IT-Sicherheitsmassnahmen in industriellen Ethernet-Netzwerken

Autor(en): **Weingartner, Hanspeter**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **102 (2011)**

Heft 8

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-856837

IT-Sicherheitsmassnahmen in industriellen Ethernet-Netzwerken

Optimale Sicherheit dank Einbezug aller OSI-Schichten

Auch in Produktionsumgebungen halten Ethernet und TCP/IP Einzug. Damit steigt auch die potenzielle Bedrohung durch Cyber-Attacken. Wie kann man seine Produktionsinfrastruktur optimal gegen solche Bedrohungen schützen? Welche Massnahmen sind möglich und sinnvoll?

Hanspeter Weingartner

Der Stuxnet-Virus war der erste, öffentlich bekannt gewordene Angriff auf eine IT-Infrastruktur in einer Produktionsumgebung, der ein relativ hohes Gefahrenpotenzial aufweist. Da die Automatisierungs- und Steuerungstechnik bisher weitgehend aus Systemen bestand, die untereinander mit proprietären Techniken und Protokollen kommuniziert haben, wurden solche Angriffe zwar theoretisch für möglich gehalten, sind aber in der Praxis nicht aufgetaucht. Doch auch in diesen Umgebungen hält die gegenwärtige Netzwerktechnik auf Basis von Ethernet und TCP/IP immer mehr Einzug. Zunächst werden die PC-Stationen vernetzt, danach werden die Ebenen der Leit- und Steuerungstechnik miteinander verbunden. Auch Speicherprogrammierbare Steuerungen (SPS) werden zunehmend an das LAN angeschlossen, und Kleinsteuerungen auf Basis von Embedded Systems werden standardmässig mit Ethernet-Schnittstellen angeboten.

Um die Bedrohungen in der Prozess-IT zu entschärfen, werden (fast) immer IT-Sicherheitsmassnahmen aus der Office-Welt eingeführt. Dazu gehören ein umfassendes Patch-Management für Server-Betriebssysteme, Virenschutz-Software, Firewalls sowie Intrusion-Prevention-Systeme (IPS/IDS) usw. Diese Lösungen eignen sich jedoch nur bedingt oder teilweise gar nicht für die Prozess-IT. Die Gründe dafür sind vielfältig: Vom fehlenden Know-how der Anlageverantwortlichen über den zu grossen administrativen Aufwand und über validierte Systeme, die nach der Inbetriebsetzung nicht mehr verändert werden können, bis zu wichtigem Datenverkehr, der aus prozesstechnischen Gründen nicht automatisch blockiert werden darf. Dies hat zur Folge, dass klassische IT-Sicherheitsmassnahmen in der Prozess-IT zu neuen Problemen führen und das Risiko durchaus grösser als der Nutzen sein kann.

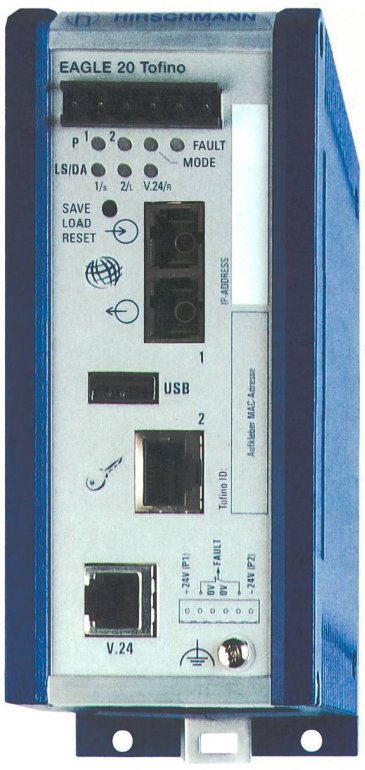
Da es in Produktionsumgebungen neben den oben erwähnten Risikopotenzialen auch um Sicherheitsbedrohungen geht, die aus Nachlässigkeit, Unachtsamkeit oder mangelndem Wissen des eigenen Personals entstehen, ist es durchaus sinnvoll, entsprechende Sicherheitsmassnahmen von der Bitübertragungsschicht (Physical Layer nach OSI-Schichtenmodell) bis zur Sitzungsschicht (Session Layer nach OSI-Schichtenmodell) zu realisieren. Aber wie wird eine IT-Infrastruktur in einer Produktionsumgebung diesbezüglich optimal und praxisgerecht geschützt?

