WILHELM BÜCHNER HOCHSCHULE
Mobile University of Technology

Studienheft

SRN02

Grundlagen eines sicheren IT-Betriebs

SRN02

Grundlagen eines sicheren IT-Betriebs

Thomas Stasch, M.Sc.

Werden Personenbezeichnungen aus Gründen der besseren Lesbarkeit nur in der männlichen oder weiblichen Form verwendet, so schließt dies das jeweils andere Geschlecht mit ein.

Falls wir in unseren Studienheften auf Seiten im Internet verweisen, haben wir diese nach sorgfältigen Erwägungen ausgewählt. Auf die zukünftige Gestaltung und den Inhalt der Seiten haben wir jedoch keinen Einfluss. Wir distanzieren uns daher ausdrücklich von diesen Seiten, soweit darin rechtswidrige, insbesondere jugendgefährdende oder verfassungsfeindliche Inhalte zutage treten sollten.

Grundlagen eines sicheren IT-Betriebs

Inhaltsverzeichnis

Vorwort

Lesen Sie schon mal Informationen über neu veröffentlichte Schwachstellen? Nein? Dann sollten Sie dies nun einmal tun. Entsprechende Adressen finden Sie im Anhang. Wenn doch, dann wissen Sie, dass es immer wieder neue Schwachstellen, mit unterschiedlichen Bedrohungen gibt. Kein System ist davor gefeit: Windows, Linux, Mac OS … selbst das neue Mobiltelefon „Pixel“ von Google wurde, nur einen Monat nachdem es auf den Markt gekommen ist, erfolgreich gehackt.

Jede Software ist generell fehlerbehaftet. Diese Fehler können zum einen zu ungewollten Effekten führen oder aber durch sogenannte Exploits ausgenutzt werden, um Nebeneffekte, wie z. B. die Erlangung von Administrationsrechten, zu erreichen.

Von großen Unternehmen werden Belohnungen ausgelobt, solche Fehler zu finden und dem Hersteller zu melden. Ziel ist es hierbei, die Schwachstellen möglichst schnell zu beheben.

Neben diesem offiziellen Ansatz werden durch Hacker identifizierte Schwachstellen aber teilweise auch im Untergrund weiterverkauft und ausgenutzt. Potenzielle Käufer sind hierbei andere Hackergruppen, das organisierte Verbrechen, aber auch die Nachrichtendienste verschiedener Staaten.

Dieses Studienheft zeigt Ihnen, wo die üblichen Ansatzpunkte für Angriffe sind und welche Möglichkeiten man als Unternehmen hat, sich davor zu schützen.

Sie werden in den Grundzügen lernen, wie Schwachstellen funktionieren, wie man diese auffinden und auch ausnutzen kann. Für diejenigen von Ihnen, die etwas experimentierfreudiger sind, wird es Tipps geben, wo Sie mehr Informationen zu dieser Thematik erhalten.

Ziel der Informationstechnologie ist es, einen möglichst reibungslosen ▸IT-Betrieb sicherzustellen. Hierzu zählen die Abwägung zwischen den verschiedenen Gefahren, das Ableiten von Vorgehensmodellen und die Entscheidungsfindung.

Freuen Sie sich auf ein hoffentlich spannendes Studienheft, das Ihnen auch Einblicke in die „dunkle“ Seite geben wird.

Ihre Studienleitung

1 Einleitung und Motivation

In der Einleitung werden Sie an die Gefahren für Betriebssysteme vorsichtig herangeführt und es werden Ihnen die entsprechenden Grundlagen vermittelt. Sie erlernen die wichtigsten Fachbegriffe im Zusammenhang mit diesem Studienheft und lernen einige praktische Beispiele kennen.

Nach der Durcharbeit des ersten Kapitels ist bei Ihnen hoffentlich das Interesse für die Bedrohungen und den Umgang mit ihnen geweckt.

Haben Sie sich schon einmal die Frage gestellt, wie z. B. Ermittlungsbehörden es schaffen können, die „Online-Durchsuchungen“ mit richterlichem Beschluss auf Rechnern durchzuführen, ohne dass der Benutzer es merkt?

Oder haben Sie sich schon einmal gefragt, wie es dazu kommen kann, dass Bankkonten plötzlich abgeräumt wurden, ohne dass man selbst die Überweisung getätigt hat?

Dann bekommen Sie hier vielleicht ein paar Ideen, wie das genau passieren kann.

Es gibt viele Möglichkeiten, Zugang zu Betriebssystemen zu bekommen, um Aktionen durchzuführen, die der Benutzer eigentlich nicht wünscht. Zum Glück gibt es aber auch in den modernen Betriebssystemen viele Techniken, die genau das verhindern wollen/sollen oder die Ausmaße der entstehenden Schäden eindämmen können.

1.1 Begriffe

Wahrscheinlich kennen Sie einige der in diesem Kapitel erläuterten Begriffe bereits aus anderen Studienheften. Wenn dem so ist, können Sie diesen Absatz guten Gewissens überschlagen.

Der wahrscheinlich wichtigste Begriff in diesem Zusammenhang ist der der Schwachstelle:

Definition 1.1:

Im Englischen wird der Begriff „vulnerability“, also Verletzlichkeit, verwendet. Ein Objekt ist dort verletzlich, wo es eine Schwachstelle (weakness) hat. Eine Schwachstelle ist eine sicherheitsrelevante Unzulänglichkeit eines Objektes (ein System oder eine Institution), sodass das Objekt verwundbar, das heißt anfällig für Bedrohungen ist.[1]

Von Schwachstellen sprechen wir insbesondere bei Fehlern innerhalb einer Software, die man für Angriffe mittels eines Exploits ausnutzen kann, oder aber auch im Zusammenhang mit Sicherheitseinstellungen, die umgangen werden können.

Definition 1.2:

Ein Angriff (attack) ist eine (absichtliche) Aktivität, um Systeme oder Daten zu kompromittieren. Mit dieser vorsätzlichen Form der Gefährdung werden unerwünschte oder unberechtigte Handlungen mit dem Ziel ausgeführt, sich Vorteile zu verschaffen oder das Opfer oder auch Dritte zu schädigen.[2]

1. Definition aus Heft EIS02
2. Definition aus Heft EIS02

Ein willentlicher Akt eines Angriffs setzt voraus, dass mehr oder weniger wirksame Sicherheitsmaßnahmen umgangen werden (bzw. dies zumindest versucht wird).[3]

Ziel von Angriffen ist es in der Regel,

- Zugriffe auf Informationen zu erlangen,
- Daten zu manipulieren,
- Datensätze anzulegen,
- Dienste einzuschränken.

Definition 1.3:

Unter einem Exploit versteht man einen Programmcode zur Ausnutzung einer Schwachstelle.

Mittels Tools wie beispielsweise Metasploit können Exploits automatisiert gegen Systeme angewandt werden, d.h., auf Knopfdruck werden bekannte Schwächen ausgenutzt, sodass eine Automation möglich ist. Entsprechende grafische Oberflächen wie z.B. Armitage[4] (vgl. Abb. 1.1) ermöglichen selbst weniger erfahrenen Benutzern die Anwendung von Exploits gegen andere Rechnersysteme.

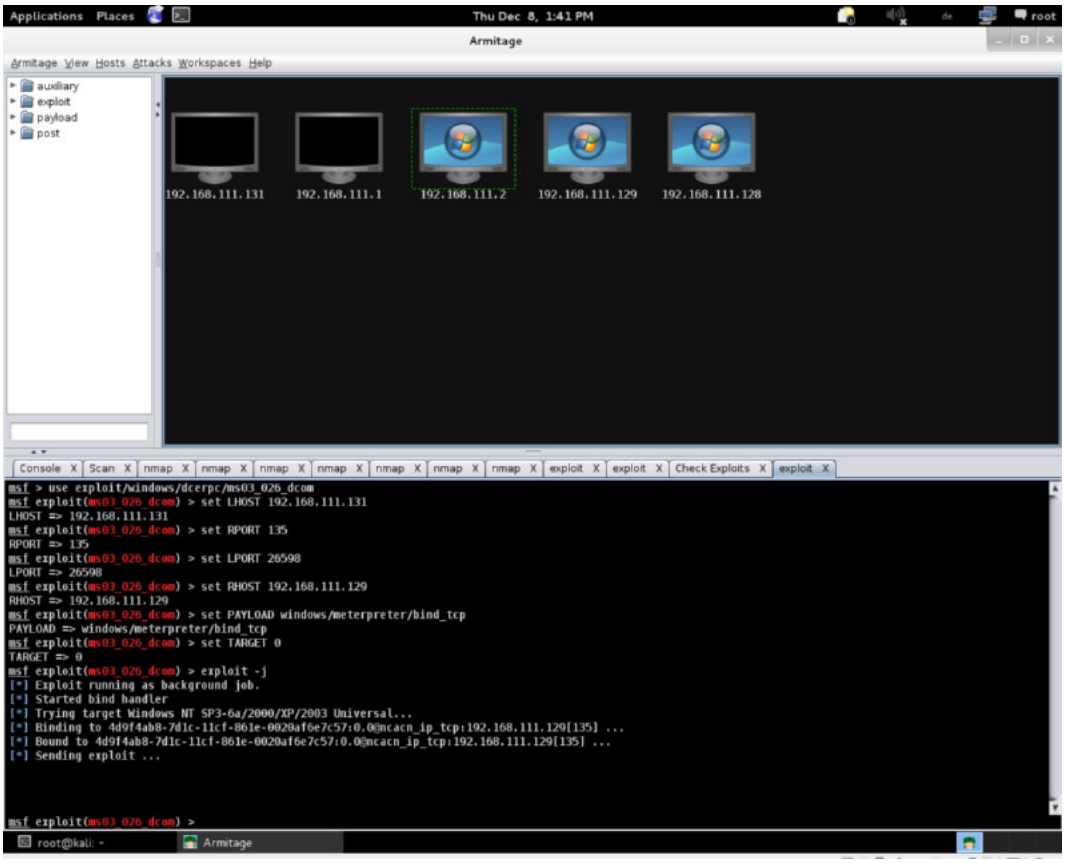

Abb. 1.1: Armitage

3. Kossakowski, 2000, Incident Response Capabilities, S. 9.
4. Oberfläche für Metasploit, z.B. enthalten im Penetrationstest Linux „Kali“, siehe http://www.kali.org.

Genau diese Automation eröffnet nahezu unbegrenzte Möglichkeiten für Angreifer. Sind Exploits erstellt, können (und werden) diese gegen Ziele im Internet eingesetzt. Insbesondere im Umfeld von Botnetzen kann so die Anzahl der aktiven Bots deutlich erhöht werden.

Definition 1.4:

Ein Botnetz ist ein Verbund von infizierten Rechnern, den sogenannten Bot-Rechnern, die miteinander kommunizieren und meist durch einen zentralen Server kontrolliert und ferngesteuert werden.[5] Diese Steuerungsinstanz bezeichnet man als Command and Control Server.

Gerade in der Kombination der automatisierten Anwendung von Exploits gegen das sogenannte Internet of Things (IoT) entsteht für Botnetze eine neue Qualität und Leistungskraft. Bot-Clients können so auf einer Vielzahl von Geräten installiert und anschließend genutzt werden. Der Vorteil von Bots auf Basis von IoT liegt insbesondere darin, dass es sich oftmals um „Haushaltsgeräte“ wie Babyphone, Fernseher, Überwachungskameras oder ähnliche Geräte handelt. Diese Geräte sind weder im Fokus ihrer Besitzer noch werden sie von den Herstellern mit einem besonderen Augenmerk für die Informationssicherheit betrachtet. Oder wann haben Sie das letzte Mal einen Betriebssystem-Patch für Ihr Babyphone installiert?

Beispiel 1.1:

Im Oktober 2016 hat das Mirai-Botnetz, bestehend aus rund 400 000 IoT-Geräten, einen massiven Angriff gegen einen DNS-Anbieter gefahren. Dieser führte unter anderem auch für sehr große Websites wie z.B. Twitter, Spotify oder GitHub zu einer Unerreichbarkeit.[6] Es wird geschätzt, dass die Gesamtangriffskapazität des Botnetzes über 1,5 Terrabit/Sekunde verfügt.

1.2 Praxisbeispiele

Verfolgt man die Fachpresse, so muss man leider feststellen, dass jeden Tag neue Schwachstellen gemeldet werden und es immer wieder zu erfolgreichen Ausnutzungen von Schwachstellen kommt.

Der Grund für den Erfolg liegt auf der Hand: Jedes Betriebssystem hat Fehler, die man bei geschickter Verwendung für unerwünschte Zwecke missbrauchen kann.

An dieser Stelle sollten Sie sich mit dem Gedanken anfreunden, dass bereits viele Geräte kleine Computer mit ▸CPU, Arbeitsspeicher und einem Betriebssystem sind. So finden Sie beispielsweise in gängigen Flachfernsehern das Betriebssystem Android, auf Internet-Routern in der Regel ein Linux-Derivat usw. Dazu kommen die Smartphones und Tablets mit Windows, IOS oder Android und vieles mehr. In unserer alltäglichen Welt sind Sie umgeben von Computersystemen – von Rechnersystemen, die im Sinne der Informationssicherheit Integrität, Vertraulichkeit und Verfügbarkeit aufweisen sollten.

Ein weiterer Punkt, den Sie gedanklich im Hinterkopf behalten sollten, ist, dass es meistens nur um Geld geht. Cyberkriminalität hat sich in Deutschland zu einem Geschäft entwickelt, mit dem ein größerer Umsatz als mit Drogen erzielt wird.

5. Definition IT-Sicherheit Eckert, 2014
6. Vgl. http://www.zdnet.de/88283474/mirai-botnet-mit-ueber-400-000-iot-bots-zu-vermieten/.

Allein im Jahr 2016 ist es zu zahlreichen Vorfällen gekommen, die von ihrer Dimension besorgniserregend waren.

Beispiel 1.2:

November 2016: „Bankräuber“ erbeuten in einem ausgeklügelten Hack knapp 30 Mio. € von der russischen Zentralbank. Bereits im Mai 2016 wurden bei einem ähnlichen Delikt 81 Mio. US-$ in Bangladesch erbeutet.

Aber nicht nur die großen Schlagzeilen sollten uns wachrufen, auch kleine Vorfälle können für den Einzelnen schmerzliche Erfahrungen bedeuten.

Beispiel 1.3: Vertraulichkeit

Überwachungskameras für den Schutz des Eigentums kommen in Deutschland mehr und mehr in Mode. In großen Discount-Märkten gab es entsprechende Modelle zu kaufen, die Einzug in viele deutsche Haushalte nahmen. Eines der deutschen Landeskriminalämter suchte nach frei erreichbaren Kameras und schickte Streifenwagen zu den entsprechenden Haushalten, um die Besitzer darüber zu informieren, dass sie sehr vertrauliche Bilder ins Internet senden.

Übung 1.1:

Besuchen Sie im Internet die Suchmaschine shodan.io. Es handelt sich um eine Suchmaschine für das IoT. Wenn Sie dort nach dem String „mcdhttpd“ suchen, finden Sie einige der besagten IP-Überwachungskameras.

Neben den bis hierher genannten Beispielen gibt es eine Vielzahl von Angriffen auf die Verfügbarkeit von Systemen. Diese sogenannten ▸DoS oder ▸DDoS-Angriffe werden entweder zielgerichtet genutzt, um Seiten oder Dienstleistungen lahmzulegen oder aber in Verbindung mit einer Erpressung („Entweder Sie zahlen oder wir greifen Sie an“) ausgelöst. Aktuell (2016) ist ein Anstieg dieser Angriffe zu verzeichnen gewesen.

Aus diesem Grund bieten große Telekommunikationsdienstleister inzwischen entsprechende Schutzmechanismen an, um beispielsweise schadhaften (DDoS) Traffic bereits auf dem Backbone herauszufiltern. Dies ist in Deutschland allerdings immer erst nach Rücksprache mit dem angegriffenen Anschlussinhaber möglich, da grundsätzlich ein Eingriff in den Datenverkehr verboten ist.

Die Telekommunikationsunternehmen haben im Rahmen der hauseigenen Cyber Defence Center sehr wohl einen recht genauen Blick auf die im Netz stattfindenden Angriffe, dürfen aber in der Regel nicht einschreiten. Eingriffe sind nur mit Einwilligung der betroffenen Kunden möglich bzw. wenn die Telekommunikationsunternehmen selbst angegriffen werden bzw. deren Infrastruktur bedroht ist.

Beispiel 1.4:

Ein Beispiel für einen großflächigen Angriff gegen die Deutsche Telekom gab es Ende November 2016. Hier wurden Internet-Router in Privathaushalten angegriffen. Rund 900 000 Kunden der Telekom hatten deswegen zeitweise keinen Internetzugang.

1.3 Risikofaktoren

Betrachtet man die Risikofaktoren, die es möglich machen, dass die Sicherheit von Systemen gefährdet wird, so kann man grundsätzlich zwischen dem Risikofaktor Mensch und dem Risikofaktor Maschine unterscheiden.

Hinsichtlich des Menschen gilt, dass zum einen Fachwissen, zum anderen die Motivation entscheidend sind. Es sollte dem Betreiber von Systemen daran gelegen sein, die Mitarbeiter gut ausgebildet zu halten und in ihrer Arbeit zu motivieren. Aus einem unmotivierten Mitarbeiter kann ganz leicht ein sogenannter Innentäter werden, der den sicheren IT-Betrieb gefährdet.

Beispiel 1.5:

Ein Mitarbeiter eines großen IT-Hauses war innerhalb seiner Firma nicht gut gelitten und so suchte die Firmenleitung nach „Fluktuationsmotivatoren“, um ihn zu einer selbst initiierten Kündigung zu bewegen. In seinem Arbeitsvertrag stand als Einsatzort: jeder Standort in Deutschland. Dieser Administrator wohnte und arbeitete eigentlich in Trier. Man fand heraus, dass der Standort Stralsund verkehrstechnisch am schlechtesten aus Trier zu erreichen wäre, und so wurde der Mitarbeiter kurzerhand dorthin versetzt. Die Konsequenz: Er kündigte.

Mitarbeiter, denen ähnliche Situationen widerfahren wie im o. g. Beispiel, können durch eine Rache-Motivation eine Gefahr für den Betrieb darstellen.

Eine weitere Gefährdung auf der menschlichen Ebene ist die Ausnutzung von Mitarbeitern im Sinne von Social Engineering bzw. durch professionelle Tätergruppen (vgl. Abschnitt 2.2.1).

Die technischen Schwächen beziehen sich auf Fehler innerhalb der Architektur, der Implementierung oder des eigentlichen Programmcodes. Grundsätzlich sind diese Punkte sicherlich auch ursprünglich auf menschliche Fehler zurückzuführen, aber innerhalb unserer Betrachtung wollen wir sie als technische Risikofaktoren betrachten.

An erster Stelle sind hierbei insbesondere die Schwachstellen zu nennen. Hierbei ist es unerheblich, ob es sich um Schwachstellen innerhalb der Virtualisierungsplattform, des Betriebssystems, der Middleware oder der eigentlichen Applikation handelt. Jede Ebene ist vom Grundsatz her verwundbar, da ein fehlerfreier Programmcode praktisch ausgeschlossen werden kann.

Neben den ausnutzbaren Schwachstellen können Programmierfehler aber auch zu unerwartetem Verhalten oder im Extremfall zu einem kompletten Systemversagen führen.

Klassische Architekturrisiken liegen beispielsweise in der Verfügbarkeit. Sind keine Redundanzen geplant, so ist eine Hochverfügbarkeit nicht zu gewährleisten (vgl. SRN01).

1.4 Grundlagen

Die wichtigste Erkenntnis im IT-Betrieb ist, dass eine absolute Sicherheit niemals gegeben sein kann. Behalten Sie dies immer im Hinterkopf und machen Sie sich Gedanken über die Notfallvorsorge!

Die gute Nachricht an diese Stelle ist: Es haben sich schon sehr viele qualifizierte Menschen Gedanken darüber gemacht, wie man einen möglichst sicheren Betrieb entwerfen und umsetzen kann.

Für den Betrieb im Allgemeinen beschreibt die Information Technology Infrastructure Library (▸ITIL) in einem Werk aus fünf Bänden sehr genau, welche Prozesse für einen erfolgreichen Betrieb erforderlich sind. Der technische Part hiervon ist im Buchtitel „Service Operation[7]“ beschrieben.

Aus der ISO 27002 lassen sich einige abstrakt beschriebene Maßnahmen ableiten, die man für die Gewährleistung eines sicheren Betriebs berücksichtigen sollte. Die hier genannten Punkte bieten keine konkreten Vorgaben oder Handlungsanweisungen, sondern beziehen sich auf die Punkte, die aus Managementsicht berücksichtigt werden sollten, d. h., es geht um das Was, nicht um das Wie.

Konkreter gefasst ist an dieser Stelle der Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (▸BSI). In den Katalogen des Grundschutzes werden konkrete Maßnahmen beschrieben, wie man die Sicherheit von Systemen gewährleisten bzw. erhöhen kann.

Zusammenfassung

Sie haben nun einige Gefährdungen kennengelernt und verstanden, dass es sich nicht nur um abstrakte Bedrohungen, sondern um konkrete Gefahren handelt. Die Notwendigkeit, sich mit dem Thema Sicherheit im IT-Betrieb zu befassen, sollte Ihnen anhand der Beispiele deutlich geworden sein.

Ebenso sollten Sie nun in der Lage sein, wichtige Begriffe zuzuordnen, und Einstiegspunkte für die Informationssicherheit im Betrieb kennen.

Aufgaben zur Selbstüberprüfung

1.1 Beschreiben Sie in eigenen Worten, was Sie unter einem Exploit verstehen.

1.2 Erläutern Sie bitte, warum der Bereich IoT in Bezug auf Botnetze eine große Gefahr darstellt.

7. Vgl. Taylor et al., 2007.

2 Betriebssysteme

Dieses Kapitel beschäftigt sich mit verschiedenen Betriebssystemen und generellen Maßnahmen zur Absicherung von IT-Systemen. Sie werden verstehen, welche Angriffsvektoren es gibt, und Gegenmaßnahmen dazu lernen. Darüber hinaus werden Sie weitere Problemstellen im Zusammenhang mit dem Betrieb kennenlernen.

Sie lernen einige konkrete Angriffe kennen und werden im Anschluss an die Bearbeitung des Kapitels verstanden haben, dass das Konzept von Benutzername und Passwort kein zukunftsträchtiges Konzept sein kann.

Starten wir mit einer Definition:

Definition 2.1:

Ein Betriebssystem umfasst die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften der Rechenanlage die Grundlage der möglichen Betriebsarten des digitalen Rechensystems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen.[8]

Gefühlsmäßig könnte man die Auffassung vertreten, dass es früher (vor 2000) eine deutlich höhere Anzahl an Betriebssystemen gegeben hätte als heute, z. B. BS2000, AS400, OS/2, Windows, PCM, UNIX(e) etc., während sich heute alles auf die Klassen Linux, Windows und IOS zu konzentrieren scheint. Oberflächlich mag das richtig sein, taucht man allerdings tiefer in die Materie ein, stellt man fest, dass jedes der Systeme eine große Zahl an unterschiedlichen Derivaten mit sich bringt und der Einsatzzweck sehr breit gefächert ist.

Beispiel 2.1:

Linux ist der gemeinsame Nenner für viele Server- und Client-Systeme. Gleichzeitig ist Linux aber auch eine Grundlage für IOS gewesen. Auch Android basiert auf einem Linux. Schaut man sich Android an, stellt man fest, dass es in den unterschiedlichsten Versionen auf Mobiltelefonen und auch Fernsehern zum Einsatz kommt.

Viele Haushaltsgegenstände besitzen oder sind heute kleine Computer. Seien es nun die Überwachungskameras, die vor Einbrechern warnen sollen, die Zugangsrouter zum Telekommunikationsprovider, das Babyphone, das am Gitterbettchen steht, oder zukünftig vielleicht auch der Kühlschrank, der automatisch die Milch nachbestellt, wenn Sie die letzte Flasche entnommen haben.

Hinzu kommen die technischen Umgebungen innerhalb von Produktionsstätten, wie Industrieanlagensteuerungen, Pumpwerke, Verkehrsleittechnik oder ähnliche Systeme.

All dies gilt es zu betrachten, wenn wir uns Gedanken über den sicheren Betrieb einer Umgebung machen wollen.

8. Deutsches Institut für Normung (DIN 44300).

2.1 Grundlagen

Die Aufgabe eines Betriebssystems liegt in der Verwaltung und Steuerung der zugrunde liegenden Hardwarekomponenten, wie Arbeitsspeicher, Prozessor, Speichersysteme, Tastatur, Grafikprozessoren usw. Diese Verwaltungseinheit stellt den darüberliegenden Programmen diese Betriebsmittel auf fest definierten Wegen zur Verfügung. Andrew S. Tanenbaum beschreibt dies mit den Worten: „Die Aufgabe des Betriebssystems ist es, den Benutzerprogrammen ein besseres, einfaches, klares Modell des Computers zur Verfügung zu stellen und außerdem die genannten Ressourcen zu steuern.“[9]

Insgesamt kann man ein Rechnersystem in verschiedene Ebenen (oder Ringe – je nach Darstellungsform) aufteilen. Zur Vereinfachung betrachten wir innerhalb dieses Studienhefts den Aufbau wie in Abb. 2.1:

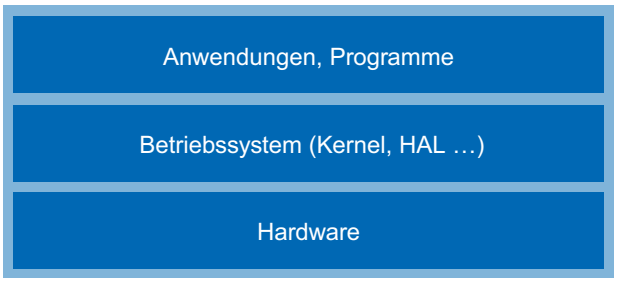

Abb. 2.1: Aufbau Betriebssystem

Ziel dieses Aufbaus ist es, dass grundsätzlich jedes Programm so laufen soll, als ob es das einzige Programm auf dem System wäre, d. h., die Programme untereinander dürfen sich weder sehen noch beeinflussen können. In der Praxis bedeutet dies, dass der Zugriff auf die jeweiligen Adressräume anderer Applikationen verboten sein muss.

Die Software darf auch ausschließlich auf die Komponenten zugreifen, die vom jeweiligen Betriebssystem zur Verfügung gestellt werden. Diese Zugriffe werden dann hinsichtlich ihrer Rechte auch durch das Betriebssystem beschränkt. Ein direkter Zugriff auf die Hardware soll auf keinen Fall erfolgen.

