Behörden Spiegel
Unabhängige Zeitung für den Öffentlichen Dien
Sonderdruck
Nr. II / 30. Jahrgang Berlin und Bonn / Februar 2014 www.behoerdenspiegel.de

Mit Honig ködern

Honeypot-Prinzip sorgt für mehr IT-Sicherheit

(BS) Christian Scheucher, Geschäftsführer und Mitgründer der secXtreme GmbH, beschäftigt sich mittlerweile seit fast 15 Jahren ausschließlich mit IT-Sicherheit. Zu seinen Kernkompetenzen gehört es, Angriffe zu erkennen, darauf zu reagieren, sie aufzuklären und IT-Sicherheitstests durchzuführen, auch bei Auftraggebern aus den Bereichen Kritische Infrastrukturen und Behörden. Behörden Spiegel-Redakteur Guido Gehrt sprach mit ihm über den Einsatz des Honeypot-Prinzips als IT-Sicherheitslösung.

Behörden Spiegel: *Herr Scheucher, ist Schadsoftware im Behördenumfeld ein zentrales Problem?*

Scheucher: Ob im Industrie- oder Office-Bereich: die zunehmende interne Vernetzung der Datenkommunikation führt zu immer neuen IT-Sicherheitsrisiken. Sicherheitsrisiken wie Denial-of-Service-Angriffe, Daten- und Systemmanipulation oder Phishing können auch in Behörden großen Schaden anrichten. Doch es kommt noch schlimmer: Angriffe erfolgen zunehmend gezielter mit Methoden und Werkzeugen, die klassische IT-Sicherheit nicht mehr erkennen oder verhindern kann.

Christian Scheucher ist Geschäftsführer der Firma secXtreme GmbH.

Foto: BS/secXtreme GmbH

Behörden Spiegel: *Warum bieten klassische Lösungen keinen ausreichenden Schutz mehr?*

Scheucher: Patch-Management, Virenschutz, Firewalls und Intrusion Prevention Systeme (IPS) eignen sich bedingt. Ein grundsätzliches Problem ist, dass zusätzliches Know-how oder hoher Zeit- und Pflegeaufwand für die Lösungen für einen nachhaltigen Schutz vor Angriffen notwendig ist. Dieser Aufwand wird leicht unterschätzt und oft sind zu wenige Ressourcen dafür eingeplant. Zudem wird bei gezielten Angriffen Schadcode eingesetzt, der zum Beispiel vom Virenschutz lange Zeit nicht erkannt wird. Bestes Beispiel dazu war Stuxnet.

Behörden Spiegel: *Kann es passieren, dass klassische Lösungen Ausfälle verursachen oder den Datenverkehr stören?*

Scheucher: Ja, das kann leider der Fall sein. Die Verfügbarkeit als ein Teilziel der IT-Sicherheit besitzt meistens sehr hohe Priorität. Firewalls und IPS stehen direkt im Datenstrom. Somit kommen neue Ausfallrisiken hinzu. Durch diese Funktionsweise kann es zudem sein, dass Datenverkehr nach einem Update, der davor noch einwandfrei übertragen wurde, danach gestört ist.

Behörden Spiegel: *Welche Eigenschaften sollte eine Sicherheitslösung denn haben?*

Scheucher: Da Behörden untereinander gut vernetzt sein müssen und Anwendungen im E-Government eine hohe Verfügbarkeit aufweisen sollten, ist es notwendig, dass die Lösung die Verfügbarkeit nicht beeinträchtigt und die Komplexität nicht zusätzlich erhöht. Es muss somit eine passive Lösung sein, die leicht zu installieren und ohne tiefgehendes IT-Sicherheits-Know-how zu bedienen ist. Sie sollte keine Fehlalarme abgeben und kostengünstig sein.

Behörden Spiegel: *Ihr Unternehmen hat die sogenannte honeyBox entwickelt. Welches Prinzip liegt dieser zugrunde?*

Scheucher: Sie basiert auf dem Prinzip der "Honeypots" (Honig-Töpfe). Honeypots funktionieren nach einem einfachen Prinzip: Sie gewähren dem Angreifer Zugriff, aber nur bis zu einem gewissen Grad. Sie sind eine Art Ressource, deren Wert darin liegt, dass sie angegriffen und für einen Bestandteil des Netzwerkes gehalten wird. Sie stellen also Köder dar, die man in großer Anzahl im Netzwerk auslegen kann. Dabei unterscheidet man zwischen einer mehr oder minder realistischen Simulation einer Ressource im Falle eines Low-Interaction-Honeypots und der Bereitstellung eines realen Systems bei High-Interaction-Honeypots.

