktualisieren
- Spamfilter des E-Mail-Clients und des E-Mail-Providers benützen
- Sicherer Übertragungskanal (Transportverschlüsselung, TLS oder SSL) gemäss Informationen des E-Mail-Providers im E-Mail-Client aktivieren
- Virenschutz einrichten, aktuell halten und dem Programm das Scannen von E-Mails und Anhängen (inklusive zip-Dateien) ermöglichen
- PC-Sicherheit generell gewährleisten

3 Vertraulichkeit gewährleisten

Werden E-Mails ohne zusätzliche Sicherheitsmassnahmen versendet, können Unberechtigte sie mitlesen oder verändern. Mit den nachfolgend beschriebenen Möglichkeiten können Benutzerinnen und Benutzer mit unterschiedlichen Informatikkenntnissen Daten in E-Mails sicher übermitteln.

3.1 Anhang verschlüsseln

Ein praktischer Ansatz ist die Verschlüsselung des Anhangs ausserhalb des E-Mail-Clients, zum Beispiel einer Microsoft-Office-Datei (Word, Excel oder Powerpoint) oder eines 7-Zip-Archivs. Das Passwort kann per SMS oder Telefon an die Empfängerin oder den Empfänger übermittelt werden. Da bei diesem Verfahren Offline-Attacken möglich sind (beispielsweise durchprobieren von Passwörtern), muss ein langes Passwort verwendet werden (mindestens 20 Zeichen).

3.2 Zentrale Datenaustauschplattform benützen

Für die vertrauliche Übermittlung und den Empfangsnachweis stehen teilweise zentrale Plattformen für die sichere Übermittlung von Dateien zur Verfügung. Der Kanton Zürich bietet für die kantonale Verwaltung dafür beispielsweise WebTransfer ZH an.

3.3 E-Mails mit GPG / PGP verschlüsseln

Die Verschlüsselung mittels GNU Privacy Guard (GPG) / Pretty Good Privacy (PGP) bietet sich insbesondere für einen häufigen Datenaustausch an. Dazu muss auf dem jeweiligen Client die entsprechende Software installiert sein und der E-Mail-Client entsprechend konfiguriert werden.

1. Zusatzprogramm herunterladen und installieren
2. E-Mail-Client für die sichere Verwendung von GPG / PGP einrichten
3. Zertifikat respektive Schlüsselpaar mit dem Zusatzprogramm generieren
4. Öffentlichen Schlüssel bekanntgeben
5. Privaten Schlüssel geheim halten

Weiterführende Links

- Gpg4win – GNU Privacy Guard (Windows)
  Signieren und Verschlüsseln von Dateien, Ordnern und E-Mails (Installationsanleitung)
- GPG Suite (MacOS)
  Signieren und Verschlüsseln von Dateien und E-Mails (Installationsanleitung)
- Enigmail für Thunderbird (Linux, MacOS und Windows)
  Signieren und Verschlüsseln von E-Mails

Die Verwendung von GPG / PGP innerhalb der öffentlichen Verwaltung ist mit den verantwortlichen Personen für die IT-Umgebung abzuklären.

3.4 E-Mails mit S/MIME-Zertifikat signieren und verschlüsseln

Neben GPG / PGP besteht mit S/MIME (Secure/Multipurpose Internet Mail Extensions) eine weitere Möglichkeit, um E-Mails zu verschlüsseln.

1. Zertifikat zum Signieren und Verschlüsseln beschaffen (zum Beispiel E-Mail-Zertifikat für S/MIME)
2. Zertifikat inklusive privatem Schlüssel in den E-Mail-Client importieren (Outlook / MacOS)
3. E-Mail-Client für die sichere Verwendung von S/MIME einrichten
4. Öffentlichen Schlüssel bekanntgeben
5. Privaten Schlüssel geheim halten

Der Zertifikatsanbieter Comodo beispielsweise bietet ein kostenloses Zertifikat zur E-Mail-Verschlüsselung für den privaten Gebrauch an. Der Einsatz von S/MIME innerhalb der öffentlichen Verwaltung ist mit den verantwortlichen Personen für die IT-Umgebung abzuklären.

3.5 Spezialisierte Anwendung für E-Mail-Signatur und -Verschlüsselung verwenden

Für grosse Benutzergruppen und bei einem Einsatz innerhalb einer öffentlichen Verwaltung können spezialisierte Anwendungen für das Signieren und Verschlüsseln von E-Mails verwendet werden. Diese oft zentralen Lösungen verringern den Aufwand für das Einrichten der Clients und die Verwaltung der Zertifikate oder Schlüssel (zum Beispiel Seppmail). Ein Einsatz ist mit den verantwortlichen Personen für die IT-Umgebung und den E-Mail-Server abzuklären.

4 Weiterführende Informationen

Weitere Informationen zu den Grundlagen der Verschlüsselung von E-Mails sind im Grundlagenwissen Verschlüsselung des Bundesamts für Sicherheit in der Informationstechnik (BSI), Deutschland, beschrieben.

Informationen zur sicheren Verwendung von GPG / PGP und S/MIME fasst beispielsweise der Artikel Efail: Was Sie jetzt beachten müssen, um sicher E-Mails zu lesen (Heise.de, Deutschland) zusammen.

V 1.3 / Juli 2018

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh