Sicherheitsnetzwerk München

Informationssicherheit für kritische Infrastrukturen (KRITIS)

Umsetzungsempfehlungen zum IT-Sicherheitsgesetz

Sicherheitsnetzwerk München

Arbeitskreis KRITISCHE INFRASTRUKTUREN

Kurzbezeichnung: AK KRITIS

Sicherheitsnetzwerk München

Inhaltsverzeichnis

Einleitung

Information und Kommunikation sind unverzichtbare Bestandteile unseres gesellschaftlichen, wirtschaftlichen und persönlichen Lebens. Zum Schutz vor Angriffen mit dramatischen Auswirkungen auf unseren Staat, unsere Wirtschaft und unsere Gesellschaft wurde das lang angekündigte und heiß diskutierte IT-Sicherheitsgesetz („Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz ITSIG) verabschiedet. Nun stellt sich vielen Unternehmern die Frage: *Was bedeutet es für mich konkret?*

Dieser Leitfaden zeigt auf, wie wichtig es gerade für die vom ITSIG betroffenen Unternehmen ist, sich mit Informationssicherheit zu befassen. Neben den Eckpfeilern des IT-Sicherheitsgesetzes wird herausgestellt, dass eine gezielte Vorsorge, eine Notfallplanung und deren Umsetzung notwendig und gleichzeitig wirtschaftlich rentabel sind. Beispiele zeigen, dass sofortiger Handlungsbedarf besteht - unabhängig von der Gesetzeslage und deren Umsetzungsform - und dass richtig umgesetzte Informationssicherheit die Investitionen nicht nur rechtfertigt, sondern dass die damit verbundene Prozessoptimierung und Effizienzsteigerung auch helfen, Geld zu sparen.

In diesem Leitfaden werden konkret das IT-Sicherheitsgesetz, die betroffenen Unternehmensbereiche und die wichtigsten Maßnahmen zur Umsetzung der Gesetzesauflagen beschrieben. Der Leitfaden orientiert sich dabei an einer pragmatischen und effizienten Vorgehensweise gemäß ISO/IEC 27001. Vom Arbeitskreis *Kritische Infrastrukturen des Sicherheitsnetzwerks München* wird eine schrittweise Umsetzung empfohlen, die wie folgt strukturiert ist:

- Einführung eines Informations-Sicherheitsmanagement Systems (ISMS) in 5 Schritten
- Einführung eines Meldewesens in 4 Schritten
- Aufbau des Krisenmanagements in 7 Schritten

Im Leitfaden wird immer wieder auf Beispiele aus der Praxis zurückgegriffen, die zum besseren Verständnis beitragen sollen. Abgerundet wird der Leitfaden mit wesentlichen wirtschaftlichen Aspekten, wobei der konkrete Nutzen im Vordergrund steht.

Neben der ISO/IEC 27001 bestehen auch andere Möglichkeiten, ein ISMS einzuführen, wie z.B. BSI IT-Grundschutz oder ISIS12. Wir haben uns in diesem Leitfaden auf ISO/IEC 27001 fokussiert.

Handlungsbedarf ist sofort

Mancher Unternehmer stellt sich die Frage: Soll ich jetzt schon handeln? Oder soll ich nicht erst mal abwarten, was das Gesetz genau für mich bedeutet und ob ich überhaupt betroffen bin?

Wir sind abhängig von der IT

Praktisch jeder Geschäftsprozess wird mittlerweile durch IT unterstützt, wenn nicht gar von ihr gesteuert z.B. beim Bereitschaftsdienst oder der Fernwartung. Wenn bestimmte IT-Systeme nicht mehr funktionieren oder, noch schlimmer, aufgrund von IT-Angriffen anders funktionieren als geplant, können wichtige Geschäftsprozesse nicht mehr ordnungsgemäß abgewickelt werden oder sogar zusammenbrechen.

