

# ZT IT-KOLUMNE

## IT-Sicherheitsmanagement nach ISO 27001 Grundschatz

Der Wunsch nach umfangreicher Sicherheit eigener IT-Infrastrukturen wächst bei Organisationen und Unternehmen. Eine Zertifizierung nach ISO 27001 Grundschatz hilft dabei, die erforderlichen Maßnahmen umzusetzen und Vertrauen bei den Kunden zu stärken. Dieser Artikel gibt einen Einstieg in die komplexe Materie.

Die Sicherheitsanforderungen an informationsverarbeitenden IT-Systemen sind in den letzten Jahren extrem angestiegen. Nicht zuletzt durch raffinierte und hochkomplexe Cyberangriffe müssen Organisationen und Unternehmen ihre Computersysteme, die immer mehr mit dem Internet verbunden sind, da-

### Was ist eine Bedrohung?

Eine Begriffserklärung des BSI: „Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesund-

schutz. Mittlerweile hat sich der IT-Grundschatz insofern weiterentwickelt, als sich das Sicherheitsmanagement an der ISO 27001 ausrichtet. Für die Maßnahmenauswahl sind weiterhin die Maßnahmenkataloge des IT-Grundschatzes und für die Gefährdungsanalysen ebenfalls die sogenannten Gefährdungskataloge zu verwenden.

Der IT-Grundschatz geht von einer für das IT-System üblichen Gefährdungslage aus und hat hierfür passende Gegenmaßnahmen parat. So kann ein Sicherheitsniveau erreicht werden, das in den allermeisten Fällen ausreicht und damit die viel teurere Risikoanalyse vollständig ersetzt. Sollte der Sicherheitsbedarf größer sein, kann der IT-Grundschatz als Grundlage für weitere Maßnahmen genutzt werden.

### Vorbereitung auf die Zertifizierung

Sollte sich ein Unternehmen für eine ISO 27001 Grundschatz-Zertifizierung entschieden bzw. für die Zukunft geplant haben, sollten unbedingt folgende wichtige Forderungen vorab schon mal geprüft werden:

- Eine gelenkte Dokumentation (ist bewertet, genehmigt, lesbar, ...).
- Sicherung von beweisrelevanten Aufzeichnungen.
- Die Organisation von internen Audits.
- Verbesserung von eingeführten Prozessen.

Wie im IT-Grundschatzhandbuch beschrieben, werden zuerst alle zu prüfenden „Gegenstände“ in einem Datenschutz-/Datensicherheitskonzept vorgestellt. Ein Sicherheitscheck vervollständigt dann die erstellten Konzepte. Folgende entscheidende Themen sollten hierbei berücksichtigt werden:

### Datensicherheitskonzept

- Organisation und Regelungen
- Gebäude und Räume

ANZEIGE

- Architektur der IT-Infrastruktur bzw. Systeme
- Anwendungen
- Personal sowie Datenschutz- und Sicherheitsmanagement

### Istzustand Analyse und Verbesserung

- Ist der Umgang mit personenbezogenen Daten gesetzestkonform?
- Sind die Ziele der Sicherheit angemessen bzw. adäquat?
- Sind die im Datensicherheitskonzept beschriebenen Maßnahmen zur Sicherheit der IT-Infrastruktur ausreichend?
- Sind Internetzugang und Server der IT-Infrastruktur sicher?

Zur Durchführung einer Analyse werden Standard-Informationen aus dem IT-Grundschatzhandbuch verwendet. Das Ergebnis der Analyse sind Verbes-

das BSI gesendet und eine Zertifizierung beantragt werden. Das BSI erteilt dann ein „ISO 27001 Zertifikat auf Basis von IT-Grundschatz“. Dieses Zertifikat ist international anerkannt und aussagekräftiger als ein reines ISO 27001 Zertifikat, da in diesem Fall – zusätzlich zu den allgemeinen Anforderungen der ISO/IEC 27001 auch – die konkreten Anforderungen des Grundschatzes eingehalten werden müssen.

### Fazit und Ausblick

Die Gefährdungslage für informationsverarbeitende Systeme und somit auch für ganze Organisationen und Unternehmen wird auch in Zukunft weiter ansteigen. Es sei den Organisationen und Unternehmen angeraten, sich für

ANZEIGE

gegen absichern. Da auch der Trend sehr stark zu cloudbasierten Anwendungen geht, geraten die Geschäftswerte (alles, was für die Geschäftstätigkeit relevant ist) und Prozesse, die in den informationsverarbeitenden IT-Systemen verarbeitet werden, in den Fokus von professionellen Hackern. Ziele der Hackerangriffe sind:

