



5 Vorbereitung auf den Ernstfall

Dieses Kapitel beschäftigt sich mit den vorbereitenden Maßnahmen beim Einsatz eines Intrusion-Detection-Systems. Hierbei handelt es sich auch um allgemeine Maßnahmen, die grundsätzlich bei der Entwicklung einer Sicherheitsstrategie ins Auge gefasst werden sollten. Bei der Umsetzung einer IDS-Struktur sind diese Maßnahmen aber besonders wichtig. Im Wesentlichen handelt es sich um folgende Fragestellung: Wer reagiert wie und wann?

1. Bildung eines Notfallteams
2. Erstellung eines Notfallplans
3. Erstellen einer Sicherheitsrichtlinie

5.1 Notfallteam: Computer Emergency Response Team

Bevor ein IDS-System implementiert wird, sollten bereits gewisse Vorkehrungen getroffen werden. Eine grundsätzliche Frage ist: Wer reagiert in einem Notfall (z.B. Einbruch)? Wird diese Frage erst gestellt, wenn der Einbruch stattgefunden hat, ist es eigentlich immer zu spät. Es finden sich möglicherweise nicht die geeigneten Personen. Die Teamarbeit dieser Personen ist nicht erprobt und die Kompetenzen sind nicht im Vorfeld abgeklärt worden. Die Kenntnisse der Personen genügen möglicherweise nicht dem Anspruch eines Notfallteams und die Personen benötigen zusätzliche Schulungen. Eine Anerkennung der Ergebnisse vor Gericht ist sehr fraglich, da die Fachkunde und die Sachkenntnis der beteiligten Personen nicht nachgewiesen werden können.

Um derartige Probleme zu vermeiden, sollte jedes Unternehmen ab einer bestimmten Größe über ein Incident Response Team oder Computer Emergency Response Team (CERT) verfügen, welches in Notfällen die Kompetenz und das Wissen besitzt, zu reagieren. Hierzu sind die folgenden Fragen zu klären:

- Wie wird dieses Team finanziert?
- Wer ist Mitglied des Teams?
- Wem ist das Team Rechenschaft schuldig und wer ist weisungsberechtigt gegenüber dem Team?
- Welche Dienste bietet das CERT?

Die Vorteile eines derartigen Teams liegen auf der Hand. Die folgende Auflistung stellt eine Auswahl der Vorteile eines vorhandenen Teams dar:

- **Wissen.** Die Mitglieder des Teams können spezifisch geschult werden und beschäftigen sich mit hoher Priorität mit den Themen, für die das Team geschaffen wurde.
- **Koordination.** Die Kompetenzen im Team können einmalig verteilt werden. Eine Koordination unter den Mitgliedern ist sehr leicht möglich, da sowohl der Leiter als auch die einzelnen Mitglieder ihre Fähigkeiten und Verfügbarkeiten gut beurteilen können.
- **Vorsorge.** Das Team ist in der Lage, Sicherheitsprobleme bereits im Vorfeld zu erkennen und deren Abhilfe anzuregen.
- **Unabhängigkeit.** Das Team kann als eigenständige Struktur im Unternehmen frei von politischen Querelen und Barrieren arbeiten.

Bei der Bildung eines Notfallteams wird häufig zu Beginn die Frage aufgeworfen, wie groß das Team werden muss. Dies hängt sicherlich von der Größe des Unternehmens und der Vielfalt der eingesetzten Systeme ab. Kleine Firmen werden kein Team bilden, da sie nicht über die personellen Ressourcen verfügen. Hier wird es sich meist um eine einzelne Person handeln, die die Aufgaben des Teams wahrnehmen wird. Je größer das Unternehmen ist und je mehr verschiedene Systeme zum Einsatz kommen, umso größer wird das Team werden. Das Team soll mindestens einen Experten für jedes eingesetzte Computersystem enthalten. Diese Personen müssen nicht ständige Mitglieder des Teams sein. Sie können bei Bedarf hinzugerufen werden. Es sollten aber einige ständige Mitglieder zur Koordination des Teams vorhanden sein.

