



# 19 Lessons Learned

Ein wichtiges Sprichwort sagt: *Nur aus Fehlern lernt man!* Hierzu ist es jedoch erforderlich, die Fehler zu erkennen, zu verstehen und in Zukunft zu vermeiden. Ein Unternehmen, welches nach einem behobenen Einbruch einfach zur Tagesordnung zurückkehrt, wird dem nächsten Angriff genauso schutzlos gegenüberstehen wie dem letzten. Es ist erforderlich, den Einbruch zu analysieren und entsprechende Schlüsse aus der Analyse zu ziehen und die Präventionsmaßnahmen anzupassen oder neu zu entwickeln.

## 19.1 Anpassen der Maßnahmen

Nachdem ein Einbruch vollständig analysiert und bearbeitet wurde, gehen viele Notfallteams wieder zum Tagesgeschäft über. Der Einbruch wurde erfolgreich analysiert und behandelt. Hiermit ist der Vorgang abgeschlossen. Ein derartiges Vorgehen lässt jedoch einen wichtigen und sehr wertvollen letzten Schritt außer Acht: das so genannte Follow-Up.

In der Follow-Up-Phase werden der gesamte Einbruch und alle eingeleiteten Maßnahmen, die Tätigkeiten der beteiligten Personen und der Zeitplan erneut betrachtet und evaluiert. Zusätzlich sollten die allgemeinen Sicherheitsrichtlinien wie auch die eigentliche Implementierung dieser Sicherheitsrichtlinien in Form von Firewalls, IDS, Virens Scanner etc. evaluiert und bewertet werden. Diese Evaluation soll bei zukünftigen Angriffen und Einbrüchen einer besseren Vorbereitung dienen.

Sie soll auch in einer Runde aller an der Bekämpfung des Einbruchs beteiligter Personen und der Verantwortlichen erfolgen. Hierbei ist es wichtig, dass tatsächlich eine Diskussion geführt wird. Schuldzuweisungen sind vielleicht erforderlich, sie sollten aber auf das notwendige Mindestmaß reduziert werden. Diese Gruppe sollte sich selbst als ein Team verstehen, welches die Zusammenarbeit fördern und nicht gegeneinander arbeiten soll.

Am einfachsten ist die Bewertung der Sicherheitssysteme. Diese kann wertfrei erfolgen, ohne andere Personen in der Runde bloßzustellen. Wenn sich das Team in diesem Zusammenhang warmgearbeitet hat, kann zu weiteren Themen übergegangen werden.

In Bezug auf die Sicherheitssysteme sind die folgenden Fragen aufzuwerfen und zu beantworten:

- Welche Systeme wurden erfolgreich bei der Bekämpfung des Einbrechers eingesetzt?
  - Sind Verbesserungen dieser Systeme möglich?
- Welche Systeme haben versagt?
  - Warum haben diese Systeme versagt?
  - Besteht die Möglichkeit, diese Systeme so einzusetzen, dass sie beim nächsten Mal nicht versagen?
  - Besteht die Möglichkeit, diese Systeme durch bessere Systeme zu ersetzen?
- Haben die Systeme schnell genug reagiert?
- Besteht die Möglichkeit, für eine schnellere und gezieltere Antwort die Systeme besser zu konfigurieren?
- Besteht die Möglichkeit, den Angriff in Zukunft durch eine automatische Antwort zu bekämpfen?
- Existieren ähnliche Probleme auf anderen Systemen im Unternehmen?

Diese Fragen sind zum Beispiel im Zusammenhang mit der Konfiguration der Firewall zu betrachten. Wie gelangte der Einbrecher in das interne Netzwerk? Wie konnte er die Sicherheitslücke ausnutzen?

Anschließend sollten der Notfallplan und die Sicherheitsrichtlinien überprüft und evaluiert werden. Diese Evaluation soll möglicherweise vorhandene Lücken aufdecken und Anpassungen der Dokumente vorschlagen.

- Sahen die Sicherheitsrichtlinien den speziellen Fall des Einbruchs vor?
- Enthielt der Notfallplan Maßnahmen, um auf die Form des Angriffs zu reagieren?
- Wurde bei der Behandlung des Einbruchs konform mit den Sicherheitsrichtlinien und dem Notfallplan vorgegangen? Wenn das nicht so war, warum nicht?
- Müssen die Sicherheitsrichtlinien modifiziert werden oder genügt eine modifizierte Implementierung dieser Richtlinien?
- Muss der Notfallplan modifiziert werden, da sich eine andere Vorgehensweise in der Praxis bewährt hat?

Der letzte Punkt in der Evaluation sollte die Arbeit im Team und die Zusammenarbeit mit weiteren, auch externen Gruppen sein. Hier ist es besonders wichtig, Koordinationschwierigkeiten, Kooperationsprobleme und fehlende Fähigkeiten zu benennen, damit diese vor dem nächsten zu behandelnden Einbruch besprochen und beseitigt werden können. Hierbei ist auch gesunde Selbstkritik durchaus erwünscht. Alle beteiligten Personen sollten darüber hinaus in der Lage sein, eigene Fehler einzugestehen und konstruktive Kritik positiv aufzunehmen.

