
COMPUTERWOCHE
VON IDG

IT-Security Reloaded

NIS-Richtlinie und neue Tools für den Mittelstand

von Dr. Michael Rath, Alexander Haasper

Foto: Mikko Lemola - shutterstock.com

Inhalt

IT-Security Reloaded

NIS-Richtlinie und neue Tools für den Mittelstand

von Dr. Michael Rath, Alexander Haasper

Das EU-Parlament hat einer Richtlinie zur erhöhten Cybersicherheit zugestimmt. Diese muss nun in den nächsten beiden Jahren in nationales Recht umgesetzt werden.

Am 6. Juli 2016 hat das EU-Parlament mit großer Mehrheit dem Kompromissvorschlag für eine Richtlinie zur erhöhten Cybersicherheit [1] (sog. NIS-Richtlinie) zugestimmt. Diese EU-Richtlinie erweitert die Verantwortlichkeit von Betreibern kritischer Infrastrukturen. Auch große Online-Dienstleister wie etwa die Betreiber von Verkehrsknoten, Domain-Registrierungsstellen oder Online-Marktplätzen wie eBay oder Amazon sollen nun von den Security- und Meldepflichten erfasst werden. Suchmaschinen wie Google und Cloud-Anbieter sind von der Richtlinie ebenfalls betroffen. Die EU-Richtlinie muss in den nächsten zwei Jahren allerdings zuerst in nationales Recht umgesetzt werden.

IT-Sicherheit als Management-Aufgabe

In Deutschland sind die Betreiber kritischer Infrastrukturen bereits durch das seit etwa einem Jahr geltende IT-Sicherheitsgesetz [2] dazu verpflichtet, bestimmte Sicherheitsstandards und Meldepflichten einzuhalten. Dieses Gesetz wird aufgrund der NIS-Richtlinie ebenfalls geändert werden müssen.

Aber auch Unternehmen, die nicht unmittelbar zum Adressatenkreis des vorgenannten Gesetzes gehören, richten das Management ihrer Informationssicherheit inzwischen oft an dem ISO 27001-Standard [3] aus. Dies ist auch sinnvoll, denn auch für den Bereich IT-Security kann man sich ein Beispiel an den regulierten Industrien nehmen, in denen oftmals die Einführung und Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 bereits Pflicht ist. So hat etwa auch die Bundesnetzagentur (BNetzA) für die Strom- und Gasnetzbetreiber einen IT-Sicherheitskatalog verabschiedet, welche die Zertifizierung nach ISO 27001 bis 2018 anordnet. Auch die BaFin verweist in ihren MaRisk [4] auf gängige IT-Standards wie ISO 27001 oder die BSI-Grundschutzkataloge. Die geplante MaRisk-Novelle wird dabei noch stärker auf IT-Sicherheitsaspekte Wert legen.

[Hinweis auf Bildergalerie: 12 Tipps für eine schlanke ISO 27001-Einführung] gal1

1 http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD)
2 http://www.computerwoche.de/a/it-sicherheitsgesetz-eine-bestandsaufnahme,3226757
3 http://www.computerwoche.de/a/wie-ein-security-audit-ablaeuft,3060470
4 http://www.computerwoche.de/a/neue-regelungen-fuer-versicherer-beim-it-outsourcing,3222511

ISMS, ISO 27001 und SANS20

Da die Themen aus dem ISO 27001-Standard über die Linienorganisation häufig kaum noch vollumfänglich bearbeitet werden können, ist es in der Regel hilfreich, ein speziell auf das Unternehmen zugeschnittenes Framework zu entwickeln. Dazu sollten Quellen wie z.B. COBIT, NIST und SANS20 herangezogen werden. SANS20 stellt dabei aufgrund seiner Prioritäten und technischen Implementierungsdetails über die 20 Fokusthemen eine gute Orientierungshilfe dar, insbesondere für kleinere und mittlere Unternehmen - besonders in kaum oder in weniger regulierten Branchen. SANS20 ist dabei nicht als vollständig detaillierte Ausgestaltung eines ISMS [5] zu verstehen, vielmehr wird die Implementierung bis auf die Ebene spezifischer Technologien konkretisiert.

Welche Trends werden über SANS 20 priorisiert?

