secXtreme Whitepaper

IT-Sicherheit in Produktionsumgebungen (SCADA[1]) honeyBox® vs. Stuxnet

Stuxnet ist der erste bekannt gewordene Angriff auf Produktionsumgebungen mit hohem Gefahrenpotential. Die klassische IT-Sicherheit hat dort versagt. Mit der honeyBox® Honeypot Appliance wäre Stuxnet mit sehr hoher Wahrscheinlichkeit bereits bei der Infektion erkannt worden, lange bevor er Mitte 2010 entdeckt wurde.

1 Abstract

Dieses Whitepaper beschreibt die Situation in der industriellen IT-Sicherheit und die Unterschiede zwischen Office-IT und Prozess-IT in diesem Bereich. Es werden IT-Sicherheitsmaßnahmen der klassischen IT beleuchtet. Es wird erläutert, welche Anforderungen an Sicherheitskomponenten in der Prozess-IT bestehen, warum diese mit den klassischen Ansätzen nicht erfüllt werden können und wie die Anforderungen mit dem Einsatz der honeyBox® Honeypot Appliance gelöst werden.

2 Ausgangslage

Die Automatisierungs- und Steuerungstechnik war bisher durch Systeme gekennzeichnet, die untereinander mit eigenen Techniken und Protokollen kommunizierten. Dazu gehört z. B. die RS-485 Schnittstelle, Profi-Bus und der CAN-Bus. Die Projektierung und Programmierung der Anlagen erfolgt dabei häufig über Software auf eigenen PCs in der Anlage.

Doch in diesen Umgebungen hält die allgegenwärtige Netzwerktechnik auf Basis von Ethernet und TCP/IP immer weiteren Einzug. Zunächst werden die PC-Stationen vernetzt und danach die Ebenen der Leit- und Steuertechnik. Speicherprogrammierbare Steuerungen (SPS) werden zunehmend an das LAN angeschlossen und Kleinsteuerungen auf Basis von Embedded Systemen werden zunehmend mit LAN-Schnittstellen angeboten.

TCP/IP auf Ethernet zieht als bewährter Übertragungsweg immer weiter in vormals „TCP/IP-freie" Bereiche von Produktions- und Steuertechnik ein. Industrial Ethernet ist im Markt angekommen und wird von verschiedenen Herstellern mit ihren Produkten abgedeckt. Selbst WLAN-Komponenten sind mittlerweile den rauen Anforderungen der Produktionsumgebungen gewachsen und im Einsatz.

Als Konsequenz daraus wächst die Datenkommunikation im Office- und Internetbereich immer weiter mit der in Produktionsanlagen zusammen. Dies ermöglicht auch Synergien. Gerade die Visualisierung und Auswertung von Prozessdaten sind hier Anforderungen, die erfüllt werden müssen. Im Energiebereich sind Erzeugungs- und Verbrauchsdaten auch zwischen Energieversorgern zeitnah auszutauschen.

1 Supervisory control and data acquisition

3 Sicherheit ist nicht gleich Sicherheit

Wenn in industriellen Umgebungen von Sicherheit gesprochen wird, geht es meist um Ausfallsicherheit, elektrische Sicherheit, Sicherheit für das Betriebspersonal, Schutz gegen Umwelteinflüsse oder um Explosionsschutz.

Die im Internet und Office-Bereich typischen Sicherheitsrisiken, wie Denial Of Service-Angriffe, Manipulation von Daten und Systemen, Ausspähen von Daten oder Systemeinbrüche werden hier oft nicht benannt, erkannt oder berücksichtigt. Dies war in der Vergangenheit dort auch oft nicht notwendig.

4 Sicherheitsprobleme

Die Nutzung von Ethernet und TCP/IP erzeugt neue Sicherheitsprobleme in Produktionsumgebungen, die vorher nicht vorhanden waren. Zudem führt die Kopplung von Prozessnetzen mit der Office-Welt oder gar dem Internet auch hier zu neuen und bedeutsamen Risiken.

