

Alarmanlagen im Netz - Interview mit Thomas Biege

[Jana Jaeger](#)

Wie können sensible Daten, seien es wichtige Geschäftsdaten oder Forschungsergebnisse, oder ..., vor fremden Augen geschützt werden und wie kommt man dem ungebetenen "Besucher" auf die Spur? Wer hat wann versucht, ins eigene Netz vorzudringen? Auch für Computernetze gibt es Alarmanlagen, die Intrusion Detection Systeme, oder kurz IDS. Thomas Biege, Mitglied des SuSE Security Teams, erklärt in einem Zweiteiler, der nächste Woche auf dem Portal erscheinen wird, wie ein solches System aufgebaut ist, welche Verfahrensweisen zum Aufspüren von "Netz-Einbrechern" benutzt werden und wann und wie es Sinn macht, ein IDS einzusetzen.

Vorab beantwortete er uns noch einige allgemeine Fragen zum Thema Netzwerksicherheit und Intrusion Detection Systeme.

Web Portal : Wie kommst Du zu den Security-Themen? Was reizt Dich so dran?

Thomas Biege : Allgemein oder im Speziellen bei SuSE? Also allgemein: Ich habe das Buch "Das Kuckucksei" von Clifford Stoll gelesen, danach war ich Feuer und Flamme für Unix, Internet, Programmieren in C und natürlich Sicherheit. Danach habe ich mir alles selbst durch Bücher und Rumprobieren angeeignet.

Im Speziellen: Ich habe eine paar Sicherheitslöcher in Linux (spez. SuSE) Software auf Bugtraq veröffentlicht oder nur zu SuSE geschickt. Irgendwann kam dann eine E-Mail von Burchard (Anmerkung d. R.: Burchard Steinbild ist einer der vier Gründer der SuSE GmbH). :-)

Was mich reizt? Hm... ich finde das Ganze irgendwie spannend, zudem lernt man viel über die Interna von Unix/Linux oder allgemein von Software. Das Thema IT-Sicherheit umfaßt so ein weites Spektrum an Wissensgebieten, daß einem nie langweilig wird. Ausserdem ist man gezwungen, immer auf dem Laufenden zu bleiben.

Web Portal : Ein paar kurze Sätze zum Thema Netzwerksicherheit... wann könnte man ein Netzwerk als sicher bezeichnen, wenn überhaupt?

Thomas Biege : Also ich kann hier nur oft Gesagtes wiederholen: :) 100%ige Sicherheit gibt es nie. Es ist immer eine Aufwands-/Nutzen- bzw. Wertabschätzung, d.h. die Kosten für einen erfolgreichen Einbruch müssen immer über dem Nutzen liegen, den ein Angreifer davon hätte.

Grundsätzlich sollte man aber die bekannten Lücken seiner Systeme schließen und sicherheitsrelevante Informationsquellen, wie die Maillingliste suse-security@suse.com oder suse-security-announce@suse.com ständig überwachen, um auf dem Laufenden zu sein. In der Regel sollte es kein Problem sein, einen Paketfilter einzusetzen. Auch für Heimanwender gibt es bereits sog. Personal Firewalls, wie beispielsweise auf SuSE 7.2, die einfach aktiviert werden können, und dem Benutzer ein recht hohes Maß an Schutz bieten.

Firmen haben natürlich das Geld, um sich Wissen und Material zu kaufen, um ihre Netze abzusichern. Sie sollten das Geld entsprechend ihrer Kapazitäten auch dafür ausgeben. Nicht jeder muss eine halbe Million DM oder mehr in ein mehrstufiges HA-Sicherheitssystem mit 24h/7d Überwachung stecken. Wie gesagt, es ist immer eine Aufwand-Nutzen Abschätzung.

Web Portal : Sicherheit ist relativ - Paranoia auch :-) Wo liegt die Grenze zwischen beiden? Geht das fließend ineinander über?

Thomas Biege : Ich denke, daß im professionellen Bereich Paranoia nicht angebracht ist. Wie oben gesagt, die Werteverhältnisse müssen stimmen. :)

Web Portal : Für wen macht ein IDS Sinn, für wen nicht?

Thomas Biege : Ein IDS macht Sinn, wenn man weiß, was es kann (man also dessen Stärken und Schwächen kennt), und wenn man die Alarmmeldungen eines IDS versteht und einschätzen kann.

Für den Heimbenutzer macht ein IDS in der Regel keinen Sinn, da es zu komplex ist (relativ) und nur verunsichern würde.

Web Portal : Was sollte der normale Heimanwender zum Thema IDS wissen - wenn er überhaupt was wissen muß?

Thomas Biege : Ich denke, daß der normale Heimanwender ein IDS nicht benötigt. Für interessierte Benutzer bieten sich Snort oder andere frei erhältliche ID Systeme an.

Web Portal : Um ein IDS aufzubauen und zu warten, muß man viel Netzwerk- und Security-Knowhow haben. Wie ist das im täglichen Leben: Muß jeder Systemadministrator, der ein derart geschütztes Netz hat, die einzelnen Details bis ins Letzte verinnerlicht haben?

Thomas Biege : Nein, das ist nicht nötig. Beispielsweise basieren die Analyseeinheiten von ID Systemen im allgemeinen auf Konstrukten der Künstlichen Intelligenz (KI). Man kann nicht erwarten, daß ein Admin, der eh schon genug zu tun hat, sich mit Neuronalen Netzwerken oder Experten Systemen im Detail auseinandersetzt.

Der Hersteller eines IDS sollte dem Endbenutzer die geeigneten Hilfen zur Seite stellen, damit er im Alltag das IDS schnell und effektiv verwalten kann, ohne viel über die Interna zu wissen. Der Admin eines IDS sollte aber, wie gesagt, die Ergebnisse der IDS Analyse verstehen und bewerten können. Um dies zu erleichtern, sollte der IDS Hersteller eine umfangreiche Online-Hilfe in sein Produkt integriert haben. Kommerzielle ID Systeme verfügen in der Regel immer über eine grafische Benutzeroberfläche und ausreichend Dokumentation, um das tägliche Arbeiten mit dem IDS-System zu erleichtern.

Web Portal : Vielen Dank für das Interview.

Thomas Biege arbeitet seit zwei Jahren im SuSE Security Team mit, studiert Allgemeine Informatik an der FH Dortmund und ist zur Zeit mit seiner Diplomarbeit - der Entwicklung eines hostbasierten Intrusion Detection Systems - beschäftigt. 