Wenn es kritisch wird

Ganzheitliche Lösungskonzepte und Betriebsprozesse durchsetzen

Reinhard Wegener

„Kritisch" ist ein alarmierendes Wort und bedeutet nicht allein „entscheidend" im Fall einer kritischen Infrastruktur, sondern assoziiert auch schnell eine gewisse Fragwürdigkeit in Bezug auf ihren Zustand. Ob zu Recht oder zu Unrecht hängt in erheblichem Maße von der Sicherheit der Vernetzung ihrer Betriebsmittel und ihren IT-Systemen ab.

Betreiber einer kritischen Infrastruktur (Kritis), wie Energieversorgungs-, Transport- und TK-Unternehmen fallen unter das IT-Sicherheitsgesetz, das im Sommer 2015 verabschiedet wurde und diese spätestens 2017 zwingt, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Das Gesetz regelt außerdem die Einbringung branchenspezifischer Sicherheitsstandards und Meldepflichten bei Sicherheitsvorfällen.

Damit sind auch gesetzgeberisch die Prozesse, die im Bereich der Unternehmens-IT seit längerem entwickelt und durch die Einführung eines IT-Sicherheitsmanagementsystems umgesetzt und überwacht werden, bei den Kritis-Betreibern als verbindliche Vorgaben angekommen. Die rasante weitere Vernetzung von technischen Betriebsmitteln in Kombination mit dem Einsatz üblicher IT-Techniken sowie der IoT-Ansatz (Internet of Things) führen zu einer neuen Dimension von Abhängigkeiten der Kritis von ihren Datenkommunikations- und Datenverarbeitungssystemen.

Zwar setzen viele Infrastrukturbetreiber auf eigene, autarke WANs (Wide Area Networks) verschiedenster Techniken, um die betriebsrelevanten Daten zu übertragen und ihre primäre Infrastruktur (Straße, Schienenweg, Verkehrsknotenpunkt, Kraft- und Umspannwerk) zu überwachen und zu steuern. Dennoch sind sie verstärkt mit spezifischen und neuartigen An- und Herausforderungen an die bereitzustellende IKT-Lösung konfrontiert.

Ganzheitliches Lösungskonzept und Design

Als technischer Partner ist man meist der Erwartung ausgesetzt, dass die Sicherheit des Netzes und der darüber vernetzen Anwendungen durch spezifische Techniken geschaffen werden muss. Selten sind es jedoch nur technische Maßnahmen oder spezialisierte „Sicherheitsprodukte", die im ersten Schritt ausschlaggebend sind.

Bewährt und sinnvoll ist zunächst die Definition des individuellen Schutzbedarfes, der Schutzziele und die Identifikation der relevanten Bedrohungen und Risiken. So wird es möglich, zunächst einmal die Anforderungen in das richtige Verhältnis zueinander zu setzen, bevor eine technische Empfehlung ausgesprochen wird.

Viele große regionale oder bundesweite Betreiber weisen unabhängig vom IT-Sicherheitsgesetz bereits umfangreiche und gefestigte Prozesse auf oder besitzen Unternehmens- oder branchenspezifische Anforderungs- und Maßnahmenkataloge. Als wichtigste Schutzziele werden in diesen oft Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität, auch Verbindlichkeit genannt. Einige Aspekte zu deren Sicherstellung sollen beispielhaft betrachtet werden.

Verfügbarkeit war schon immer ein bedeutsames Schutzziel bei Betriebsnetzen und damit ein zentrales Designkriterium für WAN-Strukturen. Vielfach hängt die Sicherheit von Anlagen oder Personen von diesen Netzen ab. Geeignete und aufeinander abgestimmte Redundanzmechanismen oder funktional höherwertige Systemtechnik tragen zur Zielerreichung bei. Unnötige Komplexität sollte vermieden werden, und die Netzstruktur einfach zu betreiben sein. Dies gilt ebenso für die Planung des Umgangs mit Fehlern und Störungen, die im Vorfeld im Rahmen von Havarieübungen erprobt werden sollten.

Technische Maßnahmen wie vorausschauendes Monitoring und organisatorische müssen ineinandergreifen. Parallel zum Technik- sollte daher das Betriebskonzept entwickelt werden.

Dr. Reinhard Wegener ist Leiter Technology Center bei der Telent GmbH in Backnang

Je stärker man sich der „produzierenden Infrastruktur“ nähert, desto mehr trifft man auf Protokolle, die für Effizienz und Echtzeitfähigkeit, aber nicht für IT-Security optimiert sind. Kritis sind vielfach Produktionsnetze, die sich jedoch nicht auf die Größe einer abgeschlossenen Fabrikhalle beschränken, sondern über weite Strecken verteilt sind.