Ein Beispiel ist der Stromausfall 2009 in Brasilien, bei dem mehr als 800 Städte und ungefähr 40 Millionen Menschen über fünf Stunden keinen Strom hatten und der Itaipu-Staudamm mit dem weltweit zweitgrößten Wasserkraftwerk vom Netz genommen wurde.[1] Auch Deutschland ist nicht vor Attacken sicher. Durch gezielte Angriffe auf Industrieanlagen fiel z.B. 2014 die Steuerung eines Hochofens in Deutschland aus, so dass er sich nicht mehr geregelt herunterfahren ließ und sich dadurch massive Beschädigungen der Anlage[2] ergaben. Ein weiteres Beispiel ist die massive Spähattacke auf das Datennetz des Deutschen Bundestags im Jahr 2015.[3] Dass auch andere kritische Infrastrukturbetreiber, wie z.B. das Transportwesen davon betroffen werden können, zeigte eine Simulation einer ungeschützten Steuerung eines öffentlichen Transportsystems auf der letzten Cebit. Diese wurde schon kurze Zeit nach ihrer Verbindung zum Internet attackiert.[4]

Folgen

Auch dann, wenn nicht gerade das Schlimmste eintrifft, haben Unterbrechungen dieser Art meist finanzielle Verluste und oft auch erhebliche Imageschäden zur Folge. Wenn bei solchen Vorfällen auch noch Kundendaten betroffen sind, kann dies weitreichende datenschutzrechtliche Konsequenzen nach sich ziehen.

Kosten können durch verlorenen Umsatz entstehen, durch Reputationsverlust oder Regressansprüche, oder auch durch den Aufwand für die Bearbeitung, Behebung, Nachbearbeitung des eigentlichen Schadens und der entsprechenden Kommunikation an

[1] http://www.zeit.de/gesellschaft/zeitgeschehen/2009-11/brasilien-stromausfall; http://www.focus.de/panorama/welt/stromausfall-mega-blackout-stuerzt-brasilien-ins-chaos_aid_453115.html

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[3] http://www.zeit.de/politik/deutschland/2015-06/it-sicherheit-hacker-angriff-bundestag

[4] http://www.n-tv.de/technik/Hacker-lassen-Zug-entgleisen-article14728321.html

alle Betroffenen. In ernsthaften Situationen werden meist externe Spezialisten benötigt, um technische, juristische, informative und andere Aufgaben zu erfüllen, für die es intern nicht ausreichend Kompetenzen oder Kapazitäten gibt.

Fazit: Je früher und besser Sie sich vorbereiten, desto geringer sind die Risiken!

Warten Sie nicht, sondern verbessern Sie Ihre Informationssicherheitslage jetzt, um den Fortbestand Ihres Unternehmens und seiner Kernprozesse zu gewährleisten. So gilt es, im Vorfeld die Risiken zu analysieren und die notwendigen organisatorischen und technischen Maßnahmen zu ergreifen. Für den Fall der Fälle ist auch eine Krisenmanagementstruktur einzurichten.

Kontinuität Ihrer Geschäftsprozesse hat höchste Priorität, falls Sie „kritische Infrastrukturen“ betreiben

Deshalb verlangt das neue IT-Sicherheitsgesetz, dass Ihr Unternehmen ein Mindestniveau an Informationssicherheit gewährleistet und relevante sicherheitstechnische Vorfälle umgehend meldet.

Gesetze wie das Bundesdatenschutzgesetz oder branchenspezifisch das Energiewirtschaftsgesetz und das Telekommunikationsgesetz sind heute schon verpflichtend.

Das IT-Sicherheitsgesetz („Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“)

Was bringt uns das IT-Sicherheitsgesetz?

Das IT-Sicherheitsgesetz wurde geschaffen, um lebensnotwendige Einrichtungen vor Angriffen auf die Informationsstrukturen zu schützen und ein wirksames Abwehrsystem zu schaffen.

Es sieht insbesondere vor, dass die betroffenen, für kritische Infrastrukturen verantwortlichen, Unternehmen organisatorische und technische Maßnahmen ergreifen, um Sicherheitsvorfälle wirkungsvoll zu erkennen und zu behandeln. Außerdem ist der Aufbau eines Meldewesens beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als neutrale Stelle vorgesehen. Diese erstellt aus den gemeldeten Informationen ein Lagebild in dem z.B. Häufigkeit, Angriffsmuster und betroffene Branchen dargestellt werden. Außerdem werden Handlungsempfehlungen ausgesprochen.

Was bringt das Gesetz für die Betreiber kritischer Infrastrukturen?

Die Betreiber kritischer Infrastrukturen können durch die Einführung der geforderten Maßnahmen von erhöhter Stabilität und Widerstandsfähigkeit ihrer Anlagen profitieren. Und für den Fall, dass doch ein Angriff erfolgt, kann der Betrieb aufgrund der Analyse bereits bekannter Vorfälle und der aktuellen Empfehlungen der Meldestelle gezielter und schneller wieder aufgenommen werden.

