Merkblatt «E-Mail»

Die Kommunikation per E-Mail ist kaum mehr aus unserer Arbeitswelt wegzudenken. Sie ist rasch, einfach und billig. Leider ist sie aber nicht in jedem Fall sicher.

Entsteht ein Schaden, weil Sie die Sicherheitsvorgaben bezüglich E-Mail nicht eingehalten haben, können Sie dafür allenfalls disziplinarisch, zivil- oder strafrechtlich haftbar gemacht werden. Folgendes müssen Sie deshalb beachten:

Eile mit Weile!
E-Mail ist ein sehr «schnelles Medium» – ein Klick und Ihre Nachricht ist unwiderruflich weg! Immer wieder gelangen vertrauliche Mitteilungen in der Hast an einen ganz falschen Adressaten. Eine häufige Fehlerquelle liegt darin, dass Outlook Ihnen beim Eintippen der Adresse gleich Vorschläge macht. Überprüfen Sie deshalb stets sorgfältig – auch und gerade in hektischen Situationen –, ob Sie den richtigen Empfänger eingegeben (falls es mehrere sind, ob tatsächlich alle Informationen an alle diese Personen zu senden sind) und ob Sie die richtigen Dokumente beigelegt haben.

Der Adressat ist nicht immer der (einzige) Empfänger
Wenn Sie vertrauliche Daten per E-Mail übermitteln, müssen Sie stets bedenken, dass allenfalls das Sekretariat oder die Stellvertretung des Adressaten über eine Zugriffsberechtigung verfügt. Falls Drittpersonen keine Kenntnis der Daten erhalten dürfen, müssen Sie mit dem Adressaten Rücksprache nehmen oder einen anderen Kommunikationsweg wählen – etwa die «Persönliche/Vertrauliche» Briefpost.

Versand innerhalb des verwaltungseigenen Netzes
Das Versenden von E-Mails innerhalb des Netzwerks des Kantons gilt grundsätzlich als sicher. Ist der Empfänger ebenfalls am verwaltungseigenen Netz angeschlossen, dürfen Sie grundsätzlich auch besonders schützenswerte Personendaten unverschlüsselt übermitteln.

Endet die Adresse auf «@zg.ch», erfolgt die Zustellung intern, ohne dass das eigene Netz verlassen wird. Im folgenden Beispiel dürfen Sie Daten somit unverschlüsselt übermitteln:
peter.muster@zg.ch an max.beispiel@zg.ch

Der Versand zwischen kantonalen Stellen und solchen der Einwohnergemeinden ist nur dann sicher, wenn die E-Mail-Adresse auf «@*gemeindename*[1].ch» endet:
max.beispiel@zg.ch an peter.muster@huenenberg.ch

Nicht sicher ist der Versand hingegen etwa hier:
peter.muster@zg.ch an max.beispiel@schulen-huenenberg.ch (Grund: diese Adresse endet *nicht* auf «@*gemeindename*.ch»).

Versand via Internet
Unverschlüsselte E-Mail-Kommunikation via Internet – somit ausserhalb des verwaltungseigenen Netzes – gilt als weniger vertraulich als der Versand einer Postkarte. Auf dem Übertragungsweg sind E-Mails an vielen Orten für Dritte direkt einsehbar, werden kopiert und können verändert oder gelöscht werden. Deshalb dürfen Sie als Mitarbeitende der kantonalen Verwaltung keinerlei Personendaten *unverschlüsselt* per E-Mail über das Internet versenden.

Reine Sachinformationen – somit Informationen, die *keinerlei* Bezug zu einer Person haben – dürfen Sie unverschlüsselt per E-Mail verschicken. So etwa die Bekanntgabe von Öffnungszeiten oder der Hinweis auf Gesetzesbestimmungen.

Personendaten hingegen dürfen Sie über das Internet nur verschicken, wenn sie *korrekt verschlüsselt* sind. Ist die direkte Verschlüsselung von E-Mails und Anhängen in Ihrem E-Mail-System nicht möglich, können Sie Office-Dokumente, PDF oder WinZip-Ordner vor dem Versand mit einem Passwort verschlüsseln. Wichtig ist, dass Sie ein sicheres Passwort verwenden und dass Sie dieses dem Adressaten nicht per E-Mail, sondern via Telefon oder SMS mitteilen.

[1] Darunter fallen auch die Stadt Zug (@stadtzug.ch) und die Gemeinde Risch (@rischrotkreuz.ch).

