FACHARTIKEL

SECURITY FÜR INDUSTRIELLE APPLIKATIONEN

YELLO NETCOM

Optimale Sicherheitsmassnahmen für industrielle Produktions- und Infrastrukturnetzwerke unterscheiden sich wesentlich von denen der Office-IT. Die Wahl der richtigen Konzepte und Komponenten hilft Ihnen, die Anforderungen von Standards wie NERV CIP, IEC 62443 und ANSI/ ISA-99 zu erfüllen und trägt dazu bei, kostenintensive Stillstandzeiten zu vermeiden und die optimale Leistungsfähigkeit Ihres Betriebs sicherzustellen.

In der täglichen Praxis erleben wir immer wieder, dass typische Steuerungsnetzwerke für simple alltägliche Sicherheitsrisiken äusserst anfällig sind. Mangelhafte Netzwerkaufteilung, ungeschützte Zugangspunkte, „weiche" Ziele wie Rechner ohne Sicherheitspatch und angreifbare speicherprogrammierbare Steuerungen sowie menschliche Fehler können signifikante Produktionsverluste und auch Sicherheitsprobleme verursachen.

Die Automatisierungs- und Steuerungstechnik war bisher durch SCADA-Systeme gekennzeichnet, die untereinander mit eigenen Techniken und Protokollen kommunizierten. Unter Supervisory Control and Data Acquisition (SCADA) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems. Die Projektierung und Programmierung solcher Anlagen erfolgte dabei häufig über Software auf eigenen PCs in der Anlage. Doch in diesen Umgebungen hält die Netzwerktechnik auf Basis von Ethernet und TCP/IP immer weiteren Einzug. Zunächst werden die PC-Stationen und danach die Ebenen der Leit- und Steuerungstechnik vernetzt. Speicherprogrammierbare Steuerungen (SPS) werden an das LAN angeschlossen und Kleinsteuerungen auf Basis von Embedded Systemen werden zunehmend mit LAN-Schnittstellen angeboten. Als Konsequenz daraus wächst die Datenkommunikation im Office- und Internetbereich immer weiter mit der in Industrie- und Produktionsanlagen zusammen.

Wenn in industriellen Umgebungen von Sicherheit gesprochen wird, geht es meist um Betriebssicherheit, elektrische Sicherheit, Personenschutz, 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. Um solche Bedrohungen zu entschärfen, werden fast immer IT-Sicherheitsmassnahmen aus der Office-Welt realisiert. Das kann durchaus zu neuen Problemen führen, die Wahrscheinlichkeit, dass dabei die Risiken sogar grösser als der Nutzen sind, ist erheblich.

Der Computerwurm STUXNET, von dem allgemein angenommen wird, dass er von westlichen Behörden geschaffen wurde, um in bestimmten Ländern industrielle Software anzugreifen, hat in letzter Zeit einige sehr fähige Nachkommen wie DUQU oder FLAME bekommen. Einige dieser Nachkommen sind eindeutig eine Weiterentwicklung von STUXNET, andere scheinen zumindest ähnliche Techniken zu verwenden. Je moderner und vernetzter unsere globale Gesellschaft wird und je leichter dieser schadhafte Code über das Internet verfügbar wird, je anfälliger werden industrielle Produktions- und Infrastrukturnetzwerke für Angriffe mit Hilfe solcher Schadsoftware.

Traditionelle Firewall-Systeme sind nicht für den Einsatz in industriellen Produktions- und Infrastrukturnetzwerken konzipiert, deshalb können solche Systeme diese Netzwerke nicht optimal schützen. Unsere Erfahrung zeigt auch, dass sich der Einsatz einer handelsüblichen Virenschutz-Software in solchen Umgebungen nicht bewährt. Das Verhalten solcher Systeme kann sich beim Erneuern von Virensignaturen unerwünscht verändern, dies ist vor allem bei validierten Steuerungs-Systemen nicht tolerierbar. Auf speicherprogrammierbaren Steuerungen kann eine Virenschutz-Software nicht installiert werden, zudem ist vielfach gar nicht bekannt, nach welcher Schadsoftware oder nach welchen Sicherheitsverletzungen überhaupt gesucht werden soll.