Zu den wesentlichen Aufgaben des Betriebssystems zählen insbesondere:

- Abstraktion von der Hardware
- Steuerung von Prozessen
- Zuteilung der Ressourcen (Hardware) an die unterschiedlichen Programme und Prozesse
- Schutzmechanismen der Programme untereinander

Definition 2.2:

Ein Programm ist eine statische Folge von Anweisungen in einer Programmiersprache unter der Nutzung von Daten. Es dient zur Codierung eines Algorithmus und liegt im Allgemeinen in Form einer Datei vor.[10]

9. Vgl. Tanenbaum, 2009.
10. Definition von Günther Hellberg, Fachhochschule für die Wirtschaft in Hannover.

Definition 2.3:

Ein Prozess (Task) ist eine dynamische Folge von Aktionen (Zustandsänderungen), die durch Ausführung eines Programms auf einem Prozessor zustande kommt. Ein Prozess ist insbesondere durch seinen zeitlich veränderlichen Zustand gekennzeichnet. Er wird im Betriebssystem infolge eines Auftrags erzeugt.[11]

Der Punkt der Steuerung von Prozessen gilt in diesem Zusammenhang nur für sogenannte Multitasking-Systeme, d. h. Betriebssysteme, die in der Lage sind, mehrere verschiedene Aufgaben (pseudo) parallel zu verarbeiten. Im Gegensatz dazu gibt es – oder besser gab es in der Vergangenheit – die Singletasking-Systeme, wie z. B. MS DOS.

Ein weiteres Unterscheidungsmerkmal im Bereich der Betriebssysteme ist die Anzahl der gleichzeitigen Benutzer an einem System. Die sogenannten Single-User-Systeme verfügen über keine Benutzerverwaltung und ermöglichen nur einem einzigen Benutzer zur gleichen Zeit die Verwendung. In diese Kategorie fallen insbesondere die ehemaligen Betriebssysteme MS DOS, Windows 95 etc.

Mehrbenutzersysteme (Multi-User-Systeme) dagegen haben eine Benutzerverwaltung und erlauben die gleichzeitige Benutzung durch unterschiedliche Anwender. Klassiker in diesem Umfeld sind die verschiedenen UNIX-Derivate, OS/390, BS2000, aber auch die aktuellen Windows-Server.

2.1.1 Kernel

Der Kernel wird teilweise mit dem Betriebssystem gleichgesetzt. Streng genommen handelt es sich allerdings beim Kernel nur um den zentralsten Teil des Betriebssystems. In früheren Zeiten war die Betrachtung Kernel = Betriebssystem sicherlich treffender, heute allerdings werden mit dem sogenannten Betriebssystem direkt viele zusätzliche Funktionalitäten, Apps und Softwarebestandteile mitgeliefert, sodass wir uns den Kernel an dieser Stelle einmal genauer anschauen werden.

Die wesentlichen Aufgaben des Kernels sind Verwaltungsaufgaben hinsichtlich

- Speicher
- Prozessen
- Peripherie
- Dateisystem

sowie die eigentliche Verbindung zur grundlegenden Hardware.

Dementsprechend sollte klar sein, dass der Kernel die weitestgehenden Rechte auf einem Computersystem besitzt. Die Rechte liegen noch oberhalb der Rechte, die ein Systemadministrator sein Eigen nennt.

Die Programmierer von Schadsoftware werden daher, wenn es ihnen möglich ist, versuchen, ihren Code im Rahmen des Kernels ausführen zu lassen, da er sich hier ideal verbergen lässt und den größten Nutzen (aus Sicht der Schadsoftwareentwickler) stiften kann.

11. Definition von Günther Hellberg, Fachhochschule für die Wirtschaft in Hannover.

Beispiel 2.2:

Ein Beispiel für Schadprogramme auf Ebene des Systems sind die sogenannten Kernel-Root-Kits. Meist handelt es sich hierbei um Trojaner, die Backdoors zu einem System eröffnen. Als Kernel-Root-Kit werden dabei Systemrechte ausgenutzt, die es unter anderem möglich machen, auch von aktuellen Antivirenprogrammen nicht erkannt zu werden, da sie – bildlich gesprochen – unterhalb des Radars fliegen.

Generell bieten Betriebssysteme heute von Haus aus einen gewissen Schutz vor solchen Programmen, da ein direkter Zugriff durch Programme unterbunden wird. Allerdings existieren in jedem Betriebssystem Fehler. Bei geschickter Ausnutzung dieser Programmierfehler lassen sich auch heute noch Schadprogramme erstellen, die auf Betriebssystemebene ablaufen.

2.1.2 Treiber

Treiber sind Softwareprodukte zur Steuerung der Hardware. Der Begriff Gerätetreiber macht dies ein bisschen deutlicher. Es handelt sich um kleine Anwendungen, die dem Betriebssystem (und darauf aufsetzenden Programmen) die Kommunikation mit (teilweise exotischer) Hardware ermöglichen. Da diese Softwarekomponenten sehr direkt mit der Hardware kommunizieren und eine virtuelle Schnittstelle bilden, laufen Treiberprogramme mit sehr weit gehenden Rechten auf einem Computersystem. Sie werden – je nach Auslegung – sogar als Teil des Betriebssystems gesehen, obwohl sie meist von anderen Herstellern als von dem des Betriebssystems kommen.

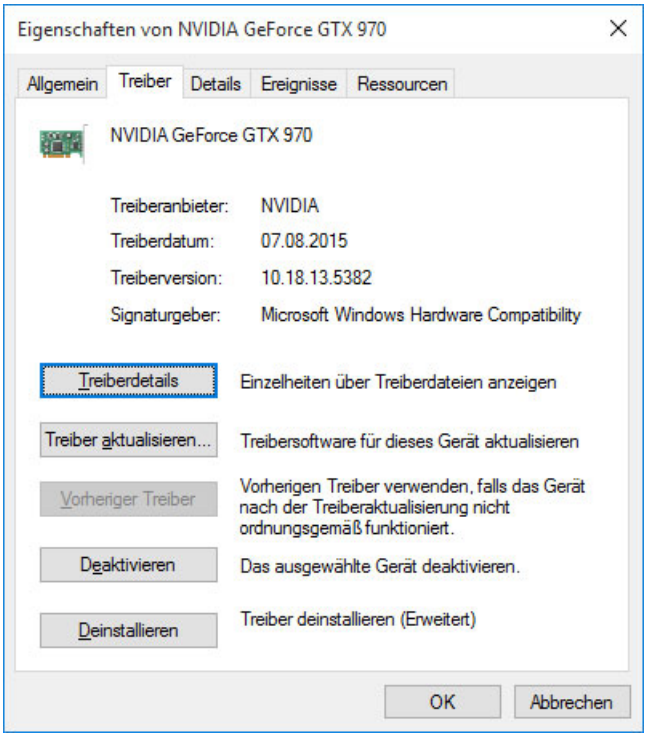

Abb. 2.2: Gerätetreiber in Windows

Abb. 2.2 zeigt ein Beispiel für einen Grafiktreiber unter Windows 10. Die Treibersoftware kommt von NVIDIA und nicht von Microsoft.

Neben den speziellen Treibern für bestimmte Hardwarebauteile gibt es auch die sogenannten Klassentreiber. Diese sind weitestgehend unabhängig vom Hardwarehersteller. Oft findet man diese Treiber im Bereich der Ansteuerung von Druckern oder für einfache Grafikkarten.

Die Berechtigung für die speziellen Treiber liegt meist in der Leistungsfähigkeit.

Bei der Auswahl von Treibern sollten Sie sich in kritischen Umgebungen bewusst machen, dass es nicht unbedingt sinnvoll ist, den neusten Beta-Treiber auszuwählen, um ein Quäntchen Performance herauszuholen und dabei die Stabilität aufs Spiel zu setzen.

Weiterhin ist es wichtig, sich Gedanken über den Ursprung der Treiber zu machen. Installieren Sie nur Treiber vom Hardwarehersteller und nicht von anderen dubiosen Webseiten.

Um sicherzugehen, dass nur „ordentliche“ Treiber, die nicht die Stabilität des Gesamtsystems gefährden, installiert werden, hat beispielsweise Microsoft die Signatur von Treibern eingeführt. Eine Installation von nicht signierten Treibern sollte daher vermieden werden.

Beispiel 2.3:

Beim routinemäßigen Austausch von Endgeräten in einem Unternehmen, der alle 4 Jahre erfolgt, musste man feststellen, dass einige Peripheriegeräte unter Windows 10 nicht funktionstüchtig waren, da es keine aktuellen Treiber gibt. Im Wesentlich handelte es sich um Drucker. Es stellte sich somit folgende Fragen:

1) Will man den Personalaufwand investieren, mit alten Treibern zu experimentieren, in der Hoffnung, die alte Hardware zum Laufen zu bringen?
2) Will man das Risiko einer Systeminstabilität wegen eventueller Software-Inkompatibilitäten eingehen?

   Oder aber ist es ggf. kosteneffektiver, neue, unterstützte Drucker anzuschaffen?

Will man eine stabile Systemumgebung haben, muss man sich mit Fragestellungen wie im obigen Beispiel beschäftigen.

2.1.3 Anwendungen

Anwendungen setzen erst auf der virtuellen Schicht auf, die das Betriebssystem zur Verfügung stellt. Die einzelnen laufenden Anwendungen sind in modernen Betriebssystemen hinsichtlich ihrer Rechte, Speicherzugriffe und Möglichkeiten zur direkten Einflussnahme auf das Betriebssystem und andere Anwendungen stark eingeschränkt.

Das Ziel von Anwendungen – auch Programme genannt – kann sehr unterschiedlich sein. Sie kennen sicherlich alle Programme zur Textverarbeitung oder Tabellenkalkulation. Aber auch Spiele und kleine Tools, wie z. B. Compiler oder Editoren, fallen unter die Kategorisierung Anwendungen. Sie alle erfüllen einen Spezialzweck, für den sie auf Ressourcen eines Computers (Hauptspeicher, Prozessor, Festplatte etc.) zugreifen müssen. Diese Zugriffe werden ihnen nur durch das Betriebssystem zu dessen Bedingungen gewährt.

Diejenigen von Ihnen, die noch mit Windows 3.11 gearbeitet haben, können sich vielleicht noch daran erinnern, dass man mit einer fehlerhaften Software den kompletten Computer zum Absturz bringen konnte.

Dank des virtuellen Aufbaus in unterschiedlichen Schichten ist ein solches Softwareverhalten heutzutage nahezu ausgeschlossen.

2.1.4 Daten

Bei Daten (oder Informationen) handelt es sich um die Objekte der eigentlichen Verwaltung durch Rechnersysteme. Computer sollen uns helfen, Alltagsprobleme besser oder schneller zu lösen. Diese Alltagsprobleme werden in der Regel durch Daten repräsentiert.

Beispiel 2.4:

Im einfachsten Fall können Daten z.B. die Einnahmen und Ausgaben eines Haushalts sein. Diese kann man in einem Haushaltsbuch händisch erfassen und am Ende des Monats aufaddieren oder aber man benutzt hierfür eine Tabellenkalkulation, die die Auswertung auf den ersten Blick und somit ein jederzeitiges Bild des persönlichen Finanzstatus liefert. Die Daten in diesem Fall sind die Zahlen und Infos rund um Einnahmen und Ausgaben.

Diese Daten werden in Form von Dateien auf einem Rechner abgelegt. Sie können in Klartext lesbar sein (z.B. TXT-Dateien) oder aber jeweils spezielle Anwenderprogramme erfordern.

Auch Bilder, Videos und Audiodateien sind Daten.

In Bezug auf Informationen, die im Dateisystem abgelegt sind, nimmt das Betriebssystem über die Rechte- und Rollenkonzepte für Dateisysteme den Schutz der Daten hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität vor.

Neben der Ablage im Dateisystem besteht auch die Möglichkeit, dass sich die Daten in Datenbanksystemen abgelegt befinden. In diesem Spezialfall liegt die Schutzaufgabe innerhalb des Datenbankmanagementsystems, das eine Rechteverwaltung implementiert hat.

2.1.5 Prozesse

Bei einem Prozess unterscheidet man entsprechend dem Kontext zwischen einem Benutzerprozess, der durch eine Anwendung oder den Benutzer initiiert und gesteuert wird, und einem Betriebssystemprozess, der in der Hand des jeweiligen Betriebssystems liegt.

Programme können aus einem oder mehreren Prozessen bestehen. Hierbei erhält jeder Prozess durch das Betriebssystem einen eigenen Speicherbereich zur Verfügung gestellt. Dieser ist in sich getrennt für statische Daten (das Programm selbst) und dynamische Daten.

Die Einflussnahme auf Prozesse kann auf verschiedenen Wegen erfolgen:

- Benutzeraktionen, wie z.B. Kommandos
- Interrupts
- durch andere Prozesse

Ein wichtiges Merkmal von Prozessen ist der jeweilige Zustand, in dem sie sich befinden. Diese Zustände sind in der internen Verwaltung begründet. In den Anfängen des Multitaskings, sprich der quasiparallelen Verwaltung von Prozessen, stand nur eine CPU mit einem Kern zur Verfügung. Um mehrere Tasks (Prozesse) für den Benutzer scheinbar parallel ausführen zu lassen, wurde die Rechenzeit aufgeteilt. In diesem Zusammenhang sprach man von Zeitscheibenmultiplexing. In der Praxis wurde durch das Betriebssystem für einen bestimmten Zeitraum der Speicher und die CPU für einen bestimmten Prozess zur Verfügung gestellt. Nach Ablauf dieser Zeitscheibe kam der nächste Prozess zum Zuge. Hieraus ergeben sich folgende Zustände für Prozesse:

- aktiv
- bereit
- wartend
- nicht vorhanden

Innerhalb des Ablaufs wechseln diese Zustände für die einzelnen Prozesse.

2.1.6 Angriffsvektoren

In der Praxis gelten grundsätzlich ähnliche Angriffsvektoren, die den meisten Administratoren bekannt sind, und trotzdem werden die ursächlichen Schwachstellen oft nicht geschlossen. An dieser Stelle möchte ich Ihnen einige der bekannten Methoden kurz vorstellen. Diese Liste ist nicht abschließend, deckt aber einen Großteil der üblichen Angriffe ab:

- Passwörter

  Passwörter dienen dazu, Systeme vor unbefugten Zugriff zu schützen. Daher sollten Passwörter einige Eigenschaften aufweisen, die ein Erraten oder Ausprobieren vereiteln bzw. erschweren. Oft kommt es vor, dass Systeme mit Default-Passworten weiterbetrieben werden, die in der Dokumentation nachzulesen sind, oder es werden Passwörter verwendet, die in Wörterbüchern zu finden sind (vgl. Tab. 2.1).

Tab. 2.1: Beliebteste Passwörter 2016
(Quelle http://t3n.de/news/beliebteste-passwoerter-deutschland-2016-779732/)

Beliebteste deutsche Passwörter 2016	
Platz	**Passwort**
1	hallo
2	passwort
3	hallo123
4	schalke04
5	passwort1

Beliebteste deutsche Passwörter 2016	
Platz	**Passwort**
6	qwertz
7	arschloch
8	schatz
9	hallo1
10	ficken

Default-Passwörter lassen sich teilweise schon mit automatisierten Schwachstellenscans (wie z.B. mit OpenVAS) erkennen.

Beispiel 2.5:

Das Problem mit den Passwörtern liegt aufseiten des Benutzers. Benutzer neigen dazu, sich einfache Passwörter auszudenken. Beim regelmäßigen erzwungenen Wechsel (z.B. alle drei Monate) kommt es zu Passwörtern wie „Februar2016“, „Mai2016“, „August2016“ ...

Ansonsten wird man häufig auch auf Zetteln (am Monitor, unter der Tastatur, in der obersten Schreibtischschublade ...) fündig.

Zu schwache Passwörter lassen sich mit entsprechenden Tools herausfinden.

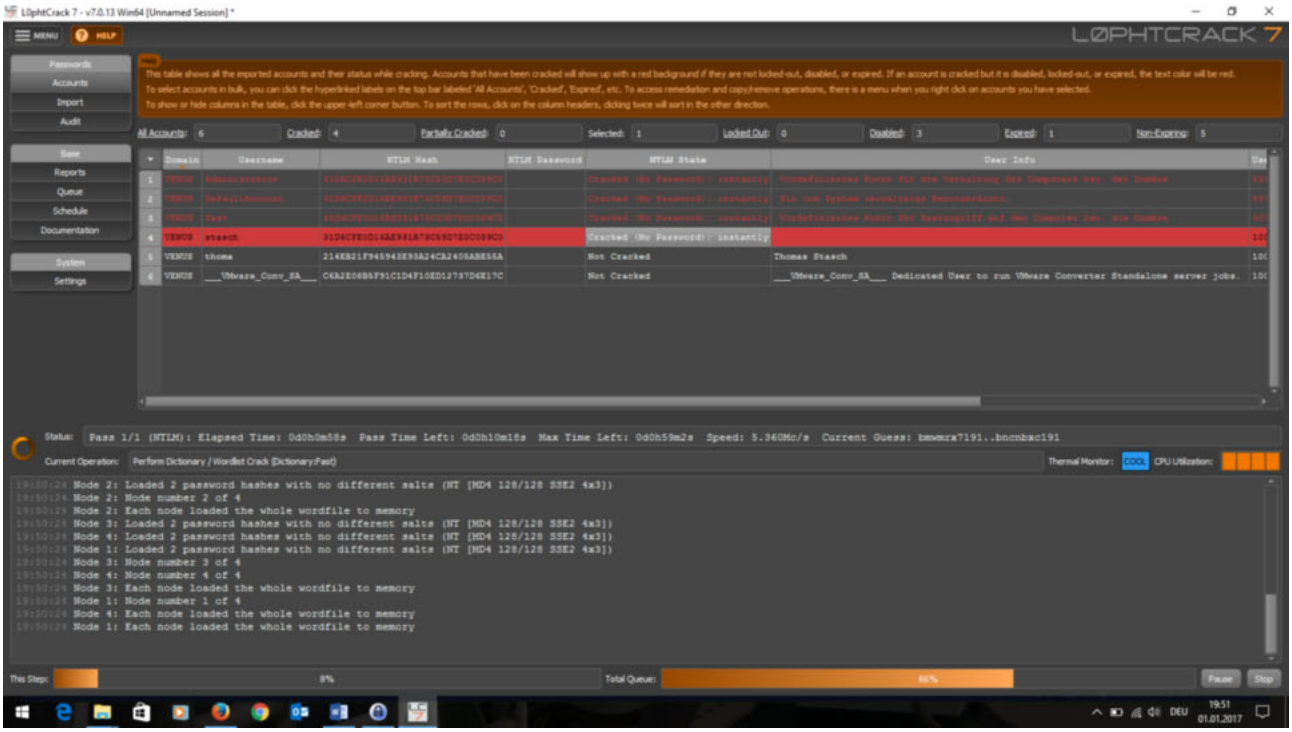

Abb. 2.3: L0phtCrack – Passwort „Auditing“ Tool

Neben den sicherlich bekanntesten wie L0phtCrack (siehe Abb. 2.3) oder John the Ripper gibt es eine Vielzahl an Tools, um Passwörter zu knacken. In den großen Forensik-Suiten sind ebenfalls entsprechende Funktionen integriert.

- Umfangreiche Zugriffsrechte

  In der Informationssicherheit gibt es ein Prinzip, das „Need-to-know-Prinzip" genannt wird. Laut Wikipedia ist es ein grundlegendes Prinzip innerhalb von Geheimdiensten. Es macht allerdings auch sehr viel Sinn, dieses Prinzip innerhalb jedes Unternehmens einzusetzen und zu beachten. Hierbei geht es weniger um das Verschweigen von Informationen als darum, jedem Mitarbeiter die Möglichkeiten zu geben, die er für seine Arbeit benötigt – aber auch nicht mehr.

Beispiel 2.6:

Ein Auszubildender fängt innerhalb eines Unternehmens in der Buchhaltung an und erhält entsprechende Zugriffsberechtigungen auf die Dokumente und Dateien. Nach drei Monaten wechselt er in den Bereich Marketing und erhält Zugriff auf die Dokumente des Marketings etc. Am Ende seiner Ausbildung besitzt er Rechte für die komplette Firma, da ihm nie Berechtigungen entzogen wurden, die er nicht mehr benötigt.

Das Thema Zugriffsrechte bezieht sich in diesem Zusammenhang nicht ausschließlich auf Dateifreigaben. Auch der Zugriff auf einzelne Anwendungen, Webservices etc. ist zu beachten.

Neben dem generellen Zugriff muss man sich auch die Frage stellen, wie weitreichend Rechte erteilt werden müssen. Reicht es, dass ein lesender Zugriff freigegeben wird oder sind auch Schreibberechtigungen notwendig?

Je mehr Rechte ein Benutzer hat, desto mehr kann auch mit der Kennung – im Fall eines erfolgreichen Angriffs – angerichtet werden.

- Fehlende Authentisierung

  Ein gravierender Fehler liegt vor, wenn es Zugänge zu kritischen Informationen gibt, ohne dass überhaupt eine Authentisierung erfolgt ist.

Beispiel 2.7:

Ein Vermessungsunternehmen hat auf seiner eigenen Webseite in einem Unterverzeichnis ein PDF-Dokument liegen gehabt, in dem der Zugang zu mehreren städtischen Katasterämtern mit Passwörtern und nötiger Software beschrieben stand. Die Offenlegung dieser Informationen ist nur durch Zufall aufgefallen. Infolge dieses Sicherheitsvorfalls entstand ein wirtschaftlicher Schaden, weil jede betroffene Kommunalverwaltung die Zugangsdaten ändern musste und eine Prüfung auf unberechtigte Nutzung durchgeführt wurde.

Informationen auf Webseiten sind – sofern keine Benutzer-Authentisierung erfolgt – generell als öffentlich anzusehen. Darüber hinaus kommt es in der Praxis auch oft genug vor, dass Software installiert wird und man ein Benutzer-/Rollenkonzept nach dem ersten Test einführen will. Ist der Test abgeschlossen, gerät der Gedanke in Vergessenheit. Infolgedessen kann jeder Benutzer auf die entsprechende Software und die darin verarbeiteten Daten zugreifen.

- Unnötige Dienste

  Dieser Punkt gerät dank der Sensibilisierung für die Informationssicherheit langsam in den theoretischen Ansatz zurück. Bis vor einiger Zeit waren die Installationsroutinen von Betriebssystemen so ausgelegt, dass nach der Installation das System verschiedenste Aufgaben ausführen konnte, ohne dass man zusätzliche Funktionen aktivieren musste. Sie waren per default (Standard-Einstellung) bereits aktiviert.

  So bekam man beispielsweise bei der Installation von Linux-Systemen direkt ein funktionsfähiges Samba wie auch einen Apache mitgeliefert – egal ob das System denn überhaupt für Dateifreigaben oder Webdienste genutzt werden sollte.

  Inzwischen hat sich der Standard dahin entwickelt, dass ein neu aufgesetztes Serversystem in der Regel gar keine Dienste mehr installiert und aktiviert hat. Benötigt man dann z.B. einen Webserver unter Linux, so muss man Apache zuerst installieren.

  Nichtsdestotrotz sollte jedes Rechnersystem – egal ob Server oder Client – dahingehend überprüft werden, ob Dienste installiert oder gar aktiviert sind, die nicht benötigt werden.

  Hintergrund hierfür ist, dass jede Softwarekomponente zusätzliche Risiken durch mögliche Schwachstellen birgt. Mit sinkender Anzahl der aktivierten Softwarekomponenten vermindert man das Risiko der Ausnutzung von Schwachstellen.

- Unsichere Systemkonfiguration

  Als unsichere Systemkonfiguration gilt generell jeder Fehler, der Sicherheitsmechanismen aushebelt oder deaktiviert.

2.2 Benutzerverwaltung

Jedes System hat einen Benutzer, der alle administrativen Rechte des Systems besitzt. Unter Windows lautet die Kennung in der Regel „Administrator“, unter Linux/UNIX in der Regel „root“. Dabei müssen Sie berücksichtigen, dass auch anderen Benutzern die gleichen Rechte zugeteilt werden können bzw. die Usernamen verändert werden können.

Anhand der SID (Windows) oder UID (Linux) lassen sich die Hauptadministratoren allerdings leicht erkennen. So hört die SID des Administrators mit dem Wert 500[12] auf. Bei Linux besitzt der Superuser (root) die UID 0.

Für jede Person, die an einem Rechner arbeitet, ist eine eigene Benutzerkennung anzulegen. Kennungen, die von mehreren Personen genutzt werden, sind zu vermeiden!

Hintergrund für diese strikte Regelung ist das Sicherheitsziel der Integrität, das auch eine Zurechenbarkeit beinhaltet, sprich es muss klar sein, wer Daten verändert hat. Dies ist nicht zu gewährleisten, wenn mehrere Personen mit der gleichen Kennung arbeiten.

12. Vgl. https://support.microsoft.com/de-de/kb/243330.

2.2.1 Personalauswahl

Im Bereich der Administration gilt es eine sehr genaue Personalauswahl zu treffen. Leider ist es heute so, dass in der Regel nur die fachlichen und sozialen Fähigkeiten innerhalb der Personalauswahl berücksichtigt werden. Lediglich bei Einstellungen im Bereich von Sicherheitsorganisationen (z.B. Bundeswehr, Nachrichtendienste) erfolgen zusätzliche Prüfungen.

Administratives Personal hat von der Aufgabenstellung her weitgehende Befugnisse und Berechtigungen innerhalb einer Organisation. Meist ist es Administratoren mit relativ geringem Aufwand möglich, an alle (auch kritischen) Informationen eines Unternehmens heranzukommen. Dieser Umstand ist zwingend in der Personalauswahl zu berücksichtigen. In der Aktualisierung des BSI-Grundschutzes wird es auch einen entsprechenden Baustein aus der Gruppe Organisation und Personal (ORP) geben, der sich mit den entsprechenden Gefährdungen und Maßnahmen beschäftigt.[13]

Zu berücksichtigen sind entsprechend den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in diesem Zusammenhang insbesondere die folgenden Aspekte. Die einzelnen Punkte sollten in jedem Unternehmen hinreichend geregelt sein:

- Umgang mit Personalausfall
- Missbrauch von Berechtigungen
- fehlende oder unzureichende Regelungen
- unzureichende Kenntnis über Regelungen
- Fehlverhalten
- Hinweise zu Social Engineering
- sorgloser Umgang mit Informationen
- unberechtigte Verwendung von Systemen
- Missbrauch sozialer Netzwerke
- Manipulation oder Zerstörung von Geräten, Informationen oder Software

Im Rahmen der Auswahl von geeignetem Personal sollten folgende Aspekte berücksichtigt werden, um die Gefahren von Innentätern zu reduzieren:

- Einholung eines polizeilichen Führungszeugnisses

  Ein polizeiliches Führungszeugnis beinhaltet Informationen über verübte Straftaten einer Person. Die Details über den Inhalt regelt § 32 ▸BZRG (Gesetz über das Zentralregister und das Erziehungsregister)

- Abgleich gegen die Sanktionsliste

  Die Sanktionsliste ist nicht mit der Antiterrordatei[14] (ATD) zu verwechseln, in der unter anderem Personen mit Bezug zum internationalen Terrorismus gespeichert sind. Es handelt sich bei der Sanktionsliste um eine Abfrage gegen eine Liste mit bekannten Mitgliedern von Terrorgruppen. Hintergrund der Abfrage sind die

13. Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Personal.pdf – Baustein im DRAFT, Stand Januar 2017.
14. Vgl. http://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbekaempfung/Antiterrordatei/antiterrordatei_node.html.

