Penetrationstests und Blackout-Übungen

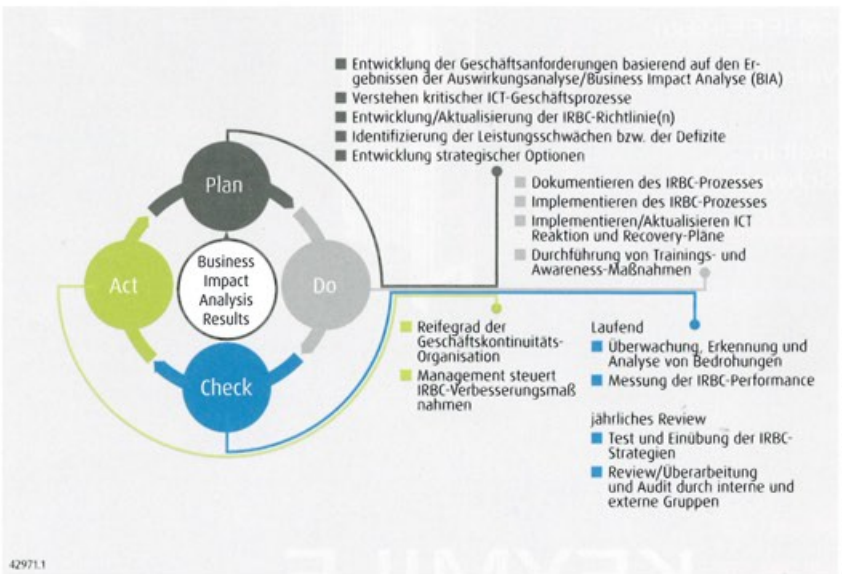
Überprüfung der Wirksamkeit eines ISMS

Der IT-Sicherheitskatalog der Bundesnetzagentur fordert im Grundsatz ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001, das sich in seinem Kern am PDCA-Zyklus orientiert. Zu diesem kontinuierlichen Verbesserungsprozess gehören auch Penetrationstests und Notfallübungen. Sie sollen sicherstellen, dass sich die umgesetzten Maßnahmen in der Praxis bewähren.

Die Digitalisierung bietet Freiräume für Wachstum und neue Geschäftsmodelle. Zugleich macht sie Unternehmen angreifbarer für Cyberkriminalität, Industriespionage und Sabotage. Gerade ihr größter Pluspunkt, die globale Vernetzung, wird dabei zum Risikofaktor – bei ungünstigem Verlauf mit kaum abschätzbaren Kettenreaktionen für kritische Infrastrukturen.

Auch wenn die Auswirkungen häufig regional beschränkt bleiben: Aufgrund zunehmend komplexer Strukturen ist die Informationsgesellschaft in ihrem Kern verwundbar. Die Energiewirtschaft ist davon besonders betroffen. Dies zeigen aktuelle Warnungen vor den Angriffen einer russischen Hackerorganisation. Mit gezielten Cyber-Attacken können Datennetze staatlicher Institutionen – wie im Jahr 2015 das Netz des Deutschen Bundestags – angegriffen oder ganze Unternehmen in ihrer Existenz gefährdet werden. Das jüngste Beispiel, der Erpressungstrojaner Locky zeigt, wie professionell und international vernetzt kriminelle Organisationen agieren.

Laut einer aktuellen Bitkom-Studie waren in den vergangenen zwei Jahren 51 % der deutschen Unternehmen von Cyberattacken betroffen. Der Gesamtschaden betrug 102,4 Mrd. € – durch Plagiate, Patentrechtsverletzungen, Erpressungen mit gestohlenen Daten und den Verlust von Wettbewerbsvorteilen. Darüber hinaus führen bekannt gewordene Attacken häufig zu einem Imageschaden für die betroffenen Unternehmen. Die Dunkelziffer bei versuchten oder tatsächlichen Cyberangriffen ist sogar noch höher, da nur jedes fünfte betroffene Unternehmen staatliche Stellen einschaltet.



