IT-Sicherheit

Axel Pemmann

03. September 2007

Ziel des Kurses, Fokus

Lernziele

1. Kennnen -und Verstehenlernen von Bedrohungsszenarien in IT-Sytemen
2. Aneignung von Fähigkeiten zum erfolgreichen Einsatz von Schutzmaßnahmen

Kurs-Fokus

1. Technische und organisatorische Maßnahmen zur Gewährleistung von IT-Sicherheit
2. Sensibilisierung für dieses komplexe Thema

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- «Faktor Mensch » als ursächliche, treibende Kraft

Die Reihenfolge der Themenschwerpunkte

Der Rote Faden durch den Kurs

Aufbau einer sicheren digitalen Infrastruktur, keine Komponente darf ausgelassen werden!

- Hardware
- Betriebssystem
- Anwendungssoftware
- Netzwerke mit ihren Techniken
- Netzwerkdienste und -anwendungen
- ≪Faktor Mensch ≫ als ursächliche, treibende Kraft

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was fällt Ihnen allgemein zum Begriff «Sicherheit» ein?

- Wohnung abschließen
- Handtasche immer fest halten
- Thema Autofahren
  - Angurten
  - Airbag
  - ABS/EBV, STC, DSTC, ...
- Blitzableiter
- Schwimmring bzw. -weste
- Absperrung einer Baustelle
- Bekleidung
- Kabelisolierung, Sicherung
- Versicherung

Was Hänschen nicht lernt...

Kindern schon muss man lernen:

- Pass auf, nimm dich in acht!
- Lass den bösen Wolf nicht herein!
- Nimm keine Bonbons von fremden Leuten!
- Vergiss nichts!

Wie verhalten wir uns?

– Anwendung altbewährter Prinzipien, gesundes Misstrauen!
– Computer sind keine Wundermittel
– Lediglich Kommunikation zwischen Mensch und Maschine

Was Hänschen nicht lernt...

Kindern schon muss man lernen:

- Pass auf, nimm dich in acht!
- Lass den bösen Wolf nicht herein!
- Nimm keine Bonbons von fremden Leuten!
- Vergiss nichts!

Wie verhalten wir uns?

– Anwendung altbewährter Prinzipien, gesundes Misstrauen!
– Computer sind keine Wundermittel
– Lediglich Kommunikation zwischen Mensch und Maschine

Was Hänschen nicht lernt...

Kindern schon muss man lernen:

- Pass auf, nimm dich in acht!
- Lass den bösen Wolf nicht herein!
- Nimm keine Bonbons von fremden Leuten!
- Vergiss nichts!

Wie verhalten wir uns?

– Anwendung altbewährter Prinzipien, gesundes Misstrauen!
– Computer sind keine Wundermittel
– Lediglich Kommunikation zwischen Mensch und Maschine

Was Hänschen nicht lernt...

Kindern schon muss man lernen:

- Pass auf, nimm dich in acht!
- Lass den bösen Wolf nicht herein!
- Nimm keine Bonbons von fremden Leuten!
- Vergiss nichts!

Wie verhalten wir uns?

– Anwendung altbewährter Prinzipien, gesundes Misstrauen!
– Computer sind keine Wundermittel
– Lediglich Kommunikation zwischen Mensch und Maschine

Was Hänschen nicht lernt...

Kindern schon muss man lernen:

- Pass auf, nimm dich in acht!
- Lass den bösen Wolf nicht herein!
- Nimm keine Bonbons von fremden Leuten!
- Vergiss nichts!

Wie verhalten wir uns?

– Anwendung altbewährter Prinzipien, gesundes Misstrauen!
– Computer sind keine Wundermittel
– Lediglich Kommunikation zwischen Mensch und Maschine

Warum einfach, wenn es kompliziert geht!

- Computer arbeiten mit digitalen Informationen
- Digitale Informationen müssen für Menschen verständlich gemacht werden
- Dazu sind je nach Aufgabe verschiedene Stufen der Übersetzung erforderlich
- Übersetzungsstufen werden mit Hilfe von Schichtenmodellen definiert
- ...

