



Einleitung

Das moderne Leben wird vom Computer geprägt. Es vergeht kein Tag, an dem man nicht mit Rechnern oder Rechnernetzen konfrontiert wird. Dies kann der Geldautomat aber auch die internetfähige Waschmaschine sein. Der Computer hat aber nicht nur eine dominante Rolle im täglichen Leben eingenommen, sondern in vielen Fällen sind Wirtschaftsprozesse oder ein normaler Lebensablauf ohne Computer nicht mehr denkbar. Ein Ausfall der Rechnersysteme führt in den meisten Fällen zu einem Chaos. Sei es im Kleinen, beim Lebensmitteldiscounter, der bei einem Rechnerausfall nicht mehr seine Kunden bedienen und die Lebensmittel kassieren kann, oder im Großen bei der Flugsicherung eines Flughafens, die bei Ausfall zentraler Rechnersysteme den Flugverkehr zur Vermeidung von Unfällen stilllegen muss.

Spätestens seit der Umstellung der Rechnersysteme auf das Jahr 2000 und den dafür notwendigen Vorbereitungen ist auch in den Managementtagen der großen wie kleinen Firmen das Bewusstsein für diese Abhängigkeit von den verwendeten Rechnersystemen entstanden. Dieses Bewusstsein wird zusätzlich geprägt von der Erkenntnis, wie fehlerbehaftet diese Systeme sind. Auch dies hat das Jahr 2000 gezeigt. Es sind zwar kaum Probleme im Nachhinein aufgetreten, jedoch war der betriebene Aufwand im Vorfeld auch immens.

Diese Abhängigkeit von den Rechnersystemen wird mit weiterer Verbreitung des Internets weiter zunehmen. Der Ende des letzten Jahrtausends begonnene *dot.com*-Boom hat dies eindrucksvoll gezeigt. Die *dot.com*-Blase ist zwar zu Beginn des aktuellen Jahrtausends geplatzt, dennoch sind die Veränderungen in der allgemeinen Wirtschaftslandschaft nicht zurückzudrehen. E-Mail ersetzt zunehmend die persönliche und klassische schriftliche Kommunikation. Geschäftsreisen werden durch Videokonferenzen ersetzt und die Gespräche online durchgeführt. Einkäufe werden über das Internet getätigt. Dies erfolgt sowohl im privaten Sektor (Ebay, Amazon) als auch im geschäftlichen Sektor, in dem der Autohersteller beim Zulieferer neue Teile *just-in-time* bestellt. Diese Entwicklung wird auch dazu führen, dass sich die *dot.com*-Industrie bald erholen wird.

Sobald hohe Geldbeträge oder geheime Informationen ausgetauscht werden, sind Diebe jedoch nicht weit. Das Internet stellt hier keine Ausnahme dar. Im normalen Leben wird jeder Hausbesitzer bei Verlassen seines Hauses die Fenster und Türen verschließen. Damit ist das Haus sicherlich nicht einbruchssicher. Es besteht die Möglichkeit, eine Fensterscheibe einzuschlagen oder gar mit einem Bagger die Hauswand

einzudrücken. Der Hausbesitzer wird sich aber dennoch keine Gedanken um die Sicherheit von Hab und Gut machen. Ein Juwelier wird stärkeren Einbruchsschutz in Form von Panzerglas installieren. Aber auch hier ist ein Bagger in der Lage, die Hauswand einzudrücken. Eine Bank wird versuchen, auch diesem Angriff vorzubeugen, indem der Safe unterirdisch angelegt wird. Im Wesentlichen vertrauen alle darauf, dass der zu betreibende Aufwand für den Einbruch sehr hoch ist. Die Entdeckungsgefahr für den Einbrecher steigt proportional mit der Zeit und dem Lärm, den er erzeugt. Hat der Einbruch tatsächlich stattgefunden, vertraut der Geschädigte, dass die staatlichen Behörden in der Lage sind, den Einbrecher zu ergreifen und zu bestrafen. Der guten Funktion dieses Systems (Rechtsstaat) ist es zu verdanken, dass wenige derartige Straftaten begangen werden. Die Abschreckung ist sehr hoch (selbst bei einer hohen Anzahl von nicht aufgeklärten Verbrechen).

Das Internet unterscheidet sich wesentlich von dieser Umgebung. Es gibt im Internet keine absolute Strafverfolgungsbehörde, die in der Lage ist, die Einbrecher zu verfolgen und zur Rechenschaft zu ziehen. Eine Verfolgung ist, durch die Anonymität oder Verschleierung die man leicht erreichen kann, fast unmöglich. Es ist daher ein Tummelplatz für Diebe, Einbrecher und Spione. Ein Einbruch oder der Diebstahl eines Dokumentes über das Internet bleibt fast immer unentdeckt und ungesühnt. Dies lockt eine ganze Armee von Angreifern an, die entweder aus Spaß oder Profitsucht wahllos oder gezielt Rechner im Internet angreifen. In vielen Fällen erfolgen diese Angriffe bereits automatisiert.