Quelle: http://perspectives.avalution.com

Bild 1. Das IT-Notfallmanagement hat die Aufgabe, ein geplantes und organisiertes Vorgehen bei IT-Notfällen zu gewährleisten, um die Kontinuität des Geschäftsbetriebs sicherzustellen (Business-Continuity-Management).

In nachhaltige Sicherheitsmaßnahmen investieren

Dennoch haben bereits viele Unternehmen die Gefahr erkannt. Im Jahr 2015 ist nach einer Schätzung des Bitkom der Umsatz mit IT-Sicherheitslösungen um 6,5 % auf 3,7 Mrd. € gestiegen. Laut Marktforschungsunternehmen Gartner Inc. wurden weltweit im Jahr 2015 rund 75 Mrd. US-$ zur Cyberabwehr ausgegeben – Tendenz exponentiell steigend.

Auch die Energie- und Wasserwirtschaft ist längst sensibilisiert und investiert in nachhaltige Sicherheitsmaßnahmen. Als Kritis-Unternehmen müssen sie laut IT-Sicherheitsgesetz zwei Jahre nach Inkrafttreten der konkreten Sicherheitsanforderungen für ihre Branche angemessene technische und organisatorische Maßnahmen ergreifen. Dabei soll der Aufwand nach dem Stand der Technik im Verhältnis zu den Folgen eines möglichen Sicherheitsvorfalls stehen.

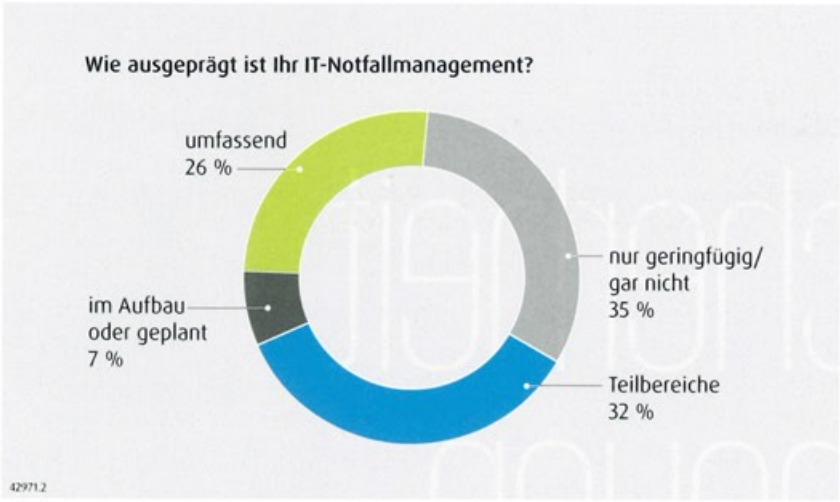
Als Mindestmaß an Informationssicherheit gelten die Anforderungen in den Normen ISO 27001 und ISO 27002 sowie in den IT-Grundschutzstandards und IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) – ergänzt um branchenspezifische Konkretisierungen zum Beispiel in der ISO 27019 für EVU oder den von der Bundesnetzagentur (BNetzA) vorgestellten Sicherheitskatalog. Zu ihrer Einhaltung müssen entsprechende Sicherheits- und Notfallkonzepte vorliegen.

Sicherheit als kontinuierlicher Verbesserungsprozess

Mindestens alle zwei Jahre ist ein nicht weiter konkretisierter Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen zu erbringen. Geprüft werden soll, ob:

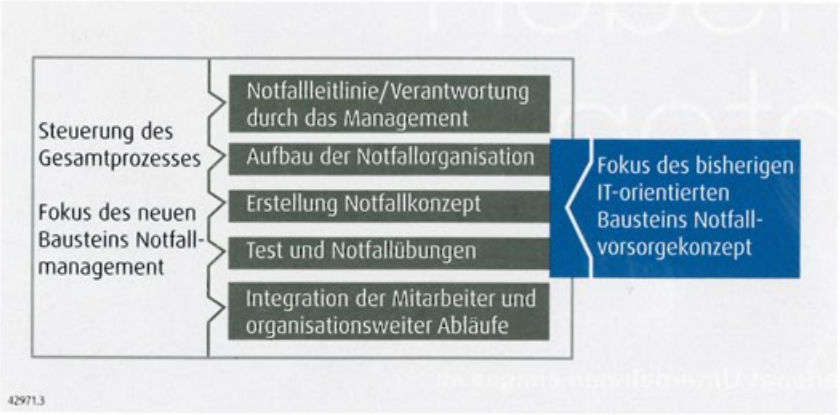
- geeignete und wirksame Maßnahmen durchgeführt werden
- ein Informationssicherheitsmanagementsystem (ISMS mit IT-Risikomanagement) betrieben wird
- kritische Assets bestimmt wurden
- ein Notfallmanagement (Business-Continuity-Management, BCM) eingeführt wurde.