- War die Koordination des Teams durch den »Leiter« erfolgreich?
- Traten Kommunikationsprobleme innerhalb des Teams auf? Wurden alle Mitglieder gleichermaßen entsprechend den Randbedingungen (Sicherheitsrichtlinien) informiert? Wusste die rechte Hand, was die linke gerade tat?
- Funktionierte die Teamarbeit oder baute sich ein Konkurrenzdenken innerhalb des Teams auf?
- War jede Person im Team in der Lage, die Aufgaben, mit denen sie betraut wurde, zu erfüllen?
- Benötigte die Behandlung des Einbruchs Fähigkeiten oder Wissen, welches nicht im Team vorhanden war? Muss vorhandenes Wissen vertieft werden?
- Konnte fehlendes Wissen durch die Einbeziehung externer Gruppen hinzugewonnen werden?
- War die Kooperation mit externen Gruppen erfolgreich?
- Kann die Zusammenarbeit mit externen Gruppen verbessert werden?
- Sehen die Sicherheitsrichtlinien eine Zusammenarbeit mit externen Gruppen vor? Sind spezielle Schritte im Vorfeld nötig (Non-Disclosure Agreement)?

Die angeführten Beispielfragen sollen einen Eindruck vermitteln, wie ein derartiger Follow-Up erfolgen kann. Wenn dieser Follow-Up in einem Team durchgeführt wird, so bindet er es meist zusätzlich und die Zusammenarbeit profitiert davon.

Ergebnis eines derartigen Follow-Ups ist häufig, dass die bisherigen Maßnahmen nicht genügen. Wenn sie genügen würden, hätte wahrscheinlich auch kein Einbruch stattgefunden. Nicht in allen Fällen können die notwendigen Maßnahmen jedoch umgesetzt werden, da möglicherweise personelle oder finanzielle Beschränkungen dies unmöglich machen.

Eine wichtige Erkenntnis eines Follow-Ups sind jedoch fehlende Fähigkeiten oder fehlendes Wissen. Hier bestehen zwei verschiedene Möglichkeiten, dieses Wissen beim nächsten möglichen Einbruch zu garantieren. Entweder das Wissen bzw. die Fähigkeit wird von außen eingekauft (Out-Sourcing) oder ein oder mehrere Mitglieder des Teams eignen sich diese Fähigkeit selbst an. Hierzu existieren mehrere Möglichkeiten der Weiterbildung.

## 19.2 Weiterbildung

Für eine erfolgreiche Behandlung von Einbrüchen und Angriffen ist es erforderlich, dass die Fähigkeiten der Mitglieder des Notfallteams immer auf dem neuesten Stand sind. Eine Weiterbildung sollte daher ununterbrochen erfolgen. Dies ist auf drei unterschiedlichen Wegen möglich:

- **Selbststudium.** Ein Selbststudium ist möglich. Es stehen eine ganze Reihe von Büchern und Informationen im Internet zur Verfügung, die das Thema Intrusion Detection und digitale Forensik behandeln. Diese Informationen behandeln in

erster Linie die Analyse von Netzwerkangriffen, jedoch wird auch die forensische Analyse einzelner Rechner betrachtet. Sicherlich eine der wichtigsten Ressourcen ist das Honeynet Project (<http://project.honeynet.org>), welches in regelmäßigen Abständen einen Scan of the Month Challenge durchführt. Hier besteht die Möglichkeit, die eigenen Kenntnisse zu testen und auf bisher nicht veröffentlichte Daten anzuwenden. Wenn die eigenen Ergebnisse eingereicht werden, werden diese anschließend auch bewertet.

Im Weiteren existieren eine Vielzahl von Mailinglisten, die sich mit dem Thema oder verwandten Themen beschäftigen. Hierbei ist es sicherlich sinnvoll, eine gewisse Auswahl dieser Mailinglisten zu abonnieren.

Ein Selbststudium ist immer mit einem sehr hohen Zeitaufwand verbunden. Es verlangt sehr viel Disziplin bei der Suche nach den entsprechenden Informationen. Bücher wollen gelesen und nachvollzogen werden. Deren Inhalt (dieses Buch eingeschlossen) wird irgendwann veraltet sein. Weitere Informationen stehen an unterschiedlichsten Stellen im Internet zur Verfügung und wollen gefunden werden.

- **Kurse.** Kurse können den hohen Zeitaufwand, der für ein Selbststudium erforderlich ist, reduzieren. Spezialkurse können diese Themen besonders aufbereitet behandeln. Der Dozent ist hierbei in der Lage, die Themen aus unterschiedlichen Sichtweisen darzustellen und auch Fragen zu beantworten. Wenn ein Buch Fragen offen lässt, so ist der Leser häufig auf sich selbst gestellt. (Ich bin jedoch gerne bereit, Anregungen entgegenzunehmen und Fragen zu beantworten, solange es das Volumen zulässt.) Ein Kurs-Dozent kann ebenfalls auf die Teilnehmer eingehen und Einzelfragen beantworten.

