

Ohne Strom keine IT, ohne IT kein Strom

Der Energieversorger RWE schützt seine Informationsinfrastrukturen mit einem umfassenden Bündel an Maßnahmen

Von Marcus Heide

Nicht immer ist der kürzeste Weg auch der schnellste. Das weiß jeder, der bei seinem Navigationssystem im Auto den Routenplaner entsprechend eingestellt hat. Das weiß aber auch Andreas Ebert, seit er sich das erste Mal nachts bei Stromausfall von seinem Büro zum Krisenmanagementraum begeben wollte. Kein Aufzug, kein Licht im Treppenhaus, suchende Kollegen in den Fluren. Und niemals hatte er tagsüber einen Gedanken daran verschwendet, wie viele Türen er auf diesem Wege durchschreiten muss – und wie viele davon wiederum einen elektrischen Impuls benötigen, um sich zu öffnen. Seitdem ist für ihn der Begriff vom „kürzesten Weg“, aber auch der vom „schnellsten“ eine relative Angabe.

Zum Glück musste Ebert diese Erfahrung nicht bei einem echten Notfall machen. Es war „nur“ eine Übung, aber eine überaus realitätsnahe. Und sie hat die RWE AG in Sachen Sicherheit ein großes Stück nach vorne gebracht, denn die Vorstände und viele Führungskräfte waren auch dabei und haben verstanden, wie wichtig es ist, auf eine echte Krise vorbereitet zu sein.

Die Übung war mittelbar ein Teil der zu Anfang des Jahres durchgeführten „Bundessonderlage IT“ im Rahmen der LÜKEX, der „Länderübergreifenden Krisenmanagement-Exercise“, die das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) im Auftrag des Bundesinnenministeriums etwa alle zwei Jahre als Stabsrahmenübung auf

politischer und administrativer Ebene durchführt. Sie gehört zum so genannten Umsetzungsplan KRITIS zum Schutz der Informationsinfrastrukturen. Für RWE als einem der größten Stromversorger Europas ist das Sicherheitsengagement auf diesem Gebiet – anders als für so manchen Wettbewerber – eine Selbstverständlichkeit. Bei der vergangenen



Die intelligente Wertesicherung !

- Elektronische Schlüsselschränke
- Elektronische Fachanlagen
- Netzwerkfreie Zugangskontrolle
- Echtzeit Objektkontrolle

02633-200334 - www.traka.de

Security 2010 – Halle 10 - Stand 405

traka
intelligent access management

LÜKEX war das Krisenszenario ein multipler Terroranschlag mit „schmutzigen“ Bomben, 2011 wird es eine multiple „Cyber-Attacke“ sein, sprich: ein Angriff auf die Informations- und Telekommunikationsnetze Deutschlands und der Kritischen Infrastrukturen.

Vom Papier über den Rechner bis zum Beamer

Und hier kommt Andreas Ebert ins Spiel. Der seit 14 Jahren bei RWE tätige Diplomingenieur für Elektro- und Nachrichtentechnik leitet innerhalb der Konzernsicherheit die Abteilung IT-Security & BCM Governance (BCM = Business Continuity Management). „Bei der ‚Informationssicherheit‘ geht es über die reine Technik hinaus um den Lebenszyklus einer Information, übrigens nicht nur im virtuellen Netzwerk, sondern auch auf dem Papier“, erzählt er im Gespräch mit SECURITY insight. „Dabei ist unter anderem zu gewährleisten, dass die Information nicht in den Einflussbereich Unbefugter gelangt. Einzubeziehen sind nicht nur die Datenströme im IT-Umfeld, sondern auch in der Telekommunikation. Das ist heute längst zusammengewachsen.“ Vorausschauenderweise wird bei RWE in einem nächsten Schritt gar die Medientechnik (zum Beispiel Beamer und elektronische Flipcharts) mit einbezogen, denn die allgemeine Vernetzung – und damit die Zahl potenzieller Angriffspunkte – schreitet voran.