Sicherheitsmaßnahmen, die in der Office-IT selbstverständlich sind, greifen hier nicht immer – Alternativen sind notwendig. Auch muss trotz aller Potenziale der Digitalisierung die Frage erlaubt sein, wo Vernetzung insbesondere über Integritätsbereiche hinweg tatsächlich erforderlich ist oder nur vorgenommen wird, „weil es geht“ oder weil aus der Vielzahl von Kommunikationsoptionen keine rigide Auswahl getroffen und verzichtbare Protokolle abgeschaltet wurden. An dieser Stelle werden wichtige Weichen für die System- und IT-Sicherheit gestellt.

Ein weiteres, spezielles Erfahrungsgebiet stellt die Konzeption und Realisierung von „Carrier-Grade“-Netzmanagementsystemen und dem dafür erforderlichen eingebetteten oder dedizierten Managementnetz dar. Üblicherweise stellt es einen eigenen Integritätsbereich, sozusagen die kritische Infrastruktur, für das Betriebsnetz des Betreibers einer Kritis dar und ermöglicht ein zuverlässiges Monitoring des Betriebszustands sowie die Netzsteuerung durch das Betriebspersonal.

Zusätzliche Brisanz gewinnt dieser Netzabschnitt durch Trends wie SDN (Software Defined Networking), die eine erhöhte Abhängigkeit von Softwarefunktionen auf einer zentralisierten IT-Infrastruktur mit sich bringen.

Telent hat eine große Zahl von Kunden über die gesamte Entwicklung ihrer Managementnetze planerisch und in der Umsetzung begleitet. Nach wie vor sind hier Spezialkenntnisse erforderlich, die über standardisierte Konzepte hinaus und weit hinein in die Besonderheiten von heterogenen Protokollwelten und Herstellerimplementierungen reichen. Oft ist die Erarbeitung von Planungsgrundlagen nur im Referenzlabor möglich.

Die zentralen Netzmanagementsysteme haben schon vor Jahren den Weg in die Rechenzentren und konsolidierten IT-Backoffice-Umgebungen der Betreiber angetreten und wurden früh als besonders schutzwürdig eingestuft. Gehärtete Konfigurationen im Sinne von restriktiver Softwareauswahl und Systemeinstellungen sind hier auch bei überwiegendem Linux-Einsatz Pflicht.

Fernwartungszugänge zeigen, dass das eigentlich „Unmögliche“ aus Gründen der Reaktionszeit bei erträglichen Kosten eben doch getan werden muss: Die Schaffung eines Zugangs zu hochgradig schutzwürdigen Systemen über öffentliche oder nur bedingt kontrollierbare Netze oder via Internet. Auch hier weisen Betriebsnetze je nach zu wartenden Systemen fallweise Besonderheiten auf (BSI-CS-108: Fernwartung im industriellen Umfeld).

Große Betreiber haben eine entsprechende Fernwartungslösung üblicherweise implementiert und vereinbaren mit Integratoren eine Zugangsart, gemäß ihren eigenen Richtlinien. Telent betreibt ihrerseits eine zertifizierte Remote-Access-Infrastruktur, die u.a. die strikte Separierung der Fernwartungs-Clients verschiedener Kunden erlaubt,

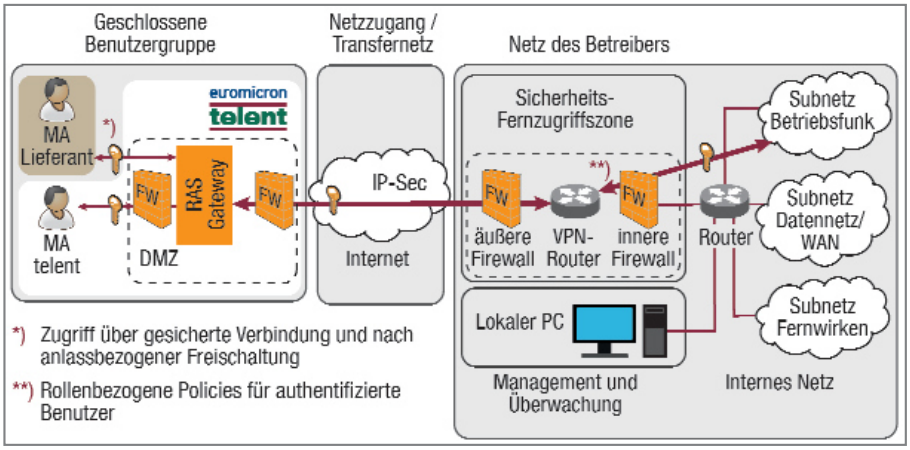

Bild 1: Typisches Fernzugriffsszenario

und kann sich auf alle geforderten Zugangsarten einstellen. Kleinere Betreiber nutzen diese Erfahrung beim Ausbau ihrer eigenen Zugänge. Lösungsdesign und Umsetzung erfolgen konsequent unter Berücksichtigung einschlägiger Empfehlungen und bei Bedarf auch unter Einbeziehung spezialisierter Partner. Eine Begutachtung durch Dritte kann eine ergänzende Maßnahme sein. Ein typisches Fernzugriffsszenario zeigt *Bild 1*.

