



# 1 Was ist eine Intrusion, was ist Intrusion Detection?

Dieses Kapitel versucht die Begriffe *Intrusion* und *Intrusion Detection* zu bestimmen. Anhand von Beispielen sollen die Begriffe erklärt und veranschaulicht werden. Dies soll zum einen die Vielfalt der möglichen Einbrüche oder Missbräuche aufzeigen und zum anderen den Blick zur Erkennung dieser Aktionen und möglicher Sicherheitslücken schärfen.

## 1.1 Was ist eine Intrusion?

Die meisten Bücher und Artikel über Intrusion Detection beginnen mit der Frage: Was ist Intrusion Detection? Die Intrusion selbst wird, wenn überhaupt, erst anschließend definiert. Es ist jedoch sinnvoll, zunächst den Begriff der Intrusion zu definieren, um anschließend ihre Detektion zu beschreiben.

Der Begriff der Intrusion ist jedoch nur schwer in wenige Worte zu fassen. Eine Übersetzung ist möglich mit den Worten: Störung, Verletzung und Eindringen. Folgende Definition der Intrusion Detection Sub Group (IDSG) des National Security Telecommunications Advisory Council (NSTAC) ist sehr allgemein:

»Eine Intrusion ist ein unerlaubter Zugriff auf oder Aktivität in einem Informationssystem.«

Fasst man diesen Ausdruck etwas allgemeiner und weiter, so kann jede unerlaubte, nicht autorisierte Handlung im Zusammenhang mit einem Informationssystem als Intrusion bezeichnet werden. Dies gilt insbesondere, wenn die Handlung die Funktion des Systems beeinträchtigt. Hierzu zählen echte Hackerangriffe und -einbrüche, aber auch Missbräuche der Systeme durch die Anwender. Ein anomales Verhalten des Systems kann ebenfalls bereits eine Intrusion darstellen, wenn eine Richtlinie existiert, die die erlaubte normale Anwendung beschreibt.

Um diese Fälle unterscheiden zu können, wird häufig in der Literatur der Einbruch (Intrusion) vom Missbrauch (Misuse) und der Anomalie (Anomaly) unterschieden. Hierbei wird als Intrusion ein Angriff/Einbruch von außen bezeichnet. Der Missbrauch (Misuse) ist ein Angriff/Einbruch von innen. Die Anomalie stellt einen unge-

wöhnlichen Zustand dar, der auf einen Einbruch hinweisen kann. Diese genaue Unterscheidung soll im Rahmen dieses Buches nicht weiter gemacht werden. Dieses Buch wird Verfahren vorstellen, die sämtliche Bereiche abdecken.

Es zeigt jedoch, dass die Definition der Intrusion auch sehr stark von der Umgebung abhängt, in der sich das zu schützende Objekt befindet. Im Folgenden sollen nun einige Beispiele das belegen.

- Portscan
  - Eine Person führt einen Portscan eines im **Internet öffentlich erreichbaren Rechners** durch. Damit ist sie in der Lage festzustellen, welche Netzwerkdienste auf dem Rechner angeboten werden.
  - Eine Person führt in einem geschützten Netzwerk einen Portscan eines nicht öffentlich erreichbaren Rechners durch.
- Es erfolgt ein Einbruch auf einem Webserver mit anschließender Installation eines Kennwortsnickers. Der Kennwortsnikker ist in der Lage, alle übertragenen Kennwörter zu protokollieren.
- Es erfolgt eine Modifikation der Firewall-Regeln auf der Firewall des Unternehmens.
- Es erfolgt eine Modifikation der Einträge in einer Routing-Tabelle.
- Ein Austausch von Systemkomponenten wurde festgestellt. Hierbei können Trojanische Pferde in Form von Hardware oder Software eingeführt worden sein.

Eine Entscheidung darüber, ob es sich bei den aufgeführten Begebenheiten um eine Intrusion handelt, ist sicherlich nicht immer ganz einfach. Einige der aufgeführten Beispiele stellen mit Sicherheit eine Intrusion dar.

Der Einbruch auf dem Webserver ist sicher eine echte Intrusion und verlangt eine Reaktion durch die verantwortlichen Personen. Die Installation des Kennwortsnickers sollte von einem Intrusion-Detection-System eindeutig erkannt werden. Eine derartige Tätigkeit wird nicht von einer autorisierten Person durchgeführt. Ein Alarm sollte uausgelöst werden.

