Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

SVS-Aufgabensammlung

3. März 2014 · http://svs.informatik.uni-hamburg.de/

Diese Aufgabensammlung wird in den Kursen des Arbeitsbereichs Sicherheit in verteilten Systemen (Prof. Dr. Hannes Federrath) verwendet. Verbesserungsvorschläge sind stets willkommen! Eine Übersicht der Aufgaben finden Sie ab Seite 40.

1 Technische Grundlagen

Aufgabe 1.1 Nachrichten, Daten, Information
In der elektronischen Datenverarbeitung kommen sehr häufig die Begriffe Nachricht, Daten und Information vor. Wie grenzen Sie die Begriffe gegeneinander ab?

Aufgabe 1.2 Anti-Spam-Tools
Analysieren Sie die am Markt befindlichen Anti-Spam-Tools nach ihrer Funktionsweise und Wirksamkeit.

Aufgabe 1.3 Sicherheit von weit verbreiteten Kommunikationsprotokollen
Die Kommunikationsprotokolle ftp, telnet und http gelten heute als unsicher. Warum? Nennen Sie jeweils das heute als sicher geltende Äquivalent!

2 Grundbegriffe der IT-Sicherheit

Aufgabe 2.1 Verteilte Systeme und Sicherheit
Welche Vor- und Nachteile bzgl. Sicherheit bietet ein verteiltes System gegenüber einem zentralen?

Aufgabe 2.2 Digitale Systeme und Sicherheit
Welche Vor- und Nachteile bzgl. Sicherheit bieten digitale Systeme gegenüber analogen Systemen bei der Übertragung und Programmierung?

Aufgabe 2.3 Sicherheit in Beispielanwendungen
Welche Schutzziele sind für folgende Anwendungen typischerweise zu realisieren? Definieren Sie jeweils ein geeignetes Angreifermodell.

a) Elektronische Archivierung von Unternehmensdaten,

b) Vernetzte Personaldatenverarbeitung,

c) Workflowmanagement,

d) Biometriedatenerfassung und -auswertung auf einer Intensivstation,

e) Anschluss von Zweigstellen einer Bank,

f) Realisierung eines elektronischen Personalausweises.

3 Aufgaben zur Sicherheit allgemein

Aufgabe 3.1 Schutzziele
Erläutern Sie die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Verdecktheit, Anonymität, Unbeobachtbarkeit, Zurechenbarkeit und Erreichbarkeit.

Aufgabe 3.2 Abgrenzung von Schutzzielen
Grenzen Sie die folgenden Schutzziele jeweils voneinander ab:

1. Anonymität, Pseudonymität und Unbeobachtbarkeit,
2. Vertraulichkeit und Verdecktheit,
3. Integrität und Zurechenbarkeit sowie
4. Verfügbarkeit und Erreichbarkeit.

Aufgabe 3.3 Integrität und Zurechenbarkeit
Worin besteht der Unterschied der Schutzziele Integrität und Zurechenbarkeit?

Aufgabe 3.4 Integrität, Verfügbarkeit und Korrektheitsbegriff
Definieren Sie die Begriffe *Integrität* und *Verfügbarkeit* unter Zuhilfenahme des Begriffs (partielle, totale) *Korrektheit*.

Aufgabe 3.5 Techniken zur Umsetzung von Schutzzielen
Nennen Sie jeweils eine geeignete Technik, mit der die Schutzziele Anonymität, Pseudonymität und Unbeobachtbarkeit, Vertraulichkeit, Verdecktheit, Integrität, Zurechenbarkeit, Verfügbarkeit und Erreichbarkeit umgesetzt werden können.

Aufgabe 3.6 Ausgewählte Angriffsformen
In der Vorlesung wurden verschiedene Angriffsformen beschrieben (Folie Nr. 24, Foliensatz „Einführung in die IT-Sicherheit“). Lesen Sie sich die beiden untenstehenden Situationsbeschreibungen durch. Überlegen Sie sich dann, wie diese Systeme auf aktive oder passive Angriffe reagieren und welche Schutzziele dadurch bedroht sind. Für welche Angriffsart bzw. Angriffsarten sind die Systeme anfällig? Was wären mögliche Gegenmaßnahmen?

1. Unmittelbar vor der Durchführung eines militärischen Kampfeinsatzes steigt die Anzahl der Essenslieferungen (Pizza, Burger, Croques, Sushi, ...), die an die Adresse des Verteidigungsministeriums geliefert werden, massiv an.
2. Viele öffentliche WLAN-Access-Points (APs) teilen allen Stationen (Clients) in Reichweite ihren Netznamen (SSID) mit. Der Nutzer einer Station wählt aus der Liste aller Stationen anhand der SSID das Netz mit dem er sich verbinden will. Damit der Nutzer diese Auswahl nicht jedes Mal wieder treffen muss, verbinden sich die Stationen automatisch mit Access Points, mit denen sie bereits verbunden waren. Hierzu wird eine Liste der bereits bekannten SSIDs auf der Station aufbewahrt. Stehen an einem Ort mehrere APs mit derselben SSID zur Auswahl, verbindet sich eine Station i. d. R. mit dem AP mit der größten Signalstärke.

4 Angreifermodelle

Aufgabe 4.1 Angreifermodell
Was versteht man unter einem Angreifermodell und warum stellt man es auf? Welche einen Angreifer beschreibenden Kriterien werden in einem Angreifermodell berücksichtigt? Geben Sie zu jedem Kriterium auch die konkreten Ausprägungen an.

Aufgabe 4.2 Konkrete Angreifermodelle
Nennen Sie Beispiele für konkrete Angreifer:

a) Außenstehende: .....

b) Nutzer des Systems: .....

c) Kommunikationspartner: .....

d) Betreiber des Systems: .....

e) Wartungsdienst: .....

f) Produzenten des Systems: .....

g) Entwerfer des Systems: .....

h) Entwerfer/Produzenten der Entwurfs- und Produktionshilfsmittel: .....

Aufgabe 4.3 Allmächtiger Angreifer
Warum ist ein bzgl. Rechenkapazität unbeschränkter Angreifer kein allmächtiger Angreifer?

Aufgabe 4.4 Angreifermodell für den Geldautomaten
Stellen Sie das Angreifermodell für das Abheben von Bargeld an Geldautomaten mit einer EC-Karte auf.

5 Sicherheitsmanagement

Aufgabe 5.1 Bedrohungsanalyse
Als Sicherheitsbeauftragter einer Bildungseinrichtung (z.B. Universität) sollen Sie eine Bedrohungsanalyse bzgl. folgender IT-Systeme durchführen:

a) System zur Erfassung und Verwaltung von Leistungs- und Prüfungsdaten der Schüler/Studenten,

b) Systeme für den Webauftritt,

c) Arbeitsstationen (CIP-Pools).

Aufgabe 5.2 Mangelnde IT-Sicherheit in Unternehmen
Nennen Sie die Ihrer Meinung nach drei häufigsten Ursachen für mangelnde IT-Sicherheit in Unternehmen.

Aufgabe 5.3 Einsatz von Sicherheitsbausteinen
Sie sind Teil eines Teams externer Sicherheitsexperten das Sicherheitsmaßnahmen vorschlagen soll, um die Fertigungssysteme zu schützen. Gegeben ist folgendes Bedrohungsszenario (basiert auf Texten der Diplomarbeit von Christof Weigl, 2005):

Die Standorte eines großen deutschen Unternehmens sind an das vom Konzern betriebene Corporate IP Netzwerk angebunden. Jedem Rechner des Unternehmens ist eine weltweit erreichbare und eindeutige IP-Adresse zugewiesen. Bei den im Fertigungsbereich genutzten Systemen handelt es sich um Steuerungs-, Produktions- und Prüfsysteme. Es kommen verschiedenste Betriebssysteme zum Einsatz. Diese Systeme werden zum größten Teil direkt vom Hersteller des jeweiligen Produktionssystems mit einem Betriebssystem ausgestattet und angeliefert. Das Ersetzen des ursprünglichen Betriebssystems durch ein modernes, einfacher zu verwaltendes ist nicht möglich. Zum Teil erlischt der Supportanspruch an den Hersteller oder die zum Betrieb der Produktionsmaschine notwendige Software wird nicht mehr korrekt ausgeführt (z.B. Timingprobleme, die zu veränderten Ausbringungsmengen führen oder Schrittmotoren falsch ansteuern). Von den Herstellern werden zum Teil veraltete und unsichere Betriebssysteme (z.B. veraltete Windowssysteme, DOS-Systeme und ältere Linux/Unix-Systeme) für den Betrieb der Produktionssysteme gestellt. Somit sind besondere Lösungen erforderlich, um Virenscans oder Betriebssystemupdates durchzuführen. Da Realtime-Scanner während der gesamten Uptime der Systeme im Hintergrund als Prozess laufen und auch Updates für die Installation die Performanz des Systems beeinträchtigen, muss auf andere Maßnahmen ausgewichen werden.

An wenigen Fertigungslinien können Standardclients eingesetzt werden. Diese Systeme haben den gleichen Sicherheitslevel wie normale Office-PCs. Die Fertigungsabteilungen sind angehalten, eine Systemlösung vom Hersteller zu beziehen, die mit einem Standard-PC zu betreiben ist. In einigen wenigen Fällen wird von den

zuständigen Supportabteilungen eine „Basisinstallation“ an den Hersteller ausgegeben, der dann die Systeme mit dieser Installation liefert.

Ausgelöst durch die erhöhte Bedrohung durch Viren und Würmer Würmer, besteht Bedarf im Unternehmen, sich verstärkt über mögliche Sicherheitsmaßnahmen Gedanken zu machen, um Verfügbarkeit und Datenintegrität in Zukunft sicherzustellen.

a) Wählen und kombinieren Sie geeignete Sicherheitsbausteine, um das System vor dem beschriebenen Angreifer zu schützen.

b) Erstellen Sie ein „Flipchart-Sheet“ oder Poster Ihrer Lösung.

c) Präsentieren Sie Ihre technische Lösung in einem Kurzreferat (max. 3 Minuten) ohne (!) Präsentationsfolien.

d) Bewerten Sie die Lösung der anderen Referenten. Erstellen Sie hierzu einen Bewertungsbogen.

Der Dozent hat die Rolle eines Repräsentanten des Unternehmens. Stellen Sie ihm etwaige Detailfragen zur Netzstruktur.

Aufgabe 5.4 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
Besorgen Sie sich den Wortlaut des KonTraG (BGBl I 1998/24) und erläutern Sie die Textstellen, die für das IT-Sicherheitsmanagement von Bedeutung sein können.

Aufgabe 5.5 Security Policy
Angenommen, Sie erstellen Ihre Diplomarbeit unf Ihrem Privat-PC oder -Laptop. Schreiben Sie eine Security Policy, mit deren Umsetzung sichergestellt wird, dass der erfolgreiche Abschluss nicht durch Sicherheitsprobleme mit der verwendeten IT gefährdet wird.

Aufgabe 5.6 Gefährdungs- und Maßnahmenkataloge nach BSI-GSHB
Sie sollen einen bereits installierten WWW-Server auf seine Sicherheit überprüfen. Entwickeln Sie hierfür einen Prüfplan. Orientieren Sie sich dabei an Maßnahme M 2.174 des GSHB.

Aufgabe 5.7 Zertifizierung nach BSI-Grundschutzhandbuch oder ISO 17799?
Ein Unternehmen strebt eine Zertifizierung der IT-Sicherheit an. Es hat die Wahl zwischen einer Zertifizierung nach IT-Grunschutzhandbuch oder ISO 17799.

a) Welche Faktoren sollten bei Ihrer Entscheidung eine Rolle spielen?

b) Erarbeiten Sie ein Vorgehensmodell, das Ihnen den Entscheidungsprozess erleichtert.

6 Rechnersicherheit

Aufgabe 6.1 Physische Sicherheit im Rechenzentrum und lokales Rechnernetz
Die physische Sicherheit der Daten vor Angriffen wird in einem Rechenzentrum – wie auch bei physisch sicheren Geräten – durch die Grundfunktionen Schirmen, Erkennen, Bewerten, Verzögern und ggf. Löschen der Daten gewährleistet.

a) Wodurch werden diese Grundfunktionen in einem Rechenzentrum konkret realisiert?

b) Welche Realisierungen für ein physisch zu schützendes lokales Rechnernetz wären ggf. sinnvoll?

- Schirmung: .....
- Erkennen: .....
- Bewerten: .....
- Verzögern: .....

- Löschen: (meist nicht realisiert, deshalb keine Antwort erforderlich)

Aufgabe 6.2 Seitenkanalangriffe
Seitenkanalangriffe können insbesondere die Sicherheit von Chipkarten gefährden.

a) Erläutern Sie die grundsätzliche Vorgehensweise des Angreifers bei einem Seitenkanalangriff.

b) Was ist das Angreifermodell eines Seitenkanalangriffs auf eine Chipkarte?

c) Wie funktioniert ein Fault-Injection-Angriff auf eine Chipkarte?

Aufgabe 6.3 Identifikation von IT-Systemen durch Menschen
Schreiben Sie ein Demonstrationsprogramm, das den Login-Screen eines Rechnersystems simuliert. Wie könnte eine auf der Eingabe von Username und Passwort basierende Login-Prozedur aufgebaut sein, die grundsätzlich vor einem solchen Angriff schützt?

Aufgabe 6.4 Zugriffs- und Zugangskontrolle
In der IT-Sicherheit unterscheidet man zwischen den Systemfunktionen *Zugriffskontrolle* und *Zugangskontrolle*. Informieren Sie sich über die beiden Techniken, die auch im Rahmen der Vorlesung behandelt werden und beantworten Sie folgende Fragen.

1. Erläutern Sie stichpunktartig den Zweck der jeweiligen Technik.
2. Ist es sinnvoll, ein System mit einer Zugangskontrolle auszustatten, jedoch keine Mechanismen zur Zugriffskontrolle zu implementieren? Begründen Sie Ihre Antwort mit einem Beispiel.
3. Die Absicherung eines Systems mittels einer Zugriffskontrolle setzt hingegen immer auch eine vorherige Zugangskontrolle voraus. Warum?
4. File-Sharing-Dienste (z. B. Dropbox) ermöglichen es ihren Nutzern, einzelne Ordner mit Hilfe eines *Share-this-Folder*-Links anderen Nutzern freizugeben (Zugriffskontrolle auf Ordner-Ebene). Mit dem Link kann jeder auf den freigegebenen Ordner zugreifen, auch wenn er kein Konto bei dem jeweiligen Dienst hat. Ein Benutzerkonto (Login) beim File-Sharing-Dienst ist zum Zugriff auf den Ordner jedoch nicht erforderlich. Scheinbar widerspricht diese Situation also der Aussage in der vorherigen Teilaufgabe. Nehmen Sie hierzu Stellung.

Aufgabe 6.5 Passwortüberprüfung
Wie funktioniert die Passwortüberprüfung unter Unix? Was ist das Angreifermodell? Oder genauer: Was ist die Annahme über die Verbreitung des Angreifers?

Aufgabe 6.6 Passwortknacken
Schreiben Sie ein Programm (z.B. in Java, C oder Ruby) zum Knacken einer Passwort-Datei mit Hilfe eines Wörterbuch-Angriffs (dictionary attack). Besorgen Sie sich ein entsprechendes deutsches Wörterbuch aus dem Internet. Die Passwörter sollen nur aus Kleinbuchstaben bestehen.

Aufgabe 6.7 Klartext-Kennwörter
Nennen Sie zwei Gründe, warum die Kennwörtern in einem IT-System nicht im Klartext abgespeichert werden sollten.

Aufgabe 6.8 Speicherung gehashter Kennwörter
Durch kryptographische Hashfunktionen (mathematische Einwegfunktionen) können Kennwörter sicherer als im Klartext hinterlegt werden. Wie funktionieren Kennwortspeicherung und -prüfung bei diesem Verfahren in der einfachsten Form? Warum ist dieses Verfahren sicherer als die Abspeicherung im Klartext? Es gibt Möglichkeiten, das ursprüngliche Passwort anhand eines gegebenen Hashwerts wieder zu ermitteln. Probieren Sie dies am folgenden Beispiel aus.

```
#user;passwordhash
leroy;06e2b745f3124f7d670f78eabaa94809
```

Aufgabe 6.9 Sicherheit alter UNIX-Kennwörter
Bei vielen Unix-Betriebssystemen wurden früher lediglich die ersten acht Stellen eines Kennwortes verwendet. Wie lange benötigt ein Passwort-Cracking-Tool maximal, das eine Million Passwörter pro Sekunde prüfen kann, wenn bekannt ist, dass das Passwort lediglich aus alphanumerischen Zeichen besteht.

Aufgabe 6.10 Rainbow-Tables
Eine leistungsfähige Technik, mit der auf Basis eines Hashwerts ein dazu passendes Passwort ermittelt werden kann, stellen sogenannte *Rainbow Tables* dar. Zur Beantwortung können Sie http://h-online.com/-746217 heranziehen. Was versteht man in diesem Zusammenhang unter dem Begriff *Time-Memory-Trade-Off*? Was ist die grundsätzliche Idee von Rainbow Tables bzw. den Vorgänger-Verfahren. Was haben Rainbow Tables mit dem Regenbogen zu tun?

Aufgabe 6.11 Salted Hashing
Einen wirksamen Schutz gegen Rainbow Tables stellt das Hinzufügen einer zufälligen Zeichenkette (auch „Salt“ genannt) vor dem Anwenden der Hash-Funktion h auf ein Kennwort dar, was als $\mathrm{h}(\mathrm{SALT}||\mathrm{PASSWORD})$ ausgedrückt werden kann. Warum?

Aufgabe 6.12 Implementierung eines Brute-Force-Angriffs mit einem Wörterbuch
Schreiben Sie ein Programm (z. B. in Java, C, Ruby, Python, Perl) zum Ermitteln eines Kennworts anhand eines Hashwerts mit einem Wörterbuch-Angriff. Besorgen Sie sich dazu ein deutsches Wörterbuch aus dem Internet. Testen Sie Ihre Implementierung mit den unten angegebenen Daten. Über das gespeicherte Kennwort sind die folgenden Fakten bekannt: Es ist ein deutsches Wort, steht im Wörterbuch, ist kleingeschrieben und nicht länger als 5 Zeichen. Das Salt wird beim Hashen vor das Passwort gestellt. Bei der Hash-Funktion handelt es sich um MD5.

```
# user;salt:hash
berta;xohth4dew5p8:199f066a0bac4140e792d1d4a434ae44
```

a) Welches Kennwort konnten Sie ermitteln?

b) Skizzieren Sie die Funktionsweise Ihres Programms anhand der wichtigsten Stellen Ihres Programms (bitte nicht separat abgeben, sondern ins PDF einfügen). Achten Sie dabei auf Verständlichkeit und Übersichtlichkeit.

c) Wie müsste das Programm erweitert werden, wenn das Salt im Vorfeld nicht bekannt wäre?

Aufgabe 6.13 Angreifermodell von SecurID
Ein Zuganskontrollsystem kombiniere das Einmalpasswortsystem SecurID (Besitz) mit dem klassischen Passwort (Wissen). Bitte beschreiben Sie das zugrunde liegende Angreifermodell eines solchen Zugangskontrollsystems, d.h. definieren Sie die maximal berücksichtigte Stärke des Angreifers, gegen den das Zugangskontrollsystem sicher ist (Rollen, Verbreitung, Verhalten, Rechenkapazität des Angreifers).

Aufgabe 6.14 Funktionsweise von SecurID
Bei SecurID wird minütlich ein Einmalpasswort aus einer internen Zeitbasis und einem Geheimnis erzeugt. Welcher Angriff wäre möglich, wenn anstelle der internen Zeitbasis das Signal eines großräumig empfangbaren Zeitzeichensenders genutzt würde?

Aufgabe 6.15 Unsichere Frage-Antwort-Verfahren
Ein klassisches Frage-Antwort-Verfahren zur Überprüfung der Echtheit einer Identitätsangabe ist folgendes:

P1: Das prüfende IT-System sendet eine Zufallszahl und erwartet von der Gegenstelle die korrekte Verschlüsselung der Zufallszahl.

Kann dieses Verfahren auch umgedreht werden?

P2: Das prüfende IT-System generiert eine Zufallszahl, verschlüsselt sie und sendet die verschlüsselte Zufallszahl. Die Gegenstelle sendet die entschlüsselte Zufallszahl zurück.

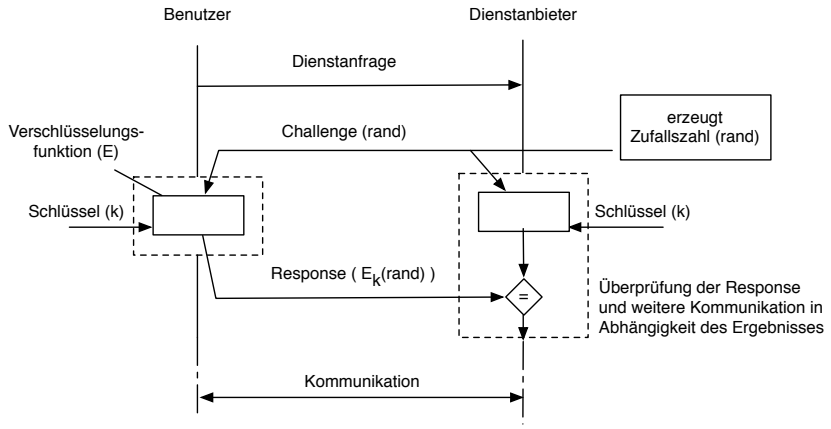
Welche Annahmen über die Zufallszahlenerzeugung liegen den Protokollen zugrunde?

Aufgabe 6.16 Authentifizierungsprotokolle

1. **Verschlüsselte Passwort-Übermittlung.** Der Nutzer eines Laptops soll sich gegenüber einem Server mit einem Benutzernamen u und einem Passwort p authentisieren. Um zu verhindern, dass Benutzername und Passwort im Klartext übertragen werden, werden diese Daten mit einem in der Vergangenheit einmalig festgelegten Schlüssel k unter Verwendung der Verschlüsselungsfunktion $\mathrm{c} = \mathrm{E_k}(\mathrm{u}, \mathrm{p})$ verschlüsselt. Es wird lediglich c an den Server übermittelt. Welche Schwäche weist dieses Protokoll gegenüber einem passiven bzw. aktiven Angreifer auf der Kommunikationsstrecke auf?

