



Umsetzung von CobiT-Zielen mit einer Public Key Infrastructure

INHALT

Umsetzung von CobIT-Zielen durch Einsatz einer Public Key Infrastructure	4
1. Planung und Organisation / PO	5
PO 3 Bestimmung der technologischen Richtung.....	5
PO 3.2 Überwachung zukünftiger Trends und Vorschriften.....	5
2. Beschaffung und Einführung / BE	5
BE 1.8 Risikoanalyse-Bericht.....	5
3. Auslieferung und Support / AS.....	5
AS 5 Systemsicherheit.....	5
AS 5.2 Identifikation, Authentisierung und Zugriff	5
AS 5.3 Sicherheit des Direktzugriffs auf Daten.....	6
AS 5.4 Verwaltung der Benutzerkonten.....	6
AS 5.5 und 5.6 Überprüfung der Benutzerkonten.....	6
AS 5.7 Sicherheitsüberwachung	6
AS 5.8 Datenklassifikation	6
AS 5.9 Zentrale Verwaltung von Identifikation und Zugriffsrechten.....	6
AS 5.10 Rapportierung von Verstößen und Sicherheitsaktivitäten	7
AS 5.11 Umgang mit Zwischenfällen	7
AS 5.13 Vertrauenswürdigkeit der Gegenpartei.....	7
AS 5.14 Genehmigung von Transaktionen	7
AS 5.15 Nicht-Abstreitbarkeit	7
AS 5.16 Vertrauenswürdiger Pfad	7
AS 5.18 Verwaltung kryptographischer Schlüssel	7
AS 5.19 Prävention, Aufdeckung und Korrektur bei bössartiger Software.....	8
AS 5.21 Schutz von elektronischen Werten.....	8
AS 11 Verwaltung von Daten	8
AS 11.17 und AU 11.27 Schutz von sensiblen Nachrichten bzw. Informationen während Übermittlung und Transport	8
AU 11.28 Authentisierung und Integrität	8
AU 11.30 Andauernde Integrität von gespeicherten Daten.....	8
Appendix: ausgewählte Cobit Kontrollziele.....	9
P03 Bestimmung der technologischen Richtung.....	9
PO 3.2 Überwachung zukünftiger Trends und Vorschriften.....	9
P08 Sicherstellung der Einhaltung von externen Anforderungen	10
PO 8.4 Datenschutz, Urheberrecht und Datenfluss.....	10
PO 8.5 Elektronischer Handel.....	10
P09 Risikobeurteilung	11
BE 1.8 Risikoanalyse-Bericht.....	11
AS 5 Systemsicherheit.....	12
AS 5.1 Handhabung von Sicherheitsmassnahmen	12
AS 5.2 Identifikation, Authentisierung und Zugriff	12
AS 5.3 Sicherheit des Direktzugriffs auf Daten.....	12
AS 5.4 Verwaltung der Benutzerkonten.....	13
AS 5.5 Überprüfung der Benutzerkonten durch das Management	13
AS 5.6 Überprüfung der Benutzerkonten durch die Benutzer	13
AS 5.7 Sicherheitsüberwachung	13
AS 5.8 Datenklassifikation	13
AS 5.9 Zentrale Verwaltung von Identifikation und Zugriffsrechten.....	13
AS 5.10 Rapportierung von Verstößen und Sicherheitsaktivitäten	14

AS 5.11	Umgang mit Zwischenfällen	14
AS 5.12	Re-Akkreditierung	14
AS 5.13	Vertrauenswürdigkeit der Gegenpartei	14
AS 5.14	Genehmigung von Transaktionen	14
AS 5.15	Nicht-Abstreitbarkeit	14
AS 5.16	Vertrauenswürdiger Pfad	14
AS 5.17	Schutz von Sicherheitsfunktionen	15
AS 5.18	Verwaltung kryptographischer Schlüssel	15
AS 5.19	Prävention, Aufdeckung und Korrektur bei bössartiger Software	15
AS 5.20	Firewall-Architekturen und Verbindungen mit öffentlichen Netzwerken	15
AS 5.21	Schutz von elektronischen Werten	15
AS 11	Verwaltung von Daten	16
AS 11.17	Schutz von sensitiven Informationen während Übermittlung und Transport	16
AS 11.27	Schutz von sensitiven Nachrichten	16
AS 11.28	Authentisierung und Integrität	16
AS 11.30	Andauernde Integrität von gespeicherten Daten	16

UMSETZUNG VON COBIT-ZIELEN DURCH EINSATZ EINER PUBLIC KEY INFRASTRUCTURE

Beim Einsatz einer PKI kann CobiT für die Sicherstellung des wirtschaftlichen, strategischen und sicheren Einsatzes angewendet werden.

