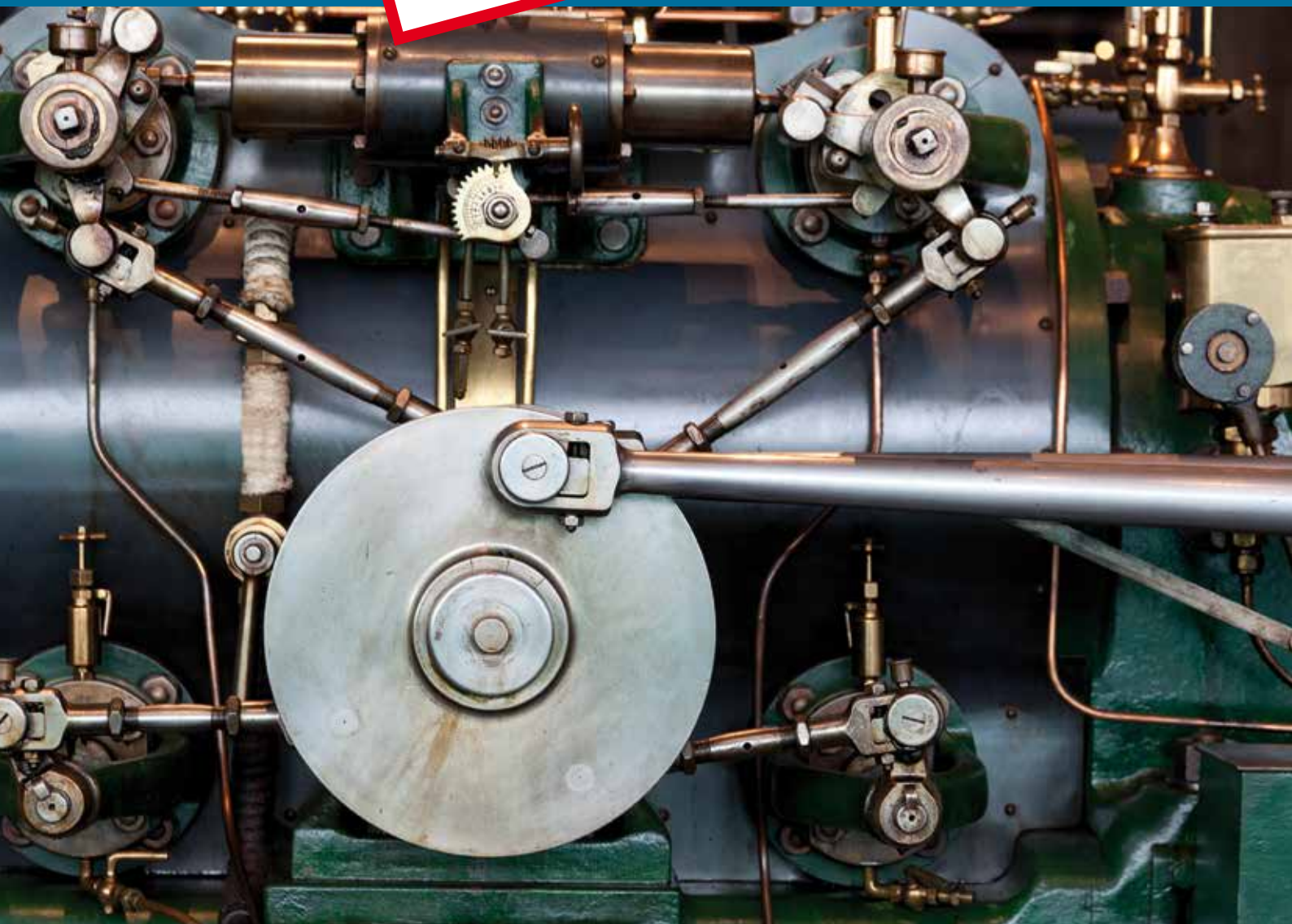
zeitschrift für automation und security

Nr. 4 · November 2013 · ISSN 2193-8555

IT-Security und Security für Systeme
der Automatisierungs-, Leit- und Steuertechnik

