Datenschutzfreundliche Protokollierung

Diskrete Logs

Protokollierung von Netzwerkdaten ist einerseits zur Fehlersuche unabdingbar, andererseits besteht die Gefahr, dass sie zum gläsernen Mitarbeiter führt. Der Widerspruch scheint unvereinbar, doch mit wenig Aufwand ist ein Ausweg realisierbar. Rainer W. Gerling und Thomas Blaß

Die gängige Vorstellung vieler ITler ist, dass der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte ständig im Clinch liegen. Der Datenschutzbeauftragte will möglichst keine Protokollierung und der IT-Sicherheitsbeauftragte will die totale Überwachung und Kontrolle.

Datenschutz und IT-Sicherheit

Das Bundesdatenschutzgesetz gibt jedoch in § 3a vor: „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogen Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen." Das beschreibt die Zielvorstellungen des Datenschutzes perfekt. Denn eine Datenverarbeitungsanlage, in der keine personenbezogenen Daten gespeichert sind, kann das Grundrecht auf „informationelle Selbstbestimmung" nicht verletzen.

Zudem ist klar, dass das Missbrauchsrisiko einer Datensammlung umso geringer ist, desto weniger personenbezogene Daten in dem System vorhanden sind. Daraus folgt, dass man für einen vorgegebenen Zweck nur die Daten erheben sollte, die zur Zweckerfüllung erforderlich sind. Eine Speicherung von Daten, die derzeit nicht benötigt werden, für den Fall, dass sie später einmal zu gebrauchen wären (Vorratsdatenspeicherung), ist nicht zu lässig.

Der IT-Sicherheitsbeauftragte muss die Sicherheit der im Unternehmen eingesetzten Datenverarbeitungsanlagen verbessern. Dazu gehört nach allgemeiner Meinung auch die Aufklärung eventueller Missbrauchsfälle. Hierzu werden Kommunikationsvorgänge protokolliert und geloggt, insbesondere wird auf Servern, Firewalls, IDS-Systemen und vielen weiteren Netzwerkkomponenten das Nutzungsverhalten der Benutzer in Protokolldateien gespeichert. In der Praxis lassen sich bei manchen Verantwortlichen allerdings immer wieder eigenartige Vorstellungen über Art und Umfang ihrer rechtlichen Verpflichtungen zur Speicherung und Aufbewahrung dieser Log-Dateien feststellen. So sind manche Verantwortliche beispielsweise der irrigen Meinung, sie müssten alle Daten bevorraten, die von einer Strafverfolgungsbehörde in der Zukunft irgendwann einmal angefordert werden könnten, weil sie sich sonst strafbar machen würden.

Das Dilemma lässt sich leicht auflösen: In einem Unternehmen dürfen alle die Daten gespeichert werden, die zur Aufrechterhaltung der IT-Sicherheit und zur Fehlersuche nötig sind. Bei der Auslegung des Begriffs „erforderlich" sind strenge Maßstäbe anzulegen. Auf keinen Fall ist es zulässig, Daten zu speichern, die man eventuell irgendwann einmal benötigt.

Für die Fehlersuche auf einem Mail-Server reicht zum Beispiel eine Speicherdauer von wenigen Tagen. Kein Nutzer geht nach einigen Monaten zum Administrator des Mail-Servers und beschwert sich, dass eine E-Mail nicht angekommen ist.

Details zu den Meldungen pro IP:

System: 193.
Meldungstyp: Bot
Zeitstempel: 2010-01-27 17:33:28 GMT+0100 (Winterzeit)
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu werden, die versucht, einen HTTP- oder IRC-basierten Bot-Netz Control-Server zu erreichen. Zu den unterschiedlichen Malwaretypen finden Sie unter der folgender Webseite mehr Informationen:
http://www.cert.dfn.de/index.php?id=bot

TCP Quellport	Malwaretyp	Zeitstempel(GMT+0000)
48988	Torpig	2010-01-27 16:33:28
46352	Torpig	2010-01-27 15:33:51

Abbildung 1: Eine typische Information einer automatisierten Warnmeldung. Wenn die IP-Adresse zu einem NAT-Gateway gehört können die beiden Quellports zu verschiedenen internen Rechnern gehören.

