
Netzwerksicherheit und Netzwerkmanagement in der Praxis

Markus Brückner (markus.brueckner@stud.tu-ilmenau.de)

Fachgebiet Telematik - TU Ilmenau

Gliederung

- Einleitung
- Theorie
 - Aufstellen einer Sicherheitspolitik
 - Umsetzung einer Sicherheitspolitik
 - Netzwerkmanagement
 - ◆ Technologien
 - ◆ Verbindung Netzwerkmanagement ↔ Netzwerksicherheit
- Praxis
 - Beispiel FeM-Net

Sicherheit ist Kontrolle

Sicherheit ist Kontrolle

Im Kontext der Netzwerksicherheit:

- sämtlicher Netzwerkverkehr folgt der Sicherheitspolitik

Sicherheit ist Kontrolle

Im Kontext der Netzwerksicherheit:

- sämtlicher Netzwerkverkehr folgt der Sicherheitspolitik
- Verstöße gegen die Sicherheitspolitik sind nicht möglich oder werden sofort entdeckt

Sicherheit ist Kontrolle

Im Kontext der Netzwerksicherheit:

- sämtlicher Netzwerkverkehr folgt der Sicherheitspolitik
- Verstöße gegen die Sicherheitspolitik sind nicht möglich oder werden sofort entdeckt
- Technische Hilfsmittel zur Sicherung werden durch rechtliche Grundlagen unterstützt

Aufstellen einer Sicherheitspolitik

Theorie ⇒ Aufstellen einer Sicherheitspolitik

Definition:

A security policy for a system is like a foreign policy for a government: It defines aims and goals [...], a digital system without a security policy is likely to have a hodge-podge of countermeasures. The policy is what ties everything together.

Bruce Schneier: Secrets & Lies - Digital security in a networked world

Theorie ⇒ Aufstellen einer Sicherheitspolitik

Fünf Schritte zur Aufstellung einer Sicherheitspolitik:

- Bestimmung schützenswerter Sachen (Daten, Rechner, ...)
- Bedrohungsanalyse
- Analyse der Schwachstellen
- Risikoanalyse
- Auswahl von Sicherheitsmaßnahmen

Bedrohungsanalyse

Beantwortung der Frage: „Welche Objekte werden wodurch bedroht?“

⇒ Auflistung der schützenswerten Objekte mit den sie betreffenden Bedrohungen und den dadurch verletzten Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit)

Beispiel:

Objekt	Bedrohung	Verletztes Schutzziel
DNS-Server	Diebstahl	Verfügbarkeit
	Rootkit	Integrität, Verfügbarkeit
⋮	⋮	⋮

Analyse der Schwachstellen

Auflistung von Schwachstellen technischer und personeller Natur, welche die Bedrohungen der schützenswerten Objekte eintreten lassen können.

Beispiel:

Objekt	Bedrohung	Schwachstelle
DNS-Server	Diebstahl	ungesicherter Serverraum bestochener Wachdienst
⋮	⋮	⋮

Risikoanalyse

- Einführung von Wahrscheinlichkeitsklassen (sehr wahrscheinlich, wahrscheinlich, . . .)
- Analyse von Eintrittswahrscheinlichkeit und Schadenshöhe eines Angriffs