Das alles spielt unter Sicherheitsaspekten eine so große Rolle, dass das Bundesinnenministerium eigens einen nationalen Schutzplan dafür erarbeitet hat und mit LÜKEX und dem damit verbundenen, vergleichsweise großen Aufwand diverse Krisenszenarien durchexerziert. Warum sich bedeutende KRITIS-Unternehmen daran beteiligen, wird deutlich, wenn man auf bereits erfolgte Cyber-Attacken zurückblickt. 2001 gab es den ersten so genannten DDoS-Angriff auf das Weiße Haus, im April 2007 wäre fast ganz Estland auf diese Weise lahmgelegt worden.

Ein Bericht des US-Rechnungshofs vom Mai 2008 bescheinigte der Tennessee Valley Authority, dem größten Stromversorger der USA, dass sie die Sicherheitsstandards für den Betrieb kritischer Computernetze nicht erfüllt habe (beispielsweise dass ihre Firewalls leicht zu umgehen sind) und sie somit durch Hacker äußerst verwundbar sei. Das hieße im schlimmsten Fall, dass in weiten Teilen des Landes der Strom ausfallen würde, wenn ein Hacker im System das Häkchen an einer sensib-



5.–8. Oktober 2010
Halle 3.0 Stand 415

Die Zukunft im Griff



Brandmelderzentrale Integral IP

Sicher
Integral IP ist die erste und einzige Brandmelderzentrale mit echter Hard- und Software Redundanz.

Vernetzt
Integral IP steht für den Umbruch in der Vernetzung von Brandmelderzentralen.



Besuchen Sie uns:
security 2010
05.10.–08.10.2010
Halle 3, Stand 610



Blick in die RWE-Sicherheitsleitstelle

len Stelle an- oder wegklickt. Das kann sich inzwischen keine Volkswirtschaft mehr leisten, vom einzelnen Unternehmen ganz zu schweigen. Für Deutschland spielt RWE eine ähnlich wichtige Rolle, weshalb die Informationssicherheit eben nicht nur in Sonntagsreden, sondern tatsächlich sehr hohe Priorität genießt.

Zwei IT-Welten

Tatsächlich arbeiten Versorgungsunternehmen parallel in zwei verschiedenen IT-Welten. Während die Verwaltung sowie interne wie externe Kommunikation über die herkömmlichen Betriebssysteme und Anwendungen ablaufen (zum Beispiel Windows, Linux, SAP, Oracle), gibt es für die Netzwerksteuerung und die Steuerung der Kraftwerkssysteme eine separate Prozessleittechnik. Freilich unterscheiden sich diese separaten Welten allenfalls über die Protokolle (also die Regeln zu Formaten, Inhalten, Bedeutung und Reihenfolge gesendeter Nachrichten), aber letztlich nicht in ihrem Wesen. RWE hat inzwischen ein „Information Security Management System“ (ISMS) nach DIN ISO 27000 eingeführt, das diese Angriffspunkte so weit wie möglich versiegeln soll. Auch hier gilt: Hundertprozentige Sicherheit gibt es nicht. Der pragmatische Ansatz ist nützlicher: „Lieber

schon heute zu 90 Prozent gewappnet sein, als übermorgen noch auf die 100 Prozent warten“, so Ebert.

Die Mitarbeiter ins Boot holen

An dieser Stelle müssen die Mitarbeiter mit ins Boot, und zwar so viele wie möglich. Dazu gehören selbstverständlich Anleitungen zum sicheren Umgang mit der Datenverarbeitung, wie man sie auch aus anderen Firmen kennt – angefangen beim Verbot, fremde Software auf die eigene Festplatte zu spielen, bis hin zur Installation abhörsicherer Telefonanlagen. Ein anderes Maßnahmenbündel dient der „Security Awareness“, wie das neudeutsche Wort heißt, das einen großen Anteil an Eberts täglicher Arbeit ausmacht: das Bewusstsein schaffen, dass Sicherheit in letzter Konsequenz nicht nur ein abstraktes Gemeinwesen – den Staat, die Stadt, die Gesellschaft – schützt, sondern obendrein den eigenen Arbeitsplatz. Wenn Informationen verloren gehen oder, schlimmer noch, auf kriminellen Wegen an Wettbewerber im In- und Ausland gehen, kann sich das auf die wirtschaftliche Situation auch eines stabilen Energiekonzerns auswirken. Das Image als Marketingfaktor nicht zu vergessen. Ein Energieversorger, der im datenschutz-



