SCHÜLERMAPPE

SELBSTLERNEINHEIT

Berufsschüler
BOTTOM-UP!
für IT-Sicherheit

LERNEINHEIT 2: SICHERE DIGITALE KOMMUNIKATION IM BERUFLICHEN KONTEXT

Um Kunden- und Mitarbeiterdaten, aber auch Firmenwissen vor **Manipulation** oder vor dem **Ausspähen** etwa durch die Konkurrenz zu schützen, ist Sicherheit in der Kommunikation sehr wichtig. **Vorbeugende Maßnahmen** und **umsichtiges Verhalten** in der Kommunikation aller Mitarbeiter*innen sind darum in Unternehmen von besonderer Bedeutung.

DIE THEMEN:

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter.

1. GRUNDLAGEN DER SICHEREN E-MAIL KOMMUNIKATION

E-Mails können verbindlich sein, solange es keinen gesetzlichen Formzwang gibt.

Kommunikation in Unternehmen gehört zum zentralen Alltagsgeschäft – mit Kunden, in der Öffentlichkeitsarbeit, aber auch unter Kollegen wird ständig kommuniziert. Dabei werden neben den herkömmlichen Kommunikationskanälen wie **E-Mail, Fax, Telefon und Post auch soziale Medien, Messenger und andere Dienste** wie geteilte Kalender oder Webangebote genutzt. Besonders die E-Mail hat sich in vielen Unternehmen als erster Kommunikationskanal zu Kollegen und Kunden, Dienstleistern etc. entwickelt. Zudem wird die E-Mail mittlerweile eingesetzt, um im Rahmen eines **Vertragsangebotes verbindliche Willenserklärungen** abzugeben. (Siehe auch die **einfache elektronische Signatur** unter 3.)

Personenbezogene Daten nur mit Einwilligung des Betroffenen übertragen.

Auf der anderen Seite spielt der **Datenschutz** eine wichtige Rolle beim Medium E-Mail. Es gilt grundsätzlich die Bedingung, dass personenbezogene Daten in Deutschland nur mit Einwilligung des Betroffenen übertragen werden dürfen. So gelten grundsätzlich strikte Bedingungen, unter denen man z.B. einen Newsletter an einen Empfänger überhaupt verschicken darf. Es verstößt auch gegen den Datenschutz, in einem Newsletter **ohne vorherige Einwilligung** der Personen deren E-Mail-Adressen für alle anderen Empfänger sichtbar zu machen (z.B. indem man alle Empfänger in das **cc-Feld** setzt). Ist sich das Unternehmen nicht sicher, ob die Empfänger diesbezüglich eingewilligt haben (was in der Regel nicht der Fall sein wird), bietet sich das **bcc-Feld** an – dabei sollte natürlich darauf geachtet werden, welche Empfänger-Adresse man ins cc-Feld setzt.

ANREGUNG

Überlegen Sie: Welche Kommunikationskanäle werden im Unternehmen genutzt? Welche davon intern und welche in der Außenkommunikation und Öffentlichkeitsarbeit?

LINK TIPP

Für weitere Informationen zum Thema Medienkompetenz in Sachen E-Mail Kommunikation, bietet der Medienführerschein Bayern weiterführende Informationen:

https://www.medienfuehrerschein.bayern.de/

Für alle Kommunikationskanäle gilt, dass ein Höchstmaß an Sicherheit notwendig ist. Denn Angriffe auf die Kommunikationsinfrastruktur von Unternehmen passieren häufiger als man annimmt.

Die Folgen können dramatisch sein: Wer die Kontrolle über seine geschäftliche E-Mail verliert und in Folge dessen selbst keine Geschäftspost mehr versenden kann, erleidet unter Umständen erhebliche **wirtschaftliche Schäden**. Wenn vom Unternehmen aus Schadsoftware und Spam verschickt werden, ist das ebenso geschäftsschädigend.

Schadsoftware ist eins der größten Probleme, dem Nutzer von Computern ausgesetzt sind. Unter dem Begriff Schadsoftware wird alle jene unerwünschte Software zusammengefasst, die dem Nutzer oder anderen Nutzern schadet: Viren, Trojaner, aber auch Spam oder Würmer. Viele Unternehmen werden mittlerweile Opfer von **Erpressersoftware**: hierbei verschlüsselt die Schadsoftware die Daten des Unternehmens auf dem Computer, und verlangt nach einer Lösegeldzahlung, um die Daten für den Nutzer wieder brauchbar zu machen.

Wichtiger Schutz: Antiviren-Programme.

Ein Großteil solcher Software wird effektiv durch aktuelle **Virenschutz-Programme** abgewehrt. Virenscanner und Spamfilter sollten nicht nur auf jedem Computer installiert sein, sondern sind Bestandteil des Serviceangebots von E-Mail-Anbietern und verrichten ihre Arbeit unsichtbar auf deren Servern. Es gibt aber immer wieder Momente, in denen Virenscanner und Spamfilter versagen, da ständig neue Arten von Spam oder Schadsoftware auftauchen. Darum ist es wichtig, die gebräuchlichsten Angriffsmethoden zu erkennen **(siehe auch hierzu Lerneinheit 1 – Grundeinstellungen für einen sicheren Arbeitsplatz).**

VERTIEFUNG: E-MAIL HEADER ERKENNEN UND AUSLESEN

E-Mail Header beinhalten viele Informationen, die beim Versand einer E-Mail über das Internet anfallen und protokolliert werden. Die Header werden Empfängern standardmäßig nicht angezeigt, man kann sie sich aber in jedem E-Mail Programm anzeigen lassen (zumeist über die Optionen für die jeweilige E-Mail). Vergleicht man eine E-Mail mit einem analogen Brief, so sieht der Empfänger (und auch der Absender) standardmäßig nur das Anschreiben (die E-Mail im Posteingang mit Absender, Betreff, Anschreiben). Der E-Mail Header stellt im Vergleich dazu den Umschlag dar, in dem das Anschreiben verschickt wird.

Der E-Mail Header beinhaltet neben Datumsstempeln und weiteren Informationen beispielsweise die IP-Adresse des Servers, von dem die E-Mail ursprünglich verschickt wurde. Diese IP-Adresse ist im Gegenzug zu den meisten anderen Angaben im Header von Spammern nicht fälschbar, und lässt so Rückschlüsse über die Quelle der E-Mail zu.

