Das Beispiel Swisscom : fokussieren auf das Vorhandene, nicht auf das Fehlende

Autor(en): **Jaton, Cédric / Zumbühl, Marcel**

Objekttyp: **Article**

Zeitschrift: **Bevölkerungsschutz : Zeitschrift für Risikoanalyse und Prävention, Planung und Ausbildung, Führung und Einsatz**

Band (Jahr): **6 (2013)**

Heft 17

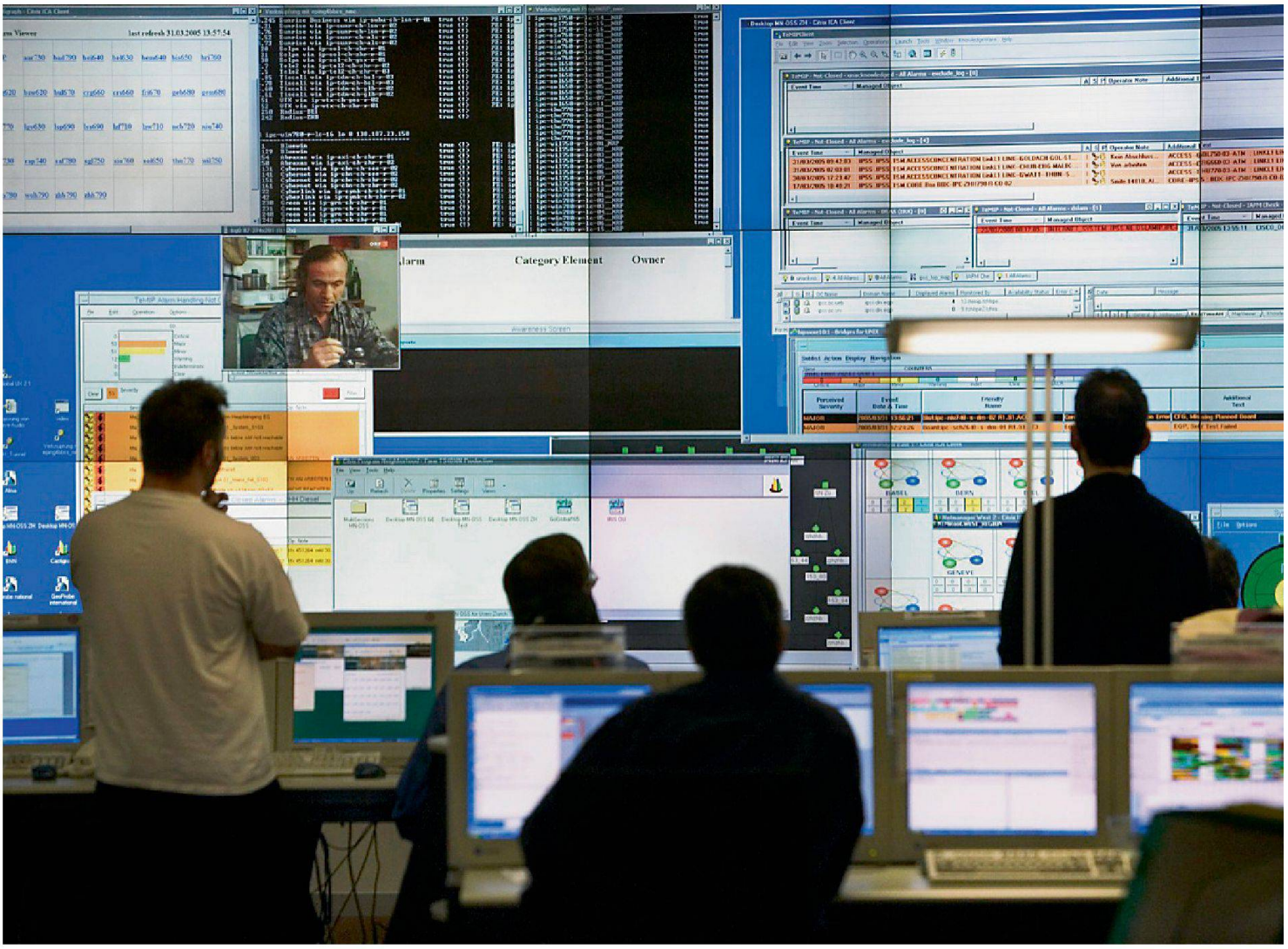
PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-391622