Beim Low-Interaction-Honeypot ist der Vorteil, dass dieser sehr leichtgewichtig ist. Das erlaubt den Einsatz sehr vieler dieser Honeypots. Der Angreifer kann ihn aber auch leichter enttarnen.

High-Interaction-Honeypots bilden echte Systeme sehr realistisch nach oder sind gar echte Systeme. Sie können dadurch auch menschliche Angreifer täuschen. Der Nachteil allerdings ist, dass Angreifer leichter aus der honeyBox-Umgebung ausbrechen können und dass die Datenauswertung sehr umfangreich ist.

Low-Interaction-Honeypots kommen daher im praktischen Einsatz vor, wohingegen High-Interaction-Honeypots in der IT-Sicherheitsforschung zu Hause sind.

Behörden Spiegel: *Sie haben also einen für eine Sicherheitslösung untypischen Ansatz gewählt. Wie ist der Honeypot ursprünglich entstanden?*

Scheucher: Es ist nicht belegt, seit wann genau die Technik der Honeypots in der IT-Umgebung eingesetzt wird.

Fakt ist, dass sie bei *Clifford Stoll* Erwähnung findet, der beschreibt, wie er einen Einbruch in die Daten des Lawrence Berkeley National Laboratory im August 1986 mithilfe erfundener Daten aufklärt. Der Angreifer wurde durch erfundene Daten gezwungen, solange online zu bleiben, bis die Telefonverbindung zurückverfolgt werden konnte.

Behörden Spiegel: *Die grundlegende Idee ist also, dass der Hacker in eine Falle tappt. Aber bieten Honeypots auch hinreichend Schutz vor internen Angriffen?*

Scheucher: Ja, der Honeypot kann auch gegen interne Attacken eingesetzt werden. Oftmals sind diese zwar durch IPS geschützt, aber nur, wenn der Angreifer genau dort vorbei kommt. Meistens werden solche Systeme am Internetzugang eingesetzt.

Was passiert aber, wenn der Angreifer diese Hürde bereits genommen oder umgangen hat? Die meisten Netzwerke sind dann schutzlos. Honeypots können hier Beachtliches leisten, da sie typischerweise intern in großer Zahl platziert werden. Er bietet typische Dienste an und bindet mehrere IP-Adressen, ohne dass es zu Performance-Problemen kommt. Es genügt oftmals schon die Information, dass ein bestimmtes System einen Verbindungsversuch unternommen hat.

Der Nachteil allerdings ist, dass nur die Angriffe registriert werden, die direkt auf einen Honeypot eingehen. Dabei erkennt der Honeypot eine sich schnell ausbreitende Schadsoftware oder automatisierte Angriffe schnell, während ein Angreifer, der gezielt mit Insider-Informationen vorgeht, unter Umständen nicht erkannt wird.

Behörden Spiegel: *Was hat nun die honeyBox aus der Honeypot-Funktionsweise übernommen?*

Scheucher: Die honeyBox bietet die Möglichkeit, eine große Anzahl an virtuellen Honeypots zur Verfügung zu stellen. Je nach Modell sind dabei 250 bis 40.000 Honeypots auf einem Gerät möglich. Dabei werden die virtuellen Honeypots als Köder in möglichst jedem Netzwerk - segment ausgerollt.

Durch die hohe Skalierbarkeit der honeyBox ist das selbst in großen Netzen relativ einfach möglich. Während der manuellen oder automatischen Erkundung des Netzwerks treffen Eindringlinge im LAN auf virtuelle Honeypots, die sich für die Angreifer als in einem schlechteren Sicherheitszustand als die übrigen Systeme darstellen.

Bereits beim ersten Kontakt erfolgt die Alarmierung über verschiedene Wege. Die Meldungen lassen sich auch in übergeordnete IT-Sicherheitssysteme integrieren.