LEITFADEN

VERHALTENSREGELN FÜR DEN SICHEREN UMGANG IM IT-UMFELD

sure[secure]

00 INHALT

01 SOCIAL ENGINEERING

Die Fälle von Social Engineering nehmen weiterhin zu. Deshalb: Sie sollten nicht jede Kontaktanfrage annehmen und nicht jede E-Mail sofort öffnen. Gesundes Misstrauen ist enorm wichtig! Kennen Sie die Person, die mit Ihnen in Kontakt treten möchte? Prüfen Sie die Fakten und beachten Sie das folgende Regelwerk:

- **Zuständigkeiten:** Leiten Sie telefonische Anfragen wie z. B. Presseanfragen an die zuständige Abteilung (z. B. Marketing) weiter bzw. verweisen Sie auf Ihre Führungskraft.
- **Unbekannte:** Seien Sie vorsichtig bei Ihnen unbekannten Personen und geben Sie keine internen oder vertraulichen Informationen an unbekannte Personen und unberechtigte Dritte weiter.
- **Standhaft bleiben:** Lassen Sie sich zu nichts überreden. Fallen Sie nicht auf Komplimente, übertriebene Höflichkeit oder Drohungen herein.
- **Öffentlichkeit:** Führen Sie in der Öffentlichkeit keine Unterhaltungen über interne Informationen mit Kollegen.

02 PASSWORT-DIEBSTAHL

Die Arbeit am PC beginnt häufig mit der Eingabe eines Passworts. Das soll den PC und das Unternehmensnetzwerk vor unbefugtem Zugang schützen. Gleiches gilt für weitere Anwendungen oder Tools. Diese Zugänge sind passwortgeschützt, damit nur Sie mit Ihrem Profil Zugang haben und deshalb sollten Sie gut auf Ihre Zugänge aufpassen.

- **Starke Passwörter:** Verwenden Sie zur Absicherung Ihrer Daten nur komplexe Passwörter, die aus Buchstaben, Ziffern und Sonderzeichen bestehen. Je mehr Zeichen Ihr Passwort hat, desto sicherer ist es. Ändern Sie Ihr Passwort regelmäßig (z. B. alle 3 Monate) und auf jeden Fall auch dann, wenn Sie glauben, dass das Passwort ausgespäht wurde.

- **Diskretion:** Geben Sie Ihr Passwort niemals an Dritte, insbesondere fremde Personen heraus – schon gar nicht via E-Mail oder Telefon.

- **Aufbewahrung:** Behalten Sie Ihre Passwörter am besten im Kopf. Benötigen Sie dennoch eine Gedächtnisstütze, achten Sie auf ausreichende Sicherheit oder nutzen Sie einen Passwortsafe: Denn Passwörter gehören nicht unter die Schreibtischunterlage oder unverschlüsselt auf Ihr Smartphone oder Ihren PC!

- **Eingabe:** Achten Sie bei der Passworteingabe darauf, dass niemand Sie beobachtet. Warten Sie mit der Passworteingabe, bis Sie unbeobachtet sind.

03 SICHERES PASSWORT

Nachdem Sie wissen, dass die Zugänge nur für Sie bestimmt sind: Es ist nicht nur wichtig, dass die Zugänge geschützt sind, sondern auch wie gut bzw. stark sie geschützt sind. Die Stärke eines Passwortes ist entscheidend für die Sicherheit der gesamten IT-Infrastruktur.

- **Passwortstärke:** Bilden Sie immer ein sicheres Passwort, das aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen besteht. Ein sicheres Passwort sollte mindestens 15 Zeichen lang sein.
- **Geheimhaltung:** Halten Sie ihr Passwort geheim und verstecken Sie es nicht an allgemein bekannten Plätzen (z. B. unter der Tastatur oder unter der Schreibtischunterlage).
- **Erraten verhindern:** Verwenden Sie keine personenbezogenen oder persönlichen Daten wie den Namen Ihres Haustiers.
- **Häufig Ändern:** Ändern Sie Ihr Passwort regelmäßig, am besten alle 3 Monate, und wenn Sie glauben, dass Ihr Passwort ausgespäht wurde.
- **Kein Standardpasswort:** Verwenden Sie für jede Anwendung ein anderes Passwort.

