SICHERE DIGITALE KOMMUNIKATION

LERNEINHEIT 2

Berufsschüler BOTTOM-UP! für IT-Sicherheit

DIE THEMEN:

1. Kommunikationspartner & -mittel
2. Datenschutz
3. Potentielle Gefahren
   > Phishing
   > Social Engineering
4. Maßnahmen zur Vorbeugung
   > Ende-zu-Ende-Verschlüsselung
   > Elektronische Signatur
5. Sicherheitstipps bei Websites und Weblogs

1. KOMMUNIKATIONSPARTNER UND -MITTEL

UNTERNEHMEN, ABTEILUNGEN,
MITARBEITER*INNEN

E-MAIL, FAX, TELEFON, POST, SOZIALE MEDIEN,
MESSENGER, WEBANGEBOTE

ÖFFENTLICHKEIT, KUNDEN, LIEFERANTEN,
INTERNE KOMMUNIKATIONSPARTNER

2. DATENSCHUTZ

Datenschutz spielt eine bedeutende Rolle bei der E-Mail-Kommunikation in und aus einem Unternehmen!

Personenbezogene Daten dürfen nur mit Einwilligung der Betroffenen übertragen werden!

Im Zweifel sollte eine ausdrückliche Einwilligung eingeholt werden.

ACHTUNG: E-Mail-Adressen können personenbezogene Daten sein! Beim Newsletter Versand muss daher darauf geachtet werden, dass die einzelnen E-Mail-Adressen nicht sichtbar sind.

> Empfänger im CC sind für alle sichtbar
> Empfänger im BCC sind für alle unsichtbar

3. POTENZIELLE GEFAHREN

SCHADSOFTWARE (VIREN, TROJANER, WÜRMER)

PHISHING (SPAM)

SOCIAL ENGINEERING

Virenschutzprogramme verwenden!

Aufmerksam sein!

Hilfe holen, wenn man auf Angriff hereingefallen ist!

3. POTENZIELLE GEFAHREN

UNBEKANNTE ABSENDER / ANHÄNGE

E-MAIL ABSENDER UNBEKANNT?

ANHÄNGE (INSBESONDERE .ZIP, .EXE, .DOC) BZW. LINKS IN DER E-MAIL?

Spam?
Phishing?

Anhänge und Links nicht öffnen!

Absender gegebenenfalls verifizieren!

E-Mail gegebenenfalls löschen!

3. POTENZIELLE GEFAHREN

PHISHING

ZIEL: DATEN VOM BETROFFENEN „ABFISCHEN“

KANÄLE: E-MAIL, TELEFON, SMS, FAX, DIREKTES GESPRÄCH

VORGEHEN DER ANGREIFER:
DRINGEND ERSCHEINENDE ANFRAGE KOMMUNIZIEREN
ZU GEFÄLSCHTER WEBSEITE HINFÜHREN
DATENEINGABE IM MOMENT DER EINGABE ABGREIFEN

OFT IN KOMBINATION MIT ANDEREN ANGRIFFEN,
Z.B. SOCIAL MEDIA, SPAM

3. POTENZIELLE GEFAHREN

SOCIAL ENGINEERING

ZIEL: ANGRIFF EFFEKTIVER DURCHFÜHREN

MENSCHLICHE BEZIEHUNG FÜR BETRUG AUSNUTZEN

VORGEHEN DER ANGREIFER:
VERTRAUTHEIT HERSTELLEN ODER VORTÄUSCHEN
VERTRAUTE PERSON, INSTITUTION ODER TECHNIK IMITIEREN
EXTREM GUTES ANGEBOT MACHEN

IMMER IN KOMBINATION MIT SCHADSOFTWARE ODER PHISHING

4. MASSNAHMEN ZUR VORBEUGUNG

1. TRANSPORTVERSCHLÜSSELUNG
2. VERMEIDEN VON ANHÄNGEN
3. ENDE-ZU-ENDE-VERSCHLÜSSELUNG DER INHALTE
4. NUTZUNG SICHERER PASSWÖRTER

4. MASSNAHMEN ZUR VORBEUGUNG

ENDE-ZU-ENDE-VERSCHLÜSSELUNG

ASYMMETRISCHE VERSCHLÜSSELUNG

> Schlüsselpaar: privater und öffentlicher Schlüssel

> Öffentlicher Schlüssel zum Verschlüsseln

> Privater Schlüssel zum Entschlüsseln

S/MIME

Zertifizierungsstelle und Zertifikate, breit unterstützt, teilweise kostenintensiv

PGP

Schlüsselweitergabe direkt oder über Schlüsselserver, Zusatzsoftware nötig

4. MASSNAHMEN ZUR VORBEUGUNG

ELEKTRONISCHE SIGNATUR

DIE ELEKTRONISCHE SIGNATUR ERLAUBT ES IM DIGITALEN SCHRIFTVERKEHR, VERBINDLICHKEITEN ZU SCHAFFEN.

EINFACHE ELEKTRONISCHE SIGNATUR

Name, Firma, Position etc., Authentizität und Unverfälschtheit jedoch NICHT garantiert

FORTGESCHRITTENE ELEKTRONISCHE SIGNATUR

mit asymmetrischen Verschlüsselungsverfahren signiert; Authentizität gewährleistet

QUALIFIZIERTE ELEKTRONISCHE SIGNATUR

Zertifikatinhaber Zertifizierungsstelle beglaubigt; Einsatz Hard- bzw. Software

5. SICHERHEITSTIPPS BEI WEBSITES UND WEBLOGS

Sichere Administration nutzen

+

Sicherheitsaktualisierungen einspielen

+

Regelmäßige Backups erstellen

SICHERE ONLINE-PRÄSENZ

Bottom-Up: Berufsschüler für IT-Sicherheit hat zum Ziel, die Mitarbeiter*innen von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittelständischen Unternehmen. **www.dsin-berufsschulen.de**

Bottom-Up: Berufsschüler für IT-Sicherheit ist ein Angebot von
Deutschland sicher im Netz e.V.
Albrechtstraße 10 / 10117 Berlin
www.sicher-im-netz.de

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:
DsiN Deutschland sicher im Netz

Initiative „IT-Sicherheit in der Wirtschaft“
Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unter-nehmen beim sicheren Einsatz von IKT-Sys-temen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.