HOMELAND SECURITY

NATIONALE SICHERHEIT UND BEVÖLKERUNGSSCHUTZ

ISSN 1614-3523, 2-2016

www.homeland-sec.de

Nationale Sicherheit - Bevölkerungsschutz - Katastrophenhilfe

Katastrophenschutz für kritische Infrastrukturen

Jürgen Kolb, Managing Director iQSol GmbH

Kernkraftwerk Grohnde bei Hameln in Niedersachsen bei Nacht. Das Kernkraftwerk Grohnde ist ein Druckwasserreaktor und liegt auf dem Gebiet der Einheitsgemeinde Emmerthal im Weserbergland an der Weser. Links im Bild die Kühltürme mit Wasserdampf, rechts im Bild die Reaktorkuppel.

Ende Mai 2016 erst war es wieder so weit: Ein von Meteorologen angekündigtes Unwetter sorgte in ganz Baden-Württemberg für pures Chaos, das sogar Menschenleben kostete. Die wirtschaftlichen Schäden sind noch nicht in vollem Umfang geklärt. Klar ist jedoch: Kein Sandsack hätte die IT von Kernkraftwerken, Energieversorgern, Krankenhäusern oder anderen kritischen Infrastrukturen (KRITIS) schützen können. Ein Blitzschlag – und das Ausmaß der Katastrophe wäre unermesslich gewesen.

Nicht nur Naturkatastrophen wie Hochwasser, Blitzeinschläge oder Brände bedrohen die öffentliche Sicherheit, die unter anderem durch eine zuverlässige Stromversorgung gewährleistet wird. Zunehmend werden auch cyberkriminelle Attacken zur Gefahr, sei es aus terroristischen Beweggründen oder aufgrund erpresserischer Aktivitäten. Besonders gefährdet sind dabei kritische Infrastrukturen (KRITIS), die durch das Bundesministerium für Sicherheit in der Informationstechnik (BSI)[1] sowie das Bundesministerium des Innern (BMI)[2] in die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur eingeordnet wurden. Bei Störungen oder Angriffen auf eben diese Branchen kann es zu Versorgungsengpässen oder Schlimmerem kommen. Nicht umsonst wurden innerhalb des neuen IT-Sicherheitsgesetzes[3] drakonische Strafen für diejenigen angekündigt, die entsprechende Vorfälle an der IT-Infrastruktur ungemeldet lassen.

Notstromaggregate genügen nicht

Inzwischen haben fast alle KRITIS-Betreiber Schutzmaßnahmen ergriffen. Diese

1 https://www.bsi.bund.de/DE/Home/home_node.html
2 http://www.bmi.bund.de/DE/Home/startseite_node.html
3 https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig.html;jsessionid=64D4480124E747862D631F2AEE173031.2_cid286

reichen von, häufig dieselbetriebenen, Notstrom- und Kühlaggregaten bis hin zu umfangreicher Unterbrechungsfreier Stromversorgung (USV). Verbunden sind diese jedoch mit weiteren Problemen im Notfall: Was, wenn der Tank nicht aufgefüllt oder bei einem Brand ebenfalls entzündet wurde, was, wenn die zu überbückende Zeit ohne Strom länger als die USV-Dauer ist? Die IT, die ursprünglich geschützt werden sollte, stürzt ab, Daten gehen verloren oder können schon innerhalb weniger Minuten durch unsichtbare Dritte ausgelesen werden.

Auf Knopfdruck Systeme hoch- und herunterfahren

Schnelles Handeln im Notfall ist unausweichlich. Doch wie nimmt man Systeme vom Netz bevor die Katastrophe eintritt, die Serverräume zu heiß oder gar überflutet werden? Verschiedene Lösungen versprechen Unterstützung. Zunächst einmal bedarf es einer Alarmierung, die bei verdächtigen Vorfällen per SMS, E-Mail oder Voice-Nachrichten das konzerninterne Team für IT und Sicherheit sowie im Bedarfsfall deren Vertreter informiert. Im Anschluss unterstützt wiederum Technik dabei, Daten und Systeme vor Schäden und Diebstahl sowie die gemeinschaftliche Grundversorgung vor dem Zusammenbruch zu schützen. Zum Einsatz kommt das Prinzip des Power Managements, das an eine USV anknüpft. Kommt es zu kritischen Situationen oder Katastrophen, kann die gesamte, auch virtuelle, IT per Knopfdruck heruntergefahren und alle Prozesse damit gestoppt werden. Dies geschieht nach Abhängigkeiten, die vorab festgelegt wurden, damit einander bedingende Systeme in der richtigen Reihenfolge beendet werden. Bei Bedarf ist es dabei sogar möglich, Daten per Live-Migration in ein anderes Rechenzentrum zu verschieben und damit sensible

Blitzschlag über einem Strommast.