04 VIRENSCHUTZ UND PRÜFUNG

Beim Thema Virenschutz laufen einige Prozesse vollautomatisiert ab und die gesamte Umgebung wird regelmäßig auf Viren geprüft. Dennoch gibt es ein paar Punkte, die Sie beachten sollten. Handeln Sie hier gemäß dem Motto: Vorbeugen ist der beste Schutz.

- **Vertrauensfrage:** Verwenden Sie nur Software aus vertrauenswürdigen Quellen.
- **Im Notfall:** Im Falle einer Infizierung trennen Sie die Netzwerkverbindung oder schalten Sie Ihren PC ab. Bewahren Sie Ruhe und melden Sie den Vorfall umgehend. Wichtig dabei ist - lieber einmal mehr als einmal zu wenig melden.
- **Aufmersamkeit:** Achten Sie auf das Verhalten Ihres Gerätes. Verhält Ihr Gerät sich untypisch (Neustart ohne erkennbaren Grund, Bewegung des Mauszeigers oder untypisch langsame Verarbeitung) trennen Sie das Gerät vom Netzwerk und melden Sie dies.
- **Meldung:** Bei der Meldung eines Sicherheitsvorfalls ist es für die IT-Abteilung wichtig folgende Informationen zu erhalten:
  - Wer sind Sie?
  - Was ist passiert?
  - Wann ist etwas passiert?
  - Welche Systeme sind betroffen?

05 E-MAIL SICHERHEIT

Das Nadelöhr für einen großen Anteil an Cyber-Attacken sind E-Mails. Deshalb ist besonders wichtig darauf zu achten mit wem Sie kommunizieren. Beherzigen Sie folgende Regeln und führen Sie wenn möglich den BSI E-Mail Quick-Check durch:

- Kenne ich den Absender?
- Ist die Betreffzeile sinnvoll?
- Erwarte ich einen Anhang?

- **Spam-Mails:** Antworten Sie nie auf Spam-Mails, öffnen Sie in der E-Mail enthaltene Links oder Anhänge nicht und löschen Sie die E-Mail umgehend.

- **E-Mail Adresse:** Nutzen Sie Firmen-E-Mail-Adressen ausschließlich dienstlich.Je häufiger Sie Ihre E-Mail Adresse im Internet angeben, desto größer ist die Chance, dass Angreifer darauf aufmerksam werden.

- **Phishing-Mails:** Kennen Sie den Absender? Vergleichen Sie ihn mit der Absenderadresse im Header, ob es eine Übereinstimmung gibt oder es sich um ein Gewirr aus Zahlen und Buchstaben handelt? Oft finden sich in der Absenderadresse sowie in dem Text der Mail Rechtschreibfehler. Weitere Auffälligkeiten sind die anonyme Anrede, die Bitte um besondere Diskretion, die untypische Aufforderung zur Durchführung von Tätigkeiten (bspw. Durchführen von Überweisungen, Preisgabe von Informationen). Kennen Sie den Absender, rufen Sie Ihn im Verdachtsfall direkt an und bitten Sie um Verifizierung der Nachricht.

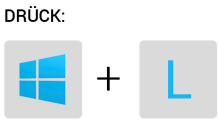
- **Virengefahr:** Öffnen Sie keine Anhänge oder Links unbekannter Absender. Da diese Schadcode enthalten können, leiten Sie die E-Mails auch nicht weiter. Melden Sie einen Verdacht der IT-Abteilung mit Nennung des Absenders, Betreffs und der Uhrzeit.