4.1 Probleme durch Nutzung von Ethernet und TCP/IP

Ethernet und TCP/IP bieten einem Angreifer oder Schadsoftware einen standardisierten Verbreitungsweg. Es ist immer weniger konkretes Wissen über die Anlagen notwendig. Das erlaubt auch standardisierte Angriffe (siehe Stuxnet).

Bestehende und neue Implementierungen von TCP/IP Protokollen in Geräten sind fehlerbehaftet. Diese Fehler können auch sicherheitsrelevant sein.

4.2 Gefahr durch Ankopplung

Über die neu geschaffenen Übergänge sind plötzlich sämtliche Bedrohungen aus dem Office- und Internetbereich in den Produktions- und Prozessnetzen präsent. Mit einem Schlag wird aus einer sicheren Enklave ein Teil des globalen Dorfes. Diese Tatsache und die daraus entstehenden Konsequenzen können das Personal der Prozess-IT an die Grenzen dessen bringen, was sie mit Ihrem Know-how im Sicherheitsbereich einschätzen und lösen können.

Andererseits ist für die klassische IT-Sicherheit im Office-Bereich die Prozess-IT mit ihren Abläufen, Anforderungen und Protokollen nicht leicht zu verstehen.

Es stellt sich dann häufig die Frage, wer nun für die IT-Sicherheit verantwortlich ist und wer das Know-how dazu hat. Aus unserer Erfahrung heraus ist hier nur ein gemeinsamer Weg beider Beteiligten zielführend. Die Prozess-IT muss sich mit den für sie neuen Bedrohungen aus der Office-Welt auseinander setzen. Zugleich ist auch die Office-IT gefordert, Know-how aus dem Bereich der Prozess-IT aufzubauen. Diese Konvergenz führt nicht selten dazu, dass die vormals getrennten Bereiche organisatorisch nach einer gewissen Zeit mehr und mehr zusammenwachsen.

4.3 Lösungsansätze mit bekannten Verfahren aus der Office-Welt

Um die neuen Bedrohungen in der Prozess-IT zu entschärfen, werden fast immer IT-Sicherheitsmaßnahmen aus der Office-Welt ins Auge gefasst. Dazu gehören:

- Patch-Management
- Virenschutz
- Firewalls
- Intrusion Prevention Systeme (IPS)

Die Lösungen eigenen sich aber nur bedingt, in Teilen sogar gar nicht für die Prozess-IT. Das hat folgende Gründe:

- Für den Betrieb ist sehr viel Know-how im Bereich IT-Sicherheit notwendig. Das betrifft in hohem Maße die Intrusion Prevention Systeme. Dieses Know-how ist zumindest initial in der Prozess-IT nicht vorhanden und müsste erst aufgebaut werden.
- Der Betrieb dieser Lösungen ist sehr zeitintensiv. Gerade IPS benötigt für einen sicheren Betrieb ständigen Pflegeaufwand. Auch der Virenschutz sollte mindestens tagesaktuelle Pattern auf allen Systemen aufweisen. Aufgrund technischer Gegebenheiten ist eine Online-Verteilung der Pattern oft nicht möglich. Der Update der Systeme aus dem Internet selbst ist aus Sicherheitsgesichtspunkten als sehr problematisch einzustufen, so dass oft nur manuelle Verfahren übrig bleiben.
- Viele Systeme der Prozess-IT sind so geprüft und abgenommen wie sie sind. Das verhindert oft das Einspielen von Patchen oder die Installation einer Virenschutz-Software.
- Das oberste klassische IT-Sicherheitsziel der Prozess-IT, die Verfügbarkeit, wird durch den Einsatz von Firewalls und IPS deutlich reduziert. Beide Lösungsansätze verlangen, dass der Datenverkehr durch diese Systeme geleitet wird. Das führt zu neuen Ausfallrisiken. Zudem sind diese Systeme dafür gebaut, Verkehr gezielt zu blockieren (IPS) oder nur manuell freigegebene Verkehrsbeziehungen (Firewall) zuzulassen. Durch die Updates bei IPS kann es durchaus zu der Situation kommen, dass Verkehr, der vor einem Update noch funktionierte, danach blockiert wird. Dies birgt erhebliche Risiken für die Verfügbarkeit der Prozessnetze.

