3. Über die asymmetrisch verschlüsselte Verbindung wird ein symmetrischer Code zwischen den beiden Geräten ausgehandelt und übertragen.

4. Der symmetrische Code wird in beiden Endgeräten etabliert und die Verbindung mit diesem Code verschlüsselt.

Schlüsselaustausch nach Diffie-Hellman

Für die Verschlüsselung verwendet man eine auf Elliptische-Kurven-Kryptographie aufbauende Variante des sogenannten Diffie-Hellman Protokolls, das in Fachkreisen bekannt ist. Das Problem, aus den ersten beiden Nachrichten den geheimen asymmetrischen Schlüssel zu berechnen, bezeichnet man als Diffie-Hellman-Problem. Es ist davon auszugehen, dass dieses für den Angreifer praktisch nicht lösbar ist. Denn wenn er die beiden Nachrichten abhört, lässt sich normalerweise der symmetrische Codeschlüssel nicht berechnen. Das Problem daran ist, dass der Schlüsselaustausch jedoch nicht mehr sicher ist, wenn es einem Angreifer gelingt, sich zwischen die beiden Kommunikationspartner zu schalten und er somit die Möglichkeit erhält, Nachrichten zu verändern. Damit diese Angriffsmöglichkeit minimiert werden kann, können weitere Protokolle wie das Station-to-Station-Protokoll eingesetzt werden. Diese versehen die Nachrichten zusätzlich mit digitalen Signaturen und Message Authentication Codes. Damit soll verhindert werden, dass während des Schlüsselaustausches zwischen den beiden Endgeräten unerlaubt manipulierte Datenpakete untergeschoben werden können.

Wieder für Nichtfachleute interessant:

1. Gemäß den Angaben der Hersteller gilt „diese Technologie als die sicherste Form der Verschlüsselung und ist für den Anwender auch sehr leicht zu bedienen".

2. Die Hersteller weisen darauf hin, dass sie mit diesem gemeinsamen Projekt Abhörsicherheit aus deutschen Landen anbieten können.

Lieferung nur an besondere Zielgruppe

3. Um die Möglichkeiten der Entschlüsselung der Gespräche einzugrenzen, legen sich die Hersteller fest, dass die Geräte nur an Abnehmer geliefert werden, die eine Sicherheitsfreigabe durch Behörden wie EU oder NATO vorweisen können.

Damit wird deutlich, dass die avisierten Käufergruppen in den Bereichen von Behörden, Gemeinden und Unternehmen mit sicherheitsrelevanten Aufgaben zu suchen sind.

Die Webadresse der snom technology AG aus Berlin lautet www.snom.com, die der Secusmart GmbH aus Düsseldorf www.secusmart.com.

Stichworte: Festnetztelefonie – Secusmart – snom – Verschlüsselung – Voice-over-IP

Sicherheitsmanagement

Maßnahmen gegen den drohenden Stromversorgungs-Blackout, Teil 2

Für Krisen- und Notfallmanager

Der *Sicherheits-Berater* hatte im letzten Heft 7/2014 zehn Maßnahmenvorschläge des österreichischen Blackout-Experten Herbert Saurugg abgedruckt, die dieser nach dem 6. SIMEDIA Netzwerktreffen für Krisen- und Notfallmanager als Gastbeitrag angeboten hatte. Wie angekündigt folgen hier nun die restlichen sieben Vorschläge.

Maßnahmen:

1. Nicht ausschließlich auf autarke Stromversorgung setzen

   Immer wieder ist zu beobachten, dass in Unternehmen rasch der Schluss gezogen wird, dass man eine autarke Energieversorgung für das eigene Unternehmen benötigt. Leider werden damit viele andere Abhängigkeiten nicht adressiert, bzw. das Unternehmen nicht als System betrachtet. Die Energieversorgung ist zwar ein ganz wesentlicher Teil eines Systems, aber eben nur ein Teil. Denn was nützt diese, wenn sonstige externe Abhängigkeiten (etwa Logistik, Wasserver- und Abwasserentsorgung, Kommunikation, Mitarbeiter) nicht substituierbar sind? Durch unsere hoch arbeitsteilige und vernetzte Arbeitsweise, die noch dazu sehr stark synchronisationsabhängig ist, gibt es viele wechselseitige Abhängigkeiten, die im Alltag kaum wahrgenommen werden.

