Betriebssicherheit

Das Kapitel A.12 der ISO-Norm behandelt alles rund um die ICT. Das Ziel ist dementsprechend einfach: «Der ordnungsgemässe und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.»

Bereits der erste Punkt ist eigentlich selbstverständlich, ist aber für viele Unternehmen eine Herausforderung: «Die Betriebsverfahren sollten dokumentiert und allen Benutzern, die sie benötigen, zugänglich sein.» Die Dokumentation muss dabei keine Doktorarbeit sein. Die Anforderung daran ist, dass eine entsprechende Fachperson mit dieser arbeiten und Anpassungen vornehmen kann. Dazu gehören beispielsweise:

- Umfang
- Viren- und Firewall-Schutz
- Aktualisierung von Systemen (Patchen)
- Mobile Datenträger
- Anforderungen an Passwörter
- Namenskonventionen (Systeme, Benutzer usw.)
- Netzwerkaufbau (IP, VLAN, Verkabelung, Zugang usw.)
- Hardware, Software, Virtualisierung
- Active Directory Konventionen
- Backup und Wiederherstellung von Systemen und Daten
- Vorgehen bei technischen Fehlern
- Verantwortliche Personen
- Art und Durchführung von Überwachungen (Monitoring)
- Lizenz-Management

Änderungen

Auch für Änderungen sollte ein Ablauf definiert werden (A.12.1.2). Dieser könnte beispielsweise so aussehen:

1. Festhalten von Änderungswünschen und neuen Anforderungen
2. Prüfen dieser Punkte, Feststellen von Abhängigkeiten
3. Genehmigung durch entsprechende Stelle
4. Planung von Änderungen (zum Beispiel in welchen Sprint wird die Änderung durchgeführt)
5. Informieren der involvierten Personen und Stellen (inkl. allfälligen Externen)
6. Durchführen der Änderung
7. Informieren der involvierten Personen und Stellen (inklusive allfälligen Externen)
8. Anpassen beziehungsweise Erweitern der Dokumentation

Die Norm hat für die Planung von Kapazitäten einen eigenen Punkt spendiert: A.12.1.3. Damit sind auf technischer Ebene CPU-Leistung, RAM, Festplattenplatz, aber auch Personen, Büros und Einrichtungen gemeint. Neben technischen Elementen ist auch die Zeit eine wichtige Ressource: wo kann Zeit beispielsweise gespart werden, wenn Prozesse optimiert werden?

Der vierte Punkt (A.12.1.4) gibt praktisch in jedem Unternehmen Anlass zur Diskussion: die Trennung von Entwicklung, Test und Produktion. Es sollte unter allen Umständen verhindert werden, dass Entwickler auf produktiven Systemen arbeiten oder Änderungen vornehmen. Trotz Widerständen in vielen Diskussionen, die ich bereits führen durfte, ist dies auf einfache Art und Weise möglich. Es braucht aber dazu den Willen und entsprechende Prozesse. Klar kann es Ausnahmen geben, wenn zum Beispiel ein akuter Vorfall vorliegt und es schnell gehen muss. Aber dann kann die Änderung im Vier-Augen-Prinzip durchgeführt werden.

Trennung

Bei einer optimalen Drei-Stufen-Architektur können Entwicklungen auf der Entwicklungsumgebung durchgeführt werden. Hier kommen nur Test-Daten zum Einsatz. Original-Daten können dafür beispielsweise anonymisiert oder pseudomisiert werden. Damit sind auch die Anforderungen aus der DSGVO der EU korrekt umgesetzt. Nach einer formellen Freigabe geht es einen Schritt weiter. In der Test-Umgebung wird auf Herz und Nieren überprüft, ob alle Anforderungen korrekt umgesetzt wurden. Je nach Definition können hier wiederum veränderte oder bei entsprechenden Sicherheitsmassnahmen auch Original-Daten verwendet werden. Auch hier erfolgt wiederum eine formelle Freigabe. Gemäss definiertem Ablauf werden die Veränderungen geplant in die Produktion eingespielt. Allfällige Abhängigkeiten müssten bereits bei den Tests entdeckt und vorbereitet werden. Sobald die Änderungen auf den produktiven Systemen durchgeführt sind, erfolgen wiederum Tests und eine finale Freigabe aller Anpassungen. Hinweis: die Norm behandelt in Kapitel A.12.5 auch Software im Betrieb. Hier gilt es sicherzustellen, dass die produktiven Systeme nicht beeinträchtigt werden, wenn Updates und Erweiterungen eingespielt werden.

