Aus dem Nähkästchen geplaudert: Wichtige Mailinglisten

Keine Wissenslücke

Wissen ist Macht, nichts wissen macht auch nichts? Auf einem vernetzen Computer ist das sträflich. Angreifer, egal ob Mensch oder Wurm, würden ihn mit Freude entern. Zu einer wirksamen Abwehrstrategie gehören tagesaktuelle Information. Gute Admins nutzen dazu mehrere Quellen. Marc André Selig

Wenn heute übers Internet eine Attacke auf einen Computer gelingt, sind fast immer Konfigurationsfehler oder bekannte Sicherheitslöcher im Spiel. Zero-Day-Exploits mit bislang nicht publizierten Lücken sind vergleichsweise selten. Das mag daran liegen, dass recht viel Geschick und Know-how zum Aufspüren und Ausbeuten eines neuen Problems gehören, wohingegen die breite Masse der Angriffe durch automatisierte Software oder wenig kompetente Nachahmer durchgeführt wird.

Gegen Konfigurationsfehler hilft saubere Arbeit eines gut ausgebildeten Admin. Gegen bekannte Sicherheitslücken helfen sorgfältige und zeitnahe Updates, siehe Kasten „Update-Strategien“. Ist noch kein Update verfügbar, bleibt das vorübergehende Deaktivieren des Dienstes als letzter Ausweg.

Wichtig ist, so schnell wie möglich zu reagieren. Unmittelbar nach einem Advisory gibt es eine kurze Phase der Ruhe vor dem Sturm der Angreifer und Mittäter. Jetzt ist Gelegenheit für überlegte Reaktionen – rasch, aber ohne Hast. Je früher der Admin von dem Problem erfährt, desto besser sind seine Chancen, ein Update rechtzeitig einzuspielen.

Ankündigungslisten

Seit langem tauschen Admins und Entwickler über Mailinglisten Informationen aus. Pflichtlektüre ist die Ankündigungsliste der eigenen Linux-Distribution. Praktisch jeder Distributor pflegt eine solche Liste, über die er sicherheitsrelevante Updates vorstellt. Die Tabelle am Anfang der „InSecurity News“ in jedem Linux-Magazin führt einige dieser Listen auf.

Leider halten die Hersteller ihre Meldung meist so lange zurück, bis sie ein eigenes Update fertig gestellt haben. Der Vorteil: Ab diesem Zeitpunkt können automatische Tools das Patch installieren. Zum Beispiel kommen nun das Red Hat Network, »apt-get update; apt-get upgrade« bei Debian oder das Yast-2-Online-Update von Suse zum Zuge. Wenn sich ein Distributor aber gewohnheitsmäßig ein oder zwei Wochen Zeit lässt, um ein Patch zu produzieren, reicht das für wichtige Systeme nicht aus.

Daher sollten umsichtige Administratoren zusätzlich die Ankündigungslisten ihrer kritischen Systemprogramme lesen. Als kritisch gelten vor allem die Serverdienste, etwa Sendmail [1], Postfix [2] oder Qmail [3], Apache [4], MySQL [5] oder OpenLDAP [6], natürlich darf auch SSH [7] nicht fehlen.

Quelle für viel Linux-Software waren BSD-Systeme. Selbst wenn die Programme sich unter Linux bereits häuslich eingerichtet haben, ist die Codebasis doch immer noch dieselbe. Sicherheitsprobleme unter OpenBSD [8], FreeBSD [9] oder NetBSD [10] können daher als Frühwarnzeichen auch für Linux-Systeme dienen.

Bugtraq

Eine der berühmtesten Security-Mailinglisten ist zweifellos Bugtraq [11]. Hier veröffentlichen Hacker, Cracker und Sicherheitsexperten neue Lücken oft früher als die bisher genannten spezifischen Listen, häufig einschließlich funktionierender Exploits.