Informationen zu schützen. Ist ein Wiederanlauf nach beseitigter Gefahrensituation wieder möglich, kann dieselbe Lösung wiederum zum geordneten Neustart aller Systeme herangezogen werden.

Die Herausforderung in nächster Zukunft ist die gesamtheitliche Betrachtung des IT-Security-Managements. Im Idealfall ist eine SIEM-Lösung implementiert, ebenso wie ein Alerting- und Enterprise-Notification-System bis hin zum integrierten Business-Continuity-Management als einheitlicher Prozess. Sprich: Aus einem Guss, vom Notfallhandbuch bis zum Wiederanlauf nach der Krise.

Menschliches Versagen durch Definitionen und Tests ausschließen

So gut Organisationen und Versorgungsunternehmen auch technisch vorgesorgt haben, so reichen die bisherigen Maßnahmen dennoch nicht aus, um einen vollumfänglichen Schutz aufzubauen. Es bedarf darüber hinaus umfassenden Wissens bei den mit der IT betrauten Personen. Welche Schritte müssen wann eingeleitet, welche Knöpfe wann gedrückt werden? Wichtig ist demnach eine klare Definition in Form eines Notfallhandbuches. Dieses muss bei jedem neu eingesetzten Mitarbeiter sowie bei jedem neuen Bestandteil der IT-Infrastruktur gepflegt, auf den neuen Stand gebracht und an alle beteiligten Mitarbeiter verteilt werden.

Ein weiterer wichtiger Schritt ist der Disaster Test, bei dem die Wiederherstellung im Notfall unter fast realen Bedingungen geprobt wird. Nur, wer eine gewisse Routine mitbringt, wird im Katastrophenfall die erforderliche Ruhe bewahren – und die richtigen Knöpfe drücken.

Homeland Security sprach mit Jürgen Kolb, Managing Director iQSol GmbH und Autor dieses Beitrags.

Business Continuity Management mit PowerApp

In der IT-Infrastruktur können Stromausfälle zum Verlust nicht gesicherter Daten

Architektur der PowerApp

sowie im Einzelfall zur Beschädigung von Geräten führen. Die iQSol GmbH ist ein österreichischer IT-Security-Hersteller und bietet u. a. die Lösung PowerApp an. Die PowerApp ist für die zentrale Steuerung eines Shutdown- und Restart-Prozederes von Servern und IT-Infrastrukturen gedacht, um in Angriffsfällen, bei Bränden oder anderen kritischen Notfällen die gesamte IT nach Abhängigkeiten schnell herunter- und wieder hochfahren zu können und somit Hardware sowie Daten zu schützen. Zudem sind auch Disaster-Tests und Live-Migrationen in andere Rechenzentren möglich. Entsprechende Log- und Alarmierungslösungen gehen damit Hand in Hand.

Homeland: Wie entstand die Idee zu PowerApp?

Kolb: Bereits vor über zehn Jahren haben wir aufgrund einer Kundenanfrage aus dem Finanzbereich ein Konzept entwickelt, wie man rasch und unter Betrachtung der komplexen Abhängigkeiten von Netzwerk und Software die IT „herunterfahren“ kann. Kurz darauf kam ein Krankenhausverbund mit sehr vielen Krankenhäusern mit derselben Anforderung auf uns zu. Nach einem technologischen Redesign wurde aus dem IT-Consulting ein eigenständiges Produkt geschaffen, das als Appliance zur Verfügung steht. Mit Consulting und auch als Managed Service verfügbar, ist damit heute eine marktreife und bewährte Lösung verfügbar.

Weitere Informationen gibt es hier:

www.iqsol.biz

Homeland: Was macht die PowerApp so besonders?

Kolb: Die Idee ist ganz einfach und jeder fragt sich, warum es so etwas bisher nicht gibt: Auf Knopfdruck ein Rechenzentrum herunter- und wieder hochfahren. Einerseits werden immense Budgets aufgewendet, um ein Data Center am Laufen zu halten. Andererseits ist jedem klar: Wenn der Notstrom nicht mehr funktioniert und im Falle eines Angriffs die IT-Security überwunden ist, ist man quasi ausgeliefert und die letzten Helferleins sind das Backup und die Daten im Ausweichrechenzentrum. Ganz abgesehen von Simulationen von Disaster Tests, an die sich kaum noch jemand herantraut in einer großen Umgebung. Compliance ist in diesem Themenumfeld zwar sehr stark im Kommen, meist auch konzeptionell und theoretisch angehaucht, faktisch ist diese aber nur mit der PowerApp nachweisbar. Weitere Aspekte sind die Mandantenfähigkeit und die PowerNodes, die eine dezentrale Option für kleinere Außenstellen in exponierten Gebieten (Asien, Osteuropa) bieten.