Betroffene Branchen

In erster Linie sind solche Unternehmen betroffen, die zu den kritischen Infrastrukturen (KRITIS) gezählt werden und somit eine besondere Bedeutung für das Gemeinwohl des Staates und seiner Bürger haben. Das Gesetz adressiert Unternehmen aus sieben von neun KRITIS-Branchen:

1. Energie
2. IT- und Telekommunikation
3. Ernährung
4. Gesundheit
5. Wasserversorgung
6. Finanz- und Versicherungswesen
7. Transport und Verkehr

Energie sowie IT und Telekommunikation unterliegen bereits eigenen Gesetzen: dem Energiewirtschaftsgesetz bzw. dem Telekommunikationsgesetz, die entsprechend angepasst wurden. Als Beispiel für den Energiesektor hat die Bundesnetzagentur gemäß § 11 Absatz 1a EnWG im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen erstellt und veröffentlicht, der dem Schutz gegen Bedrohungen der für einen sicheren Betrieb der

Energieversorgungsnetze notwendigen Telekommunikations- und elektronischen Datenverarbeitungssystemen dient (IT-Sicherheitskatalog).

Die Wirkung des Gesetzes hängt wesentlich von der Ausgestaltung der avisierten Rechtsverordnung ab, die bestimmen wird, welche Sektoren als kritische Infrastrukturen (KRITIS) gelten und wie branchenspezifische Sicherheitsstandards eingeführt werden sollen. Wesentliche Voraussetzung für die Einstufung als KRITIS-Unternehmen sind die Größe des Unternehmens und die potenziellen Auswirkungen eines Ausfalls seiner Leistungen auf das Gemeinwohl (z.B. Anzahl der betroffenen Bürger).

Zeitliche Vorgaben sind

» Umsetzung der geforderten Sicherheitsmaßnahmen in den Unternehmen und der Nachweis deren Wirksamkeit durch ein Audit oder eine geeignete Zertifizierung (z.B. ISO/IEC 27001) 2 Jahre nach den Verabschiedungen der Rechtsverordnungen.

Dabei bedeutet die Einhaltung eines Mindestniveaus an Informationssicherheit beispielsweise den Aufbau eines ISMS (z.B. gemäß ISO/IEC 27001). Dazu gehören auch Möglichkeiten, Meldungen abzusetzen oder die Einführung von Sicherheitserkennungs- und Bewertungssystemen (z.B. durch ein Security Incident und Event Management System).

Bußgelder

Handeln KRITIS-Betreiber vorsätzlich oder fahrlässig zuwider, können sie nach **§ 14 des ITSIG mit Geldbußen von bis zu 100.000,00 EUR** bestraft werden. Darüber hinaus sind verschiedene andere Ordnungswidrigkeiten geregelt, die eine Geldbuße von bis zu 50.000,00 EUR vorsehen. Zuständig für diese Bußgelder soll das BSI sein.

Die Ziele des IT-Sicherheitskatalogs der BNetzA sind

- die Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten,
- die Sicherstellung der Integrität der verarbeiteten Informationen und Systeme und
- die Gewährleistung der Vertraulichkeit der verarbeiteten Informationen.

Der IT-Sicherheitskatalog verpflichtet Strom- und Gasnetzbetreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Kernforderung ist die Etablierung eines ISMS gemäß ISO/IEC 27001 sowie dessen Zertifizierung bis zum 31.01.2018. Bis zum 30.11.2015 mussten Netzbetreiber der Bundesnetzagentur per E-Mail einen Ansprechpartner für IT-Sicherheit und dessen Kontaktdaten benennen.[5]

[5] www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html

Einführung eines Informations-Sicherheitsmanagement Systems - ISMS - in 5 Schritten

Innerhalb eines Vorprojekts wird durch eine GAP-Analyse der personelle, prozessuale und organisatorische „Reifegrad“ des Unternehmens möglichst objektiv erhoben und bewertet. Auf Grundlage des ermittelten Ergebnisses kann mit den Detailplanungen für das ISMS-Projekt begonnen werden. Es ist in fünf aufeinander aufbauende Phasen gegliedert, die ausgehend von der Festlegung des Geltungsbereichs, über die Identifizierung der schutzbedürftigen Assets, die Schutzbedarfs- bzw. Risikoanalyse und deren Maßnahmen zum ISMS-Regelbetrieb führt.

