

Hauptseminar Telematik

Netzwerksicherheit und Netzwerkmanagement in der Praxis

Markus Brückner

Matrikelnummer: XXXXX

Betreuer: Ralf Döring

31. August 2003

Inhaltsverzeichnis

1	Einleitung	2
2	Theorie Netzwerksicherheit	3
2.1	Aufstellen einer Sicherheitspolitik	3
2.1.1	Bestimmung schützenswerter Sachen	4
2.1.2	Die Bedrohungsanalyse	4
2.1.3	Analyse der Schwachstellen	5
2.1.4	Die Risikoanalyse	6
2.1.5	Auswahl der Sicherheitsmaßnahmen	8
2.2	Bedrohungs bäume	8
2.3	Umsetzung einer Sicherheitspolitik	11
2.3.1	Soziale/rechtliche Maßnahmen	11
2.3.2	Technische Maßnahmen	12
3	Das Netzwerkmanagement	13
3.1	Das Protokoll SNMP	14
3.2	Die Verbindung zwischen Netzwerkmanagement und Netzwerksicherheit .	15
4	Praktisches Beispiel FeM-Net	16
4.1	Aufstellung der Sicherheitspolitik	16
4.1.1	Bestimmung schützenswerter Sachen	16
4.1.2	Die Bedrohungsanalyse	17
4.1.3	Analyse der Schwachstellen	17
4.1.4	Die Risikoanalyse	18
4.1.5	Auswahl von Sicherungsmaßnahmen	20
4.2	Auswahl technischer Maßnahmen	21
4.3	Unterstützung durch das Netzwerkmanagement	22
5	Zusammenfassung	22

1 Einleitung

Netzwerksicherheit ist heute ein wichtigeres Thema als je zuvor. Aus dem ursprünglich als Verbund von wenigen Rechnern entstandenen ARPANET entwickelte sich innerhalb weniger Jahrzehnte ein Netzverbund mit derzeit geschätzten 500 bis 600 Millionen Nutzern. Dieses enorme Wachstum wurde nur erreicht, indem die Möglichkeiten des Internets auch technisch nicht versierten Nutzern zugänglich gemacht wurden. Daher ist davon auszugehen, dass es weltweit eine große Zahl an nicht oder nur schlecht gesicherten Systemen gibt, welche mit dem Internet verbunden sind.

Auf der anderen Seite sind durch die Masse der Nutzer auch eine Vielzahl von Angriffsszenarien interessant geworden, welche für die kleine, abgeschlossene Welt des ARPANET keinerlei Rolle spielten. In der realen Welt uninteressante Angriffe werden durch die Reichweite des Netzes plötzlich zu mächtigen Werkzeugen. Selbst der Betrug zur Erlangung von kleinsten Geldmengen wird durch tausendfache Ausführung zur gewinnbringenden Einnahmequelle. Das in der realen Welt fast unmögliche Blockieren der Infrastruktur von großen Unternehmen kann im Netz plötzlich dank vorbereiteter Software und tausender fehlerhaft konfigurierter, fremder Rechner seine bedrohliche Inkarnation als Distributed Denial of Service Attacke finden.

Aufgrund der eher militärischen und universitären Herkunft des ARPANET wurden beim Entwurf der Kommunikationsprotokolle Entscheidungen getroffen, die im heutigen Internet vollkommen unzureichenden Schutz vor Angriffen bieten. Begriffe wie Vertraulichkeit oder Integrität von Daten spielten in den Protokollentwürfen kaum eine Rolle. Das Modell eines nicht vertrauenswürdigen Nutzers war einfach nicht vorgesehen.

Aufgrund der Bedeutung, die das Internet mittlerweile für Unternehmen, Universitäten und Privatpersonen erlangt hat – keine größere Organisation kommt noch ohne Rechner und internes Unternehmensnetz aus –, ist das Thema Netzwerksicherheit eines der wichtigsten im Bereich der Informationsverarbeitung und einer der am schnellsten wachsenden Märkte der Branche.

Eine Folge der immer größer werdenden Nutzerzahlen und der immer ausgereifteren Angriffe ist eine hohe Komplexität der Sicherheitsmaßnahmen. Genügt für ein kleines Netz mit fünf Nutzern vielleicht noch ein einfacher Paketfilter, um den ein- und ausgehenden Verkehr etwas zu reglementieren, können es in großen Netzwerken durchaus mehrere zur Unterteilung in Teilnetze sein, welche von einer Menge anderer Maßnahmen, wie Application Level Gateways und Intrusion Detection Systeme begleitet werden. Um diese Menge an Maßnahmen sinnvoll zu konfigurieren und zu verwalten, benötigt die Netzwerksicherheit Unterstützung durch das Netzwerkmanagement. Ohne zentrales Management wären größere Installationen undenkbar. Der Aufwand an Personal und die Fehleranfälligkeit der Systeme würde jegliche Sicherung großer Netze unbezahlbar

machen.

Ziel dieses Hauptseminars ist es daher, die Möglichkeiten zur Netzwerksicherung, welche heute praktisch relevant sind, sowie ihre Unterstützung durch Netzwerkmanagementsysteme aufzuzeigen. Dazu werden zuerst die theoretischen Möglichkeiten zur Absicherung von Netzen betrachtet. Danach soll auf die Aufgaben des Netzwerkmanagements eingegangen werden. Zuletzt wird eine kurze Vorstellung des Studentennetzwerkes der TU Ilmenau, des FeM-Nets, erfolgen und anhand dessen die Theorie am praktischen Beispiel erprobt.

2 Theorie Netzwerksicherheit

Dieser Abschnitt dient der Vorstellung der gängigsten Maßnahmen zur Absicherung eines Netzes. Zentraler Punkt dabei ist die Aufstellung einer Sicherheitspolitik, welche versucht, alle Sicherheitsaspekte in einem umfassenden Dokument zu vereinigen und geeignete Maßnahmen zum Schutz des Systems zu finden.

2.1 Aufstellen einer Sicherheitspolitik

Die Suche nach einer allgemein akzeptierten Definition des Begriffes „Sicherheitspolitik“ fällt schwer, da viele Publikationen eine implizite Definition durch die Verwendung des Wortes im passenden Kontext vornehmen. Als eher informelle Definition soll hier daher ein Abschnitt aus [Sch00] dienen.

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.

Der Autor Bruce Schneier vergleicht hier die Sicherheitspolitik eines Systems mit der Außenpolitik eines Staates: einheitliche Vorgaben, welche alle Bereiche des Systems und deren Interaktion mit der Außenwelt betreffen. Ohne diese übergreifenden Vorgaben erhält man nur ein Wirrwarr an Gegenmaßnahmen, welche im günstigsten Fall zwar das gemeinsame Ziel erreichen, im ungünstigsten sich allerdings gegenseitig behindern.

Eine Sicherheitspolitik beschreibt, *was* zu schützen ist und *weshalb*. Sie sollte keine Aussagen über das „*Wie*“ – die technischen Details – enthalten. Diese sind im Allgemeinen umfangreich und nur für einen kleinen Kreis an Personen interessant und verständlich. Eine Sicherheitspolitik sollte allerdings von allen Personen, welche die Ressourcen

eines Netzes nutzen, verstanden werden (vgl. [EDZ01]). Des Weiteren sollte die Sicherheitspolitik keine Aussagen über nicht-technische Bedrohungen von Objekten treffen. In diese Kategorie würde beispielsweise privates Surfen am Arbeitsplatz fallen. Dies wird von vielen Arbeitgebern als Bedrohung der Ressource „Arbeitszeit“ empfunden. Eine oft verlangte technische Lösung dieses Problems kann nicht erreicht werden. Probleme sozialer oder rechtlicher Natur sind grundsätzlich durch entsprechende Maßnahmen, wie beispielsweise Arbeitsverträge und Schulungen zu lösen. Eine technische Lösung für soziale Probleme existiert meist nicht.