Der Einsatz einer PKI unterstützt aber entscheidend bei der Umsetzung bestimmter CobiT-Kontrollziele für die Informationstechnologie einer Organisation. Schwerpunktmäßig betrifft das natürlich die Sicherheitskontrollziele, aber auch andere Kontrollziele, v.a. die Verwaltung von Daten und Informationen, werden dabei tangiert.

1. PLANUNG UND ORGANISATION / PO

PO 3 *Bestimmung der technologischen Richtung*

Ein Technologie-Infrastrukturplan sollte sich mittlerweile auch mit dem Thema PKI auseinandersetzen, da die technische Reife von PKI immer weiter fortschreitet und hohes Potential an Anwendungsmöglichkeiten besitzt und Sicherheitsanforderungen abdeckt.

PO 3.2 **Überwachung zukünftiger Trends und Vorschriften**

Vor allem von staatlicher Seite wird (in Österreich: Bürgerkarte – E-Government-Gesetz, Verordnung für elektronische Rechnungen,...) wird auf digitale Signaturen gesetzt. Gute PKI Unterstützung ist mittlerweile auch in Standardsoftware vorhanden.

2. BESCHAFFUNG UND EINFÜHRUNG / BE

BE 1.8 **Risikoanalyse-Bericht**

Für jedes neue System sollte eine Risikobeurteilung gemacht werden. Durch die Integration von PKI lässt sich diese Beurteilung erheblich schneller, günstiger und problemloser gestalten, da die bestehende Bewertung dieses zentralen Sicherheitsservices dafür herangezogen werden kann.

3. AUSLIEFERUNG UND SUPPORT / AS

AS 5 *Systemsicherheit*

Durch eine PKI können zentrale Themen der Systemsicherheit umgesetzt oder zumindest effektiv unterstützt werden.

AS 5.2 **Identifikation, Authentisierung und Zugriff**

PKI ist die Infrastruktur, durch die Anwendungen, welche die PKI nutzen, einfach die Identifikation und Authentisierung umsetzen, auf welche Autorisierung aufsetzen kann. Eine aufbauende PMI könnte sogar die Autorisierung übernehmen. Die Notwendigkeit mehrfacher Anmeldungen kann minimiert werden und man braucht keine weiteren Verfahren, damit die Mechanismen wirksam bleiben. Dieses Kontrollziel kann also vollständig umgesetzt werden.

AS 5.3 Sicherheit des Direktzugriffs auf Daten

Einzelne Autorisierung baut auf Authentizität, welche die PKI sicherstellt, eine aufbauende PMI würde beispielsweise ein Autorisierungsframework darstellen. PKI ist die Basis für die technische Umsetzung dieses organisatorischen Kontrollziels.

AS 5.4 Verwaltung der Benutzerkonten

Eine PKI erleichtert die Verwaltung von Benutzerkonten und stellt Authentisierung sicher, sie ist die Basis der Vertraulichkeit. Die Rechtzeitigkeit der Suspendierung oder Schließung ist nicht mehr so kritisch, da z.B. bei einer PKI ein Austritt durch die Abgabe der Karte oder Widerruf des Zertifikats alle Konten praktisch schließt und die Löschung nur mehr eine administrative Formsache ist. Auch Drittzugriffe können brauchbar verwaltet und gemäß den Verträgen gesteuert werden.

AS 5.5 und 5.6 Überprüfung der Benutzerkonten

Die Überprüfung der Benutzerkonten wird vereinfacht, denn Benutzerkonten können übergreifend durch Widerruf des Zertifikats gesperrt werden, und Risiken durch unberechtigte Benutzung, etc, können durch eine 2-Faktor-Authentifizierung stark reduziert werden. Die Sicherheitsüberwachung durch den Benutzer wird ebenso erleichtert, da er bei einer 2-Faktor-Authentifizierung sofort erkennen kann, wenn seine Karte abhanden kommt.