2. **Authentifikationssystem auf Basis indeterministischer symmetrischer Verschlüsselung.** Ein befreundeter Systemadministrator macht den Vorschlag, das oben genannte Verfahren wie folgt zu verbessern: Der Nutzer soll nun $\mathrm{c} = \mathrm{E_k}(\mathrm{r}, \mathrm{u}, \mathrm{p})$ übertragen, wobei r eine selbst gewählte, große (kryptographisch sicher erzeugte) Zufallszahl ist, die den anderen Daten vor der Verschlüsselung vorangestellt wird. Wie beurteilen Sie die Sicherheit dieser Realisierung, d.h. welche Angriffe werden dadurch verhindert, welche sind weiterhin möglich?

3. **Challenge-Response-Authentifizierung.** Das folgende Bild zeigt ein einseitiges Challenge-Response-Authentifizierungsverfahren auf Basis eines symmetrischen Kryptosystems. Welche Angriffe, die bei Teilaufgabe 2 noch möglich waren, werden dadurch verhindert, welche sind weiterhin erfolgreich?



4. **Sichere Challenge-Response-Authentifizierung.** Das Protokoll aus der vorherigen Teilaufgabe weist eine Schwachstelle auf: Ein Angreifer kann sich gegenüber dem Benutzer als Dienstanbieter ausgeben, ohne dass der Benutzer dies erkennen kann. Erweitern Sie das Challenge-Response-Protokoll dahingehend, dass sich auch der Benutzer sicher sein kann, mit dem richtigen Dienstanbieter verbunden zu sein. Erstellen Sie dazu eine aussagekräftige Abbildung bzw. führen Sie genau auf, welche Nachrichten Nutzer und Server gegenseitig übermitteln und erläutern Sie, warum der Angriff nun nicht mehr funktioniert. Verwenden Sie dabei weiterhin ein symmetrisches Kryptosystem.

Aufgabe 6.17 Realisierung eines Online-Tickets

Ein Kino möchte den Online-Verkauf von Eintrittskarten realisieren, die sich der Kunde an seinem PC ausdruckt. Jede Eintrittskarte soll einen Strichcode enthalten, der bei der Einlasskontrolle eingelesen wird.

a) Definieren Sie ein plausibles Angreifermodell.

b) Denken Sie sich eine Realisierung aus, die gegen Ihren Angreifer schützt.

Hinweis: Die Aufgabenstellung besitzt einige Freiheitsgrade, d.h. Sie können, wenn Sie wollen, auch mehrere Angreifermodelle und Designvorschläge machen.

Aufgabe 6.18 Unsichere Implementierung von Sicherheitsfunktionen

Gegeben ist folgendes (stark vereinfachtes) Codefragment (geschrieben in der Programmiersprache C) einer Server-Implementierung. Zur Authentisierung muss der Nutzer ein Passwort angeben, das der Server mit einem lokal in einer Datenbank gespeicherten Referenzpasswort vergleicht. Welche gravierende Schwäche hat diese Implementierung (unter Berücksichtigung der verwendeten Programmiersprache)? Erläutern Sie den Angriff auf den Server.

```
...
char given_password[8];
char expected_password[8];
...

// read expected password from local database

// and store it in expected_password
...

// receive request from client
...

// receive password from client
int i=0;
char c;
c = readChar(client);
while(!(c == '\n')) {
    given_password[i]=c;
    c = readChar(client);
    i++;
}

// check correctess of given_password
if (strcmp(given_password,expected_password)==0) {
    // authentication successful
    ...
} else {
    // login rejected
    ...
}
```

Aufgabe 6.19 Biometrische Authentifizierung beim EasyPASS-System
Im Rahmen eines Pilotprojekts am Frankfurter Flughafen wird die vollautomatische Passkontrolle und Einreise in die Bundesrepublik Deutschland anhand des biometrischen Reisepasses erprobt – eine manuelle Bearbeitung durch einen Grenzbeamten kann dadurch entfallen. Am *EasyPASS*-Automat müssen die Reisenden dazu ihren elektronischen Pass selbständig einscannen. Mittels einer Kameraaufnahme wird anschließend das Gesicht des Passagiers mit dem auf dem Pass digital gespeicherten Lichtbild verglichen. Bei Fragen zur Bedienung stehen Grenzbeamte zur Verfügung. Fotostrecke: http://www.spiegel.de/fotostrecke/fotostrecke-47853.html

1. Informieren Sie sich über die biometrischen Techniken im elektronischen Reisepass der Bundesrepublik Deutschland und die Funktionsweise von EasyPASS.
2. Da inzwischen die meisten Bürger eine Webcam in ihrem Computer/Laptop eingebaut haben, wird nun im Rahmen einer eGovernment-Initiative vorgeschlagen, den elektronischen Reisepass auch zu Hause zu verwenden. Die Bürger sollen dadurch Dienstleistungen von Behörden über das Internet wahrnehmen können. Hierzu sollen Lesegeräte an die Bürger ausgegeben werden, mit denen der Pass ausgelesen wird. Mit der Webcam wird dann ein Foto des Benutzers aufgenommen und mit dem Lichtbild des Passes verglichen. Im Falle einer erfolgreichen Überprüfung werden die Informationen aus dem Pass an die Behörden-Website weitergeleitet (Authentifizierung) und der Dienst kann in Anspruch genommen werden. Nennen Sie zwei potentielle Schwachstellen dieser Realisierungsidee.

Aufgabe 6.20 Biometrische Authentifizierung anhand des Tippverhaltens
Im Rahmen eines Forschungsprojekts wurde ein Authentfizierungssystem entwickelt, welches Nutzer beim Einkauf in einem Online-Shop anhand des Tippverhaltens authentifiziert. Dabei wird die Tatsache ausgenutzt, dass praktisch jeder Nutzer die Tasten auf der Tastatur auf charakteristische Weise anschlägt (Zeitabstände zwischen den Anschlägen sowie häufige Tippfehler). Die Tippmuster werden direkt im Browser von einem Flash-Applet oder per JavaScript aufgezeichnet und verschlüsselt per SSL an den Webshop übertragen. Die bislang besten Ergebnisse werden erzielt, wenn für alle Nutzer immer derselbe Authentifizierungs-Satz (z. B. *It never rains in southern California*) verwendet wird. Bei der erstmaligen Registrierung im Online-Shop geben die Nutzer eine Tipp-Probe ab, indem sie etwa 20 mal den Authentifizierungs-Satz eingeben. Daraus errechnet das System ein charakteristisches Profil des Nutzers, welches im Online-Shop hinterlegt wird. Bei späteren Besuchen des Online-Shops gibt der Nutzer dann zur Authentifizierung seinen Benutzernamen ein und tippt den Authentifizierungs-Satz erneut ab. Der Online-Shop überprüft dann die übermittelte Tipp-Probe mit der Datenbank.

1. Welche Schwachstelle weist das oben beschriebene System auf? Stellen Sie das Angreifermodell auf, das diesem Systementwurf offenbar zugrunde liegt.

2. Welche Gegenmaßnahmen könnte der Betreiber ergreifen?

Aufgabe 6.21 Virenerkennung
Angenommen, ein Angreifer programmiert einen Virus, der seinen eigenen Code vor jedem Einpflanzen in das Wirtsprogramm modifiziert, z.B. indem der Code mit einer Zufallszahl, die vorne angehängt ist, XOR-verknüpft wird. Warum und wie können Virenscanner den Virus sehr wahrscheinlich trotzdem noch erkennen? Wo liegen die Grenzen des Erkennens?

7 Fehlertoleranz, Datensicherung

Aufgabe 7.1 Einzelnes System (Ausfallwahrscheinlichkeit)
Ein System ist insgesamt 8 Stunden 45 Minuten pro Jahr unverfügbar. Wie hoch ist seine Ausfallwahrscheinlichkeit bezogen auf ein Jahr?

Aufgabe 7.2 Einzelnes System (Verfügbarkeit)
Bitte geben Sie die Verfügbarkeit in Prozent für ein System an, das innerhalb eines Monats im Mittel höchstens 1 Stunde ausfallen darf.

Aufgabe 7.3 Einzelnes System (Ausfallzeit)
Gesucht ist die maximal tolerierbare Ausfallzeit p.a.,

a) wenn *während* der Arbeitszeit (8-18 Uhr an 260 Tagen eines Jahres) eine Verfügbarkeit von 99,99% erreicht werden soll. Von 18-8 Uhr ist jederzeit Unverfügbarkeit tolerierbar, d.h. Wartungszeiten können problemlos in diese Zeit verlagert werden.

b) wenn im 24h/7d-Betrieb p.a. 99,99% Verfügbarkeit erreicht werden sollen.

Bitte vergleichen Sie die beiden Ergebnisse miteinander und diskutieren mögliche Umsetzungsvarianten.

Aufgabe 7.4 Gekoppelte Systeme
Ein System besteht aus einer Hardwarekomponente mit einer Verfügbarkeit von $\mathrm{P}_{\mathrm{HW}} = 99,99$ Prozent und einer Softwarekomponente mit $\mathrm{P}_{\mathrm{SW}} = 99,9$ Prozent. Wie hoch ist die Gesamtverfügbarkeit? Wie hoch ist die jährliche Ausfallzeit?

Aufgabe 7.5 Doppelung
Eine Komponente mit einer Verfügbarkeit von $\mathrm{P} = 99,9$ Prozent wird gedoppelt. Wie hoch ist die Gesamtverfügbarkeit und Ausfallzeit pro Jahr?

Aufgabe 7.6 Web-Serversystem mit Lastverteiler
Ein Dienstleister stellt für ein Unternehmen ein Web-Serversystem bereit. Zur Verbesserung der Performance werden zwei Webserver eingesetzt, vor die ein Lastverteiler mit einer Verfügbarkeit von 99,99 Prozent geschaltet ist. Das gesamte Serversystem soll während der Bürostunden werktags von 8 bis 18 Uhr höchstens 5 Stunden pro Jahr (260 Arbeitstage) unverfügbar sein.

a) Welche Verfügbarkeit in Prozent für das gesamte Serversystem ist im Dienstleistungsvertrag anzugeben?

b) Welche Verfügbarkeit in Prozent ist für jeden der beiden Webserver zu gewährleisten? Erforderliche Rechengenauigkeit: 2 Nachkommastellen.

Aufgabe 7.7 Reparaturdauer
Der Erwartungswert für die Zeit bis zum Ausfall einer Komponente sei 50.000 h. Es soll eine Verfügbarkeit von $99,999$ Prozent gewährleistet werden. Wie lange darf die Reparatur maximal dauern?

Aufgabe 7.8 Reparaturdauer bei RAID
Ein Dateiserver ist fünf Jahre in Betrieb gewesen und während dieser Zeit insgesamt nur 4 Stunden und 20 Minuten unverfügbar gewesen.

a) Wie hoch war seine Gesamtverfügbarkeit in Prozent? (Erforderliche Genauigkeit: 3 Nachkommastellen)

b) Der Dateiserver soll nun durch einen neuen mit vergleichbarer Verfügbarkeit und Betriebsdauer ersetzt werden. Zur Verbesserung der Performance erwägen Sie den Einsatz eines RAID-0-Systems (Striping, keine Redundanz) mit 4 Festplatten. Die MTBF der eingesetzten Festplatten betrage ca. 50.000 Stunden je Platte, die MTTR betrage 1 Stunde je Platte (inkl. Recovery). Die Verfügbarkeit der restlichen Komponenten sei ideal 100 Prozent. Ist die geforderte Verfügbarkeit mit RAID-0 noch erreichbar? Begründung!

Aufgabe 7.9 Storage Area Network (SAN) aus RAID-5-Systemen
Eine große Behörde möchte ihr Archiv auf elektronische Datenhaltung umstellen. Es sollen zur Archivierung Festplatten eingesetzt werden, die gemeinsam ein Storage Area Network (SAN) bilden. Es sollen jeweils x Festplatten über RAID-5 zusammengeschaltet werden. Insgesamt y solcher RAID-5 bilden zusammen das (SAN). Das SAN soll insgesamt 30 Terabyte Speicher netto bereitstellen, d.h. zzgl. der Redundanz von 1 Festplatte pro RAID-5. Die Verfügbarkeit pro RAID-5 darf 99,9 Prozent nicht unterschreiten. Die MTTF einer Festplatte sei 40.000 Stunden. Die MTTR sei 2 Stunden pro Ausfall. Es werden nur gleichartige 120 Gigabyte-Platten verbaut.

a) Wieviele Platten dürfen maximal pro RAID eingesetzt werden?

b) Wieviele Platten müssen insgesamt im SAN verbaut werden?

c) Berechnen Sie die exakte Gesamtverfügbarkeit des SAN in Prozent.

Aufgabe 7.10 Serverfarm eines Webmail-Anbieters
Ein großer Webmail-Anbieter möchte damit werben, 365 Tage im Jahr verfügbar zu sein, d.h. die Ausfallzeit seines Dienstes muss pro Jahr einen Tag (24 Stunden) unterschreiten. Er verwendet zur Steigerung der Performance und Verfügbarkeit eine Serverfarm aus 150 gleichartigen Webservern, jeweils mit einer Verfügbarkeit von 95 Prozent. Im Hintergrund arbeitet eine gedoppelte Datenbank, die zudem diversitär ausgelegt ist. Der eine Datenbankserver hat 95 Prozent Verfügbarkeit, der andere erreicht 90 Prozent. Die restliche Systemumgebung hat eine ideale Verfügbarkeit (100 Prozent). Bitte beurteilen Sie, ob das Werbeversprechen (höchstens 1 Tag Ausfall pro Jahr) erfüllt werden kann.

Aufgabe 7.11 Zuverlässigkeit
Angenommen, eine Chipkarte verkraftet im Mittel etwa 100.000 Kontaktzüge, bevor sie unbrauchbar ist. Sie wird durchschnittlich zehnmal am Tag in ein Lesegerät gesteckt. Wie zuverlässig ist die Kontaktgabe nach 1, 5 und 10 Jahren?

Aufgabe 7.12 RAID-Arrays
Vergleichen Sie die RAID-Systeme der Levels 0, 1, 2, 3 und 4 bezüglich Datendurchsatz, I/O-Request-Verarbeitungszeit und Zuverlässigkeit.

Aufgabe 7.13 Vergleich RAID-1 und RAID-5
Sie suchen nach einer fehlertoleranten Speicherlösung. Der Ausfall einer Festplatte soll toleriert werden. In die engere Auswahl kommen RAID-1 und RAID-5, die das Gewünschte leisten. Bitte vergleichen Sie RAID-1 und RAID-5 hinsichtlich

a) Fehlertoleranz,

b) Performance und

c) Kosten,

damit Sie zu einer optimalen Entscheidung kommen könnten, wenn Sie sich tatsächlich entscheiden müssten.

Aufgabe 7.14 Backups bei RAID
Auch die Datensicherung birgt Risiken.

a) Welche Vorsichtsmaßnahmen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit sind beim Backup deshalb zu beachten?

b) Der Einsatz von RAID-Systemen erspart im Regelfall nicht das Backup. Warum nicht?

Aufgabe 7.15 Allgemeines zu Backups

a) Nennen Sie einige typische Probleme, die für eine Datensicherung sprechen.

b) Welche Einflussfaktoren sind bei der Wahl von Backupstrategie und Backupmedium zu berücksichtigen?

c) Auf welche Punkte sollte bei der Wahl des Backup-Aufbewahrungsortes geachtet werden?

d) Was ist der Unterschied zwischen einem inkrementellem und einem differenziellen Backup? Welche Vor- und Nachteile haben diese Varianten?

Aufgabe 7.16 Differenzielles Backup
Sie haben 2+2 Medien zur Verfügung für ein differenzielles Backup, d.h. 2 große Medien (v1 und v2) für ein Vollbackup und 2 kleinere Medien (d1 und d2) für die differenziellen Backups. Es wird wöchentlich (Montags) immer ein Vollbackup geschrieben. Dienstag bis Samstag wird differenziell gesichert. Sonntags erfolgt keine Sicherung. Bitte beschreiben Sie kurz die Wechselstrategie für 3 Wochen.

Aufgabe 7.17 Backupstrategie
Folgende Annahme: Sie schreiben gerade ihre Abschlussarbeit am Arbeitsbereich SVS. Im Rahmen dieser Arbeit führen Sie eine Studie durch, bei der mehrere Benutzer zu selbstgewählten Zeitpunkten Daten zu einem von Ihnen betriebenen Linux-Server in das Verzeichnis /var/www/superstudie/ im Tagesrhythmus hochladen. Ihnen ist besonders wichtig, dass Sie im unwahrscheinlichen Fall eines Datenverlustes möglichst viele der eingereichten Studiendaten für Ihre abschließende Auswertung zur Verfügung haben. Beschreiben sie stichpunktartig ihr Datensicherungskonzept und drucken Sie in Ihrer Lösung ggf. auch ein einfaches Backupscript ab.

Aufgabe 7.18 Backup mittels rsnapshot
Das Linux-Programm *rsnapshot* ermöglicht die Umsetzung des Großvater-Vater-Sohn-Prinzips mittels sog. *hard links*, um den Speicherplatzbedarf des Backups zu reduzieren. Gegeben sei folgender Backup-Plan:

- Zu jeder vollen Stunde (xx:00 Uhr) wird ein *hourly*-Backup durchgeführt. Es werden 24 Kopien aufbewahrt. Das Backup dauert maximal 14 Minuten. Jeden Tag wird auf Basis der *hourly*-Backups um 00:15 Uhr ein *daily-Backup* durchgeführt. Es werden 7 Kopien aufbewahrt. Dieser Prozess dauert maximal 14 Minuten.
- Jeden Sonntag wird um 00:30 auf Basis der *daily*-Backups ein *weekly*-Backup durchgeführt. Es werden 4 Kopien aufbewahrt.

a) Machen Sie sich mit *rsnapshot* und *Hard Links* vertraut. Erläutern Sie jeweils kurz die zentralen Ideen.

b) Bestimmen Sie den Speicherplatzbedarf des gesamten Backups für die Tage 06.12.2011, 07.12.2011, 08.12.2011 und 13.12.2011 jeweils um 23:59:59 Uhr, wenn folgende Ereignisse stattgefunden haben (Der Platzbedarf für *Hard Links* soll vernachlässigt werden. Gehen Sie davon aus, dass Änderungen, die während eines bereits laufenden Backups durchgeführt werden, nicht in das gerade laufende Backup einfließen):
   - 05.12.2011 23:59:59 Uhr: Das Backup wurde eingerichtet, der zu sichernde Ordner enthält noch keine Daten.
   - 06.12.2011 08:15:00 Es werden die Dateien a.dat (500 MB), b.dat (100 MB) und c.dat (50 MB) angelegt.

- 06.12.2011 18:30:00 Die Datei a.dat wird vollständig überschrieben. Neue Größe: 200 MB.
- 07.12.2011 00:10:00 Die Datei d.dat wird angelegt (100 MB).
- 08.12.2011 14:05:00 Die Datei a.dat wird gelöscht.
- 09.12.2011 01:15:00 Die Datei b.dat wird vollständig überschrieben (100 MB).
- 12.12.2011 15:10:00 Eine neue Datei mit dem Namen a.dat wird angelegt (500 MB).

8 Kryptographie I

Aufgabe 8.1 Zentrale Begriffe der Kryptographie

1. Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?
2. Alice (A) und Bob (B) haben jeweils ein Schlüsselpaar erzeugt, um vertraulich miteinander kommunizieren zu können. Sie verfügen nun jeweils über einen öffentlichen (public) Schlüssel (K_p^A bzw. K_p^B) sowie einen privaten (secret) Schlüssel (K_s^A bzw. K_s^B). Ihre öffentlichen Schlüssel haben die beiden bereits bei einem persönlichen Treffen ausgetauscht. Alice möchte Bob nun eine vertrauliche Nachricht übermitteln.
   (a) Unter welchen Umständen wird Alice dazu auf ein sog. *hybrides Kryptosystem* zurückgreifen?
   (b) Wie geht Alice im Detail vor, wenn sie ein hybrides Kryptosystem einsetzt?
   (c) Wie sieht die übertragene Nachricht in diesem Fall aus?

Aufgabe 8.2 Zufallszahlen bei Schlüsselgenerierung
Warum sind bei der Schlüsselgenerierung (echte) Zufallszahlen nötig? Warum ist XOR die geeignete Verknüpfung, wenn die Zufallszahlenanteile mehrerer Instanzen vor der Schlüsselgenerierung zwecks Erhöhung der Sicherheit zu einer einzigen Zufallszahl verknüpft werden?

Aufgabe 8.3 Verschlüsselte PIN-Übermittlung
Der Nutzer eines Laptops soll sich gegenüber einem Server im Heimatnetz durch eine PIN authentisieren. Um die vom Nutzer am Laptop eingegebene PIN nicht mitlesen zu können, wird sie vor der Übermittlung mit dem öffentlichen Schlüssel des Servers verschlüsselt. Analysieren Sie die (Un)-Sicherheit eines solchen Protokolls gegenüber einem Angreifer auf der Kommunikationsstrecke.

Aufgabe 8.4 Symmetrische Schlüssel aus Passwörtern erzeugen
Ein zwischen Sender und Empfänger vereinbartes Passwort könnte als Basis zur Erzeugung eines symmetrischen Schlüssels dienen.

a) Wieviele (zufällige und unabhängige) Zeichen im Passwort sind (mindestens) nötig, um einen 128-Bit-Schlüssel mit maximaler Entropie zu erzeugen? Der Einfachheit sei angenommen, dass als Zeichen nur (zufällige und unabhängige) Großbuchstaben $\{A : Z\}$ vorkommen.

b) Wieviele Zeichen sind erforderlich, wenn Wörter (deutsche Sprache) als Passwort verwendet werden? Die Redundanz der Sprache sei $R = 0,6375$ bit/Zeichen.