Embargomaßnahmen der Europäischen Union zur Bekämpfung des Terrorismus. Es geht dabei im weitesten Sinne darum, Mittelzuflüsse an Terrororganisationen zu verhindern.

Übung 2.1:

Prüfen Sie Ihren eigenen Namen gegen die deutsche Sanktionsliste:
http://www.finanz-sanktionsliste.de/fisalis/jsp/index.jsf

Zum Vergleich suchen Sie im Anschluss nach „Osama bin Laden".

- Sicherheitsüberprüfungen

  Hat Ihr Unternehmen mit Informationen zu tun, die in den Bereich des Geheimschutzes fallen und entsprechend mit klassifiziert wurden, so empfiehlt es sich, durch den jeweiligen Geheimschutzbeauftragten eine Überprüfung entsprechend dem Sicherheitsüberprüfungsgesetz (SÜG) durchzuführen. Hierbei werden im Wesentlichen drei unterschiedliche Stufen der Überprüfung unterschieden:
  - einfache Sicherheitsüberprüfung („Ü1")
  - erweiterte Sicherheitsüberprüfung („Ü2")
  - erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlung („Ü3")

  Die Art der Überprüfung hängt davon ab, in welchem Umfang mit welchen klassifizierten Daten die Mitarbeiter in Berührung kommen werden. Es handelt sich hierbei um die Einstufungen:
  - VS-NfD (Verschlusssache – nur für den Dienstgebrauch, int. Restricted)
  - VS-Vertraulich (int. Confidential)
  - Geheim (int. Secret)
  - Streng geheim (int. Topsecret)

2.2.2 Rollenkonzepte und Gruppen

Das BSI schreibt in seinen Grundschutzkatalogen zum Rollen- und Berechtigungskonzept: „Die sorgfältige Definition eines Berechtigungskonzeptes verhindert den unrechtmäßigen Zugriff auf Informationssysteme und schützt damit auch die Integrität, Verfügbarkeit und Authentizität der zugehörigen Daten. Berechtigungskonzepte besitzen dabei Relevanz sowohl für Anwender als auch für Administratoren von IT-Systemen."[15]

Vereinfacht ausgedrückt bedeutet dies, dass man hinsichtlich der Zugriffsrechte (vgl. „need to know", Abschnitt 2.1.6) einen restriktiven Ansatz fahren sollte. Da das Thema sehr umfangreich ist, wird an dieser Stelle nur auf die Grundlagen eingegangen und das Thema des Identitäts- und Berechtigungsmanagements in einem eigenen Studienheft behandelt.

Definition 2.4:

Eine Rolle ist eine Festlegung von Rechten und Aufgabenstellungen und abhängig von einer Person oder einem System.

15. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02191.html.

In der Regel orientiert man sich bei der Definition von Rollen an den bereits in der Firma existierenden Funktionen bzw. Rollen. Diese können zum einen hierarchisch bestimmt (z. B. Abteilungsleiter, Projektleiter, Bereichsleiter) oder zum anderen an die Aufgabenstellung (funktionsbedingt) angelehnt sein, wie beispielsweise Buchhalter, Empfang, Datenbankadministrator.

> Man weist die Rechte den jeweiligen Rollen und keinen konkreten Personen zu. Eine Person erhält keine Rechte.

Hintergrund für diese Verfahrensweise ist, dass man Personen dadurch eine oder mehrere Rollen zuweisen kann. Hierdurch kann der administrative Aufwand deutlich reduziert werden und gleichzeitig wird die Übersichtlichkeit gesteigert.

Würde man Personen die Rechte zuweisen, ergäbe sich daraus die folgende Gleichung hinsichtlich der Anzahl an Rechtezuordnungen:

$$Anzahl\ Zuordnungen = Rechte \cdot Personen$$

Durch die Verwendung von Rollenkonzepten dagegen verringert sich die Gesamtzahl, da folgende Formel gilt:

$$Anzahl\ Zuordnungen = Rechte + Personen$$

Dies verdeutlicht auch Tab. 2.2:

Tab. 2.2: User- vs. Rollenberechtigungen

Zugriff Benutzerebene	Zugriff rollenbasiert	
	Rollen	Benutzer
Berechtigung A – Benutzer 1	Berechtigung A – Rolle 1	Rolle 1 – Benutzer 1
Berechtigung A – Benutzer 2	Berechtigung B – Rolle 1	Rolle 1 – Benutzer 2
Berechtigung A – Benutzer 3	Berechtigung C – Rolle 1	Rolle 1 – Benutzer 3
Berechtigung A – Benutzer 4	Berechtigung D – Rolle 1	Rolle 1 – Benutzer 4
Berechtigung B – Benutzer 1		
Berechtigung B – Benutzer 2		
Berechtigung B – Benutzer 3		
Berechtigung B – Benutzer 4		
Berechtigung C – Benutzer 1		
Berechtigung C – Benutzer 2		
Berechtigung C – Benutzer 3		
Berechtigung C – Benutzer 4		

Ein weiterer Vorteil des Rollenkonzepts liegt in der Vererbung, d.h., Rollen können hierarchisch aufgebaut sein. Dies führt dazu, dass untergeordnete Rollen eine Teilmenge der Rechte der jeweils übergeordneten Rolle besitzen.

Ebenso besteht die Möglichkeit, dass verschiedene Rollen auf einen Mitarbeiter vereint werden können, so z.B. die Mitarbeiterin der Buchhaltung, die mit 50 % ihrer Arbeitszeit die Funktion des Datenschutzbeauftragten einnimmt. Sie besitzt dann eine Rollenzuordnung zur Buchhaltung und zum Datenschutz.

Die technische Umsetzung der Rollen findet meist in Berechtigungsgruppen statt, wobei hier einige Einschränkungen hinsichtlich des Gruppen- und Rollenverständnisses gelten. So ist eine Rolle vom Ansatz her auf die Zeit der Ausführung beschränkt, während eine Gruppenzuordnung statisch ist.

Beispiel 2.8:

Die oben beschriebene Mitarbeiterin Buchhaltung und Datenschutz nimmt beispielsweise vormittags die Rolle der Buchhalterin und nachmittags die Rolle der Datenschutzbeauftragten wahr. Durch die Gruppenzuordnung hat sie aber auch vormittags die Rechte des Datenschutzes und nachmittags der Buchhaltung, obwohl sie diese in der entsprechenden Rolle nicht benötigt.

Generell verfügen die aktuellen Betriebssysteme schon über verschiedene Gruppen mit unterschiedlichen Berechtigungen. So finden wir beispielsweise im Windows 2012 R2 Server sehr viele Standard-Sicherheitsgruppen (so lautet die Bezeichnung in Windows):

- Operatoren für das Hilfe-Steuerelement
- Konten-Operatoren
- Administratoren
- zulässige RODC-Kennwortreplikationsgruppe
- Sicherungsoperatoren
- Zertifikatdienst-DCOM-Zugriff
- Zertifikatherausgeber
- …[16]

Sehr gut zu erkennen ist hier auch, dass sich die Gruppen nicht nur auf Personengruppen beziehen, sondern auch Systeme eine Gruppenzugehörigkeit haben.

Diese sogenannten Built-in-Groups beziehen sich ausschließlich auf den Kontext der Systemverwaltung, d.h., firmenindividuelle Gruppen müssen erarbeitet und zusätzlich aufgebaut werden.

Auch in Linux/UNIX-Betriebssystemen existiert ein Gruppenkonzept, die Zuordnung von Usern zu Gruppen erfolgt hierbei jeweils in der Datei `/etc/group` (siehe Tab. 2.3).

16. Vollständige Liste siehe: https://msdn.microsoft.com/de-de/library/dn579255(v=ws.11).aspx.

Tab. 2.3: Auszug /etc/group

Auszug /`etc/group` eines Raspberry Pi (debian linux)
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:pi
tty:x:5:disk:x:6:lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:pi
...

2.2.3 Administrator

Der Administrator ist die Rolle, die sich mit der Systemverwaltung beschäftigt. Sie wird in den unterschiedlichen Betriebssystemen durch verschiedene Benutzerkennungen repräsentiert.

Zu den Aufgaben der Rolle gehören insbesondere folgende Tätigkeiten:

- Softwareinstallation, -wartung und -deinstallation
- Durchführung von Aktualisierungen (Software-Updates, Patches)
- Benutzer- und Gruppenverwaltung
- Verwaltung des Dateisystems
- Verwaltung der Systemwerkzeuge (z.B. Active Directory, LDAP)
- Überwachung und Auswertung der Protokolldateien
- Überwachung und Auswertung der Systemperformance
- Lösung von Störungen und Problemen im Systemumfeld
- Konfiguration und Verwaltung des Netzwerkes
- ...

Wie Sie bereits gelernt haben, ist für jeden Benutzer eines Systems eine eigene Benutzerkennung einzurichten und die gemeinsame Nutzung von Kennungen zu unterlassen. Dies gilt insbesondere auch für Kennungen wie „root“ und „administrator“. Für jeden

Systemverwalter ist somit eine eigene administrative Kennung anzulegen. Es empfiehlt sich sogar, diese von der „normalen“ Kennung zu trennen, um hinsichtlich der Zugriffe zu beschränken.

Beispiel 2.9:

Surft ein Systemverwalter – angemeldet mit der Kennung „administrator“ – von einem Server aus im Internet, um beispielsweise aktuelle Treiber herunterzuladen, so besteht die Gefahr, dass über einen Drive-by-Download oder Exploit Schadcode mit vollen administrativen Rechten auf dem Server-System zur Ausführung kommt.

Ein Best-Practice-Ansatz wäre, den administrativen Benutzerkennungen keine Rechte hinsichtlich E-Mail-Nutzung und Internet zu geben. Hierdurch wird das Arbeiten unter diesen Kennungen weniger attraktiv und die Gefahr durch die erweiterten Rechte der Kennungen reduziert sich.

Es sollte weiterhin sichergestellt werden, dass die allgemeinen Kennungen „administrator“ und „root“ nicht genutzt werden. Dies kann organisatorisch geregelt, besser aber mit entsprechenden Maßnahmen unterstützt werden. Das BSI schlägt im Umfeld von UNIX in der Maßnahme M 2.33 Folgendes vor: „Der Super-User-Login root kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Passwort.“[17]

Gleiches kann (sollte) unter Windows und anderen Systemen (Router, Firewalls etc.) ebenfalls etabliert werden.

Beispiel 2.10:

Um ein geteiltes Passwort im Notfall – unabhängig von zwei realen Personen – vorrätig zu haben, können die Passwortteile in separaten (versiegelten) Umschlägen in einem Safe des Unternehmens gelagert werden. Nach Benutzung der Umschläge ist eine Neuvergabe des Passwortes vorzunehmen.

Je größer das Unternehmen ist, desto stärker kann und sollte die Aufgabe des Administrators untergliedert werden. Hierdurch wird zum einen die Spezialisierung unterstützt und zum anderen das Risiko durch Rechteansammlung in einer Person minimiert. Insbesondere können hier die Aufgaben nach Betriebssystemen und/oder Middleware-Schichten (z.B. Datenbank-Administrator, Mail-Administrator) aufgeteilt werden.

Eine in der Praxis sehr häufig vorzufindende Trennung liegt in einer Separation von Netzwerk-Administration und System-Administration. Zu beachten ist, dass es umso erforderlicher ist, die Aufgaben und Kompetenzen detailliert zu beschreiben, wenn die Anzahl der agierenden Mitarbeiter steigt. Gleiches gilt für die Schnittstellen. Nur über wirksame Service-Management-Prozesse ist eine sichere, funktionsfähige Organisation erreichbar.

17. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02033.html.

2.2.4 Protokollierung

Zur Überwachung der Funktionalität und der Auffindung von Fehlern bieten IT-Systeme (Server, Clients, Software-Komponenten etc.) in der Regel die Möglichkeiten zur Protokollierung. Insbesondere die Betriebssysteme liefern standardmäßig sehr viele Informationen in Logdateien (Linux) bzw. in der Ereignisanzeige (Windows).

Tab. 2.4: Logdateien unter Linux

Beispiel für Logdateien unter Linux

```
drwxr-xr-x 8 root root 4096 Nov 25 20:45 .
drwxr-xr-x 12 root root 4096 Nov 25 19:10 ..
-rw-r--r-- 1 root root 49446 Nov 25 19:15 alternatives.log
drwxr-x--- 2 root adm 4096 Nov 25 19:10 apache2
drwxr-xr-x 2 root root 4096 Jan 3 2017 apt
-rw-r----- 1 root adm 42823 Nov 25 23:39 auth.log
-rw-r--r-- 1 root root 4044 Nov 25 20:45 boot.log
-rw-r--r-- 1 root root 74848 Nov 25 17:22 bootstrap.log
-rw------- 1 root utmp 384 Nov 25 18:42 btmp
-rw-r----- 1 root adm 241315 Nov 25 23:21 daemon.log
-rw-r----- 1 root adm 10822 Nov 25 20:45 debug
-rw-r----- 1 root adm 31 Nov 25 17:21 dmesg
-rw-r--r-- 1 root root 754740 Nov 25 19:16 dpkg.log
-rw-r--r-- 1 root root 24024 Nov 25 17:54 faillog
-rw-r--r-- 1 root root 2373 Nov 25 17:49 fontconfig.log
drwxr-xr-x 2 root root 4096 Jan 3 2017 fsck
-rw-r----- 1 root adm 223663 Nov 25 23:21 kern.log
-rw-rw-r-- 1 root utmp 292292 Nov 25 22:36 lastlog
drwx--x--x 2 root root 4096 Nov 25 20:45 lightdm
-rw-r----- 1 root adm 231723 Nov 25 23:39 messages
drwxr-xr-x 2 ntp ntp 4096 Jul 25 22:36 ntpstats
drwxr-x--- 2 root adm 4096 Jun 1 15:17 samba
-rw-r----- 1 root adm 487846 Nov 25 23:39 syslog
-rw-r----- 1 root adm 5427 Nov 25 20:45 user.log
-rw-rw-r-- 1 root utmp 21504 Nov 25 22:36 wtmp
-rw-r--r-- 1 root root 11157 Nov 25 20:45 Xorg.0.log
-rw-r--r-- 1 root root 11502 Nov 25 20:45 Xorg.0.log.old
```

Die Protokollierung gibt Aufschlüsse über die Aktionen des Betriebssystems und den Zustand. Insbesondere Monitoring-Systeme (vgl. Abschnitt 3.6) greifen auf diese Daten zu und leiten bei Bedarf Reaktionen ein.

Gerade auch für die Informationssicherheit dienen diese Protokolle als Auskunftsquelle, um Schadensverläufe oder Einbrüche nachvollziehen zu können bzw. proaktiv solche zu erkennen. Der Trend geht dahin, dass mithilfe von sogenannten ▸SIEM-Systemen auch komplexe Sicherheitsrisiken kontrolliert und erkannt werden können. SIEM steht in diesem Zusammenhang für Security Information and Event Management. Es handelt sich hierbei um eine Echtzeit-Auswertung von Events und ihrer Korrelation untereinander, um anhand einfacher oder/und komplexer Regeln Sicherheitsvorfälle erkennen zu können.

Knackpunkt dieser Lösungen sind zum einen die gewaltigen Datenmengen, da SIEM-Systeme Eingaben aus möglichst vielen unterschiedlichen Datenquellen (alle Server-Systeme, Firewalls, Monitoring, Virenschutz, Intrusion Detection etc.) erhalten und ver-

arbeiten müssen. Viele Unternehmen scheuen heute noch aus Kostengründen vor der Implementierung solcher Lösungen zurück. Doch am Markt zeichnen sich inzwischen auch günstige Lösungen ab. Die Deutsche Telekom bietet mittlerweile sogar gemanagte Systeme für den Mittelstand an[18].

Unabhängig vom Einsatz eines SIEM-Systems sollte eine regelmäßige Prüfung der Protokolldateien erfolgen, um im Zweifel manuell Bedrohungslagen zu identifizieren. Insbesondere sollte der Sicherheitsbeauftragte zusammen mit den Administratoren darüber nachdenken, welche Events aufgezeichnet werden sollen.

Beispiel 2.11:

Nur fehlerhafte Login-Versuche aufzuzeichnen liefert ggf. Hinweise darauf, ob ein unberechtigter Zugang zum System versucht wird. Es macht aber durchaus auch Sinn, erfolgreiche (vielleicht unberechtigte) Logins aufzuzeichnen.

Als Zwischenschritt vor der Implementierung eines SIEM-Systems sollte darüber nachgedacht werden, die Protokolle zentral auf einem Log-Server abzuspeichern.

Ein weiterer wichtiger Punkt in Bezug auf die Protokollierung liegt im Netzwerk-Protokoll NTP (Network Time Protocol). Das Protokoll ermöglicht eine Zeitsynchronisation innerhalb eines Netzwerkes. Gerade im Zusammenhang mit Sicherheitsvorfällen ist es zwingend erforderlich, dass die Systemzeit nachvollzogen werden kann bzw. im Idealfall auf allen Systemen identisch ist. Denn nur so lassen sich die Informationen in den unterschiedlichen Log- und Protokolldateien miteinander korrelieren und Aussagen treffen. Die Wichtigkeit dieser Voraussetzung lässt sich auch schon daraus ableiten, dass das BSI der Zeitsynchronisation eine eigene Maßnahme[19] gewidmet hat.

2.2.5 Dateisysteme

In diesem Abschnitt werden Sie keine Dateisysteme in ihrer Tiefe und dem Aufbau kennenlernen, sondern einige grundlegende Fakten zur Rechtevergabe und der Integrität und Vertraulichkeit erfahren. Mit den Unterschieden und Techniken, die hinter den unterschiedlichen Dateisystemen stecken, müssen Sie sich in der Informationssicherheit allerdings spätestens im Umfeld der Forensik (der digitalen Spurensuche) befassen.

Zu den gebräuchlichsten Dateisystemen zählen heute folgende:

- FAT32

  = File Allocation: Weiterentwicklung des Dateisystems FAT aus dem Jahr 1980. Haupteinsatzbereich liegt heute auf externen Datenträgern, wie z. B. Festplatten.

- NTFS

  = New Technology File System: Standard-Dateisystem der heutigen Windows-Systeme, das umfangreichere Sicherheitsmechanismen und Features im Vergleich zu FAT bietet.

- Ext4

  = Fourth Extended File System: Weiterentwicklung von Ext2 und Ext3. Es handelt sich hierbei um das Standard-Dateisystem unter Linux.

18. Vgl. https://www.t-systems.com/de/de/loesungen/security/loesungen/cyber-crime/cyber-security-63782.
19. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04227.html.

Daneben gibt es eine Vielzahl weiterer Dateisysteme mit unterschiedlichen Einsatzzwecken, Vorteilen und Nachteilen. An dieser Stelle sei ausnahmsweise auch ein Link zu Wikipedia erlaubt; hier finden Sie eine Liste von Dateisystemen[20].

Gemeinsam haben alle Dateisysteme ihre Aufgabenstellung: Es geht um die Verwaltung von Dateien.

Definition 2.5:

Eine Datei ist eine Menge an Daten, die logisch zusammengehören. Sie wird auf einem Medium gespeichert und ist über eine Bezeichnung identifizierbar.

Im Rahmen der Dateiverwaltung müssen folgende Punkte geregelt sein:

- Abbildung der Daten auf die physischen Einheiten (Blöcke, Cluster etc.)
- Gewährleistung von Zugriffsmethoden
- Zuordnung von Speicherplätzen und Freigabe dieser
- Zugriffsschutz entsprechend festgelegter Kriterien

Für den Benutzer stellen sich die Dateiablagen üblicherweise in Form von Verzeichnisbäumen dar. Hierbei kann in jedem Verzeichnis ein weiteres Unterverzeichnis oder aber Dateien liegen. Sie kennen dieses Aussehen von Ihrem Arbeitsplatzrechner her, wie z.B. in Abb. 2.4 für einen Verzeichnisbaum unter Windows 10.

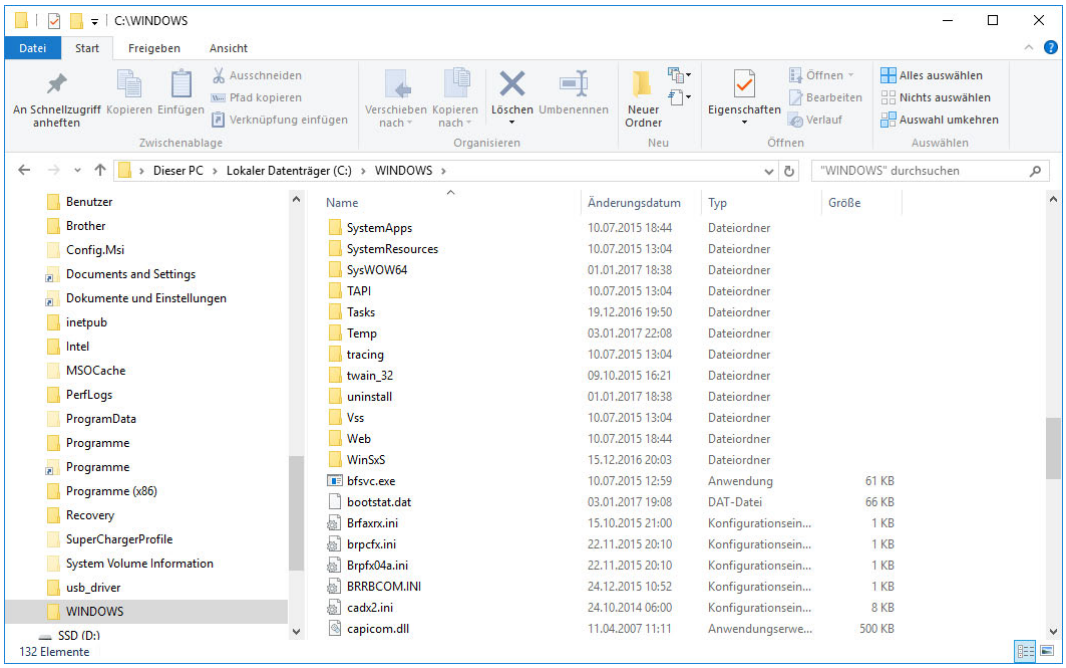

Abb. 2.4: Verzeichnisbaum unter Windows 10

Die für den Benutzer vorhandene Darstellung steht dabei in keinem Zusammenhang zur physikalischen Anordnung der Daten auf dem Datenträger. So kann es beispielsweise sein, dass eine einzelne Datei in mehrere Teile aufgespalten (fragmentiert) ist und an den unterschiedlichsten Stellen des physikalischen Mediums liegt.

20. Vgl. https://de.wikipedia.org/wiki/Liste_von_Dateisystemen.

Eine der wichtigsten Aufgaben ist es auch, den Zugriff zu Dateien zu handhaben. Die Aufgabe wird dabei durch das Betriebssystem abstrahiert und in der zum jeweiligen Betriebssystem passenden Form dargestellt.

So bieten Linux und UNIX eine Unterteilung der Zugriffe für

- den Datei-Eigentümer,
- eine zugeordnete Gruppe,
- den „Rest“,

und dies unterschieden in die Rechte

- Lesen,
- Schreiben,
- Ausführen.

Dies wird für jede Datei und jedes Verzeichnis in der Form

```
drwxrwxrwx Eigentümer Gruppe Größe Datum Dateiname
```

durch das Betriebssystem ausgegeben. Hierbei bedeuten die ersten 10 Zeichen Folgendes:

d	Dateiverzeichnis (eine flache Datei hat hier ein Minuszeichen)
r	Leserecht für den Eigentümer gegeben
w	Schreib-(Lösch-)Recht für den Eigentümer gegeben
x	Recht zur Ausführung für den Eigentümer gegeben
r	Leserecht für die Gruppe gegeben
w	Schreib-(Lösch-)Recht für die Gruppe gegeben
x	Recht zur Ausführung für die Gruppe gegeben
r	Leserecht für den Rest gegeben
w	Schreib-(Lösch-)Recht für den Rest gegeben
x	Recht zur Ausführung für den Rest gegeben

Ist ein Recht nicht gegeben, ist dies durch ein – gekennzeichnet. Ein typisches Dateiverzeichnis unter Linux sieht wie folgt aus:

```
root@kali:/etc# ls -la
total 2008
drwxr-xr-x 178 root root 12288 Jan 3 16:31 .
drwxr-xr-x 23 root root 4096 Dec 8 13:40 ..
-rw-r--r-- 1 root root 2981 Mar 3 2015 adduser.conf
-rw-r--r-- 1 root root 44 Oct 10 06:55 adjtime
```

...

Das Setzen und Verändern der Berechtigungen auf Dateiebene erfolgt mittels des Befehls `chmod`, der die Berechtigungen entsprechend für Eigentümer, Gruppe und Rest in einer binären Form ändert. Praktisch ausgedrückt, bedeutet dies, dass jeder Berechtigung ein Bit zugeordnet ist (siehe Abb. 2.5).

-	r	w	x	r	w	-	r	-	-
Typ:	read	write	execute	read	write	execute	read	write	execute
Datei	Eigentümer			Gruppe			"Rest"		
	4	2	1	4	2	1	4	2	1
	binär: 0100	binär: 0010	binär: 0001	binär: 0100	binär: 0010	binär: 0001	binär: 0100	binär: 0010	binär: 0001
	binär: 0111			binär: 0110			binär: 0100		
	7			6			4		

Abb. 2.5: Berechtigungsvergabe Linux

Um die abgebildeten Rechte `-rwxrw-r--` zu setzen, ergibt sich folgende Syntax:

```
chmod 764 Dateiname
```

Selbstverständlich bieten grafische Benutzeroberflächen unter Linux inzwischen eine Vergabe der Rechte per Mausklick an.

