KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

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

Informationssicherheit im Handwerk – Risiken und Nebenwirkungen vermeiden

Vortrag am 16. Oktober 2017 in der HWK-Oldenburg

BFE Oldenburg
Bundestechnologiezentrum für
Elektro- und Informationstechnik e.V.

Dipl.-Ing. Werner Schmit

Kurzvorstellung: Dipl.-Ing. Werner Schmit

- Dozent am Bundestechnologiezentrum für Elektro- und Informationstechnik (BFE Oldenburg)
- Arbeitsschwerpunkte
  - Informationssicherheit
  - Datennetzwerktechnik
  - GNU/Linux
  - Systempflege E-Learning-Server
  - Programmierung (C/C++, Java, PHP)
- IT-Security-Beauftragter (TÜV)
- Kontakt
  E-Mail: w.schmit@bfe.de
  Tel.: 0441-34092458

Inhalte

1. IT-Sicherheit ist Chefsache
2. Gefahren für Daten, IT-Systeme und Maschinen
3. Erforderliche Maßnahmen für die IT-Sicherheit im Handwerksbetrieb
4. Fazit

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

1. IT-Sicherheit ist Chefsache

Blick auf die aktuelle Lage der IT-Sicherheit

heise Security

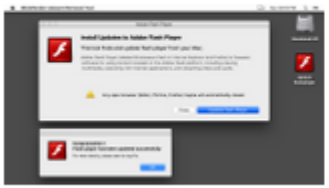
Jetzt patchen! Aktive Angriffe auf WordPress-Webseiten

08. Februar, 10:30 Uhr 30

Wer WordPress ab Version 4.7 einsetzt, sollte zügig die aktuelle abgesicherte Version einspielen: Derzeit nutzen Angreifer zielgerichtet eine kritische Sicherheitslücke aus.

MacDownloader: Iranische Malware zielt auch auf Macs ab

08. Februar, 17:40 Uhr 57



Die Malware wird gegen Menschenrechtler und Mitarbeiter von Rüstungsfirmen eingesetzt, erklären Sicherheitsforscher. Sie soll den Mac-Schlüsselbund mit den Zugangsdaten des Opfers an die angeblich iranischen Angreifer übermitteln.

Automatische Inhaltserkennung: Vizios Smart-TV spionieren ungefragt Nutzerverhalten aus

07. Februar, 08:20 Uhr 141

Der Hersteller von internettauglichen Fernsehern zahlt 2,2 Millionen US-Dollar, nachdem ihm die US-Behörde FTC vorwarf, Nutzer ausgeforscht zu haben, ohne sie um Erlaubnis zu fragen.

Was bedeuten die Meldungen für mein Unternehmen?

- **Die große Verunsicherung:**
  - Sind nur größere Unternehmen gefährdet oder bin ich als Kleinbetrieb auch betroffen?
  - Wo bin ich gefährdet?
  - Was muss ich alles machen, um mich zu schützen?
  - Wie gehe ich vor?

IT ist unsicher, aber wir haben Möglichkeiten, uns zu schützen

Viele Wege führen zur Informationssicherheit.
Welcher Weg ist der effektivste?

Quelle: BSI

Kosten und Haftung

- Wieviel kostet mich IT-Sicherheit?
- Reichen 80%-IT-Sicherheit?
- Kann ich mich gegen Schäden versichern?
- Muss ich überhaupt etwas tun?
- Wer haftet im Schadensfall?

IT-Sicherheit ist Chefsache

- Dieses Thema ist so wichtig, dass die Chefin (der Chef) sich selbst darum kümmern muss und es nicht ausschließlich bestimmten Beschäftigten oder externen Dienstleistern überlassen darf.

- Die Chefin (der Chef) muss zumindest so viel davon verstehen, dass sie (er) das Thema managen können. Um die näheren Einzelheiten können sich dann Experten kümmern.

- Die Chefin (der Chef) ist für die IT-Sicherheit zuständig, haftet im Schadensfall.

