ERNW
Enno Rey Netzwerke GmbH

# ERNW Newsletter 1 / Mai 2003

ERNW Newsletter Mai 2003

Liebe Partner, liebe Kollegen,

das Team von ERNW freut sich, Sie mit der ersten Ausgabe unseres Newsletters zu begrüssen. Jeden Monat einmal wollen wir zukünfig über aktuelle Themen im Security-Bereich berichten. Darüber hinaus halten wir Sie über ERNW auf dem laufenden.

**Thema dieser Ausgabe: Host-Security am Beispiel sendmail**

In den vergangenen Wochen sind erneut zwei gravierende Sicherheitslücken von sendmail gefunden worden. Sie sind dokumentiert in den CERT Advisories CA-2003-07 und CA-2003-12. Bei beiden handelt es sich um Buffer Overflows, deren erfolgreiche Ausnutzung dazu führen kann, dass ein Angreifer beliebigen Programm-Code mit den Rechten des sendmail-Prozesses ausführt. Da sendmail auf nahezu allen UNIX-Systemen per default installiert ist
(mit Ausnahme von Nokia IPSO) und üblicherweise als root läuft, sind besonders viele Systeme betroffen.

Kurzfristig können beide Sicherheitslücken durch Installation einer neuen sendmail-Version (zur Zeit 8.12.9) behoben werden. Langfristig aber erweist sich pures Patchen oft als unzureichend: es stellt immer nur eine Reaktion auf bereits vorhandene Lücken und Angriffe dar und wird zudem im Alltagsgeschäft meist vernachlässigt. Durch die Anwendung einiger einfacher Regeln kann solchen Sicherheitslücken präventiv entgegengewirkt werden:

**1.) Minimalsystem**
Prüfen Sie, inwieweit Mail-Funktionalität überhaupt auf einzelnen Systemen erforderlich ist (etwa für Notifications).

**2.) Einsatz sicherer Komponenten**
Muss die Mail-Funktionalität zwingend durch sendmail realisiert werden oder kann auch ein sicherer MTA wie etwa postfix oder qmail zum Einsatz kommen?

**3.) Least Privilege**
Aufgrund seiner monolithischen Architektur benötigt sendmail weitestgehend root-Rechte, was dem Least Privilege-Ansatz zuwiderläuft: Prozesse sollten nur die für ihre Aufgaben minimal erforderlichen Rechte haben und diese auch nur zeitlich begrenzt.
Gute Host-Security orientiert sich immer an diesen Fragestellungen.
Angewandt auf sendmail erscheint seine Verwendung damit höchst fragwürdig und sollte dementsprechend vermieden werden. Wir unterstützen Sie gerne dabei.

Die Gefahren für den reibungslosen Betrieb der IT sind allerdings vielfältig. Sie reichen von Angriffen über Stromausfall bis zu Hochwasser im Serverraum (leider in 2002 sehr aktuell). An dieser Stelle möchten wir deshalb unseren neuen Service "Schwachstellen-Analyse zur IT Verfügbarkeit" vorstellen. Wir führen dabei eine Analyse des allgemeinen Zustands Ihres Rechenzentrums oder Serverraums durch und berücksichtigen hier Aspekte wie Klimatisierung, Verkabelung, Zugangskontrolle und Brandschutz.
Die Ergebnisse werden in einem Bericht dokumentiert, der auch Verbesserungsvorschläge enthält. Unsere Experten haben bereits vielfach an der Planung von Serverräumen oder Rechenzentren mitgewirkt und Notfallkonzepte erarbeitet.

Schwachstellen-Analyse zur IT-Verfügbarkeit, bestehend aus eintägiger Vor-Ort Prüfung, Erstellung eines Berichts mit Verbesserungsmassnahmen und Ergebnis-Workshop.
Gesamtpreis: 2290.- Euro zzgl. MwSt.
Ansprechpartner bei ERNW ist Enno Rey (erey@ernw.de).

Zum Abschluss berichten wir stolz, dass ERNW inzwischen auch lokaler Provider ist. Wir verfügen mittlerweile über eine voll-redundante Anbindung zu unterschiedlichen Carriern und bieten ab sofort für Firmenkunden Provider-Dienstleistungen mit Security-Mehrwert an. Mehr dazu im nächsten Newsletter.

Es grüssen Sie herzlich

Enno Rey & das Team von ERNW

--

ERNW Enno Rey Netzwerke GmbH - Zaehringerstr. 46 - 69115 Heidelberg
Tel. +49 6221 480390 - Fax 6221 419008 - Mobil +49 173 6745902
www.ernw.de - PGP E5CB 9505 EA06 6380 6F12  DE3E 624E 1334 326B B70C