

## HELPDESK

# Pathologie für den Computer

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

**Frage:** Wir vermuten einen erfolgreichen Einbruch in unserem Firmennetzwerk. Was ist bei einer forensischen Analyse zu beachten und was darf man von ihr erwarten?

Angriffe auf Computersysteme sind im Internet an der Tagesordnung. In nicht umfassend gesicherten Umgebungen sind derlei Bestrebungen zwielichtiger Natur ohne viel Aufwand mit Erfolg gekrönt. Sollte der unliebsame Fall eingetroffen sein, dass von einem erfolgreichen Einbruch auszugehen ist, müssen entsprechende Massnahmen ergriffen werden.

In erster Linie ist eine Schadensbegrenzung erforderlich, so dass weiterführende Attacken verhindert und die Sicherheit anderer Systeme gewährleistet werden kann. Dabei gilt es zu beachten, dass bestehende Spuren, die Rückschlüsse auf den Täter und seine Vorgehensweise liefern können, nicht versehentlich oder aus Bequemlichkeit verwischt werden. Die unverzügliche Neuinstallation eines kompromittierten Rechners kann beispielsweise eine weiterführende forensische Analyse enorm behindern oder gar verunmöglichen. Das Umsetzen eines Log-Konzepts und

eines Change-/Release-Managements ist in Bezug auf die Sicherheit einer Umgebung genauso wichtig wie klassische Methoden des Firewallings oder Patchings. Die geregelte Aufbewahrung von Log-Daten in einem gesicherten Umfeld erleichtert eine Analyse und lässt eine solche erst effizient ausfallen. Einem Analytiker sind nämlich die Hände gebunden, wenn er sich einem Zwischenfall an-

**«Die Analyse von Angriffen und Einbrüchen auf Computersysteme kann nur mit umfassenden Log-Dateien erfolgreich umgesetzt werden.»**

nehmen muss, der nicht oder nur unzureichend dokumentiert wurde – Diese Sysphus-Arbeit wird irgendwann unwirtschaftlich.

Nach der Initiierung der flankierenden Sofortmassnahmen, wie etwa mit der Bereitstellung eines neuen Systems, kann mit der eigentlichen Analyse begonnen werden. Dabei unabdingbar ist die Korrelation sämtlicher Informationen, die mit dem Zwischenfall zusammenhängen: Die während des Angriffs gegenwärtigen Komponenten, Software-Versionen und Ein-

stellungen sind dabei genauso wichtig wie umfassende und zeitlich aufeinander abgestimmte Log-Dateien. Sowohl System-Logs als auch die Protokolle von Firewall- und Intrusion Detection-Systeme stellen die Grundpfeiler der forensischen Analyse dar.

Forensische Analysen sind zeitaufwändig und können lediglich durch hochspezialisiertes Personal effizient umgesetzt werden, da sie ein Höchstmass an Verständnis für die eingesetzten Techniken und Lösungen erfordern. Vom Analysten wird ein flexibles Reagieren verlangt, um sich innert kürzester Zeit in für ihn vielleicht bis dato unbekannte Gebiete (z.B. Pufferüberlauf-Schwachstellen auf SPARC-Plattformen) einzuarbeiten.

Elektronische Einbruchserkennung muss jedoch nicht nur auf einer rein technischen Ebene betrieben werden. Das Umsetzen von psychologischen Profiling, wie es ursprünglich durch das FBI (Federal Bureau of Investigation) bei der Analyse von Serientätern genutzt wurde, können adäquate Massnahmen für Angreifer erarbeitet werden. Das Verständnis für den Angreifer, seine Hintergründe,

Methoden und Zielen ist unabdingbar, um angemessen darauf reagieren zu können.

Als Gegenwert dieser «Investition» winkt die umfassende Aufklärung von Angriffen und Einbrüchen. Sind die bei einem Angriff ausgenutzten Schlupflöcher erkannt, können sie gestopft und ein erneuter Missbrauch via sie verhindert werden. Ausserdem lassen sich so im Nachhinein die von Angreifern mit gleichartigen Skills ausgehenden Sicherheitsrisiken bestimmen und proaktiv können Gegenmassnahmen für das anzustrebende Sicherheitsniveau ergriffen werden. Schon so manche Firma hat aus einem erfolgreichen digitalen Einbruch gelernt – wer will schon den gleichen Fehler zweimal machen. ■

ILLUSTRATION: CW/THU



**Der Autor**  
Marc Ruef ist Buchautor und Security Consultant beim Sicherheitsunternehmen Scip AG, Zürich, [www.scip.ch](http://www.scip.ch)

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: [it-security@computerworld.ch](mailto:it-security@computerworld.ch)

**Ein Archiv der Helpdeskartikel finden Sie im Internet:** [www.computerworld.ch](http://www.computerworld.ch)