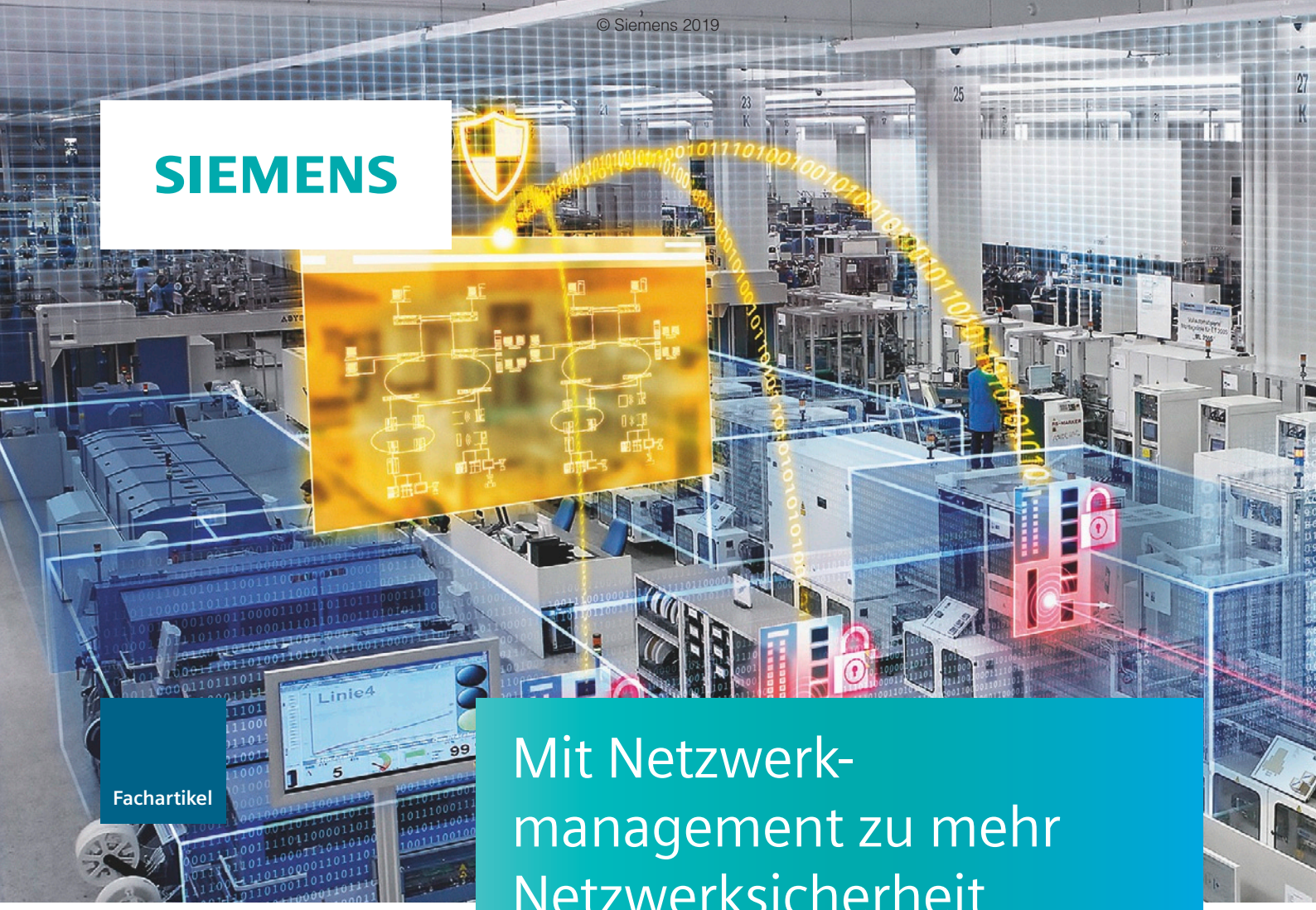
SIEMENS




Fachartikel

# Mit Netzwerk-management zu mehr Netzwerksicherheit

## Industrial Security neu entdecken

**Jedem Security-Update folgen neue Softwareschwachstellen. Jedem Schutzmechanismus neue Angriffsvektoren. Bereits seit dem erstmaligen Auftreten einer Schadsoftware besteht nun dieses Wettrennen und oft stellt sich die Frage, wie sich ein effektiver Schutz gegen das „Unbekannte" überhaupt etablieren lässt. Die Antwort darauf findet sich im nahtlosen Zusammenspiel mehrerer Maßnahmen.**