Die BNetzA hat als Verordnungsgeber für die Energiewirtschaft den IT-Sicherheitskatalog herausgegeben, der im Grundsatz ein ISMS gemäß ISO/IEC 27001 fordert, das sich in seinem Kern am PDCA-Zyklus orientiert (plan, do, check, act/adjust). Zu diesem kontinuierlichen Verbesserungsprozess gehören auch



Quelle: http://ap-verlag.de

Bild 2. Umfrage: Wie ausgeprägt ist Ihr IT-Notfallmanagement?



Quelle: www.all-about-security.de

Bild 3. Aufbau eines nachhaltigen und systematischen Notfallmanagements

Penetrationstests und Notfallübungen. Sie sollen sicherstellen, dass sich die umgesetzten Maßnahmen in der Praxis bewähren (*Bild 1*).

Aufbau eines wirksamen IT-Notfallmanagements

Im Rahmen der IT-Sicherheitsstrategie hat das IT-Notfallmanagement die Aufgabe, ein geplantes und organisiertes Vorgehen bei IT-Notfällen zu gewährleisten, um die Kontinuität des Geschäftsbetriebs sicherzustellen (Business Continuity). Damit soll die Fähigkeit eines Unternehmens gezielt erhöht werden, auf Ausfälle in der Verfügbarkeit von IT-Systemen bei ihren kritischen Geschäftsprozessen angemessen reagieren sowie die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können. Dazu müssen alle kritischen Geschäftsprozesse betrachtet und beurteilt werden (Business-Impact-Analyse, BIA). Angesichts der Schlüsselrolle der IT wird dabei das Hauptaugenmerk auf die planbare Wiederherstellung der Verfügbarkeit der entsprechenden Dienste – zum Beispiel Energieversorgung – gelegt. Diese Planungen sind über Notfallübungen auf ihre Wirksamkeit in der Praxis zu überprüfen.

Penetrationstests – Sicherheit auf dem Prüfstand

Ein Penetrationstest simuliert die Vorgehensweisen eines externen und/oder internen Cyber-Angreifers, der die Absicherungsmaßnahmen der Organisation mit erheblichem Aufwand mit automatisierten Angriffen durchbrechen will. Mit verschiedenen Werkzeugen und Techniken versucht der Penetrationstester (ethischer Hacker), Sicherheitslücken zu finden beziehungsweise diese zu nutzen, um Zugang zu sensiblen Daten zu erhalten, diese zu manipulieren und/oder die Systeme zu übernehmen.

Je nach definiertem Umfang kann ein Penetrationstest auch über die bloße Betrachtung des Netzwerks hinausgehen und zusätzlich Social-Engineering- und/oder physische Sicherheitstests enthalten. Exemplarisch für solche Tests sind:

- die Ermittlung und der Versuch der Ausnutzung von Implementierungsschwächen des im Zielsystem eingesetzten Betriebssystems
- die Ermittlung und der Versuch der Ausnutzung fehlerhafter Konfigurationen des Zielsystems, zum Beispiel Zugriff auf beliebige Dateien auf einem IIS-Server
- die Untersuchung auf unerwünscht zulässige Dienste – zum Beispiel durch fehlerhafte Konfiguration oder unzureichende Filterregeln
- der Versuch, eingesetzte Dienste durch Denial-of-Service-Attacken außer Kraft zu setzen.

Anders als ein von einem böswilligen Hacker durchgeführter Angriff, hat ein Penetrationstest nicht die Ausnutzung von Schwachstellen zum Ziel, sondern deren Bestimmung und Überprüfung. Dadurch werden auch solche Schwachstellen erkannt, die sich derzeit noch nicht ausnutzen lassen.

