Hacker nehmen Energiebranche ins Visier: Ein Umdenken in puncto Sicherheitskonzepte ist notwendig

Hacker nehmen Energiebranche ins Visier: Ein Umdenken in puncto Sicherheitskonzepte ist notwendig

Ein Kommentar von Andreas Schmid, Senior Presales Consultant, Adyton Systems
Wie kürzlich bekannt wurde, hat die Hackergruppe "Dragonfly" nun auch die Energiebranche ins Visier ihrer Angriffe genommen. Stromerzeuger, Pipeline-Betreiber und Ausrüster für den Energiebereich aus zahlreichen Ländern Europas, darunter auch Deutschland, waren bereits Opfer der Attacken. Die Kriminellen nutzen einen Schadcode, der Fernzugriffe ermöglicht und damit auch das Auslesen konkreter Systeminformationen.
Diese Art Angriffe sind besonders schwer zu bekämpfen. Dies liegt zunächst an der Struktur der Energiebranche selbst, die aktuell zwei gravierenden Umbrüchen unterliegt: Dabei handelt es sich zum einen um den Bereich Energieerzeugung, wo die Frage im Raum steht, wie Energie ins Netz gespeist werden soll. Zum anderen steht die Branche vor der Herausforderung, Technologien und Prozesse so zu definieren, um das Energienetz zu steuern und zu überwachen. Denn mittlerweile bewegt sich die Energieerzeugung in einer verteilten und vernetzten Welt. Strom wird in hunderten von kleinen Einheiten erzeugt, teilweise auf Hausdächern und mit Windrädern. Das verändert die Anforderungen an die überwachende Technik. Steuerungs- und Managementtechnologie muss angepasst und erweitert werden. Dazu gehört einerseits, die grundlegenden Funktionen über öffentliche Netze zu erbringen; andererseits muss die Technologie so abgesichert werden, dass kein Schaden entsteht.
Whitelisting ermöglicht präventives Handeln
Generell sind bei Betreibern kritischer Infrastrukturen neben klassischen, bis zum Enduser bekannten Bedrohungen wie Trojanern, auch gezielte aufwändig organisierte Cyber-Angriffe wie APT (Advanced Persistent Threats) zu beobachten. Solchen Angriffen kann mit herkömmlichen Abwehrmethoden nur sehr schwer begegnet werden. Darum ist dringend ein Umdenken in den Sicherheitskonzepten notwendig: weg von althergebrachten Blacklisting-Konzepten hin zum Konzept einer vollständigen Positivvalidierung. Im Gegensatz zum Blacklisting-Verfahren, wo bekannte Bedrohungen explizit nicht zugelassen werden, erlaubt der sogenannte Whitelisting-Ansatz ausschließlich Netzwerkverkehr, der eindeutig als gutartig validiert werden kann. Jede Transaktion im Netzwerk wird auf Anwendungsart und Inhalt analysiert und nicht bekannter Verkehr am Betreten des Netzwerkes gehindert.
Feingranulare Analyse von Applikationen
Mit herkömmlichen Firewalls war ein solches Konzept nur mit einem erheblichen Managementmehraufwand realisierbar und hat auch dann noch nicht genügend Schutz geboten. Moderne Next-Generation-Firewalls sollten jedoch darauf ausgerichtet sein, Applikationen feingranular zu analysieren anstatt anhand eines Ports zu definieren, welche Art von Netzwerkverkehr zu oder von einer Maschine gestattet ist. Es wird nicht mehr nur innerhalb großzügig erlaubten Netzwerkverkehrs versucht, einen Schadcode zu identifizieren. Vielmehr wird ausschließlich erlaubt, was im Voraus als gutartig definiert wurde. Ein weiterer Vorteil besteht darin, grundlegende Traffic-Shaping-Methoden auf diesen eindeutig erkannten Netzverkehr anzuwenden. Das heißt, die Bandbreite von weniger wichtigen Applikationen muss zugunsten von geschäftskritischen Anwendungen beschränkt werden. Streaming-Inhalt wie z.B. per YouTube wird so eingeschränkt, dass nur ein begrenzter Teil der Bandbreite zur Verfügung steht.
Weiter lässt sich die Sicherheit außerdem mittels Deep-Packet-Inspection (DPI) erhöhen - insbesondere auf Applikationsebene. Hierbei wird eine Applikation nicht nur als solche erkannt, vielmehr wird mit Hilfe von Decodern auch innerhalb einer Applikation oder eines Protokolls gefiltert. Hiermit kann eindeutig sichergestellt werden, dass der Netzwerkverkehr genau das darstellt, was er vorgibt zu sein. Ebenso kann die IT-Abteilung die Kommunikation für bestimmte Nutzer oder Geräte einschränken. Ein dedizierter User kann beispielsweise Daten auslesen, aber nicht steuern. Gerade bei sogenannten "kritischen Infrastrukturen" ist der Einsatz einer Next Generation Firewall deshalb nicht nur gerechtfertigt, sondern essenziell.
Über Adyton Systems
Adyton Systems ist ein deutsches Technologieunternehmen aus Leipzig und bietet Lösungen für die Informationssicherheit von Unternehmen. NETWORK PROTECTOR hat das Konzept der Next-Generation-Firewall revolutioniert. Der Schwerpunkt liegt auf der Verteidigung von Unternehmenswerten durch die Technologie der vollständigen Positivvalidierung in Kombination mit Applikations-Whitelisting. Adyton Systems nutzt hierfür die neueste Deep-Packet-Inspection-Lösung für ein beispielloses Niveau bezüglich Transparenz und Kontrolle sowohl innerhalb als auch außerhalb des Unternehmensnetzwerkes. NETWORK PROTECTOR ist auch für Nicht-Experten einfach zu installieren und zu verwalten und bietet ein Maximum an Informationssicherheit. Adyton Systems ist ein Unternehmen der Rohde
 Schwarz-Firmengruppe, die in über 70 Ländern aktiv ist und im Geschäftsjahr 12/13 (Juli bis Juni) einen Umsatz von 1,9 Milliarden Euro erwirtschaftet hat. Adyton Systems ist Regionalstelle Leipzig des TeleTrusT - Bundesverband IT-Sicherheit e.V. und trägt das Qualitätszeichen IT-Security made in Germany. www.adytonsystems.com

