Ausgabe 02/16

20. April 2016

Ausgabe 02 / 16

Der IT-Sicherheitsbeauftragte

Sicherheit ist kein Produkt—Sicherheit ist ein Prozess

GSG Global Service Group GmbH
EDV- und IT-Management

Themen in dieser Ausgabe:

- **Informationssicherheit**
- **Gesetzliche Vorschriften**

In dieser Ausgabe: Innenseite

Informationssicherheit

In jedem Unternehmen besteht die Notwendigkeit ***Vertrauen*** aufzubauen, Vertrauen gegenüber seinen Kunden, seinen Lieferanten und den nötigen Institutionen wie Banken oder Finanzamt. Der von uns zur Verfügung gestellte IT-Sicherheitsbeauftragte ist in erster Linie unbefangen und unvoreingenommen und kann so seine zentrale Koordinierungsaufgabe im Unternehmen wahrnehmen und somit zur Zertifizierungsreife führen, wenn dies gewollt ist.

Das IT-Security Management ist die umfassende Disziplin des Sicherheitsbeauftragten. Hierin werden alle Ebenen und Teilbereiche der IT-Security betrachtet, die zahlreiche technische und organisatorische Aspekte umfasst.

Gleichgültig, welchen Unternehmenszweck ein Unternehmen verfolgt und auch weitgehend unabhängig von der Unternehmensgröße ist es stets sinnvoll, den Bereich der IT-Security und damit auch die Aufgaben des IT-Sicherheitsbeauftragten nach bekannten Standards auszurichten. Diese Standards bestehen vor allem aus zwei Normen, die hinsichtlich des Aufbaus und Betriebes eines Information Security Management Systems (ISMS) maßgeblich von Bedeutung sind, die ISO 2700x und die Standards, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben werden. Diese beiden Standards haben sich in der Zwischenzeit weitgehend einander angenähert.

Der IT-Sicherheitsbeauftragte ist die zentrale Koordinierungsstelle im Unternehmen wenn es um die Informationssicherheit geht. Er sieht seine Aufgabe darin, ein Sicherheitskonzept zu erarbeiten, bei der Umsetzung mitzuhelfen, die umgesetzten Maßnahmen zu kontrollieren und für die anschließende weitere Betreuung zur Verfügung zu stehen.

Das Unternehmen bekommt damit die Sachkunde einen externer IT-Sicherheits-Spezialisten.

Durch verschiedene Gesetze (Basel III, KonTraG) wird die Informationssicherheit der verpflichtende Bestandteil der betrieblichen Risikoanalyse.

Gesetzliche Vorschriften

Die Handlungs– und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstandes eines Unternehmens lassen sich aus den Fragen zur Gewährleistung eines angemessenen Informationssicherheitsniveaus unmittelbar ableiten.

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) fordert ein Risikomanagement für Kapitalgesellschaften, so wird im Aktiengesetz festgelegt, dass ein Vorstand persönlich haftet, wenn Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch geeignete Maßnahmen erkannt und überwacht werden. Auch werden den Geschäftsführern einer GmbH im GmbH -Gesetz *die Sorgfalt eines ordentlichen Geschäftsmannes* auferlegt (§ 43 Abs.1 GmbHG)

Wie auch immer Sie vorgehen wollen - Schutz, Sicher, Sicherheitsbeauftragter.

So geht Sicher

Bequemlichkeit vor Sicherheit, Dringend vor Wichtig, Sparen vor Investition, Unwissenheit vor Schulung, so geht Sicher sicherlich nicht. Überwiegend sind mangelnde Ressourcen, eine Fehleinschätzung des Schutzbedarfs, ein zu knappes Budget und immer komplexer werdende IT Systeme für ein nicht vorhandenes Sicherheitskonzept verantwortlich.

Aber Achtung, verschiedene Gesetze belegen die persönliche Haftung von Geschäftsführern und Vorständen im Falle von Versäumnissen, es gilt also, Sicherheit ist generelle Chefsache.

Sicher ist sicher

Seit 2001 verfügen die USA mittels Patriot Act über immer weitreichendere finanzielle Mittel zur Verstärkung der inneren Sicherheit des Landes. Die hierzu vollzogenen Maßnahmen haben auch vor Grenzen nicht halt gemacht, weder vor Landes-, noch vor moralischen Grenzen. Jedes Mittel ist rechtens, die heutigen technischen Möglichkeiten auszunutzen, um zu Informationen zu gelangen, die sicherlich anfänglich dazu gedacht waren, terroristische Anschläge im Vorfeld zu erkennen. In der Zwischenzeit sind jedoch sowohl die technischen, als auch die finanziellen Mittel so stark gewachsen, dass eine allumfassende Informationssammlung für Terrorabwehr und Wirtschaftsspionage ausreicht, alles nach dem Motto: Wissen ist Macht.