Gerade für Fernwartungszugänge – wie für die gesamte Netz- oder Applikationslösung – besteht die betriebliche Aufgabe darin, das initiale Sicherheitsniveau aufrechtzuerhalten.

Übergang in den Betrieb

Der erfolgreiche Übergang einer Netz- oder Softwareapplikationslösung in den Betrieb setzt unter den Anforderungen eines IT-Sicherheitsmanagements voraus, dass alle beteiligten Partner eine gemeinsame Sicht auf die damit verbundenen Aufgaben haben. Diese sollten sich an den ITIL-Grundsätzen (IT Infrastructure Library) ausrichten und zwar auch für solche Komponenten, die man bislang TK- und weniger IT-Systemen zugeordnet hätte.

Man ist also gut beraten, eine exakte und vollständige Prozessvorstellung zu entwickeln, wie Betreiber und Dienstleister zusammenarbeiten wollen. Der technische Dienstleister wird hierbei aus Sicht des IT-Sicherheitsmanagements mit seinen Systemen und seinen handelnden Mitarbeitern zum Teil des Systemverbundes (*Bild 2*).

Auch wenn Teile des Betriebes fallweise an Dritte ausgelagert werden, verbleibt doch die Verantwortung für die Kritis beim Betreiber derselben. Der Integrator erbringt seine Leistung im Rahmen eines sog. „Underpinning Contract“ im Sinne von ITIL. Derartige Vereinbarungen fallen zwischen Systemintegratoren und ihren Kunden deshalb inzwischen umfangreicher und komplexer aus als klassische, reaktiv ausgelegte Support-Verträge.

Zahlreiche Aspekte eines ganzheitlichen Sicherheitskonzeptes betreffen beide Vertragspartner, vom Schulungsstatus der Mitarbeiter bis zum sicheren Austausch und Zugriff auf System- und Gerätepasswörter.
An dieser Stelle sollten vom Integrator bereits erarbeitete und wiederholt bereitgestellte Betriebsprozesse rund um die Systemtechnik auch ein Auswahlkriterium des Betreibers für die einzusetzenden Produkte sein.
Wichtig ist vor allem das Bewusstsein, dass mit dem Übergang in die produktive Nutzung die Infrastruktur (ob Netz, Applikation oder ein komplettes IT-gestütztes Verfahren) zu leben und sich zu verändern beginnt. Dies betrifft Updates, insbesondere Sicherheitsupdates, Konfigurationsänderungen, gewünschte Änderungen und Erweiterungen der Funktion. In der Vergangenheit traf man eher auf einen statisch getriebenen und auf einzelne Projektbudgets angelegten Zyklus aus Planung, Aufbau und Betrieb (im Sinn einer Entstörung). Dieser statische Ablauf weicht nun einer kontinuierlichen Aktualisierung der Systeme. Erforderlich machen dies schon die in die im Vergleich zu sonstigen Betriebsmitteln (Sensoren, Mess- und Schaltvorrichtungen usw.) dramatisch kürzeren Produktzyklen von IT-Hardware und insbesondere IT-Software.
Spätestens mit der somit unausweichlichen Einführung von Prozessen wie Incident- oder Change-Management wird eine elektronische Buchführung über das Systeminventar und dessen Konfiguration unerlässlich. Im Prozess der Übergabe von Dokumentation an den Betreiber werden zwar elektronische, aber doch meist noch statische Dokumente (pdf, Office, CAD) angefordert. Diese werden dann wiederum in die Verwaltungssysteme des Kunden eingespeist. Für die Zukunft wird eine starke Verzahnung von Errichtung und Dokumentation erwartet. Denkbar ist, die Dokumentation „live“ in den Kundensystemen vorzunehmen oder, falls diese noch nicht existieren, eine betriebsfertige Tool-Basis mitzuliefern.
Die klassische Dokumentation im Sinn von Ansichten, Verkabelungen, Blockschaltbildern ist weiter notwendig, aber immer weniger hinreichend, da die relevanten Konfigurationen in Servern, Netz- und Sicherheitskomponenten gespeichert sind und als Grundlage der ITIL-Prozesse in eine Configuration Management Database (CMDB) gehören (*Bild 3*).
Bereits in der Vergangenheit entwickelte Telent Schlüsselapplikationen für die eigenen Serviceprozesse. Das umfasst auch B2B-Schnittstellen zu einigen Großkunden zur Übermittlung von Tickets, z.B. für Provisionierungsaufträge oder die Bearbeitung von Incidents. Solche Schnittstellen werden künftig eine erweiterte Rolle spielen, z.B. um „Changes“ zu formulieren, freizugeben und ihre Umsetzung zu dokumentieren.
Es liegen zunehmend sowohl vom Kritis-Betreiber als auch von dessen System- und Servicepartnern gemeinsam zu durchlaufende Prozesse vor, manchmal mit mehrfacher Übergabe der Verantwortung für einzelne Prozessschritte. Gerade bei Zeitdruck, z.B. bei Bekanntwerden einer Sicherheitslücke, spielen elektronische Prozessschnittstellen eine wesentliche Rolle.
Die Herausforderung für Betriebsnetz-Fachleute ist, dass diese Prozesse überwiegend für die klassische Unternehmens-IT erdacht wurden. Daraus ergibt sich die Anforderung, die Konzepte des sicheren Betriebes zu verstehen und so souverän damit umzugehen, dass diese auf die heterogene Gesamtheit der anzutreffenden Systemtechnik in Betriebsnetzen adäquat anwendbar sind.