Das hat zur Folge, dass klassische IT-Sicherheitsmaßnahmen in der Prozess-IT zu neuen Problemen führen und die Risiken durchaus größer als der Nutzen sein können.

Sinn machen solche Ansätze (Firewall, IPS) durchaus am Übergang vom Office-Netz zum Prozess-Netz. Innerhalb von Prozess-Netzen sind daher andere Konzepte gefordert.

5 Anforderungen an prozessnahe IT-Sicherheitslösungen

IT-Sicherheitslösungen in der Prozess-IT müssen aus unserer Sicht folgende Anforderungen erfüllen:

- keine Verschlechterung der Verfügbarkeit
- keine Steigerung der Komplexität des Netzwerks (z. B. durch Hochverfügbarkeits-Protokolle)
- Sehr geringer Installationsaufwand
- Äußerst geringer Betriebsaufwand
- Keine Fehlalarme

- Ankoppelbarkeit der Alarmierung an die Prozess-Visualisierung
- Einfache und verständliche Meldungen (kein IT-Security-Expertenwissen notwendig)
- Industrietaugliche Hardware (Umgebungsbedingungen, Hutschienenmontage, Stromversorgung)
- Geringer Stückpreis

6 Lösung mit der honeyBox®

6.1 Funktionsprinzip

Die honeyBox® stellt in den Prozess-LANs virtuelle Opfersysteme (Honeypots) zur Verfügung, um Angriffe auf sich zu lenken. Angreifer und Schadsoftware (z. B Stuxnet) treffen dann bei den ersten Angriffsschritten (manuelle oder automatische Erkundung des LANs, Scans) auf reale Systems und virtuelle Honeypots. Diese sind für den Angreifer zunächst nicht von den realen Systemen zu unterscheidbar, stellen sich aber in einem schlechteren Sicherheitszustand dar. In den nächsten Phasen eines Angriffs lenken sie so die weiteren Aktivitäten des Angreifers oder der Schadsoftware auf sich. Bereits beim ersten Kontakt mit einem virtuellen Honeypot erfolgt die Alarmierung.

6.2 Erfüllung der Anforderungen im industriellen Umfeld

Die honeyBox® Honeypot Appliance von secXtreme erfüllt die unter Punkt 4 genannten Anforderungen vollständig:

Verfügbarkeit: Die honeyBox® wird wie ein normales Endgerät an einen Switch angeschlossen. Der Verkehr wird nicht durch das Gerät geleitet. Wenn die honeyBox® ausfällt, laufen die Produktionsdaten weiter.

Keine Steigerung der Komplexität des Netzwerks: Die honeyBox® wird wie ein einfaches Endgerät an einen Switch angeschlossen. Sie verhält sich im Normalbetrieb rein passiv.

Sehr geringer Installationsaufwand: Die honeyBox® ist bei bekannter Konfiguration innerhalb einer halben Stunde komplett konfiguriert. Bei mehreren Geräten kann die Konfiguration zudem automatisiert werden. Vor Ort beschränkt sich die Installation auf das Aufsetzen auf die Hutschiene, Anschluss der Spannungsversorgung und Einstecken des LAN-Kabels.

Äußerst geringer Betriebsaufwand: Das Einspielen von neuen Pattern und Signaturen gibt es bei der honeyBox® nicht. Es sollten lediglich in regelmäßigen Abständen die Sicherheitspatches eingespielt werden. Da die honeyBox® einen hohen Selbstschutz besitzt, ist dies nur in bestimmten Umgebungen zeitnah erforderlich. Zudem können die Updates automatisiert werden. Jede honeyBox® überwacht sich selbst und korrigiert eine Reihe von Fehlerzuständen selbständig.

Geringe Fehlalarme: Wenn kein Angriff im Netz statt findet sendet die honeyBox® auch keine Alarme aus. Die Qualität der Alarmierung ist daher sehr hoch.