AS 5.7 Sicherheitsüberwachung

Sicherheitsaktivitäten und drohende Sicherheitsverletzungen lassen sich leichter erkennen, die versuchte Verwendung eines gesperrten/widerrufenen Zertifikates ist wohl ein eindeutiges Zeichen dafür.

AS 5.8 Datenklassifikation

In Public-Key-Zertifikaten, besser aber Attributzertifikaten, kann ein Attribut aufgenommen, für welche Klassifikation bzw. Datenklasse ein Zertifikatsbesitzer autorisiert ist.

AS 5.9 Zentrale Verwaltung von Identifikation und Zugriffsrechten

Die PKI als zentrales Authentifizierungsschema ist DAS Werkzeug für eine zentrale Verwaltung der Identifikation.

AS 5.10 Rapportierung von Verstößen und Sicherheitsaktivitäten

Für den Einsatz von Zertifikaten ist es unabdingbar, einen Meldeweg und Workflow für den Widerruf zu schaffen. Für diesen Einsatzzweck kann die bestehende Art und Weise der Meldung eines Sicherheitsvorfalles genutzt werden. Wenn (noch) kein effektiver Weg existiert bietet es sich an, einen Workflow dafür zu generieren und zu kommunizieren, und diesen Meldeweg auch für allgemeine Sicherheitsvorfälle zu nutzen. Die versuchte Verwendung von gesperrten Zertifikaten kann sofort erkannt werden und sogar zeitnah Aktivitäten nach sich ziehen.

AS 5.11 Umgang mit Zwischenfällen

Wie für CobIT-Kontrollziel 5.10, gilt für dieses Ziel, dass ein „Widerrufsweg“ eingerichtet werden muss, der auch gleich für andere Vorfalldmeldungen genutzt werden könnte. Die Reaktion auf einen Vorfall kann mit einer PKI sogar äußerst zeitnah erfolgen.

AS 5.13 Vertrauenswürdigkeit der Gegenpartei

Die Vertrauenswürdigkeit von Partnern, Lieferanten, Kunden,... kann für alle elektronischen Kommunikationswege durch Zertifikate sichergestellt werden. Neben der Ausstellung von Zertifikaten ist auch eine Cross-Zertifizierung eine Möglichkeit.

AS 5.14 Genehmigung von Transaktionen

Die Erfüllung dieses Kontrollziels setzt die Verwendung einer PKI beinahe voraus. Die geforderten kryptographischen Techniken für das Unterzeichnen und Verifizieren einer Transaktion sind mit einer PKI am effizientesten umgesetzt.

AS 5.15 Nicht-Abstreitbarkeit

Nicht-Abstreitbarkeit ist eine Grundcharakteristik von PKI Anwendungen, dieses Kontrollziel nennt sogar explizit die Verwendung digitaler Signaturen und Zeitstempel.

AS 5.16 Vertrauenswürdiger Pfad

Sensitive Information müssen über einen vertraulichen Pfad transportiert werden. Effektive Verschlüsselung bedarf der Authentifizierung des Kommunikationspartners. Dies kann mittels PKI geschehen, Protokolle wie SSL verwenden PKI dafür bzw. für Etablierung einer hybriden Verschlüsselung.

AS 5.18 Verwaltung kryptographischer Schlüssel

Dieses Kontrollziel zielt auf die saubere Implementierung von kryptographischen Anwendungen ab. Das Schlüsselmanagement lässt sich mit Systemen, die auf asymmetrischen Verfahren basieren, wie eine PKI, leichter gestalten.

AS 5.19 Prävention, Aufdeckung und Korrektur bei bösartiger Software

Die Herkunft von Software kann mit digitalen Signaturen sichergestellt werden. Für die Problematik mit dem Scannen nach Maligner Software und gleichzeitiger Mailverschlüsselung gibt es für Unternehmen mittlerweile Lösungen am Markt.

AS 5.21 Schutz von elektronischen Werten

Die Integrität von sensitiven Informationen sollte kontinuierlich sichergestellt werden – für kryptographische Schlüssel besitzt eine Smart Card oder HSM ideale Eignung dafür.

AS 11 *Verwaltung von Daten*

Die Verwaltung von Daten wird durch eine PKI hinsichtlich Ihrer Sicherheit unterstützt.