Unter Windows sieht die Darstellung der Berechtigungen wie in Abb. 2.6 aus:

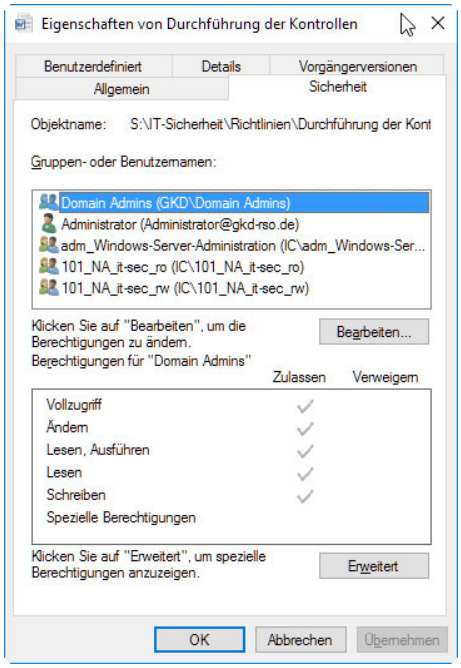

Abb. 2.6: Dateiberechtigungen unter Windows

Die Möglichkeiten der Einzelberechtigungen ähneln den Rechten unter Linux. Allerdings ist es auf Windows-Systemen möglich, jedem Benutzer individuelle Rechte auf Dateiebene zu geben.

Da Dateisysteme hierarchisch aufgebaut sind, ist zu berücksichtigen, dass die Berechtigungen ebenfalls in der Hierarchie vergeben werden. Einem Benutzer beispielsweise Rechte auf einer Datei zu erteilen, der gar nicht das Verzeichnis hineinwechseln kann, ist sinnlos.

Daraus folgt, dass man vor der Einrichtung von Dateiverzeichnissen ein Zugriffskonzept haben muss, das auch zum Rollen- und Gruppenkonzept des Unternehmens passt (vgl. Abschnitt 2.2.2).

Neben den eigentlichen Nutzdaten werden mit jeder Datei weitere zusätzliche Informationen abgespeichert, die insbesondere im Rahmen der Analyse von Sicherheitsvorfällen eine Bewandtnis haben können. So werden z. B. (wie in Abb. 2.7 zu erkennen) Informationen über die letzten Zugriffe und zusätzliche Attribute gespeichert.

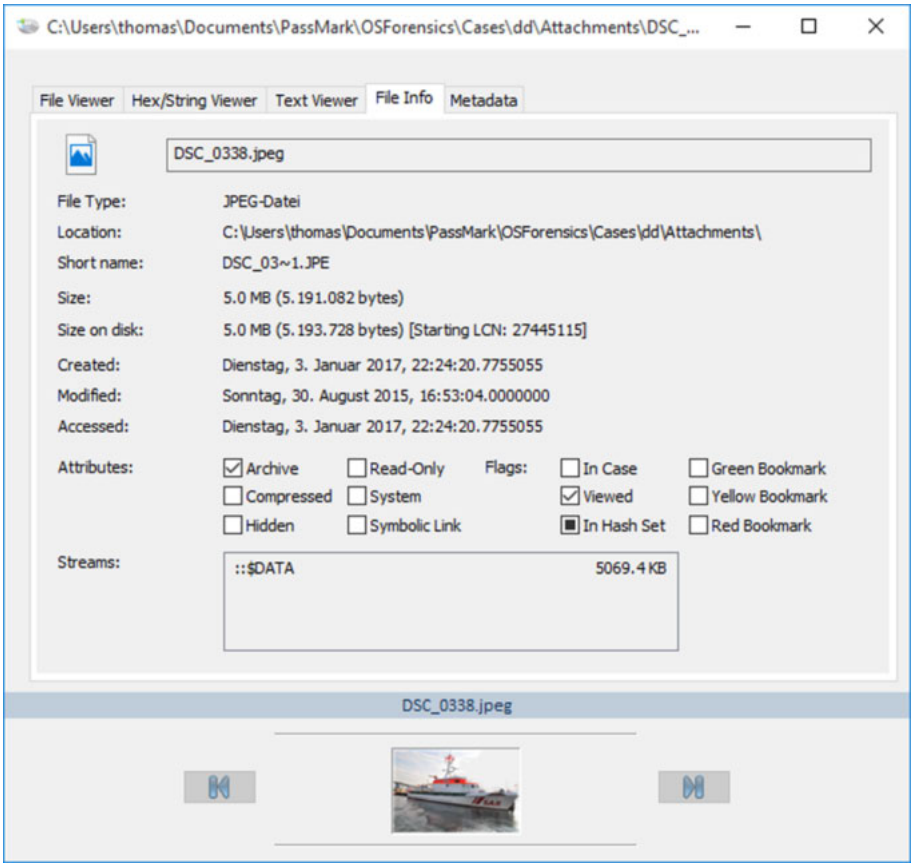

Abb. 2.7: Informationen zu Dateien

Zusätzlich zu diesen Informationen kommt in heutigen Umgebungen eine weitere Ebene der Berechtigungen hinzu. Meist liegen Dateien und Verzeichnisse nicht mehr auf dem lokalen System, sondern auf einem File-Server im Netzwerk.

Um an die Daten dieses Systems heranzukommen, sind weitere Protokolle und entsprechende Zugriffsregeln zu berücksichtigen. Die dort festgelegten Beschränkungen gelten dann additiv zu den Dateirechten, d. h., an dieser Stelle sind Fehler und Probleme vorprogrammiert.

In den meisten Fällen kommt heute das Netzwerkprotokoll ▸CIFS (Common Internet File System)zum Einsatz, das eine Erweiterung des Protokolls ▸SMB (Server Message Block) darstellt. Windows-Systeme nutzen dieses Protokoll seit Windows NT. Auf Linux-Systemen wird das Protokoll mittels Samba zur Verfügung gestellt, sodass es sich heute mittlerweile zum Standard entwickelt hat. Protokolle wie ▸NFS (Network File System) haben stark an Bedeutung verloren und kommen nur noch selten zum Einsatz.

2.2.6 Passwörter

Ein beliebter, scherzhafter Spruch in der Informationssicherheit lautet: „Passwörter sind wie Unterwäsche: Man gibt sie auch nicht dem besten Freund und wechselt sie regelmäßig."

Viele Systeme und Softwareprodukte werden heute noch über eine Kombination aus Benutzerkennung und Passwort geschützt. Dieses Vorgehen ist eine klassische Ein-Faktor-Authentisierung, die auf dem Faktor „Wissen" beruht. Wer Benutzernamen und Passwort kennt, hat einen Zugang.

Entsprechend wichtig ist es, bei den verwendeten Passwörtern einige Regeln zu beachten, die eine Kenntnisnahme erschweren oder gar unmöglich machen. Hierbei wird unter „Kenntnisnahme" auch eine Erraten oder Bruteforcen (Ausprobieren aller möglichen Zeichenkombinationen) subsumiert.

Eine grundlegende Basis ist die Aufbewahrung des Passwortes: Kann man sich ein Passwort nicht merken, ist es legitim, eine Eselsbrücke zu nutzen oder es geschützt abzulegen.

Beispiel 2.12:

Als geschützte Ablagen in diesem Zusammenhang gelten weder Post-its am Monitor, Zettel unter der Tastatur noch Hinweise auf dem an der Wand hängenden Whiteboard – wenn Sie jetzt lachen: Ich treffe genau diese Methoden heute noch fast täglich an!

Leider gibt es aber auch heute noch Anwendungsprogramme, die die Passwörter im Klartext speichern. Solche Softwarekomponenten sollten nach Möglichkeit nicht mehr zum Einsatz kommen. Lediglich Hashwerte von Passwörtern sind zu speichern.

Speichern Sie Passwörter nur in entsprechend zertifizierten Tools ab, die sicherstellen, dass Sie ein Passwort bei Bedarf zur Verfügung haben. Meist sind diese Programme auch durch ein Passwort geschützt. Dieses sollten Sie ausschließlich im Kopf haben und es sollte „unbrechbar" sein. Das BSI empfiehlt in diesem Zusammenhang Passwort-Manager wie „KeePass"[21].

Ein wichtiger Grund, warum Passwort-Verwaltungsprogramme zum Einsatz kommen sollten, liegt darin, dass Sie für jedes Verfahren, jeden Dienst, jede Benutzerkennung ein eigenes, einmaliges Passwort verwenden sollten. Kommt es zur Kompromittierung eines der von Ihnen genutzten Passwörter, bleiben die anderen bestehend und sicher. Die Medien berichten regelmäßig über den Diebstahl von Passwörtern, die dann verkauft oder sogar kostenlos angeboten werden[22].

21. Vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html.
22. Vgl. https://www.heise.de/security/meldung/LinkedIn-Hack-117-Millionen-Passwort-Hashes-zum-Download-aufgetaucht-3224212.html.

Beispiel 2.13:

Aus der eigenen Erfahrung: Zu der Zeit, als LinkedIn gehackt wurde, hatte ich in diesem Business-Netzwerk das gleiche Passwort wie bei GMail. Bei einer Anmeldung am Dienst GMail wurde ich von Google darauf aufmerksam gemacht, dass erfolgreiche Anmeldungen auf das Konto vor ca. 3 Stunden aus China erfolgt seien, was zeitlich nicht zur aktuellen Anmeldung aus Europa passen würde.

Wie das Beispiel zeigt, werden gewonnene Daten gegen andere Dienstleistungen geprüft und ausgenutzt. Das Beispiel zeigt aber auch sehr schön, dass man mittels Korrelation von scheinbar normalen Events Sicherheitsvorfälle erkennen kann. Google hat in diesem Fall erkannt, dass Anmeldungen in einem Abstand von nur drei Stunden aus zwei Ländern mit einer Entfernung zueinander von über 7000 km unwahrscheinlich sind.

Ein weiterer wichtiger Faktor ist der Aufbau eines Passwortes. Kurze Passwörter lassen sich mittels Brute-Force innerhalb sehr geringer Zeitspannen entschlüsseln. Passwörter, die (auch längere) sprachlich existente Wörter darstellen, werden über Wörterbuch-Attacken ermittelt.

Über die Länge der Passwörter kann man sich wunderbar streiten. Fakt ist, dass mit zunehmender Rechnerleistung (bzw. GPU-Leistung) die Geschwindigkeit steigt, um Passwörter zu brechen. Es macht also wenig Sinn, sich Gedanken darüber zu machen, ob man nun acht oder neun Zeichen wählen sollte. Für Accounts wie „Administrator“ empfiehlt das BSI heute schon eine Passwortlänge von mindestens 12 Zeichen.

Auch der Aufbau der Passwörter spielt eine Rolle. Um ein Ausprobieren zu erschweren, ist es notwendig, den Zeichenvorrat zu erhöhen; sprich das Ziel ist es, die Anzahl der möglichen Kombinationen für ein Passwort zu erhöhen. Nehmen wir ein Passwort, das ausschließlich aus Kleinbuchstaben besteht und sechs Zeichen lang ist. Für dieses gilt:

$$\textit{Kombinationsmöglichkeiten} = 26^6 = 308\,915\,776$$

Jeder der 26 Kleinbuchstaben des Alphabetes kann an jeder der sechs Stellen des Passwortes auftauchen.

Erhöhen wir die Anzahl der Stellen von sechs auf sieben, so ergeben sich folgende Kombinationsmöglichkeiten.

$$\textit{Kombinationsmöglichkeiten} = 26^7 = 8\,031\,810\,176$$

Zum Vergleich beschränken wir uns nun wieder auf das sechs Zeichen lange Passwort, ergänzen die Kleinbuchstaben um die Großbuchstaben, so haben wir an jeder Stelle statt 26 Möglichkeiten nun 52 verschiedene Werte. Daraus ergibt sich die folgende Berechnung:

$$\textit{Kombinationsmöglichkeiten} = 52^6 = 19\,770\,609\,664$$

Es macht also durchaus Sinn, den Zeichenvorrat zu maximieren. Dies erklärt auch die Forderung nach komplexen Passwörtern, wie sie beispielsweise in Windows-Betriebssystemen als Standard vorgesehen ist. Ein komplexes Passwort bedeutet in diesem Sinne, dass drei von vier Zeichengruppen im Passwort enthalten sein müssen. Diese vier Zeichengruppen sind:

- Kleinbuchstaben
- Großbuchstaben

- Ziffern
- Sonderzeichen

Rückgreifend auf die Forderung des BSI nach einem 12-Zeichen-Passwort für administrative Kennungen könnte man die Anzahl der Möglichkeiten wie folgt betrachten:

Zeichenvorrat = 26 Kleinbuchstaben + 26 Großbuchstaben + 10 Ziffern + 15 Sonderzeichen = 77 Kombinationsmöglichkeiten = 77^{12} = 43 439 888 521 963 583 647 921

Es gäbe über 43 Trilliarden Kombinationsmöglichkeiten!

> Mein SAP-Passwort ist durch Keepass automatisch generiert, besteht aus allen vier Zeichengruppen und ist 25 Zeichen lang.

Nun könnte man dem Gedanken verfallen, dass es ja durchaus ausreichend sein kann, ein sehr komplexes und damit (vermeintlich) sicheres Passwort dauerhaft zu benutzen. Für die Forderung nach regelmäßiger Änderung gibt es einen einfachen Grund: Ein Passwort kann auch kompromittiert werden, ohne dass man es errät oder ausprobiert, z. B.:

- Abgucken bei der Passwort-Eingabe
- Aufzeichnung des Passworts durch Keylogger oder Trojaner
- Verletzung von einer der anderen oben genannten Empfehlungen
- Speicherung im Webbrowser

Dass Passwörter auch nicht über öffentliche Medien kommuniziert werden sollten, bedarf sicherlich keiner expliziten Erläuterung. Müssen komplette Anmeldedaten (Benutzer und Passwort) übermittelt werden, so ist ein Medienbruch einzuhalten, d. h. Benutzernamen und Passwort über separate Kanäle zu übermitteln.

Zu einer sicheren Konfiguration von Systemen im Zusammenhang mit Passwörtern ist selbstverständlich auch Voraussetzung, dass man diese verwendet. Anmeldeverfahren dürfen nicht abgeschaltet werden. Auch sollten sich Systeme bei Nichtbenutzung nach einer kurzen Zeit automatisch sperren.

Eine technische Möglichkeit, die Sicherheit von Passwörtern zu erhöhen, ist das sogenannte Salting (eng. salzen). Hierdurch werden Passwörter um eine bestimmte Anzahl an systemgenerierten Zeichen (möglichst für jeden Benutzer individuell) ergänzt, bevor ein Hashing des Passwortes durchgeführt wird.

Beispiel 2.14:

Der Benutzer sucht sich das Passwort „IchBinSicher1“ aus. Für diesen Benutzer hängt das System das individuelle Salz „0der4uchN1ch+“ dran. Somit ändert sich der MD5-Hash von „481ff0db814792f8da01455c4e1eb823“ auf „dad460cebd74cb9d8c7bafcbe1af8daf“ und die tatsächliche Passwortlänge von 12 auf 27 Zeichen.

Generell stellt sich die Frage der Langfristigkeit von Anmeldungen mit Benutzername und Passwort. Wie Sie gesehen haben, ist hier ein großer Faktor an Unsicherheiten gegeben, sodass es sinnvoll ist, auf eine Mehrfaktor-Authentisierung umzustellen.

2.3 Weitere Aspekte

Im letzten Abschnitt haben Sie nun bereits viele – teils abstrakte – Sicherheitsrisiken und Lösungsansätze kennengelernt. Alle Gefährdungen abschließend zu behandeln ist im Rahmen eines Studienhefts nicht umsetzbar, sodass vielfach nur punktuell auf einige Schwachstellen eingegangen werden kann. Aus dem Kontext und den Beispielen sollten Sie allerdings in der Lage sein, einen Gesamtblick aufzubauen und auch nicht angesprochene Themen selbstständig beleuchten und behandeln zu können.

2.3.1 Boot-Prozess

Kommt man an ein System physikalisch heran, so bestehen viele Möglichkeiten, dieses zu kompromittieren. Viele dieser Gefährdungen lassen sich durch relativ einfache Möglichkeiten umgehen.

Beim Start eines Rechnersystems laufen einige Dinge ab, bevor das eigentliche Betriebssystem seinen Dienst aufnehmen kann. Beispielhaft betrachten wir an dieser Stelle Rechnersysteme einer x86-Architektur, da diese sowohl auf Server- wie auf Client-Seite stark vertreten sind.

Im ersten Schritt wird das ▸BIOS (Basic Input/Output System) aus dem ▸ROM geladen und ausgeführt. Dieses System ermöglicht die Kommunikation zu den physikalischen Geräten des Rechners. Die heutige Variante des Unified Extensible Firmware Interface (▸UEFI) wird an dieser Stelle mit unter den Begriff des BIOS subsumiert.

Im nächsten Schritt sucht das BIOS (nach einigen Tests) auf dem im BIOS eingestellten Medium nach dem Bootloader, der seinerseits das Betriebssystem nachlädt. Dieses Startprogramm wird üblicherweise im Master Boot Record (▸MBR) gespeichert.

Ab dieser Stelle übernimmt das installierte Betriebssystem den Startvorgang.

Betrachten wir den Prozess bis hierhin, so sehen wir bereits einige mögliche Ansatzpunkte, um unerwünschte Aktionen durchzuführen. Eine der ersten Möglichkeiten ist es, den Bootvorgang insofern zu manipulieren, als man das Bootmedium verändert. Das heißt, durch eine Veränderung der Bootreihenfolge im BIOS ist es möglich, einen Rechner von einer ▸CD oder einem ▸USB-Stick zu starten. Über die dort hinterlegten Programme kann dann ein Zugriff auf die Festplatte genommen werden und Daten kopiert oder manipuliert werden.

Beispiel 2.15:

Das Programm KON-BOOT ist ein Tool, das von einem externen Medium als Erstes im Rahmen des Boot-Prozesses gestartet wird. Es modifiziert Daten auf dem eigentlichen Boot-Medium (der Festplatte) und ermöglicht somit, die Anmeldung an Windows und Mac OS-Systemen zu umgehen. Nach dem Start mittels KON-BOOT besteht Zugriff mit Systemrechten auf einen Rechner, ohne dass ein Passwort erforderlich war[23].

Angriffe dieser Art lassen sich einfach durch eine fest eingestellte Bootreihenfolge der Medien und das Setzen eines BIOS-Passwortes umgehen.

23. Vgl. Image-Film von KON-BOOT: https://www.youtube.com/watch?v=C2wV2ZijxB0.

Der nächste Schritt, das Laden des Bootloaders, kann über eine Funktion namens Secure Boot validiert werden. Mit der Version 2.3.1 von UEFI wurde diese Option spezifiziert. Bei aktiviertem Secure Boot können nur noch Bootloader gestartet werden, die digital signiert sind. Die bekannten Betriebssystemhersteller unterstützen dieses Verfahren mittlerweile, sodass das Einschalten dieser Option zu empfehlen ist.

Beispiel 2.16:

Ein sehr bekannter Angriff gegen den Bootload ist der sogenannte Evil-Maid-Angriff von Joanna Rutkowska. Hierbei wird davon ausgegangen, dass Zugriff auf einen heruntergefahrenen Rechner (mit Festplattenverschlüsselung) besteht. Dieser wird von einem externen Medium gebootet, das den Bootloader derart manipuliert, dass die Passworteingabe zur Entschlüsselung des Systems mitprotokolliert wird. Zur Auslesung dieser Eingabe ist ein weiterer Start (nachdem das System einmal vom regulären User benutzt worden ist) nötig. Ein Beispiel für ein solches Szenario ist der Laptop, der zur Frühstückszeit immer unbeaufsichtigt im Hotelzimmer liegt und vom bösen Zimmermädchen (Evil Maid) angegriffen wird[24].

2.3.2 Verschlüsselung

Verschlüsselung ist ein wirksamer Schutz gegen die Manipulation oder den Diebstahl von Informationen. Sie wird somit den Schutzzielen Integrität und Vertraulichkeit gerecht. Grundvoraussetzung ist, dass wirksame Algorithmen eingesetzt werden.

Beispiel 2.17:

Eine Firma versucht ihr Sicherheitsprodukt zu verkaufen und wirbt damit, dass ein selbst entwickelter Algorithmus zur Verschlüsselung zum Einsatz kommt.

Als wirksam kann ein Algorithmus nur dann angenommen werden, wenn er nachprüfbar ist. Es gilt der Merksatz:

> Die Stärke einer Verschlüsselung liegt nicht im geheimen Code des Algorithmus, sondern in der Länge des verwendeten Schlüssels.

Heute gilt im Allgemeinen, dass die symmetrische Verschlüsselungsmethode ▸AES (Advanced Encryption Standard) als sicher angesehen wird. Sie unterstützt Schlüssellängen von 128, 192 und 256 Bits. Die mathematische Sicherheit von AES ist mehrfach wissenschaftlich nachgeprüft worden. Im Bereich der Festplattenverschlüsselung konzentrieren wir uns ausschließlich auf eine symmetrische Verschlüsselung, da asymmetrische Verfahren schon aufgrund der Geschwindigkeit ausscheiden.

Der Einsatz von AES hat sich zu einem Quasistandard entwickelt und wird selbst von Geheimdiensten für Dokumente mit geheimer Klassifikation als sicher eingestuft. Selbst die Entwickler von Ransomware-Trojanern wie Locky sind dazu übergegangen, auf AES zu setzen, um eine Entschlüsselung ohne Lösegeldzahlung zu verhindern.

24. Vgl. http://theinvisiblethings.blogspot.de/2009/10/evil-maid-goes-after-truecrypt.html.

Zur Absicherung von Systemen empfiehlt es sich, eine komplette Festplattenverschlüsselung zu implementieren. Hierdurch wird sichergestellt, dass nicht aus Versehen kritische Daten unberücksichtigt bleiben. Insbesondere bei mobilen Systemen ist eine Verschlüsselung der Festplatte zwingend vorzusehen. Somit kann im Verlustfall lediglich die Hardware als Verlust abgeschrieben werden, aber nicht die Daten.

Bei unverschlüsselten Festplatten ist es ein Leichtes, ein Image der Festplatte zu ziehen und die Daten auf physikalischer Ebene (im einfachsten Fall mit einem Hex-Editor) auszulesen.

2.3.3 Datenträger

Zum Abschnitt „Datenträger“ gehört eine Sammlung unterschiedlicher Gefährdungen und Gegenmaßnahmen im direkten Zusammenhang mit den unterschiedlichsten Datenträgern.

Zwei Arten von Datenträgern (▸HDDs und ▸SSDs) haben Sie bereits in Studienheft SRN01 kennengelernt, ebenso die physikalischen Risiken dieser Medien.

Neben diesen – in Systemen verbauten – Datenträgern gibt es eine Vielzahl an transportablen Datenträgern. Sie dienen in der Regel zum Austausch von Informationen. Zu nennen sind an dieser Stelle insbesondere

- Speicherkarten (▸SD, Flash etc.),
- Optische Medien (CD, ▸DVD etc.),
- USB-Sticks.

Durch die Verwendung von diesen externen Medien entstehen grundsätzlich die Gefährdungen des Einschleusens von unerwünschten Inhalten und des Mitnehmens von Informationen (Datendiebstahl).

Ein wirkungsvoller Schutz gegen beide Gefahren ist die technische Unterbindung der Benutzung externer Speichermedien. Insbesondere Endpoint-Protection-Suiten bieten hierzu wirkungsvolle Lösungen an. Durch die Implementierung einer derartigen Softwarelösung können nur noch vorher autorisierte Datenträger innerhalb des IT-Systems genutzt werden. Die Gefahr, dass autorisierte Datenträger für eine der beiden Gefährdungen genutzt werden, besteht weiterhin. Darüber hinaus ergibt sich die Problematik, dass ggf. Datenträger von externen Mitarbeitern, Referenten o. Ä. eingebracht werden müssen. Hierfür sind entsprechende Umgehungslösungen zu schaffen.

Das Risiko des Einbringens von unerwünschten Inhalten stellt in vielen Organisationen ein Problem dar. Oft kommt es vor, dass externe Medien mit Schadsoftware verseucht sind. Weiterhin besteht die Gefahr, dass absichtlich Schadprogramme mitgebracht und installiert werden.

Unabhängig vom Missbrauch der Datenträger gilt, dass gerade die portablen Medien sehr leicht verloren gehen können. Aus diesem Grund sollte es eine Firmen-Policy sein, dass bei Benutzung von externen Datenträgern diese stets nur verschlüsselt eingesetzt werden sollen.

2.3.4 Notwendigkeit von Diensten und Programmen

Bereits in Abschnitt 2.1.6 wurde auf das Risiko hinsichtlich des Einsatzes von Diensten hingewiesen. Es gilt die Aussage, dass nur die tatsächlich benötigten Services zu installieren und zu aktivieren sind.

Darüber hinaus ist es erforderlich, sich Gedanken über die Privilegien der einzelnen Dienste zu machen. So war es früher unter Windows üblich, Dienste ggf. mit dem Administrator-Account laufen zu lassen. Neben der Tatsache, dass die betroffenen Dienste damit übermäßig viele Rechte zugeteilt bekamen, ergaben sich auch Probleme bei Passwortänderungen des Administrator-Accounts. Aufgrund dieser Umstände sollte jeder Dienst in einem eigenen Benutzerkontext ausgeführt werden, der nur die speziell hierfür nötigen Rechte besitzt.

Beispiel 2.18:

Für einen Dienst wie z. B. einen Apache Webserver ist es nicht notwendig, dass dieser sich mit einer Benutzeranmeldung am System anmelden können darf.

Betrachten Sie beispielsweise auch mal die Einstellungen der Netzwerk-Interfaces, wie sie in Abb. 2.8 dargestellt sind.

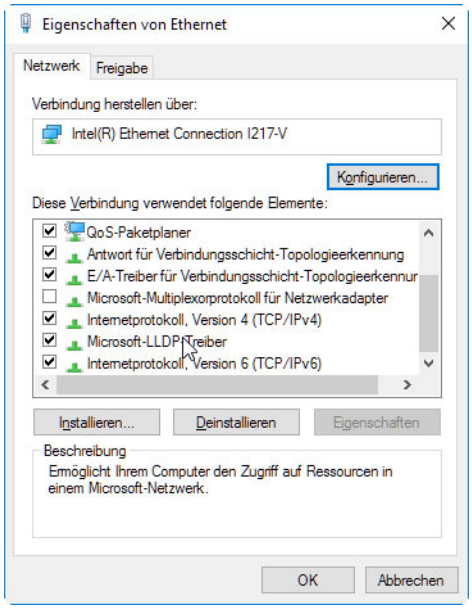

Abb. 2.8: Netzwerk-Adapter-Einstellungen

Arbeitet das System in einem reinen IPv4-Netzwerk, ist es nicht erforderlich, den IPv6-Stack aktiviert zu haben.

