

Mobil bleiben, wenn das Licht ausgeht

Kritische Infrastrukturen brauchen Schutz vor folgenschweren Netzausfällen



Orkan Kyrill offenbarte im Januar 2007 die Anfälligkeit herkömmlicher Kommunikationsdienste

Im Schlamm des Jahrhunderthochwassers an der Elbe, in der Schneekatastrophe im Münsterland und nach den Bombenanschlägen in London – überall mussten Helfer wie Betroffene erleben, dass sie von der gerade in der Notfallsituation lebenswichtigen Kommunikation abgeschnitten sind, weil nicht nur die Festnetztelefone, sondern auch die Mobiltelefonnetze zusammenbrachen. In solchen Situationen, aber auch bei dem flächendeckenden Stromausfall, den ganz Westeuropa vor nicht allzu langer Zeit erlebte, arbeiten meist nur noch die Paging-Services störungsfrei.

Die mobile Vermittlung von Informationen wird heute gerne als Selbstverständlichkeit angesehen. Doch in der Krise zeigt sich, dass die vertrauten und häufig genutzten Kommunikationsdienste ausgesprochen stör anfällig sind. Gerade bei Großschadensereignissen, Naturkatastrophen, terroristischen Anschlägen oder in Spitzenbelastungszeiten kommt es immer wieder zum folgenschweren Ausfall der nicht- oder semiprofessionellen mobilen Kommunikationsnetze. Umso wichtiger sind ergänzende Mobilfunktechnologien wie der professionelle Funkruf. Als Zweit-

alarmierungsweg bzw. Rückfallebene lässt sich mit ihm auch im Ernstfall weiterhin zuverlässig mobil kommunizieren.

Die vitale Wichtigkeit unserer Informations- und Kommunikationsnetze macht sich in erster Linie bei so genannten „Kritischen Infrastrukturen“ bemerkbar. Kommt es hier zu massiven Störungen, kann dies folgenschwere Kettenreaktionen auslösen. Da die Risiken allzu häufig unterschätzt werden, kümmert sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) um Aufklärung. Dabei werden gezielt öffentliche Bedarfsträger in Bund, Ländern und Kommunen sowie Unternehmen angesprochen.

Auch Unternehmen betroffen

Das BSI definiert als „Kritische Infrastrukturen“ Organisationen und Einrichtungen, „bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsempfänger, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ eintreten würden. Konkret zählen laut BSI zu Infrastrukturen mit kritischen, von IT abhängigen Systemen u.a. die Bereiche Transport und Verkehr, Energie (so sind herkömmliche mobile Kommunikationsdienste auf Stromversorgung angewiesen), Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen (mit IT-abhängigen Dienstleistungen), Versorgung (von Wasser bis Gesundheits- und Rettungswesen), Behörden, Verwaltung und Justiz.

Unternehmen sind dabei nicht minder stör anfällig: Auch hier gibt es kritische Infrastrukturen, auch hier können Störungen an neuralgischen Stellen zu deutlichen ökonomischen Schäden führen. Das BSI spricht beispielsweise von zwei Wochen, die in den finanziellen Kollaps führen können. Heutige Störungen sind eher von kurzer Dauer, können aber bereits zu erheblichen Problemen in der mobilen Kommunikation führen.

Fehleinschätzungen durch Unkenntnis

Dennoch zeigen Umfragen (z.B. des BSI), dass sich nur wenige Unternehmen der Risiken bewusst sind. Zwar gaben gegenüber dem BSI 98 Prozent der Befragten an, funktionierende IT-Systeme seien für den Arbeitsablauf sehr wichtig; und entsprechend hielten selbst unter den IT-Experten rund 80 Prozent ihre eigene Organisation für wenig stör anfällig. „Diese Fehleinschätzung hinsichtlich der eigenen Betroffenheit zeigt ein weiteres Problem: Unkenntnis!“ So die Interpretation des Leiters des BSI, Dr. Udo Helmbrecht, in einem Vortrag auf dem Security Kongress in München im November 2004. Denn nicht nur das Absichern eines Servers ist von zentraler Bedeutung, sondern auch eine zuverlässig funktionierende Rückfallebene bei professionellen mobilen Kommunikationsdiensten.