IT-Sicherheitslösungen in industriellen Produktions- und Infrastrukturnetzwerken 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
- Geringer Stückpreis

Priorität hat natürlich immer die sichere und effiziente Ausführung von Produktionsprozessen. Deshalb hat sich in der Praxis ein relativ einfaches, zweistufiges Sicherheitskonzept etabliert, mit dem ein industrielles Produktions- und Infrastrukturnetzwerk optimal geschützt werden kann.

Stufe 1: Deep Paket Inspection

Als erste Stufe im Sicherheitskonzept empfehlen wir für jedes Netzwerk oder jedes Modul eine Firewall, die den Datentransfer bis auf Layer 7 nach ISO/IEC überwacht. Eine traditionelle IT-Firewall überprüft den gesamten Datenverkehr, indem dieser mitgelesen und jede Nachricht gegen einen vordefinierten Satz von Regeln (so genannte Access Control Lists oder ACLs) verglichen wird. Mit der Hilfe dieser Access-Listen werden die Datenquelle (Source IP Address), die Datensenke (Destination IP Address), die Ziel IP Port-Nummer (Destination Port) sowie die Integrität eines Datenpakets überprüft. Die Weiterleitung von Nachrichten, die nicht mit den ACL's übereinstimmen, wird durch die Firewall verhindert. Eine detailliertere Kontrolle des Datenpakets ist jedoch nicht möglich, weil die gängigsten Industrie-Netzwerkprotokolle in sich eine ungenügende Granularität haben. Aus der Perspektive der IP Port-Nummer sieht ein Datenpaket mit Produktionsdaten meistens genau gleich aus wie ein Datenpaket für einen Firmware-Update. Wenn das Vermitteln von Datenpaketen von einem HMI an eine SPS über eine herkömmliche Firewall zugelassen ist, können auch Datenpakete für die Übermittlung eines Programmiercodes die Firewall passieren. Dies ist eine ernste Frage der Sicherheit.

Hirschmann EAGLE20 Tofino-Firewall

Das Ergebnis der Absicht, zum Beispiel Firmware-Upgrades über ein Netzwerk mit entsprechenden Firewall-Regeln zu verhindern, führt zur Sperrung des gesamten SCADA-Verkehrs. Da aber heute der zuverlässige Datenfluss innerhalb eines SCADA- Systemen entscheidend für die Funktionalität einer industriellen Produktionsanlage ist, entscheiden sich die meisten Ingenieure, den Datentransfer zu erlauben und nehmen dabei ein hohes Sichrheitsrisiko in Kauf.

Eine für ein industrielles Produktions- und Infrastrukturnetzwerk optimierte Firewall kann zum Beispiel bestimmen, ob eine Modbus- oder eine OPC-Nachricht einen Lese- oder einen Schreib-Befehl enthält und ist demzufolge fähig, alle Schreib-Befehle zu blockieren. Gute Industrie-Firewalls können auch „Plausibilitätsprüfung" durchführen, indem Verkehr für merkwürdig formatierte Nachrichten oder ungewöhnliche Verhaltensweisen (z. B. 10.000 Antwortnachrichten in Reaktion auf eine einzelne Anforderung) blockiert wird, weil diese Art von Nachrichten auf den Versuch hinweisen kann, eine SPS abstürzen zu lassen.

Diese Firewall-Technologie ist ein sehr mächtiges Werkzeug, weil es dem Ingenieur ermöglicht, ungewollten oder sogar bösartigen Datenverkehr zu blockieren, gleichzeitig aber unnötigen Einfluss des in einem SCADA-Systems notwendigen Datenverkehrs verhindert. Ohne eine solche Firewall haben die Designer von modernen Würmer eindeutig die Oberhand. Im Vorfeld der heutigen komplexen Bedrohungen ist diese Technologie aus unserer Sicht ein must-have in allen industriellen Firewalls.