1. Festlegung des Scopes

Der Kontext der Organisation und der Geltungsbereich des ISMS (Scope) sind festzulegen.

Es wird der Kontext der Organisation analysiert, in der das ISMS betrieben werden soll. Die aus der Kontextbetrachtung gewonnenen Erkenntnisse bilden die Grundlage für die nachfolgenden Überlegungen zur Ermittlung des Geltungsbereichs. Dabei müssen auch die Schnittstellen zu externen beteiligten Parteien z.B. Kunden, Dienstleistern oder Behörden berücksichtigt werden. Als Pflichtbestandteil des ISMS werden u.a. eine Leitlinie der Informationssicherheit sowie ein Dokumentationsrahmenwerk erstellt.

2. Identifizierung der schutzbedürftigen Informationen und Assets

Definition Asset (Wert) in Anlehnung an ISO/IEC 27001, 2.3: „Jede Art von (Vermögens-) Wert eines Unternehmens oder einer Organisation.“ Assets können somit Computerprogramme, Software, Hardware, aber auch Informationen und Dienste oder Menschen und ihre Qualifikationen sein. Es ist die Frage „Welche Assets sind schützenswert?“ zu klären. Kunden sind dabei dringend einzubinden, um die tatsächlich kritischen Assets zu identifizieren. Ein pragmatischer Ansatz zur Identifizierung relevanter Assets sind beispielsweise Interviews oder Workshops mit Schlüsselpersonen. Alle bestimmten Assets werden in einem sogenannten Asset-Register, auch Asset-Inventar genannt, klassifiziert und inventarisiert. Assets aus dem Asset-Register dienen dem Risikomanagement als Input.

3. Risikomanagement

Das Risikomanagement kann als eigener Prozess gesehen werden, dessen Input unter anderem die Assets aus dem Asset-Register sind und dessen Output Maßnahmen zur Behandlung der Risiken sind. Zur strukturierten Ermittlung von Informationssicherheits-risiken werden in einem Risikoanalyseverfahren bekannte Schwachstellen und mögliche Bedrohungen, bezogen auf schützenswerte Assets, identifiziert. Mit einer Abschätzung von Eintrittswahrscheinlichkeit (Wie häufig tritt der im Risiko beschriebene Fall ein?) und

Auswirkung (Wie hoch ist das Schadensausmaß?) kann das Risiko analysiert werden. Festgelegte Risikoakzeptanzkriterien sind bei einer Risikoeinschätzung ebenfalls notwendig. Je nach Signifikanz eines Risikos wird dem Risiko ein Maßnahmenpaket zugeordnet.

4. Etablierung von Maßnahmen zur Risikobehandlung

Nach Erstellung eines Risikobehandlungsplans werden die Maßnahmen aus dem Annex A der ISO/IEC 27001:2013 priorisiert und angewendet. Die darin enthaltenen 114 Maßnahmen sind dabei in 14 Themenbereiche zusammengefasst. Personelle Anforderungen und Kompetenzen werden festgelegt und Kommunikations- und Trainingsmaßnahmen sichergestellt. Schließlich wird ein für die Zertifizierung erforderliches Statement of Applicability (SoA) erstellt, welches die Maßnahmen zur Risikobehandlung auflistet.

5. Implementierung eines ISMS Regelbetriebs

Ein ISMS-Regelbetrieb mit Monitoring und Reporting wird implementiert und die Dokumentationsprozesse werden sichergestellt. Interne sowie Lieferantenaudits werden durchgeführt und ein kontinuierlicher Verbesserungsprozess in Form eines sogenannten Plan-Do-Check-Act Zyklus (PDCA) wird etabliert und gelebt.

Einführung eines Meldewesens in 4 Schritten

Ein wichtiger Bestandteil des neuen Gesetzes ist die Meldepflicht bedeutender Sicherheitsvorfälle. Dazu ist es notwendig, einen Sicherheitsvorfall als solchen zu erkennen, nach seiner Bedeutung einzustufen und Meldewege einzuführen.