Aufgabe 8.5 Spalten-Transpositionen
Bei der Skytala wird ein Zylinder (dessen Durchmesser – bzw. die Anzahl z der beschreibbaren Zeilen – dem Schlüssel entspricht) mit einem Papierstreifen umwickelt, beschrieben und wieder abgewickelt.

a) Eine Verbesserung dieser Spalten-Transposition ergibt sich, wenn zusätzlich auch die Spalten in ihrer Reihenfolge vertauscht werden (was beim Papierstreifen natürlich nicht gelingt, wohl aber im Rechner). Um welchen Faktor vergrößert sich dadurch der Schlüsselraum bei s Spalten?

b) Schreiben Sie eine Skytala mit 4 Zeilen und 3 Spalten (ohne Spaltenvertauschung) in Zyklenschreibweise!

Aufgabe 8.6 Unsicherheit der klassischen Verschiebechiffre
Ein klassisches Verschlüsselungsverfahren ist die Verschiebechiffre. Sie arbeitet typischerweise auf einem Alphabet $\{A : Z\}$ (Klartext, Schlüssel, Schlüsseltext). Ein Schlüsseltextzeichen ergibt sich aus dem um das Schlüsselzeichen verschobene Klartextzeichen:

```
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
u.s.w.
```

Welcher Angriff ist möglich?

Aufgabe 8.7 TextCrypter
Sie erhalten ein Programm zum Ver- und Entschlüsseln von Texten sowie drei Schlüsseltexte. Ihr Ziel ist es, die zugehörigen (deutschsprachigen) Klartexte zu ermitteln. Der TextCrypter arbeitet für Sie als Blackbox, d.h. Sie können ihn verwenden, müssen seine Arbeitsweise aber nicht verstehen. Die Verschlüsselung selbst arbeitet zuverlässig, dennoch hat das System eine entscheidende Schwäche: die Schlüssellänge ist mit einem Byte deutlich zu kurz. Sie können somit über eine vollständige Enumeration alle möglichen Schlüssel auf jeden Schlüsseltext ausprobieren und diesen probeweise entschlüsseln. Da es jedoch dennoch sehr aufwändig ist, dies manuell durchzuführen, sollen sie ein Programm implementieren, das in der Lage ist, die Entschlüsselung mit allen Schlüsseln durchzuführen und automatisiert erkennen kann, ob der entstandene Klartext sinnvoll ist. Dazu sollen Sie die Entropie des entstandenen Klartextes berechnen und mit der Entropie der deutschen Sprache vergleichen. Möglicherweise müssen Sie dazu einen Schwellwert bilden. Sie können sich zudem selbst noch weitere Texte selbst verschlüsseln und ebenfalls mit diesen arbeiten. Den TextCrypter und die drei Schlüsseltexte finden Sie unter folgender Adresse: http://www-sec.uni-regensburg.de/intern/lecturenotes/security/TextCrypter.zip

1. Erläutern Sie allgemein wie, bzw. unter welchen Voraussetzungen, bei einem solchen Brute-Force-Angriff automatisch entschieden werden kann, ob der richtige Schlüssel gefunden wurde.
2. Geben Sie eine geeignete Implementierung ab und führen Sie den Nachweis, dass Sie einen der Texte erfolgreich entschlüsselt haben (Abgabe des Anfangs eines Klartextes).
3. Um welchen Typ Angriff handelt es sich und warum? Known Plaintext-, Known Ciphertext-, Adaptively Chosen Plaintext- oder Adaptively Chosen Ciphertext-Angriff?
4. Wie stufen Sie dieses Verfahren (zu dem Ihnen keine weiteren Spezifikationen bekannt sind) in Bezug auf die gewährleistete Sicherheit ein?

Aufgabe 8.8 PGP-Verschlüsselung und -Signatur
Installieren Sie sich das Verschlüsselungsprogramm Pretty Good Privacy (PGP) oder alternativ Gnu Privacy Guard (GnuPG) und senden Sie eine *verschlüsselte* und *digital signierte* E-Mail mit Ihrem *Namen* und Ihrer *Matrikelnummer* an den Autor dieser Aufgabensammlung.

Aufgabe 8.9 Symmetrische Schlüsselverteilung
Drei Schlüsselverteilzentralen X, Y, Z sollen jeweils einen Anteil eines symmetrischen Schlüssels k der Länge l liefern. Variante 1: Jede Verteilzentrale liefert einen Teilschlüssel der Länge $l/3$. Die drei Teile werden zu k konkateniert. Variante 2: Jede Zentrale liefert einen Teilschlüssel der Länge l. Die drei Teile werden bitweise XOR verknüpft. Welche Variante ist sicherer, wenn die Teilschlüssel von X und Y kompromittiert sind? Begründen Sie Ihre Antwort!

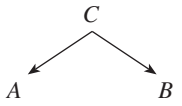
Aufgabe 8.10 Indeterministische Verschlüsselung
Beim Einsatz asymmetrischer Verschlüsselung sollte der Sender einer Nachricht diese vor der Verschlüsselung noch um (Pseudo)-Zufallszahlen ergänzen (indeterministische Verschlüsselung). Welcher Angriff kann dadurch verhindert werden?

Aufgabe 8.11 Indeterministische Verschlüsselung
Sie sollen eine indeterministische Verschlüsselung realisieren. Zur Auswahl stehen die Algorithmen RSA und ElGamal. Wie würden Sie bei beiden Algorithmen vorgehen?

9 Digitale Signatursysteme und Public-Key-Infrastrukturen

Aufgabe 9.1 Vertrauensbeziehungen in Public-Key-Infrastrukturen
Gegeben sei folgende Zertifizierungsrelation.

a)



K

$X \longrightarrow Y$ bedeutet:
X hat den öff. Schlüssel von Y zertifiziert

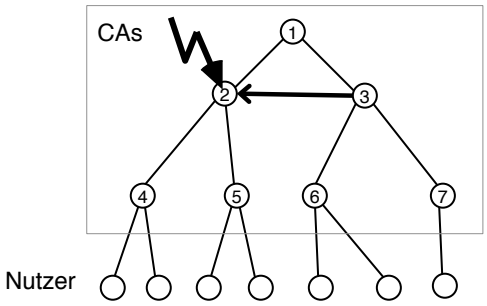
K will an A eine Nachricht M senden und ist sich jedoch lediglich sicher, dass der öffentliche Schlüssel von B authentisch ist. Unter welcher Annahme kann K der Authentizität des öffentlichen Schlüssels von A vertrauen?

Was ändert sich, wenn folgende Zertifizierungsrelation vorliegt?

b) $A \longleftarrow C \longleftarrow B$ K

Aufgabe 9.2 Cross Certification
Cross Certification ist eine Fehlertoleranzmaßnahme.

a) Welche Auswirkungen hat eine horizontale Cross Certification einer CA auf die darunterliegenden CAs und User, wenn das Zertifikat der übergeordneten CA ungültig oder zurückgerufen wird? In Abbildung 1 wird CA 2 von CA 3 zertifiziert.



b) Wie wäre es trotz des Ausfalles von CA 2 möglich, die CAs 4 und/oder 5 dennoch weiterhin/fehlertolerant an den restlichen Zertifizierungsbaum anzubinden?

Aufgabe 9.3 Verifizierung des öffentlichen Schlüssels
Der sicherheitsbewusste Karl hat den Hashwert (Fingerprint) seines öffentlichen PGP- oder S/MIME-Schlüssels auf seiner Visitenkarte abgedruckt. Damit soll es für Karls Kommunikationspartner, die von ihm persönlich die Visitenkarte erhalten haben, leicht möglich sein, die Authentizität des öffentlichen Schlüssels von Karl zu überprüfen. Wie schätzen Sie die erreichbare Sicherheit ein?

Aufgabe 9.4 Datenschutzgerechte Pseudonyme
Es ist denkbar, dass eine Zertifizierungsstelle Z den Public Key als *Pseudonym* einer ihr bekannten Person P zertifiziert. Allerdings kann die Zertifizierungsstelle dann nicht nur im Streitfall das Pseudonym aufdecken, sondern auch vollständig nachvollziehen, welche Geschäfte P gemacht hat (bzw. welche Signaturen P geleistet hat, da sie den Public Key mit der Identität von P verketten kann.

Denken Sie sich eine Variante aus, bei der eine einzige Zertifizierungsstelle hierzu nicht mehr in der Lage ist, im Streitfall aber trotzdem eine Aufdeckung des Pseudonyms möglich ist.

Aufgabe 9.5 Blinde Signaturen
Mif Hilfe digitaler Signaturen lassen sich digitale Geldmünzen realisieren. Die Bank signiert einfach die Seriennummer der digitalen Münze. Mit Hilfe sog. Blinder Signaturen (Chaum 1985) lassen sich *anonyme* digitale Geldmünzen realisieren. Überlegen Sie, welche Grundeigenschaften solche anonymen digitalen Gedmünzen aufweisen müssen.

10 Kryptographie II

Aufgabe 10.1 Hashfunktionen
Nehmen wir an, es bestehen ernste Zweifel an der Sicherheit von Hashfunktionen. Sie haben zwar mehrere zur Auswahl, wissen aber nicht für welche Sie sich entscheiden sollen. Was könnten Sie tun?

Aufgabe 10.2 Anzahl der Kollisionen einer Hashfunktion
Wieviele Kollisionen erzeugt eine kryptographisch starke kollisionsresistente Hashfunktion $y = h(x)$ mit $|X|$ Inputs und $|Y|$ Outputs? Es gilt $|X| > |Y|$.

Aufgabe 10.3 Münzwurf über das Telefon
Katrin und Emil verabreden sich für Samstag Abend am Telefon, K ist für Kino und E für Essen gehen. Sie kommen zu keiner fairen Entscheidung und wollen eine Münze werfen, um herauszufinden was sie tun. Wie muss das Protokoll aufgebaut sein, dass Betrug ausgeschlossen ist.

Aufgabe 10.4 „Mensch ärgere Dich nicht“ über das Telefon
Alice und Bob spielen leidenschaftlich gern das Brettspiel „Mensch ärgere dich nicht“. Alice macht gerade Urlaub in Alicante (Spanien), während Bob zu Hause in Bobingen geblieben ist. Davon wollen sich die beiden jedoch nicht am Spielen hindern lassen. Außer einem altmodischen Mobiltelefon (ohne Internetzugang), dem „Mensch ärgere dich nicht“-Brettspiel und einem Laptop (auch ohne Internetzugang) hat Alice nichts dabei. Bob besitzt ebenfalls ein Telefon, ein Brettspiel und einen Laptop.

1. **Protokoll.** Überlegen Sie sich ein möglichst einfaches Protokoll, mit dem die beiden eine Partie über das Telefonnetz spielen können. Welche weiteren Voraussetzungen bzw. Vereinbarungen sind hierfür nötig? Welche Spielzüge müssen im Protokoll abgebildet werden können?
2. **Würfeln über das Telefon.** Ihr Vorschlag aus Teilaufgabe 1 stößt auf wenig Akzeptanz. Alice und Bob mögen sich zwar gerne, aber bei „Mensch ärgere Dich nicht“ verstehen Sie keinen Spaß: Sie befürchten, dass beim Würfeln betrogen wird. Schlagen Sie ein Protokoll vor, bei dem keiner hinsichtlich des Würfelergebnisses schummeln kann.

Aufgabe 10.5 Informationstheoretisch sichere Verschlüsselung
Das One-Time-Pad (Vernam-Chiffre) ist ein sehr einfaches, aber infomationstheoretisch sicheres symmetrisches Verschlüsselungsverfahren: Die Klartextzeichen x_i werden einzeln XOR-verknüpft mit einer zufälligen Schlüsselfolge k_i gleicher Länge, die nur ein einziges Mal verwendet wird (Schlüsseltext $s_i = x_i \oplus k_i$ mit $i = 1, 2, \ldots$).

a) Warum darf die Schlüsselfolge nicht mehrmals verwendet werden? Überlegen Sie sich, was passieren würde, wenn der Angreifer zwei Schlüsseltexte s_1 und s_2 (oder gar noch weitere) abfangen würde, die unter dem gleichen Schlüssel $k = k_1 = k_2$ verschlüsselt wurden. Annahme: Es handelt sich um sinnvolle Klartexte.

b) Wie würden Sie die Sicherheit des Verfahrens beweisen?

c) Was erfährt der Angreifer, der den Schlüsseltext abfängt, über den Klartext?

Aufgabe 10.6 Informationstheoretisch sichere asymmetrische Verschlüsselung
Kann es informationstheoretisch sichere asymmetrische Verfahren zur Verschlüsselung (bzw. Authentikation) geben? Begründen Sie Ihre Antwort!

Aufgabe 10.7 Informationstheoretisch sichere Authentikation
Das One-Time-Pad ist ein informationstheoretisch sicheres Verschlüsselungsverfahren. Es existiert aber auch ein informationstheoretisch sicheres (symmetrisches) Verfahren zur Authentikation.

a) Welche Eigenschaft muss ein informationstheoretisch sicheres Authentikationssystem besitzen?

b) Versuchen Sie, ein solches System zu entwerfen.

c) Kann es informationstheoretisch sichere asymmetrische Verfahren zur Verschlüsselung bzw. Authentikation geben?

Aufgabe 10.8 One-Time-Pad
Ihnen sind eine Reihe verschlüsselter deutscher Substantive in die Hände gefallen. Sie gehen davon aus, dass der Urheber fahrlässigerweise alle Wörter mit dem selben One-Time-Pad byteweise verschlüsselt hat. Versuchen Sie den Schlüssel zu ermitteln, indem Sie einen geeigneten Angriff implementieren.

Hinweis: Passwort und Substantive sind ASCII-Codiert (Alphabet = A,B,C, ... ,Z)

Die Schlüsseltexte (der 6 Substantive) in Dezimalschreibweise lauten:

```
09 00 04 10
10 20 28 09
10 16 02 02
10 20 05 08
26 26 03 00
28 16 03 17
```

Aufgabe 10.9 Triple-DES
Um der Kritik des DES bezüglich seiner zu geringen Schlüssellänge von 56 Bit zu begegnen, wurde Triple-DES (3-DES) vorgeschlagen. Dabei wird mit zwei 56 Bit langen Schlüsseln k_1 und k_2 gearbeitet und beim Verschlüsseln entweder $\mathbf{E}(\mathrm{k}_1) \rightarrow \mathbf{D}(\mathrm{k}_2) \rightarrow \mathbf{E}(\mathrm{k}_1)$ (EDE-Modus) oder $\mathbf{E}(\mathrm{k}_1) \rightarrow \mathbf{E}(\mathrm{k}_2) \rightarrow \mathbf{E}(\mathrm{k}_1)$ (EEE-Modus) ausgeführt.

a) Warum begnügt man sich bei Triple-DES aus Sicherheitsgründen nicht mit zwei Verschlüsselungen? Gehen Sie von einem Known-plaintext-Angriff aus.

b) Warum wird dem EDE-Modus meist der Vorzug vor dem EEE-Modus gegeben?

c) Berechnen Sie die theoretische und die effektive Schlüssellänge des Triple-DES unter einem Known-plaintext-Angriff mit drei 56-Bit-Schlüsseln, d.h. $\mathbf{E}(\mathrm{k}_1) \rightarrow \mathbf{E}(\mathrm{k}_2) \rightarrow \mathbf{E}(\mathrm{k}_3)$.

Aufgabe 10.10 Unsicherheit des Electronic-Codebook-Modus
Eine einfache, jedoch unsichere, Technik zum Betrieb einer Blockchiffre ist der Electronic-Codebook-Modus (ECB-Modus). Dabei wird jeder Klartextblock unabhängig von den anderen Blöcken chiffriert.

a) Inwiefern stellt dies ein Sicherheitsproblem dar?

b) Demonstrieren Sie das Problem anschaulich, indem Sie ein Java-Programm schreiben, welches eine einfache Windows-Bitmap-Grafik einliest, den Bildinhalt mit dem AES-Verfahren im ECB-Modus verschlüsselt und wieder als Bitmap ausgibt. Rufen Sie zum Vergleich die Verschlüsselung noch einmal im CBC-Modus auf und vergleichen Sie die erhaltenen Resultate. Informieren Sie sich dazu über das Datenformat von BMP-Dateien und die Verwendung der Java-Cryptography-API (z.B. unter http://www.ibm.com/developerworks/java/tutorials/j-sec1/section4.html).

Aufgabe 10.11 Cipher-Block-Chaining-Betriebsmodus
Beim Cipher-Block-Chaining-Betriebsmodus wird ein Klartextblock M_i vor der Anwendung der Verschlüsselungsfunktion mit dem unmittelbar vorher erzeugten Chiffretextblock $\mathrm{C}_{\mathrm{i}-1}$ durch die XOR-Operation verknüpft. Die erzeugten Chiffretextblöcke hängen dadurch von ihren Vorgängern ab. Bei der Verschlüsselung des allerersten Klartextblocks, M_1, verwendet der Sender der Nachricht für C_0 einen von ihm gewählten Initialisierungsvektor (IV).

Gehen Sie bei der Beantwortung der folgenden Fragen davon aus, dass eine moderne Blockchiffre, z.B. AES, eingesetzt wird. Überlegen Sie sich im folgenden jeweils die Antworten auf folgende Fragen: Welche Teile des Schlüsseltextes bzw. des Klartextes verändern sich durch die Änderung beim Ver- bzw. Entschlüsseln? Inwiefern sind die Auswirkungen für die Vertraulichkeit bzw. Integrität von Bedeutung?

a) Wie unterscheiden sich zwei Schlüsseltexte, die mit demselben Schlüssel erzeugt wurden und denselben Klartext enthalten, jedoch mit unterschiedlichen IVs erzeugt wurden?

b) Wie unterscheiden sich zwei Schlüsseltexte, wenn sie sich lediglich an einer Stelle im ersten Klartextblock unterscheiden (also ein Bit gekippt wird) und ansonsten völlig identisch sind (bei gleichem IV und Schlüssel)?

c) Welche Auswirkung hat es beim Entschlüsseln, wenn durch einen Übertragungsfehler ein Bit im zweiten Schlüsseltext-Block bei der Übertragung verändert wird?

d) Welche Auswirkung hat es beim Entschlüsseln, wenn durch einen Übertragungsfehler ein Bit im Initialisierungsvektor verändert wird?

Aufgabe 10.12 Diffie-Hellman-Schlüsselaustauschprotokoll
Das Diffie-Hellman(-Merkle)-Schlüsselaustauschprotokoll (DH-Protokoll) ermöglicht es zwei Kommunikationspartnern durch den Austausch von Nachrichten über einen unsicheren Kanal einen symmetrischen Sitzungsschlüssel zu etablieren, der von passiven Angreifern nicht ermittelt werden kann.

Beim ursprünglichen DH-Protokoll, das auch als „anonymes“ DH-Protokoll bezeichnet wird, wird kein Schlüsselserver verwendet. Die Kommunikationspartner tauschen dabei erst im Moment des Schlüsselaustauschs sämtliche Protokollnachrichten über den unsicheren Kanal aus.

a) Stellen Sie den Ablauf des anonymen DH-Protokolls zwischen den beiden Teilnehmern Alice und Bob mit passend gewählten kleinen Zahlen dar.

b) Erläutern Sie, auf welcher mathematischen Annahme die Sicherheit des DH-Protokolls basiert. Welche weiteren Annahmen macht man über den Angreifer (Angreifermodell)?

c) Schutz vor aktiven Angreifern ist möglich, wenn die Kommunikationspartner einige Parameter bzw. Protokollnachrichten vorab über einen sicheren Kanal ausgetauscht haben, der vom Angreifer nicht kontrolliert werden kann. Die eigentliche Schlüsselvereinbarung erfolgt dann später über den unsicheren Kanal in Anwesenheit eines aktiven Angreifers. Welche Nachrichten müssen vorab ausgetauscht worden sein, damit aktive Angriffe verhindert werden?

Aufgabe 10.13 Hash-Funktionen bei Verschlüsselung und digitaler Signatur
Bei der Verwendung von RSA ist es sowohl beim Verschlüsselungssystem als auch beim digitalen Signatursystem empfehlenswert, eine Hash-Funktion zu verwenden. Bei Verschlüsselungssystem wird der Klartext m um ein Redundanzprädikat $\mathrm{h}(\mathrm{m})$ ergänzt, beim Signatursystem wird lediglich $\mathrm{h}(\mathrm{m})$ und nicht m mit dem privaten Schlüssel exponentiert. Beschreiben Sie die Angriffe, die dadurch abgewehrt werden.

Aufgabe 10.14 Sicherheit des RSA-Verfahrens

a) Auf welcher mathematischen Annahme basiert die Sicherheit des RSA-Verfahrens? Stellen Sie zur Erläuterung anhand eines Beispiels mit kleinen Zahlen dar, welche Informationen ein Angreifer besitzt und wie er anhand dieser Informationen eine verschlüsselte Nachricht entschlüsseln könnte, wenn die oben angesprochene Annahme nicht gelten würde.

b) Eine Schwäche des RSA-Verfahrens besteht darin, dass es deterministisch ist, d.h. es erzeugt bei einem gegebenen Schlüsselpaar aus demselben Klartextblock immer denselben Schlüsseltextblock. Daher werden Klartextnachrichten üblicherweise nicht unmittelbar mit dem RSA-Verfahren verschlüsselt, sondern zuvor mit Zufallszahlen ergänzt. Beschreiben Sie den Angriff, vor dem man sich dadurch schützt, und warum dieser bei symmetrischen Chiffren, die ja ebenfalls deterministisch sind, keine Rolle spielt.

Aufgabe 10.15 RSA
Warum kann eine mit RSA zu verschlüsselnde Nachricht m nicht gleichzeitig einen Faktor p und q enthalten?

Aufgabe 10.16 RSA-Verfahren
Das Verfahren von Rivest, Shamir und Adleman (kurz: RSA) ist eines der am weitesten verbreiteten asymmetrischen Kryptographieverfahren. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohen Aufwand aus dem öffentlichen Schlüssel berechnet werden.