Bei der Modifikation der Firewall-Regeln kann nicht so einfach eine Zuordnung erfolgen. Dies trifft auch auf die Modifikation der Routing-Tabelle zu. Hier sind zusätzliche Informationen erforderlich.

- Wer hat die Modifikation durchgeführt?
- Warum wurde diese Modifikation durchgeführt?
- War diese Person autorisiert, die Modifikation durchzuführen?

Beim Austausch der Systemkomponenten treffen alle gerade aufgeworfenen Fragen zu. Zusätzlich ist jedoch noch folgende Information erforderlich:

- Ist die Herkunft der neuen Systemkomponenten nachvollziehbar?
- Wird die Integrität der Komponenten vom Hersteller garantiert?
- Besteht die Möglichkeit, dies anhand von Zertifikaten zu überprüfen?

Das Beispiel des Portscans führt immer wieder zu Fehlinterpretationen. Hier soll nun untersucht werden, ob es sich dabei um eine Intrusion handelt. Der Portscan eines öffentlichen Rechners ist im heutigen Internet wahrscheinlich normal. Ein derartiger Portscan stellt noch keinen Angriff geschweige denn einen Einbruch dar. Er kann aber häufig ein erster Schritt in dieser Richtung sein. Der Angreifer benötigt zunächst Informationen über den Rechner, bevor er einen gezielten Angriff starten kann. Daher kann dieser als eine mögliche Intrusion angesehen werden.

Die Realität sieht jedoch inzwischen anders aus. Das Internet wird heutzutage übersät mit Portscans von so genannten Skript-Kiddies. Als Skript-Kiddies werden Personen bezeichnet, die fertige Werkzeuge und Angriffe (z.B. Portscanner und Bufferoverflows) aus dem Internet laden und ausprobieren. Hierbei erzeugen diese Skript-Kiddies zunächst ein Skript, welches einen bestimmten Adressenbereich nach interessanten Rechnern absucht und anschließend einen Angriff auf mögliche Opfer startet.

Wird zum Beispiel ein neues Sicherheitsproblem im WU-ftpD gefunden, so ist ein Skript-Kiddie in der Lage, ein Skript zu erzeugen, welches zunächst einen bestimmten Adressenbereich nach verfügbaren FTP-Servern absucht. Anschließend verbindet sich das Skript mit den gefundenen FTP-Servern und ermittelt deren Version. Handelt es sich um eine verwundbare Version, führt dieses Skript automatisch den Angriff und Einbruch durch.

Ein Portscan ist also nicht unbedingt als etwas anderes als ein spezifisches Interesse des Angreifers an einem einzelnen Rechner zu verstehen. Treten Portscans über mehrere Rechner gleichzeitig auf, so handelt es sich meist um ein derartiges automatisches Werkzeug. Tritt jedoch in einem größeren Netz ein spezifischer Portscan auf, der einen unternehmenskritischen Rechner als Ziel hat, so ist dieser Portscan ernster zu betrachten und kann auch bereits als Intrusion angesehen werden. Hierbei handelt es sich um eine nicht autorisierte und anormale Handlung.

Der Portscan eines nichtöffentlichen Rechners ist ein davon zu unterscheidendes Ereignis. Hierbei kann der Portscan nur von einer Person mit internem Zugang erzeugt werden. Es kann sich um einen Administrator handeln, dessen Aufgabe die Kartierung des Netzwerkes ist. Es kann sich aber auch um einen Mitarbeiter handeln, der in diesem Moment seine Kompetenzen überschreitet und die Richtlinien der erlaubten Verwendung (Acceptable Use) verletzt. Schließlich kann es sich auch um einen Hacker handeln, der bereits in das Netzwerk eingedrungen ist und nun versucht, weitere Informationen über dieses Netzwerk zu ermitteln. Die wesentlichen zusätzlichen Fragen sind auch hier wieder:

- Wer führt den Portscan durch?
- Warum wird dieser Portscan durchgeführt?