Da die Sicherheitspolitik als Mittel zur Beherrschung der Komplexität der Sicherung von großen Netzen naturgemäß recht umfangreich werden kann, bietet sich eine strukturierte Vorgehensweise an, um nicht den Überblick bei der Aufstellung zu verlieren. Folgende fünf Punkte können dazu herangezogen werden:

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

Die im letzten Punkt genannten Sicherheitsmaßnahmen sind hier nicht als konkrete technische Maßnahmen zu verstehen, sondern als allgemeine Zielsetzungen, welche zur Auswahl konkreter technischer Maßnahmen dienen können. Im folgenden sollen die fünf Punkte näher erläutert werden.

2.1.1 Bestimmung schützenswerter Sachen

Ziel dieser Aufgabe ist eine systematische Auflistung aller Objekte und Dienste, welche geschützt werden müssen. Dabei spielt die Gewichtung der einzelnen Objekte keinerlei Rolle. Lediglich die Vollständigkeit der Auflistung ist von Interesse. Diese Liste bildet die Grundlage der folgenden Schritte zur Aufstellung der Sicherheitspolitik und der daraus resultierenden Auswahl von Schutzmaßnahmen.

2.1.2 Die Bedrohungsanalyse

Ausgehend von der Auflistung der schützenswerten Sachen gilt es festzustellen, welche Objekte wovon bedroht werden und welche Schutzziele dadurch jeweils verletzt werden.

Diese Schutzziele lauten – wie immer im Bereich Computersicherheit – *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*. Eine übersichtliche Darstellungsform der Bedrohungsanalyse ist eine Tabelle ähnlich Tabelle 1.

Objekt	Bedrohung	Verletztes Schutzziel
DNS-Server	Diebstahl	Verfügbarkeit
	Einbruch über angebotene Dienste	Integrität, Verfügbarkeit
⋮	⋮	⋮

Tabelle 1: Bedrohungsanalyse

Aufgrund der Vielzahl möglicher Bedrohungen wird diese Aufstellung nur sehr selten vollständig sein. Zur Unterstützung dieser Arbeit ist es sinnvoll, sich im Laufe der Zeit eine Liste mit möglichen Angriffsarten gegen verschiedene Objekte aufzustellen und diese beispielsweise anhand von im Internet verfügbaren Quellen (zum Beispiel Sicherheitsmailinglisten, wie bugtraq [BUG]) immer wieder aktuell zu halten.

2.1.3 Analyse der Schwachstellen

Die in 2.1.2 aufgestellte Tabelle mit Bedrohungen für die Sicherheit von Systemen wird in einem weiteren Schritt nun verfeinert, um die konkreten Schwachstellen zu identifizieren, durch welche die abstrakten Bedrohungen realisiert werden können. An dieser Stelle ist bereits eine Vereinfachung der Tabelle möglich, da Bedrohungen, welche durch keine Schwachstelle realisiert werden, nicht weiter betrachtet werden müssen.

Als Schwachstellen im Sinne dieser Analyse gelten sowohl technische, als auch nicht-technische Schwachstellen. Auch wenn die Sicherheitspolitik letzten Endes nur Aussagen über technische Bedrohungen eines Objektes treffen soll, so sollten hier alle Arten aufgelistet werden, um auch Objekte zu identifizieren, welche technisch nicht zu schützen sind. Daraus ergeben sich dann Hinweise auf notwendige soziale und rechtliche Maßnahmen zur Komplettierung der Sicherheitspolitik, welche von den zuständigen Personen zu veranlassen sind.

Ziel der Schwachstellenanalyse ist eine neue Auflistung vergleichbar mit Tabelle 2.

Im Beispiel werden zwei Arten von Schwachstellen aufgezeigt: einerseits die technische Schwachstelle in Form des ungesicherten Serverraumes, welche auch durch technische Gegenmaßnahmen, wie dem Anbringen eines Schließsystems, zu beseitigen ist, und andererseits die nicht-technische Schwachstelle in Form der möglichen Bestechung des Wachschutzes, welcher aufgrund seiner Aufgabe eventuell auch Zutritt zu gesicherten Bereichen eines Rechenzentrums haben muss. Diese Schwachstelle ist durch techni-

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

Tabelle 2: Analyse der Schwachstellen

sche Gegenmaßnahmen nicht zu beseitigen. Ihre Behandlung sollte daher nicht Gegenstand einer Sicherheitspolitik sein, sondern über entsprechende Maßnahmen seitens der Geschäftsführung beseitigt werden.

2.1.4 Die Risikoanalyse

Die bisher aufgestellten Tabellen bergen aufgrund ihres schieren Umfanges die Gefahr, die angestrebte Übersichtlichkeit und Verständlichkeit der Sicherheitspolitik zu vernichten. Daher ist vor der Auswahl an Sicherungsmaßnahmen zwingend eine Gewichtung der einzelnen Bedrohungen notwendig. Es ist vom wirtschaftlichen Standpunkt aus unsinnig, sich gegen alle Angriffsmöglichkeiten schützen zu wollen. Teilweise kann es sinnvoller sein, mit dem Risiko einer bestimmten Bedrohung zu leben, wenn der mögliche Schaden durch eine Realisierung der Bedrohung nur einen Bruchteil der Kosten der Schutzmaßnahmen verursacht.

Die tatsächlichen Kosten, welche eine Bedrohung verursachen kann, sind abhängig von der Höhe des im Realisierungsfall auftretenden Schadens, sowie der Wahrscheinlichkeit des Auftretens. Daher kann als Formel für das Risiko gelten:

$$\text{Risiko} = \text{Schadenshöhe} \times \text{Eintrittswahrscheinlichkeit}$$

Der Begriff „Schadenshöhe“ bezieht sich dabei nicht nur auf die finanzielle Seite. In vielen Fällen lassen sich die entstehenden Schäden nicht oder nur schlecht in Form von finanziellen Verlusten ausdrücken. Auch kann die Schadenshöhe ein und desselben Schadens für unterschiedliche Unternehmen verschieden ausfallen. Beispielsweise dürfte ein Einbruch in die Firmenwebseite für ein Unternehmen, welches Netzwerksicherheit verkauft, erheblich gravierender ausfallen, als für einen lokalen Bäcker, welcher sein Angebot an Hochzeitstorten im Netz präsentiert. Während die Angelegenheit für den Bäcker ärgerlich, eventuell sogar peinlich ist, kann sie für das Sicherheitsunternehmen den Verlust des guten Rufes und daraus folgend den finanziellen Ruin bedeuten. Aus diesem Grunde bietet es sich an, die Schadenshöhe in verschiedene Klassen einzuteilen und somit die Einteilung verschiedener Schäden zu erleichtern.

Ähnliche Probleme ergeben sich bei der Festlegung der Eintrittswahrscheinlichkeit. Konkrete Zahlenwerte, wie man sie bei dem Begriff „Wahrscheinlichkeit“ erwarten könnte, lassen sich in vielen Fällen nicht festlegen, da selten gesicherte Statistiken über die Häufigkeit verschiedener Angriffe auf das Unternehmen vorhanden sind. Mit Hilfe von Erfahrungswerten ähnlicher Unternehmen lassen sich im Allgemeinen verschiedene Wahrscheinlichkeitsklassen definieren, in die dann die entsprechenden Angriffe einsortiert werden können. So gelangt man auch ohne konkretes Zahlenmaterial zu relativ verlässlichen Aussagen hinsichtlich des Risikos verschiedener Schwachstellen.