AS 11.17 und 11.27 Schutz von sensitiven Nachrichten bzw. Informationen während Übermittlung und Transport

PKI stellt oft die Basis für die Transportsicherung (Vertraulichkeit, Integrität) und die Authentizität von Nachrichten dar, da Protokolle wie S/MIME oder SSL auf PKI-Funktionalitäten aufbauen.

AU 11.28 Authentisierung und Integrität

Elektronisch vorliegende Informationen können mit Signaturen hinsichtlich ihrer Authentizität und auf ihre Integrität geprüft werden.

AU 11.30 Andauernde Integrität von gespeicherten Daten

Die Integrität von Daten kann mit HMACs oder Signaturen sichergestellt und geprüft werden. Die Integrität von elektronischen Archiven bedarf aber einiger weiterer Sicherheitsmaßnahmen.

APPENDIX: AUSGEWÄHLTE COBIT KONTROLLZIELE

PO 3 *Bestimmung der technologischen Richtung*

Kontrolle über den IT-Prozess

Bestimmung der technologischen Richtung zur Erfüllung der Geschäftsanforderungen.

Nutzen ziehen aus verfügbaren und auftauchenden Technologien um die Geschäftsstrategie zu betreiben und zu ermöglichen

wird ermöglicht durch

Schaffung und Unterhalt eines Technologie-Infrastrukturplanes, der klare und realistische Erwartungen aufzeigt und unterhält in Hinblick auf was die Technologie in Bezug auf Produkte, Dienstleistungen und Betriebsmechanismen ermöglichen kann

unter Berücksichtigung von

- Potential der gegenwärtigen Infrastruktur
- Überwachung von technologischen Entwicklungen via verlässliche Quellen
- Durchführung von Konzeptstudien
- Risiken, Einschränkungen und Gelegenheiten
- Beschaffungspläne
- Migrationsstrategien und Teilpläne
- Beziehung zu Anbietern
- unabhängige Technologie-Neubeurteilung
- Hardware- und Software-Preis- und Leistungsänderung

PO 3.2 **Überwachung zukünftiger Trends und Vorschriften**

Eine laufende Überwachung von zukünftigen Trends und gesetzlichen Voraussetzungen sollte durch die Informatikabteilung sichergestellt werden, damit diese Faktoren während Entwicklung und Unterhalt des technologischen Infrastrukturplanes berücksichtigt werden können.

PO 8 Sicherstellung der Einhaltung von externen Anforderungen

Kontrolle über den IT-Prozess

Sicherstellung der Einhaltung von externen Anforderungen zur Erfüllung der Geschäftsanforderungen

Einhaltung der gesetzlichen, regulativen und vertraglichen Verpflichtungen

wird ermöglicht durch

Identifikation und Analyse externer Anforderungen hinsichtlich ihrer Auswirkungen auf die IT und Ergreifen von geeigneten Massnahmen zu deren Einhaltung

unter Berücksichtigung von

- Gesetze, Verordnungen und Verträge
- Beobachtung der Entwicklungen von Gesetzen und Verordnungen
- regelmässige Überprüfung auf Einhaltung
- Sicherheit und Ergonomie
- Datenschutz
- Urheberrechte

PO 8.4 Datenschutz, Urheberrecht und Datenfluss

Das Management sollte die Einhaltung von Vorschriften bezüglich Datenschutz, Urheberrecht, grenzüberschreitendem Datenverkehr und Verschlüsselung sicherstellen, welche auf die IT-Praktiken des Unternehmens anwendbar sind.

PO 8.5 Elektronischer Handel

Das Management sollte sicherstellen, dass zwischen Handelspartnern formelle Verträge über Kommunikationsprozesse und Standards für die Sicherheit der Transaktionsnachrichten und der Datenspeicherung vorhanden sind.

Wird über das Internet gehandelt, sollte das Management angemessene Kontrollen durchsetzen, um weltweit die Einhaltung von lokalen Gesetzen und Sitten sicherzustellen.