Malware

Malware (Abkürzung für Malicous Software, jegliche unerwünschte Software), wie Viren, Würmer, Trojanische Pferde oder Spy-/Adware sind eine Plage. Gemäss dem unabhängigen Institut AV-Test (www.av-test.org/de/) kommen jeden Tag 350'000 neue Schädlinge dazu. Jedes Unternehmen tut gut daran, einen entsprechenden Virenschutz umzusetzen. Dies betrifft nicht nur Windows-Systeme, sondern auch Linux, Mac, Handy und Tablet. Inzwischen gibt es für alle Plattformen Ungeziefer, das man nicht auf dem eigenen Rechner möchte. Daher gilt es eine mehrstufige Abwehr zu planen, beispielsweise auf dem Gateway (zum Beispiel

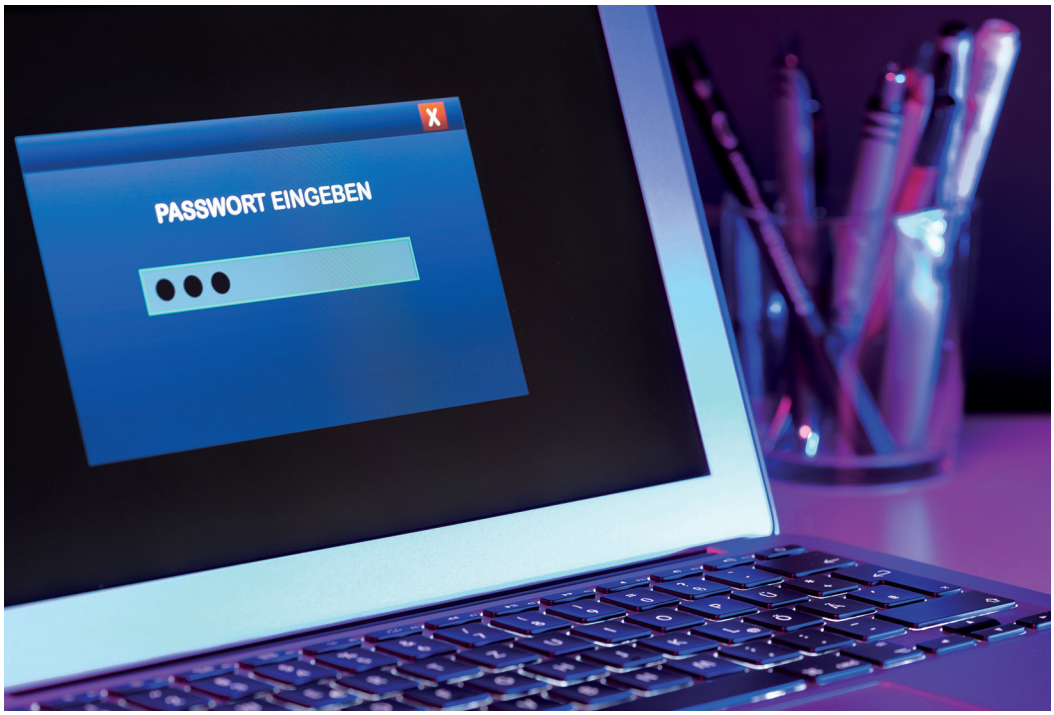

Bild: Archiv

Die Log-Informationen sind sensitiv und müssen dementsprechend vor fremden Zugriffen geschützt sein.

Firewall), dem E-Mail- und Datei-Server, wie auch auf dem Endgerät. Eine Weisung gehört ebenfalls dazu. Darin werden unter anderem der Umgang mit dem Antivirenprogramm (auf keinen Fall ausschalten), korrekte Reaktion bei Virenwarnungen, der Umgang mit mobilen Speichern (zum Beispiel USB-Sticks) und das Installations-Verbot für zusätzliche Software beschrieben. Ein Unternehmen sollte auch regeln, wie Updates von Software und Pattern (Antiviren-Aktualisierung) verteilt und installiert werden. Dies sollte möglichst zeitnah geschehen, da Hacker erfahrungsgemäss zuerst bekannte Schwachstellen angreifen.

