Fortbildung Sachbearbeiter EDV

BSB Andreas Brandstätter

November 2012

Inhalt

kurze Vorstellung

- Name
- Feuerwehr
- Wie lange bereits als Sachbearbeiter tätig?
- Tätigkeiten in der Feuerwehr im Sachgebiet EDV?
  - Computer (Anzahl)
  - Netzwerk?
  - etc...
- Wie viel Erfahrung mit EDV?

EDV ist mehr als FDISK

- EDV stellt Infrastruktur für zahlreiche Sachgebiete zur Verfügung
  - Verwaltung (nicht nur FDISK)
  - Öffentlichkeitsarbeit
  - ...
- Hardware
  - Computer
  - Netzwerk
  - ...
- Software
  - Betriebssystem
  - Office-Anwendungen
  - ev. Spezialsoftware
  - ...

Worum geht es heute?

- “EDV ist mehr als FDISK” $\Rightarrow$ um das “mehr”
- Sicherheit
  - gegen Datenverlust
  - gegen IT-Kriminalität
  - ...

Was wollen die Benutzer?

- “Ich muss FDISK verwenden können!”
- “Ich will Einladungen in Word schreiben und per Email verschicken!”
- “Ich brauche Speicherplatz für die Einsatzfotos und Presseberichte!”
- “Ich will meine Ausbildungsunterlagen abspeichern und ausdrucken!”
- . . .

Kaum jemand sagt:

- “Die Verrechnungsdaten müssen gegen unbefugte geschützt sein.”
- “Die Einladungen für vertrauliche Sitzungen dürfen keinenfalls an falsche Email-Adressen gehen.”
- “Die Einsatzfotos sollen über einen langen Zeitraum wieder auffindbar sein.”
- “Meine Ausbildungsunterlagen dürfen unter keinen Umständen verloren gehen.”
- . . .

Warum?

Warum?

- Sicherheit wird vielfach einfach nicht beachtet oder unterschätzt.
- Insbesondere Benutzer haben keine besonderen Kenntnisse im Bereich IT-Sicherheit
  - Das ist aber ok,
  - dafür sind wir Sachbearbeiter da!

Problem:

Mangelnde Sicherheit fällt erst auf, wenn es zu spät ist!

Die klassischen Schutzziele

- Schutz der Vertraulichkeit (confidentiality)
- Schutz der Integrität (integrity)
- Schutz der Verfügbarkeit (availability)

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

laut Definition des BSI, `https://www.bsi.bund.de`

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. [...] Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

laut Definition des BSI, `https://www.bsi.bund.de`

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

laut Definition des BSI, `https://www.bsi.bund.de`

Was bedeutet das für uns?

Maßnahmen zur Erreichung der Schutzziele.
aber,

- Verhältnismäßigkeit
- Zweckmäßigkeit
- Umsetzbarkeit

im Auge behalten.

Relationen

- Bedrohungspotential einer Bank $\Leftrightarrow$ Feuerwehr
- Größe der IT-Infrastruktur einer Firma $\Leftrightarrow$ Feuerwehr
- Budget einer großen Firma $\Leftrightarrow$ Feuerwehr
- ...

aber auch:

- Benutzerfreundliches System $\Leftrightarrow$ “absolut” sicheres System

Konkrete Maßnahmen

Es folgen Beispiele für konkrete Maßnahmen für durchschnittliche IT-Infrastrukturen in Feuerwehren.

Wichtig ist aber sich selbst in Hinblick auf die **individuelle** IT-Infrastruktur die notwendigen Maßnahmen zur Erreichung der Schutzziele zu überlegen!

WLAN

Kurze Umfrage:

- Wer hat WLAN im Feuerwehrhaus?
- Verschlüsselt?
- Womit?
  - WEP
  - WPA
  - WPA2

WLAN

- WEP
  - praktisch wie keine Verschlüsselung!
  - Dauer für Angriff: weniger als 5 Minuten
  - mind. seit 2005 bekannt