Diese Liste ist jedoch aus zweierlei Gründen mit Vorsicht zu genießen: Erstens ist nicht aller Code, der hier veröffentlicht wird, harmlos. Manche Advisories enthielten statt eines Exploit ein Trojanisches Pferd oder ähnliches Ungeziefer. Zweitens handelt es sich nicht um eine reine Ankündigungsliste, sondern es kommt regelmäßig zu Diskussionen über die angesprochenen Probleme. Der

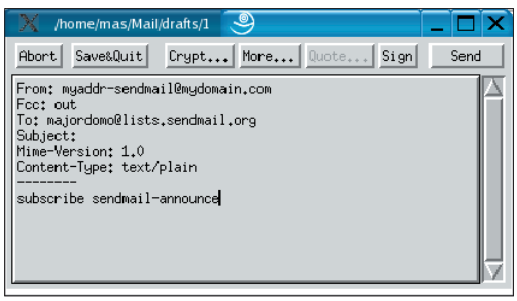

Abbildung 1: Wer beim Abonnieren einer Mailingliste ein Anhängsel hinter die eigene Adresse setzt, kann Listenmails später automatisch aussortieren: Qmail sendet »myaddr-*Liste@Domain*« an »myaddr*@Domain*« (bei Sendmail: »myaddr+*Liste@Domain*«).

Update-Strategien

Rechtzeitige Updates sind wichtig, aber nicht jedes Update ist unschädlich. Wer eine Sicherheitslücke schließt, dabei aber den Webserver seiner Firma abschießt, hat nicht viel gewonnen – die Mitarbeiter können nicht mehr arbeiten und Kunden nichts mehr bezahlen.

Für Updates kritischer Systeme empfiehlt sich ein zweistufiger Prozess. Der unverzichtbare Teil des Maschinenparks existiert doppelt in praktisch identischer Konfiguration. Eine Version erledigt den Wirkbetrieb, auf der anderen testet der Admin jede Konfigurationsänderung, bevor er sie auf den kritischen Systemen durchführt.

Beweis der Funktionstüchtigkeit

Nach einem Update muss die Testmaschine ihre Funktionsfähigkeit unter Beweis stellen. Um Zeit zu sparen, bieten sich automatische oder halbautomatische Regressionstests an, die wichtige Aufgaben rasch durchprüfen. Wichtig sind nicht nur der geänderte Dienst, sondern auch andere Teile, die mit ihm interagieren. So könnte ein Webserver seine erfolgreiche Anbindung zum Datenbanksystem oder zur Kreditkartenabrechnung demonstrieren.

Erst wenn dieser Test ohne Probleme oder Nebenwirkungen durchläuft, darf das Update auf die Produktionsmaschine. Viel Zeit sollte durch diesen Prozess nicht verloren gehen: Er dient als Rückversicherung, nicht als Spielwiese.

Procmail schafft Übersicht

Sicherheitsrelevante Mailinglisten haben ein wichtiges Problem: Der Leser muss die teilweise kritischen Informationen aus einem enormen Hintergrundrauschen herausfiltern, und zwar möglichst zeitnah. Spam- und Virusfilter sind eine erste Hürde: Meldungen über Sicherheitslücken enthalten oft Elemente typischer Spam-Mails, etwa Ausrufezeichen, ungewöhnliche Formatierung, unbekannte Absender, englische Texte, womöglich ausführbarer Code. Sicherheitslisten gehören daher auf die Whitelist des Spamfilters.

Zudem empfiehlt es sich, diese Listen in separate Folder zu sortieren. Das schafft Überblick. Folgendes kleines Procmail-Rezept mag als Beispiel dienen. Am Anfang einer »~/.procmailrc« eingesetzt speichert es Bugtraq-Mails im Folder »list/bugtraq«:

```
:0:
* ^List-Id:.*bugtraq\.list-id\
.securityfocus\.com
list/bugtraq
```

Traffic kann unangenehm hoch sein. Wer nicht hauptamtlich für Sicherheitsthemen zuständig ist, verschwendet eventuell unnötig Zeit beim Durchforsten dieser Liste nach relevanten Informationen.

In jedem Fall empfiehlt es sich, Bugtraq nur mit einem ausgefeilten Mailprogramm zu nutzen. Es sollte Bugtraq-Mails separieren, nach Betreffzeilen oder besser Threads sortieren und ein funktionsfähiges Killfile bieten, um uninteressante Themen rasch zu überspringen. Glücklicherweise gibt es unter Linux passende Software im Überfluss. Der Kasten „Procmail schafft Übersicht“ zeigt eine Procmail-Regel, die Listenmails in einem eigenen Folder unterbringt.