Wir empfehlen das von uns ausgearbeitete Modell zur Einführung des Meldewesens in vier Schritten, und zwar wie folgt:

1. Stufenweiser Aufbau einer operativen Sicherheitsorganisation

Wir empfehlen den Aufbau einer Organisation im Sinne eines CERT (Computer Emergency Response Teams) oder SOC (Security Operation Center), um Sicherheitsvorfällen vorzubeugen, Sicherheitsvorfälle im Eintrittsfall festzustellen, zu dokumentieren, strukturiert abzuarbeiten und ggf. zu melden.

2. Einsatz geeigneter unterstützender Systeme wie eines Security Information und Event Management (SIEM) Systems

Für die Überwachung der Zugriffe auf Informationen, Kommunikationswege und verarbeitende IT-Systeme sollen unterstützende Protokollierungsverfahren und Monitoringsysteme eingesetzt werden. Zusätzlich muss eine möglichst automatische Filterung und Korrelation von Ereignissen erfolgen.

3. Einstufung von Sicherheitsvorfällen

Es muss ein Kriterienkatalog aufgestellt werden, in dem festgelegt wird, welche Fehler als Sicherheitsvorfälle zu bewerten sind, welche Bedeutung sie für das Unternehmen haben und wie sie zu behandeln sind. Dabei ist auch zu berücksichtigen, welche Vorfälle der gesetzlichen Meldepflicht unterliegen.

4. Festlegung eines Behandlungs- und Meldeplans

Entsprechend der Einstufung von Sicherheitsvorfällen muss festgelegt werden, was zu tun ist, durch wen und in welcher Reihenfolge benachrichtigt werden muss.

Krisenmanagement in 7 Schritten

Jede Organisation kann von Informationssicherheitsvorfällen betroffen werden, so gut die Vorkehrungen auch sind. Absolute Sicherheit gibt es nicht. Deshalb ist es essentiell, nicht nur Prozesse und Systeme zur Vorbeugung und Erkennung von Angriffen zu installieren, sondern auch die Organisation auf den „Fall der Fälle“ vorzubereiten. Nur mit einem gut organisierten Krisenmanagement können die Folgeschäden eines Vorfalls minimiert werden. Da solche Krisen glücklicherweise nicht oft auftreten, sollte regelmäßig geübt werden – genauso wie im Fall der Brandschutzmaßnahmen.

Der Aufbau eines Krisenmanagements für IT Sicherheitsvorfälle umfasst die folgenden 7 Schritte

1. Prozess für das interne Krisenmeldewesen festlegen

Dies entspricht weitestgehend dem Behandlungs- und Meldeplan im vorangegangenen Abschnitt. Außerdem muss bei besonders schwerwiegenden Vorfällen schnell ein Krisenteam zusammengestellt werden.

2. Aufgaben und Prioritäten durch das Krisenteam festlegen

Das Krisenteam hat die Aufgabe, Ursachen zu finden, schnelle Abhilfe zu schaffen, d.h. „den Stecker zu ziehen“, um Verbreitung zu verhindern und schnelle Lösungen zu finden. Insbesondere ist die Frage zu klären, wann Juristen einbezogen werden sollten und wann die Versicherungen zu kontaktieren sind.

3. Kommunikationsplan aufstellen

Jede Krise ist anders, aber es gilt, die wichtigsten Überlegungen und Checklisten zu erstellen. Wann muss die Geschäftsführung informiert werden, wann die Behörden (Meldeplicht), wann werden Vertriebsmitarbeiter informiert (um mögliche Kundenfragen zu beantworten - passiv), wann werden Kunden aktiv informiert (und mit wie vielen Details), wann die Öffentlichkeit (Presse)? Und wer entscheidet über die Formulierungen?

4. Cybersecurity-Versicherung abschließen

Es gibt mittlerweile mehrere Anbieter von Cybersecurity-Versicherungen, die sinnvoll sein können, da viele normale Risikoversicherungen explizit bestimmte Schäden durch IT-Sicherheitsvorfälle ausschließen. Voraussetzung für solche Versicherungen ist aber meistens die Umsetzung von IT-Sicherheitsmaßnahmen (ähnlich wie im IT-Sicherheitsgesetz) und ein Krisenmanagementsystem.