06 MOBILGERÄTE UND DATENTRÄGER

Jedes mobile Endgerät bietet Angreifern einen potenziellen Einstieg ins Firmennetzwerk. Mit diesem Wissen sollten Sie deshalb z. B. immer Ihren Bildschirm sperren, um das Risiko zu minimieren.

- **Backups:** Sichern Sie wichtige Daten stets im Netzlaufwerk. Lokal gespeicherte Daten gehen bei einem Verlust oder Defekt des Endgeräts verloren. Speichern Sie lokal nur Kopien der im Netzwerk vorhandenen Daten.

- **Zugangsschutz:** Schützen Sie Ihre Gerät vor einem Zugriff durch Dritte. Diese könnten in Ihrem Namen und mit Ihren Zugriffsrechten agieren und Informationen ausspähen oder dem Unternehmen schaden. Sperren Sie Ihre Endgeräte bei Inaktivität und beim Verlassen des Arbeitsplatzes.



- **Datenübertragung:** Lassen Sie nur kontrollierte Datenübertragungen zu. Schalten Sie insbesondere die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur dann ein, wenn Sie diese bewusst zur Kommunikation mit bekannten Geräten und Netzen nutzen.

- **Fremde Datenträger:** Es ist verboten Massendatenträger (USB-Sticks, Festplatten) die nicht freigeben wurden an Steuerung etc. anzuschließen. Es ist auch untersagt, Daten aus diesen Massendatenträger über nicht genehmigte Wege in das Netz zu transferieren. Geben Sie fremde Datenträger bei den Kollegen der IT Abteilung oder bei Ihrer Führungskraft ab.

- **Entsorgung:** Im Falle der Außerbetriebnahme eines Mobilgerätes oder Datenträgers geben Sie diese in der IT-Abteilung ab. Dort wird für die entsprechende Reinigung der Systeme oder die Vernichtung der Geräte gesorgt.

07

PRIVATE SOFTWARE IST NICHT ERLAUBT!

Grundsätzlich sollten Sie das Verwenden von privater Software oder nicht autorisierter Software unterlassen bzw. mit der IT-Abteilung abstimmen. Für die Nutzung von selektiver Software beachten Sie bitte die folgenden Punkte:

- **Richtlinien:** Beachten Sie die Verhaltensrichtlinien zur Verwendung von Software.
- **Lizenzen:** Lizenzrechtliche Voraussetzungen müssen erfüllt werden. Beim Nichtvorhandensein einer gültigen Lizenz drohen hohe Straf- und Schadenersatz-zahlungen.
- **Updates:** Installieren Sie aktuelle Sicherheitsupdates umgehend.
- **Umsicht:** Gehen Sie sicher, dass das produktive Netz nicht beeinträchtigt wird.

08 DATENVERLUSTE

Datenverluste können viele negative Auswirkungen mit sich ziehen. Dazu zählen neben hohen wirtschaftlichen Schäden auch häufig Imageverluste. Um solche Ausmaße zu vermeiden, beachten Sie folgende Punkte im Umgang mit Daten:

- **Umschreiben verhindern:** Speichern Sie die wichtige Daten im Dokumentenmanagementsystem (DMS). Dort wird automatisch eine Historie angelegt, sodass auch vorherige Versionen verfügbar sind
- **Herunterfahren:** Fahren Sie Ihren Computer immer ordnungsgemäß herunter. Ansonsten können Dateien, die gerade bearbeitet wurden, verloren gehen.

09 DER SCHUTZ VON SENSIBLEN DATEN

Dokumente welche sensible, personenbezogene oder geheime Daten enthalten können in den falschen Händen enorme Schäden anrichten. Achten Sie daher darauf diese Daten besonders zu schützen.

- **E-Mails:** Versenden Sie E-Mail-Anhänge mit sensiblen Daten nur in einer verschlüsselten passwortgeschützten ZIP-Datei.

IT-Security made with  in Willich

suresecure GmbH
Hausbroicher Str. 296D
47877 Willich

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de