PO 9 Risikobeurteilung

Kontrolle über den IT-Prozess

Risikobeurteilung zur Erfüllung der Geschäftsanforderungen

Unterstützung von Management-Entscheidungen durch Erreichen von IT-Zielen und Reagieren auf Bedrohungen durch die Reduktion der Komplexität, Erhöhung der Objektivität und Identifikation von wichtigen

Entscheidungskriterien

wird ermöglicht durch

ein Engagement des Unternehmens selbst in der Identifikation von IT-Risiken und der Analyse von Auswirkungen, unter Einbezug von interdisziplinären Funktionen und Ergreifen von kostenwirksamen Massnahmen zur Verminderung der Risiken.

unter Berücksichtigung von

- Eigentümerprinzip für Risikomanagement und Verantwortlichkeiten
- verschiedene Arten von IT-Risiken (Technologie, Sicherheit, Kontinuität, Regulative, usw.)
- definierte und kommunizierte Risikotoleranz-Profile
- Ursachenanalyse und Risiko-Brainstorming-Sitzungen
- quantitative und/oder qualitative Risikobemessung
- Methodik der Risikobewertung
- Risiko-Aktionsplan
- rechtzeitige Risiko-Neubewertung

BE 1.8 Risikoanalyse-Bericht

Die Systementwicklungsmethode des Unternehmens sollte bei jedem Entwicklungs-, Einführungs- oder Änderungsprojekt eines Informationssystems für eine Analyse und Dokumentation der Sicherheitsbedrohungen, potentiellen Verletzlichkeiten und Auswirkungen, und der machbaren Schutzmassnahmen für Sicherheit und interne Kontrolle sorgen, um das identifizierte Risiko zu reduzieren oder zu eliminieren. Dies sollte im Einklang mit der allgemeinen Risikobeurteilungsmethode realisiert werden.

AS 5 Systemsicherheit

Kontrolle über den IT-Prozess: Das Sicherstellen der Systemsicherheit zur Erfüllung der Geschäftsanforderungen Schutz von Informationen vor unberechtigter Verwendung, Aufdeckung oder Änderung, Beschädigung oder Verlust wird ermöglicht durch logische Zugriffskontrollen, die sicherstellen, dass ein Zugriff auf Systeme, Daten und Programme auf berechnigte Personen beschränkt ist unter Berücksichtigung von

- Vertraulichkeits- und Datenschutzanforderungen
- Berechnigung, Authentisierung und Zugriffsschutz
- Benutzeridentifikation und Berechnigungsprofile
- Need-to-have und Need-to-know
- Verwaltung kryptographischer Schlüssel
- Problemeldewesen, Berichterstattung und Folgeaktivitäten
- Verhütung und Entdeckung von Viren
- Firewalls
- zentralisierte Sicherheitsadministration
- Benutzerausbildung
- Werkzeuge für die Überwachung der Einhaltung rechtlicher Erfordernisse, Ein-bruchsversuche und Berichterstattung

AS 5.1 Handhabung von Sicherheitsmassnahmen

IT-Sicherheit sollte so gehandhabt werden, dass die Sicherheitsmassnahmen mit den Geschäftsanforderungen in Einklang stehen. Dies umfasst:

- Umsetzung der Risikobeurteilungsinformation in IT-Sicherheitspläne
- Umsetzung des IT-Sicherheitsplans
- Aktualisierung des IT-Sicherheitsplans, um Änderungen in der IT-Konfiguration widerzuspiegeln
- Bewertung der Auswirkung von Änderungsanträgen auf die IT-Sicherheit
- Überwachung der Umsetzung des IT-Sicherheitsplans
- Ausrichtung der IT-Sicherheitsverfahren an anderen Konzepten und Verfahren

AS 5.2 Identifikation, Authentisierung und Zugriff

Der logische Zugriff auf und die Verwendung von IT-Rechnerressourcen sollte durch die Einführung von angemessenen Identifikations-, Authentisierungs- und Autorisierungsmechanismen beschränkt werden, welche Benutzer und Ressourcen mit Zugriffsregeln verknüpft. Solche Mechanismen sollten unberechnigtes Personal, Wählverbindungen und andere System-(Netzwerk-) Eintrittspunkte am Zugriff auf Rechnerressourcen hindern und die Notwendigkeit einer mehrfachen Anmeldung für berechnigte Benutzer minimieren. Es sollten auch Verfahren vorhanden sein, damit die Authentisierungs- und Zugriffsmechanismen wirksam bleiben (z.B. regelmässige Passwortänderungen).