Die neue Version 6.0, die am 15. Oktober 2015 vom CIS (Center of Internet Security) [6] veröffentlicht worden ist, hat wesentliche Änderungen der Prioritäten der einzelnen 20 Fokusfelder vorgenommen. Hier sind an erster Stelle die deutlichen Heraufstufungen von Security Monitoring [7] und eines kontrollierten Privileged Access Rights Management zu nennen. Zusätzlich wurde ein neues Fokusfeld auf der Ebene der 20 Control Areas eingeführt, das unmittelbar die Data Leakage-Risiken adressiert. Dieses soll die Konfiguration und Verwendung von Email-Systemen und Browsern sicherer machen. Das Fokusfeld "Sichere Entwicklung und Einsatz von Software" ist konsequenterweise in seiner Bedeutung herabgestuft worden, da der Einsatz von Fremdsoftware weiter steigt und sich die Software-Risiken [8] häufig auf Lücken in Verschlüsselungs- und Authentifizierungsprozeduren sowie im Patching-Prozess zurückführen lassen. Diese sind bereits über die jeweiligen SANS20-Fokusfelder im Detail abgedeckt.

Die stetig steigende Anzahl an Cyber-Angriffen [9], die nun über die Presse auch einer breiteren Öffentlichkeit bekannt werden, lassen auch die Rufe nach einem effizienten Incident Management und speziellen Threat-Intelligence [10]-Teams lauter werden. Für diese Disziplinen setzt die Automatisierung gerade erst richtig ein. Eine typische Herausforderung ist beispielsweise, in den Datenmengen die falschen Alarme herauszufiltern. Das Zusammenspiel zwischen Technik und den Teams gilt es weiter zu optimieren. Darüber hinaus ist die Transparenz zum aktuellen Sicherheitsniveau der Organisation ein Dauerthema. Viele Unternehmen entscheiden sich für die Einführung eine Systems von Key Compliance Indicators (KCIs) und die Einführung eines Compliance-Check-Tools.

Das Thema Data Leakage Prevention (DLP) [11] hat inzwischen noch einmal neu an Fahrt aufgenommen. In diesem Zusammenhang gilt es, die Informationen im Unternehmen in Bezug auf ihre Kritikalität zu klassifizieren. Typischerweise geschieht dies in der Startphase manuell, in einer späteren

[5] http://www.computerwoche.de/a/management-systeme-fuer-it-sicherheit-nehmen-fahrt-auf,3096633
[6] https://www.cisecurity.org/
[7] http://www.computerwoche.de/a/woran-sie-merken-dass-sie-gehackt-wurden,2553914
[8] http://www.computerwoche.de/a/die-groessten-risiken-im-blick,2349754
[9] http://www.computerwoche.de/a/die-groessten-cyberangriffe-auf-unternehmen,3214326
[10] http://www.computerwoche.de/a/antivirus-ist-tot-die-security-trends-2016,3220280
[11] http://www.computerwoche.de/a/sag-mir-wo-die-daten-sind,3228632

Phase auch automatisiert. Entsprechend hoch priorisiert sind das Management von Privileged Access Rights, eine effektive Netzwerksegmentierung sowie der Aufbau von Hardware- und Software-Inventories in ihrer Verknüpfung mit dem Patch Management [12].

[Hinweis auf Bildergalerie: Der CISO-Check: Taugen Sie zum IT-Security-Manager?] gal2

Framework für Cybersicherheit

Zur Entwicklung eines spezifischen Ansatzes für ein Unternehmen sollten die aktuellen Frameworks zur Cyber-Security als Pools für die Auswahl von Controls und IT-Security-Lösungen [13] verstanden werden. Aus diesen Quellen sollte sich ein Unternehmen risikoorientiert auf der passenden Implementierungsebene bedienen. Im Idealfall auf Basis eines umfassenden Risk Assessments. Insbesondere SANS20 liefert für die praktische Umsetzung umfangreiche Hilfestellungen. Einige Aspekte wie z.B. technische Details bzgl. der Sicherheit in den Kommunikations-Kanälen "Voice" und "Print" werden allerdings auch nicht über SANS20 konkretisiert. Für das generelle Management von Informationssicherheit gilt es, sich an den ISO- und COBIT-Standards zu orientieren. Den KMUs sei hierzu auch ein "ISMS-light-Ansatz" empfohlen (etwa der "VdS 3473" - VdS-zertifizierte Cyber-Sicherheit), welcher in der Regel eine Vorstufe für eine mögliche ISO/IEC 27001- und BSI IT-Grundschutz-Zertifizierung darstellt.