„Ooops, your files have been encrypted!" – mit diesen Worten sorgte noch vor wenigen Jahren eines der berühmtesten Schadprogramme weltweit für Schlagzeilen. Obwohl weder die Art der Bedrohung noch die verwendete Technologie von großer Innovationskraft geprägt waren, erreichte diese Malware binnen weniger Tage traurige Berühmtheit. Der eine oder andere mag sich nun vielleicht an weitere namhafte Würmer und Viren, wie Blaster, Sasser oder MyDoom erinnern, die bereits vor über 15 Jahren für Schäden in Milliardenhöhe gesorgt haben. Andere wiederum erinnern sich noch sehr deutlich an Stuxnet, der durch sein primäres Infektionsziel die Betreiber industrieller Anlagen in Atem hielt. Wenn man heute nach berühmten Schadprogrammen fragt, werden viele wahrscheinlich die Ransomware WannaCry nennen. Und das obwohl andere Würmer entweder deutlich mehr Geräte infizierten, größeren wirtschaftlichen Schaden anrichteten oder gar raffiniertere Angriffsvektoren nutzten. Was also war anders? Was verhalf WannaCry zu jener Bekanntheit?


Das tiefengestaffelte Industrial Security Konzept von Siemens bietet durch unterschiedliche Maßnahmen und Mechanismen auf mehreren Ebenen einen umfassenden und wirkungsvollen Schutz vor Cyberbedrohungen.

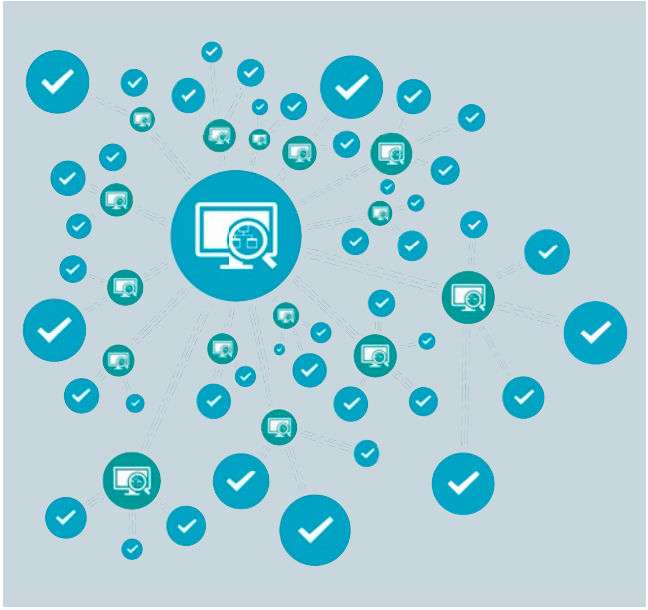
Die Beantwortung dieser Frage ist ziemlich vielschichtig. Entscheidende Aspekte waren aber wohl die rasante Ausbreitungsrate sowie die Art der infizierten Geräte. Binnen weniger Stunden breitete sich die Ransomware in über 150 Ländern auf zahlreichen Computersystemen aus und verschlüsselte die darauf abgelegten Daten. Da nicht nur Privatanwender und industrielle Unternehmen betroffen waren, sondern auch öffentliche Einrichtungen, wie Krankenhäuser oder Anzeigetafeln im Fernverkehr, legte dieser Vorfall die Angreifbarkeit unserer vernetzten Infrastruktur gnadenlos offen. Und obwohl die Ausbreitung relativ schnell gestoppt werden konnte, blieb der fade Beigeschmack jener leicht anzugreifenden Systeme sowie die Furcht vor neuen, vielleicht noch effektiveren Bedrohungen. Wie aber kann man sich nun wirkungsvoll gegen neue, heute noch unbekannte Angriffe schützen?

**Defense in Depth – Die Grundlage eines wirkungsvollen Schutzkonzeptes**

Der sicherlich wichtigste Schritt ist es, sich auch in industriellen Umgebungen mit dem Thema Cybersecurity zu befassen und die Furcht vor dem „Unbekannten" zu verlieren. So lässt sich mit professioneller Unterstützung ein wirkungsvoller Ansatz für mehr Sicherheit durch eine sogenannte tiefengestaffelte Verteidigung etablieren, die häufig auch unter dem Begriff „Defense in Depth" bekannt ist. Das Prinzip dahinter besagt, dass einem möglichen Angriff verschiedenste, unabhängig voneinander arbeitende Schutzmaßnahmen entgegengebracht werden sollen. Mit diesen soll der Angriff entweder sofort gestoppt werden oder es soll im Zusammenspiel genug Zeit für entsprechende Gegenmaßnahmen gewonnen werden.