Die gleichen Bedingungen gelten auch für die Installation von Programmen auf den Systemen. Es sind nur die Softwarekomponenten zu installieren, die tatsächlich auf einem System laufend verwendet werden.

Beispiel 2.19:

Weil es ein Problem mit der Übertragung von Daten gab, wollte ein Anwendungsbetreuer auf „seinem“ Server die Software Wireshark installieren. Hierbei handelt es sich um ein Tool zur Netzwerkdiagnose, mit dem man den kompletten Netzwerkverkehr mitschneiden und auswerten kann. Die Sicherheitsabteilung hat dies rigoros untersagt[25].

Das Beispiel zeigt, dass es durchaus Sinn macht, keine unnötige Anwendungssoftware auf Systemen installiert zu haben, da sich hierdurch die möglichen Angriffsvektoren erhöhen.

2.3.5 Datensicherung

Zu den wichtigsten Voraussetzungen eines sicheren IT-Betriebes gehört auch die Datensicherung – eine regelmäßige und funktionierende Datensicherung. Um genau zu sein, geht es um die Möglichkeit, Daten schnell und umfassend wiederherstellen zu können.

Die Bedrohung mit Verschlüsselungstrojanern hat sehr deutlich gezeigt, wie schnell ein Schaden entstehen kann, wenn Daten unbrauchbar werden.

Genauso haben aber auch praktische Bespiele gezeigt, dass man mit einer funktionierenden Datensicherung große Schäden vermeiden und einen Ausfall verringern kann.

Beispiel 2.20:

Ein Krankenhaus in Großbritannien war Opfer eines Ransomwarevorfalls geworden. Dank eines funktionierenden Backups konnten die Daten schnell zurückgespielt werden, ohne dass ein großer Schaden entstanden war.[26]

Neben solchen massiven Szenarien schützt eine funktionierende Datensicherung auch gegen versehentlich durch die Nutzer gelöschte Dateien.

Wichtig ist, dass für eine Datensicherung in jedem Fall ein Konzept vorhanden sein muss, das die Datenmengen, die Sicherungsgeschwindigkeit, die Wiederherstellungsgeschwindigkeit und die Aufbewahrung der Backups betrachtet und eindeutig regelt.

25. Vgl. Schwachstellen von Wireshark: https://www.wireshark.org/security/.
26. Vgl. http://www.golem.de/news/backup-strategie-krankenhaus-konnte-ransomware-angriff-abwehren-1611-124287.html.

Zusammenfassung

Dieses Kapitel hat eine Vielzahl an möglichen Angriffspunkten von Betriebssystemen dargestellt. Sie haben unterschiedliche Gefährdungen auf technischer und auch auf organisatorischer Ebene kennengelernt und Ideen vermittelt bekommen, wie man diese Punkte angehen kann.

Viele der Angriffsvektoren gelten für unterschiedliche Betriebssysteme. In diesem Zusammenhang sollten Sie auch immer im Hinterkopf behalten, dass auch IOS und Android „nur“ Betriebssysteme sind und für diese eine Vielzahl der Bedrohungen zum Tragen kommt. Gerade im Hinblick auf die Menge der Informationen, die wir heute auf Smartphones und Tablets verarbeiten, sollte dieses Thema niemals außer Acht gelassen werden.

Aufgaben zur Selbstüberprüfung

2.1 Erläutern Sie bitte, warum Treiber in Bezug auf Schwachstellen gefährlicher sind als Anwendungsprogramme.

2.2 Sie haben unter UNIX die `katze`, der Eigentümer ist `alf`, die Gruppe `melmac`. Mit dem Befehl `chmod 731 katze` vergeben Sie neue Berechtigungen. Was dürfen alf, melmac und der Rest nach Ausführung des Befehls?

2.3 Recherchieren Sie nach einem USB-Stick namens „Rubber Ducky“ und beschreiben Sie die von dieser Technologie ausgehende Gefahr in wenigen Sätzen oder Stichworten.

3 Updates

In diesem Kapitel werden Sie erfahren, warum Firmen wie Microsoft oder Adobe die Benutzer mit regelmäßigen Patchdays strapazieren. Sie werden auch erfahren, welche Gefahren bestehen, wenn Sie keine Updates installieren.

Ebenso werden Sie lernen, wie Sie Systeme auf Schwachstellen testen können und was Sie in diesem Zusammenhang berücksichtigen sollten.

Sie erfahren, wie es zu vielen Schwachstellen kommt.

Jedes Softwareprodukt hat Fehler. Manche dieser Fehler fallen im Rahmen der Anwendung auf und werden als sogenannte Bugs behoben. Dies gilt allerdings im Wesentlichen nur für Fehler, die im Rahmen der normalen Benutzung oder in Testverfahren auffallen.

3.1 Buffer-Overflow

Im Gegensatz zu den offensichtlichen Fehlern gibt es ein historisches Problem in der Programmierung. Diese Fehler fallen nicht unbedingt auf, können aber durch geschickte Ausnutzung zu spannenden Seiteneffekten führen.

Es handelt sich um den sogenannten Buffer-Overflow, sprich Speicherüberlauf. Hierbei wird über die Grenzen eines reservierten Speicherbereiches hinausgeschrieben, ein Programmierfehler, der häufig vorkommt, wenn Eingabegrößen nicht abgeprüft werden.

Vereinfacht handelt es sich um das im folgenden C-Programm-Ausschnitt beschriebene Phänomen:

```
char zeichenkette[11] = {0};
strcpy(zeichenkette, "Diese Zeichenkette ist deutlich laenger und
                      wird den reservierten Speicherplatz
                      ueberlaufen.");
```

In der ersten Zeile wird die Variable `zeichenkette` als Array definiert und bietet Platz für 11 Elemente des Typs `char`. Diese Elemente stehen an den Positionen 0 bis 10 des Arrays.

Die zweite Programmzeile schreibt nun den Text „Diese Zeichenkette ist deutlich länger und wird den reservierten Speicherplatz überlaufen.“ in dieses Array hinein. Wie Sie sehen, ist dieser String insgesamt 92 Zeichen lang und somit 81 Zeichen länger, als Platz im Array vorgesehen ist. Die Folge hiervon ist, dass nachfolgende Speicherbereiche überschrieben werden – egal welcher Inhalt vorher darin gestanden hat. Dies führt z. B. zu Laufzeitfehlern oder zu anderen ungewollten Resultaten.

Dieser Fehler kann aber auch bewusst durch Angreifer genutzt werden. So kann auf diesem Weg z. B. auch die Rücksprungadresse eines Unterprogramms mit beliebigen Daten überschrieben werden. Infolgedessen besteht die Möglichkeit, binären Code einzufügen, der Befehle ausführt. Diese Befehle laufen dann im Benutzerkontext (also mit den Rechten) des Programms mit der Buffer-Overflow-Vulnerability. Entsprechend interessant sind für Angreifer natürlich Module des Betriebssystems, die derartige Anfälligkeiten haben und mit Systemrechten ausgestattet sind.

Gerade in den Programmiersprachen C und C++ gibt es eine Anzahl an Funktionen, die keine Prüfung der Eingabe implementiert haben. Zu den Klassikern in diesem Umfeld zählen beispielsweise die Funktionen `gets` oder `strcpy`.

In modernen Compilern werden diese Fehler nun während der Kompilierung angegangen und Gegenmaßnahmen eingeleitet. Aufgrund der Menge des Quellcodes und der bereits im Einsatz befindlichen Kompilate wird die Anfälligkeit eine lange Zeit weiter bestehen.

Viele (aktuelle) Schwachstellen basieren auf immer neu entdeckten Buffer-Overflow-Ausnutzungen. Teilweise werden diese Schwachstellen zu horrenden Preisen im Darknet gehandelt[27].

Einzige Gegenmaßnahme an dieser Stelle ist: Austausch des Programm-Codes gegen einen nicht mehr anfälligen Code, das sogenannte Patchen.

3.2 Betriebssystem-Patches

Wie in Abschnitt 3.1 beschrieben, sind Fehler innerhalb von Betriebssystemen als besonders kritisch zu betrachten, da hiermit Schadcode mit erweiterten Rechten ausgeführt werden kann. In diesem Sinne sollten Security-Patches eine hohe Priorität innerhalb des Betriebs genießen.

Aber auch andere Patches, sprich „normale“ Fehlerbehebung, sollte nicht unberücksichtigt bleiben, da es Ziel eines IT-Betriebes sein sollte, eine möglichst stabile und damit fehlerfreie Umgebung zu besitzen.

Beispiel 3.1:

Ein Systemadministrator blickte ganz stolz auf einen Windows 2008 Server, der laut Monitoring seit 999 Tagen ohne Reboot lief. Für ihn war dies ein Zeichen von Stabilität. Die Informationssicherheit dagegen war tief betroffen. 999 Tage ohne Reboot hieß in Konsequenz: keine Updates eingespielt, keine erforderlichen Reboots durchgeführt, ein System, das wahrscheinlich inkonsistent und fehlerbehaftet war.

Je nach Betriebssystem gibt es unterschiedliche Verfahren zum Update des Systems. Der Heimanwender von Windows wird in der Regel (hoffentlich) die automatischen Updates über Microsoft eingeschaltet haben. Damit holt sich der Rechner selbstständig die benötigten Dateien aus dem Internet und installiert diese.

Innerhalb einer Firma wird für Microsoft-Umgebungen meist ein sogenannter ▸WSUS Server (WSUS = Windows Server Update Services) aufgesetzt. Hierbei handelt es sich um ein System, das sich zentral die Updates von Microsoft herunterlädt und anschließend auf die Systeme im Haus verteilt. Microsoft schreibt hierzu „Microsoft Windows Server Update Services ermöglicht IT-Administratoren die Bereitstellung der neuesten Microsoft-Softwareupdates auf Computern mit Windows-Betriebssystemen. Mit WSUS erhalten Administratoren umfassende Verwaltungsmöglichkeiten für die Verteilung von Updates, die über Microsoft Update veröffentlicht werden.“[28]

27. Vgl. http://www.zdnet.de/88252426/zerodium-veroeffentlicht-preisliste-fuer-zero-day-luecken/.
28. Vgl. https://technet.microsoft.com/de-de/windowsserver/bb332157.aspx.

Mittels dieser Technologie hat die Systemadministration die Möglichkeit, Einfluss auf die Verteilung der Updates zu nehmen, da in Produktionsumgebungen keine automatische Installation gewünscht ist (vergleiche Abschnitt 3.7). So kann beispielsweise gesteuert werden, dass lediglich Sicherheitspatches unmittelbar installiert werden sollen und für andere Updates andere Verfahren gelten.

Linux-Systeme bieten heute ebenfalls Möglichkeiten, Systemupdates automatisiert zu installieren. Die Werkzeuge hierfür unterscheiden sich je nach Derivat – insbesondere im Umfeld der Enterprise-Produkte.

Darüber hinaus gibt es mittlerweile eine Vielzahl an Dritthersteller-Komponenten, die sich mit dem Thema Patching auseinandersetzt.

Unabhängig vom Thema Patching ist allerdings das Update zu sehen. Hier handelt es sich insbesondere um die Major Updates, sprich die gravierenden Versionssprünge (Windows 2008 auf Windows 2012, SuSE SLES 11 auf SuSE SLES 12 etc.).

Diese Veränderungen einer Systemumgebung müssen in der Regel als Projekt aufgesetzt werden und führen oftmals zu einer Neuinstallation von Systemen.

Ein Knackpunkt, der im Rahmen der Updateplanungen und des Patch-Managements zu berücksichtigen ist, ist die Software, die auf den entsprechenden Systemen läuft. Updates ohne Berücksichtigung der Anwendungen und der Middleware durchzuführen kann im schlimmsten Fall zu einem Systemversagen führen.

Bevor Updates installiert werden, ist zu prüfen, inwieweit die sonstige Software auf dem betroffenen Betriebssystem Freigaben für das Update hat.

Genau diese Problematik führte dann in der Praxis oft zu der Lösung, die mit folgendem geflügelten Satz umschrieben wird: „never touch (patch) a running system." Im Extremfall führte dies zu einem Weiterbetrieb von Betriebssystemen weit über den Supportzeitraum[29] hinaus.

Beispiel 3.2:

Windows XP ist ein gutes Beispiel für eine übermäßige Strapazierung der Betriebsdauer. Am 8. April 2014 wurde der Support für Windows XP nach 12 Jahren eingestellt. Trotzdem wurde (und wird) dieses Betriebssystem weiter eingesetzt. Aus Sicht der Informationssicherheit ist der Einsatz inzwischen als grob fahrlässig einzustufen[30].

Auch heute werden Sie vereinzelt noch Systeme finden, die lange aus dem Support sind. Aufgabe der Informationssicherheit ist es, diese Systeme zu identifizieren und Lösungen zu finden.

Leider (aus Sicht der Informationssicherheit) gibt es in Einzelfällen tatsächlich den begründeten Bedarf für einen Betrieb über den Supportzeitraum hinaus. In diesen Fällen muss sichergestellt werden, dass die Systeme abgeschottet betrieben werden und von ihnen keine Gefahren ausgehen – selbst wenn sie erfolgreich gehackt worden wären.

29. Innerhalb des Supportzeitraumes werden Sicherheitsupdates zur Verfügung gestellt. Nach Ablauf des Supports gefundene Fehler und Sicherheitslücken werden nicht mehr geschlossen.
30. Vgl. https://www.heise.de/newsticker/meldung/Datenschutzbeauftragte-warnt-vor-Zeitbombe-Windows-XP-2639158.html.

3.3 Middleware

Unter den Bereich Middleware fallen insbesondere die üblichen „Zwischensysteme“ zwischen Betriebssystem und der eigentlichen Anwendung, sprich: Datenbank, Webserver etc.

Die namhaften Hersteller veröffentlichen ihrerseits regelmäßig Updates und Patches für ihre Lösungen[31]. Im Gegensatz zu den Betriebssystemen ist hier meist ein händisches Vorgehen seitens der Systemadministration notwendig. Das bedeutet, dass sich die verantwortlichen Administratoren selbst damit befassen müssen, ob Updates vorliegen (siehe hierzu auch Abschnitt 5.1). Im Anschluss müssen die entsprechenden Updates eingeplant und eingespielt werden.

Die meisten Anbieter von Middleware-Lösungen sind sich inzwischen der Problematik im Umfeld IT-Sicherheit bewusst und arbeiten aktiv an der Behebung von Schwachstellen mit.

3.4 Anwendungen

Als Anwendungen bezeichnen wir in diesem Zusammenhang alle Fachapplikationen, die auf einem Betriebssystem – und ggf. einer Middleware-Komponente – aufsetzen. Auch diese Softwareprodukte beinhalten Fehler. Aus der persönlichen Erfahrung weiß ich, dass bei den Herstellern von Anwendungssoftware eine große Bandbreite hinsichtlich des Verständnisses für Informationssicherheit vorhanden ist.

Beispiel 3.3:

> Anfrage: „Bei dem Produkt XYZ Ihres Hauses bin ich dabei über die Tatsache gestolpert, dass als Betriebsplattform auf JBOSS5 gesetzt wird [...] Die JBOSS5 hatte ein Ende des Full-Supports im November 2013 und das Ende des Maintenance Supports ist im November 2016. Darüber hinaus sind eine Vielzahl von Verwundbarkeiten für die unterschiedlichen 5er Versionen bekannt, veröffentlicht und in der aktiven Ausnutzung.“
>
> Antwort: „XYZ ist nur mit JBoss 5 wie beschrieben einsetzbar. Warum wollen Sie JBoss 7 nutzen? Die XYZ-Software ist auf JBoss 5 getestet und nur dafür freigegeben.“

Beim Betrieb von Applikationen muss man sich tatsächlich darüber bewusst sein, dass Fehler teilweise nicht behoben werden – aber vielleicht auch nicht bekannt werden.

Für die Praxis empfiehlt es sich, eine Inventur durchzuführen, um die kritischen Applikationen zu identifizieren und sich diese im Detail anzuschauen.

1. Bietet der Hersteller Patches und Updates an?
   a) Wenn ja, in welchem Intervall?
   b) Wenn nein, kann man den Hersteller „dazu bewegen“?
2. Wurden eigene Tests (Penetrationstests) gegen die Anwendung durchgeführt?

31. Beispiel: Security-Updates von Oracle: http://www.oracle.com/technetwork/topics/security/alerts-086861.html.

3. Gibt es eine Kommunikationsmatrix, d.h., ist bekannt, welche Adresse über welche Portnummern kommuniziert?
4. Lassen sich die Systeme separieren und abschotten?

Diese Fragen sollte man für sich selbst beantworten und ggf. Maßnahmen zur Absicherung treffen. Im Worst Case bleibt nur eine Risikoübernahme durch die Geschäftsleitung.

3.5 Schwachstellenerkennung

Schwachstellen-Scanning bezeichnet das automatisierte Untersuchen von Systemen nach bekannten Schwachstellen. International hat sich ein Verfahren etabliert, über das Schwachstellen in IT-Systemen katalogisiert und verwaltet werden. Hierzu hat die Mitre[32] eine Namenskonvention entwickelt. Es handelt sich hierbei um den ▸CVE-Standard (Common Vulnerabilities and Exposures). Dieser stellt sicher, dass Schwachstellen eindeutig identifizierbar sind und mit einer Nummer ausgestattet wurden.

Diese bekannten und beschriebenen Schwachstellen können mittels sogenannter Schwachstellenscanner „ausprobiert“ werden. Ein Schwachstellenscanner arbeitet hierbei in etwa in folgender Weise:

- Identifikation von Systemen
- Prüfung der offenen Ports
- Identifizierung des Betriebssystems
- Identifizierung der installierten Services und Programme
- Prüfung der entsprechenden Komponenten auf die bekannten Schwachstellen

Der Einsatz dieser Technologie ist allerdings mit einer gewissen Portion Vorsicht durchzuführen. Läuft beispielsweise ein Intrusion-Prevention-System (▸IPS) oder ein Intrusion-Detection-System (▸IDS), so werden diese Systeme den Scan im Zweifel als Angriff erkennen und einstufen.

Weiterhin unterstützen die meisten Schwachstellen-Scanner die Möglichkeit, die „Härte des Angriffs“ einzustellen. So können beispielsweise Tests auf theoretische Anwendbarkeit von Exploits gefahren werden oder aber die Exploits tatsächlich ausprobiert werden. Weiterhin kann man wählen, ob man nur passende oder alle Exploits testen möchte. Bei einem Test mit allen Exploits würden z. B. auch Linux-Schwachstellen gegen ein erkanntes Windows-System probiert werden.

Beispiel 3.4:

Im Rahmen des ersten Einsatzes eines Schwachstellen-Scanners kam die Aussage vom Leiter des Betriebs: „Testet ruhig die komplette DMZ. Eine DMZ muss so etwas aushalten können.“ 30 Minuten nach Start des Tests wurde dieser abgebrochen, da der Schwachstellen-Scanner einige Systeme komplett zum Erliegen gebracht hatte.

Die Ergebnisse eines solchen Tests sehen wie in Abb. 3.1 aus. Hier wurde mittels des freien Scanners OpenVAS ein altes Windows NT 4.0 geprüft. Die gefundenen Ergebnisse werden jeweils mit einem Schweregrad (Severity) zwischen 0 und 10 bewertet.

32. Siehe http://cve.mitre.org/.

Beispiel 3.5:

In einem Gespräch mit einem Administrator sagte dieser im Hinblick auf ein UNIX-System aus dem Jahr 1995: „Quatsch, so ein altes System ist kein Sicherheitsrisiko. Damit kennt sich doch niemand mehr aus."

Das Windows NT 4.0-System wurde speziell für dieses Beispiel aufgesetzt und befand sich ca. 20 Minuten im Internet. Der Severity Code 10 belegt, dass auf dem System innerhalb dieser Zeit offensichtlich erfolgreich ein Trojaner aufgebracht wurde. Dies demonstriert die hohe Standardisierung und Automation im Umfeld der Schadsoftware. Ungeschützte Systeme werden innerhalb kürzester Zeit erkannt und zu Teilen von Botnetzen.

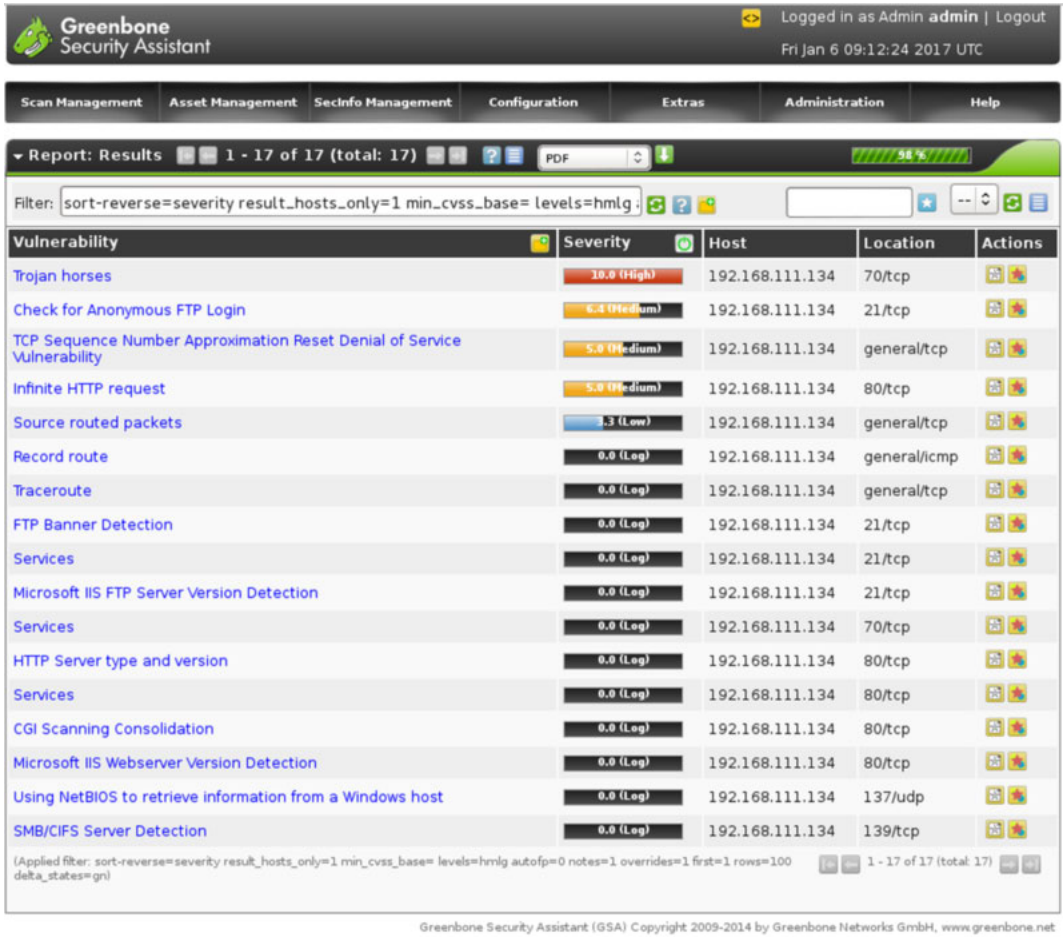

Abb. 3.1: Schwachstellen-Scan mit OpenVAS

Betrachtet man die Vulnerability im Detail, so zeigt sich das Bild, das Sie in Abb. 3.2 sehen:

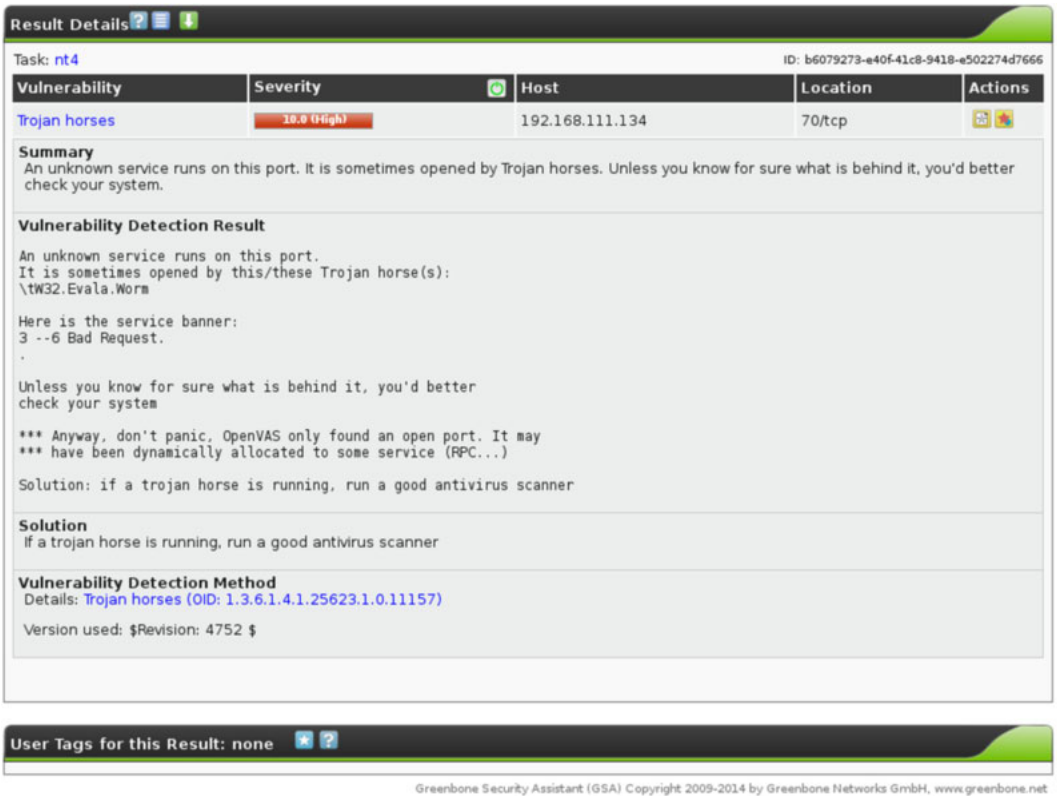

Abb. 3.2: Erkannter aktiver Trojaner

Das Durchführen von regelmäßigen Schwachstellen-Scans kann dazu genutzt werden, den Erfolg des Patch-Managements zu überprüfen. Weiterhin bietet die Funktion des System-Discovery auch die Möglichkeit, Systeme im Netz durch den Scanner auffinden zu lassen. Hierdurch fallen auch „vergessene“ Systeme auf.