5. Externe Spezialisten kontaktieren

Sehr wahrscheinlich werden externe Experten bei der Bewältigung einer Krise gebraucht: IT-Sicherheitsspezialisten, Forensiker, Juristen, Krisenkommunikationsexperten, Call Center, etc.. Wenn ein Vorfall eintritt, ist aber keine Zeit, die richtigen Experten zu suchen und zu beauftragen. Deshalb müssen diese vorab an das Unternehmen gebunden werden. Oft wird das auch von einem Cybersecurity-Versicherer gefordert und unterstützt.

6. Awareness in der ganzen Organisation etablieren

Wichtig ist, dass alle Mitarbeiter verstehen, wie abhängig ihre Geschäftsprozesse von IT-Systemen sind und was schief gehen könnte, falls es einen IT-Sicherheitsvorfall geben sollte. Alle Mitarbeiter müssen genau wissen, was sie bei einem IT-Sicherheitsvorfall tun müssen, aber noch wichtiger ist, zu wissen, was sie nicht tun sollen.

7. Krisenmanagement üben

Jede Krise ist anders. Aber es muss regelmäßig geübt werden, wie die internen Prozesse ablaufen, wie die Kommunikation funktioniert und vor allem welche Mitarbeiter möglicherweise gebraucht werden. Je mehr Personen wissen, wie Krisenmanagement funktioniert, desto reibungsloser wird eine wirkliche Krise bewältigt werden.

Diese Schritte sollen in aller Ruhe ausgearbeitet werden, dann, wenn es keine Krise mit enormen Zeitdruck und Stress gibt. Wenn ein Vorfall auftritt, ist es meist zu spät. Dann kann nur noch improvisiert werden – und so werden kostspielige Fehler gemacht.

Lassen Sie uns noch ein paar konkrete Beispiele geben:

- Vorfallbeispiel 1 - Telekommunikation:

  Ein Angreifer knackt die Verschlüsselung von personengebundenen Daten, die zwischen dem Kunden-Webportal und dem CRM-Modul (Customer Relationship Management) des ERP-Systems (Enterprise-Resource-Planning) fließen. Schaden: Der Vorfall muss gemeldet werden, rechtliche Hilfe kostet Geld und Bußgelder drohen. Auch müssen Kunden informiert werden und Passwörter zurückgesetzt werden, was der Reputation schaden kann.

- Vorfallbeispiel 2 - Energieversorger:

  Ein Angreifer hackt den Kunden-Webserver und dringt in das ERP-System ein. Über die Schnittstelle zum Prozessleitsystem platziert er dort Schadcode, der die Erreichbarkeit des Systems beeinträchtigt. Schaden: Das Kraftwerk muss direkt vom Netz genommen werden, was einen kurzen Versorgungsausfall und einen teuren Stromeinkauf vom Markt verursacht. Die forensische Arbeit und Anpassung von IT-Systemen kostet viel Aufwand.

- Vorfallbeispiel 3 - Energieversorger:

Ein Angreifer manipuliert Internetdaten des Deutschen Wetterdienstes, was zu Fehlentscheidungen des Prognosesystems und des Fahrplans der Energieversorger führt. Schaden: Es wird zu wenig Strom produziert, was durch teuren Zukauf ausgeglichen werden muss. Die Suche nach der Ursache der Fehlentscheidung kostet viel Aufwand.

- Vorfallbeispiel 4 – Transport:

Im Hafen von Antwerpen wurden IT-Systeme gehackt, die Bewegung und Position von Container steuern und überwachen. Auf diese Weise konnte Kenntnis über Ort und Sicherheitsdetails von Containern erlangt werden. Dieses Wissen konnten Drogendealer nutzen, um in großem Maße Drogen an den Kontrollen vorbei unter legaler Transportware zu verstecken und zu verschiffen. Aufgefallen ist der Vorfall, als plötzlich ganze Container verschwanden. Schaden: mind. 1,3 Mio. Euro.[6] Dieses Beispiel zeigt die Manipulierbarkeit von Warenströmen bis zur Sabotage.

[6] http://www.bbc.com/news/world-europe-24539417

Investment in Informationssicherheit bringt auch Vorteile

Der Mehrwert der Informationssicherheit besteht im Wesentlichen aus den Komponenten:

- Schaden zu minimieren
- Potenziale zur Effizienzsteigerung und zur Prozessoptimierung aufzudecken und umzusetzen
- Wert von Daten zu erkennen und besser zu nutzen
- Motivation und Engagement der Mitarbeiter zu stärken.

