SIE DÜRFEN DIESE PRÄSENTATION BELIEBIG NUTZEN UND VERÄNDERN.

HIER DIE DETAILS

- Design, Logos und Inhalte sind © by Mark Semmler GmbH.
- Sie dürfen die Präsentation insgesamt, in Teilen oder auch nur die Texte der Präsentation für beliebige Schulungs- und Informationszwecke nutzen:
  - Sie dürfen dafür das gesamte Material in jedem Format oder Medium vervielfältigen und weiterverbreiten (auch öffentlich).
  - Sie dürfen das gesamte Material beliebig bearbeiten, verändern und darauf aufbauen.
  - Dabei müssen Sie lediglich angemessene Urheber- und Rechteangaben machen und angeben, ob Änderungen am Material vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.

IT-SICHERHEIT FÜR PRIVATANWENDER

SO VIEL SCHUTZ MUSS SEIN!

Mark Semmler

DIE GRÖßTE VERWUNDBARKEIT IST DIE UNWISSENHEIT.

Sunzi

chinesischer General um 544 - 496 v. Chr.,
Militärstratege und Philosoph,
bekanntestes Werk: Die Kunst des Krieges

UM WAS GEHT ES?

- Hier finden hier einige grundlegende Maßnahmen, die Sie als Privatanwender mindestens ergreifen sollten, um Ihren Rechner und Ihre Informationen angemessen abzusichern.
- Ihr Computer ist nach der Umsetzung der Maßnahmen definitiv kein Fort Knox.
- Er ist aber so gut abgesichert, dass sich die allermeisten Angreifer die Zähne ausbeißen werden - und dass Sie im Falle eines Falles keine Daten verlieren und schnell wieder arbeitsfähig sind.

DAS WICHTIGSTE ZUERST: DATENSICHERUNG! (1/4)

- Ihr PC/Laptop/Smartphone/... wird ganz sicher irgendwann kaputt gehen und Ihre Urlaubsfotos und -videos, Ihre Briefe, E-Mails, Steuererklärungen usw. mit ins digitale Grab nehmen.
- In aller Regel geschieht dies zum denkbar ungünstigsten Zeitpunkt (Murphy's Law).
- Die erste und wichtigste Maßnahme für Ihre Sicherheit ist deshalb immer eine verlässliche Datensicherung!
- Es gilt folgendes Motto:

KEINE DATENSICHERUNG?
KEIN MITLEID!

DAS WICHTIGSTE ZUERST: DATENSICHERUNG! (2/4)

- Wählen Sie das richtige Sicherungsmedium.
  - Nutzen Sie für Ihre Datensicherung eigens dafür angeschaffte Datenträger.
  - Verwenden Sie nicht die lokale Festplatte ihres Rechners für die Datensicherung (Rechner tot → Daten und Backup weg!).
  - Verwenden Sie keine USB-Sticks für die Datensicherung (zu hohe Ausfallquote)!
  - Beste Lösung: (mindestens) eine externe USB-Festplatte.
- Führen Sie Datensicherungen in sinnvollen Abständen durch.
  - Was ist ein „sinnvoller Abstand“? Ganz einfach: Führen Sie immer dann eine Datensicherung durch, wenn Sie die Änderungen seit der letzten Datensicherung nicht mehr verlieren möchten.
  - Je nach Situation kann das einmal im Jahr oder sogar mehrmals am Tag sinnvoll sein (letzteres z. B. wenn Sie gerade an einer wichtigen Arbeit schreiben).
  - Empfehlung: Regelmäßige Sicherungen (z. B. im täglichen oder wöchentlichen Rhytmus) verhindern unliebsame Überraschungen.