Finales Ergebnis des Schwachstellen-Scannings können daraus resultierende Changes (siehe Abschnitt 3.7) zum Update oder zur architektonischen Veränderung von Systemen sein. Generell kann man die Erkennung von potenziellen Gefahren in diesem Zusammenhang auch als einen Teil eines proaktiven Problem Managements nach ITIL einstufen.[33]

3.6 Monitoring

Monitoring ist eine Methode der laufenden Systemüberwachung. Es überprüft die einzelnen Systeme im Betrieb hinsichtlich festgelegter Parameter. Insbesondere werden Systemlast, Auslastung der Plattensysteme, aber auch das Laufen verschiedener Services überwacht. Im Endausbau kann im Rahmen eines sogenannten Ende-zu-Ende-Monitorings sogar ein kompletter Geschäftsprozess regelmäßig durchlaufen werden, um die Gesamtfunktionalität zu prüfen.

33. Vgl. Stasch, 2012.

Beispiel 3.6:

Betreiber von Shopsystemen können im Rahmen eines Ende-zu-Ende-Monitorings beispielsweise einen kompletten Bestellprozess mit Zahlung durchführen, um im Fehlerfall schnell reagieren zu können.

Aber auch für die Informationssicherheit hat das Monitoring eine hohe Bedeutung. So sagt Eckert: „Notwendig ist ein Monitoring und Kontrollieren der Systemaktivitäten möglichst ohne Unterbrechung, um insbesondere auch auf neue Bedrohungen schnell reagieren zu können.“[34]

Im Fehlerfall generiert ein Monitoring-System sogenannte Events, die im Rahmen des Event-Managements nach ITIL verarbeitet werden und schlussendlich in Incidents münden.

Definition 3.1:

Ein Incident ist eine nicht geplante Unterbrechung eines IT-Service oder eine Qualitätsminderung eines IT-Service. Auch ein Ausfall eines Configuration Item ohne bisherige Auswirkung auf einen Service ist ein Incident.[35]

Aus Sicht des Betriebs spielt das Monitoring insbesondere eine Rolle im Umfeld der Überwachung-SLAs (Service Level Agreements) und der Verfügbarkeit von Systemen und Diensten.

Ein Monitoring kann ein gutes Ausgangssystem für die bereits unter Abschnitt 2.2.4 beschriebenen SIEM-Lösungen sein. Bei einem gut aufgesetzten Monitoring findet man zu jedem System auch die sicherheitsrelevanten Informationen, seien es Patch-Stände, Status des Virenschutzes mit Information über die Version des Pattern-Standes, letzter Reboot oder aber auch Auffälligkeiten hinsichtlich von Anmeldeversuchen.

Innerhalb der Maßnahmenkataloge des BSI findet man Bausteine hinsichtlich der Überwachung einzelner Technologien. Die Vorgaben sind teilweise sehr dezidiert beschrieben, sodass die Verantwortlichen für Monitoring bzw. Systemadministration daraus direkt Schwellwerte entnehmen können, die zu Events führen sollten.

Eine besonders detaillierte Beschreibung finden Sie im Baustein M4.316 zur Überwachung des Active Directory[36].

3.7 Change-Management

Change-Management ist ein Prozess zur Unterstützung von Veränderungen. Das BSI spricht in diesem Zusammenhang gerne vom Veränderungsmanagement, allerdings sollte man – meiner Meinung nach – hier die international gebräuchliche und in ITIL definierte Bezeichnung des Change-Managements anwenden.

34. Eckert, 20014 S. 214.
35. Taylor et al, 2007, S. 53.
36. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04316.html.

Definition 3.2:

Service Change bezeichnet das Hinzufügen, Modifizieren oder Entfernen eines autorisierten, geplanten oder unterstützenden Service oder einer entsprechenden Servicekomponente und der dazugehörigen Dokumentation.[37]

Für eine funktionierende Informationssicherheit innerhalb eines Unternehmens ist das Change-Management als Pflicht zu sehen.

Das Change-Management befasst sich mit beabsichtigten, planbaren Änderungen an einem Service oder einer Komponente. Wichtig im Rahmen des Change-Managements ist es, dass jeder Change dokumentiert und freigegeben werden muss. Bei Einführung dieses Prozesses innerhalb einer IT-Organisation führt dies zu Beginn meist zu einer ablehnenden Haltung bei den Mitarbeitern. Die Argumente verweisen auf einen zu starken Formalismus, Dokumentationszwang und den Verlust von Flexibilität. Diesen Argumenten gegenüber stehen allerdings eine neu gewonnene Nachvollziehbarkeit, vereinfachte Störungsbeseitigung durch Rückschlüsse aus Changes und insbesondere die Vermeidung von Fehlern durch unberücksichtigte Abhängigkeiten. Ein vermeidlicher Verlust der Flexibilität kann durch eine sinnvolle Klassifizierung und unterschiedliche Freigabeprozesse im Rahmen des Change-Managements weitestgehend vermieden werden. Die wichtigsten Punkte für die Freigabeprozesse stellen sich wie folgt dar:

Auf Basis des Standardverfahrens, wie es in ITIL beschrieben ist, werden innerhalb der ersten Prozessschritte des Change-Managements die sogenannten sieben Rs geprüft:

- Raise: Wer hat den Change initiiert?
- Reason: Was ist der Grund für den Change?
- Return: Was bringt der Change aus Sicht des Business?
- Risk: Welches Risiko besteht durch die Implementierung des Changes? Und welche Gegenmaßnahmen werden ergriffen?
- Resources: Wer führt den Change durch? Welche Ressourcen sind notwendig?
- Responsible: Wer trägt die Verantwortung für den Change (inkl. Entwicklung und Test)?
- Relationship: Welche Beziehungen oder Auswirkungen bestehen zu anderen Changes?[38]

Diese Fragestellungen werden im Rahmen des Change Advisory Board (▸CAB) beraten und anschließend freigegeben. Auch wenn der Begriff „Advisory“ auf eine eher beratende Funktion schließen lässt, so ist das CAB in den meisten Organisationen eine entscheidende Instanz. Je nach Größe der Organisation kann es vorkommen, dass es auch gestaffelte CABs gibt.

Durch die Implementierung des Change-Management-Prozesses wird insbesondere am Ziel der Verfügbarkeit gearbeitet. Ein weiterer Nebeneffekt ist aber auch, dass man im Rahmen des Freigabeverfahrens die Informationssicherheit als festen Bestandteil involvieren kann (sollte). Das Change-Management wird als einer der wichtigsten Prozesse aus ITIL innerhalb der Informationssicherheit angesehen[39].

37. Vgl. Lacy et al., 2007, S. 46.
38. Vgl. Lacy et al., 2007, S. 57.
39. Vgl. Cazemier et al., 2010, S. 59.

Neben der Beteiligung innerhalb der Freigabe und ggf. auch innerhalb des CABs besteht eine weitere enge Verzahnung mit der Informationssicherheit aus den Umfeldern des Update- und Patch-Managements, das wie weiter oben beschrieben auch aus dem Schwachstellen-Management angetriggert werden kann.

Ebenso ist im Rahmen des Change-Managements abgestimmt festzulegen, welche Patches als Pre-Authorized Changes eingestuft werden können.

Definition 3.3:

Ein Pre-Authorized Change ist eine Veränderung mit einem geringen kontrollierten Risiko, der einfach und entsprechend vorhandenen Prozeduren umgesetzt werden kann.

Beispiele für solche Changes wären z.B. Patches für Betriebssysteme, Veränderungen von Firewall-Regeln und Ähnliches. Durch die Forderung nach einem dokumentierten Prozedere kann sichergestellt werden, dass die Informationssicherheit standardmäßig eingebunden wird und ggf. eine Entscheidungsinstanz ist.

Im Rahmen von dringenden Security Patches ist im Zweifel sogar ein ▸ECAB (Emergency CAB) mit dem Notfall-Change-Prozess zu initiieren.

Beispiel 3.7:

Im Rahmen der Entdeckung der Heart-Bleed-Lücke am 03.04.2014 (CVE-2014-0160) stellte sich heraus, dass nahezu alle SSL-Implementierungen im Internet betroffen waren und bereits Angriffsvektoren bekannt und genutzt wurden.[40] Entsprechend mussten innerhalb kürzester Zeit aufseiten des Betriebs Maßnahmen erfolgen. Die Eile machte den Durchlauf eines regulären Change-Prozesses unmöglich.

Wichtig in diesem Zusammenhang ist – wie eigentlich meistens –, dass man sich im Vorfeld mit den möglichen Situationen befasst und entsprechende Vorkehrungen trifft.

Zusammenfassung

Das Themenfeld der Updates spielt in der Informationssicherheit eine zentrale Rolle. Fehlende Updates führen zu Sicherheitslücken, die aktiv genutzt werden können, oder aber zu einer Einschränkung der Betriebsstabilität.

Willkürliches Updaten auf der anderen Seite birgt andere Gefahrenquellen und kann direkte Auswirkungen auf die Verfügbarkeit haben.

Es gilt also das Themenfeld ganzheitlich vom Betriebssystem über die Middleware bis hin zu den Applikationen zu betrachten, Verfahren zu implementieren, die Lücken sichtbar machen und Prozesse einzuführen, die für eine Schließung der Schwachstellen verantwortlich sind.

40. Vgl. http://heartbleed.com/.

Aufgaben zur Selbstüberprüfung

3.1 Machen Sie sich bitte einmal Gedanken, wie Sie in einem Unternehmen automatische Windows-Updates einspielen lassen wollen. Hierbei gilt: Aufgrund der Kritikalität der Clients ist ein sofortiges Einspielen (nach Herausbringung des Patches) ausgeschlossen.

3.2 Suchen Sie nach dem CVE-Eintrag für den sogenannten Ping of Death. Mit diesem konnte man über übergroße ▸ICMP-Pakete komplette Systeme zum Absturz bringen. Bitte nennen Sie die CVE-Nummer.

3.3 Erklären Sie bitte kurz, warum auch das Update eines Browsers ein Change ist. Geben Sie bitte eine Möglichkeit an, wie man den Prozess schlank halten kann.

4 Security-Produkte

In diesem Kapitel werden Sie die aktuell gängigsten Sicherheitsprodukte kennenlernen, die zum einen die Sicherheit in Ihrem Unternehmen erhöhen (können) oder aber den Prozess der Informationssicherheit aktiv unterstützen (können). Nicht alle Lösungen werden Sie einsetzen, aber Sie werden sich nach dem Studium des Kapitels selbst ein Bild darüber machen können, welche Produkte für einen Basisschutz sinnvoll sind und was nur „nice to have" ist.

Wenn Sie im Umfeld der Informationssicherheit tätig sind oder sein werden, werden Sie Kontakt zu sehr vielen aktiven Vertriebsmitarbeitern bekommen, die Ihnen die einzig wahre Lösung verkaufen wollen, die Ihr Unternehmen absichert. An Ihnen liegt es, die Angebote zu bewerten, sie mit dem Gefährdungspotenzial abzugleichen und passend zum verfügbaren Budget Lösungen zu erarbeiten (oder das Risiko versichern zu lassen oder zu tragen).

4.1 Virenschutz

Virenschutz gehört zu den absoluten Basics in der Informationssicherheit. Keinen Virenschutz installiert zu haben wäre eine grobe Fahrlässigkeit. Systeme, die auch nur eine kurze Zeit ohne entsprechende Schutzmaßnahmen im Internet erreichbar sind, werden durch entsprechende Robots identifiziert und infiziert (vgl. Abschnitt 3.5).

Microsoft-Betriebssysteme werden heute mit dem eigenen Virenscanner Microsoft Defender ausgeliefert. Andere Systeme bringen von Haus aus keinen Schutz mit.

Auf jedes System gehört ein Virenschutz. Betriebssysteme, die sicher sind und für die keine Viren existieren, gibt es per Definition nicht. Diese Regel gilt auch für Betriebssysteme auf mobilen Devices, wie Tablets und Smartphones.

Für welches Produkt Sie sich entscheiden, ist dabei zweitrangig. Ihnen werden die Hersteller der unterschiedlichen Produkte sicherlich ▸USP (Unique Selling Propositions – Alleinstellungsmerkmale) präsentieren, aber Sie sollten darauf bedacht sein eine Produktauswahl zu treffen, die in Ihre Umgebung hineinpasst und vom Supportaufwand handhabbar ist.

Beispiel 4.1:

Im Rahmen einer Produktauswahl wurde eine Virenschutzlösung ausgewählt, die sowohl für Windows wie auch Linux-Systeme einsetzbar war. Innerhalb der Implementierung unter Linux zeigte sich, dass weder die Installation noch die Pattern-Updates automatisierbar waren und das Produkt zusätzlich eine Middleware-Komponente benötigte, die erfahrungsgemäß oft mit Schwachstellen glänzt.

Entsprechend den Erfahrungen musste eine komplette Neuauswahl erfolgen.

Innerhalb der Konzeptionsphase gilt es auch, sich Gedanken über einige grundlegende Fragestellungen zu machen. Im Rahmen des Virenschutzes ist beispielsweise eine Best Practice, sich nicht auf ein Produkt zu stützen, sondern eine sogenannte Zwei-Produkt-Strategie zu fahren. Diese besagt, dass eingehende (und ggf. auch ausgehende) Dateien

grundsätzlich die Prüfung von zwei unterschiedlichen Anti-Virus-Produkten erfahren müssen. Die Begründung hierfür ist, dass durch die unterschiedlichen Prioritäten und Pattern-Updates so eine höhere Sicherheit erreicht werden kann.

Innerhalb größerer Organisationen ist es unabdingbar, dass die zum Einsatz kommenden Produkte eine zentrale Management-Plattform bieten. Diese dient zur Überwachung der Gesamtlage. Hierzu zählen neben den Virenfunden insbesondere auch:

- Patch-Status der Clients (inkl. Patterns)
- automatisierte Ausbringung der Clients
- zentrale Verwaltung von On-Demand-Scans
- zentrale Meldung von Funden
- Steuerung der Clients mittels Regeln

Virenschutz geht im Gesamtkontext deutlich über die Installation eines Virenscanners hinaus. So gehört auch die Sensibilisierung der Mitarbeiter zu den Grundbelangen, um möglichst viele Gefahren (z.B. durch Öffnen von schadhaften Dateianhängen an E-Mails) zu verhindern.

In einem weiteren Schritt ist das operative Personal im Umfeld von Clients und Servern hinsichtlich Virenbefall zu schulen und ein Vorgehensmodell aufzustellen, wie man mit den Bedrohungen umgeht und welche händischen Möglichkeiten es noch gibt, Schadsoftware zu erkennen.

Machen Sie sich Gedanken darüber, wann Sie einer Virenschutzlösung vertrauen wollen und wann Sie bei einem Befall eine komplette Neuinstallation eines Systems verlangen[41].

Kein Virenschutz bietet eine 100%ige Sicherheit.

In der Praxis darf nie in Vergessenheit geraten, dass das Geschäft mit Schadsoftware hochprofessionalisiert funktioniert. Entsprechend werden Schadprogramme nicht mehr händisch programmiert, sondern generiert. Dies führt zu einer immens hohen Zahl an Schadprogrammen, die täglich hinzukommen. Laut Heise liegt die Anzahl derzeit bei ca. 390 000 neuen Schadprogrammen täglich![42] Dies verdeutlicht, dass Virenscanner nicht in der Lage sind, jede Bedrohung zu identifizieren. In der Praxis werden auch nicht mehr alle bekannten Viren-Patterns lokal auf Ihrem Rechner im Virenschutz vorgehalten, sondern nur noch die, die beobachtet aktuell im Umlauf sind. Ältere Schadprogramme würden wahrscheinlich wieder erfolgreich durchschlagen.

Ebenso erkennen Scanner nur bekannte Schadsoftware. Eine heuristische Erkennung liefert zwar heute gute Indizien, aber nicht sicher.

Im Rahmen einer Untersuchung habe ich beispielsweise im April 2016 eine Ransomware namens `ransom.exe` generieren lassen. Stand Januar 2017 wird dieser Verschlüsselungstrojaner nur von einer geringen Anzahl an Virenscannern erkannt, vgl. Abb. 4.1.

41. Vgl. Phan et al., 2015, S. 14 ff.
42. Vgl. https://www.heise.de/newsticker/meldung/Zahlen-bitte-Taeglich-390-000-neue-Schadprogramme-3177141.html.

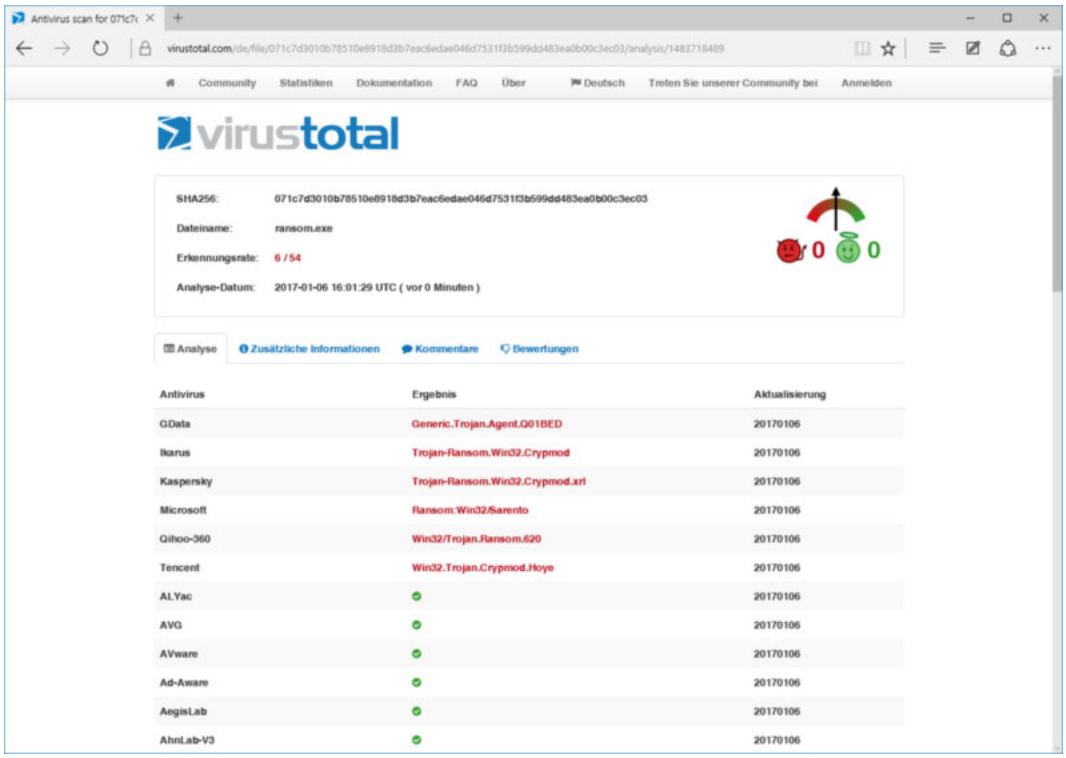

Abb. 4.1: Check einer Ransomware mittel Virustotal.com

Lediglich 6 von 54 Virenscannern erkennen die Datei `ransom.exe` als Schadsoftware.

Mindestens innerhalb der Zeitspanne zwischen der ersten Verbreitung einer Schadsoftware und der ersten Erstellung einer Signatur bzw. dem Blacklisten des dazugehörigen Hashwertes sind alle Systeme ungeschützt.

Ein wertvolles Hilfsmittel in diesem Zusammenhang ist, ein externes Boot-Medium mit verschiedenen Virenscannern zu haben, die sich aus dem Medium updaten. Ziel ist es, eine definiert saubere Startumgebung zu haben, deren Aufgabe es ist, sich das lokale Dateisystem einzuhängen und quasi von außen einen Scan durchzuführen.

Der Heise-Verlag bringt einmal im Jahr eine CD/DVD heraus, die sich hierfür sehr gut eignet: die Heise Desinfec't[43]. Die DVD 2016 basiert auf Ubuntu und beinhaltet die Virenscanner von Avira, Bitdefender, Kaspersky und ClamAV. Nach dem Start und Update der Signaturen werden die lokalen Platten im Schreib-Lese-Zugriff eingehängt und der Scan startet. Hierdurch lassen sich auf der Festplatte auch bekannte Root-Kits oder Ähnliches zu finden, die sich in einem laufenden System verbergen.

43. Vgl. https://www.heise.de/download/product/desinfect-71642.

4.2 Whitelisting

Ein weiterer Ansatz gegen Schadprogramme ist die Einführung eines sogenannten Whitelistings. Hierbei werden nur Programme ausgeführt, die in einer Whitelist stehen. Das Verfahren entspricht in etwa der Funktionsweise einer Firewall. Auch hier ist grundsätzlich alles verboten, was nicht explizit erlaubt ist. Eine schöne, kurze, aber übersichtliche Zusammenfassung zu Black- und Whitelisting finden Sie auf den Webseiten der Universität Rostock[44].

Schadprogramme, die von außen kommen, sind (logischerweise) nicht in der Erlaubnisliste enthalten und die Ausführung wird blockiert. Die Hersteller entsprechender Systeme sagen (Werbe-Aussage), dass man beim Einsatz sogar auf den Virenschutz verzichten kann.

In der Praxis funktionieren die Systeme in der Regel via Hashwert. Von erlaubten Programmen wird der Hash-Wert in einer Datenbank abgelegt und vor dem Start jeder Anwendung eine Prüfung durchgeführt.

Für Umgebungen, die keinen starken Veränderungen unterworfen sind, ist der Ansatz empfehlenswert. Ändert sich die Landschaft allerdings stetig (z.B. durch eigene Softwareentwicklung oder eine sehr hohe Anzahl an benötigter Software), so entsteht ein hoher administrativer Aufwand, um die neuen Programme zuzulassen. Dies muss entsprechend fest im Change-Management-Prozess (siehe Abschnitt 3.7) berücksichtigt werden. Die Freigabe erfolgt meist an expliziten Anlern-Rechnern.

Ein weiterer Knackpunkt liegt im Umfeld der Einführung. Da es illusorisch ist, jedes benötigte Programm händisch zu erfassen, durchläuft man zum Start eines entsprechenden Projektes eine Aufzeichnungsphase. In dieser werden alle Programmstarts registriert. Man kann die Liste im Nachgang modifizieren. Hier kann es gut sein, dass eine bereits im System aktive Schadsoftware nicht gefunden, aber im Rahmen der ersten Erfassung in die Erlaubnisliste aufgenommen wird.

Aufgrund der systemtechnischen Anforderungen mancher Software wird man auch bei einer Whitelist-Lösung wahrscheinlich einige Verzeichnisse auf Rechnersystemen aus der Überwachung ausschließen müssen. So gibt es beispielsweise Anwendungssoftware, die dynamisch ausführbare Dateien generiert. Diese können im Vorfeld nicht erfasst werden und würden in Konsequenz an der Ausführung gehindert werden.

Schon wegen dieser wahrscheinlichen Einschränkungen ist es daher nicht geraten, auf einen Virenschutz zu verzichten.

4.3 Lokale Firewall

Deaktiviert man in einem Firmennetz die lokalen Firewalls auf den einzelnen Systemen oder lässt man sie ihre Arbeit verrichten? Diese Frage wird oft genug aufgeworfen werden. Das Statement der Informationssicherheit ist hier einfach und knapp: Die Firewall wird verwendet.

44. Vgl. http://www.itmz.uni-rostock.de/software/windows/sicherheit/software-whitelisting-der-bessere-virenschutz/.

Ziel einer Firewall ist es, unerlaubten Traffic zu verhindern. Der Grund, warum innerhalb von Firmennetzen die lokalen Firewalls trotzdem oftmals disabled sind, liegt ganz simpel darin begründet, dass oftmals Kommunikationsprofile fehlen und deswegen gar nicht im Detail bekannt ist, welche Kommunikation gewünscht und erlaubt und welche ggf. verboten ist.

Die Empfehlung des BSI lautet lediglich: „Prinzipiell sollten alle Server mit hohem Schutzbedarf mit einem lokalen Paketfilter geschützt werden.“[45] Es handelt sich ansonsten um eine Kannvorschrift.

Im Sinne einer sicherheitsbewussten Gesamtarchitektur sollte der Einsatz allerdings auf allen Systemen erfolgen.

Eine ganz spezielle Frage sollten Sie aber in diesem Zusammenhang stellen und beantworten: Wie wird mit ICMP (Internet Control Message Protocol) umgegangen? Von außen wird generell empfohlen, dieses Protokoll nicht zu erlauben. Intern erleichtert es allerdings die Fehlersuche (via ping, traceroute) deutlich.

Beispiel 4.2:

Die beliebteste Rückfrage von Netzwerk-Technikern im Fehlerfall lautet: „Kannst du die Maschine pingen?“

Im Rahmen einer besseren Supportfähigkeit kann es somit schon sinnvoll sein, auf den lokalen Firewalls ICMP nicht zu blocken.

4.4 Token

Wenn in der Informationssicherheit von Token gesprochen wird, handelt es sich in der Regel um Security Token, d.h. elektronische Hilfsmittel zur Authentifizierung. Token kommen sowohl als Hardwarekomponente (Abb. 4.2) wie auch als Softwarelösung, wie Smartphone Apps, vor.

Abb. 4.2: Hardware-Token

45. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04238.html.

Der Verwendungszweck dieser Hilfsmittel liegt meist darin, eine Zwei-Faktor-Authentisierung zu ermöglichen. Hierbei fallen die Token in die Kategorie „Besitz“, da man das Token besitzen muss, um den angezeigten Sicherheitscode (der sich laufend ändert) zu kennen. In der Praxis sieht es dann in der Regel so aus, dass ein Benutzer zur Anmeldung an einem System seinen Benutzernamen und sein Passwort (Kategorie: Wissen) und den angezeigten Code auf dem Token eingeben muss.

Offensichtlicher, dass es sich um das Merkmal „Besitz“ handelt, wird es bei Token, die als Smartcard in einen Rechner eingesteckt oder per Funk in der Nähe des Rechners sein müssen.

Mittlerweile gibt es eine Vielzahl an unterschiedlichen Security Token. Hintergrund hierfür ist sicherlich auch die Erkenntnis, dass der Schutz mittels Passwörtern nicht mehr ausreichend ist. Ein Token, der theoretisch zukünftig jedem Bundesbürger zur Verfügung stehen könnte, ist die ▸eID-Funktion des elektronischen Personalausweises.

4.5 Schutzkarten (Wächterkarten)

Die Idee der Schutzkarten stammt aus dem pädagogischen Umfeld. Hier waren Schulen in der Vergangenheit mit der Problematik konfrontiert, dass die Schüler während des Unterrichts die Einstellungen und Programme an den Schulrechnern veränderten, sodass die Lehrerinnen und Lehrer sich nicht auf eine konsistente Systemkonfiguration auf allen Geräten verlassen konnten.

Abhilfe brachten dazu die Schutzkarten. Sie stellten sicher, dass man innerhalb kurzer Zeit zu einem definierten Zustand der Festplatte zurückkehren konnte. Dazu gab oder gibt es zwei verschiedene Ansätze.