Das Beispiel Swisscom

Fokussieren auf das Vorhandene, nicht auf das Fehlende

Das Sichern kritischer Infrastruktur baut auf einem Zusammenspiel von Schutz, Verteidigung und Kontinuitätsmanagement auf. Doch auch die Widerstandsfähigkeit der Bevölkerung spielt eine grosse Rolle: Flexibilität und Improvisationstalent helfen; sinnvoll ist zudem die Überlegung, wie es notfalls auch ohne Mobiltelefon und Internet ginge.



Ein zentrales landesweites Monitoring sorgt dafür, dass Trends schnell erkannt werden können.

Es ist noch nicht lange her, da gab es keine E-Mails und keine Handys. In jedem Raum stand ein Festnetztelefon. Es galt das ungeschriebene Gesetz, dass man eine Person maximal einmal im Tag anruft. Hätte das Telefon einen Tag lang nicht funktioniert, hätten wir es vermutlich nicht einmal gemerkt. Sicher gehörte damals Energie zur kritischen Infrastruktur des Landes, aber IT und Kommunikation wohl kaum. Mit der Beschleunigung des Lebens, der ständigen Erreichbarkeit und den kurzen Bearbeitungszyklen von Informationen hat sich die Abhängigkeit unserer Gesellschaft von Mobiltelefonen und Internet radikal verschärft. Wenn wir ohne Telefon aus dem Haus gehen, fühlen wir uns nackt. Funktioniert das Internet nicht, bricht die Beziehung zu Freunden und Geschäftspartnern ab.

Zum Schutz kritischer Infrastruktur gehört untrennbar die Frage nach der Widerstandsfähigkeit, der Resilienz der Gesellschaft. Wenn wir wissen, wie wir ohne Computer und Telefon unser Leben meistern können, sind wir von deren ständiger Verfügbarkeit weniger abhängig. Fällt ein Teil des Netzes aus, geht das Leben – und insbesondere das Geschäftsleben – trotzdem weiter. Es lohnt sich, Zeit für diesen Gedanken zu verwenden. Und es lohnt sich, bei der nächsten Krisenstabsübung des Unternehmens auf Telefone und Internet zu verzichten. Nur schon um zu schauen, wie man ohne auskommen kann.

Die ständige Verfügbarkeit von Telekommunikationsinfrastrukturen ist keine Selbstverständlichkeit. Dazu gehören Vorkehrungen bezüglich Schutz, Verteidigung und Kontinuitätsmanagement. Netze müssen mit einer angemessenen Robustheit gebaut werden. Überwachung und Reaktion bei Unregelmässigkeiten gewährleisten, dass Auswirkungen auf die Verfügbarkeit frühzeitig erkannt und abgewehrt werden können. Im Ernstfall zahlt es sich aus, wenn man einen Plan B in der Schublade hat.

Redundante Netze

Beim Schutz und bei der Widerstandsfähigkeit geht es zuerst einmal um die Komponenten des Netzes: Kommunikation basiert auf Endgeräten wie PCs, Telefonen, Handys etc. sowie der Netzinfrastruktur. Diese besteht aus einem Kernnetz, das mit anderen Anbietern verbunden ist, und einem Anschlussnetz für die Endgeräte. Das Kernnetz wiederum besteht aus grossen, miteinander verbundenen Rechenzentren – im Falle von Swisscom aus verschiedenen, parallel betriebenen Netzen. Fällt eines weg, wird seine Leistung nahtlos durch ein anderes Netz übernommen. So sind zum Beispiel Mobilfunk- und Festnetzkerne gegeneinander redundant und können sich bei grossen Ausfällen ergänzen. Die «letzte Meile», der Anschluss zu den Privathaushalten ist nicht doppelt geführt. Spitäler und weitere kritische Infrastrukturen werden dagegen auf zwei Wegen erschlossen; so weist der letzte Zugang eine hohe Ausfallsicherheit auf. Beim Mobilfunk erfolgt eine Zweiwegerschliessung über mehrere voneinander getrennt geführte Netztechnologien und sich überlappende Funkstrecken.