DAS WICHTIGSTE ZUERST: DATENSICHERUNG! (3/4)

- Führen Sie (wann immer möglich) Vollsicherungen durch.
  - Vollsicherung: Ihre Datensicherung umfasst das gesamte IT-System (Daten, die installierten Programme, das Betriebssystem und sämtliche Konfigurationsdateien).
  - Mit einer Vollsicherung stellen Sie sicher, dass Sie nichts Wichtiges übersehen haben und dass Sie im Falle eines Falles schnell und relativ mühelos wieder arbeitsfähig sind.
- Sichern Sie alle wichtigen Speicherorte.
  - Sichern Sie alle IT-Systeme, auf denen sich wichtige Daten befinden (könnten) - vergessen Sie nicht Ihr Smartphone, Ihr Laptop, andere digitale Helfer und mobile Datenträger (CDs, DVDs, USB-Sticks, ...).
  - Wenn Sie Daten in der Cloud speichern oder Internet-Dienste nutzen (wie z. B. Webmailer oder Online-Speicher): Machen Sie auch von diesen Daten eine Datensicherung.

DAS WICHTIGSTE ZUERST: DATENSICHERUNG! (4/4)

- Heben Sie Ihre gesicherten Daten gut auf.
  - Trennen Sie die Sicherungsmedien nach der Datensicherung von den gesicherten Systemen (Stecker ziehen).
  - Bewahren Sie die Sicherungsmedien an einem geschützten Ort (Schublade, Schrank, Tresor, ...) auf.
  - Für ganz Vorsichtige oder für wirklich wertvolle Informationen gilt: Lagern Sie (mindestens) eine Kopie der Datensicherung außerhalb Ihres Hauses.
- Gehen Sie auf Nummer sicher.
  - Heben Sie nicht nur eine Sicherung auf, sondern mehrere Generationen davon. Falls eine Sicherung defekt sein sollte, sind Ihre Daten dennoch nicht (ganz) verloren. Zusätzlich haben Sie die Möglichkeit, auf verschiedene Versionen der gesicherten Daten zurückzugreifen.
  - Nutzen Sie mehrere Datenträger für die Datensicherungen.
  - Testen Sie, ob die Datensicherung auch wirklich funktioniert (kaputte Datensicherungen sind leider häufiger als Sie denken...), z. B. indem Sie auf Fehlermeldungen der eingesetzten Software für die Datensicherung achten.
  - Verschlüsseln Sie Ihre Datensicherung, wenn Sie vertrauliche Daten besitzen.

SICHERE PASSWÖRTER – SO GEHT'S EINFACH! (1/2)

- Unsichere Passwörter wie z.B. 123456, pAssw0rt, Liebe123 etc. können von Bösewichtern leicht erraten werden – oft mit fatalen Folgen!
- Aber auch das ist wahr:
  Komplizierte Passwörter werden schnell vergessen.
- Wie erstellt man sichere Passwörter, an die man sich garantiert erinnert? Hier eine Anleitung:
  - Denken Sie sich einen Satz aus, z.B. „Mein Hamster ist schon 3 Jahre alt."
  - Stellen Sie nun die Anfangsbuchstaben der Wörter, die Ziffern und Satzzeichen hintereinander (bei unserem Beispiel: MHis3Ja.)
  - Das Passwort ist sehr sicher, aber Sie werden es garantiert nicht vergessen - der Satz bleibt im Gedächtnis!

SICHERE PASSWÖRTER – SO GEHT'S EINFACH! (2/2)

- Nutzen Sie möglichst für jedes Konto ein eigenes Passwort. Wenn ein Angreifer ein Passwort von Ihnen erfährt, bleibt der Schaden begrenzt.
- Nutzen Sie (wenn möglich) Multi-Faktor-Authentifizierung (siehe nächste Folie).
- Wenn Sie sich viele Passwörter merken müssen, sollten Sie einen Passwort-Safe verwenden. Diese Programme heben Ihre Passwörter sicher auf und sie müssen sich nur ein Passwort (das für den Safe) merken. Ein sehr beliebter Passwort-Safe ist z. B. das Programm KeePass.
- Wenn Sie Passwörter in Ihrem Webbrowser speichern: Vergeben Sie ein Master-Passwort, damit Schadsoftware diese Passwörter nicht auslesen kann.

SICHERES EINLOGGEN DURCH MULTI-FAKTOR

- Passwörter haben viele, viele, viele Nachteile und sie gelten heute (zu Recht) als viel zu unsicher.
- Deshalb wurde die Mehr-Faktor-Authentifizierung (MFA) entwickelt.
- Das Anmelden erfolgt bei MFA mithilfe mehrerer voneinander unabhängigen Faktoren (in der Regel sind es zwei), wie z. B. einem Passwort und einer App auf dem Handy.
- Was kompliziert klingt ist heute ziemlich einfach zu nutzen und bietet ein erfektes Plus an Sicherheit – Angreifer scheitern reihenweise an MFA und das wird sich auch in Zukunft nicht ändern.
- Fazit: Keine Angst vor MFA - schützen Sie möglichst alle Online-Accounts mit MFA.