Parallele Verwendung verschiedener Sicherheitsmaßnahmen

Unerwünscht: Domino-Effekt

Warum einfach, wenn es kompliziert geht!

- Computer arbeiten mit digitalen Informationen
- Digitale Informationen müssen für Menschen verständlich gemacht werden
- Dazu sind je nach Aufgabe verschiedene Stufen der Übersetzung erforderlich
- Übersetzungsstufen werden mit Hilfe von Schichtenmodellen definiert
- ...

Parallele Verwendung verschiedener Sicherheitsmaßnahmen

Unerwünscht: Domino-Effekt

Warum einfach, wenn es kompliziert geht!

- Computer arbeiten mit digitalen Informationen
- Digitale Informationen müssen für Menschen verständlich gemacht werden
- Dazu sind je nach Aufgabe verschiedene Stufen der Übersetzung erforderlich
- Übersetzungsstufen werden mit Hilfe von Schichtenmodellen definiert
- ...

Parallele Verwendung verschiedener Sicherheitsmaßnahmen

Unerwünscht: Domino-Effekt

Warum einfach, wenn es kompliziert geht!

- Computer arbeiten mit digitalen Informationen
- Digitale Informationen müssen für Menschen verständlich gemacht werden
- Dazu sind je nach Aufgabe verschiedene Stufen der Übersetzung erforderlich
- Übersetzungsstufen werden mit Hilfe von Schichtenmodellen definiert
- ...

Parallele Verwendung verschiedener Sicherheitsmaßnahmen

Unerwünscht: Domino-Effekt

Warum einfach, wenn es kompliziert geht!

- Computer arbeiten mit digitalen Informationen
- Digitale Informationen müssen für Menschen verständlich gemacht werden
- Dazu sind je nach Aufgabe verschiedene Stufen der Übersetzung erforderlich
- Übersetzungsstufen werden mit Hilfe von Schichtenmodellen definiert
- ...

Parallele Verwendung verschiedener Sicherheitsmaßnahmen

Unerwünscht: Domino-Effekt

Das Böse lauert überall!

Virus-Attacke: Landratsamt bleibt zu

Aue. Ein Computer-Virus hat das Landratsamt Aue-Schwarzenberg weiterhin im Griff. Deshalb bleibt die Behörde heute und morgen geschlossen. Betroffen sind alle 360 Verwaltungs-Computer sowie zentrale Datenspeicher. Um den Virus, der das interne Rechnernetzwerk am Dienstag befallen hat, auszumerzen, wurden eigens Fachleute einer Leipziger Spezialfirma zu Hilfe gerufen. (TRÖ)