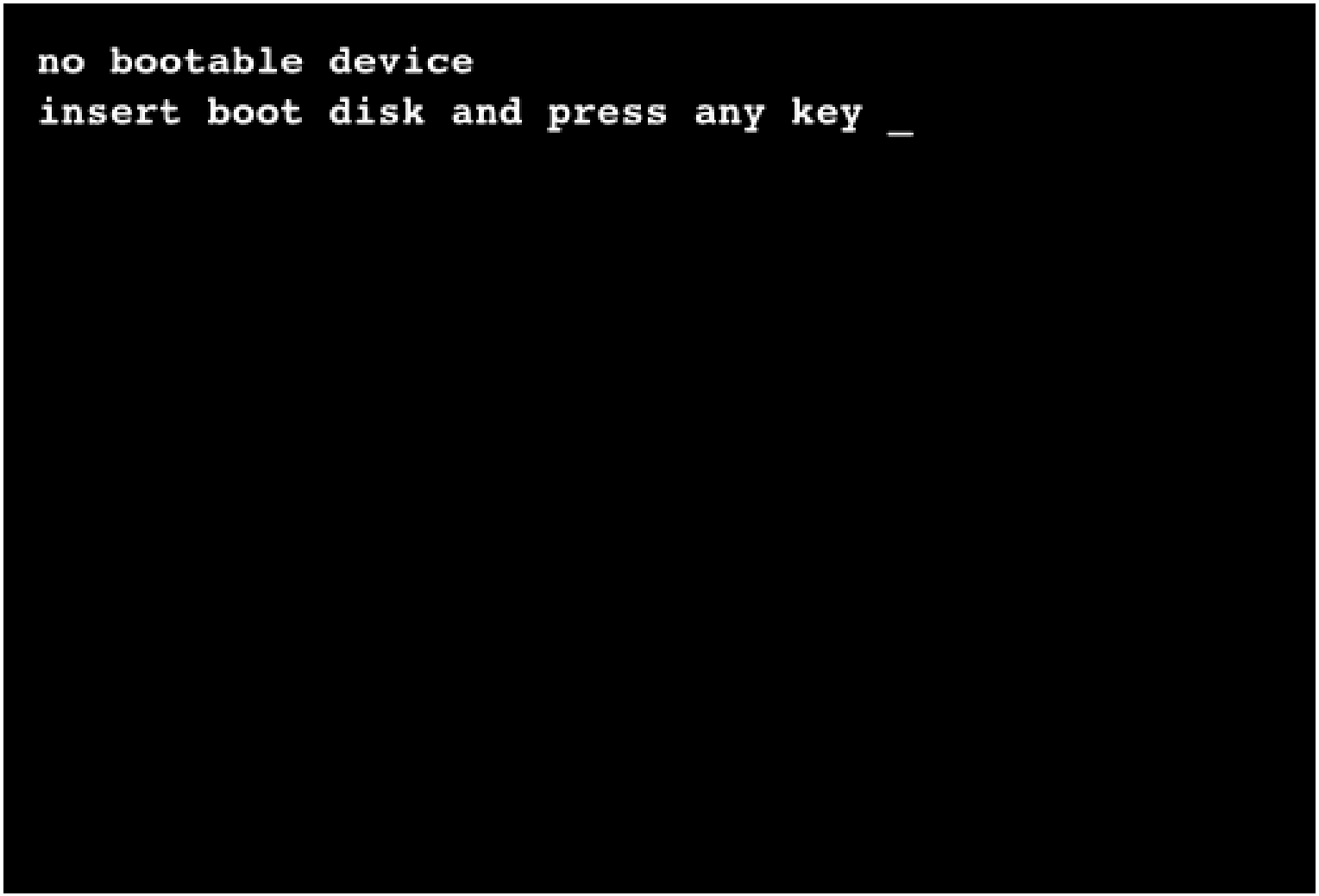
    http://www.heise.de/security/artikel/Dammbruch-bei-WEP-270672.html
- WPA
  - besser
  - Schwachstellen vorhanden

    http://www.heise.de/security/meldung/WPA-angeblich-in-weniger-als-15-Minuten-knackbar-215626.html
- WPA2
  - aktuell zu empfehlen

WLAN ctd.

- SSID verstecken
  - kein Schutz
  - eher verringerter Benutzerkomfort
- MAC-Filter
  - kein absoluter Schutz
  - kann Gefahr bei Weitergabe des Passwortes verringern
- Passwort/Pre-shared-key
  - keine Default-Passörter
  - sichere Passwörter (siehe weitere Folien)
  - sonst ist auch WPA2 Verschlüsselung nicht sicher

Datenverlust - Beispiele



Datenverlust - Beispiele

(Bild von Fehlermeldung wegen Datenverlust)

Quelle: http://www.eval.at/EVAL_CMS/support/technik_faq.aspx

Datenverlust - Beispiele

Datenspeicherung

Was machen wir in so einem Fall?