1. Wie wird beim RSA-Verfahren das Schlüsselpaar erzeugt? Wie erfolgen Verschlüsselung und Entschlüsselung? Worauf basiert die unterstellte Sicherheit des RSA-Verfahrens? Was ist die häufigste Anwendungform von RSA in der Praxis?

2. Gegeben ist der folgende Schlüsseltext. Dieser wurde durch Anwendung des RSA-Verfahrens erzeugt. Dabei wurde der ASCII-Code jedes einzelnen Zeichens separat verschlüsselt. Das dabei verwendete Schlüsselpaar wurde aus folgenden (zu Anschauungszwecken verwendeten, völlig unsicheren) Basiswerten erzeugt: $\mathrm{p} = 281$, $\mathrm{q} = 389$, $e = 67$

   Ihre Aufgabe: Ermitteln Sie den zugehörigen Entschlüsselungsexponenten d und dekodieren Sie damit den gegebenen Schlüsseltext Zeichen für Zeichen. Wie lauten d und der ursprüngliche Klartext? Bitte fügen Sie Ihrer Lösung auch Ihren Quelltext hinzu, falls Sie die Aufgabe programmatisch.

   Hinweis: Viele Skriptsprachen (wie Ruby) können mit den bei der Lösung u. U. entstehenden großen Integerzahlen umgehen. Falls Sie diese Aufgabe mit Java bearbeiten wollen, sollten Sie die Klasse *BigInteger* verwenden und sich die Methode *modPow* näher ansehen.

   ```
   103625, 71396, 5872, 102989, 10232, 36843, 71765, 5872, 10232, 14809, 108822, 108822,
   69296, 32156, 36704, 105697, 71396, 25948, 71396, 102989, 10232, 25948, 71765, 64024,
   36843, 10232, 16718, 105867, 36704, 34992, 5872, 64024, 36843, 5872, 10232, 2762, 73111,
   5872, 19729, 5872, 64024, 10232, 109169, 71765, 1086, 73111, 57424, 71765, 34992, 60372,
   10232, 108822, 1086, 73111, 71396, 57424, 40412, 40412, 71765, 5872, 36704, 5872, 82037,
   10232, 86175, 64024, 34992, 102989, 5872, 71765, 16718, 5872, 102989, 19729, 105867, 36843,
   5872, 36704, 36704, 5872, 82037, 10232, 61644, 105697, 71765, 64024, 36265, 105867, 109169,
   10232, 2762, 105697, 36265, 36704, 5872, 25948, 82037, 10232, 36843, 71765, 5872, 10232,
   89982, 27255, 64024, 69296, 62098, 108822, 71765, 1086, 73111, 5872, 102989, 73111, 5872,
   71765, 57424, 10232, 61865, 105867, 64024, 10232, 35203, 105697, 25948, 25948, 109169,
   105867, 5872, 102989, 57424, 5872, 102989, 64024, 10232, 71396, 64024, 36843, 10232, 36843,
   105697, 40412, 71396, 34992, 5872, 73111, 105867, 5872, 102989, 71765, 34992, 5872, 10232,
   86175, 64024, 34992, 102989, 71765, 16718, 16718, 5872, 82037, 10232, 57837, 71396, 34992,
   105697, 64024, 34992, 25948, 69296, 10232, 71396, 64024, 36843, 10232, 57837, 71396, 34992,
   102989, 71765, 16718, 16718, 25948, 78325, 105867, 64024, 57424, 102989, 105867, 36704,
   36704, 5872, 82037, 10232, 102020, 71765, 105867, 19729, 5872, 57424, 102989, 71765, 25948,
   1086, 73111, 5872, 10232, 52356, 5872, 102989, 16718, 105697, 73111, 102989, 5872, 64024,
   82037, 10232, 2762, 71765, 19729, 71765, 64024, 34992, 69296, 86175, 57424, 57424, 105697,
   1086, 78325, 10232, 71396, 64024, 36843, 10232, 35203, 105867, 109169, 5872, 102989, 69296,
   86175, 64024, 105697, 36704, 40103, 25948, 71765, 25948, 82037, 10232, 14809, 102989,
   71396, 64024, 36843, 36704, 105697, 34992, 5872, 64024, 10232, 36843, 5872, 102989, 10232,
   32156, 102989, 40103, 108306, 57424, 105867, 34992, 102989, 105697, 108306, 73111, 71765,
   5872, 82037, 10232, 86175, 71396, 57424, 73111, 5872, 64024, 57424, 71765, 16718, 71765,
   78325, 105697, 57424, 71765, 105867, 64024, 25948, 108306, 102989, 105867, 57424, 105867,
   78325, 105867, 36704, 36704, 5872, 82037, 10232, 36843, 105697, 25948, 10232, 61644,
   108822, 86175, 69296, 52356, 5872, 102989, 16718, 105697, 73111, 102989, 5872, 64024,
   10232, 71396, 64024, 36843, 10232, 64024, 105697, 57424, 71396, 5872, 102989, 36704, 71765,
   1086, 73111, 10232, 105697, 36704, 36704, 5872, 10232, 105697, 64024, 36843, 5872, 102989,
   5872, 64024, 10232, 59390, 64024, 73111, 105697, 36704, 57424, 5872, 82037, 10232, 36843,
   71765, 5872, 10232, 109169, 71765, 102989, 10232, 71765, 64024, 10232, 36843, 5872, 102989,
   10232, 27255, 5872, 36265, 71396, 64024, 34992, 10232, 71396, 64024, 36843, 10232, 36843,
   5872, 102989, 10232, 52356, 105867, 102989, 36704, 5872, 25948, 71396, 64024, 34992, 10232,
   36265, 5872, 73111, 105697, 64024, 36843, 5872, 36704, 57424, 10232, 73111, 105697, 36265,
   5872, 64024, 10232, 60372, 69296, 62098
   ```

3. Das von Ihnen in der vorherigen Teilaufgabe verwendete (deterministische) RSA-Verfahren ist gegen eine Chosen-Plaintext-Attack anfällig. Erläutern Sie dies an einem Beispiel und stellen Sie dar, wie der Angriff durch eine kleine Erweiterung verhindert werden kann (p, q und e sollen unverändert bleiben).

Aufgabe 10.17 MFC-Komplexität

Man gebe die MFC-Komplexität der Gleichungssysteme zur Analyse des VDES für beide Fälle (S_{nlin} und S_{lin}) an.

Aufgabe 10.18 Obere Schrake der MFC-Komplexität

Die obere Schrake der MFC-Komplexität des DES ist

$$64 \cdot \sum_{\mathrm{i}=0}^{56} \binom{56}{\mathrm{i}} = 64 \cdot 2^{56} \approx 5 \cdot 10^{18}.$$

Erklären sie, wie diese Zahl zustandekommt.

Aufgabe 10.19 MFC-Komplexität des DES
Man gebe eine obere Schranke für die MFC-Komplexität des DES mit linearen S-Boxen an.

Aufgabe 10.20 Brechen des VDES mittels MFC
Es sei ein M/C-Paar $(1,0,1,1)/(1,1,1,0)$ bekannt. Als S-Box wurde S_{lin} verwendet. Man ermittle K.

11 Steganographie und Watermarking

Aufgabe 11.1 Asymmetrische Steganographie
Wie müsste ein asymmetrisches steganographisches System aufgebaut sein, obwohl bisher kein einziges konkretes Verfahren exitsiert. Was könnte ein solches System wohl so schwer realisierbar machen?

Man kann sich jedoch mit einem asymmetrischen Kryptosystem behelfen. Wie?

Aufgabe 11.2 Vertraulicher Nachrichtenaustausch nur mittels Message Authentication Codes (MACs)

Ronald Rivest gelang es 1998 während der amerikanischen Clipper-Chip-Debatte, bei der es um ein Gesetzesvorhaben zur Regulierung von Kryptographie ging, ein Verfahren zum vertraulichen Nachrichtenaustausch nur mit Hilfe von symmetrischer Authentikation (Message Authentication Codes) zu realisieren. Das Verfahren erinnert ein wenig an Steganographie. Wie könnte das Verfahren aussehen?

Aufgabe 11.3 Spread Spectrum Watermarking
Gegeben sei ein Original (bereits frequenztransformiert)

$$N(x,y) = \begin{pmatrix} 8 & 6 & 4 \\ 5 & 3 & 1 \\ 6 & 2 & 0 \end{pmatrix}.$$

Die Basisfunktionen Φ_i seien

$$\Phi_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{und} \quad \Phi_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Es soll ein Watermark b aus zwei Bit $b = (\texttt{"0"},\texttt{"1"})$ eingebettet werden.

a) Berechnen Sie $D(x,y)$ (markiertes Original). Hinweis: Die b_i werden transformiert in Werte aus $\{-1,1\}$, d.h. Ein Null-Bit wird auf -1 abgebildet, ein Eins-Bit auf 1.

b) Durch eine Störung (bzw. einen Angriff) sei die dritte Zeile von $D(x,y)$ ausgelöscht (mit Nullen belegt), d.h.

$$\tilde{D}(x,y) = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 0 & 0 & 0 \end{pmatrix}.$$

Extrahieren Sie das Watermark. Als Schwellwert wird der Mittelwert der o_i verwendet.

12 Schutz digitaler Inhalte, Kopierschutz, DRM-Systeme

Aufgabe 12.1 Inhalte auf Datenträgern
Nehmen wir an, dass von jedem Datenträger über kurz oder lang problemlos digitale Kopien der Daten angefertigt werden können.

a) Überlegen Sie sich verschiedene Möglichkeiten, wie ein Schutzsystem aussehen könnte, das die Nutzung der Inhalte nur Berechtigten (z.B. denen, die dafür bezahlt haben) erlaubt.

b) Inwieweit unterscheidet sich die Problemstellung und Ihre Lösung(en) vom Schutz vor Raubkopien in der Software-Branche?

Aufgabe 12.2 Hardwarebaustein zum Rechtemanagement
Mit dem Einsatz eines Hardwarebausteins im PC, der für seinen Besitzer nicht ausforschbar ist, und der aus Inhalteanbieter-Sicht für eine „sichere“ Systemkonfiguration sorgt, soll digitales Rechtemanagement möglich werden. Beschreiben Sie, wie der Ablauf vom Booten des PCs bis zur Nutzung des Inhalts aussehen könnte, damit keine fremde Software an die ungesicherten Mediendaten kommt.

13 Praktische Sicherheit

Aufgabe 13.1 Erstellen von Firewallregeln
Stellen Sie mit Hilfe einer Firewall (ipfw) sicher, dass ein Server www.domain.com von außen für alle Dienste außer SSH (22/tcp) und HTTP (80/tcp) unerreichbar ist und von innen nach außen nur HTTP (80/tcp) und HTTPS/SSL (443/tcp) erlaubt. (Hinweis: Eine Anleitung zur Verwendung von ipfw finden Sie im Handbuch zu FreeBSD im Kap. 28.6, siehe http://www.freebsd.org/ unter Documentation>Handbook. Dort sind auch die Regeln beschrieben.)

Aufgabe 13.2 Notwendigkeit des inneren Paketfilters
Warum ist bei einem Screened Subnet der innere Paketfilter unverzichtbar? Eigentlich werden doch vom äußeren Paketfilter sowieso schon alle Pakete geblockt, die nicht für den Bastion-Host bestimmt sind.

Aufgabe 13.3 Denial-of-Service-(DoS)-Angriff auf bzw. mittels dynamischen Paketfilter
Angenommen, ein (äußerer) Paketfilter ist kombiniert mit einem Anomalieerkennungssystem (Intrusion Detection System, IDS), das beim Verdacht auf Angriffspakete den Paketfilter dynamisch so umkonfiguriert, dass alle Pakete von dieser Source-IP-Adresse blockiert werden. Welcher DoS-Angriff ist dann denkbar?

Aufgabe 13.4 Evaluation von Intrusion Detection Systemen (IDS)
Zur Evaluation von IDS werden diese einer Anzahl $\mathrm{n_a}$ von Angriffen und $\mathrm{n_n}$ normalen Ereignissen ausgesetzt und währenddessen das Verhalten des IDS aufgezeichnet, d.h. die Anzahl erkannter Angriffe $\mathrm{n_{tp}}$ (true-positives), nicht erkannter Angriffe $\mathrm{n_{fn}}$ (false-negatives), fälschlich erkannter Angriffe $\mathrm{n_{fp}}$ (false-positives) sowie der normalen Ereignisse $\mathrm{n_{tn}}$ (true-negatives) gezählt.

a) Die resultierenden Gütekriterien sind die Erkennungsrate $\mathrm{P(n_{tp})}$ und die False-Positive-Rate $\mathrm{P(n_{fp})}$. Wie werden diese berechnet?

b) Der Verlauf von False-Positiv- und Erkennungsrate in Abhängigkeit der Empfindlichkeit des IDS wird als Receiver-Operating-Charakteristik in einem sog. ROC-Graphen dargestellt. Auf der x-Achse wird $\mathrm{P(n_{fp})}$ und auf der y-Achse $\mathrm{P(n_{tp})}$ dargestellt. Wie sieht ein typischer ROC-Graph eines IDS aus?

Aufgabe 13.5 Sniffing zur Netzanalyse
Angenommen, Sie sollen als Netzwerkadministrator die in letzter Zeit häufig aufgetretenen Abstürze eines SMTP-Servers (mail.domain.com auf TCP-Port 25) analysieren. Sie vermuten, dass ein Angreifer eine Schwäche der Protokollimplementierung des SMTP-Servers gefunden hat und ausnutzt. (Beispielsweise könnten E-Mail-Adressen, die mehr als x Zeichen lang sind, einen Buffer Overflow verursachen und den Server zum Absturz bringen.) Sie wollen nun den am Server ankommenden Verkehr mittels des Unix-Programms tcpdump analysieren. Wie muss tcpdump aufgerufen werden, um die Kommunikationsabläufe sichtbar zu machen? (Hinweis: Die manpage von tcpdump finden Sie unter http://www.tcpdump.org/.)

Aufgabe 13.6 Verdecktes Tunneling mittels DNS
Es soll ein verdeckter Kanal von außen nach innen über eine Firewall realisiert werden – beispielsweise zur Steuerung eines trojanischen Pferdes. Der Angreifer beherrscht einen (von ihm modifizierten) DNS-Server im Internet. Wie könnte er vorgehen, um das trojanische Pferd mit Kommandos zu versorgen? Skizzieren und erläutern Sie den Ablauf der verdeckten Kommunikation. Welche Kapazität besitzt der verdeckte Kanal?

Aufgabe 13.7 Tunneling mittels SSH
Sie wollen den lokalen Server-Port 25/tcp über einen SSH-Tunnel an den Port 25/tcp des Servers mail.domain.com binden. Ein SSH-Dämon und Ihr Account (misterx) läuft auf cip.domain.com. Wie lautet der entsprechende SSH-Aufruf? Von wo nach wo verläuft der (verschlüsselte) Tunnel? (Hinweis: Die manpage von ssh finden Sie unter http://www.openssh.org/.)

Aufgabe 13.8 Real-World-Brute-Force-Angriff
Ein Arbeitsbereich hat ein Upload-Tool zur Einreichung von Übungsblättern entwickelt, das unter http://svs.informatik.uni-hamburg.de/abgabe/ erreichbar ist. Nach dem Upload erhält man einen Sicherheitscode, mit dem man eine überarbeitete Fassung hochladen kann. Bei der Entwicklung war der Schutz des Systems gegen Brute-Force-Angriffe ein wichtiges Entwurfsziel. Dadurch soll verhindert werden, dass eine Übungsgruppe die Lösung einer anderen Gruppe, welche bereits etwas hochgeladen hat, einsehen kann. Dies soll durch die hohe Länge des Sicherheitscodes verhindert werden.

In dieser Aufgabe sollen Sie auf Basis Ihrer Beobachtungen des unter o. a. URL erreichbaren Systems eine möglichst genaue Abschätzung der effektiven Sicherheit des Sicherheitscodes durchführen. Ermitteln Sie dazu anhand der vom System zur Verfügung gestellten Informationen, wie lange es im Mittel mindestens dauern würde, bis Sie Zugriff auf die Lösung von mindestens einer anderen Gruppe hätten, wenn der Webserver konstant 1000 Anfragen pro Sekunde beantworten würde. Dokumentieren Sie, wo erforderlich, Ihre Annahmen.

Hinweise:

1. Bitte überlasten Sie den Server nicht mit einem Brute-Force-Angriff! Diese Aufgabe ist analytisch zu lösen.
2. Um den verwendeten Zeichenvorrat im Sicherheitscode möglichst genau abschätzen zu können, sollten Sie sich im Abgabe-Tool durch Hochladen einiger Dateien selbst eine kleine Menge (max. 20) von Sicherheitscodes erzeugen.
3. Als Ausgangspunkt für Ihre Analyse bietet es sich an, die Ratewahrscheinlichkeit für einen einzelnen Sicherheitscode zu ermitteln.

14 Mobilkommunikation

Aufgabe 14.1 Gemeinsamkeiten und Unterschiede Festnetz- und Mobilkommunikation
Nennen und erläutern Sie je zwei

a) Gemeinsamkeiten und

b) Unterschiede

von Festnetz- und Mobilkommunikation.

Aufgabe 14.2 Funkzellen
Das Versorgungsgebiet eines zellularen Funknetzes ist in sogenannte Funkzellen eingeteilt. Warum?

Aufgabe 14.3 Archtitektur von GSM

a) Skizzieren und erläutern Sie kurz die Architektur von GSM.

b) Welche der unter a) beschriebenen Systemteile sind an der Erbringung der vier in GSM integrierten Sicherheitsfunktionen beteiligt?

Aufgabe 14.4 Begriffe und Erläuterungen

a) Was ist die IMSI?

b) Was ist die MSISDN?

c) Was ist ein Authentication Triplet?

d) Was ist das AuC?

Aufgabe 14.5 Datenbanken in GSM

a) Welche (drei) Datenbanken (Register) gibt es im GSM?

b) Welchen Zweck erfüllt jede einzelne Datenbank?

c) Wo befinden sich die Datenbanken?

Aufgabe 14.6 Sicherheitsfunktionen in GSM
Erläutern Sie die vier Sicherheitsfunktionen, die in GSM-Netzen vorhanden sind. Benutzen Sie möglichst auch graphische Darstellungen, soweit sinnvoll!

Aufgabe 14.7 Allokation von Algorithmen
In welchen Systemteilen sind die folgenden Algorithmen des GSM-Netzes vorhanden? Begründen Sie jeweils die Sinnhaftigkeit dieser Allokation!

a) Algorithmus A3 (Erzeugung von SRES)

b) Algorithmus A5 (erzeugt Pseudozufallszahlenfolge aus Kc)

c) Algorithmus A8 (Erzeugung von Kc)

Aufgabe 14.8 Geheimnis Kc
Welche Netzkomponenten im GSM kennen den Verschlüsselungsschlüssel Kc?

Aufgabe 14.9 Geheimnis Ki
Im GSM wird der geheime Schlüssel Ki vom Netzbetreiber niemals weitergegeben.

a) Warum verbleibt im GSM der geheime Ki stets beim Heimatnetzbetreiber?

b) Wie überprüft der besuchte Netzbetreiber beim Roaming, ob es sich um einen berechtigten Teilnehmer handelt?

c) Gibt es im Vertrauensmodell des UMTS hinsichtlich der Geheimhaltung von K einen Unterschied zu GSM?

Aufgabe 14.10 Verbindungsverschlüsselung
Welche Kommunikationsabschnitte sind in GSM verschlüsselt? Welche Kommunikationsabschnitte sind unverschlüsselt?

Aufgabe 14.11 TMSI-Vergabe
Jeder GSM-Mobilfunkteilnehmer bekommt vom Netz eine Temporary Mobile Subscriber Identity (TMSI) zugewiesen. Was ist das Angreifermodell?

Aufgabe 14.12 Schnittstellendefinitionen

a) Warum genügt es, bei A3/A8 die Schnittstellen der Algorithmen zu standardisieren, nicht aber den Algorithmus selbst?

b) Wie verhält sich die Standardisierung beim Algorithmus zur Festlegung der TMSI? Wer muss den Algorithmus kennen? Was ist festgelegt?

c) Wie ist die Situation bei A5?

Aufgabe 14.13 Verhindern von Betrug
Wie wird im GSM verhindert, dass ein Teilnehmer auf Kosten eines anderen Teilnehmers Telefongespräche führen kann?

Aufgabe 14.14 Zusammenspiel der Sicherheitsfunktionen
Erläutern Sie anhand des Protokollablaufs (Weg-Zeit-Diagramm) eines Mobile Originated Call Setup, wie die Sicherheitsfunktionen ineinander greifen. Verwenden Sie die Instanzen Mobilstation, besuchtes Netz, Heimatnetz.

Aufgabe 14.15 Kritik an GSM
Trotz der vorhandenen Sicherheitsfunktionen bietet GSM nur beschränkte Sicherheit hinsichtlich Vertraulichkeit. Warum?

Aufgabe 14.16 IMSI-Catcher
Erläutern Sie die Arbeitsweise des IMSI-Catchers bzgl. des „Einfangens“ der IMSIs. Die Unterdrückung der Verschlüsselung soll nicht interessieren.

Aufgabe 14.17 Gegenseitige Authentifizierung für GSM
Wie könnte eine gegenseitige Authentifizierung (Netz gegenüber MS und MS gegenüber Netz) in GSM implementiert werden, um das „Einfangen“ der IMSIs durch den IMSI-Catcher zu verhindern? Machen Sie bitte wenigstens zwei Gestaltungsvorschläge und diskutieren Sie diese!

Aufgabe 14.18 UMTS-Sicherheitsfunktionen
Mit UMTS wurden die Sicherheitsfunktionen für Mobilfunknetze neu definiert.

a) Was wurde vom GSM übernommen?

b) Was wurde gegenüber GSM verbessert?

c) Welche Restprobleme bleiben?

Aufgabe 14.19 Peilungsverfahren

a) Erläutern Sie die Laufzeitpeilung und die Richtungspeilung.

b) Welches der beiden Verfahren könnte im GSM eingesetzt werden. Kurze Begründung!