Zeitungsmeldung der „Freien Presse“ vom 19.09.2006

Eine weitere Schreckensmeldung

Gartner befürchtet Wurmattacke – Weitere Löcher entdeckt

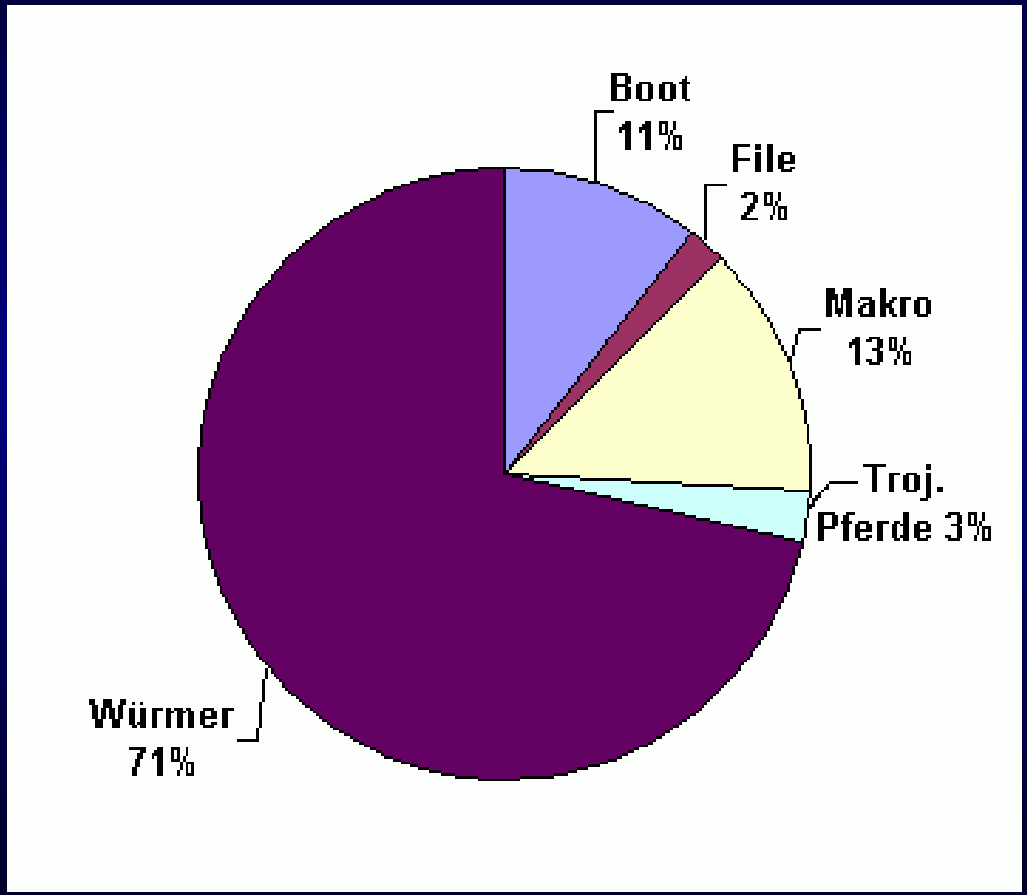
Microsoft kämpft mit Sicherheitslücken

Redmond (ab) – Mit Tipps und Updates will Microsoft seinen Kunden helfen, die Sicherheit zu verbessern. Allerdings muss man ständig neue Löcher stopfen.

Unter `www.microsoft.com` hat der Softwareriese ein weiteres Webforum zur ITSicherheit eröffnet. Zudem erläutert ein Whitepaper unter dem Titel „Security at Microsoft“, wie der Konzern selbst mit monatlich 100.000 Einbruchsversuchen sowie 125.000 virenverseuchten EMails umgeht...

Zeitschrift: COMPUTER ZEITUNG, Ausgabe: 49/2003
Mehr dazu: `http://www.netigator.de/...`

Das Böse lauert überall!



Halbjahresbericht Virenmeldungen in Deutschland 2001, Bild: BSI

Sind sie alle böse und hinterhältig?

Personen, die hinter den Angriffen stehen:

- White Hats (Hacker)
- Grey Hats
- Black Hats (Cracker)
- Script Kiddies
- Mitarbeiter (Unwissenheit lässt sich nicht patchen)

Sind sie alle böse und hinterhältig?

Personen, die hinter den Angriffen stehen:

- White Hats (Hacker)
- Grey Hats
- Black Hats (Cracker)
- Script Kiddies
- Mitarbeiter (Unwissenheit lässt sich nicht patchen)

Sind sie alle böse und hinterhältig?

Personen, die hinter den Angriffen stehen:

- White Hats (Hacker)
- Grey Hats
- Black Hats (Cracker)
- Script Kiddies
- Mitarbeiter (Unwissenheit lässt sich nicht patchen)

Sind sie alle böse und hinterhältig?

Personen, die hinter den Angriffen stehen:

- White Hats (Hacker)
- Grey Hats
- Black Hats (Cracker)
- Script Kiddies
- Mitarbeiter (Unwissenheit lässt sich nicht patchen)

Sind sie alle böse und hinterhältig?

Personen, die hinter den Angriffen stehen:

- White Hats (Hacker)
- Grey Hats
- Black Hats (Cracker)
- Script Kiddies
- Mitarbeiter (Unwissenheit lässt sich nicht patchen)

Was sind grundsätzliche Inhalte der IT-Sicherheit?

Der Schutzbedarf wird für die drei Grundwerte

- Vertraulichkeit
- Integrität
- Verfügbarkeit

definiert. Dabei muss der Schutzbedarf für alle drei Grundwerte gesondert betrachtet werden.

