10 Schritte zu mehr IT-Sicherheit

Jürgen Kunert

InformationsTechnologie Effizient Einsetzen, Hamburg

Einleitung

IT
EE
InformationsTechnologie Effizient Einsetzen

Im 21. Jahrhundert ist eine funktionierende und sichere IT-Infrastruktur die Grund-Voraussetzung für die Leistungsfähigkeit und Überlebensfähigkeit jedes Unternehmens.

„Sie sind abhängig von einer funktionierenden IT."

Risiken

- menschliches Verhalten
- das Aushebeln der technischen Mechanismen durch Schadsoftware
- Hardware-Ausfall
- Verlust von
  - Arbeitsfähigkeit
  - von vertraulichen Informationen (Preise, Produktionsgeheimnisse, ..)
  - Kommunikationsmöglichkeiten
- Erpressbarkeit
- …

Schutzziele

- **Integrität:** betrifft die Daten selbst
  Sind die Daten wirklich originalgetreu (z.B. seit Ihrer Erzeugung unverändert?)
- **Verfügbarkeit:** betrifft Zugang zu den Daten
  Sind die Daten (für Befugte!) abrufbar, wenn man sie benötigt?
  a) in dem Moment oder b) überhaupt noch
- **Vertraulichkeit:** betrifft Zugang zu den Daten
  Kann keine unbefugte dritte Person die Daten lesen?
- **Authentizität:** betrifft beteiligte Personen
  Ist die/der Autorin/Leserin der Daten wirklich die behauptete Person?

Abwägung

IT EE
InformationsTechnologie Effizient Einsetzen

- Spannungsverhältnis zwischen Aufwand und Sicherheit
- Spannungsverhältnis zwischen den Schutzzielen
  - Wie viel Integrität, Verfügbarkeit, Vertraulichkeit, … brauche ich?

- Absolute Sicherheit gibt es nicht!

1. Sensibilisierung / Training der Benutzer

IT EE
InformationsTechnologie Effizient Einsetzen

- Nachdenken vor den Agieren! – Gesunder Menschenverstand
- Nicht einfach auf Links klicken
- eMail-Adresse kontrollieren
- Anlagen im Zweifel nicht öffnen
- Beispiel: Bewerbungs-Trojaner
- Social Engineering!

- MangelndesKnowHow: führt ggf. zu unbeabsichtigtem Löschen von Daten, Senden von sensiblen Daten an Unberechtigte, fälschliches Verändern von Daten, zu fehlerhafter Konfiguration von Systemen

2. Backup

IT EE
InformationsTechnologie Effizient Einsetzen

- Daten, die nicht (**regelmäßig**) gesichert werden, können Sie auch nicht wiederherstellen!
- Backups, die nicht mindestens in einem Test erfolgreich **wiederhergestellt** wurden, verdienen den Namen „Backup“ nicht.
- Backup-Lösungen und –Daten, für die niemand in der Firma direkt **verantwortlich** ist, sind definitiv schlechte bis unbrauchbare Sicherungen.
- Sicherungen, die in Sie im **gleichen Raum/Gebäude** lagern, in dem sich auch Ihre restliche IT befindet, werden einen ernsten Zwischenfall wie Feuer, Überschwemmung und so weiter, sicher nicht überstehen.

2. Backup - Risikobetrachtung

IT EE
InformationsTechnologie Effizient Einsetzen

- Risikobetrachtung:
  - Was sind erfolgskritische Daten und Systeme?
  - Was bedeutet der Datenverlust für das Unternehmen? Kosten, Reputation, Kundenverlust, Ende, …?
  - Wie viele Tage kann ihr Unternehmen bei einem Ausfall überleben?
  - SPOF (Single Point Of Failure)

- **Katastrophenplan**
  - Was passiert, wenn Daten und/oder Systeme nicht verfügbar sind?
  - Wenn ihr PC nicht verfügbar ist, was machen Sie dann?
  - Versicherung?

2. Backup – Fragen

IT EE
InformationsTechnologie Effizient Einsetzen

- Was für Daten und Geräte haben Sie?
- Wer hat die Verantwortung?
- Was wird gesichert, wenn Dateien in Bearbeitung sind?
- Datenmenge, auch für die Rücksicherung wichtig
- Wachstum der Daten?
- Sicherungs-Rhythmus?
- Vollsicherung vs. nur Sicherung von Änderungen
- Aufbewahrungsfristen beachten
- Hardware und Betriebssystem? Server, virtuelle Maschinen, Client-PCs, Mobilgeräte?
- Lizenzen
- Installationsmedien
- Band, Festplatte, CD/DVD, Cloud, Laptop?
- Ort für dieAufbewahrung der Backups
- Datenschutz?

- Wirtschaftlichkeit?
- Versicherung abschließen?

3. Updates

IT EE
InformationsTechnologie Effizient Einsetzen

- Betriebssystem (Windows Update, iOS, Android, …)
- Anwendungen (Office Update, Domino Update, …)
- Browser
- Browser Add-Ons (Adobe Flash)
- Smartphone-Apps
- Wenn möglich automatisieren

- Windows XP, Windows Server 2003?

4. Passworte

- sichere Passworte verwenden - nicht „password“
- Für jede Stelle ein einzigartiges Passwort verwenden
- Wenn jemand Zugriff auf ihr Mail-Konto hat, dann kann er auch Passworte wiederherstellen
- Einmal-Konten verwenden
- Passwort-Manager verwenden

5. Rechtevergabe

IT EE
InformationsTechnologie Effizient Einsetzen

- nicht mit Administrator-Rechten arbeiten
- nicht zu viel Rechte
- nicht zu wenig Rechte

- Wer hat Zugriff auf welche Systeme/Funktionen?
- Ist geregelt, wer was darf, können muss?
- nicht benötigte Software deinstallieren/deaktivieren
- Wer kennt das Administrator-Passwort?
- Wer kennt das Passwort eines Kollegen? Urlaubsvertretung?
- Was passiert, wenn der einzige Mitarbeiter, der das Passwort kennt, nicht mehr da ist?

6. Firewall

IT EE
InformationsTechnologie Effizient Einsetzen

- … ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.

- Hardware-Firewall am Internet-Zugang
- Software-Firewall auf dem PC/Laptop
- **Mindestens eine davon**
- professionell eingerichtet … und gewartet

7. Schutz vor Malware

IT EE
InformationsTechnologie Effizient Einsetzen

- Empfehlung: externer Virenscanner für eMail (beim Provider)
- Ein lokaler Virenscanner mit aktuellen Patterns
- zwei Virenscanner kämpfen gegeneinander und stören den Anwender und sich gegenseitig

- Wenn Sie unsicher sind, ob sich Schadsoftware auf ihrem Rechner befindet:
  http://housecall.trendmicro.com/de/
  https://www.eset.com/us/home/online-scanner/

8. Sicherheits-Einstellungen in Programmen

IT EE
InformationsTechnologie Effizient Einsetzen

- Sicherheitseinstellungen in Programmen
  - Anzeige statt Ausführen von MS Office-Dokumenten
  - Browser-Sicherheitseinstellungen
  - Email-Programm (Javascript deaktivieren)