Kristin Preßler
Head of Marketing
Tel.+49-341-392993431
Fax+49-341-392993439
E-Mailkristin.pressler@adytonsystems.com
Internet www.adytonsystems.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=571535" width="1" height="1">

Pressekontakt

Adyton

0410 Leipzig

Firmenkontakt

Adyton

0410 Leipzig

Über Adyton Systems GmbHDie Adyton Systems GmbH ist ein deutsches Technologieunternehmen aus Leipzig und bietet Lösungen für die Informationssicherheit von Unternehmen. NETWORK PROTECTOR hat das Konzept der Next-Generation-Firewall revolutioniert. Der Schwerpunkt liegt auf der Verteidigung von Unternehmenswerten durch die Technologie der vollständigen Positivvalidierung in Kombination mit Applikations-Whitelisting. Adyton Systems nutzt hierfür die neueste Deep-Packet-Inspection-Lösung für ein beispielloses Niveau bezüglich Transparenz und Kontrolle sowohl innerhalb als auch außerhalb des Unternehmensnetzwerkes. NETWORK PROTECTOR ist auch für Nicht-Experten einfach zu installieren und zu verwalten und bietet ein Maximum an Informationssicherheit. Die Adyton Systems GmbH ist ein Unternehmen der Rohde & Schwarz-Firmengruppe, die in über 70 Ländern aktiv ist und im Geschäftsjahr 12/13 (Juli bis Juni) einen Umsatz von 1,9 Milliarden Euro erwirtschaftet hat. Adyton Systems ist zudem

Regionalstelle Leipzig des TeleTrusT ? Bundesverband IT-Sicherheit e.V. und trägt das Qualitätszeichen ?IT-Security made in Germany. www.adytonsystems.com