Sicherheitsleitlinie als wichtige Basis

Als Grundlage jeder sicherheitsrelevanten Massnahme in einer IT-Infrastruktur sollte eine Sicherheitsleitlinie (Security Police) dienen. In dieser Leitlinie sollte Folgendes kurz und verständlich beschrieben sein:

- Stellenwert der Informationssicherheit.
- Bedeutung der wesentlichen Informationen und der Informationstechnik für die Aufgabenerfüllung.
- Bezug der IT-Sicherheitsziele zu den Geschäftszielen/Aufgaben der Institution.
- Sicherheitsziele.
- Kernelemente der Sicherheitsstrategie.
- Zusicherung, dass die Sicherheitsleitlinie von der obersten Leitung durchgesetzt wird.
- Zusätzliche Leitaussagen zur Erfolgskontrolle.
- Beschreibung der für die Umsetzung des Sicherheitsprozesses eingeführten Organisationsstruktur.

Die Leitlinie kann u.a. durch die Aufzählung relevanter Gefährdungen oder einzuhaltender gesetzlicher oder vertraglicher Anforderungen, die Beschreibung der Aufgaben und Zuständigkeiten im Sicherheitsprozess und die Benennung von Ansprechpartnern sowie Hinweisen auf Schulungs- und Sensibilisierungsmassnahmen ergänzt werden. Ohne dieses Dokument sind nachhaltige und sinnvolle Massnahmen für die Sicherheit der IT-



Eagle20 Tofino MM/TX ist eine Komponente eines Systems, mit dem Sicherheitszonen in industriellen Steuerungsnetzwerken realisiert werden können. Alle Systemkomponenten werden zentral mit der Tofino Central Management Plattform, einer Arbeitsplatzrechner-Software, konfiguriert, verwaltet und überwacht.

Infrastruktur schwierig bis gar nicht realisierbar, weil diesbezüglich wesentliche Absichten und Zielvorgaben der obersten Leitung einer Institution fehlen.

Sicherheitsmassnahmen

Jede Art von IT-Netzwerk ist grundsätzlich ein Risiko. Die Tatsache, dass alle eingeführten Massnahmen immer einen Kompromiss zwischen einer optimalen Verfügbarkeit durch einfache Erreichbarkeit, höchstmögliche Performance oder möglichst einfache Administration und einer optimalen Sicherheit mit Authentifizierung, Autorisierung oder dem Sicherstellen der Integrität und Vertraulichkeit aller Daten bilden, vereinfacht die Entscheidung über zu treffende Massnahmen und erhöht das Verständnis und somit die Akzeptanz für einzuführende Massnahmen bei allen Netzwerkteilnehmern. Auch die Einsicht, dass theoretisch keine technischen Massnahmen für die IT-Sicherheit notwendig wären, wenn sich weltweit alle Netzwerkteilnehmer (inkl. WWW) an Weisungen, Richtlinien, Vorschriften und Ausführungsbestimmungen halten würden, hilft bei der Einführung solcher Massnahmen. Es gibt durchaus sicherheitsrelevante Aspekte, die mittels einer Weisung oder einer Richtlinie einfacher und vor allem kostengünstiger zu realisieren sind als durch die Einführung von entsprechenden technischen Lösungen.

Bitübertragungsschicht

Bei Sicherheitsmassnahmen in der Bitübertragungsschicht geht es hauptsächlich darum, das Risikopotenzial von Bedienungs- und Handhabungsfehlern aufgrund von Irrtum, Nachlässigkeit oder fehlendem Fachwissen zu minimieren. Das ist mit sehr einfachen Mitteln möglich: Man kann nicht benutzte Ports mit einer Abdeckung mechanisch verschliessen, das versehentliche Ausstecken von falschen Patchkabeln verhindern oder durch das Abschliessen des Steuerschranks unautorisierten Zugriff auf das Netzwerk unterbinden. Solche Massnahmen sind äusserst günstig, mit einfachsten Mitteln realisierbar und mit geringstem Aufwand administrierbar. Ausserdem sind sie gegen sicherheitsrelevante Vorkommnisse ohne kriminelle Absichten äusserst wirksam.