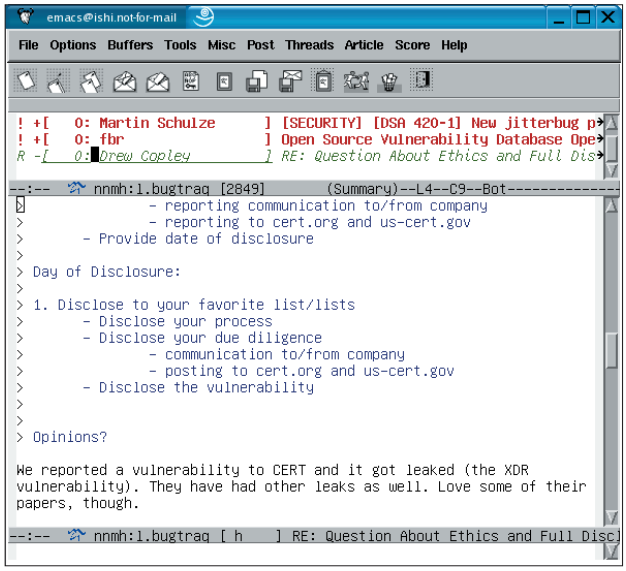

Abbildung 2: Der Newsreader Gnus eignet sich hervorragend auch für Mailinglisten mit hohem Nachrichtenaufkommen. Er bietet dem Anwender viele Bewertungs- und Filterfunktionen, unter anderem ein praktisches Killfile.

Unter dem Bugtraq-Dach [11] sind inzwischen viele interessante Listen beheimatet. Der Autor empfiehlt Security Events, Security Papers und Security Tools als nützliches Beiwerk.

CERT-Advisories

Traditionell gehören auch die Computer Emergency Response Teams (CERT) zum Pool wichtiger Informationsquellen rund um Computersicherheit. Beispielsweise gibt das US-CERT zwei technische Listen [12] heraus, die bei besonders kritischen Problemen eine Art Alarmruf darstellen. Wegen aufwändiger Qualitätssicherungsmaßnahmen erscheinen diese CERT-Mails aber meist erst sehr spät. Trotzdem eignen sie sich als Sicherheitsnetz und doppelter Boden: Wenn eine solche Mail eintrifft, ist es höchste Zeit für ein Patch.

Das DFN-Cert [13] übersetzt die Meldungen seiner Kollegen ins Deutsche. Ein Archiv der Linux- und Unix-relevanten Meldungen ist auf den Seiten der Linux-Community [14] zu finden. *(fjl)*

Infos

[1] Sendmail abonnieren: [mailto:majordomo@lists.sendmail.org] mit »subscribe sendmail-announce« im Text der Mail

[2] Postfix: »subscribe postfix-announce« an [mailto:majordomo@postfix.org] senden

[3] Bei Qmail genügt eine leere Mail: [mailto:qmailannounce-subscribe@list.cr.yp.to]

[4] Neuigkeiten zu Apache: [http://httpd.apache.org/lists.html#http-announce]

[5] Für MySQL siehe die Developer-Zone: [http://lists.mysql.com/announce/]

[6] OpenLDAP: Mail mit »subscribe« im Text an [mailto:OpenLDAP-announce-request@OpenLDAP.org] senden

[7] OpenSSH-Ports, zu denen auch die Linux-Version gehört: [http://www.mindrot.org/mailman/listinfo/openssh-unix-announce]

[8] OpenBSD: [http://lists.openbsd.org/cgi-bin/mj_wwwusr?func=lists-long-full&extra=security-announce]

[9] FreeBSD: [http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications]

[10] NetBSD: [http://www.netbsd.org/MailingLists/#netbsd-announce]

[11] Bugtraq: [http://www.securityfocus.com/subscribe?listname=1]

[12] Advisories des US-CERT: [http://www.us-cert.gov/cas/signup.html]

[13] DFN-Cert: [http://www.dfn-cert.de/infoserv/mls/win-sec-ssc.html]

[14] Advisories auf der Linux-Community: [http://www.linux-community.de/search?sectionid=22]