\Rightarrow Risiko = Schadenshöhe * Eintrittswahrscheinlichkeit

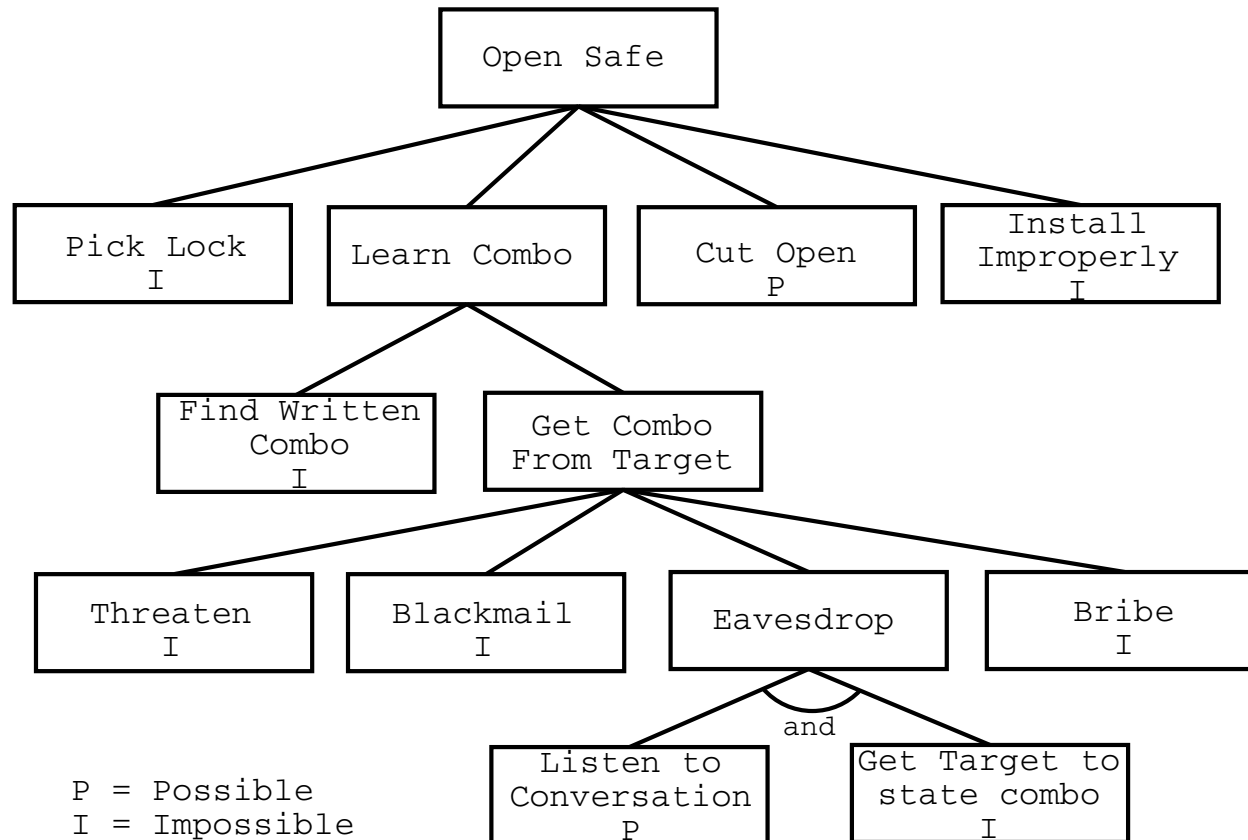
Hilfsmittel Bedrohungs­bäume („Attack trees“)

- Hilfsmittel zur Risikoanalyse
- Baumstrukturen, in deren Wurzel ein Ziel steht, welches durch verschiedene Unterziele realisiert werden kann (Kindknoten)

Theorie ⇒ Aufstellen einer Sicherheitspolitik

- Kindknoten können OR- (Erfüllung eines Unterzieles bedingt Erfüllung des Zieles) oder AND-verknüpft (Erfüllung aller Unterziele bedingt Erfüllung des Hauptzieles) sein
- Knoten können verschiedene Eigenschaften haben, welche Einfluss auf den Vaterknoten haben (Beispiel: Wahrscheinlichkeit eines Angriffs)

Beispiel Bedrohungsbaum



Nach: Bruce Schneier: Secrets & Lies - Digital security in a networked world

Umsetzung einer Sicherheitspolitik

Theorie ⇒ Umsetzung einer Sicherheitspolitik

Die gewählten Sicherungsmaßnahmen lassen sich in drei Kategorien einordnen:

Prävention Verhinderung von Angriffen

Detektion Entdeckung von Angriffen und Angriffsversuchen

Reaktion Gegenmaßnahmen bei Angriffsversuchen und Angriffen

Außerdem lässt sich eine Aufteilung in soziale/rechtliche und technische Maßnahmen vornehmen.