Seit 2009 verantwortet Andreas Ebert innerhalb der RWE AG die „Information Security“ als Group Information Security Officer. Parallel ist er seit 1997 in unterschiedlichen Fachgruppen des BITKOM e. V. tätig. Seit 2009 vertritt er zudem RWE im Nationalen Umsetzungsplan Kritische Informationsinfrastrukturen (UP KRITIS).

rechtlichen Zusammenhang ins Gerede kommt, hat schnell das Vertrauen seiner Kunden verspielt.

Zu den seichteren IT-Awareness-Kampagnen bei RWE gehört etwa das Werben mit Sicherheitssprüchen auf Mousepads,

Kaffeetassen oder Postern. Weitaus wichtiger ist beispielsweise das neue Portal zur Informationssicherheit im Intranet, auf dem die Mitarbeiter konkrete, anlassbezogene Fragen stellen können und diese auch beantwortet bekommen. Welche IT-Ausrüstung darf ich bei der Geschäftsreise nach China mitnehmen und wie muss ich sie vor Lauschangriffen schützen? Welche Gefahren drohen nach aktuellen Phishing-Vorfällen bei der Hausbank? „Die meisten Antworten werden nach wenigen Minuten auf dem Portal stehen“, erzählt Ebert. „Zeit ist ein kritischer Faktor, denn die Mitarbeiter stehen vor einem Problem, das keinen Aufschub duldet. Wenn wir schon so viel Wind um die Sicherheit machen, muss deutlich sein, dass sie für die Großwetterlage unverzichtbar ist.“

Und manchmal versuchen Ebert und sein Team auch, die Belegschaft zum Sicherheitsglück sanft zu zwingen. Beim RWE-„PatchDay“, bei dem auf die Client-Rechner im Konzern regelmäßig Software-Updates aufgespielt werden, müssen die Mitarbeiter für die Zeit der Aktualisierung die eigentliche Arbeit am PC ruhen lassen. Dabei wird künftig hin und wieder ein kleines Info-Programm zur IT-Sicherheit laufen, dessen Lektüre oder Übungen die Anwender quittieren müssen. So wird der

Leerlauf sinnvoll zur Bewusstseins-schaffung genutzt.

Drehbücher für die Sicherheit

Eines weiß Andreas Ebert allerdings gewiss: „Die nachhaltigste Sicherheitsmaßnahme ist und bleibt die praktische Übung.“ Das kann LÜKEX sein, aber auch RWE-interne Notfallübungen, in die die Vorstände und das Führungsmanagement integriert sind. Solche Übungen, wenn auch vielleicht über den IT-Sicherheitsgedanken ausgelöst (Stromausfall), geht weit über die IT-Sicherheit hinaus. Daran wird die zentrale Rolle deutlich, die ein Energieversorger als Kritische Infrastruktur eines Landes spielt: Ohne Strom keine IT, aber ohne IT auch kein Strom.

„Praktische Übungen bedeuten natürlich viel Vorbereitung von unserer Seite“, so Ebert. Er und seine Mitarbeiter müssen sich dazu zunächst in die IT-Organisation und bestimmte Konzernabläufe vertiefen, müssen Ortsbegehungen durchführen (Welches Rolltor öffnet sich mit welcher Berechtigung?) und sich möglicherweise mit anderen beteiligten Organisationen (IT-Dienstleister, Feuerwehr,) abstimmen. Dann müssen entsprechende „Drehbücher“ verfasst werden, die nicht nur wahrscheinliche Gefahren berücksichti-

Videokontrolle trifft Zutritt.