Auch das Risiko selbst ist sinnvollerweise in Klassen einzuteilen, welche eine größere Ausdruckskraft besitzen als abstrakte Zahlen. So ist leicht ersichtlich, was die Einschätzung *sehr hoch* des Risikos bedeutet, während die Zahl 100 als Risikowert für Außenstehende eher schwer einzuschätzen ist.

Ergebnis der Risikoanalyse ist wieder eine Auflistung, ähnlich Tabelle 2, in welcher die Schwachstellen der einzelnen Objekte nun mit einer Kennzeichnung des ihnen innewohnenden Risikos versehen sind. Ein Beispiel dafür ist Tabelle 3.

Objekt	Bedrohung	Schwachstelle	Risiko
DNS-Server	Diebstahl	ungesicherter Serverraum bestochener Wachdienst	sehr hoch niedrig
⋮	⋮	⋮	

Tabelle 3: Ergebnis der Risikoanalyse

Im Beispiel wurden zwei Risikoklassen gewählt. Es wurde während der Analyse festgestellt, dass das Risiko des Zutritts zum Serverraum aufgrund der nicht vorhandenen Sicherung *sehr hoch*, eine Bestechung des Wachdienstes allerdings unwahrscheinlich und dieses Risiko damit *niedrig* ist. Im Beispiel kann aus der Tabelle direkt auf die Eintrittswahrscheinlichkeit geschlossen werden. Aufgrund der Tatsache, dass der Schaden – der Diebstahl und damit verbundene Ausfall des DNS-Servers – immer gleich hoch bewertet wird, liegt der Unterschied laut der genannten Gleichung für das Risiko allein in der Eintrittswahrscheinlichkeit der Ausnutzung der verschiedenen Schwachstellen.

Aus der Tabelle kann ebenfalls abgeleitet werden, dass das Risiko für einen Diebstahl des DNS-Servers insgesamt *sehr hoch* ist, da bereits die Ausnutzung einer der Schwachstellen zur Realisierung der Bedrohung genügt. Zur Unterstützung derartiger Analysen dienen die in 2.2 vorgestellten Bedrohungs bäume.

2.1.5 Auswahl der Sicherheitsmaßnahmen

Ausgehend von der Risikoeinschätzung für verschiedene Angriffe können nun unter Beachtung der Realisierbarkeit – aus Sicht der Betriebswirte meist mit Blick auf die Kosten – Richtlinien aufgestellt werden, welche letzten Endes die Sicherheitspolitik des Unternehmens bilden. An dieser Stelle können dann auch Forderungen hinsichtlich der Nutzung bestimmter Dienste einfließen, welche eventuell von einigen Richtlinien berührt werden. Ergebnis dieses Arbeitsschrittes ist ein Dokument, welches, unterschrieben von der Geschäftsleitung, die Basis für die Realisierung verschiedener technischer Maßnahmen zur Absicherung des Netzes des Unternehmens bildet. Wie bereits erwähnt sollte dieses Dokument klare, für jeden verständliche Formulierungen enthalten, welche auch im Zweifelsfall als Begründung für bestimmte Maßnahmen gegenüber den Mitarbeitern herangezogen werden können.

2.2 Bedrohungs bäume

Zur Ermittlung des Risikos verschiedener Schwachstellen beziehungsweise Bedrohungen finden sogenannte *Bedrohungs bäume* Anwendung. Diese Baumstrukturen können aufgrund der umfassenden Parametrisierbarkeit ihrer Knoten für eine Vielzahl von Analysen zur Einschätzung von Risiken verwendet werden.

Jeder Knoten des Bedrohungsbaumes trägt eine Beschreibung (ein Teilziel) und eine Anzahl an frei gewählten Parametern. Die Werte der Parameter in den Blättern des Baumes werden dabei nach Erfahrungswerten gewählt, während sich die Werte in den darüber liegenden Knoten nach bestimmten Regeln aus den Werten in den Kindknoten ergeben. Die Wurzel eines Bedrohungsbaumes bildet das zu analysierende Ziel (eine Schwachstelle oder eine Bedrohung). Die Kinder eines Knoten bilden wiederum Teilziele des in dem Knoten beschriebenen Ziels. Somit ist eine hierarchische Zerlegung des Gesamtzieles in elementare Teilziele, welche einfach zu bewerten sind, möglich. Zwischen den Teilzielen eines Knotens können zwei Arten von Beziehungen bestehen: eine OR-Verknüpfung, bei der die Realisierung *eines* Teilziels zur Realisierung des übergeordneten Ziels führt, sowie einer AND-Verknüpfung, bei der die Realisierung *aller* Teilziele zur Realisierung des übergeordneten Ziels nötig ist. Je nach Art der Verknüpfung kommen unterschiedliche Regeln zur Ermittlung der Parameter eines Knotens zur Anwendung. Als Beispiel soll der in Abbildung 1 gezeigte Bedrohungsbaum dienen.

Als Parameter verwendet der Autor hier die Werte *Possible* für mögliche Angriffe, sowie *Impossible* für unmögliche Angriffe. Die im Baum eingetragenen Werte für die Parameter der Elementarziele sind Einschätzungen des Autors. Die Werte der zusammengesetzten Ziele ergeben sich nach folgenden Regeln:

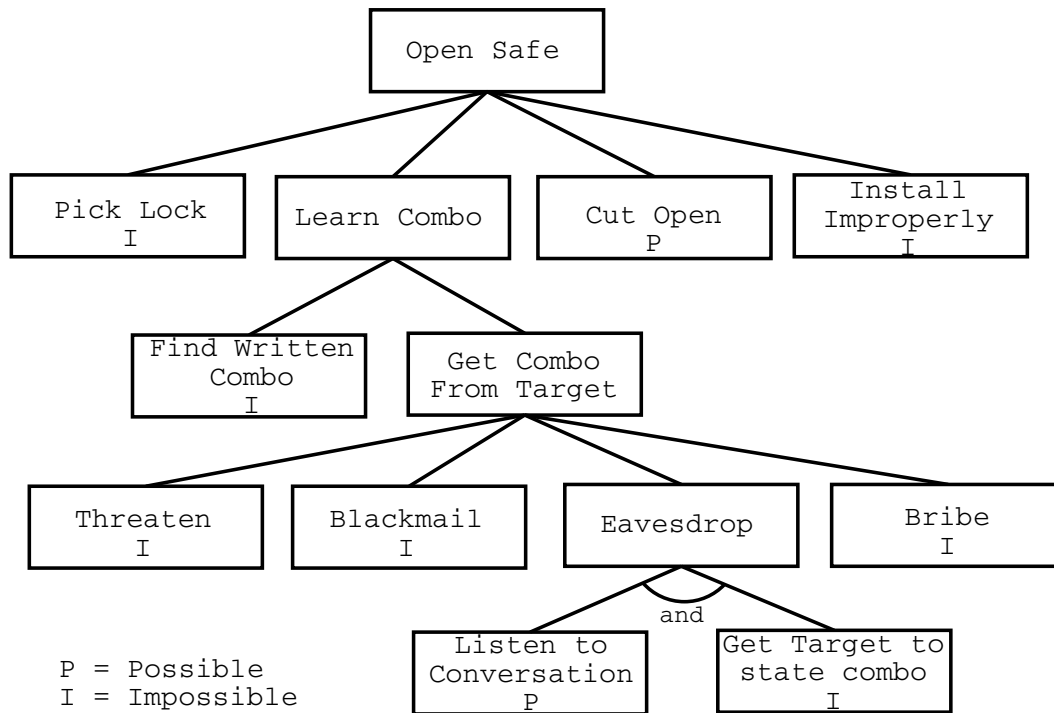


Abbildung 1: Beispiel eines Bedrohungsbaumes (nach [Sch00] Kap. 21)

- AND-Verknüpfung der Unterziele: *Possible*, wenn alle Unterziele *Possible* tragen, *Impossible* sonst.
- OR-Verknüpfung der Unterziele: *Possible*, wenn eines der Unterziele *Possible* trägt, *Impossible* sonst.