Welche Folgen ein Netzausfall hätte, zeigte im April 2014 das Beispiel der Stadtwerke Ettlingen. Ein Hacker hatte nur zwei Tage gebraucht, um die Kontrolle über das Netz des badischen Regionalversorgers zu übernehmen. Nach Angaben des Hamburger Weltwirtschaftsinstituts würde in einer Metropole wie Berlin ein einstündiger Blackout zur Mittagszeit zu Kosten von rund 23 Mio. € führen. Gravierender wäre ein gleichzeitiger Angriff auf mehrere miteinander verwobene kritische Infrastrukturen.

In einem kürzlich durchgeführten Penetrationstest der Certigo GmbH stellte ein mittelständisches Stadtwerk die Netzwarte und das Netzleitsystem in den Mittelpunkt, die sich zu diesem Zeitpunkt noch im Zertifizierungsprozess befanden. Der Test zeigte anschaulich, wie fragil die Energieinfrastruktur ist und wie wichtig umgehende, konsequente Gegenmaßnahmen sind – Anlass genug, einen umfangreichen Maßnahmenkatalog zu erarbeiten und umzusetzen. Das Spektrum reicht dabei von zielgerichteten Investitionen – zum Beispiel in zusätzliche Firewalls und Redundanz wichtiger Systemkomponenten – bis zu notwendigen Upgrades des Betriebssystem und der Aufforderung, kleine Nachlässigkeiten im Tagesgeschäft zu überwinden sowie noch sensibler mit den Bereichen Datenschutz und Datensicherheit umzugehen.

Ermutigend ist jedoch, dass Hacker bei Cyber-Attacken nur bedingt zum Ziel kommen, da bei einem Störfall meist die Alternativszenarien verlässlich greifen und die vollständige, langfristige Kont-

rolle über die kritischen Infrastrukturen ihnen so verwehrt bleibt.

Wachsende Verletzbarkeit moderner Infrastrukturen

Damit auch künftig der Ausbau intelligenter Energiesysteme mit wirksamen IT-Sicherheitsstrategien ergänzt werden kann, setzt die Legislative auf verbindliche Branchenstandards mit Meldepflichten und personellen Ressourcen.

Schon heute wächst die Abhängigkeit der Verbraucher und öffentlichen Haushalte von der Stromversorgung, wie unter anderem die Studie »Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung« des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) belegt. Ein großflächiger Blackout würde schon nach wenigen Tagen die Versorgung der Bürger mit lebenswichtigen Gütern und Dienstleistungen zum Erliegen bringen.

Zugleich hat die Energiewende fünf Jahre nach Fukushima die Netzinfrastruktur fragiler denn je gemacht – durch den zunehmenden Ausbau der erneuerbaren Energien und den Ausstieg aus der Kernenergie bis zum Jahr 2022. Waren früher Stromausfälle meist lokal begrenzt, wird sich dies in Zukunft durch die Dezentralisierung und den Umbau hin zu einem komplexen und verflochtenen System ändern. Die Gas- und Wasserversorgung lässt sich dabei nicht unabhängig von der Stromversorgung betrachten. Abwasserpumpen sind ebenso auf Strom angewiesen wie die Heizungstechnik. Ein Zusammenbruch der Stromversorgung würde unweigerlich zu Dominoeffekten bei der Gas- und Wasserversorgung führen – bis hin zu nicht abschätzbaren Folgen des Gasaustritts bei einem massenweisen Heizungsausfall.

Ganzheitliche Risikoanalyse und Transparenz

Der Grad der Vernetzung steigt stetig – zum Beispiel durch den Aufbau leistungsstarker Smart Grids oder die Kopplung der Strom- und Gasnetze. Stadtwerke müssen daher im Rahmen einer ganzheitlichen Risikoanalyse die Funktionstüchtigkeit ihrer Infrastruktur kontinuierlich überprüfen – und das über rechtlich getrennte Unternehmensbereiche hinweg. Dass die Unternehmen in einer Industrienation wie Deutschland bestens gerüstet sind, alltägliche kleine Störungen zu meistern, haben die EVU schon oft bewiesen.