Aufgabe 14.20 Bluetooth-Pairing
Bei Bluetooth erfolgt zur sicheren Gerätekopplung zunächst ein sog. Pairing, das in zwei Schritten abläuft. In Schritt 1 ist die Funktion E22 beteiligt. In Schritt 2 ist die Funktion E21 beteiligt.

a) Bitte nennen Sie die Aufgabe von Schritt 1.

b) Bitte nennen Sie die Aufgabe von Schritt 2.

d) Was sind die In- und Outputs von Schritt 1?

e) Was sind die In- und Outputs von Schritt 2?

Aufgabe 14.21 Bluetooth-Authentifikation
Bei Bluetooth wird auf Basis der Funktion E22 die Authentifikation durchgeführt. Was sind die In- und Outputs der Authentifikation?

Aufgabe 14.22 WEP
Bei der WEP-Verschlüsselung im WLAN soll durch eine Challenge-Response-Authentikation die Berechtigung des Client überprüft werden. Leider existiert eine triviale Angriffsmöglichkeit auf dieses Protokoll, die es einem unberechtigten Nutzer ermöglicht, die Authentikation zu überwinden. Bitte erklären Sie diese kurz.

Aufgabe 14.23 Broadcast
Durch Verteilung (Broadcast) von Verbindungswünschen im gesamten Versorgungsgebiet eines Kommunikationsnetzes (z.B. Mobilfunknetzes) kann auf das Speichern von Aufenthaltsdaten bzw. Routinginformation verzichtet werden.

a) Erläutern Sie den Unterschied von offenen impliziten und verdeckten impliziten Adressen.

b) Könnte man auch die explizite Adressierung verwenden, um einem mobilen Teilnehmer eine nicht notwendigerweise vertrauliche Nachricht (z.B. eine SMS) zu senden, ohne ihn lokalisieren zu können? Begründen Sie Ihre Antwort!

c) Ist bei der variablen impliziten Adressierung ein Satellit zur Verteilung einsetzbar? Begründung!

Aufgabe 14.24 Kollisionsabstand offener impliziter Adressen
Die Länge einer impliziten Adresse sei 32 Bit. Es sollen 100.000 Teilnehmer versorgt werden. Jedem Teilnehmer sind zu jedem Zeitpunkt 50 Adressen zugeordnet. Angenommen, jeder Teilnehmer erhält im Durchschnitt 1 Nachricht pro Stunde.

a) Wie groß ist der Kollisionsabstand, d.h. wie lange dauert es im Mittel, bis ein *ganz bestimmter Teilnehmer* einen Fehlalarm (Nachricht eigentlich für einen anderen Teilnehmer bestimmt) erhält?

b) Der mittlere Kollisionsabstand soll mindestens 3 Jahre betragen. Wie lang muss die offene implizite Adresse mindestens sein?

Aufgabe 14.25 TP-Methode
Die TP-Methode schützt vor der Erstellbarkeit von Bewegungsprofilen durch den Netzbetreiber.

a) Was ist ein temporäres Pseudonym?

b) Erläutern Sie den Ablauf beim Location Update!

c) Erläutern Sie den Ablauf beim Mobile Terminated Call Setup!

15 Fallstudie Timing-Angriff

Autoren: Christian Baumann, Karl-Peter Fuchs, Dominik Herrmann

Aufgabe 15.1 Timing-Attack
Ein auf einem PC installiertes Online-Banking-Programm startet erst dann, wenn der Benutzer das korrekte Passwort eingegeben hat. Das Programm sendet das eingegebene Passwort an ein Trusted Platform Module (TPM), in dem das korrekte Passwort abgelegt ist. Das TPM überprüft das eingegebene Passwort und signalisiert der Banking-Software das Ergebnis. Im TPM kommt die folgendermaßen implementierte Methode zum Einsatz.

```
boolean passwordCompare(char[] a, char[] b) {
  int i;
  if(a.length != b.length) return false;
  for(i=0; i<a.length && a[i]==b[i]; i++);
  return i == a.length;
}
```

1. Überprüfen Sie, ob diese Methode anfällig für Timing-Angriffe ist. Schreiben Sie hierzu ein kleines Java-Programm *Timer.java*, das die Laufzeit der Methode *passwordCompare* bei zwei identischen Passwörtern sowie bei zwei unterschiedlichen Passwörtern ermittelt. Verwenden Sie zur Zeitmessung die Methode *System.nanoTime()* und überlegen Sie sich, wie Sie auch auf einem schnellen PC einen signifikanten Zeitunterschied herbeiführen können. *Hinweis:* Es empfiehlt sich, den Just-in-Time-Compiler von Java zu deaktivieren, indem Sie Ihr Programm wie folgt starten: *java -Djava.compiler=NONE Timer*

2. Erläutern Sie in 1-2 Sätzen, warum hier ein Timing-Angriff möglich ist.

3. Wie geht der Angreifer beim Timing-Angriff konkret vor, um das im TPM hinterlegte Passwort mit möglichst wenig Versuchen zu ermitteln, d. h. welche Passwörter probiert er der Reihe nach aus und wie entscheidet er, welches Passwort er als nächstes probiert?

4. Ändern Sie den Quellcode der Methode *passwordCompare* so ab, dass keine Timing-Attacks mehr möglich sind. Achten Sie auf möglichst kurzen und übersichtlichen Code.

5. Exkurs für Linux- bzw. C-Liebhaber: Auf der Seite http://www.informatik.uni-hamburg.de/SVS/teaching/gss.shtml finden Sie eine übersetzte Programmbibliothek (64 bit, POSIX C), die die Funktionalität des TPMs kapselt. Darin ist das geheime Passwort (in verschlüsselter Form) sowie eine Funktion zum Passwort-Vergleich enthalten. Finden Sie dieses Passwort (Zeichenvorrat: A-Z, a-z, 0-9 sowie alle auf einer deutschen Tastatur erreichbaren Sonderzeichen) mittels eines Timing-Angriffs heraus. Um den Angriff umzusetzen, müssen Sie die gegebene Bibliothek gegen ein selbst zu schreibendes C-Programm linken. Die Passwort-Vergleich-Funktion heißt *password_compare(const char *password)*. Sie ähnelt dem oben gegebenen Java-Code. Für die Zeitmessung hat sich *time.h* bewährt. Wenn Sie weitere Angriffsmöglichkeiten finden, können Sie diese gerne in Ihrer Lösung beschreiben.

16 Fallstudie Parkhaus

Autor: Florian Scheuer

In dem kostenpflichtigen Parkhaus eines großen Einkaufszentrums kommt das neue System *iPark secure* zum Erheben der Parkgebühren zum Einsatz. Dieses gibt beim Einfahren in das Parkhaus an einer Schranke Parktickets aus Karton aus, auf die Barcodes aufgebracht werden. Vor dem Wegfahren ist an einem Kassenautomat die Parkgebühr zu entrichten (sie wird mit Hilfe der ausgegebenen Karte ermittelt) und die Schranke bei der Ausfahrt öffnet nur innerhalb einiger Minuten nach dem Bezahlen. Neben einer Vielzahl von Läden gibt es in dem Einkaufszentrum jedoch zwei Unternehmen, welche ihren Kunden besondere Parkkonditionen einräumen möchten: Ein Geschäft ermöglicht es, nach dem Einkauf die Karte besonders markieren zu lassen (dazu später mehr), damit Kunden 90 Minuten lang kostenfrei parken können, ein angeschlossenes Kino erlaubt es Besuchern (ebenfalls durch Markierung der Parkkarte) mehrere Stunden für pauschal 2,50 EUR das Fahrzeug im Parkhaus unterzustellen.

Aufgabe 16.1 Funktionsweise
Sie verfügen über acht bereits verwendete Parktickets (Abbildung 1). Die beiden rechten Barcodes werden bereits bei der Einfahrt in das Parkhaus aufgedruckt. Der dritte Code von rechts wird nach dem Bezahlvorgang durch den Kassenautomat hinzugefügt, ebenso wie die menschenlesbaren Informationen in der Ecke links unten. Hat man das Kino oder das Geschäft mit den vergünstigten Parkkonditionen besucht, so wird dort noch jeweils ganz links ein Barcode aufgebracht (dieser ist nicht auf allen Tickets vorhanden).

1. Untersuchen und vergleichen Sie die Parktickets und versuchen Sie zu verstehen, wie das System arbeitet. Wie funktioniert es, welche Daten werden vermutlich wie übermittelt und warum wurde es auf diese Art ausgestaltet?
2. Offenbart das System Schwächen? Welches Angreifermodell liegt dem System zu Grunde?

Aufgabe 16.2 Betrugsverhinderung
Nehmen Sie im Folgenden an, dass es nicht möglich ist, Daten zwischen den Komponenten des Systems auf einem anderen Weg als auf dem Ticket zu übermitteln. Wie würden Sie das System mit dem Einsatz von Kryptographie nun gestalten, um Betrug effektiv zu verhindern? Beschreiben Sie Ihr Parksystem im Detail, auch gerne unter Zuhilfenahme einer Abbildung, und begründen Sie Ihre Entscheidungen.

Aufgabe 16.3 Flatrate
Da der Betreiber des Parkhauses inzwischen in mehreren Städten das *iPSec*-System erfolgreich einsetzt, plant er eine Erweiterung: Er möchte eine Flatrate anbieten, die es Dauerparkern erlaubt, alle Parkhäuser beliebig oft und lange innerhalb eines Jahres für einen Pauschalbetrag zu nutzen. Das Ticket soll auch in diesem Fall aus Karton bestehen und Informationen in Form eines (oder mehrerer) Barcodes transportieren.

Welche zwei grundsätzlichen Möglichkeiten gibt es, dieses System sicher zu gestalten? Beschreiben Sie diese kurz und gehen sie auf die jeweiligen Vor- und Nachteile ein.

Abbildung 1: Parktickets

17 Fallstudie lundi-tec

Autoren: Christoph Gerber, Dominik Herrmann, Klaus Plößl

In dieser Fallstudie wird das fiktive Unternehmen lundi-tec GmbH beschrieben, das eine Unternehmensberatung engagiert, um das IT-Grundschutz-Vorgehensmodell anzuwenden. Sie befinden sich in der Rolle des Beraters, der sich lediglich um einen kleinen Teil des Unternehmens kümmern soll. Die Fallstudie soll am konkreten Beispiel verdeutlichen, welche Schritte im einzelnen durchzuführen sind und welchen Aufwand diese verursachen. Die Bearbeitung der Fallstudie soll ferner den Umgang mit den Grundschutzkatalogen schulen und einen groben Überblick über die verschiedenen Bausteine und Maßnahmen geben. Abschließend stehen Sie vor der Herausforderung, einen konkreten Umsetzungsplan für die einzelnen Maßnahmen zu erstellen, der eine Reihe von Nebenbedingungen erfüllt.

Disclaimer: Alle in dieser Fallstudie beschriebenen Organisationen und Personen sind fiktiv. Jede Ähnlichkeit mit lebenden oder toten Personen ist zufällig und nicht beabsichtigt. Die genannten Aufwandsschätzungen sind ebenfalls fiktive Zahlen, die nicht ohne weiteres auf die Realität übertragbar sind. Diese Fallstudie dient ausschließlich als Begleitmaterial zur Vorlesung und ist nicht zur Veröffentlichung konzipiert.

17.1 Einleitung

Die lundi-tec GmbH ist ein Unternehmen mittlerer Größe, das chemische Zwischenprodukte für die Erstellung einer Vielzahl dem Endanwender unter anderen Handelsnamen bekannten Produkten produziert. Das Unternehmen wurde 1988 von den zwei erfahrenen Chemikern Dr. Michael Reiter und Christoph Taller gegründet, die sich mit einer selbstentwickelten Verfahrenstechnik selbständig machen wollten. Mit ihrem innovativen Produktionsverfahren waren die beiden äußerst erfolgreich – der Konkurrenz immer einen Schritt voraus. Seit der Gründung sind nun 20 Jahre vergangen. Mittlerweile sind bei lundi-tec knapp 300 Mitarbeiter an zwei Standorten in Oberbayern beschäftigt, die einen Gesamtumsatz von 155 Millionen Euro und rund 3,5 Millionen Euro Gewinn erwirtschaften.

Die jüngsten Entwicklungen auf den internationalen Finanzmärkten hatten in den letzten Monaten für hitzige Diskussionen in der Chefetage gesorgt. Dabei prallten zwei fundamental unterschiedliche Ansichten aufeinander: Die Gründer der lundi-tec, die sich heute nur noch als Gesellschafter in das Unternehmen einbringen, sind relativ konservativ orientiert und blicken angesichts der drohenden abnehmenden Nachfrage mit Sorge in die Zukunft. Der junge, dynamische und aufstrebende Geschäftsführer Dr. André Färber möchte hingegen die günstige Gelegenheit nutzen, um neue Absatzmärkte zu erschließen. Er vertritt die Position, dass lundi-tec eine neue Fililale eröffnen sollte, am besten in einem Wachstumsmarkt wie Asien. Die Auseinandersetzung zwischen Gesellschaftern und Geschäftsführung endete im Sommer 2008 mit einem Kompromiss. Statt in Asien wurde die Filiale – sozusagen als Testballon für die Expansion – im vertrauteren Italien eröffnet. Von dort aus soll der südeuropäische Markt bedient werden. Die Einrichtung der IT-Infrastruktur und die Anbindung der neuen Filiale an die Zentrale wurden von einem ortsansässigen IT-Systemhaus in Zusammenarbeit mit der IT-Abteilung durchgeführt. Die Filiale hat im Juli 2008 den Betrieb aufgenommen und schon erste Kunden akquiriert.

Gleichzeitig ist lundi-tec mit einer weiteren Herausforderung konfrontiert: Ein wichtiger Kunde von lundi-tec, eine große Handelskette, wurde durch die zahlreichen Datenschutzskandale in den letzten 12 Monaten aufgeschreckt. Man fürchtet, dass sensitive Informationen über die Geschäftsbeziehung sowie den Ursprung der verschiedenen (oftmals konkurrierenden) Handelsmarken an die Öffentlichkeit gelangen könnten. Eine Fortsetzung der Geschäftsbeziehung koppelt die Handelskette daher an die Voraussetzung, dass lundi-tec innerhalb von vier Jahren eine Zertifizierung nach IT-Grundschutz durchführt.

Während die Zertifizierung in der Zentrale bereits bei Aufbaustufe B angelangt ist, wurden für den neuen Standort noch keine Maßnahmen im Hinblick auf die Zertifizierung ergriffen. Der Konzeptionsauftrag für die neue Filiale wird an eine renommierte Unternehmensberatung – Ihren Arbeitgeber – vergeben. Ihre Firma entsendet zwei Projektteams mit jeweils drei Beratern, die sich unterschiedlichen Fragestellungen widmen werden, ADRIA-UNO, das lundi-tec bei der Absicherung des neuen Unternehmensstandorts durch die Anwendung der Vorgehensweise nach IT-Grundschutz unterstützen soll sowie ADRIA-DUE, das die gesamte IT-Infrastruktur im Unternehmen unter Sicherheitsaspekten untersuchen soll, um Synergien und Konsolidierungspotentiale zu identifizieren. Sie sind Teil des Projektteams ADRIA-UNO: Unterstützen Sie lundi-tec bei der Absicherung des neuen Unternehmensstandorts nach IT-Grundschutz und sichern Sie die Zukunft der Firma!

Im August 2008 treffen Sie sich zum ersten Mal mit dem Geschäftsführer Dr. Färber, den beiden Gesellschaftern sowie dem Vorsitzenden des Betriebsrats, Herrn Axel Olevsky, in einem Kick-Off-Workshop. Sie vereinbaren, dass Sie einen Projekttag in der Zentrale verbringen werden und sich am zweiten und dritten Tag in der neuen Filiale umsehen werden, um Daten für die Sicherheitskonzeption für den neuen Standort zu sammeln.

17.2 Tag 1

Ende August treffen Sie sich in Ingolstadt mit Dr. Färber. Er erklärt Ihnen zunächst den Aufbau des Unternehmens. Die Produktion, der Sitz der IT-Abteilung sowie Forschung, Entwicklung, Qualitätskontrolle und ein Lager befinden sich am Standort Ingolstadt I. Die Geschäftsleitung sowie Buchhaltung, Einkauf und Vertrieb befinden sich am Standort Ingolstadt II. Dr. Färber gibt Ihnen den bereinigten Netzplan (vgl. Abbildung 5) für die beiden Standorte mit. Dieser Plan wurde zuletzt vor knapp einem Jahr aktualisiert, als das Unternehmen (bzw. die Zentrale) erfolgreich das Auditor-Testat Aufbaustufe B nach ISO 27001 erwarb. Im Anschluss daran findet eine Betriebsbegehung statt und Sie erhalten die Möglichkeit, sich mit den Mitarbeitern in Ingolstadt zu unterhalten, um einen besseren Einblick in die Firmenphilosophie zu erhalten sowie sich die verschiedenen internen Anwendungen erläutern zu lassen.

Schließlich treffen Sie sich wieder mit Dr. Färber, um über den neuen Standort zu sprechen. Als Standort für die neue Filiale hat die Unternehmensleitung Triest in Italien ausgewählt. Er zeigt Ihnen einen Gebäudeplan. lundi-tec hat die 2. Etage eines Bürogebäudes angemietet, in der 15 teilweise neu eingestellte Mitarbeiter modern eingerichtete Arbeitsplätze vorfinden. lundi-tec belegt dort die Räume R1.03 bis R1.07 als Vertriebsbüros sowie R1.08 bis R1.09 als Labors für die Qualitätskontrolle (u. a. bei Reklamationen).

Sie wundern sich, wieso in Triest separate Labors eingerichtet werden – es sind doch bereits ausreichende Laborkapazitäten in Ingolstadt vorhanden. Auf Ihre Frage nach dem Sinn dieser Redundanz erläutert Dr. Färber, dass Qualität eine Kernkompetenz von lundi-tec sei, an die hohe Anforderungen gestellt würden. Die Qualitätsprüfung müsse schnell und zuverlässig erfolgen, da die chemischen Substanzen, die zu einer Verunreinigung in den Hauptprodukten führen, mitunter sehr schnell zerfielen. Diese chemische Reaktion sei natürlich absolut ungefährlich. Um der firmeneigenen Auffassung von Qualität gerecht zu werden, habe man sich jedoch dafür entschieden, in Triest ein eigenes Labor aufzubauen. Die Kosten amortisierten sich durch die eingesparten Transportkosten ohnehin über die Zeit.

Schließlich fährt Dr. Färber mit dem Überblick über die Infrastruktur in Triest fort. Die absperrbaren Räume R1.01 (Technikraum) und R1.02 (Serverraum) sind vom normalen Bürobetrieb ausgenommen. Der Meetingraum R1.10 enthält lediglich ein Telefon sowie einen festinstallierten Beamer für Präsentationen.

Die Vertriebsmitarbeiter haben jeweils einen Windows-XP-Client (Professional) in ihrem Büro stehen, der mit einem Switch im Raum 1.02 verbunden ist. Die Windows-2000-Clients des Labors sind in der gleichen Weise an das Netzwerk angebunden. An diesen Switch sind weiterhin zwei Server angeschlossen. Der *Triest-Server* sowie der *Labor-Server*. Der Triest-Server wird primär als Kommunikationsserver (E-Mails, Terminkalender) und Datei- und Druckserver verwendet. Der Labor-Server stellt die Analyse-Datenbank für die Laboranwendungen bereit.

Sie erkundigen sich nach der Einrichtungsvariante der Server. Da Dr. Färber keine Details über die EDV-Installation kennt, ruft er Guido Winkler, den Leiter der IT-Abteilung von lundi-tec an, und bittet ihn, ebenfalls an der Besprechung teilzunehmen. Herr Winkler erläutert kurz darauf, dass auf beiden Servern Windows-2003-Server läuft und diese als Domain-Controller mit Active-Directory fungieren. Die Server übernehmen damit Benutzerauthentisierung für das Triest-Netz unabhängig von der Zentrale.

Die Clients werden vom jeweiligen Fachpersonal bedient, für die Administration ist Felix Zimmermann als IT-Systemadministrator am Standort Triest zuständig. Da für die Administration der Laboranwendungen zusätzliches Fachwissen benötigt wird, ist Herr Zimmermann nur für den Triest-Server zuständig. Der Labor-Server wird von einem besonders geschulten Labor-Mitarbeiter, Enrico Gallo, administriert. Neben dem Triest-Server verwaltet Herr Zimmermann auch die Firewall und den Router, welche mit einem Unix-Betriebssystem arbeiten.

Auf den Vertriebsclients werden lediglich klassische Office-Anwendungen eingesetzt. Auf den Labor-Clients ist zusätzlich noch eine Spezialsoftware installiert, die zur Ansteuerung der Labormessgeräte dient und die gemessenen Daten effizient mit der Datenbank auf dem Labor-Server abgleicht. Vertriebs- und Labor-Clients hängen am zentralen Switch und kommen über eine Firewall und einen Router ins Internet.

Der Internetzugang wird durch eine DSL-Anbindung mit 16 Megabit realisiert. Zur Absicherung hängt zwischen Router und Firewall ein Application-Gateway (Proxy-Server). Dabei handelt es sich um einen Internet-Content-Filter, der den HTTP-Datenverkehr filtert. Für ausgewählte Protokolle existieren weiterhin Firewall-Regeln, die ausgehenden Datenverkehr zulassen.

17.3 Tag 2

Sie reisen nach Triest, um sich die Gegebenheiten vor Ort anzusehen. Am ersten Tag des Aufenthalts besuchen Sie mit Herrn Winkler den neuen Standort Triest, um sich vor Ort ein Bild von der implementierten IT-Infrastruktur zu machen. In einem Rundgang mit ihm und dem lokalen Systemadministrator Felix Zimmermann verschaffen Sie sich zunächst einen Überblick.

