Gute Zeiten, schlechte Zeiten

Cybersicherheit durch situationsabhängige Steuerung des Datenverkehrs in Prozessanlagen

Grundsätzlich wollen wir in Kommunikationsnetzwerken der chemischen Produktion produktivitätssteigernde Kommunikation zulassen und in Zukunft noch deutlich steigern. Aber: Je mehr Kommunikation wir zulassen, desto höher ist die Wahrscheinlichkeit, dass auch maliziöse Kommunikation stattfindet. Hier kommt die Kommunikationssteuerung ins Spiel.

Schadkommunikation kann zufällig – also durch menschliche oder technische Fehler – oder zielgerichtet durch einen Cyber-Angriff ausgelöst werden. Kurz gesagt steigern wir mit jeder neuen Kommunikationsverbindung die Exposition gegenüber produktivitätssenkenden Ereignissen. Virtualisierung und Cloudifizierung verschärfen diesen Trend noch weiter. Wie lösen wir dieses Dilemma?

Heute bieten sich Maßnahmen wie Zugriffsschutz, Verschlüsselung, Firewalls, Patchen, Virenscanner sowie Kommunikationsüberwachung an. Der Einsatz dieser Schutzfunktionen mindert zweifelsohne die Wahrscheinlichkeit eines Schadenfalls. Komplexität und Aufwand für deren professionellen Betrieb sind jedoch enorm hoch und das verbleibende Restrisiko immer noch signifikant. Wer es nicht glaubt, informiere sich bei den – teilweise sehr renommierten und durchaus gut geschützten – Opfern von WannaCry, NotPetya und Co. Mehrere Unternehmen meldeten ein Schadensausmaß von mehr als 300 Mio. EUR. Gerichtsprozesse zwischen Anlagenbetreibern und nicht zahlungswilligen Versicherungen laufen noch.

Die Cybersecurity-Leut' haben das Prinzip der tiefengestaffelten Verteidigung (Defense in Depth) von den alten Rittersleut' übernommen. Das Konzept der „Communication Control" soll zukünftig auch das Prinzip der Situationsabhängigkeit (großes Tor / kleines Tor) nachahmen.

Fortsetzung auf **Seite 22** ▶

Je mehr Kommunikation wir zulassen, desto höher ist die Wahrscheinlichkeit maliziöser Kommunikation.

Erwin Kruschitz, CEO, Anapur

© anapur

Immerhin bringt jedes Schadensereignis einen positiven Effekt mit sich: Genauso, wie heute niemand mehr bezweifelt, dass eine Feuerwehr notwendig ist, lernen wir zu akzeptieren, dass uns selbst die besten Schutzfunktionen in der digitalen Welt nicht unverwundbar machen. Wir müssen lernen, mit Cyber-Ereignissen zu leben und angemessen damit umzugehen.

Der Kommunikations-Notfall

In einer Kommunikationsnotsituation wie bspw. beim Befall mit einer Verschlüsselungssoftware möchte man ähnlich wie bei einem roten Pilztaster – dem Not-Aus – in den „sicheren Zustand fahren", um die Ausbreitung der Malware einzudämmen und gleichzeitig die Kontrolle über das Geschehen zu behalten. Dies sollte

- sehr rasch,
- möglichst einfach,
- mit sehr klar definierter Auswirkung auf die Kommunikationsströme,
- durch entscheidungsfähiges Personal (z.B. durch den Betriebsleiter und nicht durch den Firewall Administrator) geschehen.

Stand der Technik heute ist im besten Fall, dass in einem Kommunikationsnotfall Netzwerkgeräte von Netzwerkspezialisten umkonfiguriert oder Kabelstecker gezogen werden. Das geht üblicherweise nicht rasch und nicht einfach. Darüber hinaus sind die Auswirkungen auf den Weiterbetrieb der Anlagen und Produktionsprozesse häufig schwer absehbar. Betriebsleiter, Standortleiter, Unternehmensleitung sehen sich folgenreichen Fragestellungen und ungewohnten Gesprächspartnern gegenüber: Security Operation Center, Cyber-Forensikern, IT-Netzwerkbetreibern und – nicht zuletzt – Behörden. In vielen bisher bekannt gewordenen Fällen wurden Anlagen, Standorte und ganze Unternehmen heruntergefahren, um dann in wochen- und monatelanger Arbeit wieder hochgefahren zu werden.