- Beschädigung oder Zerstörung von IT-Infrastrukturen oder Server-Systemen
  - Spionage (Industrie und Militär)
  - Beschädigung oder Zerstörung von Infrastrukturen von Ländern/Kommunen durch gezielte Angriffe auf deren IT-Infrastrukturen von Terroristen.
- Da die Cyberangriffe immer bedrohlicher und umfangreicher werden, müssen Organisationen und Unternehmen durch Schutzmaßnahmen das Vertrauen in sich und ihre IT-Infrastrukturen weiterhin sichern. Durch eine ISO27001-Zertifizierung auf Basis von Grundschatz des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden die IT-Infrastrukturen mithilfe von Anforderungskatalogen auf Sicherheit analysiert, geprüft und die Maßnahmen beschrieben. Die Organisationen und Unternehmen können dann mittels IT-Grundschatz der BSI die vorgegebenen Vorgehensweisen und Einzelmaßnahmen konkret umsetzen.

Ich möchte an der Stelle klar betonen, dass auch kleine Unternehmen ihre Unternehmensstruktur und informationsverarbeitenden IT-Systeme auf Sicherheit überprüfen sollten. Gerade der Mittelstand hat eine potenziell hohe Gefährdungslage und sollte entsprechende Maßnahmen ergreifen. Das BSI mit ihren Grundschatzkatalogen ist hierbei eine sehr gute Anlaufstelle.

heit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.“ (Quelle: BSI)

### Was bedeutet BSI-Grundschatz?

Das Ziel des BSI ist die präventive Förderung der Informations- und Cybersicherheit, um den sicheren Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft zu ermöglichen und voranzutreiben. Die sogenannten BSI-Standards sind im Prinzip Empfehlungen des BSI zu Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen bezüglich der Informationssicherheit. Organisationen und Unternehmen können diese Empfehlungen dann nach ihren eigenen und speziellen Bedürfnissen anpassen.

Das BSI gibt die IT-Grundschatz-Kataloge heraus, die Empfehlungen für Standardschutzmaßnahmen für typische IT-Systeme enthalten. In diesen Katalogen werden nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Maßnahmen erörtert. Das BSI ist die zentrale Zertifizierungsstelle für die Sicherheit von IT-Systemen in Deutschland (Computer- und Datensicherheit, Datenschutz). Prüfung und Zertifizierung ist möglich in Bezug auf die Standards des IT-Grundschatzhandbuchs. Der IT-Grundschatz wurde von der BSI in einem Grundschatzhandbuch beschrieben und schildert die IT-Sicherheit einschließlich Daten-



serungsvorschläge, die mit den Auftraggebern zusammen diskutiert werden, sodass dann die erstellten Datenschutz- und/oder Datensicherheitskonzepte geändert bzw. angepasst werden können.

### Ablauf der Zertifizierung

Eine Zertifizierung nach ISO 27001 auf Basis des IT-Grundschatzes durch das BSI liefert der Nachweis, dass die Organisation oder das Unternehmen organisatorischen, infrastrukturellen und technischen Maßnahmen der Informationssicherheit für einen definierten Geltungsbereich oder für ihr gesamtes Unternehmen getroffen hat. Ein sogenannter „BSI lizenziertes IT-Grundschatz bzw. ISO 27001 Auditor“ führt die Umsetzung der in den Standards beschriebenen Maßnahmen durch. Das Ergebnis des Auditors ist ein Prüfbericht. Sind alle Maßnahmen umgesetzt, kann der Bericht an

die Sicherheit ihrer IT-Systeme zu interessieren. Ob eine Sicherheitszertifizierung notwendig ist, muss individuell entschieden werden. Auch die vorgeschlagenen Maßnahmen dienen nur als Orientierung und sind ebenfalls individuell an die Gegebenheiten anzupassen. Auch jede einzelne Person in einer Organisation/Unternehmen, ja, sogar in der Gesellschaft, hat die Pflicht, sich mit der Sicherheit für informationsverarbeitende Systeme auseinanderzusetzen. Ebenfalls ist das Verhalten jeder einzelnen Person im Hinblick auf Datensicherheit sehr wichtig. Man denke nur an den Umgang mit Passwörtern und vertraulichen Dokumenten. **ZT**

### ZT Adresse

**Thomas Burgard Dipl.-Ing. (FH)**  
Softwareentwicklung & Webdesign  
Bavariastraße 18b  
80336 München  
Tel.: 089 540707-10  
info@burgardsoft.de  
www.burgardsoft.de



Inspiration und Know-how für das zahntechnische Handwerk

ZT

## ZAHNTECHNIK ZEITUNG

Die Monatszeitung für das zahntechnische Labor | www.zt-aktuell.de

ISSN 1617-5885 · F 47376 · www.oemus.com · Preis 5,- EUR (inkl. zgl. MwSt.) · 16. Jahrgang · Dezember 2016

---

Nr. 2 | Februar 2017 | 16. Jahrgang | ISSN: 1610-482X | PVSt: F 59301 | Entgelt bezahlt | Einzelpreis 3,50 €