Aus diesen Gründen ist es für Firmen wie für Privatpersonen wichtig, sich in diesem Zusammenhang Gedanken über ihre Sicherheitsmaßnahmen zu machen. Diese Sicherheitsmaßnahmen sollten mindestens drei Punkte berücksichtigen:

- Prävention
- Detektion
- Reaktion

Der Bereich der Prävention wird von Firmen häufig recht gut abgedeckt. Ähnlich einem Juwelier, der sein Geschäft mit Panzerglas ausstattet, werden viele Netzwerke und Rechner durch eine Firewall geschützt. Privatpersonen sind hier häufig weniger umsichtig. Während der Juwelier aber einen Einbruch meist leicht erkennen kann, ist dies im Falle eines Netzwerkes recht kompliziert. Eine Reaktion durch Strafverfolgungsbehörden und eine Verstärkung der präventiven Maßnahmen ist aber nur dann möglich, wenn zuvor der Einbruch erkannt und analysiert wurde. Viele Einbrüche auf Rechnern bleiben aber unerkannt.

Viele Firmen und Anwender wiegen sich leider auch in einer falschen Sicherheit. Begründungen wie »Wer will bei mir schon einbrechen?«, »Wir haben eine Firewall des Herstellers XY installiert.« und »Ich bin nur kurz mit dem Internet verbunden.« müssen als Erklärung für fehlende Sorgfalt beim Einspielen von Updates herhalten. Diese Gruppe verkennt die Tatsache, dass heutzutage ein Großteil der Angriffe durch automatische Werkzeuge durchgeführt werden. Programme, die sich gleich einem Wurm durch das Internet fressen, greifen jeden verwundbaren Rechner in zufälligen Berei-

chen an, brechen ein, installieren sich selbst auf dem eroberten Rechner und beginnen das Spiel von neuem.

Intrusion-Detection-Systeme (IDS) können in diesen Fällen eine sinnvolle Ergänzung der Sicherheitsstruktur darstellen. Hierbei handelt es sich um Systeme, die den Einbruch, den Missbrauch oder eine ungewöhnliche Nutzung (Anomalie-Erkennung) von Computersystemen erkennen. Es werden zwei verschiedene Arten von IDS unterschieden:

- **Netzwerkbasierte IDS (NIDS).** Diese Systeme untersuchen den Netzwerkverkehr nach unerlaubten oder ungewöhnlichen Paketen und melden diese als mögliche Einbrüche.
- **Rechnerbasierte IDS (Host IDS, HIDS).** Diese Systeme überwachen einzelne Rechner. Hier werden meist die Protokolldateien auf ungewöhnliche Ereignisse, die Systemdateien auf ihre Integrität und das Betriebssystem bezüglich seiner Ressourcenausnutzung, Netzkonfiguration und -verbindungen untersucht.

Ein Intrusion-Detection-System kann so eine Sicherheitsstruktur aus Firewall und Virens Scanner sinnvoll erweitern und zusätzliche Informationen liefern. Möglicherweise erkennt die Firewall aufgrund falscher Konfiguration oder fehlender Fähigkeit nicht den Einbruch. Der Virens Scanner erkennt vielleicht nicht die Modifikation der Systemdateien. Das IDS kann dann dennoch diesen Angriff erkennen und melden.

Häufig erfolgt der Angriff auch nicht von außen, sondern der Angreifer befindet sich bereits im Netzwerk. Schätzungen gehen davon aus, dass etwa ein Drittel sämtlicher Angriffe von innen durch Insider erfolgt. Weitere Schätzungen gehen von zwei Dritteln aus. Das australische Computer Emergency Response Team (AusCERT) hat im Jahre 2002 eine Umfrage (www.auscert.org.au/Information/Auscert_info/2002cs.pdf) veröffentlicht, in der 67% aller befragten Organisationen bestätigten, dass ein Angriff erkannt wurde. 89% dieser Organisationen waren von außen angegriffen worden. 65% dieser Organisationen wurden von innen angegriffen. 98% aller befragten Organisationen haben im weitesten Sinne Rechnerkriminalität erfahren. Hierbei handelte es sich um den Diebstahl von Laptops, Sabotage, Virusinfektionen und Betrug. Derartige Angriffe von innen können zum Beispiel auch durch einen unzufriedenen Mitarbeiter ausgeführt werden. Die Firewall wird dies nicht erkennen, da der Angriff nicht von außen kommt.

