SCHUSTER WALTHER
IT-Business AG

Sicherheit im IT Umfeld

Eine Betrachtung aus der Sicht
mittelständischer Unternehmen

Sicherheit im IT Umfeld

SCHUSTER WALTHER
IT-Business AG

- Gibt es eine Bedrohung für mein Unternehmen ?
- Das typische IT Umfeld im Mittelstand,
  welche Gefahrenquellen birgt es ?
- Sicherheit, wie wird damit umgegangen ?
- Wer trägt die Verantwortung ?
- Ist Sicherheit realisierbar ?
- Welche Maßnahmen sollten grundsätzlich durchgeführt werden ?

Gibt es eine Bedrohung für mein Unternehmen ?

Durch das stetige Steigen der Anforderungen an die IT Struktur
im Unternehmensumfeld, ist auch deren Komplexität gewachsen.

- *Unternehmensdaten werden elektronisch verarbeitet*
- *Unternehmenskommunikation findet immer öfter digital statt*
- *Unternehmensprozesse werden zunehmend EDV gestützt abgebildet*

Gibt es eine Bedrohung für mein Unternehmen ?

Jährliche Verdoppelung an bekannten Sicherheitslücken

- 70 % aller Unternehmen hatten bereits Virenvorfälle
- 36 % meldeten Datenverluste mit wirtschaftlicher Konsequenz
- 20 % bemerken DOS-Attacken oder unerlaubte Zugriffe

Ca 21 Milliarden € wirtschaftliche Schäden allein durch Viren
Ca 33 Milliarden € wirtschaftliche Schäden durch Datenverluste

Schuster & Walther IT-Business AG

Gibt es eine Bedrohung für mein Unternehmen ?

- **Höhere Gewalt**
  z.B. Blitzschlag, Feuer, Erdbeben, Personalausfall
- **Organisatorische Mängel**
  z.B. fehlende oder unzureichende Regelungen für Wartung, Dokumentation, Test und Freigabe, fehlende Auswertung von Protokolldaten
- **Menschliche Fehlhandlungen**
  z.B. fehlerhafte Systemnutzung oder -administration, fahrlässige Zerstörung, von Geräten oder Daten, Nichtbeachtung von Sicherheitsmaßnahmen
- **Technisches Versagen**
  z.B. Ausfall von Versorgungs- und Sicherheitseinrichtungen, Softwarefehler, defekte Datenträger
- **Vorsätzliche Handlungen**
  z.B. Manipulation/Zerstörung von Geräten, Manipulation an Daten oder Software, Viren, trojanische Pferde, Abhören, Maskerade

Gibt es eine Bedrohung für mein Unternehmen ?

Hacken wird als Volkssport betrieben !

- Hacking Tools können problemlos im Internet gefunden werden.
- Windows Oberflächen erleichtern die Bedienung.

Script Kiddies versuchen sich als Hacker, oftmals aber nach dem Motto:

„DENN SIE WISSEN NICHT WAS SIE TUN !!!“

Gibt es eine Bedrohung für mein Unternehmen ?

SCHUSTER WALTHER IT-Business AG

Noch nie war es so einfach mit so wenig Aufwand so grossen Schaden anzurichten !!!

Gibt es eine Bedrohung für mein Unternehmen ?

SCHUSTER WALTHER IT-Business AG

Beispiel Digitale Kommunikation

eMails sind mit Postkarten vergleichbar, jeder kann Sie lesen.

Eine eMail kann gefälscht oder verändert werden, wenn keine Schutzmassnahmen getroffen werden.

Schuster & Walther IT-Business AG

Gibt es eine Bedrohung für mein Unternehmen ?

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe

Sicherheit, wie wird damit umgegangen ?

- 68 % der Unternehmen führen keine regelmässige Sicherheits analyse im eigenen Betrieb durch
- 60 % verzichten auf den Einsatz entsprechender Programme
- 46 % der Firmen haben keine Informationspolitik zum Thema „IT-Sicherheit“
- 30 % aller Unternehmen stufen „Sicherheit“ als lästige Notwendigkeit ein
- Nur 5 % der IT Ausgaben werden für Sicherheit aufgewendet
- Sicherheit = Firewall und Virenschutz ?!

Sicherheit, wie wird damit umgegangen ?

SCHUSTER WALTHER IT-Business AG

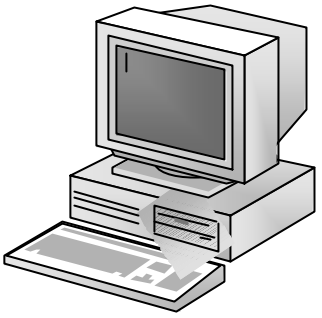
Am Arbeitsplatz

Wo sucht man, wenn man ein Passwort finden möchte ?

Unter der Tastatur

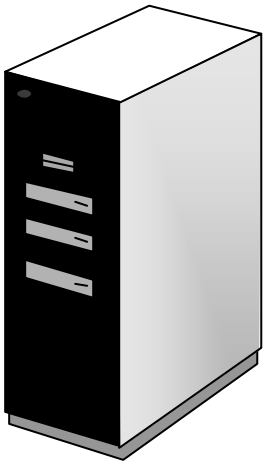
Am Monitor

In der Schublade am Arbeitsplatz



Sicherheit, wie wird damit umgegangen ?

SCHUSTER WALTHER IT-Business AG



Backup Strategien, ein Beispiel:

Sicherung eingerichtet : OK

Sicherung täglich geprüft : OK

Bänder regelmässig gewechselt: OK

Rücksicherung getestet: ???????????

