



# 6 IDS im Einsatz

Dieses Kapitel zeigt den typischen Zyklus bei der Umsetzung einer Sicherheitsstruktur auf. Hierbei wird auch auf den Einsatz eines IDS eingegangen. Der typische Zyklus besteht aus:

1. Prävention
2. Einbruch
3. Erkennung
4. Reaktion
5. Analyse
6. Recovery
7. Konsequenzen

## 6.1 Prävention

Bei der Umsetzung einer Sicherheitsstruktur wird zunächst mit der Phase der Prävention begonnen. Hierbei werden grundsätzliche Maßnahmen zur Verbesserung der Sicherheit durchgeführt. Dies sind Maßnahmen sowohl zur Verbesserung der Sicherheit auf Software-Ebene als auch auf physikalischer Ebene.

Die Prävention besteht üblicherweise aus folgenden Eckpfeilern:

- Update der Betriebssysteme
- Deaktivierung der unnötigen Dienste
- Installation von Virenscannern auf den Systemen
- Audit und Reorganisation des Netzwerks
- Räumliche Trennung und Verschluss wichtiger Systeme
- Deaktivierung nicht verwendeter Netzwerkzugänge
- Installation einer Firewall
- Installation eines IDS
- Verwendung verschlüsselter Anmeldesysteme
- Bildung eines Notfallplans und Erzeugung eines Notfallplans

Leider wird die physikalische Sicherheit und die Installation von ID-Systemen vernachlässigt. Die im Jahre 2002 durchgeführte Umfrage des Computer Security Institute (CSI) in Kombination mit dem Federal Bureau of Investigations (FBI) (503 befragte Unternehmen) zeigt, dass 84% aller Unternehmen physikalische Sicherheit implementierten, 60% aller befragten Unternehmen ein IDS und 50% verschlüsselte Anmeldesysteme verwendeten (<http://www.gocsi.com/press/20020407.html>). Die im selben Jahr vom AusCERT durchgeführte Umfrage zeigt ähnliche Werte für die australischen Unternehmen ([http://www.auscert.org.au/Information/Auscert\\_info/2002cs.pdf](http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf)).

Eine Aktualisierung der verwendeten Betriebssysteme auf den neuesten Stand und eine Deaktivierung sämtlicher nicht benötigter Dienste sollte selbstverständlich sein. Dies sollte eine allgemeine Tätigkeit der Administratoren bei der Installation und späteren Wartung eines Betriebssystems darstellen. Eine Firewall darf nicht als möglicher Ersatz der Systempflege angesehen werden!

Die Installation von Virenscannern auf allen Systemen ist ebenso erforderlich. Die reine Installation der Virenscanner auf bestimmten Servern ist nur dann möglich, wenn keine eigentlichen Client-Systeme existieren, wie zum Beispiel in einer Terminalserver-Lösung. Ansonsten bestehen zu viele Möglichkeiten des Vireneintritts in ein Netzwerk. Hierbei handelt es sich um E-Mails, Disketten und durch den Anwender hergestellte CD-ROMs. Weitere Möglichkeiten sind denkbar.

Eine Reorganisation der Netzwerkstruktur kann ebenfalls präventiven Charakter haben. Hierbei können die besonders kritischen Systeme für eine einfache Überwachung gruppiert werden. Querverbindungen können unterbunden werden, um eine Überwachung zu garantieren. Dies ermöglicht in einem weiteren Schritt die einfache Installation einer Firewall.

Die Deaktivierung der nicht verwendeten Netzwerkzugänge ist sehr wichtig. Häufig wird dies vergessen. Hiermit sind sowohl ungenutzte Modemzugänge als auch ungenutzte Patch-Dosen gemeint. Ansonsten besteht die Gefahr, dass ein Eindringling einen zusätzlichen Rechner mit dem Netzwerk verbinden kann. Dieser Rechner hat anschließend bereits die Firewall überwunden und kann ohne weitere Beschränkung im Netzwerk agieren. Interessierte mögen sich die Verwendung der Dreamcast-Spielekonsole zu diesem Zweck anschauen: <http://www.dcphonehome.com>.

Schließlich sollte eine Firewall als präventive Maßnahme installiert werden. Die Installation einer Firewall wird sehr ausführlich in verschiedenen weiteren Büchern beschrieben, eine Auswahl finden Sie in den Literaturhinweisen auf S. 820. Diese Firewall soll den Netzwerkverkehr entsprechend der Sicherheitsrichtlinie überwachen.