Anders ist es bei überraschenden, bisher undenkbaren Ereignissen. Je besser ein System funktioniert, desto gravierender sind die Folgen, wenn es ausfällt. Angesichts dieses Verletzlichkeitsparadoxons ist ein auf solche unerwarteten Ausnahmesituationen ausgerichtetes Notfallmanagement besonders wichtig – nicht zuletzt aufgrund des psychologischen Faktors. Nicht selten entwickelt sich eine vermeintlich zu vernachlässigende geringe Störung erst durch eine aus dem Ruder laufende Kommunikation zu einer medialen und gesamtgesellschaftlichen Krise.

Häufig findet eine solche Risikoanalyse jedoch nicht statt. Studien legen nicht nur hinsichtlich einer sorgfältigen Analyse und Nachbereitung Defizite offen. Schon bei der Einstufung als Notfall herrscht Unsicherheit. Dabei kann ohne präzise Definition eines Notfalls ein effektives Notfallmanagement nicht greifen. Zudem geht durch die Klärung von Zuständigkeiten wichtige Zeit verloren.

In der Praxis wird in diesem Zusammenhang von der »Goldenen Stunde« gesprochen. In diesem Zeitraum entscheidet sich, ob eine Krise erfolgreich bewältigt werden kann. Die Initialmeldung muss dabei nicht mit dem Ereigniseintritt – zum Beispiel dem Ausbruch eines Feuers – zusammenfallen. Dieser findet oft unbemerkt statt. Nach Meldung des Ereignisses beginnen dann die entscheidenden 60 min: die Goldene Stunde des Krisenmanagements.

Die Goldene Stunde bestimmt auch die Richtung der medialen Berichterstattung. Informiert der Versorger innerhalb kurzer Zeit die Presse sowie die politischen Vertreter, fällt die Berichterstattung erfahrungsgemäß neutral bis positiv aus. Entsteht durch einen Mangel an Information jedoch die Wahrnehmung, der Versorger wolle etwas vertuschen, kann die Berichterstattung schnell ins Negative kippen. Grundsätzlich steigt der Kommunikationsbedarf mit Ausweitung der Ereignisse.

Zugleich kommt es gerade bei der Initialmeldung auf die Sensibilität und das Gefahrenbewusstsein der Verantwortlichen an. Die Kommunikationskette reicht dabei vom Erstsicherer vom Dienst über den Meister vom Dienst bis zum bereichsübergreifend arbeitenden Krisenstab. Dabei müssen die Verantwortlichkeiten klar definiert sein und die Abläufe in regelmäßigen Übungen trainiert werden. Die zentrale Rolle sollte hier der Notfall- oder Krisenmanager einnehmen.

Aufbau eines effektiven Notfallmanagements

Der Aufbau eines nachhaltigen und systematischen Krisenmanagements dauert erfahrungsgemäß gut ein Jahr. Dann folgt die erste, kleine Übungseinheit, die sich lediglich auf das Krisenteam selbst beschränkt und am Schreibtisch stattfindet. Die zweite, erweiterte Übung bezieht andere Unternehmensbereiche ein. In einer dritten, großen Übung werden alle Betroffenen einschließlich Feuerwehr und Technischem Hilfswerk einbezogen. Um Trainingserfolge zu festigen, sind erfahrungsgemäß jährlich zwei Übungsgänge erforderlich – ein kleiner und ein großer. Durch regelmäßige Trainingseinheiten erlangen die Verantwortlichen Routine im Umgang mit unerwartet auftretenden Ereignissen, die durch die Erfolgserlebnisse bei deren gemeinsamer Bewältigung verstärkt wird. Dadurch entwickeln Mitarbeiter eine positive Grundeinstellung zu Krisen, die rationales Denken im Ernstfall überhaupt erst ermöglicht.

