Interne Organisation – ohne Vorgaben läuft nichts

Nach der Informationssicherheitsleitlinie geht es nun um die interne Organisation der Informationssicherheit. Das Ziel ist in der Norm wie folgt beschrieben: «Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.»

Was relativ einfach tönt, ist es oft nicht. Gerade in kleineren Unternehmen ist vor allem die Rollentrennung eine Herausforderung. Doch gerade dies macht eine sichere Umgebung aus. Die Massnahme aus A.6.1.1 lautet daher auch: «Alle Informationssicherheitsverantwortlichkeiten sollten festgelegt und zugeordnet sein.» Die Norm sieht eine Delegation vor, hält aber klar fest, dass die Verantwortung nicht delegiert werden kann. Folgende Rollen/Themengebiete können in einer Unternehmung sinnvoll sein:

- Geschäftsleitung, eventuell Verwaltungsrat
- Finanzen
- CISO
- Datenschutzverantwortlicher
- Projekt-Manager
- Ops-Team
- IT-Leiter und IT-Team
- HR
- Backoffice, Administration

In einem ersten Schritt geht es nun darum, Werte für das Unternehmen zu identifizieren und festzuhalten. Mehr dazu folgt im übernächsten Artikel (A.8 – Verwaltung der Werte). Jeder Wert wird in einem oder mehreren Prozessen genutzt. Diesem wird er zugeordnet und erhält damit eine dafür verantwortliche Person. Diese Wichtigkeit hatten wir bereits beim Risiko-Management erwähnt (siehe Maschinenbau 8/2018). Die Norm fordert dies in schriftlicher Form. Da viele Firmen bereits ein Inventar von Werten im Rahmen der Anlagebuchhaltung führen, ist dies ein idealer Ort, Prozesse und Verantwortlichkeiten anzuhängen. Natürlich muss die zugewiesene Person auch das entsprechende Wissen besitzen oder erarbeiten.

Rollentrennung

Das zweite Unterkapitel beschreibt die Rollentrennung. Die geforderte Massnahme zeigt schon die Wichtigkeit dieses Punktes: «Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sollten getrennt werden, um die Möglichkeiten zu unbefugter Änderung oder Missbrauch (…) zu reduzieren.» Dies ist gerade bei kontrollierenden Aufgaben essentiell wichtig. Es darf nicht sein, dass ein Firewall-Administrator selber das Firewall-Regelwerk auf Richtigkeit überprüft, oder der Administrator die Berechtigungen auf Dateien und Ordner; bei der physischen Sicherheit die Bestimmung und die Kontrolle der getroffenen Massnahmen bei Feuer, Wasser usw. Gerade solche Prüfaufgaben werden gerne an eine unabhängige und neutrale Firma übergeben, die im jährlichen Rhythmus die notwendigen Punkte durchgeht. Gleichzeitig können damit die Anforderungen einer unabhängigen Prüfung erfüllt werden (siehe Maschinenbau 10/2018).

Kontakt mit Behörden und Interessensgruppen

Im dritten Punkt wird der Kontakt mit Behörden gefordert. Dabei geht es darum, sich bereits im Vorfeld Gedanken zu machen, an wen sich das Unternehmen wenden muss, tritt ein Ereignis ein. Aus meiner Erfahrung wird dies oft mit Quellen für Informationen verwechselt. Gerade der umgekehrte Fall ist mit dieser Normanforderung gemeint. Das Unternehmen meldet Verstösse und holt sich so Hilfe zur Bewältigung. Die neue europäische Datenschutzgrundverordnung (DSGVO) verlangt beispielsweise, dass Datenschutzvorfälle innerhalb von 72 Std. gemeldet werden müssen. In der Schweiz haben wir diese Anforderung (noch) nicht. Jedoch müssen Datensammlungen mit besonders schützenswerten Daten in der Schweiz dem EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) gemeldet werden. Ganz trivial ist damit auch gemeint, dass ich weiss, welche Feuerwehr oder welcher Polizeiposten für mein(e) Gebäude zuständig ist.

Wo ist der nächste Arzt, an den ich mich bei Bedarf wenden kann. Ein Beispiel in meiner Firma: die Feuerwehr hat sich sehr für unseren Serverraum interessiert und eine Spezialübung durchgeführt. Jede Feuerwehrfrau und jeder Feuerwehrmann weiss nun, dass unser Serverraum nicht so gerne Löschwasser hat und können entsprechend reagieren. Weiter schützen sie sich vor einem Stromschlag durch die vorhandene USV-Anlage und kennen den Ausschaltmechanismus für die Gaslöschanlage. Somit für beide Seiten ein echter Mehrwert.

Der vierte Punkt fordert den Kontakt mit speziellen Interessensgruppen. Dazu muss ich natürlich zuerst wissen, welche Gruppen und Foren es gibt. Für die verschiedenen Rollen im Unternehmen sind dies natürlich verschiedene. Im Informationssicherheitsbereich lohnt sich beispielsweise eine Mitgliedschaft bei der ISSS (Information Security Society Switzerland, www.isss.ch). Auch die ISACA (isaca.ch/de/) und die ISC2 (www.isc2.org/) sind sehr aktiv in der Schweiz unterwegs und bieten regelmässige Informationsveranstaltungen und berichten in ihren Newslettern über aktuelle Gegebenheiten.