Theorie ⇒ Umsetzung einer Sicherheitspolitik

Soziale/Rechtliche Sicherungsmaßnahmen:

- Verschwiegenheitserklärungen
- Schulungen
- Arbeitsschutzbelehrungen
- Zuteilung von Aufgabenbereichen und Rechten
- ...

Wichtig: Alle technischen Sicherungsmaßnahmen sind nutzlos, wenn sie nicht durch soziale und rechtliche Maßnahmen unterstützt werden!

Theorie ⇒ Umsetzung einer Sicherheitspolitik

Technische Sicherungsmaßnahmen (unvollständig):

- Prävention:
 - Paketfilter
 - Proxy/ALG
 - Grafische Firewall
 - Authentifizierungs-/Autorisierungssysteme
 - PKI
 - Sichere Protokolle
- Detektion:
 - IDS
- Reaktion:
 - Portsecurity

Netzwerkmanagement

Technologien (im weitesten Sinn)

- SNMP
- Management-Konsolen per Telnet und SSH
- Webinterfaces
- SCEP
- DHCP, BOOTP
- ...

Verbindung Netzwerkmanagement \Leftrightarrow Netzwerksicherheit

- Viele verschiedene Sicherungsmaßnahmen, die Hand in Hand arbeiten sollen, erfordern zentrales Management (Konfiguration und Überwachung)
- Überblick über den Zustand des Netzwerks kann nur mit Hilfe von ausgereifter Sensorik erhalten werden
- Verschiedene Systeme liefern große Menge an Meldungen über aktuelle Vorgänge im Netz
 \Rightarrow Erkennung von Fehlern und Sicherheitsproblemen ist nur durch sinnvolle Vorfilterung durch Managementsysteme möglich

Beispiel FeM-Net

Übersicht FeM-Net

- Studentennetzwerk am Campus der TU Ilmenau
- aktuell (Juni 2003) etwa 1900 Geräte im Netz
- etwa 70 HP Procurve 2524 bzw. 2650 als Enduser-Switch
- Glas-Gigabit-Backbone mit Cisco Catalyst 6509 als Router
- Richtfunkstrecken Richtung Pörlitzer Höhe und Schlossmauer
- das größte Problem: 1500 Nutzer

Beispiel: Schutz des Netzes gegen Layer 2-Zugriff

- Bestimmung schützenswerter Sachen
 - Enduser-Switches
 - Backbone (Kabel, Router)
 - Funkstrecken

Praxis ⇒ Beispiel FeM-Net

- Bedrohungsanalyse

Objekt	Bedrohung	verletztes Schutzziel
Enduser-Switch	Anschluss eines fremden Rechners	Vertraulichkeit
Backbone	Einbau einer Bridge	Vertraulichkeit, Integrität
Funkstrecken	Einfügen einer Bridge	Vertraulichkeit, Integrität

- Analyse der Schwachstellen

Objekt	Bedrohung	Schwachstelle
Enduser-Switch	Anschluss Fremdrechner	ungesicherte Netzdose ungesicherter Serverraum

- Analyse der Schwachstellen (Fortsetzung)