Wollen Sie wirklich Ihre wichtigen Daten einer solchen Macht in einer Cloud anvertrauen, deren Speicherort vollkommen unbekannt ist, in einem Land, in welchem Datenschutz eine untergeordnete Rolle spielt? Die vielen Vorteile einer Cloud sollten deshalb sicher in Ihrem Zuständigkeitsbereich implementiert und integriert werden.

Kostenreduzierung

zufriedene Mitarbeiter

vereinfachte IT

Schutz vertraulicher Daten

Haben Sie ein angepasstes Sicherheitsniveau ?

Was ist in meinem Unternehmen schützenswert, wie hoch ist der Schutzbedarf dafür einzuschätzen, Fragen die innerhalb eines Sicherheitskonzeptes geklärt werden müssen. Im Gegensatz zu früher sind die heutigen Angriffsszenarien wesentlich zielgerichteter und gefährlicher, so z.B. sperrt erpresserische Ransomware die Daten der infizierten Rechner bis diese wieder freigekauft werden, darüber hinaus blüht der kriminelle Handel von Exploit Kits, die Schadcode ausnutzen und entweder zum Zweck des Datenabzugs oder der Erpressung eingesetzt werden. Meldepflicht, Imageschaden, Informationspflicht und finanzieller Verlust sind nur einige der Folgen eines nicht sorgsam betrachteten und mit einem zu geringen Stellenwert versehenen Sicherheitsbewusstsein.

Mit einem angepassten Sicherheitsniveau investieren Sie damit auch in das Vertrauen Ihrer Geschäftspartner und der Banken zur nachhaltigen Wertsteigerung Ihres Unternehmens.

Bedienen Sie sich eines VdS-Beraters für Cyber-Security aus unserem Haus.

VdS •Berater für Cyber-Security

Wieder beruhigt schlafen können

Risikomanagement

Risikomanagement ist keine lästige Pflicht, sondern die Chance IT-Prozesse zu optimieren und das Sicherheitsniveau zu erhöhen. Die Schwachstelle erkennen, das Risiko minimieren, die Bedrohung erfassen und den Angriff bewerten—das ist Risikomanagement in Kurzform— im Prinzip ganz einfach.

Schwachstellen werden sinnvollerweise mittels Penetrationstests ermittelt, natürlich unter Einhaltung rechtlicher Vorgaben. Die Ergebnisse aus Bedrohungs– und Risikoanalyse ergeben das momentane vorhandene Sicherheitsniveau des Unternehmens. Durch die Bestimmung des Schutzbedarfs erkennt man nun, welche Maßnahmen zur Abwehr von Bedrohungen erforderlich sind. Diese Erkenntnis wird in einem Sicherheitsregelwerk formalisiert erfasst.

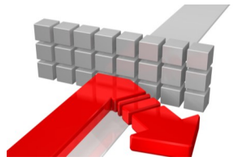
Mit diesen Maßnahmen kann das Vertrauen in Geschäftspartner und Banken nachhaltig gesteigert werden.

Bleiben Sie stressfrei.

Schütze Deine Kronjuwelen

Nach den jüngsten Ereignissen der NSA und Co sind wir alle aufgewacht, obwohl wir im geheimen immer wussten, dass es zu den Aufgaben eines Geheimdiensten gehört, sich Informationen zu beschaffen. Doch diese Sammelwut dient sicherlich nicht nur der Terrorabwehr, sondern hier sind enorme wirtschaftliche Interessen im Spiel. Wir müssen uns alle klar werden, dass die Einhaltung des Eides unserer Regierungsbeauftragten, Schaden vom deutschen Volk abzuwehren, eine Illusion darstellt. Die Konsequenz muss heißen, schütze Deine Kronjuwelen selbst.

Nicht nur der Ausspruch, „Yes, We Scan“, lässt überlegen, ob unsere bisherigen Sicherungssysteme noch so funktionieren wie erwartet oder diese wiederum entsprechend den technischen Möglichkeiten angepasst werden müssen. Es ist wegen der maßlosen und fortwährenden Datenabgriffe zwingend notwendig geworden, seine eigenen Investitionen vor dem Zugriff skrupelloser Wirtschaftsmächte zu schützen.



Hier kommst Du nicht rein

Die Aufgaben eines IT-Sicherheitsbeauftragten

Die Wahrnehmung folgender Aufgaben prägen das Bild eines IT-Sicherheitsbeauftragten:

- Erstellen einer Leitlinie
- Bestandsaufnahme und Strukturanalyse
- Modellierung des IT-Verbundes
- Aufbau eines Informations-Managementsystems (ISMS)
- Durchführen von Basissicherheitschecks
- Schutzbedarfsfeststellung
- Risikoanalyse, Notfallplanung
- Erstellen von Sicherheitsrichtlinien
- Erstellen eines Sicherheitskonzeptes
- Überprüfung von Sicherheitsvorfällen
- Mitarbeit bei sicherheitsrelevanten Projekten
- Durchführen von Schulungen und Audits
- Durchführen von Penetrationstests
- Berichterstattung an Geschäftsführung und Vorstände

Die Frage ist nicht,

ob Sie gehackt worden sind,

die Frage ist,

wann das letzte mal.