Automatische Warnungen

Für seinen Warn-Dienst wertet das DFN-CERT (Verein zur Förderung eines Deut-

schen Forschungsnetzes – DFN) eine Anzahl von öffentlichen und nicht-öffentlichen Quellen aus, um Probleme zu entdecken, die einen Bezug zu Rechnersystemen in den Netzen der Mitglieder des DFN haben. Außerdem betreibt es eigene Sensoren wie etwa Honey Pots, um die Informationsbasis weiter auszudehnen. Das DFN-CERT sammelt, korreliert und normiert diese Daten und stellt jedem DFN-Anwender den Zugriff auf die Daten seiner Einrichtung zur Verfügung. Dies umfasst die Möglichkeit zur Konfiguration einrichtungsspezifischer Einstellungen.

Viele Nutzer betreiben ihr internes Netz hinter einem NAT-Gateway, um die interne Netzstruktur zu verbergen oder auch weil nicht ausreichend offizielle IP-Adressen zur Verfügung stehen. In den Warnmeldungen findet sich dann nur die IP-Adresse des NAT-Gateways. Und damit kommt man bei der Suche nach dem möglicherweise mit Schadsoftware befallen Rechner nicht weiter. Die Konsequenz beim IT-Sicherheitsbeauftragten ist dann unter Umständen, alle Verbindungen durch das NAT-Gateway zu protokollieren. Hier kommt dann sehr schnell der Betriebs- oder Personalrat mit ins Boot, da eine Verhaltenskontrolle der Beschäftigten mit technischen Mitteln gegeben sein kann (etwa § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz oder § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz in Verbindung mit der ständigen Rechtsprechung des Bundesarbeitsgerichts). Über die Auswertung der protokollierten Verbindungen wäre schließlich die komplette Internetnutzung der Belegschaft nachzuvollziehen. Die Brisanz der Protokolle liegt auf der Hand.

Ein datenschutzfreundlicher Ansatz

Cisco führte 2005 die 5500 Serie der Adaptive Security Appliances, kurz ASA, ein. Mit den vier Zeilen aus Listing 1 lässt sich eine Protokollierung aktivieren, die nur noch die interne IP-Adresse des Rechners, die NAT-IP und den NAT-Port der Verbindung der ASA protokolliert. Da in den Warnmeldungen des DFN der Quellport der Verbindungen angegeben wird, lässt sich mit dieser Information der interne Rechner identifizieren. In Listing 2 sind die Protokoll-Einträge zu sehen, die zur Warnmeldung aus Abbildung 1 gehören. Der datenschutzrechtliche (und beschäftigtenfreundliche) Vorteil dieses Verfahrens ist, dass der Inhalt der Protokoll-Datei völlig wertlos ist, solange es keine Beschwerden von Externen gibt. Es kann lediglich ausgewertet werden, wie viele Verbindungen ein Rechner aufgebaut hat. Da die Ziel-IP und der Zielport fehlen, sind keine weiteren Auswertungen möglich.

Listing 1 zeigt die Konfiguration einer Cisco ASA um das beschriebene Protokoll zu generieren. In der zweiten Zeile wird die Nummer der Loginformation angegeben, die zusätzlich protokolliert werden soll. In der letzten Zeile wird das Logging auf einen Syslog-Server (193.aaa.bbb.ddd) konfiguriert. Hier wird zusätzlich das Protokoll (17 = UDP) und der Zielport (1514) angegeben.