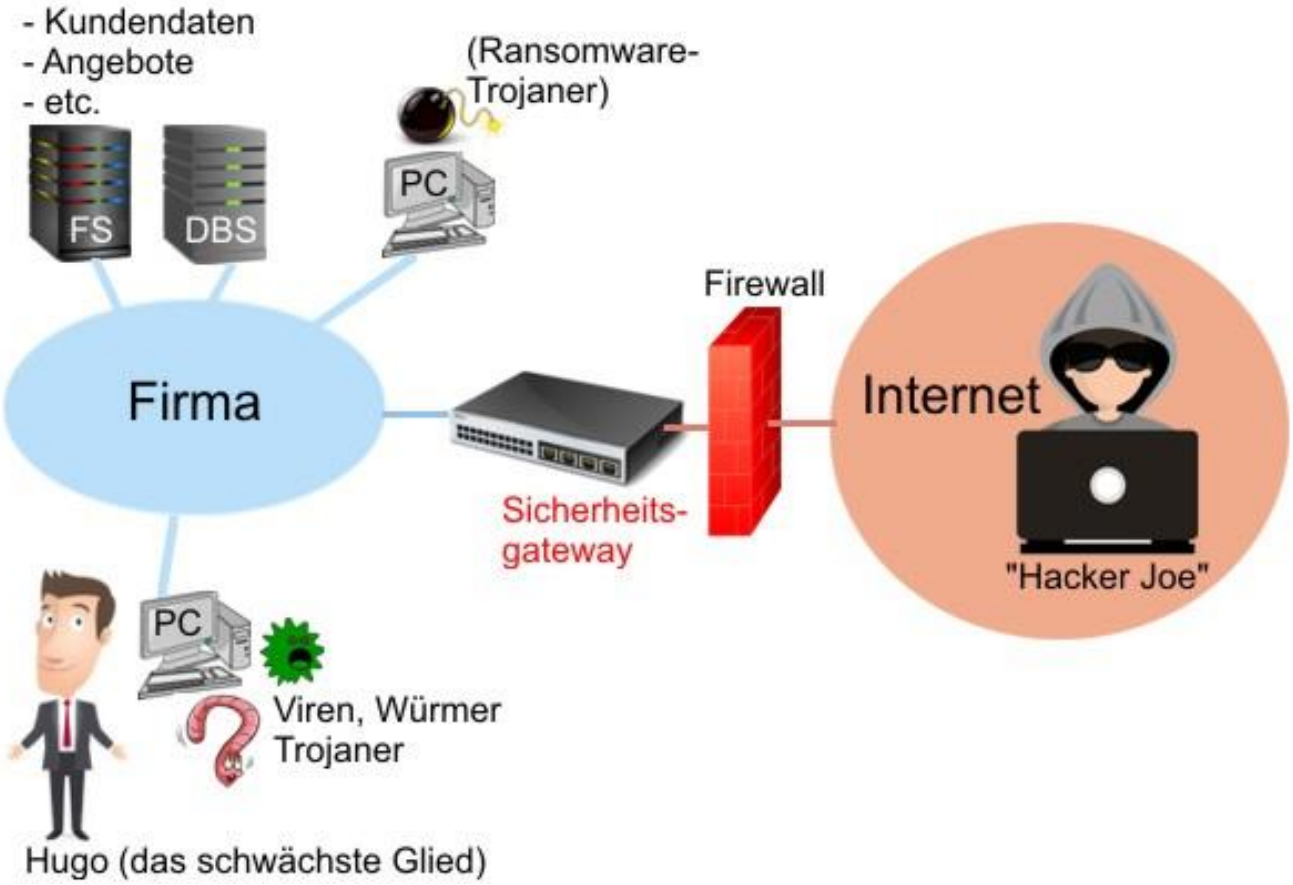
KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

2. Gefahren für Daten, IT-Systeme und Maschinen

Gefahren für Daten und IT-Systeme

- **Gefahrenpotentiale** = a)Bedrohungen und Sicherheitslücken b)Risiken

- Erst, wenn ich die Gefahren kenne, lassen sich erforderliche Maßnahmen daraus herleiten!



Schwachstelle Mensch

- **Social Engineering**
  - Cyberkriminelle setzen zunehmend auf Angriffe, bei denen nicht Schwachstellen in der Software ausgenutzt werden, sondern die Leichtgläubigkeit von Personen. Via Social Engineering können sich Bedrohungen, wie die so genannte Ransomware, rasant verbreiten.

Quelle: heise.de

Mögliche Schäden

- **Sabotage**
  - Verfälschung von Daten
  - Ausfall oder Einschränkung der Funktionsfähigkeit wichtiger IT-Systeme
  - Ausfall, Zerstörung bzw. Manipulation von Maschinen

- **Verlust von Daten**
  - Datenklau

- **Spionage**
  - Verlust der Vertraulichkeit wichtiger Unternehmensdaten
  - Kundendaten und andere sensible Unternehmensdaten
    - Forschungs- und Entwicklungsergebnisse, Strategiepapiere, Einzelheiten von Verträgen, Angebote und Preiskalkulationen, die Korrespondenz mit Geschäftspartnern, Informationen über die Besonderheiten der Unternehmens-IT, Zugangsdaten,...