Die Installation eines IDS schließt die präventiven Maßnahmen ab. Dieses IDS soll den Erfolg der präventiven Maßnahmen bestimmen. Die Installation eines IDS wird in diesem Buch recht ausführlich behandelt.

Im Wesentlichen handelt es sich bei allen anderen präventiven Maßnahmen um Vorbeugungsmaßnahmen, die die vorhandenen bekannten Sicherheitslücken schließen sollen. Hiermit soll ein Einbruch nach bestem Wissen und Gewissen unmöglich sein.

## 6.2 Einbruch

Trotz aller präventiven Maßnahmen wird ein Einbruch stattfinden. Es ist eigentlich nur eine Frage der Zeit. Im Bereich der Computersicherheit arbeitet kaum jemand, der nicht selbst Opfer eines Einbruchs wurde. Wird dies dennoch behauptet, so haben diese Personen meist einen erfolgreichen Einbruch nicht erkannt. Diese Einbrüche sind die Folge verschiedenster Aspekte. Meist sind die folgenden Punkte verantwortlich:

- Schlampige Systemwartung
- Fehler bei der Administration der Firewall oder der Router
- Vergessene Testsysteme und -zugänge
- Neue unbekannte Sicherheitslücken in scheinbar sicheren Systemen

Diese Punkte sind verantwortlich für die meisten Sicherheitslücken in modernen Netzwerken. Hierbei handelt es sich zum Beispiel um den Systemadministrator, der vorübergehend die Regeln einer Firewall zu Testzwecken modifiziert. Leider wird nach dem Test vergessen, die Modifikationen wieder rückgängig zu machen oder es existiert keine Dokumentation, die eine Wiederherstellung des Grundzustandes erlaubt.

Genauso häufig werden zu Testzwecken Webserver oder E-Mail-Server installiert, die nach Beendigung des Tests nicht deaktiviert werden. (*Wer weiß, ob wir den noch mal gebrauchen können?*)

Ein Einbruch ist also unausweichlich. Dies sollte jedem Administrator deutlich sein, der sich mit Sicherheitsfragen beschäftigt. Angriffe gehören sogar zur Tagesordnung.

## 6.3 Erkennung

Wenn der Einbruch erfolgt ist, ist es wichtig, diesen zu erkennen. Dies ist Aufgabe des Intrusion-Detection-Systems, aber auch des Personals.

Viele Einbrüche können sehr gut von ID-Systemen erkannt werden. Hierzu ist es aber auch erforderlich, dass diese Systeme so installiert wurden, dass eine Erkennung möglich ist. Wenn gewisse Rechner ausgespart werden, weil die Installation eines IDS die Nutzung, Administration und Wartung stark beeinträchtigen würde, so wird dieses System nicht durch ein IDS überwacht. Eine Überwachung kann dann nur sekundär erfolgen, da dieses System vielleicht im Netzwerk Auffälligkeiten zeigt.

Ein typisches Beispiel sind normale Arbeitsplatzrechner. Diese werden meist nicht von einem IDS überwacht. Der geringe Wert der auf dem System gespeicherten Daten rechtfertigt in vielen Fällen nicht den Einsatz eines IDS. Eine Putzfrau oder ein Wartungstechniker ist aber in der Lage, diese Systeme möglicherweise von Diskette neu zu starten oder das Kennwort von einer gelben Klebenotiz unter der Tastatur abzulesen. Anschließend können diese Personen das Netzwerk scannen, Anmeldeversuche auf anderen Rechnern unternehmen oder nur den Netzwerkbetrieb stören.

Diese Aktivitäten können nicht von einem IDS auf dem Rechner erkannt werden, da hier kein IDS existiert. Die Erkennung muss über die ID-Systeme erfolgen, welche die sekundär angegriffenen Rechner oder das Netzwerk überwachen.

Eine besondere Sorte von Angriffen kann nur vom Personal erkannt werden. Leider handelt es sich hierbei auch um einen der gefährlichsten Angriffe: *Social Engineering*. Das Social Engineering ist kein Angriff auf die Hard- oder Software, sondern auf den Menschen (genannt *Wetware*). Hierbei wird 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](http://www.cert.org/incident_notes/IN-2002-03.html)).

Damit diese Angriffe aber vom Personal erkannt und gemeldet werden können, ist es erforderlich, dass es diesbezüglich geschult wird.