Die OR-Verknüpfung wird im Bild durch die Pfade ohne Zusatz repräsentiert, die AND-Verknüpfung durch den Bogen mit dem „and“ darunter. Innerhalb der Kinder eines Knotens können niemals AND- und OR-Verknüpfungen gemischt vorkommen. Sollte das notwendig werden, so sind die AND-verknüpften Knoten durch neue Teilziele zu ersetzen, welche als Unterziele die ursprünglichen Knoten haben. Im Beispiel wäre dies der Knoten „Eavesdrop“, welches als Oberziel für „Listen to Conversation“ und „Get Target to state combo“ dient. Eine Verwendung dieser beiden Ziele als Kindknoten von „Get Combo From Target“ würde eine Ausführung der oben genannten Regeln unmöglich machen und deutete somit auf einen Fehler im Baum hin.

Durch die rekursive Anwendung der aufgestellten Regeln auf die Parameter der Knoten ergibt sich für die Wurzel letzten Endes der Wert *Possible*, da einer ihrer OR-

verknüpften Kindknoten – der Knoten „Cut Open“ – *Possible* enthält. Als Gegenbeispiel ergibt sich für den Knoten „Learn Combo“ der Wert *Impossible*, da beide Kindknoten diesen Wert tragen. Der Knoten „Get Combo From Target“ ergibt sich zu *Impossible*, da ebenfalls alle seiner Kindknoten diesen Wert enthalten. Dies wiederum ist der Fall, da „Eavesdrop“ diesen Wert annimmt, da ihn einer seiner AND-verknüpften Kindknoten trägt.

Die Knoten eines Bedrohungsbaumes können jeweils eine beliebige Zahl von Parametern tragen, was selbst komplexe Analysen der Form „Welcher mögliche Angriff, der weniger als 1000 EUR kostet und nicht mehr als 2 Personen zur Ausführung benötigt, führt zur Erfüllung des Gesamtzieles?“ ermöglicht. Allerdings werden die Bedrohungsbaume in der in Abbildung 1 gezeigten Darstellung schnell sehr groß, so dass sich eine andere Darstellung in Textform anbietet. Diese würde für den Baum in etwa wie folgt aussehen (die Beschreibungen wurden ins Deutsche übersetzt):

Ziel: Safe öffnen

1. Safe öffnen

1.1. Schloss knacken (OR)

Impossible

1.2. Kombination in Erfahrung bringen (OR)

1.2.1. Zettel mit Kombination finden (OR)

Impossible

1.2.2. Kombination vom Besitzer erfahren (OR)

1.2.2.1. Besitzer bedrohen (OR)

Impossible

1.2.2.2. Besitzer erpressen (OR)

Impossible

1.2.2.3. Kombination hören (OR)

1.2.2.3.1. Gespräch des Besitzers belauschen (AND)

Possible

1.2.2.3.2. Besitzer dazu bringen, die Kombination zu sagen (AND)

Impossible

1.2.2.4. Besitzer bestechen (OR)

Impossible

1.3. Safe aufschneiden (OR)

Possible

1.4. Safe unsicher einbauen (OR)

Impossible

Diese Darstellung mag auf den ersten Blick nicht viel übersichtlicher erscheinen, ist

aber bei größeren Bäumen schnell vorteilhaft, da sie sich auch gut zur Darstellung durch Computerprogramme eignet.

Das Erstellen des Bedrohungsbaumes zählt zu den aufwändigsten Teilen der Aufstellung einer Sicherheitspolitik, unterstützt aber durch die formale Darstellung deutlich den Überblick und damit die Vollständigkeit des Prozesses.

2.3 Umsetzung einer Sicherheitspolitik

Das Aufstellen einer Sicherheitspolitik allein verbessert noch nicht die Sicherheit eines Netzwerkes. Erst die auf ihrer Basis getroffenen Entscheidungen hinsichtlich verschiedener Maßnahmen und deren Implementierung kann die Ziele der Sicherheitspolitik erfüllen. Diese Maßnahmen lassen sich in zwei Klassen einteilen: technische und soziale/rechtliche Maßnahmen. Letztere sind wie bereits erwähnt nicht Bestandteil der Sicherheitspolitik und werden daher hier auch nur flüchtig betrachtet. Ihre Auswahl und Durchsetzung obliegt der Geschäftsführung. Die technischen Maßnahmen hingegen sollten von Technikern ausgewählt und konfiguriert werden, um die geforderten Regeln der Sicherheitspolitik durchzusetzen.

2.3.1 Soziale/rechtliche Maßnahmen

Auch wenn soziale und rechtliche Maßnahmen nicht Bestandteil der Sicherheitspolitik sind und daher auch nicht von Technikern implementiert werden, so sind sie doch zwingend notwendiger Bestandteil der Sicherung eines Netzes. Im Laufe der Erstellung der Sicherheitspolitik gibt es immer wieder Objekte und Dienste, welche technisch nicht zu schützen sind und Anforderungen von außen, welche nicht durch technische Maßnahmen erfüllbar sind. Meist betrifft dies Probleme, welche in ähnlicher Form auch außerhalb der Netzwerksicherheit existieren. Typisches Beispiel dafür ist die Anforderung der Geschäftsführung, privates Surfen im WWW am Arbeitsplatz zu unterbinden. Während das für Leute, welche keinen Internetzugang am Arbeitsplatz benötigen, technisch noch zu bewerkstelligen ist, ist es für Arbeitsplätze, welche über einen Zugang verfügen, technisch nicht machbar. Derartige Anforderungen müssen daher durch rechtliche und soziale Maßnahmen durchgesetzt werden. Derartige Maßnahmen können unter anderem sein:

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

2.3.2 Technische Maßnahmen

Nach der Fertigstellung der Sicherheitspolitik ist es die Aufgabe von Technikern, die dort geforderten Regelungen durch technische Maßnahmen umzusetzen. Das Ziel ist es, Formulierungen wie „Der Wartungszugang zu den Diensten unseres Unternehmens darf nicht ungesichert erfolgen, da Passwörter und Daten beim Weg durch das Netz mitgelesen werden können.“ in Tatsachen, wie „Für den Wartungszugang zu Diensten unseres Unternehmens setzen wir SSH ein.“ zu verwandeln.

Technische Maßnahmen können in drei Gruppen unterteilt werden

Prävention Die Maßnahme dient der Verhinderung von Angriffen.

Detektion Die Maßnahme dient der Entdeckung von Angriffen.

Reaktion Die Maßnahme dient der Behandlung von entdeckten Angriffen.