Ankoppelbarkeit der Alarmierung an die Prozess-Visualisierung: Die honeyBox® industrial bietet optional digitale Ausgänge, die an die Prozess-Steuerung angeschlossen werden können. So kann ein Angriff auch in der Prozess-Visualisierung dargestellt werden. IT-Sicherheit wird damit

integraler Bestandteil des Prozesses.

Einfache und verständliche Meldungen: Die Meldungen der honeyBox® sind ohne Expertenwissen für IT-Sicherheit interpretierbar. Sie beinhalten, was wo passiert ist (z. B. Zugriff auf einen FTP-Server eines virtuellen Honeypots mit versuchtem Login) und nicht die Meldung, dass eine Schwachstelle XY mit der Nummer CVE-yz ausgenutzt worden wäre. Die Meldungen sind so von jedem Mitarbeiter mit allgemeinem IT-Wissen interpretierbar.

Industrietaugliche Hardware: Die honeyBox® industrial ist für den Einsatz in Industrieumgebungen gebaut. Es wird ein erweiterter Temperaturbereich abgedeckt. Selbst die verwendete Flash-Karte ist eine Industrie-Ausführung. Zudem enthält das System keine beweglichen Teile. Die honeyBox® industrial ist für Hutschienen-Montage vorgesehen. Die Stromversorgung erfolgt über einen Gleichspannungseingang. Für die Inbetriebnahme und den Service ist keine Tastatur und kein Bildschirm notwendig. Der lokale Zugang erfolgt über einen seriellen RS232 Port.

Geringe Kosten: Die honeyBox® industrial ist so kalkuliert, dass der Preis einen Einsatz an vielen Stellen in der Produktion erlaubt, ohne die Kosten klassischer IPS Systeme zu erreichen. Es ist damit der Einsatz von einer größeren Zahl an Systemen bei geringeren Kosten und einer größeren Abdeckung möglich.

7 Die honeyBox® in der Praxis

Die honeyBox® wurde mit dem Bayerischen Sicherheitspreis 2009 ausgezeichnet. Im Innovationspreis IT-Mittelstand errang sie 2009 und 2010 vordere Plätze. Die Lösung ist bereits bei vielen Kunden im Einsatz und hat dort ihren Nutzen bewiesen.

8 Weiterführende Verweise

- honeyBox® Datenblatt, http://www.sec-xtreme.com/fileadmin/download/public/secXtreme_honeybox_honeypot_appliance_rel5_0_de.pdf
- honeyBox® Testbericht Linux Magazin 12/2009, http://www.sec-xtreme.com/fileadmin/download/public/LinuxMagazin-Sonderdruck_secXtreme_honeyBox_web.pdf
- Stuxnet, Wikipedia, http://de.wikipedia.org/wiki/Stuxnet
- Computervirus Stuxnet – Der Wurm, der aus dem Nichts kam, Spiegel Online, http://www.spiegel.de/netzwelt/web/0,1518,718927,00.html
- All about Stuxnet, http://www.stuxnet.net

9 Über den Autor

Christian M. Scheucher ist seit vielen Jahren im Bereich der IT-Sicherheit tätig. Er implementierte zahlreiche Lösungen zur Erkennung von Angriffen. Im Rahmen der IT-Forensik-Dienstleistungen von secXtreme klärt er Angriffe auf und in Penetrationstests prüft er Systeme auf deren Sicherheit. Er ist Initiator der honeyBox®.

10 Über secXtreme

Die secXtreme GmbH ist ein Unternehmen, das sich auf Beratungs- und Dienstleistungen in der IT-Sicherheit spezialisiert hat. secXtreme bietet Leistungen im Bereich Angriffserkennung und -verfolgung, (Web-)Anwendungssicherheit und Audits an. secXtreme entwickelt zudem Sicherheitslösungen auf Linux-Basis für spezielle Anforderungen in der IT-Sicherheit. secXtreme ist Mitglied im Verbund deutscher Notfall-Teams, dem Deutschen CERT-Verbund.

Kontaktinformation:

secXtreme GmbH

Kiefernstraße 38

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

Web: http://www.sec-xtreme.com