Da die Filiale in Triest bisher nicht direkt an das Firmennetz in Ingolstadt angeschlossen ist, ist sie in hohem Maße von anderen Informationskanälen wie Telefon, Fax oder E-Mail abhängig. Dieser Umstand ist in mehrerlei Hinsicht problematisch. Hin und wieder kommt es zum Beispiel vor, dass Kunden direkt bei Vertriebsmitarbeitern in Triest per E-Mail bestellen. E-Mail-Bestellungen werden wegen der fehlenden Authentizität von der Geschäftsführung jedoch nicht akzeptiert. Der vorgesehene Bestellweg ist das internationale Bestellinterface auf der lundi-tec-Webseite, die in Ingolstadt gehostet wird. Da viele Kunden jedoch den persönlichen Kontakt zu ihren Ansprechpartnern schätzen, ließen sich nicht alle Kunden dazu überreden, das Bestellinterface zu verwenden. Für die Mitarbeiter des Vertriebs ist es daher besonders wichtig, schnell und angemessen auf E-Mails von Kunden reagieren zu können. Daher stellen Sie besondere Anforderungen an die E-Mail-Anwendung in Bezug auf die Verfügbarkeit.

Jeden Tag gehen etwa 20-30 E-Mail-Bestellungen ein. Die Vertriebsmitarbeiter tragen diese dann von Hand in das Bestellinterface ein. Die Kunden müssen ihre Bestellungen dann noch einmal per Fax oder Post bestätigen, um die Authentizität sicherzustellen. Auf Ihre Frage, warum man die Filiale nicht an die zentrale S/MIME-Zertifikatsinfrastruktur, die in der Zentrale etabliert wurde, anschließe, wirft Herr Zimmermann Herrn Winkler einen vorwurfsvollen Blick zu… Sie wechseln das Thema und fragen nach dem Reklamationsprozess.

Der Reklamationsprozess ist noch viel komplizierter. Ihnen wird Frau Ilenia Nucci vorgestellt, die gerade im Vertrieb angefangen hat und sich primär um Reklamationen kümmert. Sie klagt Ihnen ihr Leid: Der Arbeitsablauf bei der Reklamation sei für sie viel zu umständlich. Auf ihrem Rechner laufe eine selbst programmierte Anwendung, in der die Reklamation erfasst werde. Die Daten der einzelnen Reklamation würden dann ausgedruckt und per Fax an die Zentrale geschickt. Dort würde ihr Kollege, ein Herr Tröster, den Sie nur vom Telefon kenne, die Reklamationen dann in der zentralen Reklamationsdatenbank erfassen. Herr Winkler erklärt, dass man bereits an einer Verbesserung des Prozesses arbeite. Statt dem Ausdruck solle der Export der Reklamationsdaten einmal am Tag in elektronischer Form durchgeführt werden. Die Export-Datei müsse dann nur auf CD gebrannt werden und per Datenträger-Spezialversand direkt nach Ingolstadt geschickt werden, wo alle Transaktionen auf einmal in die zentrale Reklamationsdatenbank importiert werden könnten. Derzeit sei man noch auf der Suche nach einem geeigneten Versanddienstleister.

Zur Verwaltung der Termine der Vertriebsmitarbeiter wird in Triest ein gängiges, kommerzielles CSCW-Werkzeug[1] eingesetzt. Die Mitarbeiter haben die Möglichkeit, zu erkennen, wann ihre Kollegen einen Termin für eine Besprechung oder ein Verkaufsgespräch frei haben. Wegen der noch überschaubaren Größe des Standortes wird dieser Dienst jedoch noch wenig genutzt. Oft werden solche Absprachen der Einfachheit halber auf dem Gang getroffen.

Der Benutzerauthentifizierung kommt in Triest eine zentrale Bedeutung zu. Die einzelnen Clients melden sich beim Start am Domain-Controller an, auf dem Passwörter der Benutzer verschlüsselt hinterlegt sind. Fällt der Domain-Controller aus, so kann kein Benutzer mehr zentrale Dienste zur Erledigung seiner Arbeit verwenden. Darunter fällt der Zugriff auf sein Home-Laufwerk. Er kann dann lediglich die Netzwerkdrucker sowie den Internetzugang nutzen. Immerhin ist der Laborbetrieb nicht beeinträchtigt, wenn die Benutzerauthentifizierung auf dem Triest-Server ausfällt (und umgekehrt). Herr Winkler erläutert, dass ein Ausfall der Benutzerauthentifizierung von maximal 12 Stunden gerade noch tolerierbar sei.

Eine weitere Anwendung, die in Triest aus Bequemlichkeit gerne benutzt wird, ist die zentrale Dokumentenverwaltung. Die Dokumente auf diesem System werden allen Mitarbeiten zur Verfügung gestellt. Die Mitarbeiter wissen es zu schätzen, dass sie mit dieser Anwendung auf eine Vielzahl von vorgefertigten, firmenspezifischen Formularen auf einfache Weise zugreifen können. Die ausgefüllten Dokumente speichern sie oft in Kopie auf ihrem Home-Laufwerk sowie manchmal auch auf ihrem Arbeitsplatz-Rechner lokal ab.

[1] CSCW – Computer Supported Cooperative Work

Alle Mitarbeiter der Filiale haben die Möglichkeit Daten, auf den zentralen Netzwerkdruckern zu drucken. Hierzu stehen zwei Geräte bereit: Ein Schwarzweiß-DIN-A4-Laserdrucker und ein DIN-A3-Farblaserdrucker. Größere Formate werden in Triest nicht benötigt. Es ist nicht damit zu rechnen, dass Dokumente mit vertraulichen Inhalten auf den zentralen Druckern ausgedruckt werden; Arbeitsplätze die darauf angewiesen sind, sind mit eigenen lokalen Druckern bestückt.

Von besonderer Bedeutung ist die Laboranwendung, die auf den Labor-Clients läuft und auf den Labor-Server zugreift. Bei der Einrichtung der Filiale wurde die Qualko-Datenbank aus Ingolstadt einmalig kopiert. In Triest liegen damit die Daten aus acht Jahren Qualitätskontrolle. In diesen Daten steckt ein Großteil des Firmen-Know-Hows. Ferner sind in der Datenbank auch Einstellungen für die einzelnen Labormessgeräte hinterlegt.

Sie sprechen mit Herrn Paolo Lori, der die Laboreinrichtung betreut. Er erläutert Ihnen, dass eine falsche Konfiguration der Messgeräte bei der Probe eines chemischen Stoffes zur Beschädigung der mitunter sehr teuren Laborausstattung führen kann. Sie fragen Herrn Lori, wie schlimm so ein Ausfall eines Messgeräts sei. Er erinnert sich, dass die Kollegen in Ingolstadt erzählt haben, dass zu untersuchende Proben bei sachgemäßer Lagerung (in Spezial-Kühleinrichtungen) bis zu drei Tagen aufbewahrt werden können, ohne die Messergebnisse signifikant zu verfälschen.

Die Mitarbeiter des Vetriebs verwenden in Kombination mit der zentralen Dokumentenverwaltung ein kommerzielles Office-Produkt zur Datenverarbeitung. Es ist schon öfter vorgekommen, dass die Office-Software fehlerhaft reagiert, was zu unangenehmen Datenverlusten führte. Ein Ausfall der Office-Anwendungen von bis zu einer Woche kann jedoch hingenommen werden. Im Notfall kann ein Ersatzgerät zum Einsatz kommen, auf dem die Anwendungen keine Fehler hervorrufen.

Wie schon angedeutet haben die Nutzer auf allen Clients die Möglichkeit, das Internet im Rahmen ihrer beruflichen Tätigkeit zu verwenden. Gerade für die Mitarbeiter des Vertriebs ist dies für ihr Tagesgeschäft unerlässlich. Ein Ausfall von mehr als 24h kann hier keinesfalls toleriert werden. Die Mitarbeiter sind angewiesen, keine vertraulichen Informationen über unsichere Informationskanäle zu versenden. Erhöhte Anforderungen an die Vertraulichkeit sind hier also nicht gegeben.

Beim Internet-Content-Filter setzt lundi-tec seit langer Zeit auf ein weit verbreitetes Open-Source-Produkt, das auch am neuen Standort zum Einsatz kommt. Die Konfigurationsdateien dieser Anwendung bedürfen eines besonderen Schutzes, da eine falsche, oder unabsichtlich geänderte Konfiguration hier beträchtlichen Schaden auslösen kann, zum Beispiel wenn ein Mitarbeiter in der Arbeitszeit Seiten mit kinderpornographischen Inhalten oder Raubkopien besuchen würde – der Image-Schaden im Fall des öffentlichen Bekanntwerdens wäre beträchtlich. Ein Ausfall dieser Anwendung hat ferner zur Folge, dass alle Mitarbeiter in Triest das Internet nicht benutzen können. In ähnlicher Weise gelten diese Anforderungen natürlich auch für das Application-Gateway, einem Proxy-Server, der einzelnen ausgewählten Anwendungen, Zugriff zum Internet gestattet, um Filesharing und andere unerwünschte Aktivitäten zu unterbinden.

17.4 Tag 3

Am dritten Tag versuchen Sie mit Hilfe von Interviews den Ist-Zustand der IT-Sicherheit-Infrastruktur und -Prozesse zu ermitteln. Auf dem Rückflug nach München lassen Sie die gesammelten Eindrücke Revue passieren und hören sich noch einmal Audio-Aufzeichnungen der beiden Interviews an.

Als erstes haben Sie mit Aida Lucciano, die eine der fünf Mitarbeiter im Vertrieb ist, gesprochen. Durch das Interview haben Sie einen realistischen Eindruck von der IT-Umgebung aus Benutzersicht bekommen (vgl. Abbildung 2).

Am Nachmittag hatten Sie dann noch einen Gesprächstermin bei Herrn Zimmerman, dem Systemadministrator in Triest (vgl. Abbildung 3). Er hat Ihnen Antworten auf eine Reihe von wichtigen Detailfragen gegeben, die für die Beurteilung der aktuellen Situation relevant sind.

Am Ende des Tages haben Sie dann noch einmal mit Herrn Winkler gesprochen. Sie konnten ihn beruhigen: Im Großen und Ganzen steht es um die IT-Sicherheit in Triest gar nicht schlecht. Auf einem Notizzettel (vgl. Abbildung 4) haben Sie Herrn Winkler noch während des Gesprächs die wichtigsten Punkte aufgeschrieben, die Ihnen beim Rundgang aufgefallen waren. Außerdem sagten Sie ihm zu, die Gesprächsnotizen für die geführten Interviews in Kürze auszuwerten und ihm eine Zusammenfassung aller sich daraus ergebenden Problemfelder per E-Mail zu schicken, bevor Sie dann in zwei Wochen der Geschäftsleitung Ihren Abschlussbericht vorlegen würden.

Sie: Frau Lucciano, mein Name ist Thomas Schmitt. Zusammen mit meinen Kollegen werden wir die IT-Sicherheit in dieser Filiale analysieren. Das ganze ist Teil des Projekts ADRIA-UNO, von dem Sie vielleicht schon einmal gehört haben.
Aida: Ah, das ADRIA-Projekt. Ja, Herr Winkler hat Sie angekündigt.
Sie: Na wunderbar. Ich fange gleich einmal an. Könnten Sie mir bitte kurz erklären, was die ersten Schritte sind, die Sie jeden Morgen durchführen, wenn Sie ins Büro kommen?
Aida: Ich fahre meinen Rechner hoch und melde mich dann an. Dann schaue ich erst einmal nach neuen E-Mails und bearbeite die Aufträge in der Wiedervorlage.
Sie: Wie funktioniert die Anmeldung? Mit Benutzername und Passwort?
Aida: Ja, ganz genau. Ich melde mich einfach mit *a.lucciano* und *sangiusto* an.
Sie: Äh, . . . das klingt ja wirklich einfach. . . Wissen Sie, ob Sie sich an einer Domäne anmelden oder nur am lokalen Rechner?
Aida: Nein, keine Ahnung.
Sie: Macht nichts. Können Sie sich mit ihrem Nutzer an anderen Rechnern anmelden?
Aida: Nein, ich kann mich nur an meinem eigenen Rechner anmelden. Aber selbst das ging erst, als Herr Zimmermann, unser Systemadministrator, den Benutzer auf meinem Rechner eingerichtet hat.
Sie: Verstehe. Also wahrscheinlich keine Domänenanmeldung. Wo liegen denn Ihre Dateien? Auf dem eigenen Rechner oder auf dem Netzwerkserver?
Aida: Die liegen hier unter Eigene Dateien, sehen Sie! Das ist auf Laufwerk C
Sie: Aha, verstehe, so wurde das also bei Ihnen eingerichtet. Ist das bei den anderen Nutzern auch so?
Aida: Das weiß ich jetzt wirklich nicht. Das müssen Sie schon Herrn Zimmermann fragen.
Sie: Was machen Sie, wenn Sie eine Kaffeepause machen?
Aida: Dann sperre ich meinen Computer und schalte den Monitor aus.
Sie: Und was passiert, falls Sie das einmal vergessen?
Aida: Mhhh, ich glaube dann kommt irgendwann der Bildschirmschoner.
Sie: Und Sie müssen zum Weiterarbeiten Ihr Passwort eingeben?
Aida: Nein, das glaube ich nicht. Das Passwort muss ich nur beim Einschalten eingeben.
Sie: Und wenn Sie den Computer gesperrt haben zum Entsperren?
Aida: Kann schon sein, ja. Wissen Sie, ich habe nicht Computer studiert wie Sie, ich kenne mich da nicht so aus.
Sie: Kein Problem. Was ist denn das für ein kleines Loch in Ihrem Display?
Aida: Ich glaube das ist ein Mikrofon.
Sie: Ist das angeschlossen? Haben Sie das schon einmal verwendet? Für Videokonferenzen oder sowas ähnliches?
Aida: Angeschlossen ist es, aber Videokonferenzen können wir hier nicht machen, weil unsere Internetanbindung dafür angeblich nicht kompatibel genug ist. Wir telefonieren aber jede Woche einmal mit den Kollegen in Ingolstadt.
Sie: Sie brauchen das Mikrofon also eigentlich gar nicht?
Aida: Nein, bisher nicht.
Sie: So, sehen wir mal weiter. Ich sehe, in Ihrem Rechner ist ein CD-Laufwerk eingebaut. Haben Sie schon einmal eine CD eingelegt?
Aida: Ja, natürlich. Wir bekommen jeden Monat mit der Post eine CD mit dem neuesten Preislisten aus der Zentrale.
Sie: Sie installieren das Preislisten-Update selber? Macht das nicht Herr Zimmermann?
Aida: Nein, das ist ja ganz einfach. Damit behelligen wir ihn gar nicht. Ich muss nur die aktuelle CD einlegen und kurz warten. Der Rest passiert irgendwie von alleine. Das hat bisher eigentlich immer ganz gut funktioniert. Das macht der Herr Tüllich. Herr Tüllich ist unser Ansprechpartner in der Zentrale, der immer die CDs verschickt.
Sie: In Ordnung, ich habe mir das mal notiert. Haben Sie eigentlich eine Schulung für IT-Sicherheit für Windows erhalten als Sie hier angefangen haben?
Aida: Nein, bisher nicht.
Sie: Wissen Sie, ob so etwas geplant ist?
Aida: Keine Ahnung. Da müssen Sie Herrn Zimmermann fragen.
Sie: Ah, verstehe. Ich habe gleich im Anschluss daran ein Gespräch mit ihm. Eine letzte Frage hätte ich noch. Dürfte ich einen Blick in ihren Papierkorb werfen?
Aida: Sie meinen den auf dem Desktop?
Sie: Ja, ganz genau. . . Oh, der ist aber ganz schön voll. Wann haben Sie den denn zuletzt geleert?
Aida: Daran kann ich mich nicht mehr erinnern. Vielleicht vor 2 Wochen. Ist das schlimm?
Sie: Sie sollten den Papierkorb wirklich öfter leeren, so wie das aussieht, liegen da ja noch ein paar Angebote drin, die man vielleicht nicht bis in alle Ewigkeit aufheben will. So, ich denke für's Erste reicht mir das schon.
Aida: Das ging ja schnell. Wenn Sie noch etwas brauchen, können Sie sich ja bei mir melden.
Sie: Vielen Dank für das Angebot. Schönen Tag noch.

Abbildung 2: Interview mit Aida Lucciano

Sie: Hallo Herr Zimmermann, wie Sie schon wissen bin ich im Rahmen des Projekts ADRIA-UNO hier, um die IT-Sicherheit an Ihrem Standort zu erheben.
Felix: Jaja, ich hab' schon gehört, dass sie uns irgendwann jemand schicken werden. Sie sind das also. Und was wollen Sie von mir jetzt wissen?
Sie: Nun, ich benötige ein paar Detail-Informationen zu Ihren IT-Prozessen und der Einrichtung. Haben Sie das alles hier eingerichtet?
Felix: Nein, nein, ich habe mich ja dafür angeboten, aber da haben die da oben wieder einmal ihren Kopf durchgesetzt. Eine Spezialistenfirma haben sie kommen lassen und die hat das alles eingerichtet. Das waren solche Spezialisten, das sage ich Ihnen. Nicht einmal die Patchfelder im Serverraum und die Netzwerkdosen haben sie beschriftet. Das hätten wir selber besser gekonnt, aber nein, mir traut man das ja nicht zu.
Sie: Das heißt, es gibt also auch keinen Netzwerkplan für Ihre Büros hier?
Felix: Nein, natürlich nicht. Ich bin aber auch noch nicht dazugekommen, die ganzen Kabel durch die Wände zurückzuverfolgen. Die sind nämlich in Leerrohren unter Putz verlegt. Da muss man jedes Kabel einzeln testen, wissen Sie?
Sie: Sie sind ja nicht zu beneiden. Aber fangen wir mal mit meinen Fragen an. Ich habe bei Frau Lucciano gesehen, dass ihr Papierkorb ziemlich voll war. Haben Sie wenigstens eine Software im Einsatz, die den leeren Festplattenplatz regelmäßig überschreibt, damit keine gelöschten Dateien zurückbleiben?
Felix: Nein, wir hatten bislang nicht die erforderlichen Mittel, um so eine Software anzuschaffen.
Sie: Ich habe bei Frau Lucciano auch gesehen, dass der Rechner gar nicht in einer Domäne registriert ist. Ich dachte Sie haben einen Windows 2003 Server hier im Einsatz?
Felix: Ja schon, aber der ist kürzlich für drei Tage ausgefallen und dann haben wir zwei Rechner aus der Domäne entfernt, um wenigstens im Notbetrieb weiterarbeiten zu können. Ich habe noch keine Zeit gehabt, das wieder umzustellen.
Sie: Haben Sie Roaming Profiles aktiviert oder richten Sie die ganzen Benutzeraccounts auf allen Rechnern von Hand ein?
Felix: Roaming Profiles haben wir nicht. Ich mache das von Hand, das macht weniger Probleme. Aber bei den paar Rechnern geht das ja auch recht schnell. Bisher hat sich noch keiner beschwert.
Sie: Wie behalten Sie denn da den Überblick über die eingerichteten Benutzerkonten auf den verschiedenen Rechnern? Auf Frau Luccianos Rechner habe ich zum Beispiel einen Account testuser ohne Passwort entdeckt. Wird der noch verwendet?
Felix: Nein, den haben wir nur zum Installieren der Software am Anfang benötigt. Den werd ich nachher gleich löschen.
Sie: Entschuldigen Sie meine Pingeligkeit, aber wenn ich das richtig verstehe haben Sie keine Dokumentation, welche Benutzeraccounts auf welchen Rechnern eingerichtet sind, oder?
Felix: Nein, das sollen Sie doch machen, dachte ich.
Sie: Soweit ich weiß, ist das nicht unsere Rolle im Projekt. Wir begleiten Sie nur auf dem Weg zur Zertifizierung. Die eigentliche Arbeit müssen Sie selbst durchführen. Wir suchen nur nach fehlenden Bausteinen und Maßnahmen. Kann ich dann also davon ausgehen, dass Sie auch keine Dokumentation und kein Konzept für die Netzwerkdienste haben, die auf den Clients laufen?
Felix: Natürlich nicht. Das ist bei fünf Rechnern doch auch absoluter Overkill. Die Dokumentation bin ich. Fragen Sie mich einfach etwas und ich sage Ihnen was Sie wissen wollen.
Sie: Haben Sie eigentlich von hier aus Zugriff auf die Integritätsdatenbank in Ingolstadt, um das Betriebssystem der Clients beim Booten auf Unversehrtheit zu überprüfen.
Felix: Nein. Momentan booten die Clients direkt Windows.
Sie: Wie machen Sie das denn mit dem Virenscanner? Ich habe keinen Virenscanner auf Frau Luccianos Rechner gefunden. Haben Sie einen auf dem Server oder auf dem Internet-Application-Gateway installiert?
Felix: Wir konnten uns noch nicht entscheiden, welchen Virenscanner wir verwenden. Die IT-Abteilung in Ingolstadt wollte eigentlich neue Lizenzen besorgen für unsere Rechner. Aber bisher ist nichts passiert. Ich muss da mal wieder nachhaken.
Sie: Sie könnten doch vorläufig einen kostenlosen Virenscanner einrichten, zum Beispiel ClamAV – das wäre besser als gar nichts.
Felix: Stimmt. Aber wenn dann der richtige Virenscanner kommt, müssten wir den ja wieder deinstallieren. Das ist ja dann doppelter Aufwand.
Sie: Wie ist denn eigentlich die Bootreihenfolge im BIOS eingestellt? Haben Sie sichergestellt, dass überall direkt von Festplatte gebootet wird und man den Rechner nicht mit CD oder USB-Sticks starten kann?
Felix: Jetzt haben Sie mich erwischt. Da bin ich ehrlich gesagt überfragt. Ich habe die Rechner von Herrn Winkler geliefert bekommen. Da war schon ein vorinstalliertes Windows drauf. Wir haben sie nur aufgebaut. Ich will doch hoffen, dass sich die Zentrale um eine sichere Konfiguration kümmert. Aber ich kann ja nachher einmal nachschauen, wie das BIOS eingestellt ist, wenn Sie das beruhigt.
Sie: Es geht aber gar nicht darum, mich zu beruhigen – was ich notieren muss, ist die Tatsache, dass keine Dokumentation und kein Prozess existieren, die sicherstellen, dass das BIOS korrekt und einheitlich konfiguriert ist. Wie schaut es denn bei den Browsern aus? Die Rechner haben doch alle Internetzugriff, oder? Könnten Sie mir kurz erklären, welche Maßnahmen Sie ergriffen haben, um die Rechner abzusichern?
Felix: Welche Maßnahmen meinen Sie denn? Ich habe Java und Flash und das AdobeReader-Plugin heruntergeladen und auf die neueste Version gebracht. Außerdem habe ich im Browser die automatischen Updates aktiviert. Die Rechner sollten sich also selbständig patchen, wenn Sicherheitlücken bekannt werden. Reicht das nicht?
Sie: Das heißt Sie haben ActiveX, JavaScript und Java im Browser aktiviert? Oder haben Sie so eine No-Script-Erweiterung oder Sandbox im Einsatz?
Felix: Wir brauchen Scripting, weil unser Bestellinterface braucht das. Das kann ich leider nicht abschalten. Ich würde ja gerne. Privat surfe ich ja nur unter Linux. Aber das will die Zentrale nicht auf den Unternehmensrechnern installieren. Dabei ist Linux doch viel sicherer! Ich versteh' das echt nicht! Stattdessen diskutieren Sie dauernd am grünen Tisch und schicken uns eine Firma nach der anderen vorbei. Wissen Sie, das geht jetzt nicht gegen Sie. Sie kommen ja ganz kompetent rüber. Aber diese ewigen Interviews gehen mir langsam echt auf die Nerven!
Sie: Ich kann schon verstehen, dass Sie frustriert sind. Die gute Nachricht ist: Das war's schon. Ich denke ich habe alle Infos, die ich brauche, um meinen Bericht für Dr. Färber anzufertigen. Vielen Dank für das Gespräch.