Datenspeicherung

Wir erinnern uns an die Einleitung:

...

Problem:

Mangelnde Sicherheit fällt erst auf, wenn es zu spät ist!

Datenverlust - Ursachen

- defektes Speichermedium
  - Festplatte
  - USB-Stick
  - CD/DVD
  - ...
- versehentliches Löschen/Überschreiben
- Softwarefehler (z.b. beim Speichern)
- böswillige Absichten von Angreifern
- ...

Datenspeicherung - Maßnahmen

- Backup
- Backup
- Backup
- und nochmal Backup

Backup

- periodisch
- auf getrenntem, unabhängigem System
- optional: geografisch entfernt
- idealerweise automatisch

Backup - Vorraussetzung

- geordnete Ablage von Daten
- optimalerweise zentral
  - mehrere PCs
  - verschiedene Datenträger mit verschiedenen Versionen
- klare Struktur: welches Backup wurde wann erstellt
- Recovery-Prozedur testen

Backup - Beispiele

- CD oder DVD, Daten in bestimmtem Zeitraum brennen
- Vorteile:
  - WORM - sicher gegen Fehler beim Backup
- Nachteile:
  - händische Abläufe
  - zeitaufwändig
  - Speicherplatz ev. zu wenig

Backup - Beispiele

- externe Festplatte, Daten in bestimmtem Zeitraum kopieren
- Vorteile:
  - kostengünstig
  - einfach in der Handhabung
- Nachteile:
  - händische Abläufe
  - zeitaufwändig
  - bei Fehler ev. alles verloren

Backup - Software

- führt automatisch Backups durch
- verschiedene Ziele konfigurierbar
  - Netzwerklaufwerk
  - externe Festplatte
  - ...
- Beispiele:
  - Linux: rsync in Kombination mit cron
  - OSX: Time-Machine
  - Windows: zahlreiche Programme verfügbar
- soll den individuellen Anforderungen entsprechen
- Software vor Verwendung ausreichend testen (insbesondere auch die Wiederherstellung!)

Backup - Optimierungen

- Automatische Backups
  - Network Attached Storage
  - Versionierung mittels Snapshots
- Geografisch entfernt
  - Backupmedium nicht im selben Feuerwehrhaus
  - sonst gehen ev. Hauptsystem und Backup verloren

RAID-Systeme

- heißt **R**edundant **A**rray of **I**nexpensive **D**isks bzw. **R**edundant **A**rray of **I**ndependent **D**isks
- Empfehlenswert, ersetzt aber kein Backup!

- schützt gegen
  - defekte Speichermedien (Festplatte)
  - (ausgenommen RAID 0, stripe)
- schützt **nicht** gegen
  - versehentliches Löschen/Überspeichern
  - Speicher-Fehler bei Programmabsturz
  - ...

Passwörter - Beispiele

(Bild von Passworteingabe mit Default-User)

Quelle:

http://wiki.nas4free.org/lib/exe/fetch.php?media=wiki:documentation_setup_and_user_guide_basic.auth.png

Passwörter - Beispiele

(Bild von Default-Passwoertern)

Quelle: http://www.dreamsrain.com/images/2011/08/Wireless-Router-Default-Passwords.png

Passwörter

- Default-Passwörter sofort ändern
- nicht überall das gleiche Passwort
- eventuell Programm zur Passwortverwaltung
  - hilfreich bei vielen Passwörtern
  - z.b. http://keepass.info/
  - Passwort-Datenbank wird mit Master-Passwort verschlüsselt
- Passwörter sollen sicher aber leicht merkbar sein
  - konkrete Anforderungen hängen vom Sicherheitsbedürfnis ab...

Danke für die Aufmerksamkeit!

(Comic zu Passwortsicherheit)

Seit Ihrer erfolgreichen Schulung zur Passwortsicherheit gibt es keine Passwortnotizen mehr auf den Schreibtischen...

Quelle: http://vischer-consulting.de/images/Comic_IT-Sicherheit_Passwort.jpg

weitere Informationen

- http://de.wikipedia.org/wiki/Datensicherung
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- Sichere Passwörter http://xkcd.com/936/