LINK TIPP

Genauere Informationen zum Auslesen von E-Mail Headern bieten die Seiten von Anti-spam e.V.:

https://www.antispam-ev.de/wiki/EMailHeader

Anhänge prüfen bzw. vermeiden

Schadsoftware per E-Mail: Entweder als Anhang oder Link.

Schadsoftware lässt sich in einer E-Mail nur in **zwei Formen** verstecken: Entweder ist sie als **Anhang der E-Mail beigefügt** oder es findet sich im **E-Mail-Text ein Link** zu einer Webseite, wo die Schadsoftware heruntergeladen wird. Wenn eine E-Mail aus reinem Text besteht und keine Anhänge hat, ist sie am sichersten (hierzu die Option „Nur Text“ im E-Mail-Programm wählen; im Gegensatz zu HMTL-E-Mails stehen damit viele bekannte Funktionen nicht zur Verfügung – z.B. Verlinkungen im Text).

Viele E-Mail-Programme blockieren mittlerweile **Anhänge** mit **Dateiendungen**, die in der Vergangenheit besonders anfällig und kritisch für einen **Schadsoftwarebefall** waren. Zu diesen Dateien gehören: **.ADE, .ADP, .BAT, .COM, .CPL, .EXE, .VBS, .WSC** (Liste unvollständig). Der Versand und Empfang dieser Dateien ist im alltäglichen Geschäftsverkehr für die meisten Mitarbeiter auch nicht relevant.

E-Mail-Anhänge im Geschäftsalltag.

Hingegen gibt es Anhänge mit Dateiendungen, die im geschäftlichen Alltag geläufig ausgetauscht werden – sei es nur unter Kollegen:

> Text- und Office-Dateien: .TXT ist in der Regel als sicher zu betrachten. Allerdings können Schadprogramme (wie bei allen anderen Dateien auch) eine .TXT-Endung vortäuschen - die Datei endet wirklich auf z.B.TXT.EXE. Dateien mit der Endung .PDF können in der Regel nur durch bestehende Sicherheitslücken im Adobe Reader gefährlich werden. .DOC(X), .XLS(X) und .PPT(X) können sogenannte Makroviren enthalten. Hier bietet sich an, Makros zu deaktivieren, oder sich die Dateien mit Programmen anzeigen zu lassen, die keine Makros unterstützen.

> Komprimierte Dateien: Dateien mit den Endungen .ZIP und .RAR werden oftmals zum Übertragen von Schadsoftware von Angreifern ausgenutzt.

> Bilddateien: .JPG und .GIF können potentiell mit Schadsoftware beladen sein.

E-Mail-Anhänge nur öffnen, wenn Vertrauenswürdigkeit sicher ist!

Zur Sicherheit sollte man sich die **Dateiendung vor dem Öffnen** der Datei im E-Mail-Programm oder im Dateisystem komplett anzeigen lassen. Des Weiteren sollten solche Anhänge vom Empfänger auch nur dann geöffnet werden, wenn der **Sender bekannt oder sorgfältig geprüft** wurde: Stammt die E-Mail wirklich von dem angegebenen Sender? Ist die Übersendung des Anhangs plausibel?

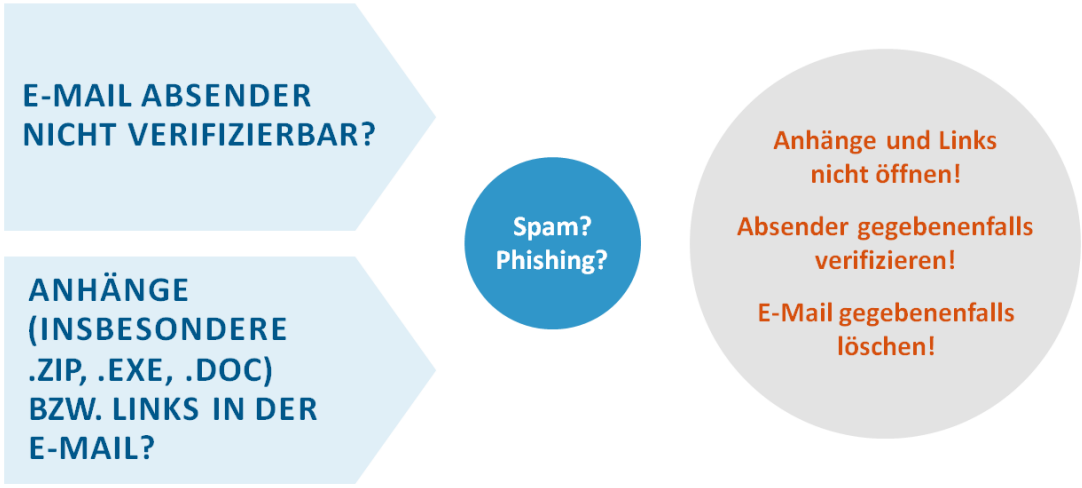
VERIFIZIERUNG VON ABSENDERN

Wie in der Infobox oben beschrieben, bietet der E-Mail-Header zusätzliche Informationen zum Ursprung der E-Mail und des Absenders. Da Absenderadressen leicht gefälscht werden können, bieten **elektronische Signaturen** (siehe Kapitel 3) zuverlässigere Möglichkeiten zur Verifizierung des Absenders einer E-Mail.

LINK TIPP

Die **eco Kompetenzgruppe E-Mail** bietet Best Practices für E-Mail Marketing an. Dabei dreht sich auch einiges um das Thema Sicherheit und Authentifizierung beim Versand von Massenmails.

https://e-mail.eco.de/wp-content/blogs.dir/26/files/eco_best_practices_fur_e-mail-marketing.pdf



2. PHISHING UND SOCIAL ENGINEERING

Phishing: durch Täuschung Wertsachen oder Informationen erschleichen.