Abbildung 3: Interview mit Felix Zimmermann

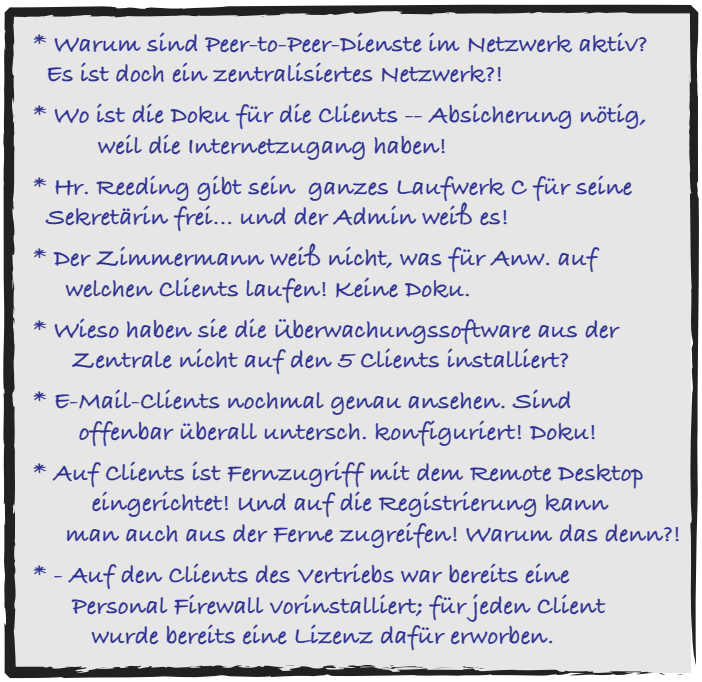


Abbildung 4: Notizzettel mit Auffälligkeiten beim Rundgang

17.5 Aufgabe: Erstellung einer Sicherheitskonzeption

Der Geschäftsführer Dr. Färber hat Sie zunächst damit beauftragt, eine Sicherheitskonzeption nach IT-Grundschutz durchzuführen und eine Präsentation der wichtigsten Ergebnisse vorzubereiten. Bei der Durchführung sollen Sie sich am IT-Grundschutz-Vorgehensmodell orientieren (vgl. BSI-Standard 100-2[2], Kapitel 4). Ihre Präsentation sollte die Ergebnisdokumente für die folgenden Analyseschritte beinhalten:

1. Zunächst führen Sie die Strukturanalyse durch. Zeichnen Sie einen bereinigten Netzplan für den Standort Triest.

2. Nehmen Sie eine Zuordnung der in Triest laufenden Anwendungen zu den Servern, den Clients sowie zu den Netzkomponenten vor. Hierzu ist es nötig, die einzelnen Anwendungen zu identifizieren, die in Triest verwendet werden. Überlegen Sie sich ferner, ob bei den einzelnen Anwendungen personenbezogene Daten verarbeitet werden und kennzeichnen Sie diese gegebenenfalls. *Hinweis: Orientieren Sie sich bei der Erstellung der Zuordnungstabellen am Beispiel des BSI*[3].

3. Ermitteln Sie danach den Schutzbedarf für alle Anwendungen, Server, Clientgruppen, und Netzkomponenten. Im Anschluss daran ermitteln Sie den Schutzbedarf für die einzelnen Räume des Standorts Triest. *Hinweise: Der Schutzbedarf der Kommunikationsverbindungen kann in diesem Beispiel vernachlässigt werden. Sie können sich bei der Erstellung der Tabellen am Beispielunternehmen RECPLAST des BSI orientieren. Erklärende Erläuterungen finden sie im Grundschutz-Kurs des BSI*[4].

4. Nun können Sie die Modellierung nach IT-Grundschutz durchführen. Verwenden Sie dazu die bisherigen Erkenntnisse und modellieren Sie den Informationsverbund mit den IT-Grundschutz-Bausteinen, indem Sie die Bausteine aus den Grundschutzkatalogen ermitteln, die ihrer Meinung nach für den Standort Triest relevant sind. Erstellen Sie dann eine Tabelle, die angibt, für welche Zielobjekte die einzelnen Bausteine jeweils anzuwenden sind. *Verwenden Sie hierzu die IT-Grundschutz-Kataloge 2012*[5]. *Falls ein Baustein in Triest Ihrer Meinung nach nicht anzuwenden ist, müssen Sie ihn nicht aufführen.*

[2] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002_pdf.pdf, Zugriff: April 2013.

[3] Bundesamt für Sicherheit in der Informationstechnik, Das Beispielunternehmen RECPLAST, https://www.bsi.bund.de/cae/servlet/contentblob/479048/publicationFile/31005/recplast_pdf.pdf, Zugriff: April 2013.

[4] Bundesamt für Sicherheit in der Informationstechnik, Webkurs IT-Grundschutz, https://www.bsi.bund.de/cln_165/DE/Themen/weitereThemen/ITGrundschutzSchulung/itgrundschutzschulung_node.html, Zugriff: April 2013.

[5] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 12. Ergänzungslieferung, https://www.bsi.bund.de/cln_165/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, Zugriff: April 2013.

5. Abschließend soll der Basis-Sicherheitscheck durchgeführt werden. Das in der vorherigen Aufgabe erstellte Modell wird dabei als Prüfplan verwendet, um einen Soll-Ist-Vergleich durchzuführen. Erfreulicherweise werden die umfangreichen Bausteine B1 und B2 von Ihren Kollegen bearbeitet. Sie sollen sich lediglich um die Bausteine kümmern, die für den Betrieb der fünf Clients im Vertrieb zu prüfen sind *(Hinweis: Hauptgruppe B3 IT-Systeme)*. Führen Sie anhand Ihrer bisherigen Ergebnisse, der geführten Interviews und Notizen einen Basis-Sicherheitscheck für die Clients des Vertriebs durch. Anhand des Basis-Sicherheitschecks sollen Sie der Geschäftsleitung dann erläutern, welche Maßnahmen bereits umgesetzt sind bzw. wo noch Handlungsbedarf besteht. *Hinweis: Sollten Sie in Ihrer Schutzbedarfsanalyse zu der Überzeugung gelangt sein, dass für die Clients erhöhter Schutzbedarf im Bezug auf Vertraulichkeit, Integrität oder Verfügbarkeit besteht, so ist an dieser Stelle, der Einfachheit halber, trotzdem keine Gefährdungsübersicht und Risikoanalyse zu erstellen.*

Fertigen Sie eine Dokumentation (Textdokumente bzw. Präsentationen) der Analyse an, die Sie der Geschäftsführung präsentieren (und am Tag der Präsentation per E-Mail einreichen).

17.6 Aufgaben Umsetzung der Sicherheitskonzeption

Mit der Präsentation Ihrer bisherigen Ergebnisse haben Sie lundi-tec von Ihrer Kompetenz überzeugt. Ihr Projekt wurde daher verlängert und basierend auf den bisherigen Analysen sollen Sie nun einen Plan für die Umsetzung der Sicherheitskonzeption anfertigen.

Ziehen Sie dazu die Erkenntnisse aus dem Basis-Sicherheitscheck heran. In Zusammenarbeit mit der IT-Abteilung und den Fachabteilungen haben Ihre Kollegen bereits eine große Anzahl von möglicherweise relevanten Tätigkeiten identifiziert und mit Aufwandsschätzungen versehen. Die angefertigte Übersicht soll als Basis für Ihren Realisierungsplan dienen (vgl. Anhang 17.8). Ermitteln Sie für die Tätigkeiten aus Anhang 17.8 die passenden Maßnahmennummern aus den Grundschutzkatalogen. Beziehen Sie bei der Planung auch Maßnahmen ein, die Ihre Kollegen auf dem ADRIA-DUE-Projekt identifiziert haben (Anhang 17.9). Treffen Sie auch hier eine sinnvolle Selektion.

Beachten Sie die Budgetrestriktionen, die lundi-tec Ihrer Firma auferlegt hat:

- Das Umsetzungsprojekt darf das genehmigte Budget nicht überschreiten: Die einmaligen Umsetzungskosten dürfen 21.000 Euro nicht überschreiten. Ihre Unternehmensberatung darf maximal 80 Arbeitstage abrechnen.
- Projektbeginn ist am 01.01.2009. Das Projekt hat eine Laufzeit von maximal 4 Monaten. Spätestens dann müssen alle Maßnahmen implementiert sein.
- Die Realisierung soll von 1 Consultant durchgeführt werden, der nicht mehr als 20 Arbeitstage im Monat arbeitet.
- Die nachgelagerten jährlichen Aufwendungen sollen 1.500 Euro/Jahr und 52 Arbeitstage/Jahr nicht überschreiten.

In Ihrem Umsetzungsplan sollen die ausgewählten Maßnahmen in einer vernünftigen Reihenfolge (z. B. nach der Wichtigkeit für die Sicherheit des Standortes Triest, nach Aufbaustufe oder entsprechend der Abhängigkeiten zwischen einzelnen Maßnahmen) abgearbeitet werden. Außerdem soll aus Ihrer Dokumentation hervorgehen, in welchem Monat welche Maßnahmen durchgeführt werden. Achten Sie darauf, dass die Auslastung des Consultants im Rahmen bleibt.

Ziel ist die optimale Absicherung des Standortes Triest gegen alle Gefahren. Das Erreichen der Aufbaustufe B der Zertifizierung ISO 27001 ist dabei sicher wünschenswert, bei angemessener Begründung wird lundi-tec jedoch auch andere Lösungen akzeptieren.

Fertigen Sie eine 15-20-minütige Präsentation an, in der Sie die Geschäftsführung und die Gesellschafter von Ihrer Realisierungsstrategie überzeugen. Sie können dabei gegebenenfalls auch konstruktive bzw. innovative Vorschläge zur Verbesserung der Infrastruktur machen. Begründen Sie die getroffene Auswahl der Maßnahmen und legen Sie dar, inwieweit Ihre Lösung die Budgetrestriktionen erfüllt. *Hinweis: Falls erforderlich, können Sie plausible Annahmen über Sachverhalte treffen, auf die nicht in der Fallstudie eingegangen wird. Bleiben Sie bei Ihrer Argumentation jedoch so nah wie möglich am gegebenen Sachverhalt.*

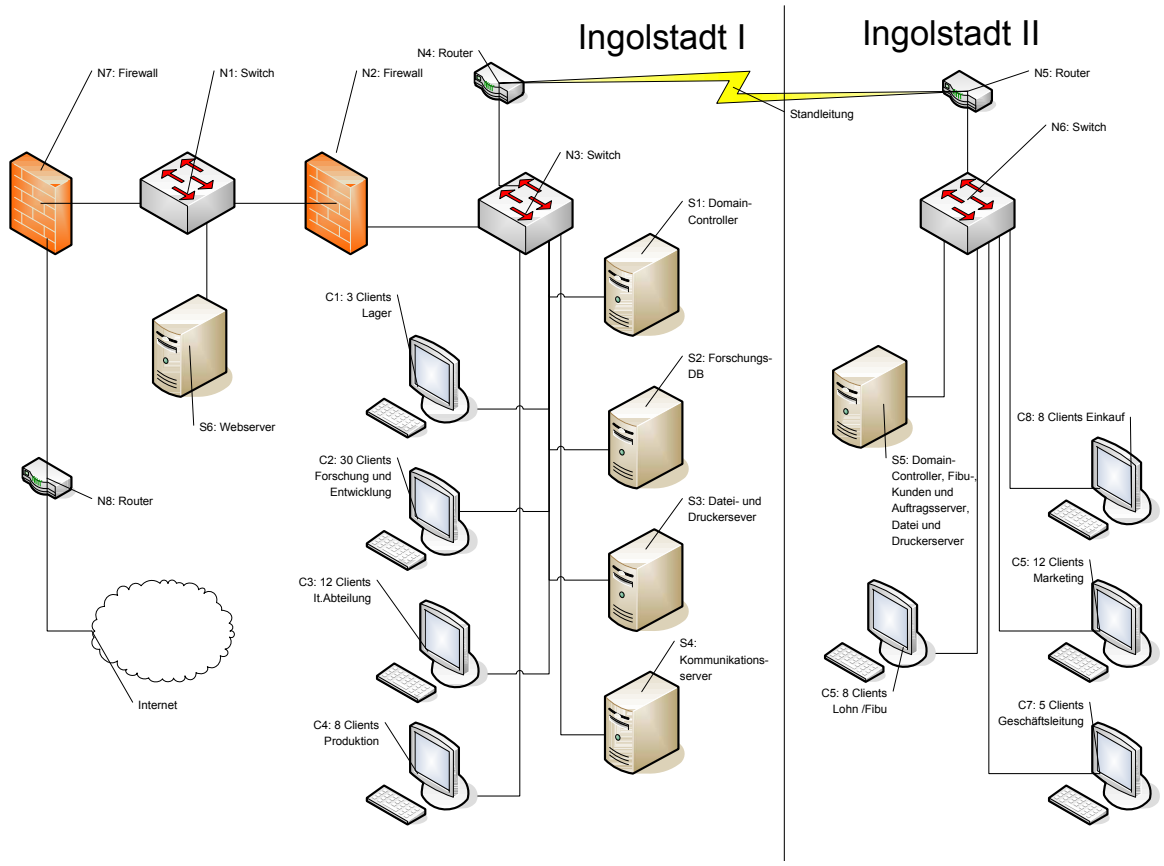


Abbildung 5: Netzplan

17.7 Aufgabe Risikoanalyse auf der Basis BSI 100-3

Seit Ihrer Beauftragung sind zwei Jahre vergangen. Dank Ihrer Hilfe hat der Standort Triest — für Sie allerdings nicht ganz nachvollziehbar — damals die Aufbaustufe B auf der Grundschutzleiter erklommen. Leider gab es vor kurzer Zeit jedoch einen kleinen Sicherheitszwischenfall, bei dem geheime Daten aus der Forschungsdatenbank an die Öffentlichkeit gelangt waren. Nichts schlimmes, lediglich ein paar Umweltschützer zeigten sich besorgt. In der Folge wurde ein Spezialunternehmen für IT-Forensik damit beauftragt, die Ursache für das Datenleck zu ermitteln sowie herauszufinden, wie die Eindringlinge von außen auf die geheimen Daten, die eigentlich nur auf dem aus dem internen LAN erreichbaren Labor-Server vorliegen, zugreifen konnten. Das IT-Forensik-Projektteam förderte in seinem 60-seitigen Ergebnisbericht überraschende Erkenntnisse zu Tage: Nicht der Labor-Server, sondern das unglückliche Zusammenwirken mehrerer Sicherheitsprobleme auf dem Triest-Server sowie diverse Policy-Verstöße der Mitarbeiter machten es den Angreifern erst möglich, an die sensiblen Daten zu gelangen! Ihre Unternehmensberatung wurde nun damit beauftragt, Maßnahmen vorzuschlagen, die sicherstellen sollen, dass sich ein solcher Vorfall nicht mehr wiederholt — oder zumindest im Frühstadium erkannt werden kann. Bei der Sichtung der Dokumentation des seit Ihrer letzten Beauftragung fortgeschriebenen Sicherheitskonzepts stellen Sie jedoch schnell fest, dass lundi-tec immer noch keine Risikoanalyse für den Triest-Server durchgeführt hat — obwohl Sie in Ihrem Abschlussbericht vor zwei Jahren die Geschäftsleitung auf die Wichtigkeit dieser Analyse hingewiesen hatten! Sie empfehlen dem Unternehmen daher, zunächst nach BSI-Standard 100-3 *Risikoanalyse auf der Basis von IT-Grundschutz* vorzugehen, um die Risikoanalyse zumindest für den Triest-Server, dem Sie damals einen hohen Schutzbedarf attestiert hatten, nachzuholen. Erst dadurch werde es möglich, ein klares, vollständiges Bild der Gefahrenlage, der dieser zentrale Server ja offenbar ausgesetzt sei, zu zeichnen. Im Zuge der Analyse würden dann alle identifizierten Risiken bewertet und adäquat adressiert werden. Schon vor der Beauftragung machen die lundi-tec-Geschäftsführer jedoch deutlich, dass sie — in Anbetracht der aktuellen Krise — eine vollständige Risikoanalyse auf absehbare Zeit nicht finanzieren könnten. Die Berater sollten daher zunächst lediglich die ihrer Einschätzung nach wichtigsten Bausteine betrachten. Aus früheren Projekten wissen Sie, dass die Geschäftsführer bei akuten Sicherheitsvorfälle durchaus sensibilierbar sind; die Risikoexposition hat schließlich direkte Auswirkungen auf Finanzierungsverhandlungen bei den Banken. Sie hoffen daher, dass sie die Geschäftsführer doch noch überzeugen können, eine vollständige Analyse durchzuführen. Die IT-Forensik-

Experten haben in ihrem Abschlussbericht weiterhin empfohlen, ein sog. Security-Dashboard zu implementieren, das zum einen dem Systemadministrator einen operativen und zum anderen der Geschäftsleitung einen taktischen/strategischen Überblick über die aktuelle Sicherheitslage ermöglichen könnte. Da solche aufwändigen Implementierungsmaßnahmen im Jahresbudget allerdings nicht vorgesehen waren, steht die Beauftragung eines spezialisierten Systemhauses zu diesem Zweck nicht zur Debatte. Vielmehr hat sich die Geschäftsleitung dazu entschieden, Kosten zu sparen, indem die Implementierung von einem Praktikanten, Alfons Gruber aus Ingolstadt, durchgeführt werden soll. Die fachliche Betreuung soll hingegen durch externe Berater erfolgen, um sicherzustellen, dass das Dashboard auch seinen Zweck erfüllt und alle wesentlichen Risiken erfasst. Angesichts der mit der Krise einhergehenden schwachen Auftragslage haben Sie sich (etwas widerwillig) bereit erklärt, diese verantwortungsvolle Aufgabe zu übernehmen.

Aufgabenstellung

Bearbeitungshinweise: Halten Sie sich an die Vorgehensweise des oben erwähnten BSI-Standard 100-3. Treffen Sie bei der Bearbeitung sinnvolle Annahmen, falls die Fallstudie keine Angaben zu einem Sachverhalt enthält. Berücksichtigen Sie jedoch, dass bereits Aufbaustufe B erreicht ist. Die sog. *Zusätzliche Gefährdungen* müssen nicht betrachtet werden, auf den Ausweis von *Risiken unter Boebachtung* sowie die *Konsolidierung* kann verzichtet werden. Ihre eigentliche Mission lautet: Sie sollen die Geschäftsleitung überzeugen, Sie mit einer vollständigen Risikoanalyse zu beauftragen.

1. Präsentieren Sie dazu zunächst eine Liste aller Bausteine, die relevante Gefährdungen für den Triest-Server enthalten. Geben Sie bei Ihrer Darstellung auch einen Überblick über die Anzahl der relevanten Gefährdungen in den einzelnen Bausteinen.

2. Ihrer Meinung nach sind die Bausteine *Serverraum*, *Allgemeiner Server* und *E-Mail* besonders relevant und daher für die abgespeckte Risikoanalyse am ehesten geeignet. Erstellen sie für diese Bausteine eine nach Schichten sortierte Liste aller Gefährdungen — natürlich ohne Duplikate. Machen Sie der Geschäftsleitung in der Präsentation deutlich, warum man nicht auf die Betrachtung der anderen Bausteine verzichten sollte.

3. Wählen Sie aus den oben genannten Bausteinen einen einzelnen Baustein aus, der Ihnen geeignet erscheint, um die Gefährdungsbewertung und die Behandlung von Risiken zu demonstrieren. Sie stehen bei diesem Auftrag unter Zeit- und Kostendruck; gehen Sie bei der Baustein-Wahl also pragmatisch vor. Für diesen einen Baustein führen Sie nun die Gefährdungs- und Risikoanalyse nach BSI-Standard 100-3 durch, um der Geschäftsleitung plastisch aufzuzeigen, welche Inhalte sie von einer vollumfassenden Analyse erwarten kann. Geben Sie dabei auch an, wie für den gewählten Baustein die verbleibenden Risiken behandelt werden sollten, also welche Handlungsalternativen Sie empfehlen (vgl. Standard 100-3, Abschnitt 6.1). Versuchen Sie durch Ihre Präsentation, der Geschäftsleitung den offensichtlichen Nutzen einer solchen Analyse zu vermitteln und sie dazu zu bewegen, Sie mit einer vollumfassenden Analyse zu beauftragen. Hinweis: Sie müssen eventuell mit Nachfragen zum erwarteten zeitlichen Aufwand für eine vollumfassenden Gesamtanalyse rechnen. Sie können sich zumindest teilweise darauf vorbereiten, indem Sie den Gesamtaufwand auf Basis der von Ihnen durchgeführten Teil-Analyse abschätzen und im Fall des Falles eine plausible Herleitung parat haben.