Homeland: Welche Anwendungsszenarien gibt es?

Kolb: Sehr viele: Wenn das Rechenzentrum physikalisch (Stromausfall, Überhitzung, Sensoralarm) bedroht ist oder auch bei starken Umwelteinflüssen (Unwetter, Chemieunfall, Eis) einer Gefahr ausgesetzt ist, kann die Entscheidung notwendig werden, das Data Center stillzulegen. Hier steht vor allem der Schutz der IT im Vordergrund und nicht, die Verfügbarkeit um jeden Preis zu halten. Der „Klassiker“ der Kunden sind aber Stromausfälle oder auch geplante Stromabschaltungen aufgrund von Wartungsarbeiten. Wenn dann mehrere 100 oder 1.000 Server abgeschaltet werden sollen, ist das auf Knopfdruck viel effizienter als manuell. Viele Mehrwerte ergeben sich natürlich, wenn ausgewählte Server

herunter- und hochgefahren werden – sei es wegen Update-Mechanismen, Wartungsfenstern oder aus Energiespargründen.

Homeland: Wie funktioniert die PowerApp bei einer Cyberattacke?

Kolb: PowerApp ist kein Security-Tool an sich, sondern das Kernelement einer Business-Continuity-Strategie, sprich: Es ist das Werkzeug, wenn Security überwunden ist oder Sensoren anschlagen. Im Falle von Trojanerangriffen wie Ransomware oder wenn Daten abgezogen werden macht es natürlich schon Sinn, die betroffenen Maschinen erstmal „schlafen zu legen", vom Netz zu trennen oder zu isolieren, um eine Ausweitung zu verhindern oder die Situation zunächst zu überprüfen. Zum Cyberschutz wird eine zentrale SIEM- und Log-Management-Lösung empfohlen, die wir auch anbieten.

Homeland: Wie erfährt der Nutzer von einem Ausfall des Systems bzw. einem Shutdown- und Restart-Prozedere?

Kolb: Der Nutzer ist der verantwortliche Administrator oder der Business-Continuity-Manager. Im Krisenfall ist dieser bereits per Alarmierungslösung informiert, die Alarme aus Sensoren oder Schwellwerten von Monitoringlösungen generiert. Der Shutdown kann manuell oder automatisch erfolgen, je nach Prioritäten und individuellen Anforderungen. Aus Sicherheitsgründen gibt es natürlich keine „App mit rotem Knopf" von uns für den IT-Shutdown der gesamten Infrastruktur. In der Regel erfolgt die Alarmierung sofort bei USV-Einsatz und dann kann eben automatisch/individuell oder nach gewissen Zeitfenstern die weitere Vorgangsweise erfolgen.

Homeland: Wie sieht die weitere Entwicklung aus?

Kolb: Wir sehen hier eine Konvergenz von IT-Security, Alarmierung und IT-Krisenmanagement auf Software-Basis. Es werden laufend Kundenanforderungen eingearbeitet und Szenarien abgebildet. Täglich passieren Dinge, auch Kaskadeneffekte, die man nicht für möglich hält und die keiner eingeplant hatte. Wir ziehen hier permanent nach, bieten aber immer die Möglichkeit, aktiv in der Krise einzugreifen. Das ist schon sehr beruhigend für die Kunden, die begeistert sind und sich sehr rasch für die Lösung entscheiden – leider oft erst nach einem Vorfall.

Homeland: Was wünschen Sie sich für die Zukunft?

Kolb: Wir alle möchten unseren Lebensstandard halten, die Sicherheit verbessern und auf soziale Systeme vertrauen können. Dies funktioniert ohne Strom in den Verkehrs- oder Wassernetzen, ohne IT-Systeme bei Polizei und in Krankenhäusern oder in angegriffenen Rechenzentren leider überhaupt nicht. Deswegen müssen wir schnellstmöglich die Resilienz steigern, denn nicht nur Terroristen bedrohen die Nationen.

Homeland: Vielen Dank für das interessante Gespräch.

