INDUSTRIAL NETWORKS

YELLO NETCOM

In sensiblen Netzwerkbereichen Schadsoftware zuverlässig erkennen

Da manuelle Angriffe und Schadsoftware im internen Netzwerk immer auf demselben Vorgehenskonzept basieren, sind diese grundsätzlich einfach und effizient feststellbar. Die bestens bekannten Lösungen gegen Schadsoftware (VirenScanner usw.) versuchen zu verhindern, dass sich solche in produktive Systeme einnisten, verbreiten und Schaden anrichten können. Die Nachteile solcher Lösungen sind offensichtlich: Die Schadsoftware muss bekannt sein und man muss mit dem Installieren von Software aktiv in produktive Systeme eingreifen. Die Absicht, in komplexen Umgebungen ohne Eingriffe in Produktivsysteme und in die Netzwerktopologie eine hochwirksame Überwachung gegen manuelle Angriffe und Schadsoftware realisieren zu können, ist durch den Einsatz einer honeyBox Appliance von SecXtreme möglich. Das System emuliert eine grössere Anzahl von angreifbaren Systemen (low interaction honeypots) in verschiedenen Netzsegmenten. Bei einem Angriff sind diese emulierten Systeme primär gefährdet, weil sie durch entsprechende Einstellungen für einen Angriff geeignet erscheinen und diese deshalb automatisch auf sich ziehen. Die Daten eines Angriffs werden auf der honeyBox aufgezeichnet und die zuständigen internen Stellen werden automatisch alamiert, so dass sofort entsprechende Gegenmassnahmen eingeleitet werden können. Dadurch gewinnt man Zeit und erhält eine Übersicht, was im Netzwerk bezüglich aktiver Schadsoftware überhaupt passiert. Da eine honeyBox nicht wie bei IDS/IPS- und Virenscan-Systemen nach verdächtigen Datenmustern sucht und nicht in den Datenstrom eingeschleift wird, müssen keine periodischen Pattern Files geladen werden, es sind keine Eingriffe in Betriebssysteme notwendig, es können keine Fehlalarme generiert werden und eine Beeinträchtigung der Netzwerkverfügbarkeit ist nicht möglich.

Die honeyBox Honeypot-Appliance wurde bereits im Jahr 2009 mit dem Bayerischen Sicherheitspreis für herausragende und innovative Sicherheitsprodukte der betrieblichen Sicherheit ausgezeichnet. Als besonders auszeichnungswürdig wurden praxisgerechte Lösungen für unternehmensinterne Sicherheitsmassnahmen betrachtet.

Wir sehen die honeyBox Appliance von SecXtreme als hochwirksame Ergänzung zu bestehenden Sicherheitslösungen in sensiblen Netzwerkbereichen. Bei Interesse stehen wir gerne für weitere Auskünfte oder für eine Teststellung zur Verfügung.

YELLO NETCOM GMBH
Birkenallee 115-117
48432 Rheine