So verschlüsseln Sie Dokumente

1. Einzelne oder mehrere beliebige Dokumente können Sie mit dem Programm WinZip wie folgt verschlüsseln:

Bei den Programmen finden Sie unter «Werkzeuge» das Programm WinZip. Öffnen Sie es, fügen Sie die zu verschlüsselnden Dokumente ein und sichern Sie den Ordner wie folgt:
Reiter «Extras» → «Archiv verschlüsseln». Bedenken Sie, dass der *Name* des WinZip-Ordners und die *Namen* der enthaltenen Dokumente für Dritte sichtbar sind (nicht aber der *Inhalt*). Der Dokumentenname darf daher nicht einen Hinweis auf den Inhalt des Dokuments geben (der Name des Dokuments darf somit nicht lauten «fristlose_Entlassung_Müller.doc», sondern etwa «HR_27NOV2013»).

2. Office-Dokumente (Word, Excel, PowerPoint)

Reiter «Datei» → «Informationen» → «Dokument schützen» → «Mit Kennwort verschlüsseln».

3. PDF

So speichern Sie ein Office-Dokument (Word, Excel, PowerPoint) als verschlüsseltes PDF ab:
Reiter «Datei» → «Speichern unter» → «Dateityp» als PDF auswählen → «Optionen» → «Dokument mit einem Kennwort verschlüsseln» ankreuzen.

Wenn Sie obige Sicherheitsmassnahmen einhalten, haben Sie grosse Gewähr, dass nur der berechtigte Adressat Kenntnis vom Inhalt erhält. Wenn es sich jedoch um ein Dokument mit vertraulichem Inhalt handelt, ist der Versand per Briefpost oder die persönliche Übergabe der elektronischen Zustellung vorzuziehen.

Ein ergänzender Hinweis, falls Sie die Anwendung «Web-Mail» des AIO nutzen:

Diese Anwendung verschlüsselt den Datenverkehr *zwischen dem Web-Mail Nutzenden und dem AIO*. Dadurch entspricht der Zugang auf das eigene E-Mail-Konto demjenigen an Ihrem Arbeitsplatz im Büro. Die vorstehenden Hinweise bezüglich des Versendens von E-Mails sind ebenfalls zu beachten.

Nachdem Sie sich beim Web-Mail abgemeldet haben, müssen Sie die temporär gespeicherten Dokumente und Informationen beim Internet-Explorer[1)] wie folgt löschen: unter «Extras»/Zahnradsymbol «Internetoptionen» anklicken, Reiter «Allgemein» wählen, unter «Browserverlauf» auf «Löschen» klicken, alle Optionen mit Häkchen versehen und auf «Löschen» klicken.

Erhalt von E-Mails

E-Mails können Schadprogramme enthalten und deshalb Risiken und Gefahren für Ihre IT-Umgebung, Ihren Computer oder Ihre Daten darstellen. Beachten Sie deshalb Folgendes:

- E-Mails von zweifelhafter Herkunft müssen Sie *ungeöffnet* löschen.
- *Ungeöffnet* löschen müssen Sie auch Beilagen und Bilder von zweifelhafter Herkunft.
- Bei verwaltungsexternen Anfragen per E-Mail haben Sie grundsätzlich *keinerlei* Gewissheit über die Identität des Absenders, da der Sender die Informationen über seine Identität problemlos beliebig selber definieren kann. Im Zweifelsfall müssen Sie beim angegebenen Absender telefonisch nachfragen.
- Selbst wenn Ihnen der verwaltungsexterne Absender bekannt ist, müssen Sie bezüglich Beilagen vorsichtig sein, da dessen System bzw. dessen Infrastruktur durch Schadprogramme infiziert sein kann.

Vorgehen bei Abwesenheit

- Sie müssen Absender von E-Mails mit einer automatischen Antwort über Ihre Abwesenheit informieren und angeben, an wen man sich während Ihrer Abwesenheit wenden kann.
- Das automatische Um- oder Weiterleiten sowohl an externe wie auch an interne E-Mail-Adressen ist nicht gestattet. Soll Ihr Outlook-Kalender oder Ihr Post-Eingang bei Abwesenheit durch Ihre Stellvertretung geführt werden, darf dies nur nach *vorgängiger* Absprache zwischen Ihnen und Ihrer Stellvertretung über die Outlook-Freigabefunktionen auf genau bezeichnete Ordner geschehen.

[1)] Falls Sie den Firefox im Einsatz haben: Wählen Sie den Menüpunkt «Extras» (oder bei neueren Versionen «Chronik») und wählen Sie «Neueste Chronik löschen», wählen Sie «Alles löschen» und klicken Sie auf «Jetzt löschen».