Zutrittskontrolle mit integrierter Videoüberwachung erhöht die Effizienz Ihres Wachpersonals. Das spart Ihnen Zeit und Geld. Durch die Integration von Video in Ihr Zutrittssystem haben Sie jederzeit den Überblick. Anschauliche Bilder statt abstrakter Alarmmeldungen. Setzen Sie nicht auf Insellösungen, sondern auf das „2in1-System“ von PCS: www.pcs.com

PCS. The terminal people®

- Zeiterfassung
- Zutrittskontrolle
- Videoüberwachung



Pfälzer-Wald-Straße 36 · 81539 München
Fon +49-89-68004-550 · Fax +49-89-68004-555
E-Mail: intus@pcs.com · www.pcs.com

Funk-Alarmsysteme



www.daitem.de





Foto: Mario Abascia



Ohne Strom letztlich nur geformtes Blech



Kraftwerke sind nicht nur durch Zäune gut geschützt, sondern auch durch virtuelle Maßnahmen.

gen, sondern obendrein noch „pädagogisch wertvoll“ sind.

Übungen wie LÜKEX sind deshalb so wertvoll, weil praktisch der gesamte Sicherheitsapparat auf Herz und Nieren geprüft wird. „Aber es muss nicht immer der ganz große Aufwand betrieben werden. Wichtig ist, dass Übungen überhaupt auf der Agenda stehen und durchgeführt werden.“ Das ist eine der drei zentralen Erkenntnisse, die Andreas Ebert in den letzten Jahren gesammelt hat. Die zwei anderen: Das Management mit einbeziehen. Und: Der Teufel steckt im Detail, nichts ist selbstverständlich. Wie stimmt man beispielsweise in hohem Tempo eine Presseerklärung mit dem Pressesprecher ab, wenn die Medien bereits vor dem Werkstor stehen? Wer ist in Entscheidungsprozesse einzubeziehen und wie sehen Kommunikationswege aus?

Schließlich: Funktionieren überhaupt die Telefone, mit denen sich die Verantwortlichen über diese Fragen verständigen?

Know-how-Transfer für alle

Dass es RWE dabei nicht nur um den eigenen Schutz geht, sondern durchaus auch eine soziale Komponente mitschwingt, lässt sich aus einer Bemerkung schließen, die Ebert in einem Nebensatz versteckt, als das Gespräch auf Zusammenarbeit und Know-how-Austausch kommt: „In Sachen Sicherheit dürfen wir keine Wettbewerber sein.“ Tatsächlich bietet sich der Konzern als Anlaufstelle für den Know-how-Transfer innerhalb seiner Netzwerkpartner an, von dem auch Stadtwerke profitieren sollen. Des Weiteren arbeitet RWE eng mit Unternehmen anderer Branchen der Kritischen Infrastrukturen unter Moderation des Bundesamts

für Sicherheit in der Informationstechnik zusammen. Beispiele sind Banken (Welche Gefahr droht beim Online-Banking?) oder die Deutsche Flugsicherung: Wenn ihre Mitarbeiter selbst – wieder nur ein Beispiel – nicht wissen, wie sich die Vulkanasche in den nächsten Stunden auf den Flugplan von London-Heathrow auswirken wird, so kennen sie zumindest jemanden, der Auskunft geben kann. Auch das ist vielleicht weder der kürzeste noch der schnellste Weg zum Ziel. Aber es ist ein Weg, im Chaos möglicherweise der am nächsten liegende und effektivste. Am Ende zählt nur, dass man sicher ankommt.

WWW.RWE.COM

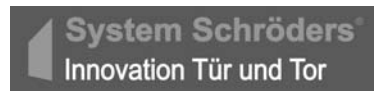


T-90 Feuerschutztür mit Einbruchschutz WK-4

Schutz & Sicherheit

Seit über 30 Jahren steht der Name Schröders für die Entwicklung modernster Stahlsicherheitstüren und -tore. Unsere Lösungen bieten hervorragenden Feuerschutz, Rauchschutz, Einbruchschutz und Schallschutz.

Die patentierten **System Schröders®** Türen und Tore werden ausschließlich in Lizenz von autorisierten und qualitätsüberwachten Fertigungsbetrieben gefertigt.



Produktinformationen, Referenzen und Herstellernachweis:

www.system-schroeders.de

System Schröders
Zuverlässiger Partner bei Sicherheitstüren und -toren

System Schröders
Gerhard-Welter-Str. 7
41812 Erkelenz
Tel.: 02431 8084-0