Die Anforderungen an das Team und seine Funktionen müssen die folgenden Punkte umfassen:

- Das Notfallteam und die betroffene Abteilung führen gemeinsam die Tätigkeiten zur Behandlung des Notfalls durch. Jedoch sollte grundsätzlich geklärt sein, wer in diesem Fall weisungsberechtigt ist. Es ist auch möglich, dass das Team die vollständige Kontrolle übernimmt. Dies führt jedoch häufig zu einer fehlenden Bereitschaft zur Zusammenarbeit bei den betroffenen Abteilungen.
- Das Notfallteam sollte den Kontakt zu anderen Teams weiterer Unternehmen oder zu öffentlichen Notfallteams zum Zwecke des Informationsaustausches aufrechterhalten und pflegen. Hierbei sind die nationalen CERTs, CERT-Bund (<http://www.bsi.bund.de/certbund>) und DFN-CERT (<http://www.cert.dfn.de/>) sowie das CERT/CC (<http://www.cert.org>) besonders zu erwähnen.
- Das Notfallteam sollte Werkzeuge zur Verbesserung der Sicherheit entwickeln und/oder evaluieren.
- Das Notfallteam sollte Planungen für den Fall eines Einbruches oder eines Angriffes durchführen. Übungen ähnlich einer Feuerwehrrübung können die Funktionsweise des Plans testen und nachweisen.

- Das Notfallteam muss seine eigenen Fähigkeiten in Schulungen erweitern und durch Schulungen der Mitarbeiter diese Informationen auch weitergeben.

In vielen Fällen werden die Unternehmen jedoch nicht selbst ein Team bilden wollen, welches diese Funktionen wahrnimmt, sondern diese Leistung extern einkaufen. Dies kann, insbesondere für kleinere Unternehmen, eine sehr effektive und kostengünstige Variante darstellen, da das Team nur mit den tatsächlich vorkommenden Ereignissen umgehen muss. Es muss nicht rund um die Uhr vor Ort verfügbar sein. Leider kennen derartige externe Notfallteams häufig nicht die internen Strukturen und Anforderungen des Unternehmens gut genug, um auf diese eingehen zu können. Des Weiteren sind diese Teams nicht immer verfügbar. Die Qualität ihrer Arbeit ist schwer zu beurteilen. Es existieren unterschiedlichste Anbieter mit den unterschiedlichsten Dienstleistungen in diesem Bereich des Marktes. Der teuerste ist nicht immer unbedingt der beste Anbieter.

5.2 Notfallplan

Ein ausgearbeiteter Notfallplan ist bei einem sicherheitsrelevanten Ereignis schnell in der Lage, Organisation in das entstehende Chaos zu bringen. Meist entsteht bei einem sicherheitsrelevanten Ereignis, wie zum Beispiel einem Einbruch auf einem Webserver, eine ziellose ungeordnete Aktivität, bei der verschiedenste Personen unterschiedliche Richtungen in der Behandlung des Ereignisses einschlagen.

Ein Einbruch ist vergleichbar mit einem Feuer. Das Notfallteam stellt die Feuerwehr dar. Eine Feuerwehr ohne Organisation und Plan kann nur die einfachsten und kleinsten Feuer löschen. Sobald ein Mehrfamilienhaus oder eine Lagerhalle mit unbekanntem Inhalt brennt, kann sie nicht mehr adäquat reagieren. Müssen zuerst Menschen gerettet werden? Mit welchen Löschmitteln darf gelöscht werden? Ist Atemschutz zu tragen? Kann das Feuer auf andere Gebäude übergreifen? Die Antworten auf diese Fragen und die Reihenfolge der auszuführenden Arbeiten können nur durch sorgfältige Planung und Training im Vorfeld bestimmt werden. Das Notfallteam steht vor denselben Fragen.

Der Notfallplan sollte die folgenden Fragen beantworten:

- Wie erfolgt die Alarmierung des Notfallteams?
Dies beinhaltet die Adressen der Mitglieder, Mobiltelefon-Nummern und Regeln der Eskalation.
- Reaktion auf die üblichen Gefahren
 - Virus-Infektion
 - Auf einem Rechner
 - Infektion aller/vieler Rechner
 - Angriff eines Servers
 - Einbruch auf einem Server

- Darf der Rechner abgeschaltet werden?
- Wie lange darf der Rechner vom Netzwerk getrennt werden?
- Angriff/Einbruch auf einer Workstation
- Recovery
 - Wird eine forensische Analyse durchgeführt?
 - *Wer* stellt *wann* den sicheren Zustand des Rechners *wie* wieder her?
 - Wer darf entscheiden wann ein sicherer Zustand wieder erreicht ist?
 - Wer darf (in welchem Umfang) kurzfristig Finanzmittel freigeben?
- Berichterstattung
 - *Wer* erstattet *wann* und in welchen Abständen Bericht?
 - *Wie* ausführlich ist dieser Bericht?