Cyber-Not-Aus

Brauchen wir zur Beherrschung solcher Situationen den Cyber-Not-Aus? Eigentlich schon. Diese Funktion im Sinne eines Tasters zu sehen, der sämtliche Kommunikation kappt, ist aber in vielen Fällen zu kurz gesprungen. Ein Cyber-Not-Aus als gesamtheitliches Konzept erscheint schon eher das Mittel der Wahl zu sein. Ein Konzept, das Funktionen identifiziert, die im Notfall aufrechterhalten werden müssen und entsprechende Kommunikation, die dazu stattfinden muss, und umgekehrt Kommunikation zu definieren, die dann nicht mehr stattfinden soll.

Die alten Rittersleut' haben sich durch Wälle, Burggräben und Mauern vor Feinden geschützt. In Friedenszeiten wurde der Verkehr über Zugbrücken und Tore gesteuert. Nachts konnte man nur durch eine kleine Tür passieren. Denn große Fuhrwerke mit potenziell gefährlichem Inhalt (á la Trojanisches Pferd) müssen normalerweise nicht passieren. Passanten werden einzeln überprüft. Tagsüber an Markttagen und nur in Friedenszeiten wird das große Tor für die Marktlieferanten mit ihren Pferdefuhrwerken geöffnet. In Krisenzeiten wird über das Schließen der Tür hinaus noch eine Zugbrücke hochgezogen.

Wir müssen lernen, mit Cyber-Ereignissen zu leben und angemessen damit umzugehen.

Felix Kahrau, Senior OT Security Engineer, Anapur

© anapur

Im Gegensatz zu dieser flexibel einsetzbaren Tür sind aktuelle Firewalls kaum anpassungsfähig. Die Regeln der Firewall definieren was durchgehen darf und das wird dann auch tatsächlich durchgeleitet – jederzeit. Was jedoch in der industriellen Kommunikation durchgehen soll und was nicht, hängt sehr stark davon ab, in welcher Situation sich die Anlage gerade befindet. Im Stillstand oder einer Wartungssituation ist ganz andere Kommunikation notwendig als im laufenden Betrieb und im Cyber-Notfall sieht es wiederum ganz anders aus.

Wo stehen wir heute?

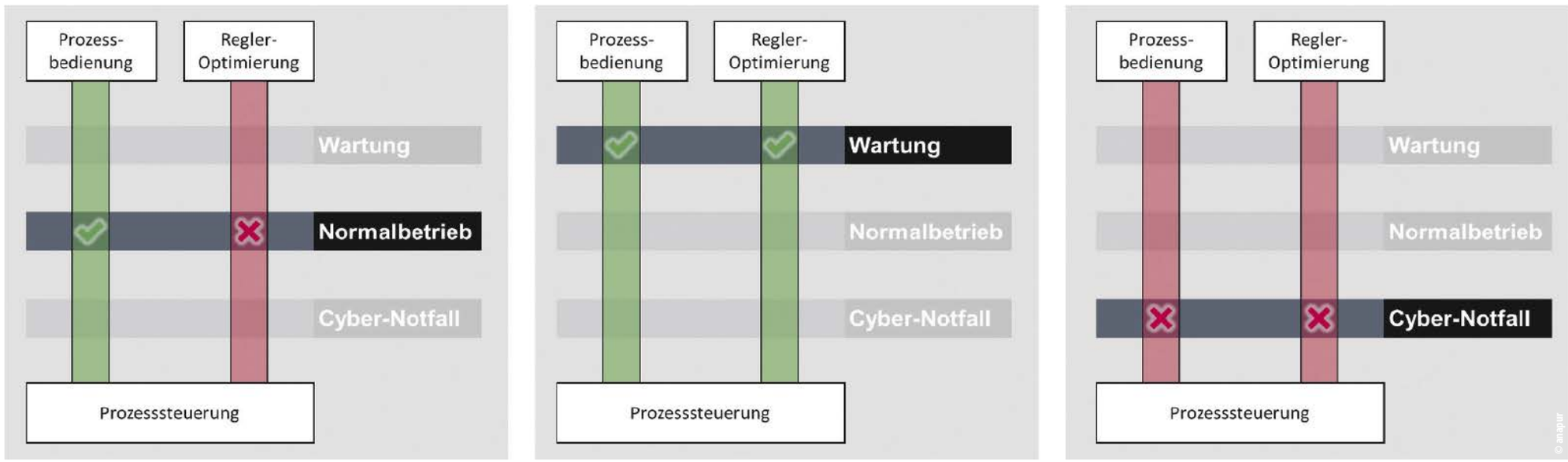
Die Cybersecurity – Leut' haben sich das Prinzip der tiefengestaffelten Verteidigung aus dem ritterlichen Verteidigungsgebrauch ausgeliehen. Im Cyber-Fachjargon spricht man von Defense in Depth, von Segmentierung, Firewalls und demilitarisierten Zonen. Das oben beschriebene Prinzip der Situationsbezogenheit wurde von der Cybersecurity Community noch nicht adaptiert. Sollte es aber.