Weitere spannende Newsletter sind BSI für Bürger (www.bsi-fuer-buerger.de/) oder von heise Security (www.heise.de/security/). Zudem empfehle ich, die Newsletter der Hersteller der eingesetzten Produkte zu abonnieren. Mit dieser Massnahme soll sichergestellt werden, dass die verantwortlichen Personen auf dem Laufenden sind, was aktuelle Sicherheitsmassnahmen, neue Schwachstellen inklusive deren Bewältigung und ein Zugang zu Fachberatungen vorhanden sind.

Informationssicherheit im Projektmanagement

Der fünfte Subpunkt ist ebenfalls sehr wichtig: «Informationssicherheit im Projektmanagement.» In jedem Projekt, unabhängig um was es sich dabei handelt, muss die Informationssicherheit berücksichtigt werden. Vielleicht hat dieses Projekt auf den ersten Blick gar keine Berührungspunkte, doch dies kann sich oft und sehr schnell ändern. Informationssicherheit im Nachhinein einzubringen, ist regelmässig eine schwierige Aufgabe (Aussage: «Es lief ja doch auch schon vorher gut»). Die Informationssicherheit sollte dabei immer ein zu berücksichtigendes Ziel sein. Vermutlich lohnt es sich, bereits früh eine Risiko-Analyse durchzuführen:

- Werden schützenswerte Daten verarbeitet?
- Erfolgt ein Zugriff auf kritische Systeme?
- Müssen Durchgänge durch die Firewall geöffnet werden?

Das damit verbundene Risiko sollte schriftlich festgehalten und durch den Projektleiter entweder (bewusst) akzeptiert oder mit begleitenden Massnahmen versehen werden.

Für mich an der falschen Position ist das Kapitel A.6.2 «Mo-

bilgeräte und Telearbeit». Passender wäre es im Kapitel A.12 Betriebssicherheit versorgt gewesen. Mobilgeräte sind heute nicht mehr wegzudenken. Von überall auf der Welt kann ich auf die Daten in meiner Firma zugreifen und damit arbeiten. Nur schon der Blick am Morgen beim Bahnhof zeigt, praktisch alle haben ein Handy vor der Nase. Dieses neue Arbeiten muss unbedingt berücksichtigt werden. Zuerst gilt es zu definieren, ob das eigene Gerät überhaupt zu Firmenzwecken genutzt werden darf. Oft erlebe ich, dass der Zugriff auf E-Mails, Kalender, Kontakte und Notizen erlaubt ist. Doch damit gehen bereits vertrauliche Informationen wie Kundendaten und E-Mails weg aus dem geschützten Bereich der Firma. Daher muss das Unternehmen Vorgaben zum Schutz der Geräte definieren, wie zwingendes:

- sicheres Passwort,
- sofortige Bildschirmsperre bei Nichtnutzung,
- die Verschlüsselung der Daten,
- die baldige Aktualisierung des Betriebssystems und der genutzten Apps,
- dem Verhindern der Installation unerwünschter Software auf dem Gerät und
- Vorgaben zur Nutzung von Web-Diensten.

Weiter gilt es zu definieren, wie das Back-up sichergestellt oder das Löschen aus der Ferne (Remote Wipe) bei einem Verlust durchgeführt wird. Auch gilt es Vorgaben zu definieren, wie fremde Wireless-Netzwerke genutzt werden dürfen. Immer wieder kann gelesen werden, dass Hacker über das Hotel-Netzwerk Zugriff auf ihre Opfer erlangen konnten. Eine einfache Schutzmethode ist es, dass zwar das Hotel-Netzwerk genutzt werden darf, jeglicher Zugriff auf Dienste nur verschlüsselt erfolgen kann (VPN, HTTPS usw.).

Telearbeit

Der zweite Teil umfasst die Telearbeit. Damit ist beispielsweise das Arbeiten zu Hause gemeint. Einige Firmen ermöglichen den Mitarbeitenden das Arbeiten via Citrix oder RDP (Remote Desktop) auf dem privaten Gerät. Dabei gilt es zu berücksichtigen, wie die Zugangsdaten gespeichert werden, ob noch andere Personen (Partnerin/Partner, die Kinder usw.) ebenfalls das gleiche Gerät nutzen dürfen, wie der physische Schutz des Gerätes (Stichwort Diebstahl) sichergestellt ist sowie Anforderungen an das vorhandene Heimnetzwerk. Zu berücksichtigen sind auch Anforderungen an die Firewall, das Antivirenprogramm und die regelmässige Aktualisierung des Geräts. Gerne vergessen wird die Nutzung von Software. Im Vorfeld muss das Unternehmen abklären, wie die Software korrekt lizenziert wird, damit es nicht zu einer hohen Geldstrafe kommt.

Mit diesen Vorgaben kann auch ein Arbeiten von unterwegs oder zu Hause sicher durchgeführt werden und die Hoheit der Daten bleibt beim Unternehmen erhalten.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Anzeige