Werden diese Fragen bereits im Vorfeld für die in Frage kommenden Rechner in einer Sicherheitsrichtlinie beantwortet und diese von der Unternehmensleitung abgesegnet, so kann das eigentliche Problem wesentlich schneller, reibungsloser und zielgerichteter behandelt werden.

5.3 Entwicklung der Sicherheitsrichtlinie

Eine Frage, die bisher noch gar nicht betrachtet wurde, soll in diesem Abschnitt gestellt werden: *Was* ist ein sicherheitsrelevantes Ereignis? Sicherlich ein Angriff oder ein Einbruch. Wie wird dieser Angriff, Einbruch oder Missbrauch definiert? Darf ein Anwender unternehmenseigene Dateien per E-Mail versenden? Darf ein Anwender auf JavaScript-haltige oder pornografische Seiten zugreifen? Darf ein Anwender ein Modem installieren?

Diese Fragen berühren das Intrusion-Detection-System nicht nur am Rande. Ein Intrusion-Detection-System ist, wie eine Firewall, in der Lage, bei vielen dieser Fragen das Einhalten einer Sicherheitsrichtlinie zu überprüfen. Hierzu muss allerdings eine Sicherheitsrichtlinie existieren, die mithilfe der Firewall und des IDS-Systems umgesetzt werden kann.

Dieses Kapitel soll einige Hilfen bei der Erstellung einer derartigen Sicherheitsrichtlinie geben.

Es sollten Richtlinien für die folgenden Bereiche entwickelt werden:

- Zugänge
 - Login-Name und Kennwortlänge
 - Verschlüsselung
 - PKI und Smartcards
- Akzeptierte Benutzung (Acceptable Use)

- Allgemeine Verwendung der Systeme
- Verhalten bei Viren
- Physikalische Sicherheit
 - Netzwerkarchitektur
 - Physikalischer Zugang zu den Rechnern und dem Netzwerk
- Fernzugriff
 - Internetzugriff
 - VPN-Zugriff
 - Websurfen
 - E-Mail

Wichtig ist es bei der Verfassung der Sicherheitsrichtlinien, die Zielgruppe nicht aus den Augen zu verlieren. Die Sicherheitsrichtlinien müssen so verständlich geschrieben sein, dass ein normaler Benutzer in der Lage ist, sie zu verstehen. Dies kann nur durch kurze prägnante Richtlinien erreicht werden. Ein Anwender wird Sicherheitsrichtlinien, die länger als zehn Seiten sind, nicht lesen. Daher sollte für jeden der oben angesprochenen Aspekte eine eigene kurze Richtlinie verfasst werden, die der Anwender bei Bedarf gezielt lesen kann. Eine Benutzerordnung, die versucht, alle Punkte in einem Dokument zu erschlagen, wird wahrscheinlich ein Misserfolg sein, da keiner außer vielleicht der Verfasser selbst sie liest.

Einige der Sicherheitsrichtlinien werden für die Administratoren geschrieben, um sie bei der Umsetzung von Sicherheitsstrukturen zu unterstützen. Hierbei wird der Verfasser nicht bereits die fertige Lösung einer Sicherheitsstruktur vor Augen haben, sondern möglichst allgemein die Richtlinie definieren. Insbesondere die Nennung von bestimmten Produkten und Herstellern, möglicherweise von exakten Technologien, sollte unterbleiben. Werden derartige Spezifikationen in einer Sicherheitsrichtlinie festgelegt, so erschwert dies eine spätere Migration auf eine bessere Lösung eines anderen Herstellers, da zunächst die Richtlinie neu geschrieben werden muss. Dies lässt sich durch eine allgemeine Formulierung vermeiden.

Die Entwicklung von Sicherheitsrichtlinien lässt sich am einfachsten an Beispielen nachvollziehen. Im Folgenden sollen zwei Beispiele vorgestellt werden: E-Mail und Acceptable Use.

5.3.1 E-Mail-Sicherheitsrichtlinie

E-Mail ist die häufigste Anwendung des Internets. E-Mail stellt auch eine der ältesten Anwendungen mit den meisten inhärenten Sicherheitslücken dar. Viele Viren und Würmer der letzten Jahre verwendeten das E-Mail-System für ihre Verbreitung.