WINDOWS ABSICHERN!

- Aktuelle Versionen von Windows machen es Angreifern mittlerweile richtig schwer. Wenn man ein paar Kleinigkeiten beherzt:
  - Arbeiten Sie nur als Administrator auf Ihrem PC, wenn es unbedingt sein muss (das ist nur ganz selten der Fall). Legen Sie sich ein eigenes Benutzerkonto mit eingeschränkten Rechten an und verwenden Sie dieses für die tägliche Nutzung. Wenn etwas schief gehen sollte, bleibt der Schaden begrenzt.
  - Schalten Sie die Firewall von Windows nicht aus (die ist wirklich gut).
  - Entdeckte Sicherheitslücken und sonstige Fehler in Windows werden von Microsoft behoben und entsprechende Aktualisierungen (Updates) herausgegeben. Schalten Sie die automatische Installation der Updates nicht aus.
  - Microsoft hat die Unterstützung für eine ganze Reihe seiner alten Betriebssysteme mittlerweile eingestellt. Für sie gibt es keine Aktualisierungen mehr; Sicherheitslücken bleiben offen und Ihr PC wird immer verwundbarer (weil mit der Zeit mehr und mehr Sicherheitslücken entdeckt werden). Ersetzen Sie alte Windows-Versionen (wie z. B. Windows XP und Windows 7/8 und bald auch 10) gegen ein aktuelles Windows oder steigen Sie auf Mac OS oder Linux um (letzteres z. B. wenn der Rechner mit aktuellen Versionen von Windows nicht mehr vernünftig läuft).

UPDATES, UPDATES, UPDATES!

- Über die Updates von Windows wird nur die Software von Microsoft aktuell gehalten - Lücken in anderen Programmen werden nicht gestopft. Angreifer wissen das und gehen den Weg des geringsten Widerstands.
- Hier die Maßnahmen:
  - Sorgen Sie dafür, dass auch jene Software auf Ihrem Rechner aktuell bleibt, die nicht von Microsoft stammt (Java, Adobe Acrobat Reader, LibreOffice, Thunderbird, Firefox, ...):
  - Informieren Sie sich, wie Ihre Anwendungssoftware mit Updates versorgt werden kann. Aktivieren Sie (wenn möglich) die automatische Updates Ihrer Anwendungssoftware.
  - Prüfen Sie in regelmäßigen Abständen, ob die Software auf Ihrem Rechner noch aktuell ist. Empfehlenswert sind hier z.B. Software-Up-To-Date oder Secunia PSI. Führen Sie in regelmäßigen Abständen (z. B. monatlich) ggf. auch manuell ein Update durch.
  - Webbrowser und entsprechende Plugins sind besonders gefährdet, weil sie Inhalte aus dem Internet herunterladen und interpretieren. Achten Sie darauf, dass Browser und Plugins auf dem neuesten Stand sind.

VORSICHT VOR FREMDEN PROGRAMMEN!

- Unseriöse Webseiten versuchen Ihnen (z. B. durch reißerische Anzeigen, Sicherheitswarnungen oder Gewinnbenachrichtigungen) Schadsoftware unterzuschieben, die als ein harmloses/nützliches Anwendungsprogramm getarnt ist.
- Hier die Maßnahmen:
  - Installieren Sie keine Programme, über die Sie sich nicht (z.B. durch eine kurze Google-Recherche) informiert haben.
  - Diese Empfehlungen gelten vor allem für angebliche Sicherheits-Updates und Antivirus-Programme.
  - Beherzigen Sie immer die folgenden Grundsätze:
    - Nicht aktiv danach gesucht? Wird nicht installiert!
    - Nicht darüber informiert? Wird nicht installiert!