Die Schutzziele beim BSI

Studieren Sie dazu:
`www.bsi.de/gshb/webkurs/gskurs/seiten/s4140.htm`

Was sind weitere Inhalte der IT-Sicherheit?

Zusätzlich gibt es für die Kryptographie die Grundziele:

- Authentizität
- Verbindlichkeit

Die Schutzziele zur Kryptographie beim BSI

Studieren Sie dazu:
`www.bsi.de/gshb/deutsch/m/m03023.htm`

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Wer kann die harte Nuss knacken?

Die Hardware spielt in der IT-Sicherheit eine erste, wichtige Rolle:

- Zertifizierte Hardware
- Spiegelung von Festplatten, am besten mit Hardware-Raid
- Sicherungstechnik im Gerät (Magnetband, DVD-Brenner)
- Unterbrechungsfreie Stromversorgung (USV)
- Sicheres Bootverhalten
- Hardware Lock, Authentifizierung mit Hilfe von Dongles

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Weich und anfällig: Killing me softly?

Die Software haucht Rechnern einen Anflug von Leben ein:

- Betriebssystem (Verwaltet Hardware und ist Schnittstelle zum Menschen)
- Anwendungen (Eigentliche Programme, die einem bestimmten Zweck dienen)

Daneben benötigt man unter Umständen weitere Software:

- Treiber für die Inbetriebnahme bestimmter Hardware
- Effiziente Werkzeuge für Verwaltungsaufgaben (z.B. Server, Benutzer, Dateien)
- Werkzeuge für Verbesserung der Sicherheit (Virenscanner, Intrusion Detection Systems)
- Betriebssystem-Add-Ons für erweiterte Fähigkeiten (Java-Runtime-Umgebung, MS-Dot-Net-Umgebung)
- Add-Ons für Anwendungen (Firefox-Browser, Thunderbird-Mailclient)

Softly, aber ein bisschen sicherer

Gute Software ist nicht nur eine Sache der Programmierung. Die ganze Komplexität dieses Vorhabens muss sich in einem adäquaten Netzwerk an Informationen widerspiegeln, das über technologische Aspekte hinaus reicht. Die darin gespeicherten Abhängigkeiten bilden den Dreh- und Angelpunkt in der Schaffung eines stabilen, sich entwickelnden Produktes.

`http://www.gute-software.com/geist`

Das KISS-Prinzip: Ein Professor bringt es auf den Punkt

There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies.

Der erste Teil dieses Zitates von Prof. Charles Antony Richard Hoare (Emeritus Professor of Computing, University of Oxford) ist eines unserer Leitmotive.

`http://www.o3-software.de/de/Philosophie.xhtml`

Unterstützung durch die Disziplin «Softwaretechnik»

Qualitätsmerkmale von Software

Klassifikation von Qualitätsmerkmalen

- externe Qu.: sichtbar für Nutzer
- interne Qu.: sichtbar für Entwickler

} in engem Zusammenhang, keine scharfe Unterscheidung

Qualitätsmerkmale:

- Korrektheit
- Zuverlässigkeit
- Robustheit
- Effizienz
- Benutzerfreundlichkeit
- Verifizierbarkeit
- Wartbarkeit
- Korrigierbarkeit
- Wiederverwendbarkeit
- Wachstum/Evolution
- Portabilität
- Verständlichkeit
- Interoperabilität
- Produktivität
- Pünktlichkeit/Aktualität
- Sichtbarkeit

Einführung Softwaretechnik 30

Quelle: L. Rosenhainer, TU - Chemnitz

Sichere Installation eines Betriebsystemes

Bereits bei der Installation sind ein paar Dinge zu beachten:

1. Installation ohne physische Anbindung an ein Netzwerk (Im ungepatchten Zustand ist die Anfälligkeit für Viren und Würmer hoch!)
2. Einspielen aller notwendiger Patche
3. Deaktivieren kritischer Registry-Einträge (am besten mit xp-antispy)
4. Deaktivieren unnötiger administrativer Freigaben (`http://wiki.winboard.org/index.php/Administrative_Freigabe`)
5. Installation einer Firewall

Sind wir sauber? Machen wir die Probe aufs Exempel!