Schadenminimierung

Die Schäden können sehr unterschiedlicher Art sein. So können in einem Unternehmen der Ausfall von Fertigungsanlagen oder Lücken in der Zulieferer- oder Auslieferungskette katastrophale Folgen haben, während in einem anderen der Verlust und Missbrauch von Kundendaten zum Ruin führen kann. Auch Datenschutzverletzungen können mit gerichtlichen Abmahnungen das ‚Aus' für ein Unternehmen bedeuten. Durch durchgängige, gezielte Maßnahmen, zum Beispiel dem Schutz der Produktionsanlagen gegen Fehlbedienungen, Einschleusen von Malware, Sabotage etc. können Ausfall und Lieferverzögerungen verhindert werden.

Wirksame und durchgängige Zugangs- und Zugriffskontrollmechanismen sowie Protokollierungssysteme tragen zum Schutz personenbezogener Daten und zur Verhinderung von Datenmanipulation bei. Systeme zum Schutz und zur Vorbeugung von Datenverlust helfen Entwicklungs- und Geschäfts-Know-How zu bewahren.

Nutzung von Potenzialen zu Effizienzsteigerung und Prozessverbesserung

Meist trifft man bei der Analyse der Geschäftsprozesse auf Bruchstellen, zum Beispiel beim Übergang von Zuständigkeiten oder Systemen. Hier hilft ein Aufbrechen des ‚Silo-Denkens' durch Förderung der Kommunikation zwischen Abteilungen und ein Sichtbarmachen der Gesamtabläufe. Dabei entstehen oft Lösungen, die nicht nur Zeit und Kosten sparen helfen, sondern auch Ideen zur Optimierung.

Häufig ist die IT-Systemlandschaft historisch gewachsen und nicht optimal aufeinander abgestimmt. Dies führt zu langsamen und fehlerhaften Abläufen sowie zu Reibungsverlusten und zu Frustration der Mitarbeiter. Nehmen wir das Beispiel von Passwörtern. Wer mag sich schon für jedes System, und es sind meistens mehrere im täglichen Arbeitsablauf, ein anderes und sicheres Passwort merken. Sinnvoll eingesetzte Single-Sign-On-Lösungen erleichtern die Arbeit der Mitarbeiter und erhöhen die Sicherheit.

Der Wert der Daten und ihre Nutzung

Daten und Informationen sind oft über die ganze Organisation verstreut und an verschiedenen Orten abgelegt. Nur wenige haben noch einen Überblick über die Zusammenhänge und Informationsflüsse. Mit dem Aufbau eines ISMS werden die schützenswerten Informationen, die Kommunikationswege und unterstützenden IT-Systeme systematisch erfasst und so die notwendige Transparenz und Dokumentation geschaffen. Hierdurch wird nicht nur der wirksame Schutz vertraulicher Daten ermöglicht, sondern auch die Möglichkeit effizienter Verarbeitung und gemeinschaftlicher Nutzung über Bereichs- und Prozessgrenzen hinweg (z.B. Synergien im Einkauf oder in der Produktion).

Motivation und Engagement der Mitarbeiter

Die Analyse von Sicherheitsvorfällen zeigt immer wieder, dass eine Vielzahl durch menschliches Fehlverhalten, gewollt oder ungewollt, verursacht wurde. Bequemlichkeit, Unachtsamkeit und Sorglosigkeit prägen oft den Umgang mit Informationen, dem Internet und sozialen Medien, im geschäftlichen wie privaten Umfeld. Dabei ist Sensibilisierung höchst wirksam, kostet nicht viel und nutzt allen - dem Unternehmen und dem einzelnen Mitarbeiter.

Über uns

Das Sicherheitsnetzwerk München als Kooperationsplattform bündelt die Kompetenzen aus Forschung und Industrie im Großraum München zur anwendungsorientierten Entwicklung von Technologien, Produkten, Dienstleistungen und Lösungen im Bereich IT-Sicherheit. Es dient der Innovationsförderung durch Forschungs- und Entwicklungskooperationen zwischen den Mitgliedern und beschäftigt sich u.a. mit den Schwerpunktthemen Industriesicherheit, sichere kritische Infrastrukturen, sichere Cloud sowie Absicherung mobiler Applikationen.