WINDOWS: ES GEHT NICHT OHNE ANTIVIRUS

- Schadsoftware ist und bleibt ein massives Problem. Es gibt seit Jahren eine hoch professionelle Industrie, die für Kriminelle maßgeschneiderte Schadsoftware erstellt (Arbeitsteilung).
- Allerdings sind Sie auch hier nicht machtlos:
  - Installieren Sie auf Windows-Rechnern eine Antivirus-Software oder nutzen Sie zumindest den Antivirus, der in Microsoft Windows bereits eingebaut ist (Microsoft Security Essentials).
  - Achten Sie darauf, dass die Antivirus-Software permanent im Hintergrund aktiv ist, damit Schädlinge entdeckt, bekämpft und entsorgt werden, bevor sie sich einnisten können (das ist bei allen guten Antiviren der Fall).
  - Achten Sie darauf, dass die Antivirus-Software regelmäßig Updates erhält (das ist bei allen guten Antiviren der Fall).
  - Hinweis: Viele namhafte Hersteller von Antiviren bieten ihre Produkte für Privatanwender kostenfrei oder zu einem sehr geringen Preis an.
  - Vermeiden Sie den Hersteller Kaspersky. Dieser Hersteller muss durch die aktuelle geopolitische Lage (Angriffskrieg Russlands gegen die Ukraine) als reales Sicherheitsrisiko angesehen werden.

EXKURS: IST MEIN RECHNER BEREITS INFIZIERT?

- Wie kann man herausfinden, ob ein Computer bereits infiziert ist?Viele Hersteller von Antivirus-Software bieten hierfür spezielle Werkzeuge. Im Jargon werden diese Tools „Rescue-CDs“ genannt („Rettungs-CDs“).
- So können Sie Ihren Rechner gründlich auf ggf. vorhandene Infektionen überprüfen:
  - Suchen Sie im Netz nach „antivirus rescue cd“.
  - Laden Sie die Rescue-CD eines namhaften Herstellers (z. B. Avast, AVG, Avira, TrendMicro, ...) herunter und erstellen Sie eine entsprechende CD, DVD oder einen USB-Stick. Die Anleitung dafür finden Sie beim Hersteller.
  - Starten Sie den Computer von dem gerade erstellten Medium; so können Sie sicher sein, dass keine Schadsoftware aktiv ist.
  - Überprüfen Sie nun den Rechner (das kann durchaus eine Stunde oder länger dauern).

NICHT AUF BÖSARTIGE MAILS REINFALLEN! (1/3)

- E-Mails sind ein massives Sicherheitsproblem:
  - Links im Text oder in den Anhängen der E-Mail können zu bösartigen Webseiten führen. Die Webseiten fordern Sie dann auf, Zugangsdaten (z. B. für ebay, Amazon oder Online-Banking) preiszugeben oder sie bieten Schadsoftware zum Download an.
  - Links im Text oder in den Anhängen der E-Mail können direkt auf Schadsoftware zeigen. Der Klick auf den Link startet den Download der Schadsoftware.
    Ein zweiter Klick startet die heruntergeladene Schadsoftware .
  - Die Anhänge einer E-Mail können selbst Schadsoftware sein.
    Ein Klick startet die Schadsoftware.
- Sie sehen: Ohne Ihr „KLICK“ laufen bösartige E-Mails ins Leere.

NICHT AUF BÖSARTIGE MAILS REINFALLEN! (1/3)

- Das sind die wichtigsten Maßnahmen für den sicheren Umgang mit E-Mails:
  - Schalten Sie den Schadsoftware-Filter Ihres E-Mail-Anbieters ein. Viele Mails mit Schadsoftware sowie SPAM-Mails werden so entsorgt, noch bevor sie auf Ihren Rechner gelangen (das spart Zeit und Nerven).
  - Schauen Sie sich E-Mails mit Links und/oder Anhängen in aller Ruhe an, bevor Sie klicken.