Jürgen Kolb ist Managing Partner der österreichischen iQSol GmbH und verantwortet den Bereich Sales, PR & Marketing. Nach verschiedenen beruflichen Stationen in der öffentlichen Verwaltung sowie in der freien Wirtschaft gründete Kolb das Unternehmen gemeinsam mit seinem Partner aufgrund vorangegangener Erfahrung aus verschiedenen IT-Projekten und -Audits. iQSol ist seine zweite erfolgreiche Unternehmensgründung, denn auch am Aufbau der Antares NetlogiX Netzwerkberatung GmbH ist er schon seit Beginn im Jahr 2000 beteiligt.

Impressum

Herausgeberin: Dr. Nadine Seumenicht
Chefredakteurin: Dr. Nadine Seumenicht

Beirat
Vernetzte Sicherheit: Harald Kujat, General a. D.
Vernetzter Einsatz: Dr.-Ing. Andreas Groth; Ralph D. Thiele, Oberst a. D.

Internationales Redaktionsteam
Ressort Vernetzte Sicherheit: Dr. Stefan Queisser, Fregattenkapitän d. R.; Michael Hartung, Oberleutnant d. R.
Ressort Zivil-Militärische Zusammenarbeit: Dipl. Verw. Joachim Zacher
Ressort Innere Sicherheit: Niels Czajor, Dipl.-Verw-Wiss.; Oberstleutnant d. R., Polizeifreiwilliger des Landes Baden-Württemberg
Ressort IT-Security: Georg Wenner, EDS-CSO Germ. Gov. a. D.; Jim Litchko, CISSP-ISSEP, MBCI, MAS
Ressort Robotics Unstructured Environments: Prof. Dr.-Ing./Univ. Tokio Thomas Bock
Ressort Internationale Kriminalwissenschaften: Robert F. J. Harnischmacher
Ressort Ausbildung und Training für die Sicherheit in der Wirtschaft: Klaus-Dieter Jörn; Robert F. J. Harnischmacher
Ressort Canada: Prof. Dr. Darryl Plecas
Ressort China: Prof. Dr. Gu Minkang
Ressort Japan, Korea: Prof. Dr. Minoru Yokoyama; Prof. Dr. Dr. h.c. mult. Haruo Nishihara; Prof. Dr.-Ing./Univ. Tokio Thomas Bock
Ressort Mexiko: Walter M. McKay, M.A.
Ressort Norwegen: Superintendent Prof. Rune Glomseth; Prof. Dr. Petter Gottschalk
Ressort Österreich: Hofrat Mag. Maximilian Edelbacher
Ressort Polen: Prof. Dr. Dr. h.c. Brunon Holyst
Ressort Südafrika: Prof. Dr. Cornelis Roelofse
Ressort USA: Prof. Dr. Dilip K. Das; Prof. Dr. Otwin Marenin; Prof. Dr. Linda Keena
Hauptstadtbüro Berlin: Heike Barnitzke
Ressort Geschichte: M. A. Volker Hollmann
Ressort Politik: Dipl. Verw. Joachim Zacher
Ressort Wissenschaft: Prof. Dr.-Ing. Michael Gerke; Dr. Nadine Seumenicht

Design und Layout: Larissa Seumenicht

Verlag:
HOMELAND SECURITY UG
(haftungsbeschränkt)
Deilinghofer Straße 2, D-58675 Hemer
Tel.: 02372-9 35 26 10
Fax: 02372-9 35 26 19
redaktion@homeland-sec.de
www.homeland-sec.de

Einzelbezugspreis:
10,- EURO (inkl. Versand in D)

Jahresabonnement:
27,- EURO (3 Ausgaben inkl. Versand in D)
Der Aktion Deutschland Hilft e. V. kommt pro Abo 1,- EURO zugute.

Auflage:
16.000 Exemplare
ISSN 1614-3523 (Print)
ISSN 2194-4849 (Online)

Bildnachweis:
Titelbild: Bosch Security

Aktion Deutschland Hilft e. V., Axis Communications, BBK, BMI, Bosch Security, Comexposium Security, creatyp, Rouven Brunnert/DRK, Mark Hofmann/DRK, EW Medien und Kongresse, Homeland Security, ib consultancy, iQSol, Messe Essen, North Atlantic Treaty Organization, ORTEC Messe und Kongress, OSCE/Mikhail Evstafiev, Progres Partners Advertising s. r. o., Henning Schacht, THW, THW/Julia Dehn, THW/Michael Matthes, THW/Markus Schrems