Die Einsatzgebiete von SANS20 reichen von einer Standortbestimmung im Sinne einer Risikoanalyse, weiter über das Auswählen geeigneter konkreter Lösungen, bis zur laufenden Verfolgung von Aktivitäten und kontinuierlichen Bewertung der identifizierten Risiken. Fehlende Kontrollen eines IT-Security-Management [14]-Systems lassen sich z.B. über ein Experten-Mapping von SANS20-Kontrols zu den ISO2700X-Standards identifizieren und entsprechend zielgerichtet ergänzen. SANS20 ist daher insgesamt ein Schlüssel-Framework, vor allem stark nach den allgemeinen IT-Security-Risiken fokussierendes "Tool", welches den Anwendern eine übergreifende Orientierung für die IT-Security-Solution bietet. (fm)

[Hinweis auf Bildergalerie: Das Einmaleins der IT-Security] gal3

Bildergalerien im Artikel:

gal1 12 Tipps für eine schlanke ISO 27001-Einführung

[12] http://www.computerwoche.de/a/handlungsbedarf-beim-patch-management,3225603

[13] http://www.computerwoche.de/a/moderne-security-loesungen-fuer-kmu,2546148

[14] http://www.computerwoche.de/a/management-systeme-fuer-it-sicherheit-nehmen-fahrt-auf,3096633

Fürsprecher in der Chefetage gewinnen
Ein Managementsystem für die Informationssicherheit kann nur fruchten, wenn es auf allen Ebenen des Unternehmens eine wirksame Unterstützung erfährt. Deshalb sollte frühzeitig ein Schulterschluss mit der Geschäftsleitung herbeigeführt werden, indem sie aktiv in die Planungen zu ISO/IEC 27001 einbezogen wird.

Branchenspezifische Anforderungen
In zunehmendem Maß entwickeln Branchenverbände Vorschriften für die Informationssicherheit, teilweise werden sie auch – wie etwa im Fall der Energieversorger – vom Gesetzgeber vorgegeben. Sie müssen zwingend in die Ausrichtung des ISMS einbezogen werden, sofern sie nicht sowieso bereits Bestandteil der eigenen Compliance sind.

Nicht nur ein Zertifikat besitzen wollen
So wichtig gegenüber Kunden und Geschäftspartnern eine Zertifizierung als Ausweis der Informationssicherheit sein kann, so wenig liegt der eigentliche Wert in einer solchen Etikettierung. Vielmehr muss das ISMS zu einem integralen Element der Unternehmensorganisation werden.

Mit einer GAP-Analyse beginnen
In der Regel bestehen bereits rudimentäre IT-Sicherheitsmaßnahmen. Mit einer GAP-Analyse finden Sie heraus, auf welchen von ihnen sich aufbauen lässt. Dadurch sinkt der Aufwand der Implementierung eines ISO-konformen ISMS erheblich.

Unrealistische Projektierungszeiten vermeiden
Zu anspruchsvolle Ziele können bei einer ehrgzeigen Projektplanung auch kontraproduktiv sein. Umgekehrt wiederum kann sich bei einem zu langsamen Projektablauf das Engagement verlieren. Deshalb sollten Unternehmen die Balance zwischen der ambitionierten Ausrichtung und dem Machbaren versuchen zu wahren.

Schlanke Realisierungsmethoden nutzen
Die Höhe des Einführungs- und Administrationsaufwands trägt wesentlich zur Akzeptanz eines ISO/IEC 27001-basierten ISMS auf den Managementebenen bei. Allein aus diesem Grund sollten ressourcen- und kostenschonende Lean-Methoden eingesetzt werden, ohne dass sie jedoch zu Kompromissen bei den Qualitätszielen zwingen.

Augenmaß bei der Komplexität
Zwar muss den von der ISO-Norm geforderten Elementen einer Sicherheitsrichtlinie für das ISMS entsprochen werden. Aber in der Praxis hat sie mitunter einen Umfang von vielen Dutzend Seiten, der nicht praktikabel ist. Denn je komplexer sie ist, desto geringer ist die Bereitschaft, sich daran zu orientieren.

Keine standardisierte Policy anderer nutzen
Jedes Unternehmen hat ein spezielles organisatorisches Profil und individuelle Sicherheitsbedingungen. Dementsprechend lässt sich eine Security-Richtlinie auch nicht aus einem nach unklaren Kriterien entwickelten Standard ableiten, auch wenn dies auf den ersten Blick eine erhebliche Aufwandsersparnis verspricht.