Sonderdruck für

secXTREME
Information Security



Sicherheitsrisiken in Prozessumgebungen eindämmen

Honeypots ziehen Angriffe auf sich

Sophia Häberle, Marketing / Vertriebsassistenz, secXtreme GmbH

Schutzmechanismen im Netz sind meistens aktiv, sie gehen direkt gegen Angriffe vor oder versuchen Fehlverhalten zu unterbinden. Einen anderen Ansatz verfolgen Honeypots. Sie laden Angreifer geradezu ein, sich mit ihnen zu beschäftigen und geben Administratoren so Zeit, Attacken zu erkennen und abzuwehren. Das Konzept passt mit Anpassungen auch in den ICS-Bereich.

Angriff mit System: Honeypots binden Ressourcen des Angreifers in wichtigen Phasen der Attacke

Netzwerktechnik auf Basis von Ethernet und TCP/IP verbindet immer häufiger Datenkommunikation im Office- und Internetbereich mit der Datenkommunikation in Produktionsanlagen. Dadurch entstehen nicht nur positive Synergien, auch Sicherheitslücken und Angriffe wie Denial-of-Service können von einem Netz ins andere übergreifen. Die Folge davon ist, dass Produktions- und Prozessnetze von vielen Sicherheitsrisiken aus dem Office- und Internetbereich bedroht sind, die das Personal der Prozess-IT kaum mehr überschauen und eingrenzen kann.

Sicherheitslösungen aus dem Office-Bereich reichen nicht

Patch-Management, Virenschutz, Firewalls und IPS sind nur bedingt für ICS geeignet, da entweder zusätzliches Know-how notwendig oder der Betrieb der Lösungen zeitintensiv ist. Das äußert sich zum Beispiel in Form eines hohen Pflegeaufwands beim Virenschutz. Am Übergang vom Office-Netz zum Prozess-Netz sind Ansätze wie Firewalls sinnvoll, doch innerhalb der Prozessnetze müssen zusätzliche Lösungen wie Honeypots eingesetzt werden.

Honeypots funktionieren nach einem einfachen Prinzip: Sie gewähren dem Angreifer nur bis zu einem gewissen Grad Zugriff. Sie sind eine Ressource, deren Wert darin liegt, dass sie angegriffen und für einen Bestandteil des Netzwerkes gehalten werden. Dabei unterscheidet man zwischen der mehr oder minder realistischen Simulation einer Ressource im Falle eines Low-Interaction-Honeypots und der Bereitstellung eines realen Systems bei High-Interaction-Honeypots. Vorteil des Low-Interaction-Honeypots ist, dass er viele Dienste simulieren kann. Das Prinzip dahinter ähnelt einer Filmkulisse: Es werden ganze Straßenzüge mit geringem Aufwand nachgebildet. Der Nachteil daran ist aber, dass der Angreifer den Täuschungsversuch erkennen kann. Die meisten Low-Interaction-Honeypots muss man sich aus Open-Source-Software zusammenstellen.

Echtes System täuscht Angreifer wirkungsvoll

Für High-Interaction-Honeypots werden in der Regel echte Systeme genutzt. Sie können dadurch auch menschliche Angreifer über einen längeren Zeitraum täuschen. Der Nachteil ist allerdings, dass Angreifer leichter aus der Honeypot-Umgebung ausbrechen können und die Honeypots sogar als weitere Sprungbretter verwenden können. Zudem ist die Datenauswertung umfangreich und der Betrieb einer High-Interaction-Honeypot Infrastruktur sehr zeitintensiv.