Wie rasch gerade im Zusammenspiel der Infrastrukturbereiche Störungen im Sinne des Domino-Effekts eskalieren können, erklärt Dr. Helmbrecht an einem Beispiel: „In der Schweiz fällt ein Baum um und in ganz Italien geht das Licht aus, so wie im September 2003 tatsächlich geschehen. Kleine Ursache, große Wirkung.“ Eine Kettenreaktion lässt sich dann so beschreiben: „Der Stromausfall kann zum Ausfall des Telefonnetzes führen, alle Betroffenen greifen auf ihr Mobiltelefon zurück. Wenn dadurch das Mobilfunknetz in einer Region nicht ebenfalls komplett zusammenbricht, sind irgendwann die Akkus leer und spätestens dann geht nicht mehr viel.“



Bei Stromausfall bleiben Leitstelle und Kommunikationsdienste des e*BOS-Systems einsatzbereit

Von Blitzen unbeeindruckt

Gerade herkömmliche Kommunikationsdienste sind hinsichtlich Stromversorgung immer anfällig. Dies zeigen auch die Erfahrungen im Landkreis Börde (Sachsen-Anhalt). Hier hat die digitale Alarmierung mit dem e*BOS-System von e*Message ihre erste „Feuerprobe“ beim Orkan Kyrill im Januar 2007 bestanden: Als flächendeckend der Strom und teilweise auch Handynetze ausfielen, die Sirenen nicht funktionierten und zu allem Überfluss ein Blitz in einen Sendemast einschlug, zeigte sich dieses System von all dem unbeeindruckt; die Leitstelle konnte die Einsatzkräfte jederzeit erreichen und effektiv koordinieren.

Ähnliche Kettenreaktionen gibt es auch in betrieblichen Strukturen. Schon die Tatsache, dass der Außendienst nicht erreichbar ist oder Lkws unzureichend dirigiert werden und ihre Ware nicht just-in-time beim Kunden anliefern oder abholen, kann zu folgenschweren Verwerfungen führen. Mobile Kommunikationsdienste zählen immer dann zu den Kritischen Infrastrukturen, wenn ihr Ausfall entscheidende Abläufe in Produktion, Verwaltung oder Gesellschaft intensiv und nachhaltig negativ beeinflusst. Ursachen für den Ausfall der Mobilkommunikation können unterschiedlicher Art sein: Stromausfälle, Katastrophen, Unfälle oder auch Anschläge sind vorstellbare und keineswegs abwegige Szenarien, nicht nur für den Großraum Berlin-Brandenburg.

Redundanzen und Rückfallebenen

Je professioneller das Anforderungsprofil ist, desto zuverlässiger und krisenresistenter muss die Technik sein. Zudem bedarf es redundanter Systeme, die Informationsvermittlung auch dann sicherstellen, wenn ein Medium ausgefallen ist. Vorbilder für diese Methode gibt es reichlich. Dass z.B. der Mensch über zwei Nieren verfügt, ist eine kluge Vorsichtsmaßnahme: Fällt eine aus, kann die andere die Entgiftung des Körpers vollständig übernehmen.

In der Natur gibt es viele Beispiele für redundante (lat. redundare = im Überfluss vorhandene) Lösungen, die durch mehrfaches Vorhandensein von „Komponenten“ die Ausfallsicherheit erhöhen. In der Technik wird diese Strategie überall dort adaptiert, wo eine Störung zum folgenschweren Totalausfall führen könnte. So sind in der Raumfahrt oder im Luftverkehr zahlreiche Systeme redundant ausgelegt. Gleiches gilt für Kernkraftwerke oder die Stromversorgung von Krankenhäusern.

Beizeiten schwimmen lernen

Gerade der IT-Bereich hat hier einen deutlichen Nachholbedarf. Zwar ist vieles doppelt ausgelegt (z.B. Server), aber die verantwortlichen Kommunikationsleiter denken selten an Mobilfunk. Das so genannte „Mobile Security Konzept“ wird oft ausschließlich im Sinne von Mithören, Virenangriffen und Missbrauch gedacht. Dass aber der Ausfall von professionellen Kommunikationsdiensten zu erheblichen Verwerfungen mit messbaren ökonomischen Schäden führen kann, ist oft nicht im Blickfeld.

Die IT-Sicherheit und die Absicherung professioneller mobiler Informationsdienste sind somit für Unternehmen ebenso wichtig wie für vergleichbare Strukturen im Gemeinwesen. Ein Grund für die häufig stiefmütterliche Behandlung dieses Themas mag in den Investitionen begründet liegen. Denn zunächst kostet die Absicherung potenziell kritischer Infrastrukturen Geld; und was sich nicht sofort bezahlt macht, wird gerne zurückgestellt, bringt Dr. Helmbrecht das Dilemma auf den Punkt. Vorsorge mit Paging-Lösungen, wie sie e*Message anbietet, müsse aber vor dem Eintritt eines Schadens erfolgen: „Wer ins Wasser fällt und nicht schwimmen kann, der kann es auch dann nicht mehr lernen.“

Kontakt:

e*Message Wireless Information Services Deutschland GmbH, Berlin
Tel.: 030/4171-0
info@emessage.de
www.emessage.de