Phishing: Diese betrügerische Methode ist sehr weit verbreitet und erstreckt sich über fast alle Kommunikationskanäle: **E-Mail, Post, Fax, Messenger, soziale Medien wie Facebook oder sogar im direkten Gespräch**. Hier geht es darum, den Betroffenen durch Täuschung Wertsachen oder Informationen zu entlocken. Das kann Geld sein, das können aber auch Informationen sein: **Passwörter, TANs, Geburtsdaten, Adressen oder vieles mehr**. Das Vorgehen der Angreifer ist immer ähnlich. Es gibt eine angeblich dringende Anfrage, mit der ein Handlungs- und Entscheidungsdruck beim Betroffenen erzeugt wird. Ziel ist es, das Opfer zu einer schnellen Entscheidung zu drängen, da ihm bei längerem Nachdenken der Betrug vermutlich auffallen würde. Gelingt das, werden die Betroffenen z.B. auf gefälschte Webseiten oder Apps gelockt und dort aufgefordert, **persönliche Daten oder Daten des Unternehmens mitzuteilen**. Die Daten werden dann durch verschiedene Techniken abgefischt und an den Betrüger umgeleitet.

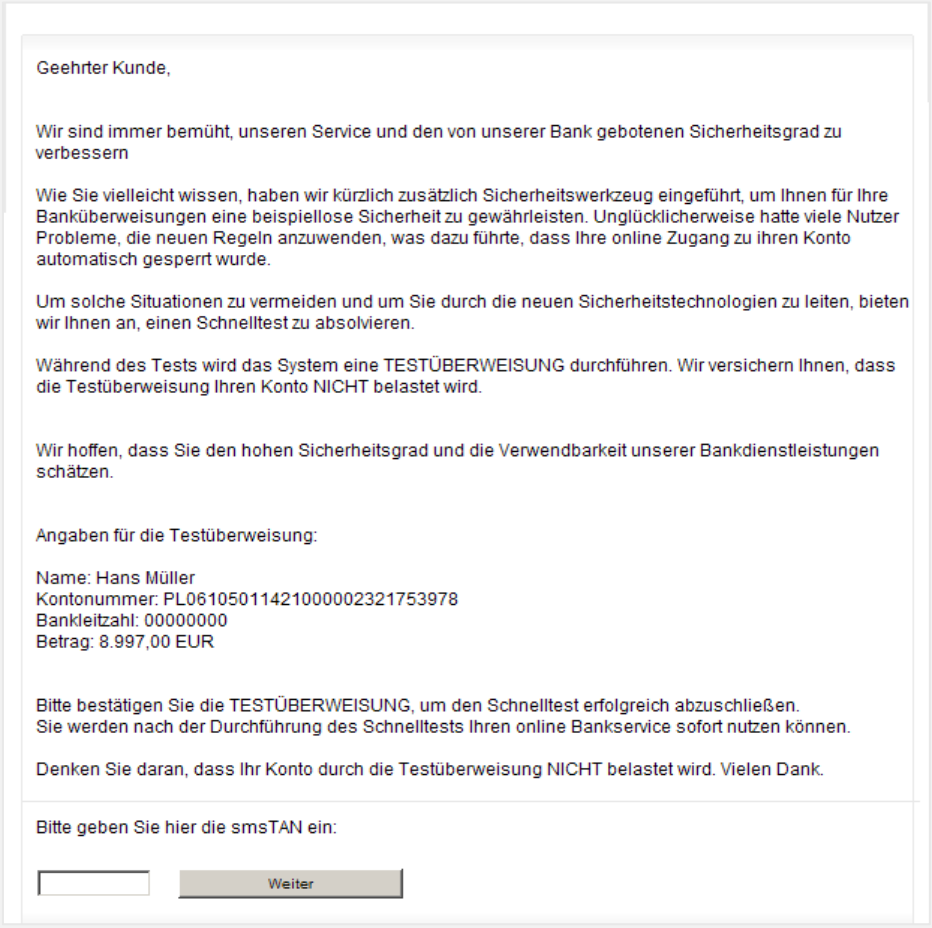
WENN SICH DER BETRÜGER ALS CHEF AUSGIBT

Hierbei spricht man von „CEO-Fraud“, „Fake President“ oder „Mandate-Fraud“. Betrüger schreiben gezielt E-Mails vermeintlich im Namen des Chefs und fordern darin eine Geldüberweisung. Dabei werden die betroffenen Mitarbeiter oftmals unter Zeitdruck gesetzt.

Betrüger recherchieren dafür im Vorfeld entsprechende Firmeninterna, und die auch über den Weg des Social Engineerings.

Phishing-Angriffe sind manchmal leicht zu identifizieren. Wenn man in einer **E-Mail einer fremden Bank in schlechtem Deutsch aufgefordert wird,** Bankdaten und Passwörter auf einer im Ausland registrierten Webseite einzugeben, sollte sofort klar sein, dass hier ein Betrug vorliegt. Erkennt man eine **Phishing-E-Mail**, ist die Gefahr durch **Löschen der E-Mail** schnell gebannt. Viele Phishing-Mails kommen dazu mit kompromittierten Anhängen (siehe unten).

BEISPIEL PHISHING-MAIL: ANGEBLICHE MAIL EINER BANK



Geehrter Kunde,

Wir sind immer bemüht, unseren Service und den von unserer Bank gebotenen Sicherheitsgrad zu verbessern

Wie Sie vielleicht wissen, haben wir kürzlich zusätzlich Sicherheitswerkzeug eingeführt, um Ihnen für Ihre Banküberweisungen eine beispiellose Sicherheit zu gewährleisten. Unglücklicherweise hatte viele Nutzer Probleme, die neuen Regeln anzuwenden, was dazu führte, dass Ihre online Zugang zu ihren Konto automatisch gesperrt wurde.

Um solche Situationen zu vermeiden und um Sie durch die neuen Sicherheitstechnologien zu leiten, bieten wir Ihnen an, einen Schnelltest zu absolvieren.

Während des Tests wird das System eine TESTÜBERWEISUNG durchführen. Wir versichern Ihnen, dass die Testüberweisung Ihren Konto NICHT belastet wird.

Wir hoffen, dass Sie den hohen Sicherheitsgrad und die Verwendbarkeit unserer Bankdienstleistungen schätzen.