Mögliche Folgen

Produktionsverzögerung oder **Lieferverzögerungen**

Auftragsverlust

Kundenverlust

spürbare finanzielle Einbußen

Insolvenz

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

3. Erforderliche Maßnahmen für die IT-Sicherheit im Handwerksbetrieb

- Umfang
- Organisation
- Umsetzung
- Tipps für die praktische Umsetzung

IT-Sicherheitsmaßnahmen nach Kategorien

- **Organisatorische Maßnahmen**
- **Infrastrukturelle Maßnahmen**
- **Personelle Maßnahmen**
- **Technische Maßnahmen** inklusive **Systempflege**
- **Notfall-Maßnahmen**

Unkoordinierte „Insellösungen“ vermeiden

Ein ganzheitliches Konzept ist erforderlich!

Wichtigster Faktor und gleichzeitig größte Schwachstelle ist der Mensch!

Organisatorische Mängel lassen sich nicht mit Technik erschlagen!

Das schwächste Glied in der Kette bestimmt die IT-Sicherheit

Organisatorisches (1)

- **Grundvoraussetzung**: **Dokumentationen**
  - Aktuelle Inventarliste (Hardware, Software)
  - Netzwerkplan (physikalische und logische Netzkonfiguration)
  - Serviceheft von jedem IT-System (enthält Konfiguration u. Änderungen)

- **Grundvoraussetzung: „Kronjuwelen“ betrachten**
  - **Überblick über die wichtigsten Daten, Anwendungen und IT-Systeme**
  - Bedrohungen und Risiken erkennen, bewerten und Maßnahmen definieren
  - Wo lauern für mich die Gefahren? Wie hoch ist der mögliche Schaden? Was muss geschützt werden? Was muss ich dagegen tun?

- Zuständigkeiten (**Verantwortlichkeiten**) **festlegen** und **dokumentieren**
  - Wer ist für die IT-Sicherheit zuständig? → *IT-Sicherheitsbeauftragter*
  - Wer ist für Systempflege zuständig?
  - Wer führt das Backup durch?
  - Vertretungsregelungen

Organisatorisches (2)

- Wichtig! **Sich über die Sicherheitslage informieren**
  - Zum Vergleich: Autofahrer sind ebenfalls verpflichtet, sich über Änderungen von Regeln im Straßenverkehr zu informieren

- **Zutritts- / Zugangs- und Zugriffsberechtigungen festlegen und dokumentieren**
  - Wer darf was und wo?
  - Rollen und Profile für Benutzer anlegen
  - Zutrittsberechtigungen zu Räumen
  - Zugangsberechtigungen zu IT-Systemen (Anmeldung an einem IT-System)
  - Zugriffsberechtigungen auf Daten und IT-Anwendungen
    - Benutzerrechte
    - need to know-Prinzip (weniger ist mehr)

Organisatorisches (3)

- **Firewallkonzept**

- **Konzept und Umsetzung der Netzwerkstruktur**
  - Sicherheitszonen (min. 3 nach BSI)
  - Sicherheitssegmente (Netzsegmentierung)
  - Kommunikationskontrolle über Firewalls

- **Checklisten**
  - Eintritt neuer Mitarbeiter und bei Austritt von Mitarbeitern

- **Merkblätter**
  - Eintreten eines Virenvorfalls
  - Schutz vor Schadsoftware
- **Listen**
  - Liste mit Passwörtern für Notfälle hinterlegen
  - Liste mit Kontaktdaten für Notfälle hinterlegen

Organisatorisches (4)

- **Sicherheitsrichtlinien** (engl. Security Policies)
  - Richtlinie für Mitarbeiter (u. a. Passwörter, private Nutzung von E-Mail und Internet, Verhalten in sozialen Netzwerken)
  - Richtlinie für Administratoren
  - Richtlinie für den Umgang mit mobilen Datenträgern
  - Richtlinie für den Einsatz von Smartphones

- **Verfahren** (Regelungen, Anleitungen, Betriebshandbücher)
  - Verfahren für Updates / Patches (Update-/Patchmanagement)
  - Verfahren zur Datensicherung, Datenwiederherstellung und Archivierung

- **Vertraulichkeitsvereinbarungen für Externe oder Mitarbeiter**
  - Unterschreiben lassen