- **Architektur.** Das Unternehmen ist verantwortlich für die Einrichtung und Wartung eines Systems für den sicheren und zuverlässigen Austausch von E-Mails in-

nerhalb des Unternehmens und mit anderen Personen und Firmen über das Internet.

- **Untersuchung der E-Mail.** Um die Sicherheit der Firma zu gewährleisten, werden alle E-Mails auf Viren, Würmer, Trojaner und SPAM untersucht. Möglicherweise infizierte E-Mails werden zur Gewährung der Sicherheit nicht zugestellt, sondern für eine spätere Analyse abgespeichert. Der Absender und der Empfänger erhalten eine Benachrichtigung.
- **Aufgaben des Benutzers.** Eine E-Mail darf lediglich dienstliche oder berufliche Zwecke verfolgen. Private E-Mails dürfen nicht versandt werden. Bei der Versendung von E-Mails sind diese digital zu signieren, um eine spätere Modifikation zu verhindern.
- **Inhalt.** Sensitive oder vertrauliche Informationen dürfen nur geeignet verschlüsselt über das Internet an bevollmächtigte Personen gesendet werden. Die E-Mail eines Anwenders wird mit dem Unternehmen identifiziert. Persönliche Meinungen und Stellungnahmen müssen daher als solche gekennzeichnet werden. Der Inhalt einer E-Mail sollte nicht 100 KByte überschreiten. Das Versenden von Microsoft Office-Dokumenten in ihrem nativen Format ist nicht erlaubt. Derartige Dokumente dürfen nur als PDF versandt werden.

5.3.2 Acceptable Use

Diese Richtlinie beschreibt den Zugriff und die Benutzung elektronischer Systeme, die Weitergabe elektronisch gespeicherter Informationen und die Nutzung elektronischer Kommunikationsdienste. Diese Richtlinie betrifft alle Anwender, die die Rechnersysteme der Firma nohup.info verwenden. Das schließt alle Angestellten und externen Berater ein. Als Kommunikationsdienst wird jede Form der elektronischen Kommunikation angesehen (einschließlich des lokalen Netzwerkes, des Internets und der Telekommunikation).

- **Verwendung der Kommunikationssysteme.** Sämtliche Systeme zur Informationsverwaltung und -übertragung dürfen lediglich für dienstliche/berufliche Zwecke genutzt werden. Private Nutzung ist nur im Notfall erlaubt.
- **Überwachung.** Sämtliche Daten, die über die Systeme transportiert werden, sind geistiges Eigentum des Unternehmens. Alle Mitteilungen werden als dienstlich eingestuft. Das Unternehmen hat das Recht, diese Mitteilungen zu überwachen, zu kopieren, zu speichern oder zu löschen.
- **Missbrauch.** Der Missbrauch der Systeme ist nicht erlaubt. Es dürfen keine Daten, die dem besonderen Datenschutz unterliegen, über diese Systeme ausgetauscht werden. Die Anwendung dieser Systeme zum Schaden des Unternehmens ist verboten. Illegale Aktivitäten dürfen nicht auf diesen Systemen ausgeführt werden. Angriffe oder Einbrüche gegen die Systeme des Unternehmens oder Systeme im Internet sind verboten.

- **Software-Installation.** Die Installation zusätzlicher Software durch den Anwender ist nicht erlaubt. Eine Installation darf nur durch die autorisierten Personen vorgenommen werden. Hierbei sind die Lizenzbestimmungen der Software zu prüfen und anzuwenden. Die Anfertigung einer Kopie von Software, die das Eigentum des Unternehmens darstellt, ist nicht erlaubt. Die Kopie lizenzierter Software ist nur nach spezieller Autorisierung erlaubt.
- **Virenschutz.** Anwender dürfen nicht bewusst Viren erzeugen oder in das Netzwerk einschleusen. Bevor Daten auf Unternehmenssysteme übertragen werden, sind die entsprechenden Daten (Dateien, Datenträger) auf Viren zu testen.

Dieses Beispiel orientiert sich sehr stark an Beispielen des anglo-amerikanischen Raumes. Im Kapitel 17, »Datenschutz-Aspekte in einem Unternehmensnetzwerk« werden Beispielregelungen für den deutschen Raum vorgestellt.