Prävention und Zertifizierung

Eine bewusste Vorbereitung auf den Krisenfall schützt das Unternehmen auf unterschiedlichen Ebenen vor unangenehmen Konsequenzen. Mangelndes Krisenmanagement führt aufgrund der hohen Sensibilität bei Sicherheitsthemen schnell zu einem Imageverlust. Ein funktionierendes Störungs-, Notfall- und Krisenmanagement sichert einen Versorger aber auch finanziell ab. Jeder in Prävention investierte Euro spart dem Unternehmen im Durchschnitt 7 € an Folgekosten.

Die Bewältigung einer Krise kann schnell mehrere 100 000 € kosten. Inwieweit die Betriebshaftpflichtversicherung greift, hängt jedoch auch vom Verhalten des Unternehmens im Ernstfall ab. Kommt der Versicherer zu dem Schluss, dass die Kosten aufgrund irrationaler Entscheidungen aus dem Ruder gelaufen sind, können sie die Haftung in Teilen verweigern. In diesem Fall muss der Versorger die Kosten selbst übernehmen. Ein funktionierendes Krisenmanagement bewahrt das Unternehmen außerdem vor Schadenersatzansprüchen durch die Kunden in Millionenhöhe.

DVGW und VDE stellen Führungskräften der Versorgungsbranche aktuelle Leitfäden zur Verfügung. Neben der G/W/S 1000, in der die Grundsätze zur Organisation von Versorgungsunternehmen zu Friedenszeiten geregelt werden, behandelt das Arbeitsblatt GW 1200 die Grundlagen zum Störungsmanagement. Die Hinweisblätter G/W/S 1001 und 1002 regeln die Vorbereitung und die Umsetzung von Notfall- und Krisenmanagementsystemen. Diese Vorgaben bilden zusammen die Basis für ein ganz-

heitliches Ereignismanagement in den Bereichen Störung, Notfall und Krise.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für das IT-Notfallmanagement den Standard 100-4 entwickelt. Auch die internationale Standardisierungsorganisation ISO hat einen allerdings nicht direkt zertifizierbaren internationalen Standard zum Thema Business-Continuity-Management (ISO 22301) herausgegeben. Dieser kann mit einer Konformitätserklärung an eine bestehende ISO/IEC 27001-Zertifizierung angebunden werden.

Erfahrene Partner einbinden

Voraussetzung für eine erfolgreiche Haftungsabwehr ist die inhaltlich konsequente und vollständige Umsetzung der genannten Vorgaben aus den Regelwerken sowie verschiedener regulatorischer Vorgaben zum IT-Notfallmanagement – ergänzt durch eine regelmäßige externe Überprüfung zum Beispiel in Form einer ISO 27001- oder TSM-Zertifizierung.

Im Rahmen einer effizienten Notfallplanung und eines effektiven Business-Continuity-Managements entwickelt Certigo einen Vorsorgeplan, der auf das jeweilige Unternehmen und dessen Geschäftsprozesse zugeschnitten ist. Handlungsempfehlungen und Maßnahmen zur Notfallvorsorge basieren auf den Erkenntnissen umfangreicher GAP- und Business-Impact-Analysen. Kontinuitäts- und Wiederherstellungspläne – mit regelmäßigen Übungen und kontinuierlicher Weiterentwicklung – sorgen dafür, dass das Notfallmanagement jederzeit funktionsfähig ist. Certigo orientiert sich dabei am internationalen Standard ISO 22301, dem BSI-Standard 100-4 sowie an Best Practices und dem Know-how erfahrener Security Consultants und Auditoren. Darüber hinaus gehört zum Serviceportfolio des Unternehmens die Reifegradbestimmung für bestehende Notfallkonzepte unter Berücksichtigung der jeweiligen Branchenspezifika.

Sensibilisieren, das eigene Sicherheitsengagement verstärken, nachhaltige Schutzmechanismen etablieren und frühzeitig kompetente Partner einbinden: Mit einem effektiven ISMS sind Unternehmen gut gerüstet, sich auf die positiven Seiten der Digitalisierung zu konzentrieren.

>> **Jan Arfwedson**,
Geschäftsführer,
Certigo GmbH, Gelnhausen

Dr. **Anke Schäfer**,
Dr. Schäfer PR- und Strategieberatung,
Rostock

>> jan.arfwedson@certigo.de

>> www.certigo.de

42971