- **Sichere Kommunikation mit Kunden und Geschäftspartnern**

Personelles

- **Schulung** der Mitarbeiter
- **Einweisung** im Umgang mit Anwendungen und Systemen
- **Einarbeitung**
- **Sensibilisierung** (**Awareness**)
  - Sicherheitsbewusstsein schaffen
- **Verhalten am Arbeitsplatz**
- **Umgang mit Kennwörtern**
- **Verhalten in sozialen Netzwerken**
- **Umgang mit mobilen Datenträgern**
- **Private Nutzung von E-Mail und Internet**
- **Einsatz von Smartphones**
  - BYOD = Bring Your Own Device

Technisches (1)

- **Endgeräte (Clients) absichern**
  - **Absicherung** und **Härtung** der Arbeitsplatzcomputer
  - Maßnahmen für **sicheres „Surfen“**
  - **Zusätzliche** Sicherheitsmaßnahmen für **mobile Endgeräte (**Notebooks und „mobiler Kleintierzoo“)

- **Server absichern und härten**

- **Netzwerk absichern**
  - Unterschiede zwischen Office-Netz und ICS-Netz (Produktionsnetz)
  - LAN
    - **Firewalls**,
    - **IDS/IPS** (Eindringlinkserkennungssysteme)

Technisches (2)

- **Netzwerk absichern**
  - **Sichere Funknetze (WLANs)**
  - Absicherung Unternehmensnetz nach „Draußen“
    - **Sicherheitsgateway** (Unternehmensfirewall), Fritz!Box reicht nicht aus!
  - Sicherer Betrieb **managebarer Switches**
  - Sicherer Betrieb **Router**

- Zugriff von Außen **- Sicherer Fernzugriff** auf das Unternehmensnetz
  - **VPN-Server (Gateway)**

- **Monitoring**

Systempflege

- **Update-/Patchmanagement** → Sicherheitsupdates, Allgemeine Updates
  - Betrifft PCs, Notebooks, „mobiler Kleintierzoo“, Server, Router, Switches, Sicherheitsgateway, IP-Kameras und sonstige IP-Geräte
  - zeitnah installieren, Verantwortlichkeiten, …
- **Virenschutz**
  - Erforderlich für sämtliche Endgeräte
  - Empfehlung: kostenpflichtige Produkte wählen
- **Datensicherung** (Backup) und **Archivierung**
  - Konzept. Was soll alles gesichert werden?
  - Wie häufig? Wo gespeichert? Wer führt durch? Funktioniert Wiederherstellung?
  - Zurückspeichern testen
- **Nutzungsanpassungen**
- **Aktuelle Sicherheitsvorgaben** berücksichtigen

Infrastruktur

- Anforderung **Elektrotechnische Verkabelung**
- Anforderung **IT-Verkabelung**
- **Serverräume und IT-Systeme**
  - Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung, Stromausfall, Blitzeinschlag und Einbruch
- **Verteilerschrank (**bzw**. Netzwerkschrank)**
  - abschließbar, enthält Patchfeld, Switch, Router
- **Zugangs- und Zutrittskontrolle**
  - Für IT-Systeme und Serverräume
  - Nachweisebare Ausgabe von Schlüsseln nur an Berechtigte
  - Authentisierung von Zugriffen
  - Zutrittskontrollsysteme
  - Kontrolle der Aktionen Betriebsfremder
- **Arbeitsplatz** (gilt auch für Home Office)

Notfallvorsorge

- **Notfallmanagement und Desaster Recovery**
  - „Katastrophenschutzübungen“
  - Wiederanlauf nach einem (Super-)Gau
  - Wiederherstellung vom Backup üben
  - Dazu gehören u. a. Notfallhandbuch, Alarmierungsplan, Datensicherungsplan, Desaster Recoveryplan, Ersatzsysteme

Wie organisieren wir diese Maßnahmen?

