B4 - Awareness Training

AGENDA „IT-SICHERHEIT“

- „Drei Schutzziele, ein Ziel: „Sicherheit“
  - Notwendigkeit
- Sicherheitslücken im Überblick
- Wie erstelle ich sichere Passwörter
- Verhalten bei Gefahren
  - Typische Gefahren „E-Mail“
- PHISHING kurz erklärt
- Folgen von Angriffen
- Wie und wo speichere ich meine Daten?
- Typische Fehler
- Vorteile beim Hosting über die Bite AG / Fragerunde

DREI SCHUTZZIELE, EIN ZIEL: SICHERHEIT

Vertraulichkeit – Verfügbarkeit - Integrität

SCHUTZZIELE DER INFORMATIONSSICHERHEIT

Datenzugriff nur für Berechtigte

Unversehrtheit und Korrektheit der Daten

Daten stehen zum geforderten Zeitpunkt zur Verfügung

NOTWENDIGKEIT

1. Kontinuität der Geschäftsabläufe sicherstellen
2. Beibehaltung des guten öffentlichen Rufes
3. Erhaltung der Informationswerte
4. Gewährleistung des Schutzes von personenbezogenen Daten
5. Einhaltung von gesetzlichen Vorgaben
6. Reduzierung der im Schadensfall entstehenden Kosten

➡ **Sicherung Ihres Arbeitsplatzes!**

SICHERHEITSLÜCKEN

Finde die neun Sicherheitslücken bzw. möglichen Gefahren auf dem Bild

AUFLÖSUNG „SICHERHEITSLÜCKEN“

1. Türen und Fenster stehen offen: Rechner und Zubehör könnten aus den Räumen gestohlen werden.
2. Der Bildschirm und damit möglicherweise auch vertrauliche Informationen können von Unbefugten eingesehen werden.
3. Ein Zettel mit Passwörtern ist sichtbar und könnte von Unbefugten missbraucht werden.
4. Eine mit „Save“ beschriftete und damit deutlich als Sicherung gekennzeichnete DVD liegt zugänglich herum.
5. Ausdrucke und Kopien mit vertraulichen Daten liegen an Druckern und Kopieren.
6. Rechner mit direkter Verbindung ans Internet können den Schutz des Netzes durch die Firewall aushebeln.
7. Durch private Datenträger (im Bild eine DVD) kann Schadsoftware in das Unternehmensnetz gelangen
8. Austretende Flüssigkeiten gefährden die Hardware.
9. Rauchen bedeutet Brandgefahr.

WIE ERSTELLE ICH SICHERE PASSWÖRTER?

- **Verwende jedes Passwort nur für EIN System**
- **Nutze keine Wörter mit logischem Bezug (Bite, Ludwigsburg, Namen ...)**
- **Verwende so viele Zeichen (Groß-, Kleinschreibung, Zahlen, Sonderzeichen) wie möglich, mindestens jedoch 12!**
- **Bei einer Brute-Force Attacke benötigt man ca. 122 Tage, um ein 10-stelliges Password zu knacken. Ein 8-stelliges ca. 34 Minuten, ein 6-stelliges nur ein paar Sekunden.**
- **Notiere deine Passwörter nicht oder lege es an einem sehr sicheren Platz ab (Password Safe etc.)**
- **Denk Dir einen Satz aus, den nur Du kennst:**
  Beispiel: FC Bayern München wird 2025 deutscher Meister? -> FCBw2025dM?
- **Bitte keine Passwörter im Browser (Chrome, Edge..) abspeichern**