INTERMEZZO

(ANATOMIE EINER BÖSARTIGEN MAIL)

GEFÄLSCHTE MAIL IN DER INBOX

GEFÄLSCHTE MAIL IN DER INBOX

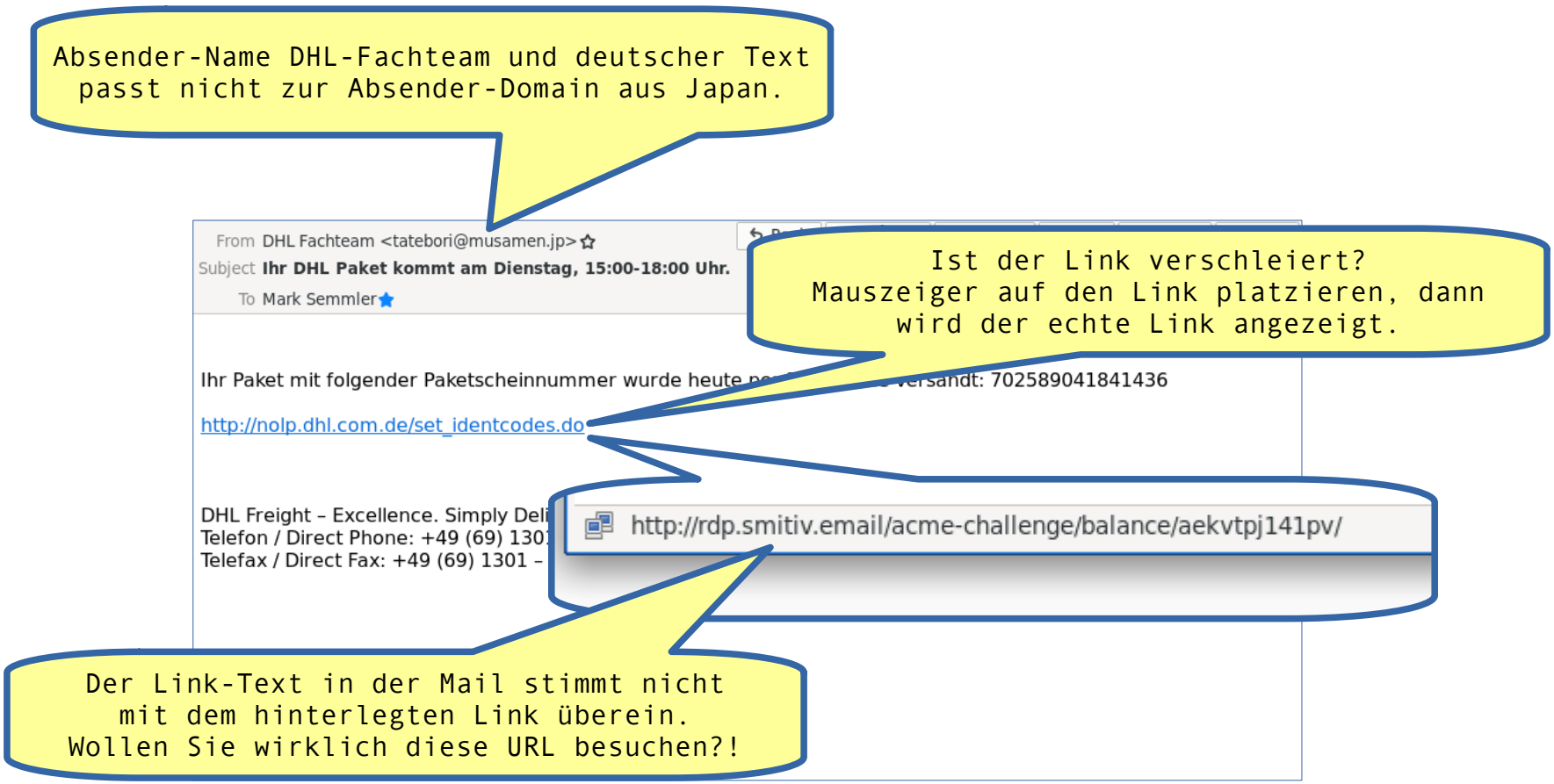
Absender-Name DHL-Fachteam und deutscher Text passt nicht zur Absender-Domain aus Japan.

GEFÄLSCHTE MAIL IN DER INBOX

Absender-Name DHL-Fachteam und deutscher Text passt nicht zur Absender-Domain aus Japan.

Ist der Link verschleiert?
Mauszeiger auf den Link platzieren, dann wird der echte Link angezeigt.