Wir brauchen ein Konzept, eine strukturierte Vorgehensweise, einen Prozess zur Implementierung und Etablierung (Entwicklung und Umsetzung) von Informationssicherheit im Unternehmen

→ Ein Qualitätsmanagement (QM) für IT-Sicherheit
→ Ein durchdachtes Sicherheitskonzept
→ vereinfacht: Wir brauchen einen „**Plan**“

Ganz nebenbei: **IT-Sicherheit ist ein fortlaufender, nie endender Prozess!!!**

So sieht der „Plan“ aus

Step 1: **Organisatorisches**

- Erforderliche Dokumente erstellen / aktualisieren
- Verantwortlichkeiten festlegen

Step 2: **Erfassung, Analyse und Bewertung**

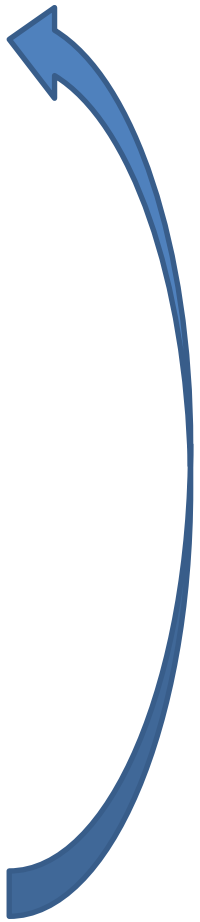
- Analyse der Daten und der IT-Struktur
- Erforderliche Sicherheitsmaßnahmen definieren
- Ist-Soll-Vergleich

Step 3: **Implementierung der Sicherheitsmaßnahmen**

- Sicherheitsmaßnahmen umsetzen

Step 4: **Check**

- Kontrolle der Maßnahmen anhand von Checklisten



Fortsetzung des „Plans“

Dazu immer parallel („täglicher Betrieb“)**:**

- Sensibilisierung der Mitarbeiter für IT-Sicherheit
- Systempflege inkl. Patchmanagement
- Virenschutz
- Backup und Archivierung
- Notfallmanagement

Wie kann ich diese Ziele erreichen? (1)

- **Eigene Fähigkeiten für IT-Sicherheit realistisch bewerten**
  - Was kann ich selber machen? Wo hole ich mir Hilfe? Was ist mein Kernkompetenz?
  - KMU: Mangelnde Ressourcen, geringes IT-Know How

- **Richtige Werkzeuge auswählen und auch richtig einsetzen**
  - Nicht nur die richtigen Werkzeuge für IT-Sicherheit auswählen, sondern auch richtig einsetzen
  - Die Werkzeuge sind nur so gut, wie der sie anwendet

- **Fachkundiges und geschultes IT-Personal**
  - Gut qualifizierte Experten
  - Ständige Weiterbildung erforderlich
  - Erfahrung und Expertenwissen

- **Den richtigen Partner aussuchen**

Wie kann ich diese Ziele erreichen? (2)

- **IT-Security Monitoring**
  - Überwachen der verschiedenen Einfallstore für Cyberangreifer
- **Best Practices**
- **Organisatorische Maßnahmen**
- **Awareness-Trainings**
- **Gelebte Compliance**
  - Von außen herangetragene Anforderungen
  - Vorgaben durch Gesetze, Auftraggeber, aber auch interne Regelungen
- **Vertrauen schaffen**
  - „Vertrauen ist die Basis für IT-Sicherheit“

Ziel nicht erreicht - Sicherheitsmaßnahmen im praktischen Einsatz

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

4. Fazit

Fazit

- IT-Sicherheit ist möglich, es gibt allerdings keine 100%-Sicherheit.
- IT-Sicherheit bedeutet weit mehr als Firewalls einsetzen, Router und Switches
- sicher zu konfigurieren und das WLAN abzusichern.
- Die größte Schwachstelle, der Mensch (Mitarbeiter) muss einbezogen und über-
- zeugt werden.
- Ein ganzheitlicher Ansatz ist erforderlich.
- **IT-Sicherheit ist ein fortlaufender Prozess! Dauerhafte Betreuung und**
- **Systempflege erforderlich!**
- **Voraussetzungen für erfolgreiche IT-Sicherheit**:
  - Das Thema „IT-Sicherheit“ in das Unternehmen integrieren
  - Experten für die Beratung und Umsetzung suchen
  - Eine vertraglich gesicherte und zyklisch ausgeführte Systempflege wird empfohlen.
  - **Es gibt viel zu tun. Fangen Sie einfach an.**

Spezieller Workshop im kommenden Jahr

- **Maßnahmen und Checklisten für ein sicheres IT-Netz im Handwerksbetrieb**
  - IT-Sicherheitsmanagement im Handwerksbetrieb
  - Ermittlung der „Kronjuwelen“
  - Organisatorische Maßnahmen
  - Technische Maßnahmen
  - Personelle Maßnahmen
  - Infrastrukturelle Maßnahmen
  - Notfall-Maßnahmen
  - Einsatz von Checklisten

Vielen Dank für Ihre Aufmerksamkeit