In der Praxis konzentrieren sich viele Sicherheitsmaßnahmen auf den Bereich der Prävention und lassen die beiden anderen Punkte vollkommen außer Acht. Das führt zu einem sehr hohen Risiko bei der Implementierung der Maßnahmen, da bereits ein Fehler das gesamte System – möglicherweise unbemerkt – außer Kraft setzt. Aus diesem Grund ist es sinnvoll, auf das Prinzip der „defense in depth“, der mehrstufigen Sicherung, zu setzen. Dabei geht man grundsätzlich davon aus, dass durch Fehler im Konzept oder in der Konfiguration eine Sicherheitsmaßnahme ihre Wirkung verlieren kann. Um trotzdem eine möglichst starke Sicherung zu erhalten, baut man sein System so auf, dass niemals die Umgehung einer Maßnahme genügt, um Zugriff auf das System zu erhalten. Vergleichbar ist dies mit dem Aufbau von Festungsanlagen aus dem Mittelalter, welche oft mehrere, unabhängige Wälle und Gräben hatten, welche vom Eindringling einzeln überwunden werden mussten. Ein typisches Beispiel für diese Vorgehensweise ist eine Absicherung mittels zweier Paketfilter und dazwischen liegender DMZ (DeMilitarized Zone – nach der Grenzregion zwischen Nord- und Südkorea benannt). Innerhalb dieser DMZ stehen alle Rechner, welche Dienste in das äußere Netz anbieten. Diese sind nochmal vom inneren Netz durch einen Paketfilter getrennt. Im Interesse der mehrstufigen Sicherung bietet es sich in diesem Fall an, verschiedene Paketfilter zwischen äußerem Netz und DMZ, sowie zwischen DMZ und innerem Netz zu verwenden, um es einem Angreifer im Falle einer Verwundbarkeit des äußeren Filters zu erschweren, den inneren Filter zu überqueren.

Im Folgenden werden einige Beispiele für technische Maßnahmen zur Sicherung von Netzen, sowie ihre Einteilung in die drei genannten Gruppen aufgeführt. Maßnahmen, die in mehr als eine Gruppe fallen, wurden dabei auch mehrfach genannt.

- Prävention:
 - Paketfilter
 - Proxy/Application Level Gateway
 - Grafische Firewall
 - Authentifizierungs-/Autorisierungssysteme
 - Public Key Infrastructure
 - Sichere Protokolle
- Detektion:
 - passives Intrusion Detektion System
 - Authentifizierungs-/Autorisierungssysteme
 - Public Key Infrastructure
 - Sichere Protokolle
- Reaktion:
 - Portsecurity
 - aktives Intrusion Detektion System
 - Authentifizierungs-/Autorisierungssysteme

3 Das Netzwerkmanagement

Große Netzwerke sind im Allgemeinen keine statischen Gebilde, welche – einmal eingerichtet – für Jahre ihren Dienst tun. Sie verändern sich ständig: neue Geräte werden dem Netz hinzugefügt, alte verschwinden, Nutzer kommen und gehen, mit neuer Software kommen neue Anforderungen und Möglichkeiten. Des Weiteren treten ständig kleinere und größere Fehler im Netz auf, welche analysiert und behoben werden müssen. Daher muss, um den Aufwand des Netzbetriebes in Grenzen zu halten, eine weitgehend automatisierte Unterstützung Verwendung finden. Eine umfassende Lösung für derartige Probleme zu finden ist Aufgabe des Netzwerkmanagements.

Der Begriff „Netzwerkmanagement“ ist etwas unscharf gewählt. Er bezeichnet, je nach Hersteller, eine Vielzahl an Technologien, die eine Unterstützung bei der Verwaltung von Netzwerken anbieten. Das kann von einfachen Login-Systemen zur Administration von Netzwerkausrüstung bis zu ausgefeilten Systemen zur Überwachung und

Verwaltung komplexer Installationen mit tausenden von Clients reichen. Im Folgenden soll stellvertretend für diese Technologien das Protokoll SNMP ([JC]) kurz vorgestellt werden, welches sich als herstellerübergreifender Standard weitgehend durchgesetzt hat.

3.1 Das Protokoll SNMP

Als Standard im Bereich des Netzwerkmanagements gilt das Simple Network Management Protocol (SNMP). Nahezu jedes managebare Gerät im Bereich Netzwerkausrüstung verfügt über einen sogenannten SNMP-Agent, über welchen eine Kommunikation mit dem Gerät möglich ist.

SNMP – in der meist gebräuchlichen Version SNMPv1 – baut auf ein einfaches Modell des Netzwerkmanagements auf: es existieren eine oder mehrere Management Stations, welche über die auf den Geräten laufenden SNMP-Agents auf sogenannte *managed objects* zugreifen können. Diese können jeden Aspekt des Zustandes eines Netzwerkgerätes repräsentieren, von Verwaltungsinformationen, wie Gerätename und Standort, über Statistikinformationen bis hin zu komplexen Sicherheitsfunktionen. Diese Informationen werden bei SNMP in einer Baumstruktur, der sogenannten *Management Information Base*, kurz MIB organisiert. Teile dieser MIB sind durch die International Standards Organization (ISO) standardisiert, andere Teile werden von den Herstellern in speziellen Unterbäumen frei vergeben. Des Weiteren existiert bei SNMP das Konzept der *Communities*, eine Anwendung des *Compartment-Modells*, welches verschiedenen Gruppen, identifiziert über ein Passwort – den *community string* –, bestimmte Rechte in der MIB einräumt.

Die Kommunikation geht bei SNMP meist von der Management Station aus. Diese sendet eine Lese- oder Schreibanforderung über bestimmte Variablen an den SNMP-Agent auf dem betreffenden Host, welcher die angeforderte Aktion abhängig von den Rechten der gegebenen Community ausführt und mit Variablen und ihren Werten antwortet. Einzige Ausnahme von diesem System bilden die bei SNMP definierten *Traps*, mit welchen ein Agent in der Lage ist, eine Management Station von bestimmten Ereignissen in Kenntnis zu setzen. Diese Traps werden vom Agent versendet und bedürfen keiner Antwort. Somit bietet SNMPv1 die notwendigen Voraussetzungen, um sowohl die Konfiguration als auch die Überwachung von Netzwerkgeräten effizient durchzuführen. In den folgenden Versionen SNMPv2 und SNMPv3 wurden einige Vereinfachungen der verwendeten Datenformate und Verbesserungen hinsichtlich der Sicherheit des Protokolls vorgenommen. Des Weiteren wurde das Prinzip des *Manager of Managers* eingeführt, welches es ermöglicht, bestimmte Aufgabengebiete an andere Manager zu delegieren und diese wiederum von einer zentralen Management Station aus zu kontrollieren. Leider wurden viele der Erweiterungen von den Herstellern nicht implementiert, so dass

größtenteils noch SNMPv1 Verwendung findet.

Die Architekturprinzipien von SNMP sind typisch für Netzwerkmanagementsysteme. Zur effizienten Verwaltung eines Netzes ist eine zentrale Konfiguration, sowie eine zentrale Alarmierung über Fehlerzustände notwendig. Alle kommerziell erhältlichen Pakete zum Netzwerkmanagement verstehen SNMP und implementieren ähnliche Prinzipien. Oft ergänzen sie diese durch eine effiziente Vorfilterung der auftretenden Alarme oder durch die Verbindung von zentralen Datenbanken mit SNMP zur Konfiguration von Netzwerkgeräten.

3.2 Die Verbindung zwischen Netzwerkmanagement und Netzwerksicherheit

Sicherheit in technischen Systemen kann generell nur erreicht werden, wenn Kontrolle über das System besteht. Dazu ist es notwendig, jederzeit den Zustand des Systems einsehen zu können, zentral alle Elemente aufeinander abzustimmen und über auftretende Veränderungen schnell informiert zu werden. Während die Netzwerksicherheit die Vorgaben und Techniken liefert, um einzelne Aspekte eines Netzes abzusichern, muss das Netzwerkmanagement die Technologien bieten, um diese Systeme zentral zu überwachen und zu steuern, um so kurze Reaktionszeiten auf auftretende Probleme zu realisieren. Des Weiteren ist durch die Vielzahl an Sensordaten in großen Netzen eine automatisierte Vorverarbeitung von Alarmen zwingend notwendig. Eine Überflutung mit belanglosen Statusmeldungen eines Netzes führt bei Administratoren zwangsläufig zum Übersehen wichtiger Alarme. Um dies zu vermeiden, ist es Aufgabe des Netzwerkmanagements, Techniken zu liefern, um eintreffende Messdaten zu analysieren und dann auch zu priorisieren. Ein Mensch ist in der Lage, nur eine geringe Anzahl an Meßdaten gleichzeitig im Auge zu behalten. Netzwerkmanagementsysteme müssen ihm diese geringe Menge an relevanten Daten liefern.