Wenn auch die Automatisierungskomponenten bereits während deren Entwicklungsphase Security-Aspekte hinreichend berücksichtigen, kann das Konzept auf einem tragenden Fundament verankert werden. Aus diesem Grund ist der sichere Produktlebenszyklus gemäß IEC 62443 bei Siemens Digital Industries fester und zertifizierter Bestandteil des Entwicklungsprozesses. Da diese Prozessanforderungen und das Konzept der tiefengestaffelten Verteidigung inklusive der gängigen Mechanismen wie Firewalls oder weiterführender Anwendungen zur Angriffserkennung im Standard IEC 62443 beziehungsweise in einschlägiger Literatur bereits ausführlich beschrieben sind, soll an dieser Stelle auf eine detaillierte Auflistung der Möglichkeiten verzichten werden. Der Fokus soll stattdessen auf ein Szenario gelegt werden, das zeigt, mit welchen Mitteln zusätzlich gearbeitet werden kann, um Produktionssysteme vor neuen, bisher unbekannten Angriffswellen zu schützen.

Obwohl über alle möglichen Angriffsvektoren und ausnutzbaren Schwachstellen heute maximal spekuliert werden kann, werden einige Aspekte im zeitlichen Verlauf der meisten Angriffswellen weiterhin einem bekannten Muster folgen. Nachdem erste Infektionen sehr überraschend zugeschlagen haben, werden Security-Experten weltweit aktiv, beginnen das Verhalten und die Funktionsweise der Schadsoftware so schnell wie möglich zu analysieren und leiten wirkungsvolle Gegenmaßnahmen ein. Diese reichen zum Beispiel von ersten Empfehlungen zum Eindämmen infizierter Systeme, über neue Signaturen für Virenscanner oder Deep-Packet-Inspection-Firewalls bis hin zu Security-Updates betroffener Anwenderprogramme.



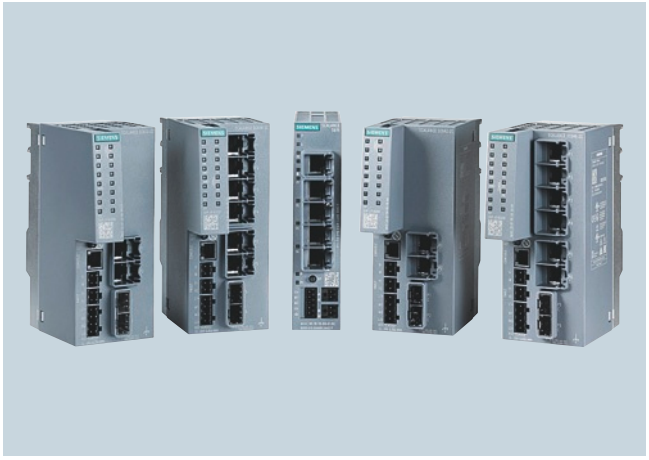
Transparenz und detaillierte Informationen über die Teilnehmer eines Netzwerkes sind ein Schlüsselfaktor, um Security-Maßnahmen effektiv und zielgerichtet einsetzen zu können.

Da jene spezifischen Gegenmaßnahmen jedoch erst ausgerollt werden können, nachdem die Schadsoftware erkannt und analysiert wurde, wird weiterhin daraufgesetzt, die Erstinfektion mit den bereits vorhandenen Maßnahmen der tiefengestaffelten Verteidigung abzuwehren. Bevor sich das Angriffsmuster nun verändert, wie es bei sogenannten polymorphen Angriffen gängig ist, oder falls es trotz präventiver Schutzmechanismen zu einer Infektion einzelner Systeme gekommen ist, sollten lokale Ausbreitungswege unterbunden und genutzte Schwachstellen dauerhaft geschlossen werden. In beiden Fällen zeigt die Verwendung eines zentralen Netzwerk-Management-Systems (NMS) deutliche Vorteile und hilft dabei die dafür nötige Transparenz im Netzwerk zu erreichen.

**Verwundbarkeiten identifizieren - Kommunikation kontrollieren**

Nach den ersten Analysen der Security-Experten veröffentlichen renommierte Produkthersteller wie Siemens entsprechende Security-Alerts, die darüber informieren, ob Produkte von einer Schwachstelle betroffen sind. Unter Zuhilfenahme des Netzwerk-Management-Systems lassen sich im ersten Schritt die Assets – die Komponenten und Teilnehmer des Netzwerkes – ohne großen Aufwand auflisten und mit den Informationen der Security-Alerts abgleichen. Bei möglichen Übereinstimmungen können nun weitere Eindämmungsmaßnahmen im Produktionsnetzwerk ergriffen werden, bis Security-Updates der Produktlieferanten für die betroffenen Komponenten letztlich zur Verfügung stehen.