Ausufernde Dokumentationen vermeiden
Ebenso ist es bei den ISO/IEC 27001-Dokumentationen hilfreich, sich an dem Prinzip „Think big, do small“ zu orientieren. Sie sollten inhaltlich die erforderliche Aussagekraft erlangen, sich dabei aber nicht in einer unnötigen Tiefe verlaufen.

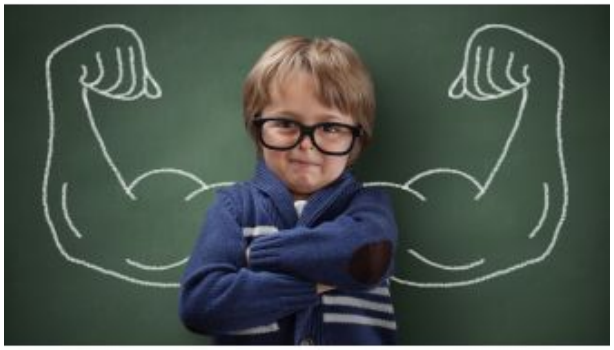
Für ein breites ISMS-Verständnis sorgen
Das Informationssicherheits-Managementsystem funktioniert letztlich nur so gut, wie es von allen Prozessbeteiligten akzeptiert wird. Deshalb sind Awareness-Maßnahmen notwendig, die der aktiven Mitwirkung dienen. Wikis und andere Aktivitäten können zum internen ISMS-Marketing gehören.

Geschäftsleitung in die Schulungen einbeziehen
Erst wenn sich das Top-Management auch auf einer konkreten statt nur auf der abstrakten Ebene in dem Thema einfindet, wird es ein nachhaltiges Verhältnis für die Bedeutung eines ISMS entwickeln. Aus diesem Grund sollte es motiviert werden, zumindest partiell an den betreffenden ISO-Schulungen teilzunehmen.

Frühzeitig für eine KVP-Kultur sorgen
In einem Kontinuierlichen Verbesserungsprozessen (KVP) werden die Sicherheitsmaßnahmen weiterentwickelt. Das verlangt auch ein organisatorisches Selbstverständnis, das über Schulungen hinauentwickelt werden muss.

 (Tipps zusammengestellt von der mikado AG)

gal2Der CISO-Check: Taugen Sie zum IT-Security-Manager?



Glauben Sie ...
... an die Möglichkeit, ihre Systeme gründlichst verteidigen zu können und versuchen Sie daher, alles dafür zu tun, alle Bereiche des Unternehmens jeden Tag ein bisschen besser zu schützen?
Foto: Brian A Jackson - www.shutterstock.com

Schauen Sie ...
... sich nach neuen Instrumenten um, die Funktionsumfang und -tiefe der bestehenden Security-Werkzeuge verbessern?
Foto: STILLFX - www.shutterstock.com

Überwachen Sie ...
... alle Sensoren Ihres Netzes - sowohl visuell als auch mit technischen Mitteln?
Foto: chombosan - www.shutterstock.com

Suchen Sie ...
... kontinuierlich nach neuen Wegen, um Sensordaten besser zu untersuchen und zueinander in Beziehung setzen zu können?
Foto: holbox - www.shutterstock.com

Widmen Sie ...
... der Sicherheit Ihrer geschäftskritischen Anwendungen samt der dort verarbeiteten vertraulichen Daten erhöhte Aufmerksamkeit?
Foto: Olivier Le Moal - www.shutterstock.com

Versuchen Sie ...
... Tag für Tag, Ihr Business besser zu verstehen, damit Sie die IT-Risikoanalyse dem anpassen und stetig verbessern können?
Foto: docstockmedia - www.shutterstock.com

Behalten Sie ...
... Ihre Zulieferer im Blick, damit der Zugriff von Dritten auf vertrauliche und sensible Daten kontrolliert werden kann?
Foto: JunPhoto / www.shutterstock.com

Arbeiten Sie ...
... eng mit den Geschäftsentscheidern zusammen, um die Aufmerksamkeit für das Thema IT-Sicherheit konstant hoch zu halten und über das gesamte Unternehmen hinweg eine Awareness zu erzeugen?
Foto: totojang1977 - www.shutterstock.com