Sind diese Informationen bekannt, so kann entschieden werden, ob es sich bei dem Ereignis um eine Intrusion handelt oder nicht. Zusätzlich kann entschieden werden, ob es sich um den Spezialfall eines echten Angriffes/Einbruches (Intrusion) oder um einen Missbrauch (Misuse) handelt.

Im Grunde macht es Sinn, als Oberbegriff für Intrusion, Misuse und Anomaly einen neuen Begriff zu wählen. Hierbei wird in vielen anderen Veröffentlichungen der Begriff *Incident* gewählt. Dieser bezeichnet jedes Ereignis im Zusammenhang mit einem Informationssystem, welches eine Reaktion durch die Administratoren erfordert. Dies können auch zum Beispiel Programmabstürze sein, die nicht aufgrund einer Intrusion oder Misuse erfolgen.

## 1.2 Was macht die Intrusion Detection?

Nachdem der letzte Abschnitt versucht hat, ein wenig Verständnis für den Begriff der Intrusion aufzubauen und diesen genauer zu definieren, soll dieser Abschnitt nun die Intrusion Detection beschreiben. Ihre Aufgaben und ihre Verfahren sollen kurz und allgemein dargestellt werden.

Die Intrusion Detection besteht heute aus den drei Teildisziplinen:

- Angriffs-/Einbruchserkennung (die eigentliche Intrusion Detection)
- Missbrauchserkennung (Misuse Detection)
- Anomalie-Erkennung, die Erkennung ungewöhnlicher Verhaltensmuster (Anomaly Detection)

Die bereits zitierte Intrusion Detection Sub Group (IDSG) definiert Intrusion Detection als einen Prozess, der »feststellt, dass eine Intrusion versucht wurde, gerade erfolgt oder in der Vergangenheit erfolgte«.

Die Intrusion Detection verwendet unterschiedliche Technologien und Systeme für die Erkennung dieser Ereignisse. In diesem Buch soll nicht weiter zwischen diesen einzelnen Teildisziplinen unterschieden werden, sondern es sollen praxisrelevante Beispiele gegeben werden. Die Technologien und Systeme werden in weiteren Kapiteln besprochen. Im Folgenden werden die drei Teildisziplinen der Intrusion Detection daher nur kurz angerissen.

### 1.2.1 Angriffs-/Einbruchserkennung

Diese Teildisziplin versucht einen nicht autorisierten Zugriff von außen zu erkennen. Der Einbruch auf dem Webserver, der im vorigen Abschnitt erwähnt wurde, stellt einen derartigen Einbruch von außen dar.

### **1.2.2 Missbrauchserkennung**

Diese Teildisziplin versucht den Missbrauch durch Insider zu erkennen. Hierbei kann es sich zum Beispiel um Benutzer handeln, die bei Verletzung der Sicherheitsrichtlinien versuchen, Zugriff auf gewisse Dienste im Internet zu erhalten oder auf ihrem Rechner einen Dienst zu installieren, der Online-Spiele ermöglicht.

### **1.2.3 Anomalie-Erkennung**

Diese Teildisziplin versucht ungewöhnliche Zustände der Systeme und des Netzwerkes zu erkennen. Benötigt ein Benutzer zum Beispiel für seine Anmeldung zehn Versuche oder werden plötzlich Netzwerkpakete versandt, die ein bisher nie genutztes Protokoll verwenden, so ist es Aufgabe dieser Disziplin, diese Ereignisse zu erkennen.

## **1.3 Was macht die Intrusion Prevention?**

Die Intrusion Prevention ist eine neue Erfindung der letzten vier bis fünf Jahre. Ausgehend von der Intrusion Detection versucht diese Disziplin direkt den erkannten Angriff wirksam zu verhindern. Die Hersteller der Intrusion-Detection-Systeme versuchen hier Ihre Produkte mit neuen Namen an neue Kunden zu verkaufen.

Um den Angriff wirksam verhindern zu können, muss ein Intrusion Prevention System (IPS) den laufenden Angriff erkennen und vor seiner Vollendung hindern. Das System muss proaktiv arbeiten. Ein klassisches IDS, welches lediglich mit einer Protokollmeldung reagiert, genügt hier nicht. Die verschiedenen Methoden zur Implementierung eines IPS werden im nächsten Kapitel beleuchtet.