Im ersten Ansatz ist die zu schützende Partition durch die Schutzkarte schreibgeschützt. Schreiboperationen werden auf eine separate Partition umgelenkt, von der dann die „variablen“ Daten wieder gelesen werden. Nach außen hin wird allerdings eine normale Festplatte angezeigt, d.h., selbst für das Betriebssystem bleibt diese Aufteilung transparent. Durch ein Leeren der Partition mit den variablen Daten lässt sich der Ursprungszustand sofort wiederherstellen.

Der zweite – wesentlich zeitintensivere – Lösungsansatz ist, dass es ein verstecktes Image der Festplatte gibt, das bei Bedarf zurückgespielt werden kann.

Schutzkarten bieten sich insbesondere bei Systemen an, bei denen man keinen direkten Einfluss auf die Benutzer hat, sprich Systeme, an die jeder gehen kann.

Beispiel 4.3:

In einer öffentlichen Bücherei werden Rechner für das Surfen im Internet zur Verfügung gestellt. Um sicherzustellen, dass die Systeme jeden Morgen auf einem definierten Stand sind, werden Wächterkarten eingesetzt.

Die Verwendung dieser Schutzmechanismen hat in der Praxis drastisch abgenommen. Vielfach lassen sich ähnliche Schutzfunktionen über Software, Virtualisierung oder Thin Clients einstellen.

4.6 Thin Clients/Zero Clients

Thin Clients sind sehr abgespeckte Rechner, die im Wesentlichen die grafische Ausgabe von Inhalten übernehmen, die serverseitig generiert werden. Anders ausgedrückt entspricht das Prinzip dem alten Hostprinzip: Ein Server mit hoher Rechenleistung arbeitet im Hintergrund, der Benutzer sitzt an einem Terminal.

Heutige Thin Clients arbeiten meist auf Basis von ▸RDP (Remote Desktop Protocol). Die Software auf den Clients kann ein abgespecktes Linux oder Windows sein. Seitens des Servers können entweder nur spezielle Anwendungen ausgeliefert werden oder aber ein kompletter virtueller Client dargestellt werden. Im letzten Fall ist das Arbeiten nahezu wie an einem normalen Rechner. Lediglich grafikintensive Anwendungen stellen in der Praxis noch ein Problem dar.

Die sogenannten Zero Clients sind eine Teilmenge der Thin Clients. Sie zeichnen sich durch noch weniger eigene Funktionen aus und unterstützen meist auch nur ein einziges Protokoll.

4.7 Appliances für verschiedene Zwecke

Appliances für unterschiedlichste Zwecke erobern immer mehr den Markt. Hinter der Bezeichnung verbergen sich Serversysteme für ganz bestimmte Zwecke. Der Grund für den Erfolg dieser Systeme hängt damit zusammen, dass sie für die Administration meist einen sehr geringen Aufwand bedeuten.

Vielfach werden Appliances mit entsprechenden Service-Verträgen geliefert, sodass die Systemadministration keinerlei Verantwortung im Betrieb übernehmen muss. Leider ist man dadurch auf die Vertragspartner angewiesen. Ein direkter Einfluss auf die Patch-Strategie besteht ebenso wenig wie die Möglichkeit der Einflussnahme auf die Dienste, die auf den Appliances aktiviert sind.

Auch wenn die Geräte die Administration vereinfachen, so darf man die Gefahren nicht vernachlässigen, die man sich mit dem Einsatz ins Haus holt.

Vielfach besteht auch die Möglichkeit, keine physikalische Appliance zum Einsatz zu bringen, sondern eine virtuelle. Dies setzt allerdings entsprechende Virtualisierungslösungen beim Kunden voraus. Der Vorteil an dieser Stelle ist meist eine bessere Skalierbarkeit.

Beispiele für gängige Appliances sind:

- Mail-Gateways
- Archivierungssysteme
- Schwachstellenscanner
- u.v.m.

Besonders im Umfeld der Informationssicherheit gibt es ein großes Angebot an integrierten Maschinen.

4.8 Sandboxing

Wie oben bereits erläutert, haben Virenscanner in der Praxis immer eine Lücke in der Erkennung: dann wenn Viren ganz neu sind bzw. nur punktuell zum Einsatz kommen. Diese Lücke soll mittels Sandboxing-Systemen geschlossen werden.

Der Ansatz ist – wie so oft – simpel, die Ausführung allerdings kompliziert. Sandboxing-Lösungen sollen schadhafte Programme anhand ihres Verhaltens erkennen. Hierzu werden fragliche Programme in einer geschützten, virtuellen Umgebung gestartet und beobachtet.

Der Input für solche Lösungen kommt meist aus dem Maileingang oder dem Download aus dem Internet.

Die Problematik besteht darin, dass Entwickler von Schadsoftware um die Existenz solcher Technologien wissen und teilweise Funktionen in ihre Software integrieren, die Sandboxing-Systeme austricksen. Hiergegen müssen die Anbieter der Sandboxing-Lösungen kämpfen. Für eine Software müssen sich die einzelnen virtuellen Maschinen wie echte Rechner mit einem Nutzer davor verhalten und auch unterschiedliche Softwarezusammenstellungen haben, für den Fall, dass Schadsoftware nur in ganz bestimmten Konstellationen ausgeführt wird.

Das Prüfen von Software auf diesem Weg führt allerdings dazu, dass es zu einem Zeitversatz kommt, da die Prüfung teilweise bis zu 15 Minuten andauern kann.

Der Einsatz von solchen Umgebungen ist meist mit einem hohen Kostenfaktor verbunden. Diesen Kosten sollte man die Ersparnis gegenüberstellen, die durch die Vermeidung von beispielsweise einem Ransomware-Befall entsteht.

4.9 Containerlösungen

Mit den Containerlösungen erfolgt jetzt ein kleiner Schwenk hinsichtlich der Geräte: weg von Server-Systemen oder ▸PCs, hin zu mobilen Endgeräten. Dieser Anwendungsfall wurde von mir bewusst ausgewählt, um noch einmal darauf aufmerksam zu machen, dass auch Geräte wie Smartphones und Tablets mit in die Konzeption der Informationssicherheit aufgenommen werden müssen, da deren Leistungsfähigkeit und auch der Einsatz sehr zugenommen hat.

Beispiel 4.4:

> Vielfach höre ich die Argumentation: „Die Smartphones sind ja nicht wirklich in unser Netz eingebunden. Ich habe keinen Zugriff auf die Server. Ich lese doch nur Mails und nutze den Kalender."

Ist es wirklich so? Kann ich die smarten Endgeräte vernachlässigen? Schauen wir allein auf die E-Mails. Durch die E-Mail-Adressen und insbesondere auch die kompletten Footer-Angaben haben wir hier es hier mit personenbezogenen Daten nach dem deutschen Datenschutz (vgl. § 3 ▸BDSG) zu tun. Das heißt, als Unternehmen hat man technische und organisatorische Maßnahmen (vgl. § 9 BDSG) zu treffen, um diese angemessen zu schützen.

Darüber hinaus werden Sie mir sicherlich zustimmen, dass oftmals Anlagen an Mails zu finden sind, die sogar unternehmenskritische Daten beinhalten, und diese Dokumente auch teilweise an Termine gekoppelt werden. Entsprechend sollte man auch den Betrieb von Smartphones berücksichtigen.

Schauen wir einfach einmal auf die Patch-Zyklen von Smartphones: Die Anbieter der Betriebssysteme IOS und Android sind in Bezug auf regelmäßiges Patchen ihrer Systeme recht gut. Werden Schwachstellen bekannt, so können Sie bei einem iPhone oder einem Google Pixel-Handy davon ausgehen, dass die Schwachstellen zügig per Patch geschlossen werden.

Die anderen Hersteller von Smartphones hinken in der Regel sehr lange hinterher bzw. teilweise wird nach dem initialen Betriebssystem kein weiterer Patchlevel mehr angeboten. Sicherheitslücken bleiben offen und können ausgenutzt werden.

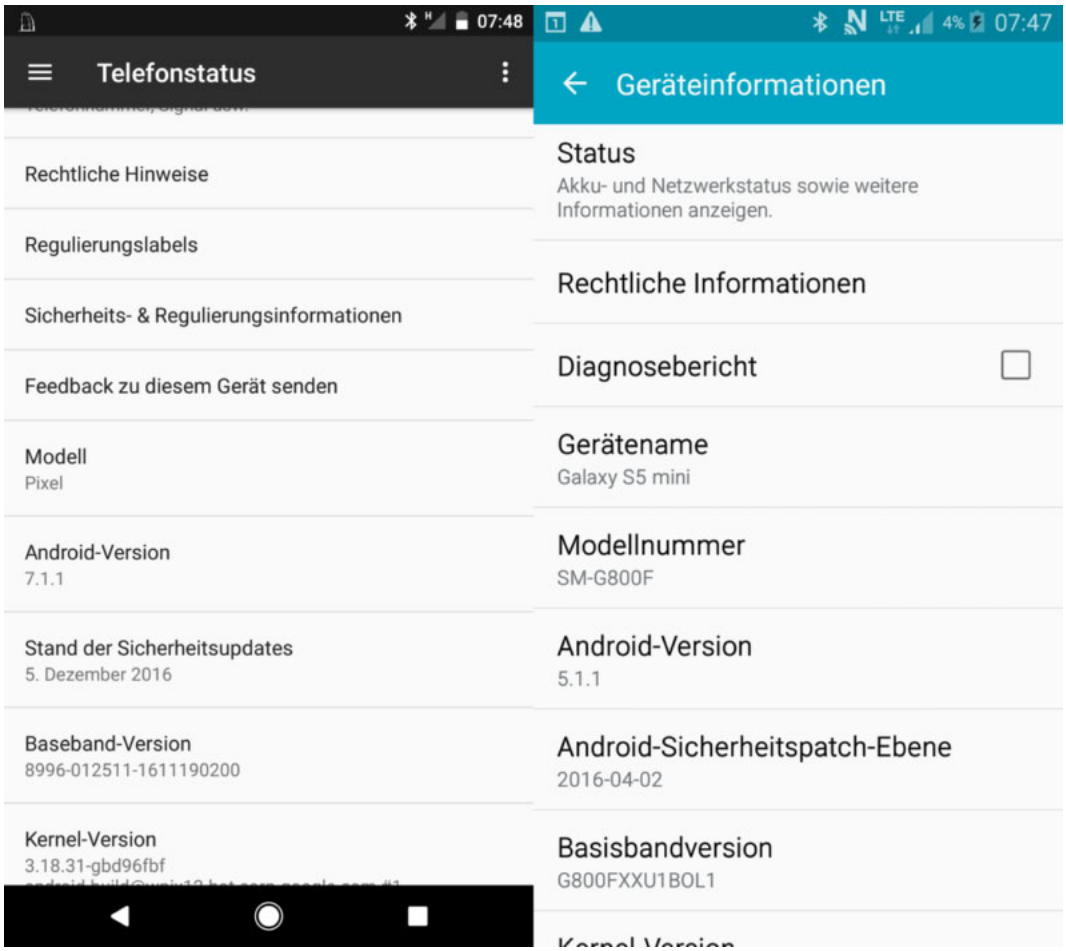

Abb. 4.3: Vergleich Patchlevel auf Android, Stand 16.12.2016

In Abb. 4.3 sehen Sie zwei Screenshots von Android-Mobiltelefonen. Beide Screenshots wurden am gleichen Tag aufgenommen. Wie Sie sehen können, hat ein Gerät einen Patchstand von Dezember 2016, während das andere noch auf einem Stand von April 2016 ist. Auf beiden Telefonen war der jeweils aktuellste Patchlevel, der verfügbar war, installiert.

Aufgrund dieser Situation haben wir auf Mobiltelefonen und Tablets ein erhöhtes Gefahrenpotenzial hinsichtlich Schwachstellen und entsprechende Sicherungsmechanismen sollten zusätzlich etabliert werden.

Eine solche Möglichkeit ist der Einsatz von Containerlösungen. Hierbei werden die kritischen Daten innerhalb separater, verschlüsselter Dateien (Container) auf den Geräten vorgehalten. Der Zugriff auf diese Container erfolgt dann meist mit entsprechenden Apps des Herstellers der Lösung.

Beispiel 4.5:

Wenn Sie eine Containerlösung für E-Mail einsetzen, ist oft auch kein Zugriff mit der nativen E-Mail-App mehr möglich.

Durch die Kapselung von Daten innerhalb eines Containers kann auch sichergestellt werden, dass beispielsweise die Facebook-App keine Kontaktdaten aus dem Container in die USA transferiert (vgl. hierzu auch die gesetzlichen Regelung von § 4b BDSG zur Übermittlung personenbezogener Daten ins Ausland).

Im Idealfall werden Container im Zusammenhang mit einem Mobile Device Management (▸MDM) genutzt. Damit hat das Unternehmen zentral die Möglichkeit, Einfluss auf die Gerätesteuerung zu nehmen und Regeln auf dem Gerät einzustellen. Solche Regeln können beispielsweise das Verbot von Cloud-Diensten, Passwortsperren mit entsprechenden Vorgaben oder Ähnliches sein.

Beispiel 4.6:

Viel beworben durch die Anbieter von MDM-Lösungen ist auch das Remote Wiping, das Löschen der Geräte bei Verlust. Betrachtet man die Funktion genauer, stellt man fest, dass sie nur bei vorhandenem Netz funktioniert. Geht ein Gerät verloren und ein „normaler“ Finder bekommt es in die Hände, kommt er aufgrund der Verschlüsselung sowieso nicht an die Daten.

Der Profi, der es auf die Daten abgesehen hat, wird das Gerät in seine Gewalt bringen, als Erstes die SIM-Card entfernen und anschließend – ohne Online-Connect – den Angriff auf den Container fahren. Oder aber er wird eine SIM-Card für ein eigenes lokales GSM-Netz einsetzen, das er komplett kontrolliert (ein Verfahren, welches z.B. die Forensiker der Polizei nutzen).

4.10 Security aus der Cloud

Sicherheit aus der Cloud ist ein Schlagwort, das einem regelmäßig begegnet. Wir wollen einmal betrachten, was sich dahinter verbergen kann. Es gibt viele Einsatzmöglichkeiten und auch einige sehr gute Lösungsansätze.

So zum Beispiel im Hinblick auf den Virenschutz. Während früher Virenscanner ausschließlich lokal gearbeitet haben und nur zentral mit neuen Pattern-Dateien zur Erkennung von Schadsoftware versorgt wurden, gibt es heute viele cloudbasierende Ansätze. Im einfachsten Fall geht es darum, Informationen untereinander auszutauschen. Oft trifft Schadsoftware in größeren Wellen auf, d.h., eine schadhafte Datei wird via Spamming versandt und taucht damit in einem größeren Umfang plötzlich in Mailboxen auf.

Durch den Informationsaustauch der Virenschutzindustrie werden Hashwerte von untersuchten Dateien (mit Ergebnis) zentral – in der Cloud – gespeichert. Tritt also ein Hashcode plötzlich in einer großen Zahl auf, ist dies ein Indiz, dass etwas nicht stimmt.

Ein weiterer Ansatz ist, Dateien die als fragwürdig erkannt wurden, zur tieferen Analyse in die Cloud – mit mehr Performance und Möglichkeiten – zu senden. Erst nach einem Ergebnis aus der Cloud erfolgt dann die Freigabe.

Ähnliche Cloud-Lösungen gibt es im Firewall-Umfeld. Hier werden Informationen über IP-Adressen und Portnummer ausgetauscht, bei Application Level Firewalls sogar teilweise detailliertere Inhalte.

Weitere Anwendungen im Zusammenhang mit Informationssicherheit aus der Cloud sind beispielsweise Schwachstellen-Scanner. Hierzu werden lokal Appliances im Netz installiert, die ihre Daten dann gesammelt an einen Dienstleister in der Cloud übermitteln. Via Internetseite kann der Sicherheitsverantwortliche sich einen Überblick über die aktuelle Situation einholen.

Beispiel 4.7:

In einer Produktpräsentation wurde ein Schwachstellenscanner für Webseiten vorgestellt, der online direkt eine Art Siegel zur Qualität in einer Webseite einbinden kann. Zusätzlich konnte man dann über einen Link die Details der jeweiligen Scans anschauen. Schwachstelle des Anbieters war, dass man mit diesen Informationen in der Lage war, sich die URLs aller Kunden anzeigen zu lassen, und damit Kenntnis über deren Schwachstellen erlangte.

Das obige Beispiel zeigt, dass man sich sehr genau damit befassen sollte, an welcher Stelle Lösungen aus der Cloud sinnvoll sind. Nur weil hier meist günstigere Preise als bei einer Vor-Ort-Installation aufgerufen werden, muss es nicht immer die bessere Lösung sein.

Eine sehr wirkungsvolle und für Unternehmen interessante Lösung wird im Umfeld des DDoS-Schutzes von den großen Telekommunikationsunternehmen angeboten. Über entsprechende Sensoren an den Netzübergabepunkten können DoS- und DDoS-Angriffe erkannt werden. Meist erst nach Rücksprache mit dem Sicherheitsverantwortlichen kann der Netzbetreiber den schadhaften Traffic wegleiten.

Beispiel 4.8:

Die großen Telekommunikationsprovider bemerken im Rahmen ihrer Überwachung sehr wohl Angriffswellen auf den Backbones. Aufgrund der gesetzlichen Regelungen ist es ihnen aber nicht erlaubt, Eingriff zu nehmen. Sie dürfen in der Regel erst dann eingreifen, wenn ein betroffener Kunde sie beauftragt oder sie selbst Opfer des Angriffes geworden sind.

Weitere Ansätze für Security aus der Cloud sind auch:

- Backup-Dienstleistungen
- Disaster-Recovery-Szenarien
- IDS- oder IPS-Dienste
- Identity und Access Management
- SIEM-Lösungen

Abb. 4.4 zeigt, welche Lösungen heute im Mittelstand bereits als Cloud-Security-Lösungen zum Einsatz kommen und wie die Pläne für die Zukunft aussehen.

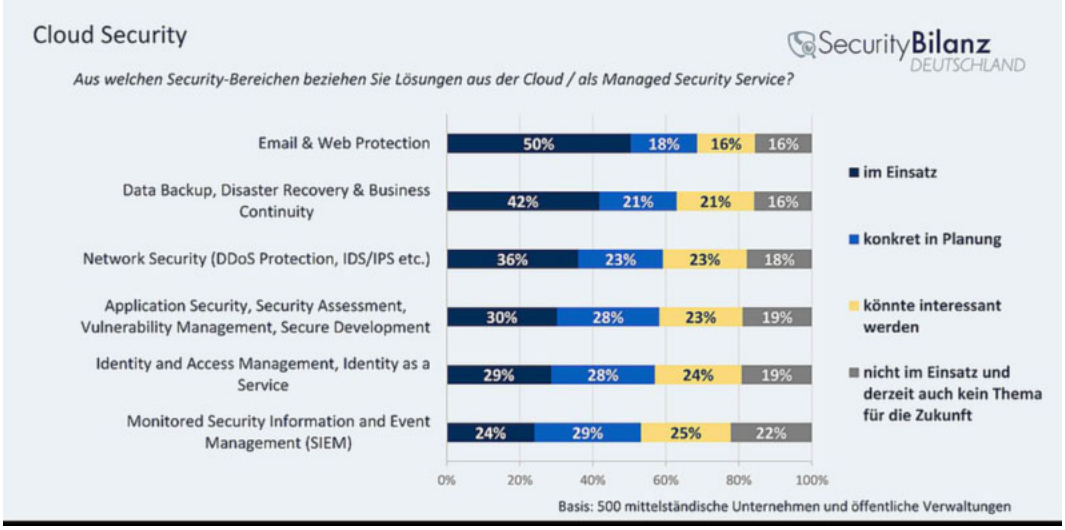

Abb. 4.4: Umfrage über den Einsatz von Cloud-Security-Lösungen (Quelle Techconsult/AP Verlag)

Oftmals wird generell der Betrieb in einer Cloud auch als Sicherheitslösung verkauft. Die Argumentation ist hier, dass große Cloud-Dienstleister sicherlich bessere Sicherheitsinfrastrukturen aufbauen und betreiben können.

4.11 Honeypots

Mit Honigtöpfen fängt man Bären … mit Honeypots (hoffentlich) Hacker.

Definition 4.1:

Honeypots sind präparierte Ausführungsumgebungen, in denen ein Angreifer keinen Schaden anrichten kann.[46]

Honeypots werden in der Regel in Unternehmen „aufgestellt“, die sich mit der Wahrscheinlichkeit von erfolgreichen Angriffen befasst haben. Ziel ist es, Angreifer dadurch zu entdecken, dass sie versuchen, auf einen Honeypot zuzugreifen. Um die Honeypots interessanter zu gestalten, werden dort evtl. Schwachstellen scheinbar offen gelassen oder Informationen abgelegt, die Interesse wecken sollen. Da Angreifer aber auch von der Existenz dieser Technologie wissen, ist der Einsatz genau zu überlegen. Beispielsweise würde eine Maschine, die offen ist wie ein Scheunentor, in einer sonst sicher konfigurierten Systemarchitektur auffallen und ein Hacker würde direkt Verdacht schöpfen.

Ein weiteres Anwendungsgebiet ist die Sicherheitsforschung. Durch Honeypots kann man neue Angriffsmuster erkennen und das Verhalten von Hackern beobachten. Ebenso lassen sich Angriffswellen detektieren. Die Deutsche Telekom betreibt beispielsweise eine große Honeypot-Infrastruktur. Hierbei handelt es sich teilweise um angebliche Server, Mobiltelefone und vieles mehr. Die laufenden Angriffe kann man auf einer In-

46. Vgl. Eckert, 2014, S. 750.

ternetseite der Telekom[47] betrachten und sich sogar Details anzeigen lassen. Die entsprechenden Background-Infos und auch den Honeypot selbst stellt die Telekom unter http://dtag-dev-sec.github.io/ zur Verfügung.

Bei Honeypots kann man ein paar Grundklassen unterscheiden:

- Low-Interaction Honeypot

  Hierbei handelt es sich um Lösungen, die keine oder nur geringe Eigenmaßnahmen durchführen. Sie stellen meist ein paar Dienste zur Verfügung und warten auf die Nutzung dieser Dienste, um dann Alarm zu schlagen.

- High-Interaction Honeypot

  Bei dieser Gattung handelt es sich meist um speziell eingerichtete Server, auf denen entsprechende Überwachungsprogramme (versteckt) mitlaufen. Anhand dieser Server können manuelle Angriffe beobachtet und bewertet werden. Diese Erkennung, dass es sich um einen Honeypot handelt, ist dabei für den Angreifer deutlich schwieriger.

- HoneyNet

  Von HoneyNet redet man dann, wenn es mehrere zentral verwaltete Honeypots gibt.

Integriert man die durch Honeypots gewonnenen Daten wiederum in ein SIEM, lassen sich Sicherheitsvorfälle deutlich schneller und besser erkennen. Betrachtet man die angeblichen Werte, wie lange Hacker unerkannt auf einem System ihr Unwesen treiben können[48], so ist jede Reduzierung dieser Dauer nur wünschenswert.

Zusammenfassung

In diesem Abschnitt haben Sie einen Überblick über gängige Lösungen bekommen, die die Informationssicherheit (mehr oder weniger) unterstützen. Sie sind nun selbst in der Lage, sich – bezogen auf Ihre Situation – ein Bild über den sinnvollen Einsatz zu machen.

Ebenso haben Sie einige Nachteile von bestimmten Lösungen kennengelernt und mitgenommen, dass es kein technisches Allheilmittel für die Informationssicherheit gibt.

Aufgaben zur Selbstüberprüfung

4.1 Machen Sie sich bitte einmal Gedanken darüber, warum es sinnvoll sein könnte, regelmäßige Komplett-Scans durch den Virenschutz durchführen zu lassen.

4.2 Erläutern Sie bitte kurz, warum es bei der Nutzung von Sandboxing-Systemen im E-Mail-Verkehr zu Verzögerungen in der Zustellung von Mails mit Anhang kommt.

4.3 Bewerten Sie die Behauptung, dass der Betrieb in der Cloud sicherer ist als lokal, und begründen Sie dies.

47. Vgl. http://www.sicherheitstacho.eu/.
48. Vgl. http://www.security-insider.de/datendiebstahl-bleibt-im-schnitt-469-tage-unbemerkt-a-539640/.

5 Übergreifende Themen für einen sicheren Betrieb

Dieses Kapitel hat einen globalen Ansatz. Es geht im Wesentlichen um angrenzende Themenfelder, die in Kombination oder Anwendung sekundär helfen, den Betrieb sicherer zu gestalten. Sie werden lernen, warum eine Zusammenarbeit sinnvoll und wichtig ist und es dabei gilt, auch gedankliche Barrieren zu durchbrechen. Weiterhin werden Sie ein paar organisatorische Ideen für den Aufbau eines Teams zur Informationssicherheit kennenlernen und sich mit dem IT-Grundschutz als Nachschlagewerk und Grundlage für ein Sicherheitskonzept beschäftigen.

Informationssicherheit ist kein rein lokal an Ihr Unternehmen gebundenes Thema. Es beschäftigen sich in allen größeren Unternehmen Experten mit den Problemen der Sicherheit. Daraus resultierend kommt es leider immer wieder dazu, dass das Rad zigfach neu erfunden wird. Sicherheit ist ein Thema, das nach Synergien schreit. Hier werden Sie ein paar Ansätze kennenlernen, die Ihnen auf diesem Weg helfen (können).

5.1 CERT

▸CERT steht für Computer Emergency Response Team und ist ein häufig synonym für ▸CSIRT (Computer Security Incident Response Team), ein Begriff, der nach ▸RfC 2350[49] definiert ist. Ein CERT zeichnet sich dadurch aus, dass es einer Zielgruppe bei der Bewältigung von Sicherheitsvorfällen hilft. In diesem Zusammenhang sollen die Auswirkungen und Schäden reduziert werden.

Neben diesem rein reaktiven Ansatz gehört im Sinne eines PDCA-Zyklus auch die Verbesserung dazu, mit dem Ziel, zukünftige Ereignisse zu verhindern.

Kossakowski unterteilt das Leistungsspektrum innerhalb eines CERT in drei Klassen mit unterschiedlichen Dienstleistungen[50]:

- reaktive Dienstleistungen
  - Behandlung von Anfragen
  - Verifikation
  - Schwachstellenanalyse
  - Reaktionen auf Sicherheitsvorfälle
- präventive Dienstleistungen
  - Verbreitung von Informationen
  - Untersuchungen
  - Toolentwicklungen
- Security-Quality-Management-Dienstleistungen
  - Risk Analysis
  - Business-Continuity-Planung
  - Beratung
  - Sensibilisierung

49. Vgl. https://www.ietf.org/rfc/rfc2350.txt.
50. Kossakowski, Incident Response Capabilities, 2000, S. 118.

Vielfach wird der Begriff CERT lediglich mit der Verbreitung von Warnmeldungen gleichgesetzt, wie man es ggf. von CERT-Bund[51] kennt. Dies ist allerdings nur ein kleiner Teilbereich.