AS 5.3 Sicherheit des Direktzugriffs auf Daten

In einer Online-IT-Umgebung sollte das IT-Management in Einklang mit dem Sicherheitskonzept Verfahren zur Bereitstellung einer Zugriffskontrolle implementieren, welche auf der erwiesenen Notwendigkeit der einzelnen Person basiert, Daten einzusehen, hinzuzufügen, zu ändern oder zu löschen.

AS 5.4 Verwaltung der Benutzerkonten

Das Management sollte Verfahren einrichten, um ein rechtzeitiges Handeln bezüglich Anforderung, Einrichtung, Herausgabe, Suspendierung und Schliessung von Benutzerkonten sicherzustellen. Ein formelles Genehmigungsverfahren sollte darin enthalten sein, das die Daten- oder Systemeigner bezeichnet, welche die Zugriffsrechte gewähren. Die Sicherheit von Dritt-Zugriffen sollte vertraglich definiert und die Anforderungen an Administration und Vertraulichkeit festgehalten werden. Outsourcing-Vereinbarungen sollten die Risiken, Sicherheitsmassnahmen und -verfahren für Informationssysteme und Netzwerke im Vertrag zwischen den Parteien regeln.

AS 5.5 Überprüfung der Benutzerkonten durch das Management

Das Management sollte einen Kontrollprozess implementiert haben, um Zugriffsrechte periodisch zu überprüfen und zu bestätigen. Periodisch sollten Vergleiche zwischen den Ressourcen und den Aufzeichnungen gemacht werden, um das Risiko für Fehler, Betrug, Missbrauch oder unberechtigter Veränderung zu reduzieren.

AS 5.6 Überprüfung der Benutzerkonten durch die Benutzer

Benutzer sollten systematisch die Aktivität ihrer eigenen Benutzerkonten kontrollieren. Auch sollten Informationsmechanismen vorhanden sein, die ihnen ermöglichen, sowohl die normale Aktivität zu überwachen als auch bei ungewöhnlichen Aktivitäten rechtzeitig alarmiert zu werden.

AS 5.7 Sicherheitsüberwachung

Die IT-Sicherheitsadministration sollte sicherstellen, dass Sicherheitsaktivitäten protokolliert werden und jedes Anzeichen einer drohenden Sicherheitsverletzung sofort allen internen und externen Betroffenen gemeldet und dass automatisch darauf reagiert wird.

AS 5.8 Datenklassifikation

Das Management sollte Verfahren einführen, um sicherzustellen, dass alle Daten hinsichtlich ihrer Sensitivität durch eine formelle und explizite Entscheidung des Dateneigners entsprechend dem Datenklassifikationsschema klassifiziert werden. Sogar Daten, die "keinen Schutz" benötigen, sollten erst durch eine formelle Entscheidung als solche bezeichnet werden. Eigner sollten sowohl die Zuordnung und das Teilen von Daten bestimmen als auch, ob und wann Programme und Dateien gewartet, archiviert und gelöscht werden. Nachweise für die Zustimmung des Eigners und die Zuordnung der Daten sollten aufbewahrt werden. Richtlinien sollten aufgestellt werden für die Neu-Klassifikation von Daten, welche auf geänderter Sensitivität basiert. Das Klassifikationsschema sollte Kriterien für den Informationsaustausch zwischen Unternehmen beinhalten, welche sowohl die Sicherheit als auch die Einhaltung relevanter Gesetze anspricht.

AS 5.9 Zentrale Verwaltung von Identifikation und Zugriffsrechten

Kontrollen sind vorhanden, um sicherzustellen, dass die Identifikation und Zugriffsrechte von Benutzern, ebenso wie die Identität von System- und Dateneignern eindeutig und zentral eingerichtet und verwaltet werden, um Konsistenz und Wirtschaftlichkeit des globalen Zugriffsschutzes zu erlangen.

AS 5.10 Rapportierung von Verstößen und Sicherheitsaktivitäten

Die IT-Sicherheitsadministration sollte gewährleisten, dass regelmässig Verstöße und Sicherheitsaktivitäten protokolliert, gemeldet, überprüft und geeignet eskaliert werden, um Vorfälle mit unberechtigten Aktivitäten zu identifizieren und abzuklären. Der logische Zugriff auf Nachvollziehbarkeitsinformationen der Rechnerressourcen (Sicherheits- und andere Protokolle) sollte basierend auf dem Prinzip des "least privilege" oder "need-to-know" gewährt werden.