Typischer Schadcode: Malware
(Kunstwort aus Malicious Software)

- Viren
- Würmer (selbständige Verbreitung in Netzen)
- Trojaner
- Bot-Netze (Zusammenschluss gekaperter PCs)
- Spyware, Adware, Dialer

Virenscanner

Installieren Sie den Open Source-Virenscanner *ClamWin* und verifizieren Sie ihn mit dem Testvirus EICAR.

Sind wir gefährdet? Machen wir die Probe aufs Exempel!

Erweiterter Schadcode: Exploits

- Nutzt Sicherheitslücken in Software aus (Softwarefehler)
- Entsteht oft aus fehlender Längenabfrage einer Variablen
- Injiziert Shellcode als Nutzlast zum Ausführen von Aktionen

Angriffe aus dem Netz

Installieren Sie die Software *Framework* von `http://metasploit.com` und starten Sie Angiffe auf ein ungepatchtes System. Wiederholen sie die Tests nach dem Installieren von Patches.

Das wird eine hammerharte Sache!

Die Kunst, Unnützes wegzulassen:

- Dienste deaktivieren
- Kritische Software entfernen
- Protokolle deaktivieren bzw. deinstallieren

Siehe auch: `http://www.lrz-muenchen.de/services/betriebssysteme/nt/w2ksicherheit/`

Noch härter geht kaum noch: Ausbau zur Bastion

Aus dem Gloassar des BSI:

Bastion-Host: Application-Gateway, das exponiert steht und als erster Teil einer Firewall angegriffen wird.

Geeignete Betriebssysteme

- Workstations (Keine Home-Betriebssysteme!)
- Server-Betriebssysteme
- Spezielle Distributionen (z.B. IPCop)

Die beiden folg. Eigenschaften muss ein Betriebssystem unbedingt aufweisen:

- Manipulationssicherheit (engl. Untamperability)
- Unüberbrückbarkeit (engl. Unbypassability)

Quelle: `http://www13.informatik.tu-muenchen.de/lehre/seminare/WS0405/hauptsem/Ausarbeitung01.pdf`

Tools für MS-Windows 2000

- An Bord: Snap-In ≪Sicherheitskonfiguration und -analyse≫
- Nachinstallierbar: Microsoft Baseline Security Analyser

Testen Sie die Werkzeuge

Recherchieren Sie dazu im Internet, um weitere Informationen zu diesen Möglichkeiten zu finden.

Mehr Sicherheit durch Vertrauensbeziehungen

Sicherheit durch Anmelden an einem MS-Windows 2000 Domänen-Controller:

- Vertrauensstellung von Maschinen UND Benutzern zu einer Organisationseinheit
- Maßnahme: Gründen einer Domäne
- Begriffe in diesem Umfeld PDC/BDC, Kerberos

Sihe auch
`http://de.wikipedia.org/wiki/Domain_Controller`

Mehr Sicherheit durch zentrale Pflege

Erweiterung der Sicherheit durch Benutzung eines zentralen Verzeichnisdienstes:

- Ab Windows 2000 Server fester Bestandteil

Siehe dazu
`http://de.wikipedia.org/wiki/Active_Directory`

Supersicher mit Unix/Linux

- An-Bord-Werkzeuge:
  rpm, apt, find, md5sum, lsmod, netstat, john,
  SuSE-Skript: secchk, ...
- Software-Update bei Debian:
  apt-get update && apt-get upgrade
- Nachinstallierbar für hostbasierte Einbruchserkennung:
  Aide, Tripewire, ...

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Was sagt der Gesetzgeber zu Schadsoftware?

Verstöße gegen das Datenschutzgesetz können Ärger bringen:

- § 43 BDSG: Ordnungswidrigkeit (Unbefugte Verarbeitung nicht offenkundiger Daten)
- § 44 BDSG Straftat (Handlungen im Sinne von § 43 Abs. 2 mit Schädigungs-, Bereicherungsabsicht oder gegen Entgelt)
- § 303 a StGB Datenveränderung
- § 263 a StGB Computerbetrug
- § 202 a StGB Ausspähen von Daten

Vielen Dank für Ihre Aufmerksamkeit!

IT-Sicherheit

Axel Pemmann

03. September 2007

Ende