## 6.4 Reaktion

Nach Erkennung des Einbruches erfolgt die erste Reaktion. Die wichtigste Regel an dieser Stelle ist:

### Do Not Panic!

Anschließend sollten die folgenden Schritte unternommen werden. Dies kann auch im aufgestellten Notfallplan spezifiziert werden.

- Stopp des Einbruchs, wenn möglich: Trennung des Systems vom restlichen Netzwerk, Deaktivierung des Benutzerkontos etc.<sup>1</sup>
- Analyse und Dokumentation aller Umstände
- Spiegelung des Systems für eine spätere Analyse
- Einschätzung des Vorfalles
- Berichterstattung

Die Analyse und die Dokumentation der vorgefundenen Umstände des Systems sind wichtig für die nun erfolgende Einschätzung des Vorfalles. Es ist nun zunächst wichtig zu ermitteln, wie viele Rechner in welchem Ausmaß und in welcher Form kompromittiert wurden. Dies kann sicherlich nicht sofort in allen Einzelheiten bestimmt werden. Das ist die Aufgabe einer späteren forensischen Analyse. Dennoch sollte durch eine Auswertung der IDS-Daten versucht werden, die betroffenen Rechner und Anwendungen zu bestimmen. Hierbei sollten die folgenden Fragen beantwortet werden:

- Wie viele Rechner sind betroffen?
- Wie viele Netzwerke sind betroffen? War der Einbrecher in der Lage, zum Beispiel über ein VPN auf andere Netze zuzugreifen?

<sup>1</sup> Bei einer Trennung vom Netz ist jedoch zu beachten, dass möglicherweise die Daten über die aufgebauten Netzwerkverbindungen verloren gehen. Diese müssen dann im Vorfeld gesichert werden.

- Hat der Einbrecher privilegierte Rechte (*root*) erlangen können?
- Sind weitere Rechner ähnlich verwundbar?

Die Antworten auf diese Fragen sollten einen groben Eindruck vom Ausmaß des Einbruchs geben. Außerdem sind dies die Fragen, die auch in einem ersten Bericht beantwortet werden müssen.

Die Abgabe eines Berichtes ist verpflichtend. Dies ist am einfachsten mit einer Sicherheitsrichtlinie (Security Policy) zu erreichen. Diese Richtlinie muss die folgenden Punkte definieren:

- **Form des Berichtes.** Dies kann E-Mail, Papierform, mündlich etc. sein.
- **Empfänger des Berichtes**
- **Zeitpunkt des Berichtes.** Wie schnell muss dieser Bericht verfasst werden?
- **Inhalt.** Welche Informationen muss dieser Bericht enthalten und bei welchen Vorfällen muss ein Bericht angefertigt werden?

Dann sollte entschieden werden, wie reagiert wird. Dies kann von einer kompletten Abschaltung bis hin zu einem Ignorieren des Vorfalls reichen, wenn er sich als harmlos herausstellt.

## 6.5 Analyse

Im Folgenden wird der Vorfall genauer analysiert und der sichere Zustand wiederhergestellt. Die Reihenfolge dieser beiden Punkte wird meist von äußeren Umständen diktiert.

In Abhängigkeit vom betroffenen System oder Benutzerkonto kann das System für mehrere Stunden oder Tage aus dem Betrieb genommen werden. Einige Systeme dürfen jedoch nicht einmal für wenige Minuten oder Stunden den Betrieb einstellen. So wird die Entscheidung über das weitere Vorgehen nicht von den Administratoren, sondern von den Bedürfnissen des Unternehmens entschieden.

Ein Webserver, der eine E-Commerce-Lösung anbietet, wird wahrscheinlich bei einem kleineren Einbruch nicht sofort abgeschaltet werden. Hier steht das Unternehmensziel im Vordergrund, über diese Lösung weiterhin Kunden bedienen zu können. Wenn jedoch der Webserver auch einen Zugriff auf (Kreditkarten-)Informationen der Kunden ermöglicht, sollte über eine Abschaltung doch nachgedacht werden. In vielen Fällen wird eine Wiederherstellung des sicheren Zustandes im laufenden Betrieb angestrebt werden. Die Behandlung der unternehmenskritischen Systeme sollte auch in einer Sicherheitsrichtlinie definiert werden, damit später nicht zu viel Zeit für die Entscheidung verloren geht.

Ein Rechner, der lediglich als Backup zur Verfügung steht, kann unter Umständen für einige Tage oder Stunden von seiner Aufgabe für eine genauere Analyse und die folgende Wiederherstellung entbunden werden.