Die tatsächliche Verfügbarkeit zeigt sich am Endgerät. Bei den alten Kupferdrahtnetzen wurde der elektrische Strom zum Betrieb des Endgerätes gleich mitgeliefert. Bei schnurlosen Telefonen genügt der mitgelieferte Strom jedoch nicht mehr, bei Glasfaser wird Licht, aber überhaupt kein Strom geführt. So fällt bei Stromausfällen das Telefon mit aus, auch wenn der Hausanschluss noch funktioniert. Anders verhält es sich bei Mobiltelefonen: Diese sind mit einer autonomen Batterie ausgerüstet und können über Stunden eingesetzt und im Notfall sogar im Auto aufgeladen werden. Hier entscheidet sich die Verfügbarkeit an der Strom- und Batteriepufferung der Antennen.

Keine Schwachstellen akzeptiert

Neben der physikalischen zählt die logische Widerstandsfähigkeit: Technische Anlagen müssen gegen Manipulationen und Hackerangriffe geschützt werden. Kritische Infrastrukturen sind nur dann sicher, wenn sie keine Schwachstellen aufweisen. Genau solche Schwachstellen gilt es regelmässig durch gezieltes Scanning oder durch Audits aufzudecken und zu beseitigen. Dabei kann es nützlich sein, ein ganzes System einem Hackertest zu unterziehen. Zur Verteidigung von Systemen gehört aber auch die gezielte Auswertung von Ereignissen. Jedes Sicherheitssystem liefert Daten. Wenn diese gezielt untersucht werden, können mögliche Einbruchsversuche aufgedeckt und abgewehrt werden.

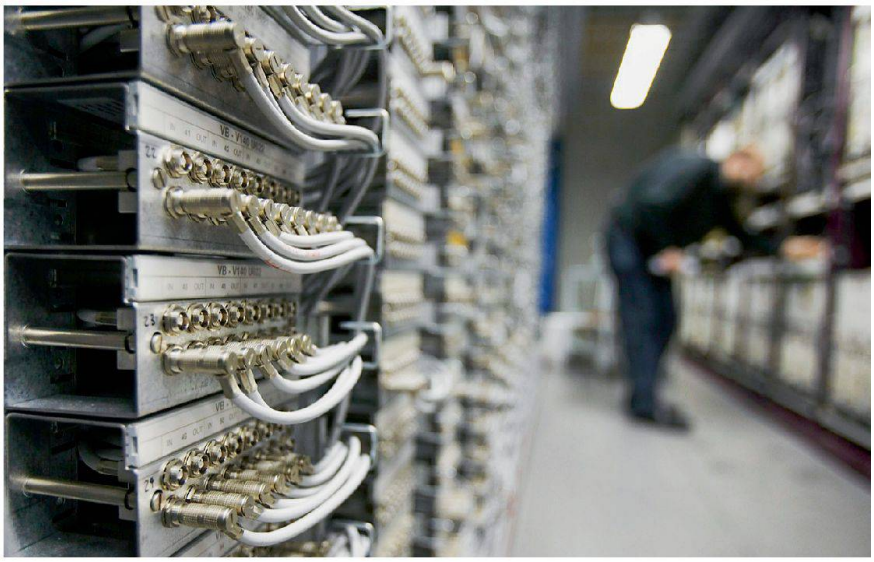
Nur wenn Unterbrüche früh erkannt, analysiert und behoben werden, ist das Netz stabil. Dies gilt auch für die unterstützende Grundinfrastruktur. Ereignisse werden an die übergeordnete Netz- und Service-Überwachungsstelle von Swisscom gemeldet. Ein zentrales landesweites Monitoring sorgt dafür, dass Trends schnell erkannt werden können. Dazu wird zentral mit allen Regionalverantwortlichen eine wöchentliche Alarm- sowie Ereignisanalyse durchgeführt. Eine interne Plattform unterstützt den regelmässigen regionenübergreifenden Austausch über Massnahmen vor und nach kritischen Tätigkeiten oder Situationen wie einer Hitzewelle oder einem Unwetter. Diese Austausche und Vorbereitungen helfen die Feedbackkultur zwischen den Regionen zu fördern. Änderungen werden nur im Rahmen eines übergeordneten Change-Prozesses durchgeführt. Sie werden unter strikter Einhaltung des Vier-Augen-Prinzips vorgenommen. Ereignisse und auch Vorfälle, die nicht zu einem Ereignis führen, werden in Zusammenarbeit mit den Partnern analysiert. Damit wird sichergestellt, dass die eigenen Ansprüche an die Förderung der Sicherheitskultur nicht nur intern, sondern auch bei den wichtigen Partnern vermittelt und gelebt werden.