Zweiter Aspekt der Unterstützung durch das Netzwerkmanagement ist die Ermöglichung von kurzen Reaktionszeiten auf auftretende Probleme. Wenn bei einer weltweit verteilten Organisation ein technisches Problem im Netz auftritt, so kann es bis zur Lokalisation der Ursache und deren Behebung recht lang dauern, wenn die benötigten Experten immer erst vor Ort sein müssen. Mit Hilfe von Netzwerkmanagementsystemen sind viele Probleme aus der Ferne lösbar, was wesentlich kürzere Reaktionszeiten ermöglicht. Speziell bei Sicherheitsproblemen sind kurze Reaktionszeiten manchmal das einzige, was zwischen einem kurzen Störfall und einer totalen Katastrophe unterscheidet. Daher ist hier die Unterstützung durch das Netzwerkmanagement zwingend notwendig.

4 Praktisches Beispiel FeM-Net

Im Folgenden sollen die bisher vorgestellten Verfahren am praktischen Beispiel demonstriert werden. Dazu wurde das Studentennetzwerk der TU Ilmenau, das FeM-Net, als Beispielnetzwerk ausgewählt. Das von der Forschungsgemeinschaft elektronische Medien e.V. ([FEM]) betriebene Netz umfasst aktuell etwa 1900 Geräte. Das Netzwerk ist bis auf wenige Ausnahmen vollständig mit Switches der Marke HP Procurve 2524 bzw. 2650 ausgestattet. Diese werden über einen Gigabit-Ethernet-Glasbackbone mit einem Cisco Catalyst 6509 als Router und Paketfilter verbunden. Des Weiteren betreibt FeM noch zwei Funkstrecken auf Basis von IEEE 802.11b zur Pörlitzer Höhe und zur Schlossmauer in Ilmenau. Beide Funkstrecken verlaufen mehrere hundert Meter bzw. mehrere Kilometer über öffentlichen Grund. Die größte Herausforderung für das Netzwerkmanagement sind allerdings die etwa 1500 Nutzer im Netz, deren Rechner aufgrund der Vereinsstruktur nicht unter zentraler Verwaltung stehen können. Unter diesen Gesichtspunkten fallen einige Möglichkeiten zur Sicherung der Rechner weg und müssen durch eine Verbesserung in der Sicherung des Netzes ersetzt werden. Ein konkretes Beispiel dafür ist das aufgrund eines Kooperationsvertrages mit dem Rechenzentrum der TU Ilmenau bestehende Verbot des Angebotes von Diensten aus dem FeM-Net in das Internet. Da auf den Nutzerrechnern keine entsprechenden Maßnahmen getroffen werden können, muss dieses Verbot über einen Paketfilter auf dem Catalyst 6509 durchgesetzt werden.

4.1 Aufstellung der Sicherheitspolitik

Die Aufstellung einer umfassenden Sicherheitspolitik für das FeM-Net würde den Rahmen dieser Arbeit sprengen. Daher wird sich das folgende Beispiel auf einen Aspekt der Netzsicherung konzentrieren, nämlich die Verhinderung eines Zugriffs auf Schicht 2 des ISO OSI Modells ([OSI]). Im FeM-Net werden die Aufgaben dieser Schicht vom Ethernet-Protokoll übernommen. Aufgrund der Struktur dieses Protokolls und der Interaktion zwischen Ethernet und dem darüber angesiedelten IP bieten sich durch Zugriff auf Schicht 2 Angriffsmöglichkeiten, welche zum Verlust der Integrität, Vertraulichkeit und Verfügbarkeit großer Teile des Netzes führen können.

4.1.1 Bestimmung schützenswerter Sachen

Als schützenswerte Objekte sind hier alle Punkte festzuhalten, an welchen ein Zugriff auf Ethernet-Ebene erfolgen kann. Damit kommen drei Punkte in Frage:

Switches Aufgrund ihrer Eigenschaft als Schicht-2-Vermittler sind natürlich die verbauten HP Procurve Switches naheliegender Angriffspunkt für den Zugriff auf Ethernet

Ebene.

Backbone (Kabel, Router) Da auch im Backbone des FeM-Net Ethernet verwendet wird, ist dieser ebenfalls ein möglicher Angriffspunkt. Ob der Zugriff dabei durch die Kabel oder direkt am Router erfolgt, ist zweitrangig.

Funkstrecken Auch über die von FeM betriebenen Funkstrecken laufen Ethernetpakete. Diese sind damit auch aufgrund ihres Verlaufs über öffentlichen Grund ein denkbarer Punkt für einen Zugriff.

4.1.2 Die Bedrohungsanalyse

Nun gilt es, die Bedrohungen für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu identifizieren, welche durch die im vorigen Abschnitt aufgezeigten Objekte bestehen.

Einfachster Fall für den Angreifer ist sicherlich ein direkter Anschluss eines Rechners an einen der Switches. Dieser Angriff ist mit dem geringsten Aufwand verbunden und führt aus Sicht der FeM zu einem Verlust der Vertraulichkeit bestimmter Daten. Potenziell ermöglicht dieser Angriff weitere Maßnahmen des Angreifers (zum Beispiel das sogenannte ARP-Spoofing), welche zum Verlust der Integrität oder der Verfügbarkeit von Netzdiensten führen können.

Im Bereich des Backbones gibt es grundsätzlich die Möglichkeit des Einbaus einer Bridge, welche alle über sie laufenden Daten analysieren, verändern und filtern kann. Damit droht auch hier eine Verletzung sämtlicher Schutzziele.

Durch die Funkstrecken sind drei Arten von Angriffen denkbar. Einerseits das bloße Mitschneiden von Informationen, wodurch das Schutzziel Vertraulichkeit verletzt wird. Des Weiteren ist durch geeignete Funktechnik eine Störung der Signalstrecke und damit ein Abbruch der Funkverbindung möglich. Dieser, immer wieder versehentlich ausgeführte Angriff führt zum Verlust der Verfügbarkeit von Ressourcen innerhalb des Netzes. Zuletzt ist auch hier das Einfügen einer Bridge in die Funkstrecke denkbar, welche die Verletzung sämtlicher Schutzziele zur Folge hat.

Damit ergibt sich die in Tabelle 4 gezeigte Aufstellung der Bedrohungen.

4.1.3 Analyse der Schwachstellen

Als nächster Schritt zur Aufstellung der Sicherheitspolitik werden konkrete Schwachstellen aufgelistet, welche zu einer Realisierung der in der Bedrohungsanalyse aufgezeigten Bedrohungen führen können.

Objekt	Bedrohung	verletzte(s) Schutzziel(e)
Switches	Anschluss eines Fremdrechners	Vertraulichkeit (evtl.: Integrität, Verfügbarkeit)
Backbone	Einbau einer Bridge	Vertraulichkeit, Verfügbarkeit, Integrität
Funkstrecken	Mitschneiden von Paketen	Vertraulichkeit
	Störung der Signalstrecke	Verfügbarkeit
	Einfügen einer Bridge	Vertraulichkeit, Verfügbarkeit, Integrität

Tabelle 4: Bedrohungsanalyse Schicht 2 des FeM-Net

Im FeM-Net existieren prinzipiell zwei Schwachstellen, welche den Anschluss eines Fremdrechners an einen Switch ermöglichen könnten. Einerseits die ungesicherten Netzwerkdosen, welche in den Wohnungen der Studentenwohnheime außerhalb der Kontrolle des Vereins liegen, andererseits der Switch selbst, welcher im Betriebsraum erreichbar ist.