Kurse bieten aber noch einen weiteren Vorteil. Der Teilnehmer ist in der Lage, sich für einige Tage (für die Kursdauer) nur mit diesem Thema zu beschäftigen. Wenn die Weiterbildung parallel zur üblichen Arbeit erfolgt, besteht meist nicht die Möglichkeit, sich derartig konzentriert ohne weitere Ablenkung mit dem Thema zu beschäftigen. Daher sind solche Kurse, vorausgesetzt der Inhalt entspricht den Ansprüchen, meist ihr Geld wert.

- **Konferenzen.** Schließlich bietet sich noch die Möglichkeit, Konferenzen zu besuchen, die sich mit diesem Thema beschäftigen. Hierbei kommen sowohl allgemeine Computer- und Netzwerkkonferenzen in Frage, bei denen sich in den letzten Jahren immer einige Vorträge mit der Rechnersicherheit beschäftigen, als auch spezielle Konferenzen, die sich mit der Sicherheit beschäftigen.

Allgemeine Linux-Konferenzen in Deutschland, die jährlich stattfinden, sind der Linuxtag (<http://www.linuxtag.org>), der Internationale Linux-Kongress (<http://www.linux-kongress.org>), die LinuxWorld in Frankfurt am Main (<http://www.linuxworldexpo.de>) und das Frühjahrsfachgespräch der German Unix Users Group (GUUG, <http://www.guug.de>).

Konferenzen, die sich mit der Rechnersicherheit beschäftigen, sind in Deutschland leider dünn gesät. Der bekannteste und größte Event ist sicherlich der Chaos

Computer Club Congress, der üblicherweise zwischen Weihnachten und Silvester in Berlin stattfindet (<https://www.ccc.de>).

Das DFN-CERT führt einmal jährlich einen Workshop »Sicherheit in vernetzten Systemen« durch (<http://www.dfn-cert.de/events>). Weitere Termine werden auf der Webseite <http://www.veranstaltungen-it-sicherheit.de/> vorgehalten.

Nun bleiben die internationalen Konferenzen, die in ihrem Rahmen meist ein sehr ausführliches Tutorial-Programm anbieten. Diese Tutorien dauern üblicherweise einen oder wenige Tage. Hier besteht die Möglichkeit, einen Kurs während der Konferenz zu besuchen. Jedoch sind diese Tutorien mit sehr vielen Teilnehmern besetzt (50-500). Persönliche Fragen an den Dozenten sind meist nicht möglich.

Allgemeine Linux/UNIX-Konferenzen werden jährlich mehrfach von der USE-NIX (<http://www.usenix.org>) abgehalten. Diese Konferenzen finden meist in den USA statt.

Spezielle Konferenzen zum Thema Rechnersicherheit werden von verschiedenen Instituten organisiert. Sehr bekannt ist die DefCon-Konferenz, die jeden Juli in Las Vegas stattfindet. Hierbei handelt es sich um das nordamerikanische Pendant zum CCC-Congress (<http://www.defcon.org>). Der Organisator der DefCon, Jeff Moss, organisiert seit einigen Jahren in derselben Woche in Las Vegas eine weitere Konferenz: Blackhat Briefings. Diese Konferenz zielt weniger auf den (jugendlichen) Hacker, sondern mehr auf Unternehmen, die die neuesten Informationen über Sicherheitslücken erfahren wollen und die entsprechenden Personen kennen lernen möchten (<http://www.blackhat.com>). Diese Konferenzen werden inzwischen mehrmals jährlich angeboten. Seit zwei Jahren wird eine jährliche Konferenz auch in Amsterdam durchgeführt.

Das SANS Institute (System Administration and Network Security) bietet ebenfalls mehrfach jährlich Konferenzen, die in erster Linie Schulungen und Tutorials bieten. Das SANS Institute hat auf der Basis dieser Schulungen auch ein Zertifizierungsprogramm (GIAC) entwickelt (<http://www.sans.org>). SANS bietet seit 2002 erstmals auch internationales Training in Europa und seit 2001 Online-Training.

Eine rein europäische Veranstaltung ist die SANE (System Administration and Networking), die alle zwei Jahre von der niederländischen Unix Users Group ausgerichtet wird (<http://www.nluug.nl>). Sie fand im Mai 2004 statt und wird alle zwei Jahre stattfinden.

International ausgerichtet ist auch die Konferenz des FIRST (Forum of Incident Response and Security Teams, <http://www.first.org>). Diese Konferenz findet jährlich statt. Weitere Informationen finden sich auf der Webpage von FIRST.

Dies zeigt, dass es reichlich Konferenzen gibt, die das Thema besetzen. Die aufgezählten Veranstaltungen stellen lediglich eine Auswahl dar. Es existieren sicherlich weitere Veranstaltungen oder werden in der nächsten Zukunft geschaffen. Diese Aufzählung soll lediglich als Orientierungshilfe dienen.