Eine Kette ist nur so sicher, wie ihr schwächstes Glied.

Computerkriminalität bedroht uns alle

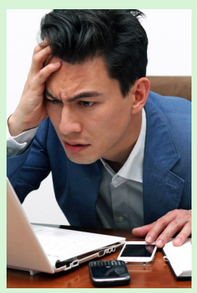
Viren, Würmer, Trojaner, Botnetze sind heute so raffiniert geworden, dass man sie nicht mehr in eine Schublade stecken kann, sie werden nun mit Malware bezeichnet.

Vollautomatisch werden heute Anwendungen und Betriebssysteme auf bekannte Schwachstellen ausprobiert und dann Malware darauf verteilt, wenn eine Schwachstelle gefunden wurde.

Die Manipulation von Webseiten gehört heute zu den einträglichsten Geschäften. Sie werden aufgefordert, diese zu besuchen und fangen sich damit automatisch einen Schädling ein.

Schutzmaßnahmen hierfür sind ein aktueller Virenschutz, aktuelles Betriebssystem und Anwenderprogramme, eine funktionierende Firewall und ein gehörige Portion Vorsicht und Misstrauen im Umgang mit dem Internet (Gratisprogramme, *schlüpfrige* Webseiten, Raubkopien, Email-Anhänge).

Nutzen Sie die Möglichkeit, sich mit eingeschränkten Rechten am System zu bewegen und vergessen Sie nicht Ihre Daten zu sichern am Besten über ein Komplett-Image (wegen der leichten Wiederherstellbarkeit).



Wie...?
Alles weg...?

ung
http://www.dr-thiele.it

Darmstädter Straße 53
D 64354 Reinheim

Telefon: (049) 6162 1051
Fax: (049) 6162 1055
E-Mail: gsg@gsg-edv.de

SIE FINDEN UNS AUCH IM WEB UNTER:
WWW.IT-SICHERHEITS-CENTER.DE

Weitere Informationen zu diesen Themen finden Sie auch in unserem deutschen IT-Security Blog:

DR-THIELE.IT

GSG-Portfolio:

- IT-Consulting
  - Datenschutz
  - Datensicherheit
- Kunden-Schulung und Support
- Hard– und Software Handel
- IT-Infrastruktur Administration und Wartung
  - Serversysteme
  - Netzwerke
  - Clientsysteme
  - Monitoring und Services
- Cloud-Provider und Managed-Services

Dr. Thiele
IT-Beratung

Das Security Framework

IT-Security kann nur dann vor Gefahren schützen, wenn Sie ganzheitlich und nach gewissen Vorgaben implementiert wird.

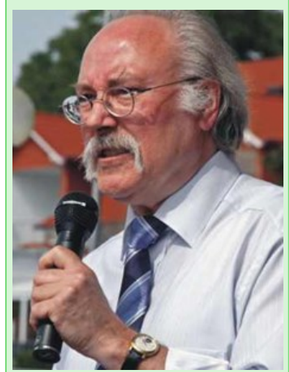
Wir entwickeln im Dialog mit Herstellern und Ihnen ein individuelles Sicherheitskonzept, welches ganzheitlich von uns eingerichtet, betreut und überwacht wird.

Vom Basisschutz bis hin zur Mitarbeiterschulung, von Social Engineering bis zu Penetrationstests, von Notfallmanagement über Schwachstellenanalyse bis hin zum Sicherheitskonzept bieten wir alle Möglichkeiten der Analyse und Umsetzung einer angepassten Sicherheitslösung. Entsprechend einzusetzende Produkte werden durch uns implementiert, angepasst und übergeben oder weiter betreut. Hierfür bieten wir auch cloudbasierte Lösungen an.

GSG kann auf eine lange Tradition von Partnerschaften zurück blicken, diese bilden ein ganz besonderes Potential bezüglich Reaktionszeiten und Support. So sind für uns (und damit auch für Sie) die besonders wichtigsten Partnerschaften auf dem Gebiet der IT-Security, IBM, Microsoft, Sophos, SecurePoint, GDATA und auch Kaspersky.

Profitieren Sie von unseren Erfahrung und lassen Sie uns Ihr Sicherheitsempfinden updaten um zu klar definierten Erkenntnissen zu gelangen, an welcher Stelle Änderungen oder Nachbesserungen vorgenommen werden müssen.

Lassen Sie uns mit einem Gespräch beginnen.



Ihr Dr. Frank H. Thiele

IT-Sachverständiger, Datenschutzexperte, IT-Sicherheitsbeauftragter und Vorstand des Kirchheimer-Kreises e.V.