Eine besondere Stellung nehmen Aktivitäten zum Themenbereich kritischer Infrastrukturen ein, mit denen sich ein spezieller Arbeitskreis aus dem Sicherheitsnetzwerk München befasst. Von großem Vorteil ist die heterogene Zusammensetzung des Arbeitskreises, wodurch alle notwendigen Kompetenzen, die für Beratungs- und Integrationsleistungen benötigt werden, vorhanden und abrufbar sind.

Im Arbeitskreis findet eine Vernetzung von Unternehmen statt, die mit ihren unterschiedlichen Kompetenzen einerseits durch einen regen Informationsaustausch für die Verbreitung von profundem Fachwissen sorgen und andererseits ein umfassendes, regionales Leistungsportfolio in Form von Beratungsleistungen sowie zur Einführung von ISMS oder/ und zur Umsetzung von Maßnahmen anbieten.

Unsere Leistungen

In unserem Sicherheitsnetzwerk vereinen wir die Kompetenzen, die Sie auf dem Weg zur Erhöhung der Informationssicherheit in Ihrem Unternehmen bis zur Erfüllung des IT-Sicherheitsgesetzes benötigen.

Dies reicht von allgemeiner Beratung über Top-Management-Beratung zur Erstellung eines Informationssicherheitsmasterplans (z.B. Einsetzung eines Informationssicherheits-beauftragten, Durchführung einer GAP-Analyse) bis zur Unterstützung bei der Einführung eines ISMS nach ISO/IEC 27001, IT-Grundschutz oder ISIS12 und dem Management aller dazugehörigen Projekte.

Wir helfen Ihnen bei der Umsetzung der notwendigen organisatorischen, physischen und IT-Sicherheitsmaßnahmen. Und natürlich gehören auch Penetrationstests sowie die Sensibilisierung und Schulung Ihrer Mitarbeiter dazu.

Letztlich unterstützen wir Sie bei der Vorbereitung der Zertifizierung und der Durchführung von internen Audits.

Aus dem Leistungsportfolio

- Top-Management-Beratung zur Einführung eines ISMS (z.B. Erstellung eines Informationssicherheitsmasterplans, Verankerung des Risikomanagements, Durchführung einer GAP-Analyse, Assetmanagement, etc.)
- Implementierung von organisatorischen Maßnahmen
- Implementierung von physischen Maßnahmen
- Implementierung von IT-Sicherheitsmaßnahmen
- Unterstützung und Durchführung von internen Audits
- Schulung
- ISMS nach ISO/IEC 27001, IT-Grundschutz und ISIS12
- Projektmanagement und
- allgemeine Beratungsleistungen

Abkürzungen

Abs.	Absatz
AK KRITIS	Arbeitskreis Kritische Infrastrukturen
AktG	Aktiengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BNetzA	Bundesnetzagentur
CERT	Computer Emergency Response Team
CRM	Customer Relationship Management
ERP	Enterprise-Resource-Planning
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
ISIS12	**I**nformations-**Si**cherheitsmanagement **S**ystem in **12** Schritten
ISMS	Informations-Sicherheitsmanagement System
ISO / IEC 27001	Information technology – Security techniques – Information security management systems (ISMS) – Requirements spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informations-Sicherheitsmanagement Systems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation
IT	Informationstechnologie
ITSIG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, kurz IT-Sicherheitsgesetz
PDCA	Plan-Do-Check-Act Zyklus
SoA	Statement of Applicability
SOC	Security Operation Center

Ansprechpartner Mitwirkender Unternehmen

Unternehmen	Name	Straße	Ort	E-Mail	Telefon
akm software GmbH	Richter, Hans Georg	Hauptstraße 1	82008 Unterhaching	Hansgeorg.richter@akm.de	+49 89 678207-43
ESG Consulting GmbH	Dr. Bartels, Dina	Livry-Gargan-Str. 6	82256 Fürstenfeldbruck	Dina.bartels@esg-consulting.com	+49 89 9216-1737
Fraunhofer AISEC	Windhorst, Iryna	Parkring 4	85748 Garching	Iryna.Windhorst@aisec.fraunhofer.de	+49 89 3229 986-157
IT-Security Panev	Panev, Mirko	Am Ried 16a	83661 Lenggries	Mirko.panev@it-security-panev.de	+49 1607414598
WBX Consulting	Bulthuis, Willem	Fischerstraße 30	82266 Inning am Ammersee	Willem.bulthuis@wbx-consulting.com	+49 1728304996