Schuster & Walther IT-Business AG

Wer trägt die Verantwortung ?

SCHUSTER WALTHER IT-Business AG

„Sicherheitsvorfälle sind immer Chefsache !!!“

Ist Sicherheit realisierbar ?

SCHUSTER WALTHER IT-Business AG

IT Sicherheit im Unternehmen zu etablieren muss nicht teuer sein !

Ist Sicherheit realisierbar ?

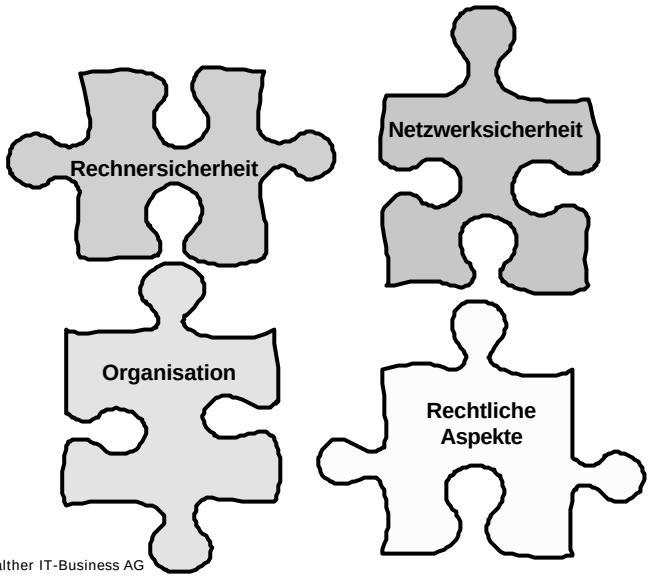
Was muss getan werden ?

- Analyse des Sicherheitsbedarfs durchführen
- Bewusstsein für IT Sicherheit im Unternehmen wecken
- Erstellung einer verständlichen Sicherheitsrichtlinie
- Konsequente Überwachung der Sicherheitsrichtlinie

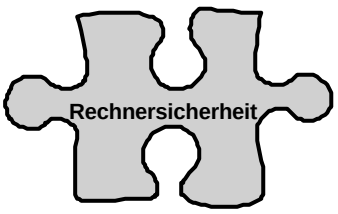
Welche Maßnahmen sind wichtig !

- Einführung eines unternehmensweiten Virenschutz Systems
- Bei Anbindung an das Internet grundsätzlich Einsatz einer Firewall
- Verlässliches Backup System (Software und Hardware auf aktuellem Stand sowie konsequente Überprüfung)
- Zeitnaher Austausch bzw. Entfernen fehlerhafter Hardware
- Schulung und Sensibilisierung der Mitarbeiter
- Ausbildung und Benennung eines Sicherheitsbeauftragten für IT Sicherheit

Ist Sicherheit realisierbar ?



Ist Sicherheit realisierbar ?



Alle Clients sollten mit adäquatem Virenschutz ausgestattet sein

Anmeldung an Serversystemen nur mit sicherem „Starkem“ Passwort

keine Individual Anbindung an das Internet (Modem, ISDN, etc…)

defekte Hardware zeitnah austauschen

Ist Sicherheit realisierbar ?

Internetzugang nur über Firewall

Mailserver mit Virenschutz versehen

Administrator Account = Everyone

Datenbestand über Backup Strategien absichern

Ist Sicherheit realisierbar ?

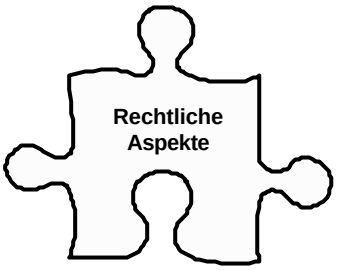
Durchführung einer Risiko und Sicherheitsanalyse

Erstellung einer Sicherheitsrichtlinie

Benennung eines Verantwortlichen für die IT Sicherheit

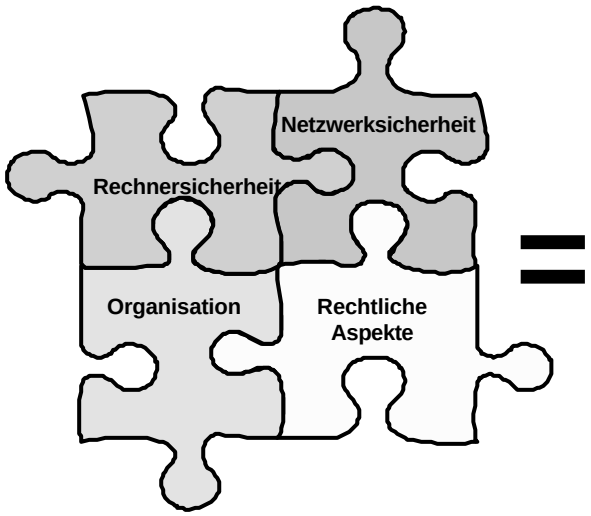
konsequentes Überwachen der Sicherheitsrichtlinien

Ist Sicherheit realisierbar ?



Einbeziehen der Geschäftsleitung in die Sicherheits Strategie

Ist Sicherheit realisierbar ?



=

Sicherheit im IT Umfeld

Informationsquellen

Bundesamt für Sicherheit und Informationstechnik
www.bsi.de

Virtuelles Datenschutzbüro
www.datenschutz.de

IT Security Forum
www.it-security-forum.de

Industrie und Handelskammern
www.ihk.de