AS 5.11 Umgang mit Zwischenfällen

Das Management sollte die Fähigkeit zum Umgang mit Ereignissen betreffend die Computersicherheit aufstellen, um Sicherheitsvorfälle durch Bereitstellung einer zentralisierten Plattform (mit genügend Sachverstand und ausgestattet mit schnellen und sicheren Kommunikationseinrichtungen) anzugehen. Verantwortlichkeiten und Verfahren für das Ereignis-Meldewesen sollten eingerichtet sein, um eine geeignete, wirksame und rechtzeitige Antwort auf Sicherheitsvorfälle zu gewährleisten.

AS 5.12 Re-Akkreditierung

Das Management sollte sicherstellen, dass periodisch eine Re-Akkreditierung der Sicherheit (z.B. durch "Tiger Teams") durchgeführt wird, um das formell genehmigte Sicherheitsniveau und die Akzeptanz des Restrisikos auf dem aktuellen Stand zu halten.

AS 5.13 Vertrauenswürdigkeit der Gegenpartei

Unternehmensrichtlinien sollten sicherstellen, dass Kontrollpraktiken zur Verifizierung die Authentizität der Gegenpartei, welche elektronische Anweisungen oder Transaktionen durchführt, eingeführt sind. Dies kann durch vertrauenswürdigen Austausch von Passwörtern, Tokens oder kryptographischen Schlüsseln eingerichtet werden.

AS 5.14 Genehmigung von Transaktionen

Unternehmensrichtlinien sollten sicherstellen, dass, wo geeignet, Kontrollen zur Gewährleistung der Authentizität von Transaktionen und zur Sicherstellung der Gültigkeit der von einem Benutzer gegenüber dem System angegebenen Identität eingerichtet werden. Dies bedingt die Verwendung von kryptographischen Techniken für das Unterzeichnen und Verifizieren der Transaktionen.

AS 5.15 Nicht-Abstreitbarkeit

Unternehmensrichtlinien sollten sicherstellen, dass, wo notwendig, Transaktionen von keiner Partei geleugnet werden können und dass Kontrollen eingeführt sind, um die Nicht-Abstreitbarkeit von Herkunft oder Empfang sowie Beweis der Aufgabe und Empfang der Transaktionen zu liefern. Dies kann durch digitale Signaturen, Zeitstempel und vertrauenswürdige Drittparteien erfolgen – mit entsprechenden Richtlinien, welche die relevanten regulatorischen Bestimmungen berücksichtigen.

AS 5.16 Vertrauenswürdiger Pfad

Unternehmensrichtlinien sollten sicherstellen, dass sensitive Transaktionsdaten nur über einen vertrauenswürdigen Pfad ausgetauscht werden. Sensitive Informationen umfassen Informationen des Sicherheitsmanagements, sensitive Transaktionsdaten, Passwörter und kryptographische Schlüssel. Um dies zu erreichen, müssen möglicherweise vertrauenswürdige Kanäle unter Verwendung von Verschlüsselung zwischen den Benutzern, zwischen Benutzern und Systemen, und zwischen den Systemen eingerichtet werden.

AS 5.17 Schutz von Sicherheitsfunktionen

Die gesamte für Sicherheit eingesetzte Hard- und Software sollte jederzeit gegen Manipulationen geschützt sein, um ihre Integrität zu erhalten und die Aufdeckung geheimer Schlüssel zu verhindern. Zusätzlich sollten Unternehmungen ihr Sicherheitsdesign "nicht an die grosse Glocke hängen", aber ihre Sicherheit nicht darauf aufbauen, dass das Design geheim ist.

AS 5.18 Verwaltung kryptographischer Schlüssel

Das Management sollte für Erstellung, Änderung, Widerrufung, Zerstörung, Verteilung, Zertifizierung, Speicherung, Eingabe, Verwendung und Archivierung von kryptographischen Schlüsseln zu verwendende Verfahren und Protokolle definieren und implementieren, um den Schutz der Schlüssel gegen Veränderung und unberechtigte Aufdeckung sicherzustellen. Falls ein Schlüssel kompromittiert wird, sollte das Management sicherstellen, dass diese Information durch die Verwendung von Widerruflisten für Zertifikate oder ähnlicher Mechanismen jeder betroffenen Partei weitergegeben wird.