Wechselseitige Abhängigkeiten

2. Notbetrieb bzw. Notabschaltung sicherstellen

   Daher bleibt bei einem solchen Szenario nur mehr der Notbetrieb bzw. die Notabschaltung als Option. Sprich, es muss innerbetrieblich beantwortet werden, welche Ressourcen und Vorbereitungen erforderlich sind, um das Unternehmen und nicht nur Einzelkomponenten unter diesen Bedingungen sicher „herunterfahren" zu können. Zum Beispiel ist es für eine Molkerei ganz erheblich, ob bei einem Blackout die Anlage bzw. die Tankfahrzeuge noch gereinigt werden können, oder ob während des Stillstandes eine Verkeimung droht. Oder ob eine Aushärtung von Grundstoffen in Produktionsanlagen droht. Oder dass bei einem längeren Stromausfall wichtige Prozesse (wie die Kühlung) unterbrochen werden und damit schwere Folgeschäden drohen (etwa in der Forschung).

Sicheres „Herunterfahren"

3. Notfall-/Krisenplan „Blackout" vorbereiten

   Natürlich gab es bisher auch schon Ausfallszenarien, auf die man sich vorbereitet hat. Aber dabei wird meistens davon ausgegangen, dass nur Teilbereiche betroffen sind bzw. externe Hilfe zugeführt werden kann. Bei einem Blackout ist das sehr unwahrscheinlich. Beim wetterbedingten Zusammenbruch der slowenischen Stromversorgung Anfang Februar 2014 waren zu Beginn rund 200.000 Haushalte betroffen. Internationale Hilfskräfte aus Deutschland, Österreich und Tschechien haben das Schlimmste verhindert. Bei einem europäischen Blackout sind möglicherweise 200 Millionen Menschen gleichzeitig betroffen! Daher muss ein Notfall-/Krisenplan „Blackout" weit über den gewöhnlichen Betrachtungsraum hinausgehen. Was bisher kaum der Fall ist. Darüber hinaus muss in Betracht gezogen werden, dass es durch Sekundärschäden zu Engpässen an zum Beispiel Ersatzteilen (etwa bei Aufzügen) oder bei Nahrungsmitteln aus der Glashausproduktion bzw. Massentierhaltung kommt. Es ist auch ein Unterschied, ob eine Kläranlage ausfällt, oder ob möglicherweise Tausende ausgefallen sind.

200 Mio. Betroffene?

4. Auf Ausnahmezustand vorbereitet sein

   Ein besonders heikles Thema ist das Verhalten der Bevölkerung. Besonders wenn unklar bleibt, wie lange der Ausnahmezustand anhält bzw. wenn es zu Rückschlägen kommen sollte und sich die Versorgungslage in urbanen Räumen zuspitzt. Dann können wohl auch einzelne Plünderungen nicht mehr ausgeschlossen werden. Wobei hier der wesentliche Schaden nicht durch die Entwendung von Waren, sondern durch die möglicherweise Zerstörung von Infrastruktur (Scheiben, Kassensystem, Regale) entsteht. Damit würde es zu längeren Ausfällen in der lokalen Versorgung kommen. Daher sollte der Handel Überlegungen anstellen, wie mit solchen Situationen umgegangen werden könnte. Es ist mit Sicherheit

Verhalten der Bevölkerung

günstiger, nur die Waren zu „verlieren" oder besser zu verschenken, als wenn auch unnötig die Infrastruktur zerstört wird. Das muss aber vor der Krise überlegt und vorbereitet werden. Natürlich gibt es auch Unternehmen, die auch in einer solchen Situation noch handlungsfähig sein müssen. Etwa Sicherheitsdienstleister. Die Frage ist, wie unter derartig gravierenden Einschränkungen noch gehandelt werden kann. Ohne vorherige Überlegungen und Vorbereitungen wird das aber mit Sicherheit dem Zufall und Chaos überlassen. Dabei muss auch berücksichtigt werden, dass die organisierte/staatliche Hilfe ebenfalls nur eingeschränkt bzw. nur temporär handlungsfähig bleiben wird. Daher ist der Übergang in einen „gesellschaftlichen Notbetrieb" umso wichtiger.