17.8 Anhang: Tätigkeiten aus dem Baustein-Katalog B2 (IT-Systeme)

Die nachfolgende Tabelle enthält Tätigkeiten, die für die die Vertriebsclients relevant sind. Im Rahmen der Umsetzungsplanung sollen Sie eine plausible Auswahl vornehmen. Alle Aufwände wurden von Ihren Kollegen auf Basis von Voruntersuchungen, technischer Erfarung und Experteninterviews geschätzt. Stand: Juli 2008.

Legende: AT=Arbeitstage, A: Einmalige Investitionskosten (Euro), B: Einmaliger Personalaufwand (AT), C: Wiederkehrende Kosten (Euro/Jahr), D: Wiederkehrender Personalaufwand (AT/Jahr). Angegebene Einheiten gelten nur falls nicht anders angegeben. Beachten Sie, dass bei einigen Tätigkeiten mehrere Handlungsalternativen zur Verfügung stehen – wählen Sie die Ihnen am geeignetsten erscheinende Alternative aus.

Nr.	Tätigkeit	A	B	C	D	Bemerkung
1	Einschränken der Peer-to-Peer Funktionalität an den einzelnen Clients		1		0,5	

Nr.	Tätigkeit	A	B	C	D	Bemerkung
2	Sichere Grundkonfiguration für alle Clients manuell vornehmen		2		1	Umfasst alle Einstellungen der sicheren Grundkonfiguration, die nachfolgend nicht explizit behandelt werden
3	Administrationsscripte der Hauptverwaltung zur sicheren Grundkonfiguration für Triest anpassen		4		0,5	
4	Aktivierung des Windows-Passwortschutzes beim Beenden des Bildschirmschoners für alle Clients		0,5			
5	Jährliche Schulungen zu den betriebssystemeigenen Sicherheitsmechanismen		2		1	
6	Beschaffung und Installation des gleichen Virenscanners, der auch in Ingolstadt Verwendung findet	400	3	80	1	
7	Physikalischer Diebstahlschutz aller Clients des Vertriebs durch Stahlseile und Vorhängeschlösser	86	0,5			
8	Physikalischer Diebstahlschutz aller Clients des Vertriebs durch entsprechende Client-Schutzschränke	660	1,5			
9	Einsatz eines GPL-lizensierten Virenscanners auf den Clients		3		3	
10	Installation kommerzieller Software, die lediglich ein Arbeiten mit verschlüsselten Wechselmedien (USB-Sticks) zulässt.	320	2	100	3	Unverschlüsselte Medien werden ignoriert, oder müssen entsprechend vorbereitet werden.
11	Verwendung einer kommerziellen Schutzsoftware, die das Arbeiten an fremden Clients ohne Anmeldung verhindern soll (RFID-Dongle)	600	2	100		
12	Physikalisches Trennen des Rechnermikrofons an allen Clients		1			
13	Zusammenstellen, Auswählen und Umsetzen eines geeigneten Maßnahmenpakets zur Absicherung der Webbrowser in den Clients		8		3	
14	Regelungen für die private Nutzung des Internets treffen und implementieren		1		1	
15	Internetschulungen für Mitarbeiter abhalten			930	1	
16	Die Bootreihenfolge im BIOS wird so verändert, dass die interne Festplatte das erste Medium der Bootreihenfolge ist.		0,5			
17	Deinstallieren nicht benötigter Komponenten auf den Clients		4			
18	Regelmäßiges Updaten der gekauften Personal Firewall			60	1	
19	Zusammenstellen, auswählen und umsetzen eines geeigneten Maßnahmenpakets zur Absicherung der E-Mail-Clients in den Rechnern		5		2	
20	Fernzugriff auf allen Clients in Triest deaktivieren		1			
21	Fernzugriff auf allen Clients einheitlich konfigurieren und absichern		0,5			
22	Schulung der Mitarbeiter im Umgang mit Fernzugriff	150			1	
23	Entwerfen eines Überwachungskonzepts, Umsetzung und Protokollierung (Zusatzsoftware). Regelmäßige Logfileprüfung.	760	8		5	
24	Deaktivieren der automatischen CD-ROM-Erkennung bei allen Clients	0,5				
25	Erstellung und Einsatz eines Scriptes, das die Windows-Registry der einzelnen Arbeitsplätze schützt		1,5			
26	Deaktivieren der Datei- und Druckerfreigabe an allen Clientrechnern		1			
27	Einheitliche Aktivierung der Datei- und Druckerfreigabe an allen Clients; Absicherung		3		5	
28	Erwerb und Installation einer kommerziellen Systemsicherungssoftware, die alle Tastenanschläge der Vertriebsmitarbeiter protokolliert und bei unautorisierter Abweichungen den Benutzer automatisch abmeldet	1800	1		3	
29	Bedarfsanalyse über gebrauchte Systemdienste der Clients duchführen		2			
30	nicht benötigte Systemdienste der Clients deaktivieren		0,5			
31	Erwerb und Implementierung einer kommerziellen Software zum sicheren Löschen von Dateien auf Datenträgern	380	1,5			
32	Einheitliche Konfiguration für den Windows Papierkorb an allen Clients vornehmen		0,5			

Nr.	Tätigkeit	A	B	C	D	Bemerkung
33	Einspielen der aktuellen Sicherheitspatches für die Internet-Clients des Vertriebs				8	

17.9 Anhang: Maßnahmen aus dem AQUA-DUE-Projekt

Die nachfolgende Tabelle enthält Tätigkeiten, die im Rahmen des ADRIA-DUE-Projekts identifiziert wurden. Im Rahmen der Umsetzungsplanung sollen Sie auch diese Tätigkeiten berücksichtigen. Alle Aufwände wurden von Ihren Kollegen auf Basis von Voruntersuchungen, technischer Erfarung und Experteninterviews geschätzt. Stand: Juli 2008. Die Tätigkeiten wurden bereits konkreten Maßnahmen aus den Grundschutzkatalogen zugeordnet.

Legende: AT=Arbeitstage, A: Einmalige Investitionskosten (Euro), B: Einmaliger Personalaufwand (AT), C: Wiederkehrende Kosten (Euro/Jahr), D: Wiederkehrender Personalaufwand (AT/Jahr). Angegebene Einheiten gelten nur falls nicht anders angegeben. Beachten Sie, dass bei einigen Tätigkeiten mehrere Handlungsalternativen zur Verfügung stehen – wählen Sie die Ihnen am geeignetsten erscheinende Alternative aus.

Nr.	Stufe	Tätigkeit	A	B	C	D	Bemerkung
M5.63	Z	Einsatz von GnuPG oder PGP		3		0,5	Installation eines Plugins im E-Mail-Client; Erzeugung und Austausch der Schlüssel. Schulung der Mitarbeiter. Abwicklung des verschlüsselten Datenaustauschs zw. Triest und Ingolstadt sowie zu ausgewählten externen Kommunikationspartnern.
M5.110	Z	Absicherung von E-Mail mit SPHINX (S/MIME)	900	6	150	1	Integration von Triest in die S/MIME-Zertifikatsinfrastruktur und Anpassung der E-Mail-Clients. Schulung der Mitarbeiter. Zur Absicherung der E-Mail-Kommunikation zw. Triest und Ingolstadt sowie zu allen Kunden.
M2.314	Z	Verwendung von hochverfügbaren Architekturen für Server	9300	8		1	Migration des Triest-Servers auf eine Hochverfügbarkeitsarchitektur
M4.93	B	Regelmäßige Integritätsprüfung	340	2	150	2	Zur regelmäßigen Integritätsprüfung wird ein kommerzielles Tool verwendet.
M5.8	B	Regelmäßiger Sicherheitscheck des Netzes		1		8	Der Sicherheitscheck muss monatlich erfolgen.
M4.280	A	Sichere Basiskonfiguration von Windows Server 2003		3		1	Eine sichere Grundkonfiguration für den Triestserver erstellen.
M2.370	A	Administration der Berechtigungen unter Windows Server 2003		3		0,5	Konfiguration der Berechtigungen anhand eines Berechtigungskonzepts
M4.56	C	Sicheres Löschen unter Windows Betriebssystemen		1			Richtiger Dateiumgang
M6.99	A	Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003	2200	2	800	1	Hierzu wird ein kommerzielles Produkt verwendet. Es werden zusätzlich die Nutzerdaten gesichert.
M2.75	A	Geeignete Auswahl eines Application-Level-Gateways		3	80	2	Hierzu wird das bereits gekaufte Produkt implementiert.
M2.76	A	Auswahl und Einrichtung geeigneter Filterregeln		4		2	Richtige Konfiguration der Firewall wird vorgenommen.
M3.43	C	Schulung der Administratoren des Sicherheitsgateways	600	3	100	1	Hierfür gibt es eine Schulung die jährlich aufgefrischt wird.
M2.302	Z	Sicherheitsgateways und Hochverfügbarkeit	9300	2	150	1	Bereitstellung eines Hochverfügbarkeits-Gateways.
M4.100	C	Sicherheitsgateways und aktive Inhalte		3		1	Filterung aktiver Inhalte auf dem Sicherheitsgateway und Erstellung einer Whitelist für vertrauenswürdige Websites.
M4.101	C	Sicherheitsgateways und Verschlüsselung	1400	6	240	1	Installation eines VPN-Gateways in Triest und Anbindung an die Zentrale zur Absicherung sämtlicher Kommunikationsinhalte zwischen Triest und Ingolstadt.
M5.59	C	Schutz vor DNS-Spoofing		1		1	Maßnahmen entsprechend des Katalogs vornehmen.
M5.120	A	Behandlung von ICMP am Sicherheitsgateway		0,5			Entsprechende Vorkehrungen sind am Sicherheitsgateway zu treffen.

Nr.	Stufe	Tätigkeit	A	B	C	D	Bemerkung
M1.43	A	Gesicherte Aufstellung aktiver Netzkomponenten	800	1			Hierfür wird ein eigener, kleiner Schutzschrank angeschafft.
M2.282	A	Regelmäßige Kontrolle von Routern und Switches				1	Regelmäßige Prüfungen der Netzkomponenten, sowie Dokumentation dieser Tätigkeit durch einen Administrator.
M4.206	C	Sicherung von Switch-Ports	460	2		1	Mac-Locking für den Standort Triest einrichten. Es wird ein neuer Switch benötigt.
M1.32	B	Geeignete Aufstellung von Druckern und Kopierern	430	3	100		Die Drucker sollen in einem eigenen, absperrbaren Büroraum installiert werden; Mietmehrkosten.
M4.302	C	Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten		1		0,5	Zum besseren Erkennen von Verstößen gegen die Sicherheitsrichtlinien werden Druckprotokolle gespeichert.
M4.7	A	Änderung voreingesteller Passwörter		1			Überprüfen und ggf. ändern von Standardpasswörtern in Geräten.
M6.52	A	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten		2		1	Im Zuge der Notfallvorsorgung werden diese Daten automatisch gesichert.
M1.36	A	Sichere Aufbewahrung der Datenträger vor und nach dem Versand	2500				Datenträgerpakete werden in einer Schutzbox beim Posteingang eingesperrt, und nur dem entsprechendem Empfänger persönlich ausgehändigt.
M2.43	A	Ausreichende Kennzeichnung der Datenträger beim Versand				12*	*) Einheit: 12 Minuten/Tag! Datenträger müssen bei Versand entsprechend gekennzeichnet werden (Stichprobenartige Kontrolle).
M4.34	Z	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	1500	2	300	0,5	Datenträger werden verschlüsselt bevor sie postalisch verschickt werden. Hierzu wird ein kommerzielles Produkt mit wohluntersuchtem Verschlüsselungsverfahren verwendet.
M3.60	C	Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern	800	2	300	1	Durchführung einer regelmäßigen Schulung zu diesem Thema
M4.32	B	Physikalisches Löschen von Datenträgern vor und nach Verwendung	400	1		3	Austauschdatenträger werden mit Spezialsoftware gelöscht.

Aufgabenübersicht

1 Technische Grundlagen **1**

1.1 Nachrichten, Daten, Information 1

1.2 Anti-Spam-Tools 1

1.3 Sicherheit von weit verbreiteten Kommunikationsprotokollen 1

2 Grundbegriffe der IT-Sicherheit **1**

2.1 Verteilte Systeme und Sicherheit 1

2.2 Digitale Systeme und Sicherheit 1

2.3 Sicherheit in Beispielanwendungen 1

3 Aufgaben zur Sicherheit allgemein **2**

3.1 Schutzziele 2

3.2 Abgrenzung von Schutzzielen 2

3.3 Integrität und Zurechenbarkeit 2

3.4 Integrität, Verfügbarkeit und Korrektheitsbegriff 2

3.5 Techniken zur Umsetzung von Schutzzielen 2

3.6 Ausgewählte Angriffsformen 2

4 Angreifermodelle **2**

4.1 Angreifermodell 2

4.2 Konkrete Angreifermodelle 2

4.3 Allmächtiger Angreifer 3

4.4 Angreifermodell für den Geldautomaten 3

5 Sicherheitsmanagement **3**

5.1 Bedrohungsanalyse 3

5.2 Mangelnde IT-Sicherheit in Unternehmen 3

5.3 Einsatz von Sicherheitsbausteinen 3

5.4 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) 4

5.5 Security Policy 4

5.6 Gefährdungs- und Maßnahmenkataloge nach BSI-GSHB 4

5.7 Zertifizierung nach BSI-Grundschutzhandbuch oder ISO 17799? 4

6 Rechnersicherheit **4**

6.1 Physische Sicherheit im Rechenzentrum und lokales Rechnernetz 4

6.2 Seitenkanalangriffe 5

6.3 Identifikation von IT-Systemen durch Menschen 5

6.4 Zugriffs- und Zugangskontrolle 5

6.5 Passwortüberprüfung 5

6.6 Passwortknacken 5

6.7 Klartext-Kennwörter 5

6.8 Speicherung gehashter Kennwörter 5

6.9 Sicherheit alter UNIX-Kennwörter 6

6.10 Rainbow-Tables . . . 6
6.11 Salted Hashing . . . 6
6.12 Implementierung eines Brute-Force-Angriffs mit einem Wörterbuch . . . 6
6.13 Angreifermodell von SecurID . . . 6
6.14 Funktionsweise von SecurID . . . 6
6.15 Unsichere Frage-Antwort-Verfahren . . . 6
6.16 Authentifizierungsprotokolle . . . 7
6.17 Realisierung eines Online-Tickets . . . 7
6.18 Unsichere Implementierung von Sicherheitsfunktionen . . . 7
6.19 Biometrische Authentifizierung beim EasyPASS-System . . . 8
6.20 Biometrische Authentifizierung anhand des Tippverhaltens . . . 8
6.21 Virenerkennung . . . 9

7 Fehlertoleranz, Datensicherung **9**
7.1 Einzelnes System (Ausfallwahrscheinlichkeit) . . . 9
7.2 Einzelnes System (Verfügbarkeit) . . . 9
7.3 Einzelnes System (Ausfallzeit) . . . 9
7.4 Gekoppelte Systeme . . . 9
7.5 Doppelung . . . 9
7.6 Web-Serversystem mit Lastverteiler . . . 9
7.7 Reparaturdauer . . . 9
7.8 Reparaturdauer bei RAID . . . 10
7.9 Storage Area Network (SAN) aus RAID-5-Systemen . . . 10
7.10 Serverfarm eines Webmail-Anbieters . . . 10
7.11 Zuverlässigkeit . . . 10
7.12 RAID-Arrays . . . 10
7.13 Vergleich RAID-1 und RAID-5 . . . 10
7.14 Backups bei RAID . . . 11
7.15 Allgemeines zu Backups . . . 11
7.16 Differenzielles Backup . . . 11
7.17 Backupstrategie . . . 11
7.18 Backup mittels rsnapshot . . . 11

8 Kryptographie I **12**
8.1 Zentrale Begriffe der Kryptographie . . . 12
8.2 Zufallszahlen bei Schlüsselgenerierung . . . 12
8.3 Verschlüsselte PIN-Übermittlung . . . 12
8.4 Symmetrische Schlüssel aus Passwörtern erzeugen . . . 12
8.5 Spalten-Transpositionen . . . 12
8.6 Unsicherheit der klassischen Verschiebechiffre . . . 13
8.7 TextCrypter . . . 13
8.8 PGP-Verschlüsselung und -Signatur . . . 13
8.9 Symmetrische Schlüsselverteilung . . . 13
8.10 Indeterministische Verschlüsselung . . . 13
8.11 Indeterministische Verschlüsselung . . . 13

9 Digitale Signatursysteme und Public-Key-Infrastrukturen **14**
9.1 Vertrauensbeziehungen in Public-Key-Infrastrukturen . . . 14
9.2 Cross Certification . . . 14
9.3 Verifizierung des öffentlichen Schlüssels . . . 14
9.4 Datenschutzgerechte Pseudonyme . . . 14
9.5 Blinde Signaturen . . . 14

10 Kryptographie II **15**
10.1 Hashfunktionen . . . 15
10.2 Anzahl der Kollisionen einer Hashfunktion . . . 15
10.3 Münzwurf über das Telefon . . . 15
10.4 „Mensch ärgere Dich nicht“ über das Telefon . . . 15
10.5 Informationstheoretisch sichere Verschlüsselung . . . 15
10.6 Informationstheoretisch sichere asymmetrische Verschlüsselung . . . 15
10.7 Informationstheoretisch sichere Authentikation . . . 15
10.8 One-Time-Pad . . . 16
10.9 Triple-DES . . . 16
10.10 Unsicherheit des Electronic-Codebook-Modus . . . 16
10.11 Cipher-Block-Chaining-Betriebsmodus . . . 16
10.12 Diffie-Hellman-Schlüsselaustauschprotokoll . . . 17
10.13 Hash-Funktionen bei Verschlüsselung und digitaler Signatur . . . 17
10.14 Sicherheit des RSA-Verfahrens . . . 17
10.15 RSA . . . 17
10.16 RSA-Verfahren . . . 17
10.17 MFC-Komplexität . . . 18
10.18 Obere Schrake der MFC-Komplexität . . . 18
10.19 MFC-Komplexität des DES . . . 19
10.20 Brechen des VDES mittels MFC . . . 19

11 Steganographie und Watermarking **19**
11.1 Asymmetrische Steganographie . . . 19
11.2 Vertraulicher Nachrichtenaustausch nur mittels Message Authentication Codes (MACs) . . . 19
11.3 Spread Spectrum Watermarking . . . 19

12 Schutz digitaler Inhalte, Kopierschutz, DRM-Systeme **19**
12.1 Inhalte auf Datenträgern . . . 19
12.2 Hardwarebaustein zum Rechtemanagement . . . 19

13 Praktische Sicherheit **20**
13.1 Erstellen von Firewallregeln . . . 20
13.2 Notwendigkeit des inneren Paketfilters . . . 20
13.3 Denial-of-Service-(DoS)-Angriff auf bzw. mittels dynamischen Paketfilter . . . 20
13.4 Evaluation von Intrusion Detection Systemen (IDS) . . . 20
13.5 Sniffing zur Netzanalyse . . . 20
13.6 Verdecktes Tunneling mittels DNS . . . 20
13.7 Tunneling mittels SSH . . . 20
13.8 Real-World-Brute-Force-Angriff . . . 20

14 Mobilkommunikation **21**
14.1 Gemeinsamkeiten und Unterschiede Festnetz- und Mobilkommunikation . . . 21
14.2 Funkzellen . . . 21
14.3 Archtitektur von GSM . . . 21
14.4 Begriffe und Erläuterungen . . . 21
14.5 Datenbanken in GSM . . . 21
14.6 Sicherheitsfunktionen in GSM . . . 21
14.7 Allokation von Algorithmen . . . 22
14.8 Geheimnis Kc . . . 22
14.9 Geheimnis Ki . . . 22
14.10 Verbindungsverschlüsselung . . . 22
14.11 TMSI-Vergabe . . . 22
14.12 Schnittstellendefinitionen . . . 22
14.13 Verhindern von Betrug . . . 22
14.14 Zusammenspiel der Sicherheitsfunktionen . . . 22
14.15 Kritik an GSM . . . 22
14.16 IMSI-Catcher . . . 22
14.17 Gegenseitige Authentifizierung für GSM . . . 23
14.18 UMTS-Sicherheitsfunktionen . . . 23
14.19 Peilungsverfahren . . . 23
14.20 Bluetooth-Pairing . . . 23
14.21 Bluetooth-Authentifikation . . . 23
14.22 WEP . . . 23
14.23 Broadcast . . . 23
14.24 Kollisionsabstand offener impliziter Adressen . . . 23
14.25 TP-Methode . . . 24

15 Fallstudie Timing-Angriff **24**
15.1 Timing-Attack . . . 24

16 Fallstudie Parkhaus **25**
16.1 Funktionsweise . . . 25
16.2 Betrugsverhinderung . . . 25
16.3 Flatrate . . . 25

17 Fallstudie lundi-tec **27**
17.1 Einleitung . . . 27
17.2 Tag 1 . . . 28
17.3 Tag 2 . . . 29
17.4 Tag 3 . . . 30
17.5 Aufgabe: Erstellung einer Sicherheitskonzeption . . . 33
17.6 Aufgaben Umsetzung der Sicherheitskonzeption . . . 34
17.7 Aufgabe Risikoanalyse auf der Basis BSI 100-3 . . . 35
17.8 Anhang: Tätigkeiten aus dem Baustein-Katalog B2 (IT-Systeme) . . . 36
17.9 Anhang: Maßnahmen aus dem AQUA-DUE-Projekt . . . 38