AS 5.19 Prävention, Aufdeckung und Korrektur bei bösartiger Software

Bezüglich bösartiger Software wie Computerviren oder Trojanischen Pferden sollte das Management einen Rahmen angemessener präventiver, aufdeckender und korrekativer Kontrollmassnahmen sowie Reaktion auf Vorfälle und Berichterstattung einrichten. Das Management der Fachbereiche und der Informatik sollten sicherstellen, dass unternehmensweite Verfahren eingerichtet werden, um die Informationssysteme und Technologie vor Computerviren zu schützen. Die Verfahren sollten Virenschutz, Virenerkennung, Reaktion auf Vorfälle und Berichterstattung einschliessen.

AS 5.20 Firewall-Architekturen und Verbindungen mit öffentlichen Netzwerken

Wenn Verbindungen zum Internet oder anderen öffentlichen Netzwerken existieren, sollten geeignete Firewalls in Betrieb sein, um vor "Denial-of-Service" und allen unberechtigten Zugriffen auf interne Ressourcen zu schützen; sie sollten jeden Fluss der Handhabung von Anwendungen und Infrastruktur in beiden Richtungen kontrollieren und vor "Denial-of-Service-Attacks" schützen.

AS 5.21 Schutz von elektronischen Werten

Das Management sollte die andauernde Integrität aller Karten oder ähnlicher physischer Geräte schützen, die zur Authentisierung oder Speicherung von Finanz- oder anderen sensitiven Informationen verwendet werden – unter Beachtung der damit verbundenen Einrichtungen, Geräte, Angestellten und verwendeten Validierungsmethoden.

AS 11 Verwaltung von Daten

Kontrolle über den IT-Prozess

Verwaltung von Daten zur Erfüllung der Geschäftsanforderungen

Sicherstellen, dass die Daten während Eingabe, Aktualisierung und Speicherung vollständig, genau und gültig bleiben

wird ermöglicht durch

eine wirksame Kombination von Anwendungs- und generellen Kontrollen über den IT-Betrieb

unter Berücksichtigung von

- Formularentwurf
- Kontrollen der Quelldokumente
- Eingabe-, Verarbeitungs- und Ausgabekontrollen
- Datenträger-Identifikation, Transport- und Bibliothekswesen
- Datensicherung und Wiederherstellung
- Authentizität und Integrität
- Daten-Eigentümerprinzip
- Datenverwaltungskonzepte
 - Datenmodelle und Daten-Repräsentationsstandards
 - Integration und Konsistenz über Plattformen hinweg
 - rechtliche und vertragliche Anforderungen

AS 11.17 Schutz von sensiblen Informationen während Übermittlung und Transport

Das Management sollte sicherstellen, dass für sensitive Informationen während Übermittlung und Transport ein angemessener Schutz gegen unberechtigten Zugriff, Änderung und Falschadressierung besteht.

AS 11.27 Schutz von sensiblen Nachrichten

Für die Datenübertragung über das Internet oder irgend ein anderes öffentliches Netzwerk sollte das Management zu verwendende Verfahren und Protokolle definieren und implementieren, um Integrität, Vertraulichkeit und Nicht-Abstreitbarkeit von sensiblen Nachrichten sicherzustellen.

AS 11.28 Authentisierung und Integrität

Die Authentisierung und Integrität von Informationen, deren Ursprung ausserhalb des Unternehmens liegt, sei es durch Empfang über Telefon, Voice-Mail, Papier, Fax oder E-mail, sollten geeignet geprüft werden, bevor möglicherweise kritische Aktionen erfolgen.

AS 11.30 Andauernde Integrität von gespeicherten Daten

Das Management sollte sicherstellen, dass die Integrität und Richtigkeit von Daten in Dateien oder auf anderen Datenträgern (z.B. elektronischen Karten) periodisch geprüft wird. Besondere Aufmerksamkeit sollten Wertkarten, Referenzdateien und Dateien mit datenschutzrelevanten Informationen erhalten.

CRYPTAS it-Security & Media GmbH
Modcenterstrasse 22/B2
A-1030 Wien, Austria
T +43 (1) 798 96 96 – 0
F +43 (1) 798 96 96 – 99
info@cryptas.com

www.cryptoshop.com
www.cryptas.com
www.croptomedia.com