GEFÄLSCHTE MAIL IN DER INBOX

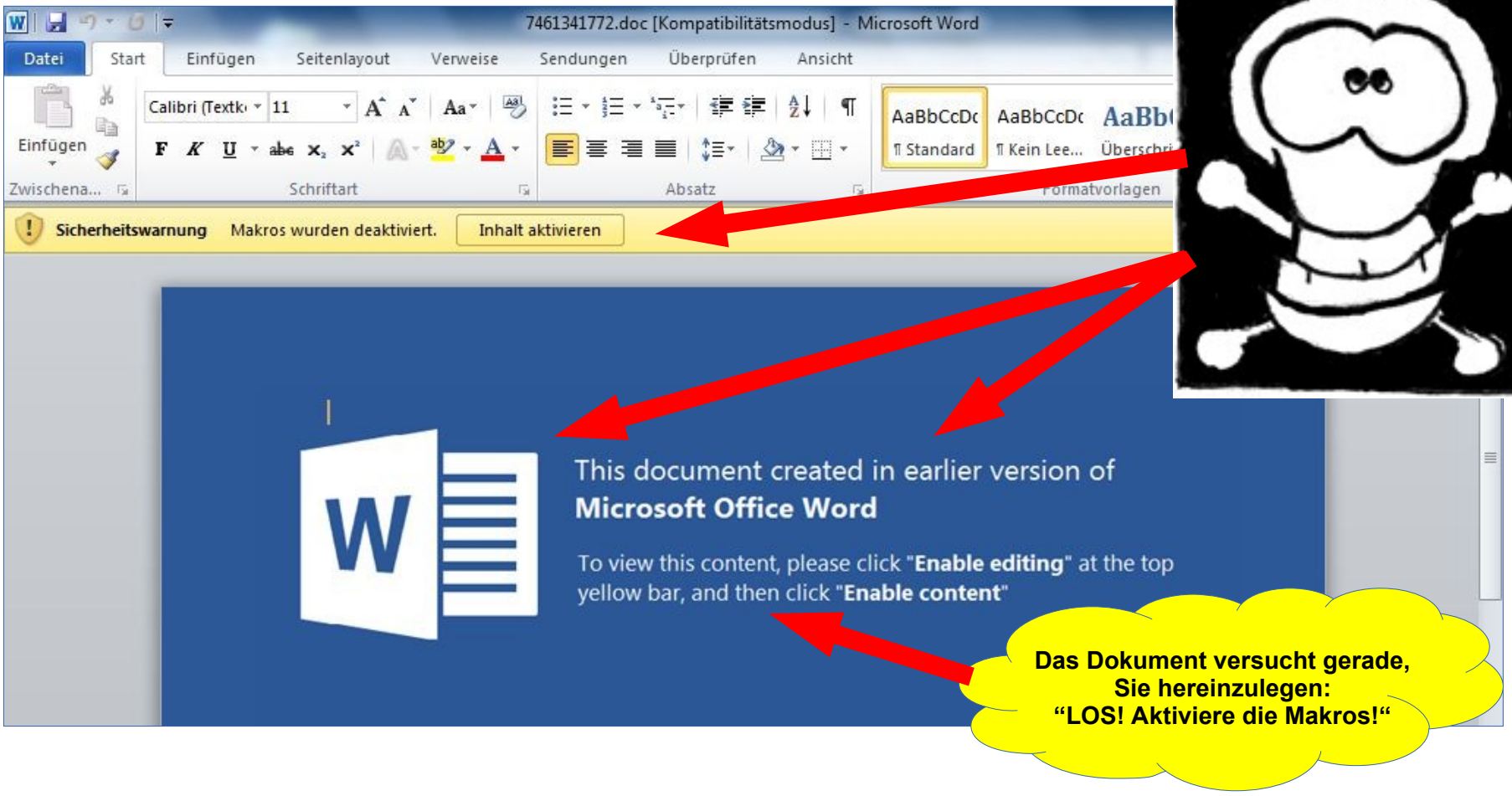


INTERMEZZO
ENDE

NICHT AUF BÖSARTIGE MAILS REINFALLEN! (2/3)

