it-sa 2019

ISO 27001
Die Rückkehr der ISMS-Ritter

Version 1.0
Stand 25. September 2019

Jörg Völker

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

1 Die dunkle Seite der Macht 3
2 Die Versuchungen 3
3 Was tun? 4
4 Was fordert ISO / IEC 27001 5
5 Wie setze ich ISO/IEC 27001 konkret um? 5

1 Die dunkle Seite der Macht

Die Tätigkeit als Informationssicherheitsbeauftragter gleicht dem Kampf eines Jedi-Ritters gegen die dunkle Seite der Macht. Die dunkle Seite der Macht ist äußerst verführerisch, da sie schnellen, einfachen und unkomplizierten Erfolg verspricht.

Doch die negativen Seiten der dunklen Macht sind den Meisten zu Beginn völlig unklar, oder noch schlimmer, egal.

Im Star Wars Universum äußert sich die Hingabe zur dunklen Seite der Macht in gesteigerter Wut, Hass und Aggression. Übertragen auf die Informationssicherheit im beruflichen Umfeld verführt die "dunkle Seite der Macht" zum leichtfertigen Umgang oder zur unbedarften Preisgabe vertraulicher, geschäftlicher Informationen sowie persönlicher und personenbezogener Daten.

Die Versuchungen sind dabei groß, bspw. die leichtfertige Verteilung von Unterlagen, die unbedachte Nutzung von mobilen Datenträgern, ein sorgloser Umgang mit Passwörtern, das lautstarke Telefonieren in der Öffentlichkeit, und zunehmend die Nutzung von Online Collaboration Tools wie bspw. monday.com, Doodle, WhatsApp, WeChat, Dropbox, Slack, etc.

Vielen Beschäftigten ist häufig nicht klar, dass die Nutzung solcher Online Dienste quasi dem Betrieb einer „Schatten-IT“ gleich kommt. Das bedeutet, dass das Unternehmen keinerlei vertragliche, oder rechtliche Ansprüche gegenüber den Betreibern dieser Online-Dienste geltend machen kann. Unberücksichtigt bleiben dabei häufig bspw. Fragestellungen wie:

- Welche Service-Qualitäten bietet der Dienstleister eigentlich konkret an?
- Wo werden die Daten gespeichert? Nicht zuletzt durch die Verschärfungen der EU-DSGVO gerade hinsichtlich der Speicherung personenbezogener Daten eine recht brisante Frage!
- Wer kann auf die Daten tatsächlich zugreifen? Diese Frage betrifft sowohl eigene Mitarbeiterinnen und Mitarbeiter, als auch Dritte, wie Geschäftspartner, aber auch Beschäftigte des Service-Erbringers.
- Wie kann zuverlässig sichergestellt werden, dass Benutzer, die eigentlich keinen Zugriff mehr benötigen, die Zugriffsrechte entzogen werden?
- Wie werden die Daten grundlegend geschützt (Verschlüsselung), wie gesichert (Backup) und bei Bedarf zuverlässig gelöscht?
- Ist die geschäftliche Nutzung dieser Dienste überhaupt gestattet, oder ist die durch die AGBs der Betreiber untersagt?

Dies sind nur ein paar der Fragen, die sich stellen. Sie zeigen aber deutlich, dass gerade aus Sicht der Informationssicherheit hier ein dringender Handlungsbedarf besteht.

2 Die Versuchungen

Die Probleme und Gefahren, die durch den leichtfertigen Umgang mit Informationen und der Nutzung solcher Online-Dienste entstehen, werden häufig durch die Mitarbeiterinnen und Mitarbeiter unterschätzt.

Doch woran liegt das? Warum neigen Menschen dazu diese Gefahren zu übersehen oder zu ignorieren?

Wie so häufig gibt es auch in diesem Fall keine einfache Erklärung. Mögliche Ursachen sind:

Unwissenheit:

- Den Beschäftigten ist der eigentliche Wert der Informationen, mit denen sie arbeiten, nicht bewusst.
- Evtl. Geheimhaltungsvereinbarungen mit Kunden oder Lieferanten sind nicht allen Beteiligten bekannt.
- Häufig sind Beschäftigten die Gefahren nicht bewusst, die mit der Nutzung solcher Online-Dienste verbunden sind.
- Häufig werden den Beschäftigten nicht die geeigneten technischen Hilfsmittel zur Verfügung gestellt, oder sie werden nicht über die bestehenden Möglichkeiten informiert.