VERHALTEN BEI GEFAHREN

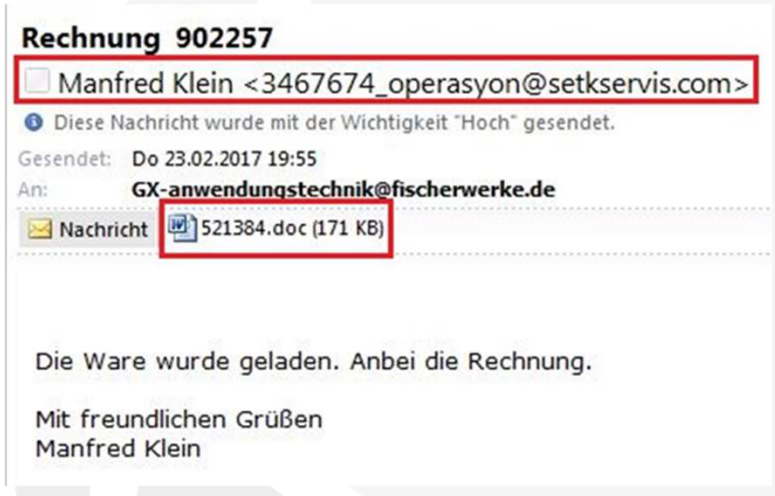
- **Wenn Du eine verdächtige Mail erhältst:**
- **eigene IT / Dienstleister informieren**
- **Die E-Mail nicht weiterleiten!**
- **Einen Kollegen zu Rate ziehen. Wenn dadurch keine 100%ige Klarheit besteht.**
- **Wenn Du evtl. auf etwas „verdächtiges“ geklickt hast und/oder sich dein Computer merkwürdig verhält:**
- **Gerät abschalten, Netzwerkstecker ziehen! Notfalls Stromstecker ziehen!**
- **Interne IT informieren**
- **Weitere Schritte mit IT besprechen**

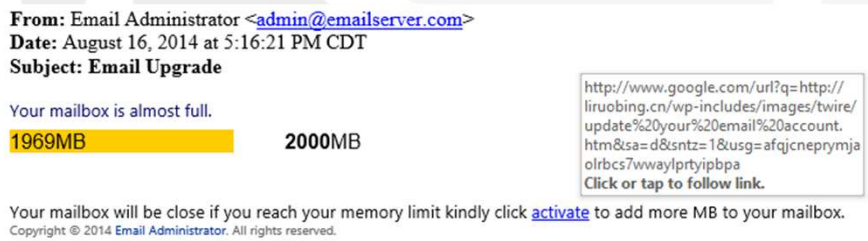
TYPISCHE GEFAHREN „E-MAIL“

E-Mail-Anhänge sind kritisch, wenn

- du den Absender nicht kennst
- die Absenderadresse etwas kryptisch ist
- persönliche Anrede des Empfängers fehlt
- wenn verdächtigt bzw. Zahlung verlangt wird, Rücksprache mit Absender
- sich Dateien im Anhang befinden
- sich Links in der E-Mail befinden, die beim Überfahren mit der Maus kryptische Links zeigen und nach Passwörtern gefragt wird
- der Mailinhalt sehr allgemein gehalten ist sowie Rechtschreibfehler enthält

- **Beispiele**





Bite AG

PHISHING KURZ ERKLÄRT?

„FOLGEN VON ANGRIFFEN“

Du klickst in einer „komischen“ E-Mail einen Link an oder öffnest einen Anhang

Ransomware WannaCry befällt Rechner der Deutschen Bahn

13.05.2017 11:22 Uhr – Volker Briegleb vorlesen

Zwischen Neckar und Alb

Metabo wird Opfer von Hacker-Angriff

Cyberkriminalität In Nürtinger Firma haben Hacker zugeschlagen. Deshalb konnte tagelang nicht produziert werden.

03.07.2017 Archivartikel

Mittwoch, 05. Juli 2017

Cyber-Attacke

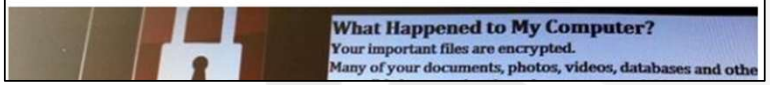
Beiersdorf erleidet beträchtlichen Schaden

Die zu Erpressungszwecken verbreitete Schadsoftware "Petya/NotPetya" hat Beiersdorf Ende Juni kräftig zugesetzt. Den Dax-Konzern kostet diese Attacke wohl "viele Millionen". Noch sind die wirtschaftlichen Folgen nicht genau beziffert.

Daimler: WannaCry hat offenbar neue Opfer gefunden

UPDATE

29.09.2017 14:31 Uhr – Ronald Eikenberg vorlesen



Automatisierungsunternehmen Pilz von Hackerangriff betroffen

Am Sonntag, den 13. Oktober, hat auf das Unternehmen Pilz in Ostfildern ein Cyberangriff stattgefunden.

Donnerstag, 27. April 2017

50 Milliarden Euro Schaden

Cyber-Attacken treffen unzählige Firmen

Kriminelle Angriffe über das Internet finden so geräuschlos statt, dass Unternehmen sie erst Monate später bemerken. Der Verfassungsschutz warnt, es gebe immer mehr Angriffsziele. Treffen kann es auch selbstfahrende Autos oder vernetzte Herzschrittmacher.

