Anregung

Die Verwaltung übernimmt untenstehende Tips bzw. erstellt einen Leitfaden für den Versand und den Umgang mit elektronischen Nachrichten (E-Mails).

Begrün(d)ung

Einige städtische Mitarbeiter packen beim Versand von E-Mails den kompletten Verteiler in die Adreßzeile (An/To bzw. Kopie/CC):

Damit bekommen nicht nur die Empfänger eine komplette Liste aller E-Mail-Adressen, sondern diese sind auch für Dritte wertvoll und für verschiedene Zwecke des Marketings, Phishing oder Spam verwertbar.

Die komplette Adreßliste landet **ohne weiteres Zutun** bei Dritten, wenn **einer** der Empfänger zum Beispiel

- Facebook oder andere soziale Netzwerke nutzt.
  Facebook hat Zugriff auf sämtliche Kommunikation, die im Smartphone rein und raus geht, und lädt bei Anmeldung zunächst das komplette lokale Adreßbuch auf seine Server.
- Android- und Apple-Smartphones nutzt, die „automatisch“ Daten „in die Cloud“ laden.
- sich eine Schadsoftware eingefangen oder sich eine „kostenlose“ Taschenlampen-App installiert hat, die in Facebook-Selbstverständnis E-Mail-Adressen zu Spam-Zwecken abgreifen und im Internet weiterverscheuern.

Die Installation von Antiviren- und sog. Sicherheitssoftware ist reines Schlangenöl[1], dad das einerseits die Angriffsfläche auf das Computernetzwerk erhöht und andererseits das Denken der Mitarbeiter nicht ersetzt, vgl. Phishing wie „*Hallo Herr Lederer, hier ist Schneidewind. Bitte 500.000€ überweisen an XY. Ganz dringend!*“

1 **Schlangenöl** (aus dem Englischen *snake oil*) ist die spöttische Bezeichnung für ein Produkt, das wenig oder keine echte Funktion hat, aber als Wundermittel zur Lösung vieler Probleme vermarktet wird.

Falls es bisher keine Leitlinien der Stadtverwaltung zum Umgang mit E-Mails gibt, wird zum Start folgendes angeregt. Andernfalls sollte folgende als *Best Practice* ergänzt werden:

(1) Der E-Mail-Versand mit mehreren Empfängern, davon mindestens einer extern (außerhalb von wuppertal.de), erfolgt grundsätzlich im Adreßfeld der *BCC/Blindkopie*. Im An/To-Feld wird die eigene E-Mail-Adresse eingetragen.

Die Empfänger erhalten damit eine Kopie der Nachricht, ohne daß ihre Adresse für die anderen angegebenen Empfänger sichtbar wird. Damit wird auch Diensten wie Facebook oder Spammern die komplette Empfängerliste vorenthalten.

Dies entspricht dem datenschutzrechtlichen Grundsatz der Datensparsamkeit.

Siehe dazu auch: Wikipedia, Header (E-Mail). https://de.wikipedia.org/wiki/Header_(E-Mail)#BCC

(2) E-Mails werden grundsätzlich im Textmodus versandt (kein HTML).

```
<table style=3D"FONT-SIZE: 12px; MAX-WIDTH: 512px; FONT-FAMILY: arial, sans-serif; WHITE-SPACE: normal; WORD-SPACING: 0px; TEXT-
TRANSFORM: none; FONT-WEIGHT: 400; COLOR: rgb(0,0,0); FONT-STYLE: normal; MARGIN: 0px auto; ORPHANS: 2; WIDOWS: 2; LETTER-SPACING:
normal; BACKGROUND-COLOR: rgb(255,255,255); font-variant-ligatures: normal; font-variant-caps: normal; -webkit-text-stroke-width:
0px; text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial" cellspacing=3D"0" cellp-
adding=3D"0" width=3D"512" bgcolor=3D"#ffffff" border=3D"0">
```

Ein Beispiel für eine Tabelle in HTML.

HTML ist bei vielen Büroprogrammen wie Microsoft Outlook oder Mozilla Thunderbird standardmäßig aktiviert. Es ist eine Auszeichnungssprache, die mittels Markierungen (engl. *tags*) versucht, Text in Tabellen oder verschiedenen Schriftarten/-größen zu formatieren. Spammer versuchen, wenig (Spam-) Text in viel HTML-Tags unterzurbringen und dadurch Antispamprogramme zu verwirren.

HTML ist kein E-Mail-Standard. Verwendete Schriftarten sind nicht auf jedem Computersystem installiert. Nachrichten mit HTML benötigen mehr Platz auf der Festplatte, mehr Energie zur Übertragung und zum Säubern (Antiviren- oder Antispamprogramme) und sind damit umweltschädlicher als Nachrichten aus reinem Text. Letztlich erscheint zum Beispiel eine mit Outlook geschriebene Nachricht

auf einem Computersystem, das E-Mails als reinen Text darstellt

immer mit 2 oder 3 Leerzeilen.

HTML ermöglicht das Fälschen von Internetadressen (URI, z.B. https://wuppertal.de). Der Klick zur (vermeintlichen) Verifikation des Bankkontos landet dann nicht bei sparkasse.de, sondern einer anderen (Phishing-) Website.

HTML ermöglicht auch das Verstecken von Zeichen, die beim Kopieren in die Zwischenablage aber mitkopiert werden. Wird zum Beispiel ein scheinbarer Link zu wuppertal.de mit einem zweiten „r“ kopiert und im Webbrowser eingefügt, wird die Seite „wupperrtal.de“ aufgerufen.

Ähnliches Beispiel: wuppertal.de ⟶ einmal kopieren und in ein Textprogramm einfügen.

(3) E-Mail-Knigge: Der ultimative Leitfaden für professionell wirkende E-Mails

⟶ https://blog.mailfence.com/de/the-ultimate-email-etiquette-guide-to-make-your-emails-professional/