Handverlesene Krisenmanager

Offen bleiben diejenigen Ereignisse mit geringer Eintrittswahrscheinlichkeit und grosser Schadensschneise. Hier hilft nur vorbereitetes Personal, das flexibel reagieren kann. Krisenmanagement ist eine Disziplin, die jeder gute Systembetreiber beherrschen muss. Abläufe müssen einstudiert und regelmässig geübt werden, wenn sie auch im Ernstfall sitzen sollen. Die Mitglieder des Krisenstabs sind handverlesen und nicht mit den Spitzen der Tagesorganisation identisch. Gute Krisenstäbe zeichnen sich dadurch aus, dass sie das Top-Management entlasten und nicht von diesem geführt werden. So kann das Top-Management in ausserordentlichen Lagen dort agieren, wo die Präsenz vor Ort am wirkungsvollsten ist.
Krisen lassen sich nicht vorhersehen, aber sie lassen sich teilweise planen. Wenn die wichtigsten Systeme und Leistungen einer Organisation bekannt sind, kann sich der Stab auf deren Aufrechterhaltung konzentrieren. Darüber hinaus können in sogenannten Service-Continuity-Plänen die Abhängigkeiten in der Technik, den Prozessen, von Schlüsselpersonen, Lieferanten und Betriebsgebäuden systematisch geprüft werden. Worst-Case-Szenarien lassen sich durchspielen und notwendige Gegenmassnahmen einüben, so dass sie im Ereignisfall rasch und sicher abgerufen werden können. Dabei ist es wichtig, dass man es nicht bei Trockenübungen belässt. Nur wenn man beispielsweise in einem Power-Off-Test die Stromstecker auch wirklich auszieht, sieht man, ob die Dieselanlage im Notfall genau so funktioniert, wie man sich das vorstellt. Regelmässiges Üben führt dazu, dass sich sämtliche Beteiligten konstant mit der Disziplin des Krisenmanagements auseinandersetzen. Die Rollen im Krisenfall sind klar und eingespielt. Dazu gehört die Schulung von Partnern. Zentrale Aspekte der Infrastruktursicherheit bleiben jedoch immer in der Verantwortung von Swisscom und werden nicht an Dritte ausgelagert. Für den Fall einer Naturkatastrophe, etwa einer Überflutung oder eines Erdrutsches, besteht eine übergeordnete Notfallorganisation mit lokalem Führungsstab. Dieser beinhaltet ein lokales Führungsteam, das auf die Grundinfrastruktur spezialisiert ist.
Das Sichern von kritischer Infrastruktur baut auf einem Kreislauf von Schutz, Verteidigung und Kontinuitätsmanagement auf. Vor allem sind wir aber alle gefordert, uns immer wieder Gedanken zu machen, wie es wäre, wenn wir auf kritische Infrastrukturen verzichten müssten. Genau diese Überlegung ermöglicht es uns, in einer Ausnahmesituation auf das zu fokussieren, was wir haben. Nicht auf das, was fehlt.

Cédric Jaton
Head of General Infrastructure bei Swisscom (Schweiz) AG

Marcel Zumbühl
Head of Security Swisscom (Schweiz) AG



Swisscom betreibt parallel mehrere Netze. Fällt eines aus, wird seine Leistung nahtlos durch ein anderes Netz übernommen.