DATEN IM DARK WEB

Motel One von Ransomware-Attacke betroffen

Die Hotelkette Motel One wird offenbar von der Ransomware-Bande BlackCat erpresst.

Bite AG

WIE UND WO SPEICHERE ICH MEINE DATEN?

- Daten sollten grundsätzlich auf den Netzlaufwerken oder in dem entsprechenden IT-System (OneDrive) gespeichert werden
- Daten dort werden regelmäßig gesichert und stehen daher im Bedarfsfall in fast allen abgespeicherten Versionen zur Verfügung
- Daten für Partner außerhalb unseres Unternehmens sollten möglichst nur zeitlich begrenzt über die Austauschplattform NextCloud zur Verfügung gestellt werden
- Daten dürfen nicht auf privaten OneDrive / iCloud Umgebungen liegen

TYPISCHE FEHLER

- Passwörter werden an Kollegen weitergegeben oder liegen offen
- Der Computer wird beim Verlassen des Arbeitsplatzes auch im Homeoffice nicht gesperrt
- USB-Sticks von Fremden / mit unbekanntem Inhalt werden genutzt
- Unternehmensdaten liegen auf einem Cloud-Dienst wie Dropbox / iCloud
- Programme werden von unbekannter Quelle (Webseiten) heruntergeladen / installiert und Versionsstände (Sicherheitslücken) sind veraltet.
- geschäftliche Daten werden auf privaten Computern gespeichert
- „Passwort“, „123456“ oder „Disponic1#“ sind KEINE sicheren Passwörter!
- Von der IT vergebene Passwörter sollten sofort geändert werden
- Es werden öffentlichen WLANs / Hotspots (Hotel / Bahnhof) genutzt

ZERTIFIZIERTES ISO27001 RECHENZENTRUM FÜR „DISPONIC“

Vorteile beim Hosting über Bite

- **Physische Sicherheit:**

  Moderne Zutrittskontrollen, Kameraüberwachung, Brandschutzsysteme und Notstromversorgungen.

- **Technische Sicherheit:**

  Redundante Internet-Backbones, separate Netze für Backups und moderne Überwachungssysteme.

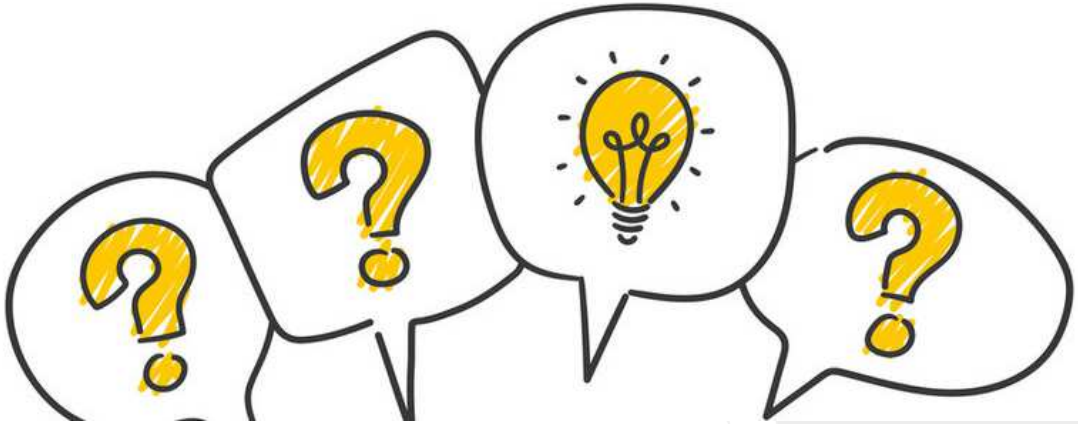
- **Organisatorische Sicherheit:**

  Umfassende Prozesse für den Betrieb, die ständige Überprüfung und kontinuierliche Verbesserung der Sicherheit.

Bite AG

NOCH FRAGEN?

- **Vielen Dank für Ihre Aufmerksamkeit**




DISPONIC®
PROFESSIONELLE DIENSTLEISTUNG

... EIN PRODUKT DER BITE AG

Bite AG

Im Köller 3
D-70794 Filderstadt
+49 711 380 155 00
www.bite.de
www.disponic.de
www.youtube.com/@disponic

Hotline:
hotline@disponic.de
+49 711 380 155 180