Kommunikation steuern statt abschalten

Damit die Vorteile der Digitalisierung nicht durch Cyber-Zwischenfälle zunichte gemacht werden, müssen wir sie zunächst einmal „rückwärts denken", um sie vorwärts zu bringen. Wir stellen uns vor, wie es ohne Vernetzung aussehen würde bzw. vor der Vernetzung ausgesehen hat. Konkreter: Welche Funktionen müssen in welcher Situation zuverlässig arbeiten?

Gute Zeiten, schlechte Zeiten

◀ Fortsetzung von **Seite 21**



Mit der Steuerung seiner Kommunikationskanäle (Communication Control) kann der Betreiber einer verfahrenstechnischen Anlage bei einem Sicherheitsvorfall die Schadensauswirkung deutlich begrenzen.

Welche Kommunikationsstränge sind in der betreffenden Situation für die korrekte Ausführung dieser Funktion notwendig? Und umgekehrt: Welche Kommunikationsstränge sind in der entsprechenden Situation nicht essentiell und können somit unterdrückt werden? Diese Betrachtungsweise kann – und soll – ohne IT- bzw. Automatisierungs-Know-how durchgeführt werden. Es geht dabei primär um die Funktion und nicht um das Gerät, das System oder die Softwareapplikation, die diese Funktion ausführt. Mit der Steuerung seiner Kommunikationskanäle (Communication Control) kann der Betreiber einer verfahrenstechnischen Anlage bei einem Sicherheitsvorfall die Schadensauswirkung deutlich begrenzen.

Die feingranulare Steuerung und Überwachung von Kommunikationsbeziehungen kann darüber hinaus auch genutzt werden, um aktiv auf Sicherheitsvorfälle zu reagieren und z.B. im Fall des Bekanntwerdens einer kritischen Schwachstelle oder eines vermuteten Angriffs Kommunikationsmöglichkeiten an diese Situation anzupassen und das Automatisierungssystem situativ abzusichern. Rein organisatorisch findet eine „Emanzipation" des Bedieners statt, d.h. im Falle eines Sicherheitsereignisses wird nicht der Firewall Administrator aus dem Bett geholt. Der Betriebsleiter drückt den „Knopf" und weiß dann auch genau, was dieser bewirkt.

Welche Einsatzfälle sollen beherrscht werden?

Analog zu Friedens- und Kriegszeiten bei den Rittersleut' kennen wir heute verschiedene Stufen der Unsicherheit. Im harmloseren Fall wie aktuell mit „Log4j" wird eine Schwachstelle in einer weit verbreiteten Softwarebibliothek bekannt. Da muss zunächst nicht viel mehr getan werden, als die Aufmerksamkeit der Security Leute zu erhöhen. Niemand wird wegen einer „Ungewissheit" seine Produktion herunterfahren. Je nach Risikoeinschätzung wird man in solchen Fällen in Betracht ziehen „riskante Kommunikationsströme" wie z.B. Konfiguration/Engineering zu unterbinden oder zumindest deren Freischaltung nur mit höheren Zugriffsrechten erlauben.

Am anderen Ende der Skala wäre der Krisenfall in einem OT System, wenn z.B. an der Integrität des Automatisierungssystems gezweifelt werden muss durch Fehlfunktion einer Komponente, Fehlkonfiguration eines gutmeinenden Kollegen, durch Ransomware oder durch einen vorsätzlichen maliziösen Angriff. In diesem Fall möchte man Kommunikationsströme unterbrechen. Und zwar rasch und mit klar absehbaren Auswirkungen auf die Produktionsanlage. Es wird aber auch Kommunikationsströme geben, die man gerade in einer solchen Situation zulassen möchte. Dies gilt bspw. für Diagnosefunktionen. Kritische Kommunikationsströme, wie z.B. die Brückung von Verriegelungen möchte man ggf. sogar zurücksetzen und entsprechende Rücksetzbefehle aussenden.

Umsetzung in neuen Technologien

Nun stellt sich die Frage, wer bzw. welches Gerät die Communication Control durchführen soll. Der Einbau einer weiteren Komponente (als dynamische Firewall) ins Netzwerk wäre denkbar, aber vermutlich nicht die beste Lösung. Logischer scheint die Aufrüstung vorhandener Konzepte und Lösungen um den Aspekt der situationsbasierten Kommunikationssteuerung. Im Folgenden sind drei mögliche Umsetzungsvarianten beschrieben.