Stufe 2: Virtuelle Opfersysteme

SecExtreme Industrial Honeybox

Die zweite Stufe im Sicherheitskonzept für industrielle Produktions- und Infrastrukturnetzwerke wird mit virtuellen Honeypots realsiert. Als Honigtopf oder auch englisch Honeypot wird eine Einrichtung bezeichnet, die einen Angreifer vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, den ihn sonst nicht interessiert hätte. Der Ursprung stammt aus der Überlegung, dass Bären mit einem Honigtopf sowohl abgelenkt als auch in eine Falle gelockt werden könnten. Um Angriffe auf sich zu lenken, werden in industriellen Produktions- und Infrastrukturnetzwerken virtuelle Opfersysteme (Honeypots) eingerichtet. Angreifer und Schadsoftware treffen bei ihren ersten Angriffsschritten (manuelle oder automatische Erkundung des Netzwerks) immer auf reale Systeme und automatisch auch auf diese virtuellen Honeypots. Auf diesen werden beliebige Betriebssysteme bekannter Softwarehersteller, aktive Netzwerkkomponenten oder speicherprogrammierbare Steuerungen emuliert. Deshalb sind diese für einen Angreifer zunächst nicht von realen Systemen unterscheidbar, stellen sich diesen aber in einem schlechteren Sicherheitszustand dar. Aus diesem Grund wird in den nächsten Phasen eines Angriffs die Aufmerksamkeit und somit die weiteren Aktivitäten des Angreifers oder der Schadsoftware auf den Honeypot gelenkt. Da es sich bei solchen virtuellen Honeypots nicht um reale, produktive Systeme handelt, kann bereits ein erster Kontakt mit einem solchen einen Angriff darstellen und entsprechend alarmiert werden.

Mit dem Einsatz von virtuellen Honeypots gewinnt man während eines Angriffs wertvolle Zeit, weil man einen solchen schnell feststellen und in einem ersten Schritt, um einer weiteren Verbreitung der Schadsoftware vorzubeugen, entsprechend rasch reagieren kann. Dabei sind Fehlalarme ausgeschlossen, weil die emulierten Systeme für die eingentliche Produktion nicht gebraucht und demzufolge nicht relevant sind. Um weitere Informationen über Angriffsmuster und Angreiferverhalten zu erhalten, kann bei Bedarf in einem zweiten Schritt eine genauere Analyse des Angriffs durchgeführt werden. Dies ist möglich, weil ein Honeypot die gesamte Kommunikation mit ihm lückenlos aufzeichnet und abspeichert.

Bei diesem Ansatz geht es nicht darum, einen Angriff zu verhindern, sondern möglichst zeitnah feststellen zu können, dass ein Angriff überhaupt stattfindet. Über die Erkennung und Aufzeichnung von Angriffen erhält man jederzeit einen aktuellen Informationsstand aus dem industriellen Produktions- und Infrastrukturnetzwerk. Man kann bei Angriffen zeitnah Massnahmen einleiten, um den Angriff einzudämmen, weil man in der Lage ist, infizierte Systeme schnell zu erkennen und so die Ausbreitung von Schadsoftware zu verhindern.
Unsere eigenen Erfahrungen zeigen, wie schnell und einfach nicht genügend geschützte Produktions- und Infrastrukturnetzwerke angegriffen werden können. Dabei finden nicht nur professionell durchgeführte Attacken und von langer Hand geplante Angriffe von Ausserhalb der eigenen Organisation statt, sondern es entstehen auch vermehrt ungewollte, unbewusst herbeigeführte oder durch zufällig entstandene Situationen von innerhalb potentielle Gefahrenmomente, die durch geeignete Schutzmassnahmen grösstenteils verhindert oder zumindest entschärft werden können.

DDS NETCOM AG / YELLO NETCOM GMBH
Hanspeter Weingartner
Allmendstrasse 6
CH-8320 Fehraltorf

YELLO NETCOM

YELLO NETCOM GMBH
Birkenallee 115/117
D - 48432 Rheine
Telefon +49 (0) 5971 / 96176-0
Telefax +49 (0) 5971 / 96176-25
rheine@yello-net.de

www.yello-net.de