Der Einbau einer Bridge in den Backbone könnte entweder direkt im Betriebsraum durch einfaches Umstecken der Netzverbindungen erreicht werden oder an den Glas-kabeln stattfinden, welche die Verbindungen zwischen den einzelnen Blöcken auf dem Campus herstellen. Diese liegen größtenteils nahezu ungeschützt in stillgelegten, begeharen Heizungstrassen unter dem Campus der TU Ilmenau. Auch wenn die zweite Möglichkeit eher unwahrscheinlich erscheint, so ist sie hier doch mit aufzulisten, da eine Analyse der Wahrscheinlichkeiten von erfolgreichen Angriffen auf die Schwachstellen erst im nächsten Schritt erfolgt.

Die zentrale Schwachstelle, welche zur Realisierung aller drei Bedrohungen der Funkstrecke führen kann, ist deren Verlauf über öffentlichen Grund. Aus Sicht der FeM besteht keinerlei Möglichkeit, Leute daran zu hindern, auf öffentlichem Grund die Signale der Funkstrecke aufzufangen und auszuwerten. Des Weiteren besteht keine technische Möglichkeit, eine Störung der Funkstrecke durch Fremdsignale zu verhindern.

Aus der Analyse der Schwachstellen ergibt sich somit Tabelle 5.

4.1.4 Die Risikoanalyse

Zur Analyse des Risikos einzelner Schwachstellen bzw. Bedrohungen wird ein Bedrohungsbaum aufgestellt, in welchem die Wahrscheinlichkeit der erfolgreichen Ausnutzung einer Schwachstelle analysiert werden kann. Aufgrund des Fehlens genauer Messwerte für die Wahrscheinlichkeiten einzelner Angriffe werden einfach zwei Klassen definiert: mögli-

Objekt	Bedrohung	Schwachstelle
Switches	Anschluss Fremdrechner	ungesicherte Netzdose ungesicherter Serverraum
Backbone	Einbau einer Bridge	Einspleissen in das ungeschützte Glaskabel ungesicherter Serverraum
Funkstrecken	Mitschneiden von Paketen	Verlauf über öffentlichen Grund
	Störung der Signalstrecke	siehe oben
	Einfügen einer Bridge	siehe oben

Tabelle 5: Analyse der Schwachstellen

che und unmögliche Angriffe. Unmögliche Angriffe sind dabei nicht zwingend technisch unmöglich, sondern auch Angriffe, welche aufgrund ihres Aufwandes beziehungsweise ihrer Kosten nicht praktikabel erscheinen. Zur Vereinfachung der Analyse des Risikos werden zusätzlich noch drei Risikoklassen definiert: niedrig, mittel und hoch. Vereinfacht soll gelten, dass die Verletzung eines Schutzzieles ein niedriges Risiko, die Verletzung zweier Schutzziele ein mittleres und die Verletzung aller Schutzziele ein hohes Risiko darstellt. Diese Annahme ist zu Demonstrationszwecken ihrer Einfachheit wegen geeignet, in einer realen Analyse wäre eine feinere Granulierung der Risikoklassen angebracht, welche auch die Risiken von Folgeangriffen und die Wichtung der einzelnen Schutzziele beachten kann.

Der Bedrohungsbaum für diese Analyse sieht wie folgt aus (Attribute der einzelnen Blätter stehen in eckigen Klammern):

Ziel: Zugriff auf das FeM-Net auf Ethernet-Ebene

1. Zugriff auf das FeM-Net auf Ethernet-Ebene

1.1 Anschluss eines Fremdrechners (OR)

1.1.1 Zugriff über die Netzdose (OR)

1.1.1.1 Absprache mit Nutzer (OR)

[möglich]

1.1.1.2 Einbruch in die Wohnung des Nutzers (OR)

[unmöglich]

1.1.2 Zugriff im Serverraum (OR)

[möglich]

1.2 Einbringen einer Bridge in das Netz (OR)

1.2.1 im Glasbackbone (OR)

1.2.1.1 Zutritt zum Serverraum (AND)

[möglich]

- 1.2.1.2 Einbindung in die Kabelstrecke (AND)
 - 1.2.1.2.1 Umstecken der Verbindungen (OR)
[möglich]
 - 1.2.1.2.2 Einspleissen in die Glasfasern (OR)
[unmöglich]
- 1.2.1.3 Unbemerkttes Bridgen von 1 GBit/s (AND)
[unmöglich]
- 1.2.2 auf der Funkstrecke (OR)
 - 1.2.2.1 Unterbrechung der Funkstrecken (AND)
[unmöglich]
 - 1.2.2.2 Verwendung der passenden MAC und SSID (AND)
[möglich]
- 1.3 Mitschneiden von Paketen auf den Funkstrecken (OR)
[möglich]

Betrachtet man nun die drei Kindknoten der Wurzel als neue Bedrohungs bäume und analysiert deren Wahrscheinlichkeiten, so erhält man als Ergebnis, dass sowohl der Anschluss eines Fremdrechners, als auch das Mitschneiden von Paketen auf den Funkstrecken möglich sind, während das Einbringen einer Bridge in das Netz als unmöglich betrachtet werden kann. Da durch den Anschluss eines Fremdrechners ein totaler Verlust aller Schutzziele gegeben ist, ist das Risiko dieser Bedrohung als *hoch* einzuschätzen. Das Mitschneiden von Paketen auf der Funkstrecke verletzt nur das Schutzziel *Vertraulichkeit* und hat daher niedriges Risiko. Eine durch äußere Zwänge begrenzte Auswahl von Sicherungsmaßnahmen würde sich daher hier auf das Einbringen eines Fremdrechners konzentrieren. Insgesamt geht laut dieser Analyse von einem Schicht-2-Zugriff ein hohes Risiko aus, da er möglich ist und alle drei Schutzziele verletzt werden.

4.1.5 Auswahl von Sicherungsmaßnahmen

Nachdem im letzten Abschnitt die Risiken einzelner Bedrohungen festgestellt wurden, können nun passende Gegenmaßnahmen für die zur Realisierung dieser Bedrohungen verantwortlichen Schwachstellen ausgewählt werden. So ist das Einbringen eines Fremdrechners entweder über die Absprache mit dem entsprechenden Nutzer und die Verwendung von dessen Netzwerkdose oder über direkten Zugriff auf den Switch im Serverraum möglich. Während im ersten Fall als nicht-technische Maßnahme ein Verbot des Anschlusses von Fremdrechnern durch den Vorstand empfohlen werden kann, sind im zweiten Fall zweierlei technische Maßnahmen möglich: entweder die Identifizierung von angeschlossenen Rechnern am Switch und das Aussperren von Fremdrechnern oder die

Verhinderung des physischen Zugriffs auf den Switch durch abschließbare Schränke im Serverraum. Die erste Maßnahme erschwert auch gleichzeitig noch den Zugriff nach Absprache mit dem Nutzer und ist so zur Sicherung sehr zu empfehlen.

Das Mitschneiden der Funkstrecke kann im Grunde genommen nur durch eine Verschlüsselung des gesamten Verkehrs erreicht werden, da eine räumliche Begrenzung der Signale auf nicht-öffentlichen Grund prinzipbedingt nicht möglich ist.

Die Formulierung der Sicherheitspolitik könnte daher in etwa wie folgt aussehen:

Um den Anschluss fremder Rechner an das FeM-Net zu verhindern, findet eine Identifizierung der Nutzerrechner und ein Aussperren fremder Rechner statt. Um einer Manipulation der betreffenden Netzwerktechnik vorzubeugen, sind die Schränke, in denen sich diese befindet, abgesperrt.