Angaben für die Testüberweisung:

Name: Hans Müller
Kontonummer: PL06105011421000002321753978
Bankleitzahl: 00000000
Betrag: 8.997,00 EUR

Bitte bestätigen Sie die TESTÜBERWEISUNG, um den Schnelltest erfolgreich abzuschließen.
Sie werden nach der Durchführung des Schnelltests Ihren online Bankservice sofort nutzen können.

Denken Sie daran, dass Ihr Konto durch die Testüberweisung NICHT belastet wird. Vielen Dank.

Bitte geben Sie hier die smsTAN ein:

Weiter

Schwieriger sind solche Angriffe zu erkennen, wenn sie von einem Finanzinstitut kommen, das man selbst nutzt, und der Ton und die Gestaltung der E-Mail täuschend echt sind. Noch schwieriger wird es, wenn die Angreifer die Phishing-E-Mail auf die **Person des Betroffenen angepasst haben**: Beispielsweise im Namen von tatsächlichen Geschäftspartnern schreiben, sich als Firmenchef oder als Systemadministrator vorstellen. Werden dann noch verschiedene Kommunikationskanäle miteinander kombiniert, sodass die dringende Anfrage per Telefon und per E-Mail vorgetragen wird, ist die Wahrscheinlichkeit, darauf hereinzufallen, groß.

BEISPIEL PHISHING-MAIL: ANGEBLICHE SPARKASSEN-NACHRICHT

ANREGUNG

Überlegen Sie: Wen sollen Sie im Unternehmen im Falle von Phishing oder eines Schadsoftware-Verdachts informieren?

LINK TIPP

Weitere Phishing-Beispiele auf den Seiten des BSI unter

http://t1p.de/eh1s (verkürzter Link zum BSI)

Social Engineering ist die zwischenmenschliche Beeinflussung mit dem Ziel, bei Personen bestimme Verhaltensweisen hervorzurufen.

Wenn persönliche Informationen für den Betrug benutzt werden, spricht man vom **Social Engineering**. Dabei wird eine befreundete Person, eine Autorität oder eine Technik imitiert und die persönliche Situation des Betroffenen gezielt in die Planung des Angriffs einbezogen. Bekanntestes Beispiel für einen Social Engineering-Phishing-Angriff ist der sogenannte **Enkel-Trick** – und der funktioniert ganz und gar offline: Rentner werden ausgespäht und dann von ihren angeblichen Enkeln – den Betrügern – kontaktiert. Diese suggerieren, sie bräuchten ganz dringend eine hohe Summe Bargeld. Haben die Rentner gezahlt, sehen sie ihr Geld nie wieder.

Die **Opfer solcher Angriffe** schämen sich meist so sehr, dass sie keine Strafverfolgungsbehörden einbeziehen und nicht einmal Familienmitglieder informieren. Der Betrug bleibt dadurch oft unbemerkt.

Wer auf Phishing oder Social Engineering reingefallen ist, muss **schnellstmöglich Hilfe holen**. Informieren Sie Ihre Vorgesetzten und Kollegen, damit gegebenenfalls größerer Schaden abgewendet werden kann.

Allgemeine Informationen zu Phishing und anderen gefährlichen Nachrichten

Die nachfolgenden Informationen wurden aus den Schulungsunterlagen der Technischen Universität, welche im **Projekt KMU Aware** erarbeitet und vom Bundesministerium für Wirtschaft und Energie gefördert wurden, entnommen.

Internetbetrüger nutzen verschiedene Strategien, um Unternehmen zu schaden. Hierunter fallen beispielsweise die Verbreitung von Schadsoftware oder das Täuschen über E-Mails, um an sensible Informationen zu gelangen:

> Die Nachrichten fordern auf, mit verschiedenen sensiblen Daten wie Zu**gangsdaten** oder Kreditkartendaten zu antworten. Ziel der Betrüger ist es, an die geforderten Informationen zu gelangen und diese womöglich zu missbrauchen.

> Die Nachrichten fordern zu **Überweisungen oder Anrufen** auf, z.B. an vermeintliche Geschäftspartner.

> Die Nachrichten enthalten **einen oder mehrere gefährliche Links**. Ziel der Betrüger ist es hierbei, dass der Empfänger auf einen der Links klickt. Diese Links leiten ihn dann z.B. zu einer betrügerischen aber authentisch aussehenden Webseite, bei der er sich einloggen soll, oder zu einer Webseite, die ihm auf seinem Gerät Schadsoftware installiert. Solche Links müssen nicht einmal zur direkten Eingabe von Daten auffordern. Bereits Nachrichten, die lediglich auf Informationen hinweisen, können gefährliche Links enthalten. Also Vorsicht: Die **Angabe einer Webadresse als Link in der Nachricht kann manipuliert** sein. Daher ist es wichtig die tatsächliche Webadresse auch hinter diesem Link zu prüfen.

> Die Nachrichten enthalten eine **gefährliche Datei** (z.B. einen Anhang in einer E-Mail). Ziel der Betrüger ist es hierbei, dass der Nachrichten-Empfänger den Anhang öffnet bzw. ausführt, wodurch auf dem Gerät Schadsoftware installiert wird.

LINK TIPP

Video zum Thema Schutz vor Phishing von SECUSO:

https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/nophish/video/

7 REGELN, DIE HELFEN GEFÄHRLICHE NACHRICHTEN ZU ERKENNEN

Die Forschungsgruppe SECUSO (Security, Usability and Society) der Technischen Universität (TU) Darmstadt hat im Rahmen des Projekts KMU AWARE eine Schulungseinheit zur Sensibilisierung für Phishing entwickelt. Die Schulungseinheit kann über eine kostenfreie App sowie nach Registrierung auch über die gängigen Browser absolviert werden. Die nachfolgenden Regeln wurden aus einem der Flyer auf der Webseite entnommen:

1. Regel: Prüfen Sie Absender und Inhalt jeder empfangenen Nachricht auf Plausibilität (z.B. ob der Absender zur Nachricht passt, sensible Daten abgefragt werden oder Sie dort überhaupt ein Nutzerkonto haben). Ist die Nachricht nicht plausibel ist, löschen Sie diese!

- ✗ Der Absender shop@sye.jp ist bei einer Amazon E-Mail nicht plausibel.
- ✓ Der Absender rechnung@amazon.de ist bei einer Amazon E-Mail plausibel.

2. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen **Link enthält, prüfen Sie, ob es sich um eine gut gemachte betrügerische Nachricht handelt** und die Nachricht z.B. gar nicht vor dem (vermeintlichen) Absender stammt. Dazu müssen Sie zunächst herausfinden, welche Webadresse tatsächlich hinter dem Link steckt bevor Sie darauf klicken.

Die Information, welche Webadresse tatsächlich hinter einem Link steckt, ist je nach Gerät, Software und Dienst (z.B. Amazon, Dropbox, Skype, WhatsApp, Facebook, Google+, Xing, LinkedIn) an unterschiedlichen Stellen zu finden. Sie sollten sich also vor der Nutzung eines Geräts, einer Software bzw. eines Dienstes damit vertraut machen, wo die tatsächliche Webadresse eines Links zu finden ist. Ein Link kann meist daran erkannt werden, dass der Text blau hinterlegt und unterstrichen ist.

Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren ohne ihn aber zu klicken. Der Link wird entweder in der Statusleiste am Fuß des Fensters oder in dem Infofeld, welches auch Tooltip genannt wird, erscheinen.

Bei mobilen Geräten (Smartphones und Tablets) hängt das Vorgehen zum Identifizieren der Webadresse eines Links stark vom Gerät ab. Meist ist es so, dass Sie für mindestens 2 Sekunden mit dem Finger auf dem Link verweilen oder diesen für mindestens 2 Sekunden drücken. Achten Sie darauf, dass Sie den Link dabei nicht versehentlich klicken, d.h. kurz antippen. Dadurch wird die Webadresse oben einem Dialogfenster angezeigt.

3. Regel: Wenn Sie die Webadresse hinter dem Link gefunden haben, **identifizieren Sie als nächstes den sogenannten Wer-Bereich** in der Webadresse. Der Wer-Bereich besteht immer aus den letzten beiden Begriffen vor dem ersten alleinstehenden „/“ (in diesem Fall facebook.com) einer Webadresse.

Der Wer-Bereich ist der wichtigste Bereich für die Erkennung gefährlicher Webadressen und damit von betrügerischen Nachrichten mit Links. In der Fachsprache wird er Domain genannt. Falls hier zwei Zahlen stehen, handelt es sich um eine sogenannte IP Adresse und ist daher wahrscheinlich eine gefährliche Webadresse.

4. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, **prüfen Sie, ob der Wer-Bereich einen Bezug zu dem (vermeintlichen) Absender und/oder dem Inhalt der Nachricht hat** und ob er korrekt geschrieben ist. Wenn nur eines davon zutrifft, dann folgen Sie diesem Link nicht!

- ✗ http://shoppen-im-web.de/https://www.amazon.de/
- ✗ https://95.130.22.98/amazon.de.secure-login.de/
- ✓ https://www.amazon.de/shoppen-im-web/
- ✗ https://www.immobiliennscout24.de/
- ✓ https://www.immobilienscout24.de/
- ✗ https://www.mediarnarkt.de/
- ✓ https://www.mediamarkt.de/

5. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, Sie den Wer-Bereich aber nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen z.B. mittels einer Suchmaschine. Wenn Sie den Wer-Bereich nicht als vertrauenswürdig einstufen, löschen Sie die Nachricht!

- ✗ https://de-de.facebook-secured.com/
- ✓ https://de-de.facebook.com/

6. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen **Anhang** enthält, dann **prüfen Sie, ob dieser Anhang ein potentiell (sehr) gefährliches Dateiformat hat.** Potentiell (sehr) gefährliche Dateiformate sind:

> Direkt ausführbare Dateiformate (sehr gefährlich): z.B. .exe, .bat, .com, .cmd, .scr, .pif.

> Dateiformate, die Makros enthalten können: z.B. Microsoft Office Dateien wie .doc, .docx, .ppt,. .pptx, .xls, .xlsx.

> Dateiformate, die Sie nicht kennen.

7. Regel: Wenn das Dateiformat (sehr) gefährlich ist, dann **öffnen Sie den Anhang nur, wenn Sie diesen genauso von dem Absender erwarten.** Falls Sie unsicher sind, ob Sie die Nachricht einfach löschen können, sollten Sie weitere Informationen einholen. Dabei aber nicht die Kontaktmöglichkeiten aus der Nachricht verwenden. Rufen Sie z.B. den Absender an.

NOPHISH – SCHULUNGSEINHEIT VON KMU AWARE

Die Schulungseinheiten wurden innerhalb des vom Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative IT-Sicherheit in der Wirtschaft geförderten **Projekts KMU AWARE** entwickelt.

http://www.it-sicherheit-in-der-wirtschaft.de

https://www.secuso.org/schulung/

https://www.secuso.org/nophish/

Zu den Schulungseinheiten gibt es eigenständige Schulungsunterlagen zum Selbststudium und für Seminare, zum Teil in Lang- und Kurzfassung (NoPhish Lernkonzept). Bei erfolgreicher Absolvierung der NoPhish-Schulungseinheit kann ein **Zertifikat** erworben werden.

https://www.secuso.org

SECUSO SECURITY · USABILITY · SOCIETY

TECHNISCHE UNIVERSITÄT DARMSTADT

KMU AWARE AWARENESS IM MITTELSTAND

LINK TIPP

Die **SiBa-App** von DsiN informiert über neueste Bedrohungen durch Schadsoftware und Betrügereien, die z.B. durch neuartige Phishing-Mails verbreitet werden:

https://www.sicher-im-netz.de/ratgeber-tools-ratgeber-tools-fuer-alle/siba-aktuelle-meldungen

LINK TIPP

Das Onlinespiel zum Thema „E-Mail“ von Sichere Identität Berlin Brandenburg.

http://www.sichere-identitaet-bb.de/microsites/sicheriminternet/episode2/

3. E-MAIL UND MESSENGER VERSCHLÜSSELUNG

Neben einem aktuellen Virenschutz gibt es **vorbeugende Maßnahmen**, die eine **sichere Kommunikation unterstützen**. Dazu gehört die Abfrage von E-Mail in einem E-Mail-Programm statt im Webbrowser. **Im E-Mail-Programm** ist der Nutzer besser durch seinen eigenen **Virenscanner geschützt** und kann zusätzlich **Ende-zu-Ende-Verschlüsselung** komfortabel benutzen.