Es ist nicht genau belegt, seit wann die Technik der Honeypots in der IT-Umgebung eingesetzt wird. Fakt ist, dass sie 1989 bei Clifford Stoll Erwähnung findet. In seinem Buch „Cuckoo's Egg" beschreibt er, wie er einen Ein-

bruch in die Computersysteme des Lawrence Berkeley National Laboratory im August 1986 mithilfe erfundener Daten aufklärt. Weil er weiß, dass der virtuelle Einbrecher nach Dokumenten mit Geheiminformationen sucht, legt er zahlreiche Ordner an, die mit interessant klingenden aber frei erfundenen Informationen gefüllt sind. Zusätzlich beschränkt er die Download-Geschwindigkeit, damit der Angreifer möglichst lange mit dem System verbunden bleibt und die Telefonnummer des anrufenden Modems zurückverfolgt werden kann.

Eine der ersten Varianten des Honeypots war der sogenannte „Tarpit", auf Deutsch heißt das in etwa „Teergrube". Im übertragenen Sinn soll der Angreifer am Teer kleben bleiben. Die Taktik einer Tarpit ist, dass unerwünschte eingehende Verbindungen zwar nicht abgebrochen werden, aber der Dienst immer langsamer antwortet. Wird ein Scan vom Angreifer durchgeführt, muss er viel Zeit und Geduld mitbringen. Das behindert den Angreifer und soll ihn letztendlich zur Aufgabe zwingen.

Funktionsweise von Honeypots

Es gibt verschiedene Einsatzgebiete von Honeypots. Der Einsatz gegen interne Attacken ist sicherlich eines der wichtigsten. Office-LANs sind zwar oftmals durch Intrusion Prevention Systeme geschützt, die das Netzwerk im Hintergrund nach unerwünschtem oder gefährlichem Netzwerkverkehr filtern. Dadurch wird aber oft auch Netzwerkverkehr blockiert, der an sich nicht gefährlich ist.

Ein Honeypot funktioniert anders, da er nicht den Inhalt, sondern das Verhalten des Angreifers überwacht. Durch den Honeypot können mehrere Stufen des Angriffs abgefangen und unschädlich gemacht werden. Dazu gehört der erste Scan auf verfügbare IP-Adressen und Ports sowie die Zuordnung von ausnutzbaren Sicherheitslücken und die Versuche, Zugriff zum Opfer zu erlangen. Der Honeypot bietet typische Dienste an und ist auf vielen IP-Adressen erreichbar, ohne dass es zu Performance-Problemen kommt. Oftmals genügt schon die Information, dass ein bestimmtes System einen Verbindungsversuch unternommen hat. Der Nachteil allerdings ist, dass nur die Angriffe registriert werden, die den Honeypot direkt zum Ziel haben. So erkennt der Honeypot eine sich ausbreitende Schadsoftware schnell, während ein manuell agierender Angreifer, der gezielt mit Insider-Informationen vorgeht, unter Umständen nicht erkannt werden kann.

Einfaches Prinzip: Virtuelle Köder sollen Angreifer anziehen und aufhalten

1. Informationsrecherche (im Internet)
2. Scannen (ARP, ICMP, Ports, Betriebssysteme)
3. Erkunden (Dienste, Benutzer, Software), Low-Interaction Honeypot
4. Auf Systeme zugreifen
5. Privilegien ausbauen
6. Suche nach Vertrauensbeziehungen, Passwörtern
7. Hintertüren einbauen
8. Spuren verwischen