Da die Funkstrecken zum Anschluss der Pörlitzer Höhe und der Schlossmauer über öffentlichen Grund verlaufen und somit ein Empfang der Signale nicht verhindert werden kann, wird der gesamte Verkehr auf diesen Strecken verschlüsselt um ein Mitschneiden von Informationen zu verhindern.

4.2 Auswahl technischer Maßnahmen

Ausgehend von der allgemein verständlichen Sicherheitspolitik kann nun die Auswahl konkreter technischer Maßnahmen zur Realisierung der geforderten Bedingungen erfolgen. Diese müssen dann nicht mehr für technische Laien verständlich sein, da mit ihrer Konfiguration und Dokumentation nur Techniker in Berührung kommen sollten.

Die Forderung nach Identifizierung der Nutzerrechner und Aussperrung fremder Systeme ist relativ einfach durch die von den HP Procurve angebotene Port Security zu realisieren. Dabei kann auf den Switches für jeden Port eine MAC-Adresse einer Netzwerkkarte konfiguriert werden, welche als zulässig erkannt wird. Des Weiteren kann eine Aktion beim Auftreffen einer falschen MAC-Adresse ausgelöst werden, welche vom Ignorieren des Vorfalls, über das Blockieren der Pakete bis hin zur Abschaltung des betreffenden Ports reichen kann.

Um eine Manipulation des Netzwerkequipments zu verhindern, ist die Ausstattung der verwendeten 19-Zoll-Schränke mit einem Schließsystem nötig. Da die Schränke mit Standardschlössern ausgeliefert werden, deren Schlüssel weiträumig im Umlauf sind, bieten sie keine ausreichende Sicherheit. Ein Austausch der Schlösser ist daher notwendig.

Zur Verschlüsselung der Signale der Funkstrecken eignet sich das im passenden IEEE-Standard 802.11b vorgesehene *Wired Equivalent Privacy (WEP)*. Auch wenn dieses System in den vergangenen Jahren einige Schwächen gezeigt hat, so ist doch über einen regelmäßigen Wechsel der Schlüssel – welcher Aufgabe des Netzwerkmanagements ist –

eine ausreichende Sicherheit erreichbar. Sollte höhere Sicherheit gewünscht werden, so kann WEP durch anerkannte Verfahren wie IPSec ersetzt werden.

4.3 Unterstützung durch das Netzwerkmanagement

Selbst bei der relativ einfachen Auswahl an technischen Sicherungsmaßnahmen ist bereits eine Unterstützung durch das Netzwerkmanagement sinnvoll. Speziell die Konfiguration der einzelnen Switchports mit den passenden MAC-Adressen ist perfekt automatisierbar. Im FeM-Net wird dies realisiert über eine Anbindung der zentralen Nutzerdatenbank an das Management der Switches via SSH. Denkbar wäre zwar auch eine Lösung über SNMP, da die Switches auch das Management mit Hilfe dieses Protokolls beherrschen, aber aus Sicherheitsgründen – die Agents der Switches implementieren nur SNMPv1 – wurde die andere Lösung vorgezogen. Der regelmäßige Wechsel der Schlüssel für die Sicherung der Funkstrecke kann relativ einfach über das Telnet-Interface der die Strecke versorgenden Accesspoints erfolgen. Die Generierung neuer Schlüssel sowie deren Konfiguration auf den Accesspoints kann von einem Rechner im Netz automatisch ausgeführt werden. Zur Sicherung der Übertragung an die Accesspoints können zwei Rechner mit je einer dedizierten Leitung zu einem der beiden verwendet werden. Diese können den Austausch des notwendigen gemeinsamen Schlüssels untereinander durch Protokolle wie SSL absichern.

5 Zusammenfassung

Ziel des Hauptseminars war die Vorstellung von Verfahren zur Sicherung von Netzen und deren Verbindung mit den Techniken des Netzwerkmanagements. Als zentraler Punkt der Netzwerksicherheit wurde dabei auf die Sicherheitspolitik als globales Konzept hinter den eigentlichen technischen Maßnahmen eingegangen. Es wurde ein möglicher Weg zu ihrer strukturierten Erstellung aufgezeigt. Dieser Weg führt in vier Analysestufen bis zur Formulierung der eigentlichen Sicherheitspolitik. Dabei werden quasi als „Nebenprodukt“ besondere Schwachstellen und Bedrohungen ebenso aufgezeigt, wie Empfehlungen für nicht-technische Maßnahmen gegeben. Diese sind zwar nicht Bestandteil der Sicherheitspolitik, werden aber nahezu immer zu ihrer Umsetzung benötigt. Zur strukturierten Risikoanalyse, welche für eine sinnvolle Auswahl von Sicherungsmaßnahmen zwingend notwendig ist, wurde das Hilfsmittel der Bedrohungsbäume vorgestellt. Diese universell zu Analyse Zwecken einsetzbaren Bäume bieten eine Vielzahl von Möglichkeiten und machen den Prozess der Risikoanalyse – und damit letzten Endes die Auswahl von Sicherungsmaßnahmen – transparent und wiederholbar.

Im Bereich des Netzwerkmanagements wurden globale Konzepte kurz anhand des Protokolls SNMP erläutert. Dieses Protokoll hat sich, seit es 1989 zuerst beschrieben wurde, als Standard für das Management von Netzwerkgeräten durchgesetzt. Nach einer kurzen Vorstellung der Protokollarchitektur wurde kurz auf Probleme hinsichtlich der Sicherheit und auf Erweiterungen diesbezüglich eingegangen. Zuletzt wurde das Netzwerkmanagement unter dem Aspekt der Netzwerksicherheit betrachtet. Kernpunkt dabei waren die durch ein funktionierendes Management drastisch verkürzten Reaktionszeiten, welche oft die einzige Möglichkeit sind, Sicherheitsprobleme zu umgehen.

Im letzten Teil der Arbeit wurden die vorgestellten theoretischen Möglichkeiten am praktischen Beispiel demonstriert. Als Anwendungsfall diente dabei das Ziel eines Schicht-2-Zugriffes auf das Campusnetz der Forschungsgemeinschaft elektronische Medien e.V. in Ilmenau.

Abschließend bleibt festzustellen, dass eine strukturierte Vorgehensweise zur Absicherung von Netzen aufgrund der Komplexität des Problemfeldes zwingend notwendig ist. Auch wenn die eigentliche Analysearbeit immer ein hohes Maß an Kreativität fordert, so unterstützen doch die vorgestellten Hilfsmittel den Prozess durch das Einbringen von Übersichtlichkeit und Reproduzierbarkeit. Eine Absicherung großer Netzwerke ist ohne ein übergreifendes Konzept und ohne die Unterstützung durch automatisiertes Netzwerkmanagement nicht mehr denkbar.

Literatur

- [BUG] *BugTraq*.
<http://www.securityfocus.com/archive/1>.
- [EDZ01] ELIZABETH D. ZWICKY, SIMON COOPER UND D. BRENT CHAPMAN: *Einrichten von Internet Firewalls*. O'Reilly, 2001.
- [FEM] *Forschungsgemeinschaft elektronische Medien e.V.*
<http://www.fem.tu-ilmenau.de>.
- [JC] J.D. CASE, M. FEDOR, M.L. SCHOFFSTALL J. DAVIN: *A Simple Network Management Protocol (SNMP)*.
<http://www.ietf.org/rfc/rfc1157.txt>.
- [OSI] *Das OSI Referenzmodell*.
http://www.rvs.uni-bielefeld.de/~heiko/tcpip/kap_1_3_osi.html.
- [Sch00] SCHNEIER, BRUCE: *Secrets & Lies - Digital Security in a Networked World*. John Wiley & Sons, Inc., 2000.