Transport-Verschlüsselung nutzen

Transport Verschlüsselung: E-Mail wird für den Transport verschlüsselt. Kann aber unverschlüsselt auf den Servern liegen.

Beim Einrichten des E-Mail-Accounts sollte unbedingt die **Transportverschlüsselung** (SSL/TLS) ausgewählt werden. Bei vielen E-Mail-Anbietern handelt es sich hier inzwischen um eine Standardeinstellung. Die **Transport-Verschlüsselung** beim Postausgang (SMTP) **sichert die E-Mail** nach dem Verlassen des Computers bis zum eigenen Mailserver ab. Von dort wird die E-Mail meistens verschlüsselt über andere Server bis zum Server des Empfängers weitergeleitet. Dort kann der Empfänger die Nachricht dann aus dem Posteingang seines Mailservers via IMAP oder POP3 auf seinen Computer herunterladen – wiederum verschlüsselt mit SSL/TLS.

Die TLS-Verschlüsselung gibt es nicht nur für E-Mail, sondern auch für Webseiten. Dort ist sie durch **https://** und ein **grünes Schloss** vor der Webadresse gut zu erkennen. Das bedeutet, dass die Daten, die der Nutzer auf der Webseite eingibt, verschlüsselt auf den Webserver übertragen werden und so **vor unbefugten Dritten geschützt** sind.

BEISPIEL

Wenn Can Yazar neues Material für die Firma im Internet bestellt, achtet er darauf, dass die Adresszeile im Browser mit https beginnt. So weiß er, dass die eingegebenen Rechnungsdaten nicht von Dritten mitgelesen werden können.

Ende-zu-Ende-Verschlüsselung der E-Mail-Inhalte

Ende-zu-Ende-Verschlüsselung: Die Nachricht ist während der gesamten Übertragung verschlüsselt und kann nur vom Empfänger wieder entschlüsselt werden.

Da eine E-Mail auf dem Weg zwischen verschiedenen E-Mail-Servern nur unzureichend vor Ausspähen geschützt ist, sollten **sensible Daten des Unternehmens nur Ende-zu-Ende verschlüsselt** oder alternativ auf dem Postweg versendet werden. Bei der Ende-zu-Ende-Verschlüsselung wird die E-Mail vom Sender auf seinem Rechner verschlüsselt. Entschlüsselt werden kann die E-Mail nur vom Empfänger persönlich, mit seinem individuellen privaten Schlüssel. Dritte können die E-Mail zwar abfangen, sie aber nicht lesen.

BEISPIEL

Ronny Ehrich kommuniziert für seinen Betrieb mit der Steuerberaterin Kathrin Jülisch. Die übergebenen Daten unterliegen dem Geschäftsgeheimnis und müssen unbedingt vor dem Zugriff Dritter geschützt werden. Ronny Ehrich wählt deshalb den sicheren Weg und verschlüsselt seine E-Mails an seine Steuerberaterin. Dafür hat sie ihm vorher den öffentlichen Teil ihres Schlüssels geschickt, mit dem er E-Mails an sie verschlüsseln, aber nicht entschlüsseln kann. Damit Kathrin ihm antworten kann, schickt er ihr auch seinen öffentlichen Schlüssel.

Es gibt **zwei Möglichkeiten**, Ende-zu-Ende-Verschlüsselung für E-Mail zu benutzen. **S-MIME und OpenPGP** sind zwei unterschiedliche, nicht kompatible Verfahren, die beide als sichere Verschlüsselung einzuordnen sind.

PGP steht für „ziemlich gute Privatsphäre“ (englisch: Pretty Good Privacy) und ist Software, mit der man seine E-Mails verschlüsseln kann. Um die Verschlüsselungsfunktion direkt im E-Mail-Programm nutzen zu können, müssen noch zusätzliche Programmerweiterungen installiert werden, die je nach genutztem E-Mail-Programm und Betriebssystem unterschiedlich sind. Das OpenPGP-Verfahren ist ein sogenanntes **asymmetrisches Verschlüsselungssystem**. Es basiert auf dem Prinzip, dass jeder Kommunikationsteilnehmer ein Schlüsselpaar besitzt, das aus einem **geheimen und einem öffentlichen Schlüssel** besteht. Die öffentlichen Schlüssel werden an die jeweils anderen Kommunikationspartner weitergegeben und dienen zum Verschlüsseln einer Nachricht (die öffentlichen Schlüssel werden z.B. im Anhang einer E-Mail verschickt, die vom E-Mail-Programm des Empfängers automatisch als Schlüssel erkannt und gespeichert werden). Nur mit dem zweiten, geheimen Schlüssel können die Nachrichten dann wieder entschlüsselt werden. **PGP unterstützt daneben auch digitale (elektronische) Signaturen** (siehe weiter unten). PGP erlaubt den Nutzern, ein eigenes „Web of Trust“ (Vertrauensnetz) aufzubauen, ohne dabei auf eine zentrale Authentifizierungs- oder Zertifizierungsstelle (vgl. S/MIME) angewiesen zu sein. Das Vertrauensnetz hat die gleiche Rolle wie die Zertifizierungsstelle bei der S/MIME-Verschlüsselung. Diese sollen garantieren, dass ein Schlüssel gültig (authentisch) ist, ohne dass man diesen selber signiert hat – also der Besitzer des Schlüssels wirklich die Person oder Institution ist, für die sie sich ausgibt.

Bei PGP beglaubigen die Nutzer untereinander die Vertrauenswürdigkeit eines Absenders.

BEISPIEL

Während Ronny Ehrich und die Steuerberaterin PGP einsetzen, benutzt Ayse Reinhard S-MIME. Beide können daher einander keine verschlüsselten E-Mails schreiben, denn PGP und S-MIME sind nicht kompatibel. Aber Ayse Reinhard weiß, wo sie sich informieren kann, um PGP zu installieren.