Die identifizierten, angreifbaren Komponenten müssen besonders vor der Bedrohung geschützt werden, indem die Ausbreitung der Schadsoftware über offene Ports diverser Protokolle und Netzwerkdienste im lokalen Netzwerk eingeschränkt wird. Folglich wäre der nächste Schritt, jene Protokolle und Netzwerkdienste durch Firewalls zu blockieren. Während sich dieses Vorgehen am Zonenübergang von der Büro- zur Fertigungsumgebung noch relativ mühelos umsetzen lässt, zeigt sich bereits an den Zellenfirewalls eine gewisse Komplexität. Die zusätzlichen Regeln müssen an vielen Firewalls angewendet werden und dürfen bei einigen Zellen gegebenenfalls nur temporär oder gar nicht aktiv geschaltet werden, um den Produktionsprozess nicht zu beeinflussen. Möchte man zudem als weitere Maßnahme auch sekundäre Systeme wie Archivierungsserver im Rahmen einer Notfall-Policy zeitweise komplett vom Anlagennetzwerk trennen, indem neben den Ports ganze Schnittstellen am Switch oder Router deaktiviert werden, wird das Ausmaß der Komplexität schnell deutlich. Kombiniert man aber Firewall- und Netzwerkmanagement in einem einzelnen System, bieten sich dem Anwender einfache und flexible Varianten, die Kommunikationsbeziehungen zwischen den Netzwerkzellen zu begrenzen und die Produktion mit, zum Beispiel eingeschränkten Diagnose- oder Zugriffsmöglichkeiten, weiterhin am Laufen zu halten.



Mit einem Zellenschutzkonzept und mit SCALANCE S Industrial Security Appliances lassen sich einzelne Produktionsbereiche effektiv vom Anlagennetzwerk trennen und schützen.

## Security-Updates – Ein Muss für langfristigen Schutz

Für einen nachhaltigen Schutz müssen die angreifbaren Komponenten letztlich dauerhaft vor dieser spezifischen Bedrohung geschützt werden. Dazu müssen die von den Herstellern bereitgestellten Software- und Firmwareupdates zeitnah eingespielt werden. Je nach Netzwerk- und Systemarchitektur kann dies bereits während des laufenden Betriebs oder in einem Wartungszyklus der Produktion erfolgen. In beiden Fällen kann das mit enormen Aufwänden verbunden sein. Bei Computersystemen in geschlossenen Domänen hat sich daher eine zentrale Variante über sogenannte Updateserver etabliert. Um diese Vorzüge ebenso bei industriellen Infrastrukturkomponenten wie Switches, Router oder Firewalls genießen zu können, bedarf es erneut eines zentralen Netzwerkmanagements, mit dem Firmwareupdates zentral eingespielt werden können.

Ist die Schwachstelle auf allen Komponenten behoben, können die zuvor gesetzten restriktiven Firewall-Regeln und die abgekoppelten Systeme wieder in den normalen Betrieb zurückgesetzt werden. Dadurch kann das gesamte Produktionsnetzwerk wieder im vollen Umfang mit Datenarchivierungen oder weiterführende Diagnosen wie gewohnt genutzt werden. Reflektiert man die gewonnen Erkenntnisse auf die Verbreitung von WannaCry, erkennt man sehr deutlich das Potential eines Netzwerk-Management-Systems. Während die Erstinfektion zwar nicht verhindert worden wäre, hätte die Ausbreitung im lokalen Netzwerk im Vorfeld soweit eingedämmt werden können, bis das bereits vorhandene Security-Update auf verwundbaren Systemen ausgebracht worden wären.

Ein modernes Netzwerk-Management-System steht also nicht nur für rein administrative oder diagnostische Einsatzzwecke. Vielmehr unterstützt es ebenso im Rahmen einer tiefengestaffelten Verteidigung und im Zusammenspiel mit Firewalls und weiteren Security-Komponenten die Anlagenverfügbarkeit auch in Bedrohungslagen aufrechtzuerhalten. Gerade vor dem Hintergrund kontinuierlich zunehmender Cyberangriffe und stetig variierender Angriffsszenarien kann ein Netzwerk-Management-System den entscheidenden Vorteil bieten. Als kompetenter Partner für industrielle Kommunikation und Industrial Security unterstützt Siemens mit umfassenden Beratungsleistungen, integrierten Lösungen und durchgängigen Konzepten, Produktionsnetzwerke auch gegen künftige Bedrohungen zu rüsten.

Weitere Informationen zu Industrial Security:
**www.siemens.de/industrial-security**

Weitere Informationen zu Netzwerk-Management:
**www.siemens.de/sinec-nms**

## Securityhinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts. Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter
**https://www.siemens.com/industrialsecurity**

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Fachartikel
DI-PA-18/19-16
PDF 1219 4 De
Produced in Germany