Jedoch ist auch ein IDS fehlbar. Auch das IDS erkennt nur die Angriffe, für die es konfiguriert wurde. Dies trifft auch auf die Anomalie-Erkennung zu. Zunächst muss der Administrator des IDS definieren, was **normal** ist! Aus diesem Grunde kann zusätzlich die Installation eines Honeypots erwogen werden. Ein Honeypot ist ein System, dessen einziger Zweck der Angriff und der Einbruch durch den Cracker sind. Durch Vergleich der hier gewonnenen Daten mit den Daten des IDS kann das IDS und auch die Firewall angepasst werden, so dass derartige Angriffe in Zukunft abgewehrt werden. Zusätzlich erlaubt ein Honeypot die Schulung der im Falle eines echten Angriffs erforderlichen Fähigkeiten der forensischen Analyse und des Recovery.

Einer der gefährlichsten Angriffe ist jedoch das Social Engineering. Hierbei handelt es sich um einen Angriff und einen Einbruch in die Vertrauenssphäre des Anwenders. Der Angreifer versucht durch Täuschung sicherheitsrelevante Informationen zu erhalten. Das CERT/CC hat hierzu zwei Informationen herausgegeben (<http://www.cert.org/advisories/CA-1991-04.html> und http://www.cert.org/incident_notes/IN-2002-03.html). Hier werden Angriffe beschrieben, bei denen ein Benutzer zur Installation von Programmen oder zur Eingabe seines Kennwortes aufgefordert wird. Der Benutzer ist hierbei in dem guten Glauben, das Richtige zu tun. Social Engineering erfolgt heutzutage meist über E-Mail und Telefon. Hierbei werden Benutzer zum Beispiel auf bestimmte Webseiten gelockt, die anschließend Sicherheitslücken ihrer Webbrowser-Software ausnutzen. Dieses Vorgehen beschreibt Kevin Mitnick in seinem Buch *The Art of Deception* sehr eindrucksvoll. IDS-Systeme können nur dann diese Angriffe erkennen, wenn sie sinnvoll und richtig konfiguriert wurden. Weiterhin sollte eine Schulung der Mitarbeiter durchgeführt werden, um derartigen Angriffen zu begegnen.

Dieses Buch wird einige Werkzeuge, Möglichkeiten und Verhaltensweisen auf der Basis des Linux-Betriebssystems aufzeigen, mit denen der zuständige Anwender einen Einbruch erkennen kann. Die Anwendung der Werkzeuge ist aber nicht auf das Linux-Betriebssystem beschränkt. Einige Anwendungen existieren auch für andere Betriebssysteme wie zum Beispiel Microsoft Windows, einige Anwendungen können weitere Betriebssysteme überwachen.

Das Buch ist in mehrere Teile aufgeteilt. In Teil I wird eine Einführung in die Intrusion Detection und Prevention, ihre Aufgaben, Möglichkeiten und Grenzen gegeben.

In Teil II werden die verschiedenen Open-Source-Softwarelösungen vorgestellt und ihre Konfiguration an Fallbeispielen erklärt.

Der Teil III behandelt Intrusion Prevention Systeme.

Teil IV erläutert dann den Einsatz dieser Produkte in größeren Netzen. Hier wird die zentrale Administration und Überwachung dieser Produkte besprochen. Der Anwender soll nicht die Überwachung sämtlicher Systeme von Hand vornehmen müssen.

In Teil V werden die Ergebnisse der IDS-Systeme analysiert. Hierbei werden modifizierte Dateien auf ihre Änderungen hin untersucht und die Erkennung von Rootkits erläutert. Falls die Dateien gelöscht wurden, werden verschiedene Methoden des Wiederherstellens besprochen. Schließlich werden verdächtige Netzwerkereignisse analysiert.

Der Teil VI erläutert die Reaktion auf derartige Einbrüche. Diese reichen von einfachen Benachrichtigungen an verschiedene zentrale Gremien bis hin zur Übergabe an die Strafverfolgungsbehörden.

Der letzte Teil VII bespricht den Aufbau von so genannten Honeypots. Hierbei handelt es sich um Rechner, welche spezifisch auf den Angreifer zielen. Die Analyse und Überwachung dieser Rechner kann sehr interessante Einblicke in die Vorgehenswei-

se des Angreifers geben. Der Einsatz derartiger Honeypots ist jedoch unter Umständen von Rechts wegen als problematisch einzustufen.

Die Anhänge wiederholen wichtige Grundlagen der TCP/IP-Protokollfamilie und bietet weitere nützliche Informationen bei der Einrichtung eines IDS und IPS.