S/MIME steht für „Sichere/Multizweckmäßige Internet E-Mail Erweiterung“ (englisch: Secure/Multipurpose Internet Mail Extension) und ist auch ein **asymmetrisches Verschlüsselungsverfahren**, dass auf einem **öffentlichen und privaten Schlüssel** basiert. Der Hauptunterschied ist, dass die Schlüsselpaare vergleichbar wie bei der Transportverschlüsselung von einer **Zertifizierungsstelle** beglaubigt werden. Der öffentliche Schlüssel wird zu der Zertifizierungsstelle hochgeladen, die auf dessen Basis dann ein Zertifikat erstellt, das dann wiederum im Browser oder E-Mail-Programmen gespeichert wird. S/MIME hat dadurch zwar gegenüber PGP den Nachteil, dass dem Unternehmen Kosten durch die Zertifizierungsstelle entstehen, dafür wird die S/MIME Verschlüsselung von den meisten E-Mail-Programmen ohne zusätzliche Software unterstützt.

LINK TIPP

Mehr Informationen zum Thema E-Mail-Verschlüsselung findet sich in der Lehrbuchsammlung von Wikipedia „Wikibooks“:

https://de.wikibooks.org/wiki/Privacy-Handbuch:_E-Mails_verschlüsseln

Auf der Website des Informationsportals für Verbraucher „Verbraucher Sicher Online“ finden Sie weitere Erläuterungen und Installationshinweise:

https://www.verbraucher-sicher-online.de/thema/e-mail-verschluesselung

Die elektronische Signatur

Elektronische und digitale Signatur werden weitgehend synonym verwendet. Streng genommen bezieht sich die digitale Signatur auf ein kryptografisches Verfahren, während die elektronische Signatur ein rechtlicher Begriff ist.

Durch eine elektronische (digitale) Signatur können im Rechtsverkehr Verbindlichkeiten geschaffen werden, die gerichtlich leichter durchzusetzen sind. In den meisten Fällen reicht für die Abgabe von Willenserklärungen über E-Mail eine **einfache elektronische Signatur** aus, die keine besonderen Anforderungen stellt. Dies trifft z.B. bei Kaufverträgen und Angebotsannahmen zu.

Deswegen muss am Ende einer geschäftlichen E-Mail eine **gesetzlich vorgeschriebene Signatur stehen, analog zu einem Geschäftsbrief.** Abhängig von der Rechtsform der Firma müssen spezielle Angaben gemacht werde, wie etwa die Namen der Geschäftsführer und Aufsichtsratsvorsitzenden. Das gilt für alle E-Mails – egal ob an Geschäftspartner oder Kunden.

Elektronische Signatur in der Geschäftskommunikation gesetzlich vorgeschrieben.

Eine einfache elektronische Signatur sollte den **Namen des Unternehmens, den Ansprechpartner, die Adresse, eine Telefonnummer, E-Mail Adresse sowie Webadresse** beinhalten.

BEISPIEL

Qualifizierte elektronische Signatur: akkreditierte Zertifizierungsstelle plus Einsatz von Hard- oder Software.

Daneben gibt es auch die **fortgeschrittene elektronische Signatur sowie die qualifizierte elektronische Signatur**: beide Verfahren stellen die **Authentizität und Unverfälschtheit** der durch sie signierten Daten anhand asymmetrischer Verschlüsselungsverfahren sicher. Die fortgeschrittene elektronische Signatur (wie z.B. von OpenPGP unterstützt) kann von Empfängern jederzeit genutzt werden, um die Authentizität des Absenders zu überprüfen.

Bei der **qualifizierten elektronischen** Signatur muss zudem das zum öffentlichen Schlüssel zugehörige **Zertifikat** von einer **akkreditierten Zertifizierungsstelle** ausgestellt sein, die die **Identität des Zertifikatsinhabers** sicherstellt. Zudem kommt spezifische **Hard- bzw. Software** auf Seiten des Zertifikatsinhabers zum Einsatz. Diese Form der elektronischen Signatur kann damit die in Deutschland per Gesetz oder Verordnung geforderte notwendige Schriftform, die für einige Verträge und notarielle Beglaubigungen gilt, ersetzen.

LINK TIPP

Weiterführende Informationen zur elektronischen Signatur bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI):

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/elektronischesignatur_node.html

Messenger-Dienste und Verschlüsselung

Messenger-Dienste - zumeist als auf mobilen Endgeräten installierte Apps – haben über die vergangenen Jahre stark an Popularität gewonnen. Über die Dienste lassen sich Nachrichten inklusive Bildern/Videos und Anhängen an Kontakte verschicken. Der Vorteil zur klassischen SMS ist, dass **Messenger eine höhere Funktionalität** bieten, und der Versand bei einer bestehenden WLAN-Verbindung keine zusätzlichen Kosten für den Versender/Empfänger verursacht. Mittlerweile sind Messenger-Dienste weit verbreitet, und kommen auch geschäftlich zum Einsatz, beispielsweise für die **Terminkoordination mit Außendienstmitarbeitern**.

Auch die Kommunikation über Messenger sollte stets verschlüsselt stattfinden.

Die Mehrheit der Messenger-Dienste sind geschlossene Systeme (**Walled Gardens**): man kann nur mit Kontakten auf demselben Dienst kommunizieren. Mittlerweile gibt es allerdings Messenger, die anhand des **Open-Source XMP-Protokolls** (auch **Jabber** genannt) plattformunabhängig miteinander kommunizieren (**Federation**). Dies ist analog zur E-Mail, wo das SMTP-Protokoll ermöglicht, dass Kunden unterschiedlicher Provider sich E-Mails schicken können. Als Identifikator fungiert bei diesen Diensten nicht die Telefonnummer des Smartphones, sondern ein Nutzerkonto/Name, ähnlich einer E-Mail-Adresse. Dieser Identifikator kann dann wiederum auf allen XMPP-Clients (mobil sowie Desktop) zur Kommunikation genutzt werden.

LINK TIPP

Liste von XMPP-Clients:

https://de.wikipedia.org/wiki/Liste_von_XMPP-Clients

Ebenso hat die verschlüsselte Kommunikation über Messenger-Dienste an Aufmerksamkeit gewonnen. Eine **Ende-zu-Ende-Verschlüsselung** ist insbesondere bei der **geschäftlichen Kommunikation ratsam**. Die Mehrheit der geschlossenen Messenger-Dienste setzt dabei auf **proprietäre Infrastrukturen und Lösungen**, deren Sicherheit von außen nicht immer geprüft werden kann. Der Nutzer muss sich hier auf die Sicherheit des Systems verlassen. Die Open-Source Lösungen bieten hier wiederum XMPP-Clients und der OMEMO-Protokollerweiterung eine alternative. Für einige Dienste muss die Verschlüsselung erst **manuell aktiviert** werden.