Backup

Das dritte Kapitel umfasst die Lebensversicherung für ein Unternehmen: die Sicherung von Daten und Programmen. Allein darüber könnte ein ganzer Artikel geschrieben werden. In der Ausgabe 2008.7 finden Sie Informationen dazu. Das Wichtigste zusammengefasst:

- Aktuelle Dokumentation
- zu sichernde Daten (und Systeme)
- Sicherung von mobilen Datenträgern und mobilen Geräten
- Art der Sicherung (vollständig oder nur Veränderungen)
- Intervall der Sicherung
- Speichermedien
- Lagerung/Aufbewahrung
- Zuständigkeiten
- Wiederherstellungs-Tests

Protokollierung

Protokoll-Daten helfen, Fehler zu erkennen und Massnahmen zu ergreifen. Aus diesem Grund verlangt A.12.4: «Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.» Dies können Meldungen von Servern, Netzwerkgeräten, Störungen, Alarme, Zugriffe, (Konfigurations-)Änderungen, Nutzung von privilegierten Programmen usw. sein, die idealerweise zentral gesammelt und regelmässig ausgewertet werden. Darin enthalten sollten mindestens sein: Datum/Uhrzeit, Benutzer und/oder System und/oder IP-Adresse, Aktivität. Damit eine Korrelation der verschiedenen Daten möglich ist, müssen die Systemzeiten auf allen Systemen korrekt konfiguriert sein. Dazu stehen im Internet diverse Zeitserver zur Auswahl. Eine gute Anlaufstelle ist www.pool.ntp.org/zone/ch.

Die Log-Informationen sind sensitiv und müssen dementsprechend vor fremden Zugriffen geschützt sein. Da auch Log-Daten von Administratoren gesichert werden, müssen diese so geschützt sein, dass auch Administratoren diese nicht löschen können. Ein dafür zentrales System ist eine gute Möglichkeit dafür. Als Open-Source-Lösung bietet sich Graylog an (kostenloser Download unter www.graylog.org/, ebenfalls die Enterprise Lösung bis 5 GB pro Tag).

Technische Schwachstellen

Schwachstellen können jederzeit auftreten. Oft im ungünstigsten Zeitpunkt (Murphy lässt grüssen). Daher ist es wichtig, bereits im Vorfeld entsprechende Schritte zu planen und Verantwortlichkeiten zu definieren. Tritt ein Vorfall ein, gilt es diesen als erstes zu bewerten: Mit welchen Folgen ist zu rechnen? Welche Risiken sind damit verbunden? Welche weiteren Systeme, Prozesse und Personen sind davon betroffen? Gibt es Ausweichmöglichkeiten? Welche Ressourcen werden zur Behebung benötigt? Kann der Vorfall allein bewältigt werden oder ist externe Unterstützung notwendig?

Sind alle Fragen beantwortet, kann ein Zeitplan zur Behebung erstellt werden. Allenfalls muss bereits eine Notfallmassnahme umgesetzt werden. Dies muss mit der entsprechenden Vorsicht geschehen. Anschliessend wird die Schwachstelle gemäss Plan behandelt. Die Informationssicherheit darf dabei unter keinen Umständen vernachlässigt werden. Wenn immer möglich sollten Massnahmen im Vier-Augen-Prinzip umgesetzt werden. Wichtig bei allen Schritten ist eine saubere Dokumentation über die getätigten Schritte, damit die Nachvollziehbarkeit erhalten bleibt. Damit dies alles in einem Notfall auch funktioniert, sollte es mindestens einmal pro Jahr geübt werden.

Audits

Der letzte Punkt in diesem Kapitel (A.12.7) behandelt die Sicherheit von Audits. Jedes Unternehmen sollte ihre Informationssicherheit regelmässig durch eine unabhängige Firma überprüfen lassen (das heisst nicht durch den bestehenden IT-Partner). Dies ist aber immer mit einem gewissen Risiko verbunden. Auch wenn der Dienstleister vorsichtig vorgeht, bin ich selbst für eine aktuelle Datensicherung verantwortlich. Wird ein Audit beauftragt, sollten im Minimum folgende Punkte berücksichtigt werden: Umfang und Ablauf, Zeitpunkt, involvierte Personen (eigene und die des Dienstleisters), eingesetzte Tools, Dokumentation/Information, die notwendig ist, Grenzen des Audits, Umgang mit den Resultaten (Scan-Resultate, Screenshots, Log-Daten, Bericht, Präsentation, usw.), Vertraulichkeit sowie Haftung. Werden diese Punkte sauber berücksichtigt, steht einem gewinnbringenden Audit nichts im Wege.

Fazit

Das Kapitel A.12 der ISO 27001 zeigt, wie die technische Umgebung dokumentiert, unterhalten, vor Viren geschützt, gesichert, überwacht sowie auditiert wird. Zudem bereitet es das Unternehmen auf technische Schwachstellen vor. Durch externe Audits wird die Sicherheit von externen Spezialisten auf Herz und Nieren überprüft. Sind alle Punkte sauber umgesetzt, kann aus technischer Sicht ein optimales Umfeld für die Business-Prozesse gewährleistet werden.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

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