Bewegen Sie ...
... sich in neuen Geschäftsfeldern, in denen disruptive Technologien zum Einsatz kommen und in denen Sie Ihr Security-Wirken schon entfalten können, bevor es richtig ernst wird?
Foto: Lightspring - www.shutterstock.com

Verlieren Sie ...
... nie die Security-Grundlagen aus den Augen - wie beispielsweise das regelmäßige Patchen?
Foto: ChristianChan - www.shutterstock.com

gal3Das Einmaleins der IT-Security

Sichere Passwörter
IT-Sicherheit beginnt mit Sensibilisierung und Schulung der Mitarbeiter sowie mit einer klaren Kommunikation der internen Verhaltensregeln zur Informationssicherheit:

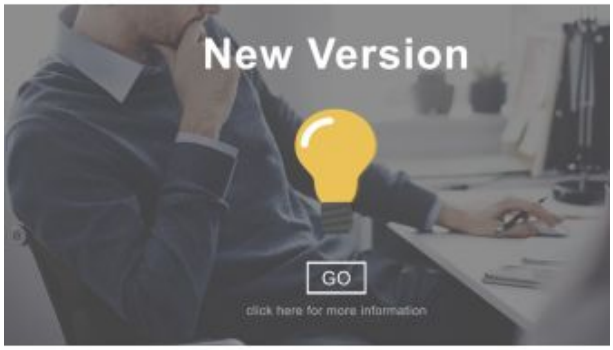
 Komplexe Passwörter aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, mindestens achtstellig.
Foto: wk1003mike - www.shutterstock.com

Passwortdiebstahl
Niemals vertrauliche Daten weitergeben oder/und notieren.
Foto: Brian A Jackson - www.shutterstock.com

E-Mail-Sicherheit
E-Mails signieren, sensible Daten verschlüsseln, Vorsicht beim Öffnen von E-Mail-Anlagen und Links.
Foto: ra2studio - www.shutterstock.com

Soziale Manipulation
Bewusst mit vertraulichen Informationen umgehen, nur an berechtigte Personen weitergeben, sich nicht manipulieren oder aushorchen lassen.
Foto: lolloj - www.shutterstock.com

Vorsicht beim Surfen im Internet
Nicht jeder Link führt zum gewünschten Ergebnis.
Foto: karen roach - www.shutterstock.com

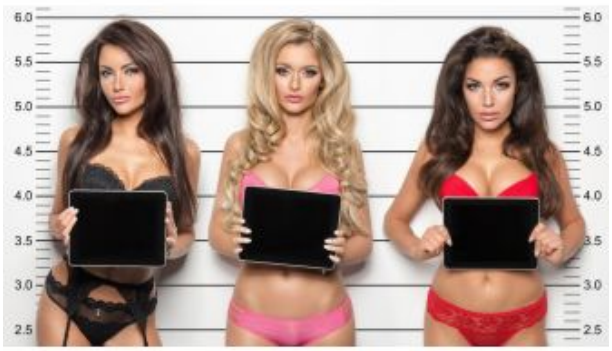


Nur aktuelle Software einsetzen
Eine nicht aktualisierte Software lässt mehr Sicherheitslücken offen.
Foto: Rawpixel.com - www.shutterstock.com

Verwendung eigener Software
Unternehmensvorgaben beachten und niemals Software fragwürdiger Herkunft installieren.
Foto: Pressmaster - www.shutterstock.com

Unternehmensvorgaben
Nur erlaubte Daten, Software (Apps) und Anwendungen einsetzen.
Foto: jesadaphorn - www.shutterstock.com

Backups
Betriebliche Daten regelmäßig auf einem Netzlaufwerk speichern und Daten auf externen Datenträgern sichern.
Foto: Andrea Danti - www.shutterstock.com



Diebstahlschutz
Mobile Geräte und Datenträger vor Verlust schützen.
Foto: Studio10Artur - www.shutterstock.com

Gerätezugriff
Keine Weitergabe von Geräten an Dritte, mobile Geräte nicht unbeaufsichtigt lassen und Arbeitsplatz-PCs beim Verlassen sperren.
Foto: turlakova - www.shutterstock.com

Sicherheitsrichtlinien
Die organisatorischen Strukturen im Hintergrund bilden den erforderlichen Rahmen der IT-Sicherheit. Hier gilt es, klare Regelungen zu formulieren und einzuhalten:

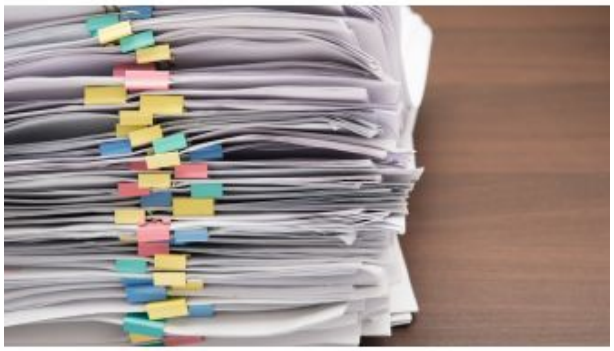
Definition und Kommunikation von Sicherheitsrichtlinien
Foto: Vasin Lee - www.shutterstock.com

Zugriffsrechte
Regelung der Zugriffsrechte auf sensible Daten
Foto: nasirkhan - www.shutterstock.com

Adminrechte
Keine Vergabe von Administratorenrechten an Mitarbeiter
Foto: Potapova - www.shutterstock.com

Softwareupdates
Automatische und regelmäßige Verteilung von Softwareupdates
Foto: Rawpixel.com - www.shutterstock.com

Logfiles
Kontrolle der Logfiles
Foto: turgaygundogdu - www.shutterstock.com



Dokumentation
Vollständige und regelmäßige Dokumentation der IT
Foto: Freer - www.shutterstock.com

Datensicherung
Auslagerung der Datensicherung
Foto: www.BillionPhotos.com - www.shutterstock.com

Sicherheitsanalyse
Regelmäßige Überprüfung der Sicherheitsmaßnahmen durch interne und externe Sicherheitsanalysen
Foto: Kopytin Georgy - www.shutterstock.com

Notfallplan
Erstellung eines Notfallplans für die Reaktion auf Systemausfälle und Angriffe
Foto: Maria Maarbes - www.shutterstock.com

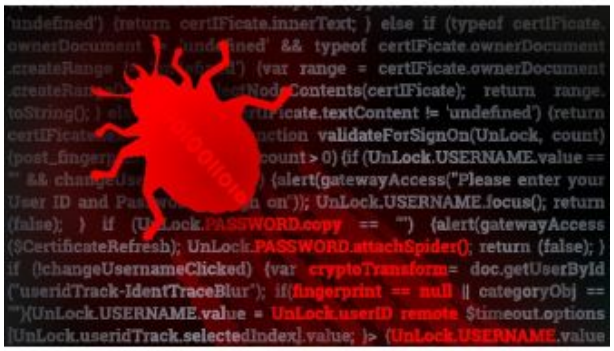
WLAN-Nutzung
Auf technischer Ebene muss ein Mindeststandard gewährleistet sein. Dieser lässt sich größtenteils ohne großen Kostenaufwand realisieren:

Dokumentation der WLAN-Nutzung, auch durch Gäste
Foto: Thomas Reichhart - www.shutterstock.com

Firewalls
Absicherung der Internetverbindung durch Firewalls
Foto: Goritza - www.shutterstock.com

Biometrische Faktoren
Einsatz von Zugangsschutz/Kennwörter/Biometrie
Foto: Patrick Foto - www.shutterstock.com

Zugangskontrolle
Physische Sicherung/Zugangskontrolle und -dokumentation
Foto: Dmitry Kalinovsky - www.shutterstock.com



Schutz vor Malware
Schutz vor Schadsoftware sowohl am Endgerät als auch am Internetgateway, idealerweise durch zwei verschiedene Antivirenprogramme
Foto: Blue Island - www.shutterstock.com

Webzugriffe
Definition einer strukturierten Regelung der Webzugriffe
Foto: Anteromite - www.shutterstock.com

Verschlüsselung
Verschlüsselung zum Schutz von Dateien und Nachrichten mit sensiblen Inhalten
Foto: Piotr Zajda - www.shutterstock.com

Löschen
Sicheres Löschen der Daten bei Außerbetriebnahme
Foto: Lightspring - www.shutterstock.com

Update der Sicherheitssysteme
Sicherstellung regelmäßiger Updates der Sicherheitssysteme
Foto: voyager624 - www.shutterstock.com

Monitoring
Permanente Überwachung des Netzwerkverkehrs auf Auffälligkeiten
zusammengetragen von Giegerich & Partner (https://www.gie-pa.de/)
Foto: Andrey Popov - www.shutterstock.com

12.07.2016

IDG Business Media GmbH