Für den Fall, dass ein Automatisierungssystem zukünftig mit NAMUR Open Architecture (NOA) kommuniziert, gibt es aktuell die Vorstellung eines „Verification of Request (VOR). Die exakte Ausgestaltung dieser Funktion ist noch nicht erarbeitet. Jedenfalls erscheint VOR prädestiniert dafür, ein situationsbasiertes Konzept umzusetzen.

Noch naheliegender ist die Umsetzung der situationsbasierten Kommunikationssteuerung in modularen Anlagen. Im Gegensatz zu monolithischen Anlagen wird die Segmentierung der Kommunikation bei modularen Anlagen bereits durch die mechanisch-verfahrenstechnische Abgrenzung vorgegeben. Aus der Sicht eines Moduls sind sowohl die Kommunikationsströme als auch die Kommunikationssituationen klar ausgeprägt und durch das Konzept der situationsbasierten Kommunikationssteuerung gut beherrschbar.

Beinahe zwingend ist die Umsetzung situationsbasierter Kommunikationssteuerung in Cloud-Anwendungen. Das Edge Device – das Gerät an der Grenze zwischen Produktionsanlage und Cloud – bildet die Schnittstelle an der der Betrieb selbst entscheidet, welche Kommunikationsflüsse er in der jeweiligen Situation zulässt und welche nicht.

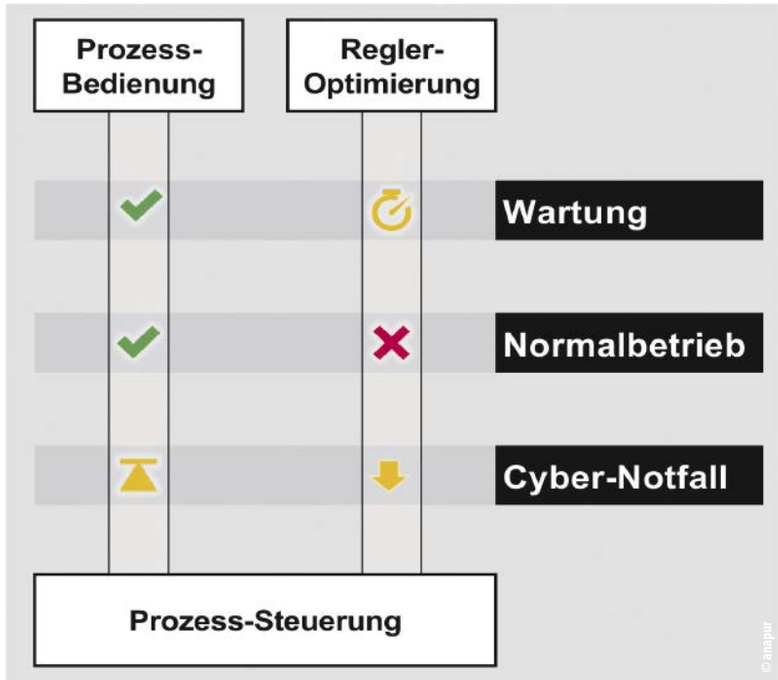
Komplexität und Skalierbarkeit

Damit sich die Regeln nicht zu einem kryptischen Firewall-Rätsel weiterentwickeln ist ein längst fälliger Schritt notwendig: Es müssen klare, transparente und – besonders für größere Anlagen – skalierbare Kommunikationsregeln geschaffen werden, die von den technischen Parametern (z.B. IP-Adressen, Ports, Paketinhalten etc.) entkoppelt werden.

Die Automatisierungstechnik der letzten 30 Jahre bediente sich der Technologien, die im Office-Umfeld weite Verbreitung erlangt und sich dort bewährt haben. Die in der Produktion im Fokus stehende Machine-to-Machine-Kommunikation hat eine spezielle Ausprägung: Die Kreativität und Vielfalt von Maschinen und deren Kommunikation kann, darf und soll limitiert sein. Entsprechend können, dürfen und sollen wir die die Kommunikation auch entsprechend limitierend steuern. Und genauso wie die alten Rittersleut' irgendwann zu moderneren Verteidigungsstrategien übergegangen sind, werden wir das auch in der Informationstechnologie für verfahrenstechnische Anlagen tun.

Erwin Kruschitz, Vorstand, und Felix Kahrau, Senior OT Security Engineer, Anapur AG, Frankenthal

- e.kruschitz@anapur.de
- www.anapur.de



Das Instrumentarium zur situationsabhängigen Steuerung der Kommunikationsströme (Communication Control) umfasst auch Operationen wie die Kommunikation in nur eine Richtung (Diodenfunktion), eine erzwungene Kommunikation oder eine zeitlich oder im Datenvolumen limitierte Kommunikation.