Bequemlichkeit

- Sicherheitsaspekte zu berücksichtigen und entsprechend zu handeln ist häufig mit Aufwand verbunden (bspw. ist es deutlich einfacher größere Datenmengen über Dropbox zu verteilen, anstatt diese auf CD/DVD zu brennen und per Post zu versenden).

Sorglosigkeit

- Auch die Motivation aktuelle Trends nutzen zu können ist eine nicht zu unterschätzende Triebfeder. Dem Reiz neuer Technologien unterliegen gerade technik-affine Menschen recht schnell, insbesondere, wenn einem vermeintliche Vorteile aus dem privaten Umfeld suggerieren, diese Vorteile auch im geschäftlichen Bereich anwenden zu können (bspw. WhatsApp, WeChat, …).

Alles mögliche Gründe, warum Beschäftigte der „dunklen Seite der Macht“ erliegen und Informationen nicht gemäß dem eigentlichen Schutzbedarf der Informationen behandeln.

3 Was tun?

Was kann man gegen diese „dunkle Seite der Macht“ unternehmen? Wie kann man dem Unternehmensinteresse, aber auch den stetig steigenden Anforderungen von Kunden und Auftraggebern (Beispiel: Anforderungen zur Informationssicherheit in der Automobilindustrie, TISAX), oder gesetzlichen Vorgaben (Bespiel: IT-Sicherheitsgesetz, BSI-Gesetz für Betreiber kritischer Infrastrukturen und Anbieter bestimmter digitaler Dienste) gerecht werden?

Ein zielgerichtetes, strukturiertes Vorgehen erleichtert das Identifizieren der Informationssicherheits-Risiken für ein Unternehmen und die Umsetzung angemessener Maßnahmen.

Die ISO/IEC 27001 „Informationssicherheitsmanagementsysteme – Anforderungen“ bietet hier eine entsprechende Hilfestellung.

Die Norm definiert Anforderungen an den Aufbau, die Umsetzung und die Prozesse für Betrieb, Überwachung, Überprüfung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS). Der Standard umfasst ebenfalls Anforderungen an die Implementierung von Sicherheitsmaßnahmen, die an die individuellen Bedürfnisse eines Unternehmens angepasst werden müssen.

Bei Bedarf ermöglicht ISO/IEC 27001 zudem eine Zertifizierung des Informationssicherheitsmanagementsystems.Damit hat ein Unternehmen einen unabhängigen Nachweis, dass es Informationssicherheit ernst nimmt und lebt.

4 Was fordert ISO / IEC 27001

ISO/IEC 27001 stellt quasi eine Toolbox zur Verfügung um Informationssicherheit im Unternehmen zu steuern.

Die Umsetzung von ISO/IEC 27001 erfordert:

Prozesse zu etablieren

ISO/IEC 27001 fordert die Etablierung von Informationssicherheitsprozessen. Dazu zählen u.a. Prozesse zur Festlegung der generellen Informationssicherheitsziele des Unternehmens (Informationssicherheitspolitik), Ausarbeitung von Vorgaben (Richtlinien) zur Informationssicherheit, Bewertung der Informationssicherheit, Durchführung von Audits, Verbesserung der Informationssicherheit.

Risiken zu identifizieren und bewerten

Informationssicherheitsrisiken müssen identifiziert, analysiert und bewertet werden. Basierend auf diesen Risikoanalysen muss der Umgang mit den Risiken dargelegt werden und ggf. Maßnahmen zur Risikoreduzierung ergriffen werden.

Geeignete Sicherheitsmaßnahmen umzusetzen

Grundlage für die Ergreifung von Sicherheitsmaßnahmen bilden also sowohl die festgelegten, generellen Informationssicherheitsziele als auch die durchgeführten Risikoanalysen. Dieses Vorgehen soll gewährleisten, dass die für ein Unternehmen geeigneten und wirtschaftlich vertretbaren Sicherheitsmaßnahmen ergriffen werden und nicht unbedingt die absolut möglichen technischen und organisatorischen Maßnahmen.