Unabhängig davon, ob die Analyse vor der Wiederherstellung, parallel oder anschließend durchgeführt wird, sollten die Daten des Systems für die Analyse gesichert werden. Die Analyse eines Systems wird im Kapitel 20, »Analyse des Rechners nach einem Einbruch« beschrieben.

Das Ziel der Analyse ist ein umfassendes Verständnis des Einbruchs. Dieses Verständnis ist erforderlich, um bei einer Wiederherstellung des Systems einen erneuten anschließenden Einbruch mit den gleichen Methoden verhindern zu können. Im Einzelnen soll die Analyse die folgenden Fragen beantworten:

- Welche Methode hat der Angreifer angewendet?
- Welche Systemkomponente wurde angegriffen und weist sie Sicherheitslücken auf?
- Welche Tätigkeiten hat der Angreifer anschließend ausgeführt?
- Welches Ziel verfolgte der Angreifer mit diesen Tätigkeiten?
- Wurden wichtige Unternehmensdaten modifiziert oder gelöscht?
- Wie kann dieser Angriff in Zukunft verhindert werden?

Es kann hier nicht verschwiegen werden, dass nicht immer alle Fragen beantwortet werden können. In Abhängigkeit von den Fähigkeiten des Angreifers und der analysierenden Person besteht auch die Gefahr, dass die Analyse keine Erkenntnisse liefert. Dies ist möglich, da der Angreifer in der Lage war, effektiv alle Spuren zu verwischen, oder die analysierende Person nicht über die Geräte, Fähigkeiten und Erfahrungen verfügt, diese Spuren zu erkennen.

## 6.6 Recovery

Die Wiederherstellung des Systems in einen sicheren Zustand ist die nächste Phase im Zyklus. Hierbei ist es das Ziel, das System in einen Zustand zu versetzen, der es erlaubt, den Dienst auf diesem System wieder aufzunehmen.

Erfolgte im Vorfeld eine Analyse des kompromittierten Systems, so existiert ein Verständnis für den Vorfall. Die ausgenutzte Sicherheitslücke und die anschließenden Tätigkeiten des Einbrechers sind hoffentlich in der Analyse erkannt worden. Dies erlaubt eine sehr zielgerichtete Wiederherstellung des Systems. Unter Umständen ist es sogar möglich, das System ohne eine Neuinstallation wieder in einen sicheren Zustand zu versetzen.

In vielen Fällen wird jedoch die Analyse nicht mit endgültiger Sicherheit sämtliche Tätigkeiten des Einbrechers erkennen lassen. Außerdem existieren häufig Sicherheitsrichtlinien, die bei einem Einbruch auf einem System eine Wiederherstellung des System von originalen Datenträgern und Sicherungen verlangen. Dann sollte das System mit den entsprechenden Datenträgern und Sicherungen wiederhergestellt werden. Es dürfen dazu nur Sicherungen verwendet werden, bei denen eindeutig si-

chergestellt ist, dass der Einbrecher zu diesem Zeitpunkt noch nicht in das System eingedrungen war.

Ein derartiges Recovery wird jedoch auch die alte Sicherheitslücke im System wieder einführen. Bevor das System nun seinen Betrieb wieder aufnimmt, sollte diese Sicherheitslücke behoben werden. Dies kann möglicherweise durch eine Deaktivierung des Dienstes erfolgen und benötigt somit keine weitere Modifikation des Betriebssystems oder der Anwendung. In den meisten Fällen wird jedoch dieser Dienst benötigt und eine Abschaltung stellt keine Option dar. Dann bestehen immer noch zwei Möglichkeiten:

1. Patch des Herstellers
2. Modifikation der Firewall, so dass der Angreifer nicht mehr zugreifen kann:

Der Punkt 1 ist sicherlich die Methode der Wahl. Leider stehen jedoch gerade bei proprietären Anwendungen nicht immer Patches zur Verfügung. Wenn es sich um eine sehr neue Sicherheitslücke handelt, so erfolgte häufig noch keine Reaktion des Herstellers und ein Patch ist erst in Tagen oder Wochen verfügbar. Dann kann versucht werden, einen erneuten Zugriff des Angreifers auf diesen Dienst zu verhindern. Dies ist sicherlich nicht bei allen Diensten möglich. Besonders bei Diensten, die im Internet angeboten werden sollen, wird dies recht problematisch. Ein intelligentes IDS, welches in der Lage ist, den Angriff zu erkennen und die Verbindung zu unterbrechen, kann hier den letzten Ausweg darstellen.