Die Zuordnung der Einträge aus dem NAT-Gateway (Linsting 2, ASA mit Version 8.2) zur Warnmeldung aus Abbildung 1 erfolgt über die Quellports. Über den Quellport wird dann die interne IP aufgedeckt. Die Uhrzeit in diesem Log ist in Mitteleuropäischer Zeit (GMT + 0100) angegeben.

Eine Mitarbeitervertretung tut sich leicht, einem solchen Protokoll zuzustimmen, da letztendlich keine Überwachung der Beschäftigten möglich ist. Erst eine Beschwerde oder Warnmeldung liefert die Zusatzinformation, die erforderlich ist um eine konkrete Verbindung aufzudecken. Und in diesen Fällen ist es dann auch zwingend erforderlich den Vorfall zu verfolgen.

Manchmal kommt eine Beschwerde, die keine Quellports beinhaltet. Ein Apache Web-Server protokolliert zum Beispiel typischerweise nur die Quell-IPs und nicht die Quellports. Da aber das Protokoll eines solchen Abrufs in der Regel mehrere Verbindungen beinhaltet, kann über die zeitlichen Abstände der Verbindungen zueinander in den meisten Fällen der interne Rechner identifiziert werden. Die zeitlichen Abstände der Verbindungen eines Abrufs sind dafür individuell genug, so dass sie eindeutig gefunden werden können. Dieses Verfahren hat sogar noch den Vorteil, dass es keine wirklich synchronisierten Uhren auf beiden Seiten benötigt. Ein eventueller Offset der Uhren der beteiligten Rechner fällt beim Bilden der Zeitdifferenzen heraus.

Fazit

IT-Sicherheit und Datenschutz sind bei sachgerechter Anwendung der Protokollierung (unter Maßgabe der Erforderlichkeit, das heißt die Daten sind tatsächlich nötig) kein Widerspruch. Mit ein bisschen Kreativität lassen sich sehr datenschutzfreundliche Lösungen finden. Diese Lösungen schützen die Beschäftigten vor permanenter Überwachung und stellen gleichzeitig den IT-Sicherheitsbeauftragten zufrieden, da er Sicherheitsvorfälle aufklären kann. Datenschutz und IT-Sicherheit müssen kein Widerspruch sein. (*jcb*) ■

Die Autoren

Prof. Rainer W. Gerling ist seit 1993 Datenschutzbeauftragter und seit 2006 auch IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft in München und seit 2003 Honorarprofessor für das Fachgebiet „IT-Sicherheit" im Fachbereich Informatik an der Hochschule München. Er ist Mitglied des Herausgeberbeirats der Zeitschrift „Datenschutz und Datensicherheit" und veröffentlichte zahlreiche Beiträge in verschiedenen Fachzeitschriften und Büchern, darunter als Koautor das Buch „Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht". Außerdem ist er Mitglied des Präsidiums der GDD-Datenschutz-Akademie sowie seit Anfang 2008 des Ausschusses für Recht und Sicherheit des DFN-Vereins.

Thomas Blaß ist Gruppenleiter IT-Sicherheit in der Generalverwaltung der Max-Planck-Institute. Seit fünf Jahren betreut sein Team die VPN- und Firewall-Infrastruktur in rund 80 Standorten und entwickelt sie stetig weiter.

Listing 1: Protokollierung auf einer Cisco ASA

```
01 logging list DefaultFilter level warnings
02 logging list DefaultFilter message 305011
03 logging trap DefaultFilter
04 logging host extern 193.aaa.bbb.ddd 17/1514
```

Listing 2: Logeinträge des NAT-Gateway

```
01 Jan 27 16:33:47 193.aaa.bbb.cc %ASA-6-305011: Built
   dynamic TCP translation from
02 intern:10.90.x.14/2551 to extern:193.aaa.bbb.cc/46352
03 Jan 27 17:33:25 193.aaa.bbb.cc %ASA-6-305011: Built
   dynamic TCP translation from
04 intern:10.90.x.2/3427 to extern:193.aaa.bbb.cc/48988
```