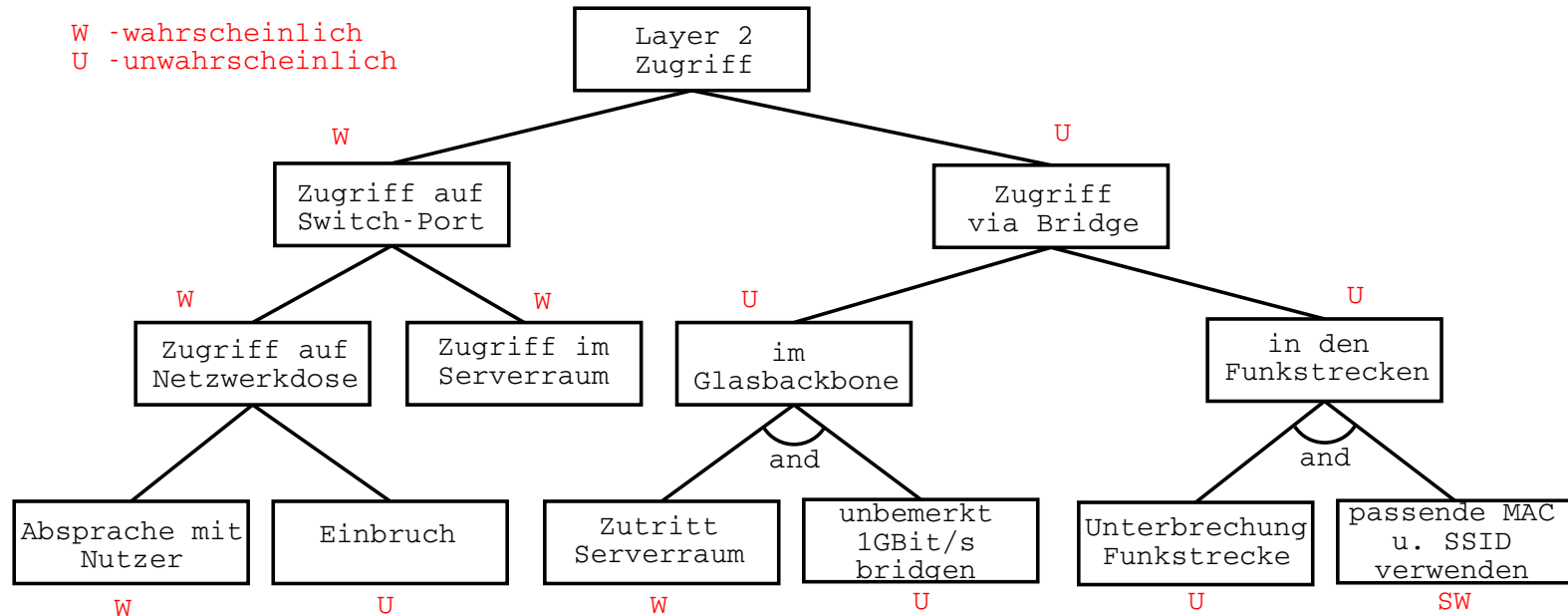
Objekt	Bedrohung	Schwachstelle
Backbone	Einbau einer Bridge	ungesicherter Serverraum Einspleissen einer Verbindung in das Glasfaserkabel
Funkstrecken	Einfügen einer Bridge	Verlauf der Strecken über öffentlichen Grund

- Risikoanalyse

- 4 Wahrscheinlichkeitsklassen: sehr wahrscheinlich, wahrscheinlich, unwahrscheinlich, unmöglich
- 3 Schadensklassen: groß, mittel, klein

Praxis ⇒ Beispiel FeM-Net

- Risikoanalyse (Fortsetzung) Bedrohungsbaum zur Bestimmung der Angriffswahrscheinlichkeit



⇒ Ein Zugriff auf Layer 2 ist wahrscheinlich.

⇒ Verlust von Vertraulichkeit und Integrität stellen große Schäden dar (Nutzerpasswörter etc.) ⇒ hohes Risiko

Auswahl von Sicherheitsmaßnahmen

- Technisch:
 - abschließbare Schränke (verhindern physischen Zugriff auf Patchfelder und Switches, Prävention)
 - Schranküberwachung (bemerkt Aufbrechen des Schrankes, Detektion)
 - Port-Security (bemerkt und verhindert fremde Netzwerkkarten, Detektion & Reaktion)
- Sozial/Rechtlich:
 - Zugangsverbot für Fremdrechner in der Nutzerordnung

Unterstützung der technischen Maßnahmen durch Netzwerkmanagement

- Scripting der HP2524 aus einer zentralen Datenbank per SSH
- Sammeln und Auswerten der Meldungen der Schranküberwachung an zentraler Stelle
- Auswertung von SNMP-Traps die die HP2524 bei Auftreffen eines Fremdrechners versenden können

Fragen? Anregungen? Öffentliche Hinrichtung?

**Fragen? Anregungen?
Öffentliche Hinrichtung?**

Danke für die Aufmerksamkeit

Danke für die Aufmerksamkeit

Folien: <http://www.slash-me.net/work/hs-nws/vortrag.pdf>

Kontakt: Markus Brückner <vortrag@slash-me.net>