LINK TIPP

Artikel über die Verschlüsselung von Messenger-Diensten auf Wikipedia:

https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern#Verschl.C3.BCsselung

4. WEBSITES UND WEB-BLOGS SICHER BETREIBEN

Websites sind eine gute Möglichkeit, mit Kunden in Kontakt zu treten und über die Tätigkeit des Unternehmens zu informieren. Aber auch hier gilt: Wenn die eigene Unternehmenswebsite nicht abgesichert ist, ist die **Reputation des Unternehmens gefährdet.**

Verschlüsselung der Übertragung bei Kontaktformularen auf der Unternehmenswebseite.

Zunächst sollte **der Zugang zum Server der Website sicher sein**. Waren früher ftp-Verbindungen üblich, sollte heute **mindestens ftp mit Transportverschlüsselung (s-ftp)** benutzt werden, um sich auf dem Server einzuloggen. Dabei ist selbstverständlich ein **sicheres Passwort für diesen Login** von besonderer Bedeutung (siehe auch Lerneinheit 1 für sichere Passwörter).

Es gibt viele Websites, die direkt über den Webbrowser administriert werden. Hier ist der **Schutz des Administratoren-Kontozugangs** elementar. Neben einem **sicheren Passwort** muss auch hier darauf geachtet werden, dass die Verbindung zur Administration der eigenen Website nur über **https://** ablaufen sollte. Viele Online-Dienstleister bieten **TLS-Zertifikate** an. Diese sollten von den Website-Betreibern unbedingt eingerichtet werden, so dass dann eine https://-Verbindung zur eigenen Seite möglich ist. Das **Telemediengesetz** fordert mittlerweile, dass Webseiten gegen Verletzungen des Schutzes von personenbezogenen Daten abgesichert sind. Somit müssen alle beruflich betriebenen **Webseiten**, die Besuchern die Möglichkeit geben, **personenbezogene Daten einzugeben**, mit einer **Verschlüsselung** für die Datenübertragung ausgestattet sein (für Kontaktformularseiten bietet sich HTTPS-Verschlüsselung an, für E-Mail TLS-Verschlüsselung).

Wer mit **Content Management Systemen (CMS)** arbeitet, sollte darauf achten, dass alle sicherheitsrelevanten Aktualisierungen immer schnellstmöglich eingespielt werden. Denn werden **Sicherheitslücken** einmal veröffentlicht, reichen teilweise schon wenige Tage oder Stunden, bis es zu Angriffen kommt. So könnte beispielsweise **Schadcode** auf der Website hinterlegt werden, der sich bei jedem Besucher installiert. Teilweise werden Websites aber auch dazu missbraucht, **Spam** zu verbreiten. Dazu werden oftmals die **Kommentarfunktionen** genutzt, die daher auch immer vor Spam abgesichert sein sollten.

Falls doch einmal etwas schief geht, liegt das Hauptaugenmerk darauf, Zugang zu den eigenen Daten zu behalten. Darum ist ein **regelmäßiges Backup** der Online-Präsenz für jedes Unternehmen unerlässlich (siehe auch Lerneinheit 3).

LINK TIPP

Die Initiative-S des eco Verband der Internetwirtschaft überprüft Unternehmenswebseiten auf Schadcodes hin:

https://www.initiative-s.de/de/index.html

QUIZ Q2

(Mehrfachnennung möglich)

Sie können das folgende Quiz alternativ auch in Form eines Online-Spiels direkt auf ihrem Smartphone oder Computer durchführen.

Das Online-Quiz ist verfügbar auf der Bottom-Up-Webseite:
https://www.dsin-berufsschulen.de/unsere-online-quiz.

1. Wie versende ich am besten Dokumente, die sensible Informationen enthalten wie beispielsweise Personaldaten?

A Über die Chatfunktion eines sozialen Netzwerks.
B Als komprimierten Dateianhang (z.B. .ZIP) per E-Mail.
C Per Briefpost oder verschlüsselter E-Mail (S-MIME oder PGP).

2. Wie kann ich mich gegen Social Engineering schützen?

A Den Virenschutz aktualisieren.
B Die Daten auf der Festplatte sicher verschlüsseln.
C Die Absender von Nachrichten auf Vertrauenswürdigkeit hin überprüfen.

3. Was ist der Vorteil einer Ende-zu-Ende-Verschlüsselung?

A Die Kommunikation ist nur vom Sender und vom Empfänger lesbar.
B Nur der Sender kann die E-Mail wieder öffnen.
C Ich bin effektiv gegen Phishing und Spam geschützt.

4. Was sind personenbezogene Daten?

A Daten, die nur von einer bestimmten Person eingesehen werden dürfen.
B Sensible Personendaten, die besonders schutzwürdig sind.
C Daten, bei denen man nachverfolgen kann, wer sie im System hinterlegt hat.

5. Für was dient das bcc-Feld einer E-Mail?

A E-Mail-Adressen in diesem Feld sind für die Empfänger nicht einsehbar.
B In dieses Feld wird der Betreff der E-Mail geschrieben.
C In dieses Feld kann ich Adressen schreiben, die ich sperren möchte.

6. Was mache ich mit dem Anhang einer E-Mail, deren Absender unbekannt ist?

A .ZIP- oder .EXE-Dateien im Anhang der E-Mail immer sofort öffnen.
B Auf keinen Fall öffnen, bevor der Absender nicht verifiziert werden kann.
C Im Zweifelsfall vorsorglich löschen, und den Absender nach erfolgreicher Verifizierung kontaktieren.

Lösung: 1 C, 2 C, 3 A, 4 B, 5 A, 6 B+C

BOTTOM-UP:
BERUFSSCHÜLER FÜR IT-SICHERHEIT

hat zum Ziel, die Mitarbeiter 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 mittleren Unternehmen.

www.dsin-berufsschulen.de

Bottom-Up 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:

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 mittlere Unternehmen beim sicheren Einsatz von IKT-Systemen 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.