- Besonders häufig werden verseuchte Office-Dokumente per Mail verschickt.
- Wenn Microsoft Office (z. B. Word) Sie dazu auffordert „Aktive Inhalte (zu) aktivieren“ sollten bei Ihnen alle Alarmglocken klingeln.
- Aktive Inhalte (auch „Makros“ genannt) sind ganz einfach Programme, die in den Dokumenten eingebettet sind und Schadsoftware installieren können.
- So reagieren Sie richtig:
  - Finger weg!
  - Finger weg – egal welche Begründung im Dokument steht!
  - Finger weg – egal wie überzeugend diese Begründung zu sein scheint.
  - Rufen Sie im Zweifelsfall den Autor des Dokuments an.
  - Deaktivieren Sie am besten Makros in Microsoft Office generell.

NICHT AUF BÖSARTIGE MAILS REINFALLEN! (3/3)



LÄSTIGE WERBEMAILS (SPAM) VERMEIDEN!

- Geben Sie Ihre Mailadresse nicht leichtfertig weiter und veröffentlichen Sie Ihre Mailadresse nicht ungeschützt auf Webseiten. Spammer suchen hier gezielt nach Mailadressen und überschwemmen Sie mit unerwünschten Mails.
- Viele Webseiten verlangen bei einer Registrierung eine Mailadresse. Darunter können auch schwarze Schafe sein, die ihre Mailadresse missbrauchen. Legen Sie sich für diese Fälle eine spezielle Mailadresse zu (z.B. `ihr.name_spamfalle@irgendein-mailprovider.com`) und halten Sie Ihre eigentliche Mailadresse unter Verschluss.
- Kaufen Sie keine mit SPAM beworbenen Produkte. Sie ernähren sonst die SPAM-Versender.
- Antworten Sie niemals auf SPAM und klicken Sie niemals auf Links in SPAM-Mails („Wenn Sie keine Mails mehr erhalten wollen, klicken Sie hier!“). Sonst weiß der SPAM-Versender, dass Sie seine Mail gelesen haben und schickt Ihnen nur noch mehr SPAM.

MOBILE GERÄTE SCHÜTZEN!

- Mobilen Geräte (Laptops, Smartphones usw.) können verloren/geklaut werden. Fremde besitzt dann Ihr Gerät und – was meistens noch schlimmer ist - Ihre Daten!
  - Verschlüsseln Sie die Datenträger von mobilen Geräten, wenn auf ihnen persönliche oder vertrauliche Informationen gespeichert sind. Das geht sehr einfach und Programme zum Verschlüsseln von Festplatten, Laptops und USB-Sticks gibt es kostenlos im Netz (z.B. VeraCrypt) oder sind bereits in den Betriebssystemen integriert (z. B. Bitlocker in Windows).
  - Nicht alle mobilen Geräte unterstützen die Verschlüsselung der lokalen Daten. Achten Sie beim Kauf auf dieses wichtige Feature. Fragen Sie nach und bestehen Sie vor dem Kauf auf eine Antwort!
  - Bei Laptops gilt: BIOS-Passwort und Festplattenkennwort setzen. Dadurch können Fremde gefundene oder gestohlene Geräte nicht so einfach verwenden bzw. weiterverkaufen.
  - Bringen Sie an allen mobilen Geräten einen Aufkleber mit (anonymen) Kontaktdaten an und versprechen dem (un)ehrlichen Finder einen großzügigen Finderlohn. Verlorene und geklaute Geräte kommen so häufig zum Besitzer zurück...
  - Konfigurieren Sie Ihr Gerät so, dass es sich bei Nichtbenutzung nach wenigen Minuten sperrt.
  - Aktivieren Sie - falls vorhanden - Funktionen zum Auffinden des mobilen Gerätes.

EIGENE DATEN SCHÜTZEN!