Kommerzielle Lösungen auch für ICS verfügbar

Kommerzielle Honeypot-Systeme, wie die honeyBox industrial von secXtreme wurden speziell für das industrielle Umfeld entwickelt. Die honeyBox und andere Lösungen können in Industrie-Umgebungen sowohl Low- als auch High-Interaction Honeypots bereitstellen. Sie simulieren in den Prozess-LANs virtuelle Opfersysteme als Köder, die die Angreifer auf sich ziehen. Während der manuellen oder automatischen Erkundung des Netzwerks durch den Eindringling trifft er im LAN auf virtuelle Honeypots, die augenscheinlich schwächere Sicherheitsvorkehrungen aufweisen, als die übrigen Systeme darstellen. Bereits beim ersten Kontakt wird der Administrator über den Angriffsversuch informiert. Die Qualität der Alarmierung ist hoch, weil nur auf aktive Angriffsversuche reagiert wird. Die Alarmierung kann zur besseren Übersicht im Idealfall auch an die Prozessvisualisierung angekoppelt werden. Alle Meldungen sollten klar und verständlich formuliert sein, damit auch IT-technisch ungeschultes Bedienpersonal sofort die Tragweite des Vorfalls erkennt.

Wichtig ist, dass die Systeme die Ansprüche des industriellen Umfelds erfüllen. Die Geräte müssen schnell und einfach installiert werden können und transparent für das Netz agieren. Bandbreitenintensive Signatur-Updates sind in der Regel nicht notwendig, nur Updates der Software und mögliche Patches und Hotfixes können auf dem Honeypot-Host erforderlich sein, was auf Wunsch automatisierbar sein sollte. Natürlich muss der Host, auf dem der Honeypot läuft, und dessen Software möglichst resistent gegen Angriffe sein.

Für den Betreiber der Industrieanlage ist es das oberste Ziel, die Verfügbarkeit der Systeme nicht zu gefährden. Ein Honeypot muss daher in jeder Situation transparent für den Rest des LANs sein und andere Systeme auch bei einem Ausfall nicht beeinflussen. Normalerweise agieren die Honeypot-Hosts rein passiv, sodass auch keine Auswirkungen auf andere Bereiche des LANs zu erwarten sind. Mit einem richtig konfigurierten und angepassten Honeypot können die Betreiber von Industrieanlagen einen wichtigen zusätzlichen Sicherheitslevel etablieren, der aktive Schutzmechanismen wie Firewalls, Anti-Virus oder Intrusion Prevention Systeme optimal ergänzt. ■

Sorgen Sie sich um die Sicherheit in Ihrer IT. Nutzen Sie die Vorteile der honeyBox.

Die Produkte aus der honeyBox Famile sind passend für Industrie– und Officeumgebungen.

- zuverlässige Erkennung von Angreifern im Netz
- sehr schnelle Detektion von Wurmausbrüchen
- äußerst wenig Fehlalarme
- hohe Skalierbarkeit
- einfache Integration in das Netzwerk
- Keine Änderung der Netzwerkstruktur notwendig
- Einsatz beeinflusst die (Hoch-)Verfügbarkeit des Netzwerks nicht
- sehr geringer Betriebsaufwand
- zentrale Auswertung der Sicherheitsmeldungen
- sehr geringe Kosten je Netzsegment

Kundenmeinung von Reinhard Görtner Leiter IT & Services RTL II:

„Die professionelle Implementierung und die technische Kompetenz von secXtreme haben uns gezeigt, dass die Entscheidung für die honeyBox richtig war“.

secXtreme GmbH
Kiefernstraße 38
D-85649 Brunnthal-Hofolding

Tel. +49(0)89-18 90 80 68-0
Fax.+49(0)89-18 90 80 68-77
E-Mail: info@sec-xtreme.com
WWW: www.sec-xtreme.com

Über secXtreme: Die secXtreme GmbH hat sich auf die Sicherheit Ihrer Informationen spezialisiert. Dazu gehören die Bereiche Audit, Penetration Testing, Sicherheitsanalysen und Trainings. Neben diesen Bereichen entwickelt secXtreme Sonderlösungen im Sicherheitsumfeld. secXtreme ist Mitglied im Deutschen CERT-Verbund und unterstützt seine Kunden bei Incident-Management- und Forensik-Aufgaben.

Auszeichnungen für die honeyBox® Appliance Familie