Sicherungsschicht

Durch die Einführung von virtuellen lokalen Netzwerken (VLAN) können IT-Infrastrukturen einfach, sicher und übersichtlich segmentiert werden. So können Netzwerke mit verschiedenen Sicherheitsbedürfnissen über die gleiche physische Infrastruktur betrieben werden, was sich äusserst positiv auf die Kosten für die gesamte IT-Infrastruktur auswirkt. Die für VLAN notwendigen Parameter im Ethernet-Header der Datenpakete werden ausschliesslich von den aktiven Netzwerkkomponenten verwaltet, sodass die VLAN-Technologie für die am Netzwerk angeschlossenen Endgeräte völlig transparent ist. Mit den VLAN-Informationen werden automatisch auch Daten für die Priorisierung der Datenpakete (Quality of Service, QoS) mit in den Ethernet-Header eingefügt. Aus diesem Grund werden in der Praxis VLAN-Topologien für Video-, Voice-, Daten- und Management-Datenpakete nicht nur bezüglich Sicherheit, sondern auch bezüglich dem Priorisieren von Daten konzipiert.

Vermittlungsschicht

Durch Fehlmanipulationen wie das unbeabsichtigte Herstellen von Netzwerkschlaufen, die Vergabe von doppelten IP-Adressen oder nicht korrekten Konfigurationen der aktiven Netzwerkkomponenten können Broadcast-Stürme entstehen, die das Vermitteln von Daten von und zu Endgeräten verhindern und somit das IT-Netzwerk für den Betrieb nutzlos machen.

Das Weiterleiten solcher Broadcast-Datenpakete kann durch den Einsatz von Routern verhindert werden. Zudem können verschiedene VLAN auf dieser Schicht sicher miteinander verbunden werden, indem über Zugriffslisten auf Routern die erlaubten Verbindungen zwischen den entsprechenden VLAN definiert werden. Das Verbergen von internen Netzwerk-Strukturen gegen aussen ist eine weitere wichtige Funktion von Routern, weil man damit zum einen modulare Systemlösungen auf das Netzwerk übertragen und zum anderen den Zugriff von vielen Komponenten im Netzwerk über eine einzige Adresse gegen aussen realisieren kann.

Transport- und Vermittlungsschicht

Auf der Transport- und Vermittlungsschicht werden Firewalls für den kontrollierten Datenfluss vom bzw. zum IT-Netzwerk eingesetzt. Dabei sind die Firewalls selber transparent und können somit nicht angegriffen werden.

Es gibt Portfilter-Firewalls, bei denen einzelne TCP/IP-Ports statisch geöffnet oder geschlossen werden, und Stateful-Inspection-Firewalls, die zusätzlich durch gezielte Manipulation der TCP/

Bilder: Hirschmann

Die «Industrial Firewall» Eagle20 wird direkt an Maschinen und Anlagenteilen eingesetzt.

UDP-Session-Nummern die Integrität der übermittelten Daten sicherstellen. Da die Firewalls in vielen Fällen an der Schnittstelle zwischen dem internen Netzwerk und dem Internet stehen, werden auf diesen auch VPN-Verbindungen terminiert, die sichere Remote- oder Site-to-Site-Netzwerke via Internet ermöglichen. Diese Verbindungen sind wegen den heute verfügbaren Bandbreiten auch auf dem Mobilfunknetz via GPRS oder UMTS keine Seltenheit mehr. Die Authentifizierung, Autorisierung und Verschlüsselung von VPN-Remote-Verbindungen erfolgen via Username/Passwort (allenfalls zusätzlich mit einem Token-System geschützt, wie man es vom Internet-Banking kennt), zertifikatsbasierend oder aufgrund eines Schlüsselpaares, das zwischen den einzelnen Teilnehmern ausgetauscht wurde.