5. Zuständigkeit zur Ausrufung des Notstandes festlegen

„Gesellschaftlicher Notbetrieb"

Eine ganz wesentliche Frage lautet daher, wer ruft die Krise „Blackout" in welcher Form aus und erklärt damit den Notstand, damit auch die weitreichenden Maßnahmen für den „gesellschaftlichen Notbetrieb" gerechtfertigt sind? Welche Kommunikationskanäle stehen dafür noch zur Verfügung, wenn nicht rasch gehandelt wird? Ganz abgesehen von den ungeklärten haftungsrechtlichen Fragen. Aber hier gilt genauso wie im klassischen Krisenmanagement – lieber zu früh alarmieren und genügend Kräfte mobilisieren, als zu spät. Und in letzter Konsequenz sind wir nicht nur für das verantwortlich, was wir tun, sondern auch für das, was wir nicht tun.

6. Krisenpläne nicht in Krisenstäben unter Verschluss halten

Mitarbeiter vorab informieren

Wie sich daraus ableiten lässt, ist wohl kaum ein Krisenstab auf ein solches Szenario vorbereitet. Denn in der Regel wird davon ausgegangen, dass die technischen Kommunikationskanäle funktionieren, ohne die ein Krisenstab kaum handlungsfähig ist, und dass im Zweifelsfall auf externe Unterstützung zurückgegriffen werden kann. Auch wenn vereinzelt ausfallsichere Kommunikationskanäle verfügbar sind, werden die gewohnte Kommunikation und damit die Handlungsfähigkeit doch wesentlich eingeschränkt sein. Es macht daher wohl wenig Sinn, den Krisenplan „Blackout", wie sonst üblich, unter Verschluss zu halten. Ganz im Gegenteil. Diesen sollten möglichst viele Mitarbeiter kennen.

7. Mitarbeiter sensibilisieren

Neue Ideen einfordern

Es geht nicht darum, alles bis ins letzte Detail zu planen oder vorzubereiten, denn das ist nicht möglich. Aber vorausgegangene Überlegungen schaffen Handlungsspielräume, die es unvorbereitet nicht gibt. Dabei ist wichtig, dass diese Überlegungen nicht nur im kleinen Rahmen durchgeführt, sondern möglichst viele Sichten eingebunden werden. Ein erfolgversprechender Weg ist, die eigenen Mitarbeiter auf dieses Thema zu sensibilisieren und zur persönlichen Vorbereitung aufzufordern. Wenn das persönliche Umfeld vorbereitet und versorgt ist, bleiben Ressourcen für andere Bereiche, wie etwa für das Unternehmen. Darüber hinaus entstehen neue Ideen oder Handlungsoptionen, an die man sonst nicht denkt. Die Stabilisierung im persönlichen familiären Umfeld und dann in der Gesellschaft selbst ist die Basis, damit Unternehmen wieder funktionieren können. Daher geht eine Vorbereitung im Unternehmensbereich weit über die Grenzen des Unternehmens hinaus. Genau genommen wird nur die Realität abgebildet. Denn Mitarbeiter sind nicht emotionslos zu betrachtende Systemelemente des Unternehmens, sondern soziale Akteure, die auch in anderen Bereichen eingebunden sind.

Stichworte: 6. Netzwerktreffen für Krisen- und Notfallmanager – Blackout – Herbert Saurugg – SIMEDIA – Stromversorgung