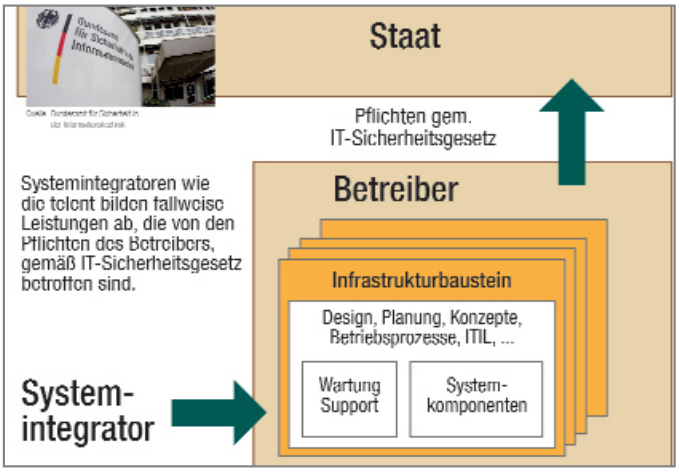

Bild 2: Der technische Dienstleister wird Teil des Systemverbundes

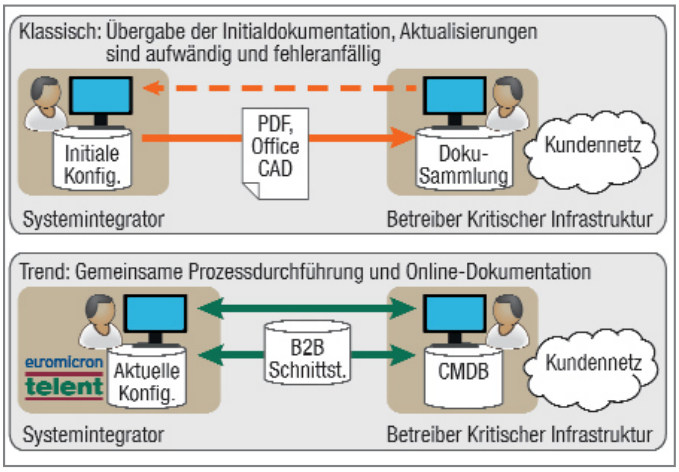

Bild 3: Durchgehende Serviceprozesse und Dokumentation

Anforderungen in Lösungen umsetzen

Der Systemintegrator trägt in vielfältiger Weise dazu bei, die IKT-Infrastruktur von Kritis-Betreibern aufzubauen sowie sicher und zuverlässig betreiben zu können. Große Betreiber von Kritis werden unter Einbeziehung ihrer Integratoren die IT-sicherheitsgerichteten Prozesse weiter verfeinern und transparenter gestalten müssen. Kleinere Betreiber sind gezwungen, ein IT-Sicherheitsmanagement initial aufzubauen und dabei ihre Prozesse zu überdenken und ggf. zu ergänzen.
IT-Sicherheitsaspekte werden darüber hinaus zum Basiskriterium für Netze, Systeme und die zugehörigen Betriebsprozesse. Dies führt zu neuen Formen der Zusammenarbeit zwischen Kritis-Betreiber und seinem Integrator und Dienstleister für die betriebliche Kommunikationsinfrastruktur. *(bk)*