Darstellungs- und Anwendungsschicht

Die bis jetzt beschriebenen Massnahmen beziehen sich ausschliesslich auf die sichere Übermittlung von Datenpaketen und auf die Authentifizierung oder Autorisierung von Netzwerkteilnehmern. In den beiden obersten Schichten des ISO/OSI-Modells müssen Daten interpretiert werden, deshalb kommen in diesen beiden Schichten nur noch softwarebasierte Sicherheitssysteme zum Einsatz. Der Einsatz von Intrusion-Prevention-Systemen (IPS) in Netzwerk und Viren-Scannern auf Client- und Serversystemen ist heute Standard, obwohl dies in der Praxis in Produktionsumgebungen nicht immer sinnvoll oder sogar unmöglich ist. Weil industrielle Steuerungen heute über Ethernet kommunizieren, aber oft keine diesbezüglichen Sicherheitsmassnahmen möglich sind, wählt man alternative Massnahmen, um auch diese IT-Infrastrukturen zuverlässig schützen zu können. Wir verwenden für solche Bedürfnisse separate Systeme, die im IT-Netz-

Konkretes Projekt

IT-Netze bei Energieunternehmen

Wie Energieversorger IP/MPLS-Netze auch für zeitkritische Dienste nutzen können, lesen Sie im Beitrag von C. Struth und M. Maurer im nächsten Bulletin (9/2011).

werk ungenügend geschützte Rechnersysteme simulieren, um so potenzielle Angreifer anzuziehen und bei entsprechenden Vorkommnissen alarmieren zu können. Das funktioniert gut, weil bei gezielten Angriffen auf IT-Netzwerke immer zuerst festgestellt wird, wo sich leicht angreifbare Systeme befinden, um diese dann tatsächlich angreifen zu können. Durch diese passiven Systeme finden keine automatischen Reaktionen wie das Abschalten von Ports oder das Schliessen von bestehenden Verbindungen statt, die in Produktionsumgebungen fatale Folgen haben können.

Nach erfolgter Alarmierung sind manuelle Eingriffe durch das Fachpersonal notwendig. Dadurch kann sichergestellt werden, dass die Produktion nicht gestört und das kontinuierliche Weiterarbeiten ermöglicht wird. Neueste Schadsoftware wie der kürzlich bekannt gewordene «Stuxnet»-Virus können so sicher erkannt und mit entsprechenden manuellen Gegenmassnahmen eliminiert werden.

Fazit

Bei der Planung, dem Aufbau und im Betrieb einer IT-Infrastruktur in einer Produktionsumgebung ist es wichtig, sinnvolle Sicherheitsmassnahmen auf allen Schichten zu realisieren. Dabei ist zu beachten, dass die gewählten Massnahmen immer einen Kompromiss darstellen; die absolute Sicherheit kann nur dann erreicht werden, wenn die einzelnen Systeme völlig autonom arbeiten, d.h. weder vernetzt sind noch die Möglichkeit besteht, potenziell infizierbare Speicher (USB-Stick und ähnliche) anzuschliessen.

Angaben zum Autor

Hanspeter Weingartner befasst sich seit über 10 Jahren als Projektleiter mit der Planung, Realisierung und dem Unterhalt von Kunden-Netzwerken in industriellen Produktionsumgebungen.

DDS NetCom AG, 8320 Fehraltorf
hanspeter.weingartner@dds.ch

Résumé

Mesures de sécurité informatique dans les réseaux Ethernet industriel

Sécurité optimale grâce à l'intégration de toutes les couches OSI

L'utilisation croissante de l'Ethernet et TCP/IP au lieu de technologies de communication propriétaires dans les environnements industriels va de pair avec une augmentation du risque de cyberattaques. Comme base pour minimiser ces risques dans une infrastructure informatique, on devrait établir une directive de sécurité (Security Policy) définissant entre autres l'importance de la technologie de l'information pour l'accomplissement des tâches, les éléments clés de la stratégie de sécurité ainsi que la structure d'organisation requise. Pour une sécurité optimale on pourra mettre en place des mesures sur toutes les couches OSI (couche physique, liaison, réseau et d'autres). No