Zu kommunizieren und zu sensibilisieren

Die Norm sieht explizit vor, dass Beschäftigte über die Vorgaben und die damit verbundenen Sicherheitsmaßnahmen ausreichend geschult werden. Dies umfasst auch das Schaffen einer allgemeinen Awareness für Informationssicherheit, also die Sensibilisierung der Beschäftigten in der Art, dass Informationssicherheit alle betrifft und alle für die Wahrung einer angemessenen Informationssicherheit mitverantwortlich sind.

Zu kontrollieren und zu verbessern

Durch regelmäßige Prüfungen sollen Missstände und unpassende Prozesse und Maßnahmen aufgedeckt sowie Verbesserungspotentiale aufgezeigt werden. Dies soll einer stetigen Optimierung und Verbesserung des Informationssicherheitsmanagementsystems und somit letztendlich der Informationssicherheit im Unternehmen dienen.

5 Wie setze ich ISO/IEC 27001 konkret um?

Beispielsweise mit dem System ***ISMS ready2go*** von Secorvo. ***ISMS ready2go*** enthält ein vollständig einsatzbereites Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC ISO 27001.

Durch ***ISMS ready2go*** können mit überschaubarem Aufwand und geringen Anpassungen in kurzer Zeit die Anforderungen und Vorgaben von ISO/IEC 27001 erfüllt und eine Zertifizierung effizient vorbereitet werden.

Das ***ISMS ready2go*** enthält:

Vordefinierte Prozesse

Alle notwendigen ISMS-Prozesse sind vordefiniert und implementiert. Für alle Prozesse ist festgelegt, wann und wie diese Prozesse durchgeführt werden und welche Tätigkeiten dabei durchzuführen sind. Zu diesen Prozessen zählen u. a.:

- Erstellung und Verabschiedung von Richtlinien und Maßnahmenvorgaben
- Durchführung von Risiko-Analysen
- Planung von ISMS-Schulungen
- Durchführung von internen und externen Audits
- Behandlung von Ausnahmegenehmigungen

Vordefiniertes Rollenkonzept

Alle ISMS-relevanten Rollen, Funktionen und Tätigkeiten sind beschrieben. Hinter den Prozessen liegen rollenbasierte Arbeitsabläufe, sodass die Prozesse direkt durchgeführt werden können.

Muster-Vorlagen

Alle nach DIN ISO/IEC 27001 erforderlichen Dokumentationen liegen bereits vollständig ausformuliert vor und können bei Bedarf an eigene Erfordernisse angepasst werden. Hierzu zählen u. a.:

- Vorlage für die Ausgestaltung des Geltungsbereichs
- Prozessbeschreibungen
- Informationssicherheitsrichtlinie
- Richtlinie zur Informationsklassifizierung
- Vorgaben und Maßnahmen gemäß Anhang A DIN ISO/IEC 27001
- Vorlagen für die Gestaltung von Management- und Auditberichten

Dokumentation und Reporting

Alle ISMS-relevanten Dokumente werden mit dem integrierten Dokumentenmanagement automatisch versioniert und die Freigaben dokumentiert. Berichtsverfahren und dokumentierte Nachweise belegen die korrekte Anwendung der DIN ISO/IEC 27001.

Getrennte Bereiche

Das ***ISMS ready2go*** umfasst drei separate Bereiche für die interne ISMS-Steuerung und den -Betrieb sowie einen öffentlicher Bereich zur Bekanntgabe von Dokumenten, Vorgaben und Regelung.

Ferner ist ein Bereich „Archiv“ enthalten, in dem obsolete oder nicht mehr benötigte Dokumente aufbewahrt werden können.

Der interne Bereich ist dem ISMS-Kernteam vorbehalten. Hier werden alle ISMS-Prozesse durchgeführt, ISMS-Dokumente erstellt, und freigegeben, sowie notwendige ISMS-Berichte erzeugt. Daher können auf den internen Bereich und das „Archiv“ nur registrierte Anwender mit den erforderlichen Zugriffsrechten zugreifen.

Anpassungen und Erweiterungen

Das ***ISMS ready2go*** kann an das Corporate Design des Auftraggebers angepasst werden. Bereits vorhandene Richtlinien oder sonstige relevante Dokumente können direkt in das ***ISMS ready2go*** eingebunden werden.

Web-Tool zur Durchführung von Risiko-Analysen

Die notwendigen Risiko-Analysen gemäß der definierten Risiko-Management-Methodik können mit einem ebenfalls in ***ISMS ready2go*** enthaltenen Web-basierten Tool durchgeführt werden.