Viele lokale CERTs erarbeiten die Warnmeldung mittlerweile nicht mehr selbst, sondern kaufen diese von anderen CERTs als Warndienst ein.

Übung 5.1:

Besuchen Sie einmal die Seite https://web.nvd.nist.gov/view/vuln/search-results und schauen Sie sich die dort veröffentlichten Schwachstellen an.

Neben einem koordinierten Vorgehen im Fall von sicherheitskritischen Vorfällen und der Prävention innerhalb des Unternehmens, dem das CERT zugeordnet ist bzw. für das es verantwortlich ist, haben sich CERTs in Deutschland zu Verbünden zusammengeschlossen. Diese tauschen sich regelmäßig über Sicherheitsvorfälle, Erkenntnisse usw. aus. Hierdurch können deutliche Synergien erzielt werden, Vorfälle reduziert bzw. schneller angegangen werden.

In Deutschland gibt es hier zwei wesentliche Verbünde:

- CERT-Verbund[52]

  Der CERT-Verbund ist die Allianz deutscher Sicherheits- und Computer-Notfallteams mit heute über 40 Mitgliedern.

- Verwaltungs-CERT-Verbund

  Verbund im Bereich der staatlichen Verwaltung. Entsprechend den Vorgaben des IT-Planungsrates tauschen sich hier die einzelnen Bundesländer-CERTs aus.

Global zusammengefasst existiert das Forum for Incident Response and Security Teams (▸FIRST)[53], das international alle Mitglieder aus den Regierungs- und Wirtschafts-CERTs vereint.

5.2 SOC

Der Begriff ▸SOC (Security Operation Center) stellt eine interne Organisation dar, in der alle sicherheitsnahen Mitarbeiter und Teams zusammenarbeiten. Vielfach sind IT-Unternehmen säulenmäßig nach verschiedenen Technologien organisiert, d.h., es gibt einzelne Teams für Datenbanken, UNIX, Netze, Firewalls usw.

Ein SOC bildet nun einen horizontalen Ansatz, um aus Sicherheitsgesichtspunkten alle einzelnen Einheiten zu vereinen bzw. adressieren zu können. Ziel ist eine Lösungsorientierung und das Durchbrechen der technologischen Säulen, sprich ein Team für den operativen Betrieb der Informationssicherheit.

51. Vgl. https://www.cert-bund.de/.
52. Vgl. https://www.cert-verbund.de/.
53. Vgl. https://www.first.org/.

Man könnte ein SOC als personelle Ausgestaltung eines SIEM ansehen. Die Computerwoche hat es in einem Artikel ziemlich genau auf den Punkt gebracht mit dem Satz: „Wenn große Unternehmen heute eigene SOCs aufbauen, geht es daher oft auch darum, etablierte Silostrukturen aufzubrechen und bereichsübergreifend Sicherheitskompetenz in einem SOC neu zu bündeln und mit erweiterten Befugnissen auszustatten."[54]

Nicht jedes Unternehmen wird in der Lage sein, ein eigenes Team aufzubauen. Mittlerweile bieten daher auch Dienstleister das SOC als einkaufbare Leistung an, meist in Kombination mit SIEM-Lösungen.

5.3 Kooperationen und Informationsaustausch

Um Sicherheit weiterentwickeln zu können, ist ein Austausch mit anderen erforderlich. Neben dem formellen Aufbau im Rahmen von CERTs ist für Mitarbeiter in der Informationssicherheit eine Vernetzung wichtig. Ziel eines jeden Verantwortlichen in der Informationssicherheit sollte es sein, Kooperationen auf einer vertraulichen Ebene mit anderen in der gleichen Branche, aber auch anderen Branchen zu erhalten.

Durch einen Austausch und eine Zusammenarbeit lassen sich Vorsprünge erarbeiten und neue Blickwinkel einnehmen, die verhindern, dass eine „Unternehmensblindheit" einsetzt.

So macht es beispielsweise Sinn, sich mit der Polizei zusammenzusetzen, um theoretisch das Vorgehen bei Sicherheitsvorfällen abzusprechen. Vielfach gibt es auf Landesebene – bei den ▸LKAs – eigene Teams für Computerkriminalität. Mit den Spezialisten zusammen können mögliche Bedrohungslagen besprochen werden. In diesem Zusammenhang sollten Sie auch immer im Hinterkopf behalten, dass Sicherheitsvorfälle durch Hacker Straftatbestände (§§ 202a ff. ▸StGB) darstellen, die zur Anzeige gebracht werden sollten.

In vielen Organisationen ist es nicht wirklich gewünscht, Strafanzeigen zu stellen. Die Unternehmensführung möchte meist nicht, dass Informationen nach außen dringen. Die Folgen davon sind:

- Viele Straftaten werden nicht angezeigt. Fasst eine Ermittlungsbehörde nun einen Täter, ist die ihm zugeordnete Anzahl an Straftaten geringer als in Wirklichkeit und die Strafe fällt entsprechend geringer aus.
- Den Ermittlungsbehörden fehlt der Nachweis an Vorfällen und damit die formelle Begründung für notwendige Personalverstärkungen.

Nichtsdestotrotz gilt das Bundesdatenschutzgesetz (BDSG), wo in § 42a geregelt ist, dass, falls personenbezogene Daten abhanden gekommen sind, offengelegt wurden etc., entsprechende Veröffentlichungspflichten greifen. Die Pflichten gehen bis zur Veröffentlichung des Vorfalls in der Tageszeitung.

54. Vgl. http://www.computerwoche.de/a/wer-ein-security-operations-center-braucht,3096963,3.

Beispiel 5.1:

Das Jahr 2016 hat sich in der Informationssicherheit durch den massiven Befall von Ransomware ausgezeichnet. Gerade in den Monaten Januar bis Mai fanden die großen Wellen von Locky&Co statt. Dem BSI sind für das 1. Quartal 2016 aber nur 60 Fälle von Ransomware gemeldet worden[55]. Dies zeigt die Meldebereitschaft und die Dunkelziffer.

Einen weiteren Ansprechpartner stellt auch der Verfassungsschutz dar. Hierbei geht es um das Thema der Wirtschaftsspionage und der angewandten Techniken. Dieser Faktor sollte im Rahmen der Informationssicherheit ebenfalls in Betracht gezogen werden, da es Staaten gibt, in denen schon in der Verfassung festgelegt ist, dass die Auslandsgeheimdienste dazu da sind, die lokale Wirtschaft mit Informationen zu unterstützen.

Auch Kooperationen in puncto Sicherheit mit Marktbegleitern sollten in Betracht gezogen werden. Nutzen bringen hier Branchenverbände oder ähnliche Einrichtungen, die vielfach inzwischen Plattformen für den Austausch zu Fragen der Informationssicherheit bieten.

In der Informationssicherheit gilt der Satz „Nur gemeinsam sind wir stark“ in besonderer Weise!

5.4 BSI-Kataloge

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit seinen IT-Grundschutzkatalogen ein umfassendes Nachschlagwerk zur Informationssicherheit an. Die erste Ausgabe als sogenanntes IT-Grundschutzhandbuch fand 1994 statt. Der Grundschutz hat eine eigene Methodik zur Istanalyse und Umsetzung der Informationssicherheit entwickelt, die im Idealfall in einer Zertifizierung nach ISO27001 auf Basis von BSI-Grundschutz mündet. Aber auch ohne eine Zertifizierung anzustreben, bieten sich die Kataloge für eine Verwendung an.

Die beiden wesentlichen Elemente des Grundschutzes sind die Gefährdungs- und Maßnahmenkataloge. Im Ersteren finden sich detaillierte Beschreibungen der Gefahren, die in sechs Kataloge gruppiert sind:

- G 0: Elementare Gefährdungen
- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

55. Vgl. https://www.welt.de/wirtschaft/article154677618/BSI-Chef-warnt-vor-Toten-durch-Hackerangriffe-auf-Autos.html.

Innerhalb der Maßnahmenkataloge geht es um die konkrete Gefahrenabwehr, d. h., hier sind Sicherheitsmaßnahmen beschrieben. Das BSI sagt zu seinen Maßnahmen:

„Bei den in den IT-Grundschutz-Katalogen aufgeführten Maßnahmen handelt es sich um Standard-Sicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Basis-Sicherheit zu erreichen."[56]

Die einzelnen Maßnahmen beinhalten nicht nur technische Einstellungen oder organisatorische Regeln, die man treffen muss, um eine Gefährdung zu reduzieren oder auszuschließen, sondern ein komplettes Phasenmodell von der Planung einer Maßnahme über eventuell notwendige Beschaffungen mit Auswahlprozess bis hin zur Umsetzung, dem Betrieb und zur Aussonderung. Ebenso wird auch die Notfallvorsorge angesprochen.

Es handelt sich somit auch um eine Adaption eines PDCA-Zyklus, um fortwährende Verbesserungen anzustreben und nicht auf einem Stand zu verbleiben.

Das Modell des BSI unterscheidet drei Schutzstufen, an denen man sich mit den drei Schutzzielen ausrichten soll: normal, hoch und sehr hoch. Die Maßnahmen der Kataloge decken dabei das Niveau normal ab. Besteht ein Bedarf nach einem höheren Schutz, so sind zusätzliche Sicherheits- und Risikoanalysen notwendig, um ggf. weiter individuelle Maßnahmen zusätzlich zu implementieren.

Aktuell findet eine Überarbeitung des BSI-Grundschutzes statt, die voraussichtlich Ende 2017 abgeschlossen sein soll. Hier steht insbesondere eine einfachere Einführung im Vordergrund.

Neben der Standardabsicherung, die dem heutigen Grundschutz entsprechen soll, wird es eine Basis und eine Kernabsicherung geben. Die Basisabsicherung soll hierbei das unterste Level darstellen, das heißt die zwingend erforderlichen Maßnahmen.

In der Kernabsicherung geht es dann um die Absicherung der essenziellen Werte eines Unternehmens. Beide Formen können auch miteinander kombiniert werden.

Hinsichtlich bestehender Grundschutzprojekte gilt die Aussage des BSI, dass das neue Modell kompatibel zum bestehenden Grundschutz sein soll.

Zusammenfassung

In den übergreifenden Aspekten haben Sie nun konkrete Beispiele für Kooperationen im Rahmen von CERTs und anderen Partnerschaften kennengelernt und erfahren, dass eine enge Zusammenarbeit auch über die Unternehmensgrenzen hinaus für die Informationssicherheit essenziell ist.

Innerhalb des Unternehmens ist eine Zusammenarbeit über die verschiedenen Fachdisziplinen erforderlich, sodass ein SOC eine Art Matrix-Organisation im IT-Betrieb darstellt.

56. Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/einstieg/01001.html;jsessionid=22F8A63AB0544D407C0ADC6C817FAC03.1_cid351.

Und zu guter Letzt haben Sie einen rudimentären Einblick in den Grundschutz des BSI erhalten, der international über die ISO27001 verdrahtet ist und mittlerweile ein hohes Ansehen auch im Ausland besitzt.

Aufgaben zur Selbstüberprüfung

5.1 Beschreiben Sie stichpunktmäßig den Unterschied zwischen einem CERT und einem SOC.

5.2 Welche der folgenden Aufgaben ordnen Sie einem SOC zu:

- Unterstützung im Rahmen eine Sicherheitsvorfalls
- Betrieb und Auswertung einer SIEM-Lösung
- Virenschutz
- Sensibilisierung von Mitarbeitern
- Regelmanagement von Firewalls

5.3 Welche Sicherheitslevel für Verfügbarkeit, Integrität und Vertraulichkeit unterscheidet das BSI in seinen Grundschutz-Katalogen und auf welche Stufe sind die Maßnahmen ausgerichtet?

Schlussbetrachtung

Die Grundlagen für einen sicheren IT-Betrieb haben viele verschiedene Ansatzpunkte, beginnend bei der konkreten Absicherung von Betriebssystemen und Applikationen, bis hin zu einer Zusammenarbeit über das Unternehmen hinaus.

Hierbei kann man nicht sagen, dass einzelne Teile wichtig oder unwichtig sind. Die Sicherheit kann man sich als ein großes Mosaik vorstellen, das seine Wirkung nur dann voll entfalten kann, wenn es komplett zusammengesetzt ist.

Welche Maßnahmen in welcher Reihenfolge durchgeführt werden oder welches Restrisiko ein Unternehmen bereit ist zu tragen muss von Fall zu Fall individuell entschieden werden.

Ich hoffe, das Studienheft konnte Ihnen die Komplexität der Materie ein wenig näherbringen. Dass das Thema viel zu komplex für ein Studienheft oder eine Reihe zur Informationssicherheit ist, können Sie schon allein daran erkennen, dass es mittlerweile Bachelor- und Master-Studiengänge zur Informationssicherheit gibt.

A. Lösungen der Übungen im Text

2.1 Die Suche nach Ihrem Namen sollte (hoffentlich) erfolglos verlaufen sein. Bei der Suche nach Osama bin Laden finden Sie die Aussage: „Die 100 %-Suche nach ‚Osama bin Laden' ergab 2 Treffer" sowie weitere Details

5.1 Wie Sie sehen, ist der Aufbau der Schwachstellenmeldungen immer gleich gehalten, sodass man auf Anhieb erkennen kann, welche Software betroffen ist und wie die Gefahr aussieht.

B. Lösungen der Aufgaben zur Selbstüberprüfung

1.1 Unter einem Exploit versteht man ein Programm, ein Shell-Script oder einen anderen ausführbaren Code, der eine bekannte (oder unbekannte) Schwachstelle eines Systems dahingehend ausnutzt, dass er dem Ausführenden Rechte oder Möglichkeiten eröffnet, die er bei normaler Programmnutzung nicht hätte.

1.2 Das Internet of Things besteht aus einer Vielzahl von unterschiedlichen Geräten, die ihrerseits kleine Computer sind. Diese einzelnen Systeme lassen sich unter Ausnutzung von Schwachstellen mit Schadcode infizieren und somit zu aktiven Mitgliedern eines Botnetzes machen. In der Regel liegt seitens der Benutzer keine große Aufmerksamkeit auf den Schwachstellen von Geräten, sodass die Gefahr des Entdecktwerdens gering ist. Aufgrund der hohen Anzahl der Systeme im IoT entsteht eine gewaltige Kraft für ein Botnetz auf Basis solcher Geräte.

2.1 Ausnutzbare Fehler in Treibersoftware stellen eine größere Gefahr für das Gesamtsystem dar, da Treiber meist schon in einem Kontext mit deutlich höheren Berechtigungen laufen als ein normales Anwendungsprogramm. Hierdurch sind ggf. keine zusätzlichen Rechte-Eskalationen mehr nötig.

2.2 Nach Ausführung des Befehls sieht der Verzeichniseintrag wie folgt aus:

```
-rwx-wx—x alf melmac ...
```

Der Benutzer alf hat damit volle Rechte: Er darf lesen, schreiben und ausführen.
Die Gruppe melmac hat eingeschränkte Rechte: Sie darf schreiben und ausführen.
Alle anderen haben eingeschränkte Rechte: Sie dürfen ausführen.

2.3 Rubber Ducky ist ein Produkt, das man in den USA für Penetrationstests bestellen kann[57]. Äußerlich handelt es sich um einen USB-Stick. Beim Einstecken in einen Port gibt sich der Stick als Tastatur aus, sodass auch Kontrollsysteme für USB-Ports ausgetrickst werden, weil Tastaturen in der Regel zugelassen sind. Mittels des Mikrochips und der Speicherkarte lassen sich über die Tastatur Befehle auf dem angeschlossenen Rechner ausführen und auch Schadsoftware installieren.

3.1 Vorweg: Es gibt kein klares Richtig oder Falsch! Eine mögliche Lösung wäre, auf einem Testrechner die Patches zu installieren, an diesem Testszenarien zu fahren und bei fehlerfreier Funktion die Patches für alle freizugeben.

Ein anderes Szenario wäre, einen geringen Prozentsatz der Clients automatisch zu betanken. Meldet innerhalb einer Woche niemand einen Fehler, kann der Patch auf alle Systeme ausgebracht werden.

3.2 Den sogenannten „Ping of Death“ finden Sie unter der CVE-Nummer: CVE-1999-0128.

57. Vgl. https://hakshop.com/products/usb-rubber-ducky-deluxe.

3.3 Jede Veränderung eines Dienstes oder einer Komponente ist im Rahmen des Betriebs als Change zu behandeln. Hintergrund ist, dass jede (noch so kleine) Änderung eine potenzielle Fehler- und Gefahrenquelle darstellt.

Um kleine Änderungen, wie z.B. Minor Updates, ohne einen großen Prozess-Overhead zu realisieren, gibt es die Möglichkeit, Standard-Changes zu definieren. Hierzu wird einmalig geprüft, welche Gefährdungen bestehen, und dann eine generelle Freigabe für eine bestimmte Art von Veränderungen erteilt. Nichtsdestotrotz muss auch ein Browser-Update als Change erfasst und (automatisch) dokumentiert werden.

4.1 Full Scans beim Virenschutz prüfen (in der Regel) alle Dateien erneut – unabhängig davon, ob sie bereits einmal geprüft wurden. Da die Signaturen täglich aktualisiert werden, findet man auf diese Weise Schadsoftware, die beim „on access"-Scan im Augenblick des Speicherns noch nicht erkannt werden konnte.

4.2 Sandboxing-Systeme sind dazu gedacht, in dem geschilderten Fall die E-Mail-Anlagen zu öffnen bzw. auszuführen. Eine „Beobachtung" dessen, was aufgrund der Aktion geschieht, entscheidet dann darüber, ob eine Anlage als gefährlich eingestuft wird oder nicht. Lädt beispielsweise ein Word-Dokument beim Öffnen automatisch Code aus dem Internet nach, ist dies ein Indiz für eine ungewollte Aktion.

Da diese Tests einen gewissen Zeitanteil benötigen, wird die Weiterleitung einer Mail mit Anlage verzögert, bis die Tests abgeschlossen sind. Dies kann mehrere Minuten dauern. Als Faustwert kann man 15 Minuten im Hinterkopf behalten.

4.3 Der Betrieb in der Cloud stellt ein Outsourcing der eigenen IT-Landschaft dar. Entsprechend gibt es eine Vielzahl Punkte zu beachten. Aus Sicht der Informationssicherheit ergeben sich beispielsweise folgende Pro-/Kontra-Argumente:

Pro:

- meist ein zertifizierter Betrieb: ISO27001, ISO20000, ISO9001
- bessere Schutzinfrastruktur durch bessere Synergien
- in der Regel sehr hohe Verfügbarkeiten
- vertragliche Garantien, ggf. mit Pönalen

Kontra:

- lohnenswerteres Ziel für Angreifer
- weniger Möglichkeiten, direkten Einfluss auf die Sicherheit zu nehmen und sie selbst zu überwachen
- meist schwierige Szenarien einem Rückzug aus der Cloud

5.1 Ein CERT hat die Hauptaufgabe der Reaktion auf Sicherheitsvorfälle. Dies erklärt sich teilweise auch schon aus dem Namen (Emergency Response), während das SOC eine operative Einheit ist, die die Sicherheit ganzheitlich – über verschiedene Disziplinen hinweg – betrachtet und im laufenden Betrieb versucht sicherzustellen.

5.2 Die Zuordnung zu CERT und SOC sieht wie folgt aus:

Unterstützung im Rahmen eine Sicherheitsvorfalls	CERT
Betrieb und Auswertung einer SIEM-Lösung	SOC
Virenschutz	SOC
Sensibilisierung von Mitarbeitern	CERT
Regelmanagement von Firewalls	SOC

5.3 Das BSI unterscheidet bei allen drei Zielen der Informationssicherheit einzeln die Stufen:

- normal
- hoch
- sehr hoch

Die in den Grundschutzkatalogen beschriebenen Maßnahmen beziehen sich jeweils auf die Schutzbedarfskategorie „normal“.

C. Abkürzungsverzeichnis

AES	Advanced Encryption Standard
BDSG	Bundesdatenschutzgesetz
BIOS	Basic Input/Output System
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)
CAB	Change Advisory Board
CD	Compact Disk
CERT	Computer Emergency Response Team
CIFS	Common Internet File System – Protokoll für Netzwerkfreigaben
CPU	Central Processing Unit, Prozessor
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service (Angriffsform)
DoS	Denial of Service (Angriffsform)
DVD	Digital Versatile Disc
ECAB	Emergency Change Advisory Board
eID	electronic Identity (Personalausweis)
FIRST	Forum for Incident Response and Security Teams
HDD	Hard Disk Drive
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network, lokales Netzwerk
LKA	Landeskriminalamt
MBR	Master Boot Record
MDM	Mobile Device Management

NFS	Network File System – Protokoll für Netzwerkfreigaben
PC	Personal Computer, Rechner
RDP	Remote Desktop Protocol
RfC	Request for Comments
ROM	Read Only Memory
SD	Secure Digital, Speicherkarte
SIEM	Security Information and Event Management
SMB	Server Message Block – Protokoll für Netzwerkfreigaben
SOC	Security Operation Center
SSD	Solid State Drive
StGB	Strafgesetzbuch
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus, serielles Bussystem
USP	Unique Selling Proposition
WSUS	Windows Server Update Services

D. Literaturverzeichnis

Verwendete Literatur

Baumgarten, U. et al. (2007).
Betriebssysteme.
6. Aufl., München: Oldenbourg.

BSI (2016).
BSI-Grundschutzkataloge.
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.
Bonn: BSI.

Cazemier, J. A. et al. (2010).
Information Security Management with ITIL V3.
Best Practice.
Amersfoort: Van Haren Publishing.

Deutsches Institut für Normung (o.J.).
ISO-27002.
DIN ISO/IEC 27002.

Deutsches Institut für Normung (o.J.).
ISO-27001.
DIN ISO/IEC 27001.

Eckert, C. (2014).
IT-Sicherheit.
Konzepte – Verfahren – Protokolle.
Garching: De Gruyter.

Lacy, S. (2007).
Service Transition.
Norwich: TSO.

Phan, M. et al. (2015).
Malware-Analyse und die Methode der Triage.
<kes> Die Zeitschrift für Informationssicherheit.
Ingelheim: SecuMedia.

Stasch, T. (2012).
Security-Problem-Management.
<kes> Die Zeitschrift für Informationssicherheit.
Ingelheim: SecuMedia.

Tanenbaum, A. S. (2009).
Moderne Betriebssysteme.
3. aktualisierte Aufl., München: Pearson Education Deutschland.

Taylor, S. et al. (2007).
Service Operation.
OGC – Information Technology Infrastructure Library.
Norwich: TSO.

Internetlinks

Schwachstellen-Veröffentlichungen:

https://www.cert-bund.de/overview/AdvisoryShort

https://www.heise.de/security/

https://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on

http://www.zerodayinitiative.com/advisories/published/

https://www.us-cert.gov/ncas/alerts

E. Abbildungsverzeichnis

F. Tabellenverzeichnis

G. Sachwortverzeichnis

H. Einsendeaufgabe Typ A

Grundlagen eines sicheren IT-Betriebs

Einsendeaufgabencode:
SRN02-XX1-N01

Name:	Vorname:	Tutor/-in:
Postleitzahl und Ort:	Straße:	Datum:
Matrikel-Nr.:	Studiengangs-Nr.:	Note:
Heftkürzel: **SRN02**	Druck-Code: **0317N01**	Unterschrift:

Bitte reichen Sie Ihre Lösungen über StudyOnline ein. Falls Sie uns diese per Post senden wollen, dann fügen Sie bitte die Aufgabenstellung und den Einsendeaufgabencode hinzu.

1. Erläutern Sie, warum komplexe Passwörter die Sicherheit hinsichtlich der Brechbarkeit nicht unbedingt erhöhen, und bringen Sie entsprechende Beispiele.

   10 Pkt.

2. Beschreiben Sie, wie man einen Rechner gegen den Einsatz von KON-BOOT absichern kann. Erläutern Sie, welche Maßnahmen kombiniert nötig sind bzw. schon einzeln den Angriff verhindern. Gehen Sie bitte nur auf Techniken ein, die gegen diesen konkreten Angriff helfen.

   20 Pkt.

3. Erklären Sie die Problematik, die sich aus einer Absicherung eines Client-Betriebssystems in Bezug auf Schadwarevorfälle ergeben kann. Welche Schwierigkeiten können auftreten?

   25 Pkt.

4. Sie haben folgende Verzeichnisstruktur auf einem Linux-System (Darstellung mit Wechseln durch die Dateiverzeichnisse):

```
root@kali:/tmp/tmp# ls -la
total 12
drwxr-xr-x 3 root root 4096 Jan 14 14:57 .
drwxrwxrwt 11 root root 4096 Jan 14 14:59 ..
drwxr-xr-x 3 root root 4096 Jan 14 14:58 dvz
root@kali:/tmp/tmp# cd dvz
root@kali:/tmp/tmp/dvz# ls -la
total 12
drwxr-xr-x 3 root root 4096 Jan 14 14:58 .
drwxr-xr-x 3 root root 4096 Jan 14 14:57 ..
drwxr-x--- 2 root root 4096 Jan 14 14:58 WBH-DVZ
root@kali:/tmp/tmp/dvz# cd WBH-DVZ/
root@kali:/tmp/tmp/dvz/WBH-DVZ# ls -la
total 8
drwxr-x--- 2 root root 4096 Jan 14 14:58 .
drwxr-xr-x 3 root root 4096 Jan 14 14:58 ..
-rw-r--r-- 1 wbh wbh-group 0 Jan 14 14:58 LeereDatei
root@kali:/tmp/tmp/dvz/WBH-DVZ#
```

Im System gibt es die Kennung `wbh`, die der Gruppe `wbh-group` zugeordnet ist. Kann diese Kennung die Datei `LeereDatei` lesend öffnen?

25 Pkt.

5. Ein Hersteller einer Appliance schreibt in seinem Whitepaper folgenden Text: „Unsere Software ist automatisch mit einem Update-Server verbunden. Dieser Server kann die aktuellen Komponentenstände aller Einzelteile des Systems liefern. Wenn der Hersteller aktuellere Versionen der Komponenten freigibt, werden diese neuen Komponenten automatisch installiert."

   Nehmen Sie bitte kurz Stellung zu dieser Aussage. Beschreiben Sie evtl. Probleme und erläutern Sie diese.

   20 Pkt.

Gesamt: 100 Pkt.