- Einige kurze Worte über den Umgang mit den eigenen Daten – hier wird aktuell viel zu viel falsch gemacht.
  - Veröffentlichen Sie nur solche Informationen über sich im Netz (z.B. in sozialen Medien, auf der eigenen Homepage, in Foren usw.), die Sie auch auf Plakatwänden in Ihrem Wohnort (zusammen mit Ihrer Anschrift) schreiben würden.
  - Prüfen Sie vor der Weitergabe von Informationen, Fotos, Filmen etc. genau, was Sie gerade tun. Hier gilt: Einmal veröffentlicht – für immer außerhalb Ihrer Kontrolle.
  - Seien Sie vorsichtig, mit wem Sie Gespräche über welche Themen über die Webcam führen. Ihr Gegenüber kann Sprache und Bild unbemerkt aufnehmen. Diese Aufnahmen können ggf. gegen Sie verwendet werden.
  - Die häufigste Form der Kriminalität ist hier die Erpressung bei sexuellen Inhalten.
  - Sprechen Sie unbedingt mit Ihren Kindern über diese Themen.

SOZIALE MEDIEN: RAUS AUS DER FILTERBLASE!

- Soziale Medien sind Segen und Fluch zugleich. Sie sind ein Ort der freien Meinung, der völlig durchgeknallten Verschwörungstheoretiker und der professionellen Manipulation.
- Seien Sie vorsichtig und verantwortungsvoll in dieser Welt:
  - Viele vermeintliche Gesprächspartner/Beifallklatscher sind gesteuerte Manipulatoren, die für offensive Meinungsmache eingesetzt/bezahlt werden. Merke: Ein Trend in Sozialen Medien ist noch lange keine Mehrheits-Meinung oder gar die Realität.
  - Verlangen Sie Quellen für jede Behauptung, die Sie in sozialen Medien lesen - vor allem wenn die Behauptung besonders toll oder besonders empörend ist. Häufig gibt es keine oder keine seriösen Quellen. Lesen Sie die Quellen kritisch. Recherchieren Sie. Hinterfragen Sie. Bilden Sie sich erst dann eine Meinung.
  - Merke: Soziale und angeblich „alternative“ Medien (Schwurbel-Webseiten, Telegram-Kanäle, YouTube-Videos und Twitter-Accounts) sind keine verlässlichen Informationsquellen.
  - Geben Sie Behauptungen niemals ungeprüft weiter – auch wenn sie Ihrem Weltbild entsprechen. Sonst werden Sie allzu schnell selbst zum Teil des Problems.
  - Nutzen Sie „herkömmliche“ Medien (etablierte Zeitungen, Ferseh- und Radiosender).
  - Üben Sie sich darin, Verschwörungstheorien zu erkennen (das kann viel Spaß machen).

TRACKING: DIENSTE GEGEN DATEN (1)

TRACKING: DIENSTE GEGEN DATEN (2)

- Das erfolgreichste Geschäftsmodell im Internet lautet „Daten gegen Dienste“: Wenn Sie (vermeintlich) kostenfreie Webseiten, Dienste oder Apps nutzen, werden (permanent) Daten über Sie gesammelt und ein möglichst genaues Profil von Ihnen erstellt (Alter, Geschlecht, Krankheiten, politische Überzeugung, Hobbies, Aufenthaltsorte, Gewohnheiten, ...).
- Dieses Vorgehen wird „Tracking“ genannt.
- Die gesammelten Daten werden am häufigsten dazu genutzt, Ihnen „passende“ Werbung einzublenden.
- Andere Nutzungen sind möglich, weil die Daten auch auf dem „freien Markt“ angeboten werden. In der Vergangenheit wurden Profile bereits verwendet, um politische Entscheidungsprozesse zu manipulieren (Beispiel: Brexit).

DATENSAMMLER IN DIE SCHRANKEN WEISEN

- So wehren Sie sich gegen Datensammler:
  - Konfigurieren Sie Ihren Webbrowser so, dass beim Beenden des Browsers sämtliche Cookies gelöscht werden. So schütteln Sie viele Tracking-Mechanismen ab.
  - Achten Sie darauf, welche Berechtigungen Apps auf Ihrem Smartphone haben möchten. Häufig haben Sie die Möglichkeit, solche Berechtigungen zu verweigern oder nur einmalig zu vergeben.
  - Lesen Sie vor der Installation von Apps bzw. vor der Nutzung von Cloud-Diensten deren Datenschutzbestimmungen.
  - Seien Sie bereit, für Apps und Dienste ein wenig Geld auszugeben.
    Wie viel ist Ihnen Ihre Privatsphäre wert?

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!