## 6.7 Konsequenzen

Der letzte Schritt im Intrusion Detection-Zyklus sollte die Konsequenzen für das Netzwerk und die Sicherheitsstrukturen ermitteln. Leider wird dieser Teil viel zu häufig vergessen und versäumt. In diesem Schritt sollen die Netzwerkstruktur, die vorhandenen Sicherheitsstrukturen, die Vorgehensweise bei der Behandlung des Vorfalls, die Fähigkeiten der beteiligten Personen etc. unter dem Lichte des Vorfalls betrachtet werden.

Wird ein Vorfall anschließend derartig aufgearbeitet, so lassen sich meist sehr nützliche Lektionen erlernen. Die Vorteile einer derartigen Aufarbeitung sind sehr vielfältig.

Zunächst wird die gesamte Netzwerkstruktur erneut einem Audit unterworfen. Hierbei werden spezifisch die Teile des Netzwerks untersucht, die überhaupt erst den Erfolg des Angriffs (oder zukünftiger ähnlicher Angriffe) möglich gemacht haben. Das Ergebnis dieser Untersuchung sollte entweder eine Modifikation der Netzwerkstruktur empfehlen oder ergeben, dass das Netzwerk optimal aufgebaut wird.

Anschließend sollen die Sicherheitsstrukturen (Firewall, IDS, Virens Scanner, Anmeldesysteme etc.) untersucht und geprüft werden, inwieweit sie den Angriff oder ähnliche Angriffe ermöglichen. Auch dieser Audit kann zwei verschiedene Ergebnisse bringen. Entweder waren die Sicherheitsstrukturen optimal eingesetzt und konfigu-

riert oder es werden Verbesserungsvorschläge entwickelt. Diese Verbesserungsvorschläge können auch zum Austausch von Sicherheitsstrukturen führen. So kann zum Beispiel ein einfaches Anmeldesystem mit Login/Kennwort ersetzt werden durch ein Smartcard-System.

Die Evaluierung der Vorgehensweise und der Fähigkeiten der Personen, die mit der Behandlung des Vorfalls beauftragt wurden, soll mögliche Lücken aufzeigen. Hier sollte nicht eine Schuldzuweisung erfolgen oder gar schmutzige Wäsche gewaschen werden. Es ist jedoch wichtig, dass Lücken bei der Vorgehensweise und fehlende Fähigkeiten erkannt werden, damit diese in Zukunft beseitigt werden können.

Wenn erkannt wurde, dass eine oder mehrere Personen ein bestimmtes Wissen oder die notwendige Erfahrung nicht besitzen, sollten diese Personen nicht ausgeschlossen werden. Sie wurden im Vorfeld auch aus bestimmten Gründen in das Team aufgenommen und haben bereits die Arbeit kennen gelernt. Vielmehr sollten diese Personen anschließend geschult werden. Dann werden sie auch bereit sein, selbst die Lücken zuzugeben und sich im Weiteren noch besser in ein Notfallteam einzugliedern.

Wenn jedoch die Lücken nicht richtig erkannt werden und keine Abhilfe durch Schulungen oder ähnliche Verfahren geschaffen wird, besteht die Gefahr, dass beim nächsten Einbruch wertvolle Fähigkeiten fehlen.

Diese Bewertung und die gezogenen Konsequenzen sollten immer zum Ziel haben, die Stabilität, die Fähigkeiten und die Zusammenarbeit des Teams zu verstärken. Daher muss sehr stark darauf geachtet werden, dass keine Konkurrenz zwischen den einzelnen Mitgliedern während der eigentlichen Behandlung des Vorfalls oder der Evaluierung entsteht.

Wenn die Evaluierung durchgeführt wurde und die entsprechenden Konsequenzen gezogen wurden, befindet sich der Zyklus wieder in der Phase 1: Prävention. Wir befinden uns an einem Punkt, an dem alle präventiven Maßnahmen abgeschlossen sind und das Notfallteam, das Computer Emergency Response Team, auf das nächste sicherheitsrelevante Ereignis (Einbruch) wartet. Dies sollte jedoch keine tote Phase sein, sondern sie muss stets eine weitere Verbesserung der Sicherheitsstrukturen und der Aufmerksamkeit der Anwender zum Ziel haben.