**9. DDT in Hagen**  
Kurzentschlossene können sich jetzt noch zum Kongress am 17. und 18. Februar anmelden.

Am 17. und 18. Februar 2017 lädt das Dentale Fortbildungszentrum Hagen (DFH) in Kooperation mit der OEMUS MEDIA AG Zahnärzte und Zahntechniker zum neunten Mal zum Kongress „Digitale Dentale Technologien“ (DDT) ein. Das Leitthema 2017 ist „Zirkon – Ein Werkstoff für alle Fälle?“. Mit der Entwicklung von CAD/CAM-Arbeitsprozessen für die Bearbeitung von Zirkonoxid wurde vor 15 Jahren das digitale Zeitalter im Dentallabor eingeleitet. Die erste Generation von Zirkonoxid wurde vor sehr hart und opaque. Heutzutage wird „Zirkon“ in sehr unterschiedlichen Qualitäten produziert und ist im Bereich festzahnender Ersatz nahezu universell einsetzbar. Transzentes Multilayer-Zirkon steht für überlegene Ästhetik. Auch die sehr harten und opaken Varianten haben ihre Berechtigung und werden z. B. für herausnehmbaren Zahnersatz genutzt. Die Indikationsstellung sowie die Vergleichbarkeit mit anderen Werkstoffen ist jedoch komplizierter geworden. Die Veranstaltung hilft, die Zusammenhänge zu verstehen, und gibt Ratschläge für den täglichen Umgang mit Zirkonoxid. Natürlich wird auch die digitale Fertigungstechnik auf dem Kongress behandelt. Die zahlreichen Workshops am Freitag und die Vorträge hochkarätiger Referenten am Samstag werden von einer umfangreichen Industrieausstellung begleitet. ■■

Eine Anmeldung ist über [www.oemus.com](http://www.oemus.com) jederzeit möglich.

Quelle: OEMUS MEDIA AG

---

**ZT Aktuell**

**Arten des Erfolgs**  
Warum gibt es erfolgreiche Menschen? Marc M. Galal hat Antworten.  
*Wirtschaft*  
▶ Seite 6

**Mein Weg zum ästhetischen Zahnersatz**  
ZTM Tobias Köhler über die individuelle Ästhetik in der Zahntechnik und der Zahnmedizin.  
*Technik*  
▶ Seite 10

**20 Jahre digitale Innovationen**  
Dental Direkt feiert 20-jähriges Jubiläum und blickt zurück auf eine Erfolgsgeschichte.  
*Service*  
▶ Seite 18

**Der Wettbewerb beginnt**  
Einsendeschluss der Meisterarbeiten im Wettbewerb um den Klaus Kanter Förderpreis ist am 31. Mai 2017.

Es ist wieder so weit – die Klaus Kanter Stiftung ruft die Besten der Besten zur Teilnahme am Wettbewerb um den Klaus Kanter Förderpreis auf. Der Gewinner des ersten Preises für die beste praktische Meisterarbeit des vergangenen Jahres eines jeweiligen Kammerbezirks wird mit 3.500 Euro belohnt. Gleichzeitig wird in diesem Wettbewerb mit dem PEERS-Preis eine Meisterarbeit veröffentlicht. Auch in der Fachwelt finden diese Zertifikate hohe Anerkennung. Die Devise heißt also: Mitmachen und anmelden, denn nur wer mitmacht, kann gewinnen! ■■

Die Arbeiten sind einzusenden an:  
galler Zahntechnik  
z. Hd. Herrn H.-D. Deusser  
Dreihäusergasse 12  
60433 Frankfurt am Main

Quelle:  
Klaus Kanter Stiftung

---

**Bessere Zuschüsse ja – bestehende Instrumente aktivieren**  
Der VDZI zu den Forderungen der SPD nach Entlastung der Versicherten bei Zahnersatz.

Zu den Vorstellungen des stellv. SPD-Fraktionsvorsitzenden Prof. Dr. Karl Lauterbach über eine Entlastung gesetzlich Krankenkassenversicherter bei den Kosten für Zahnersatzleistungen, äußert sich der Präsident des Verbandes Deutscher Zahntechniker-Innungen (VDZI), ZTM Uwe Breuer: „Die von Herrn Lauterbach beklagte Kostenbelastung der Versicherten ist maßgeblich eine direkte Folge der Entscheidungen des Gesetzgebers. Dazu gehören die Neugestaltung des Zuschussystems und die Neufestlegung des Leistungsanspruches mit größerer Wahlfreiheit der Versicherten bei veränderten Abrechnungsmodalitäten ab 2005. Das hat in der Tat zu drastischen Milliardenersparungen der Krankenkassen und zu einer höheren Belastung der Versicherten geführt. Der Finanzierungsanteil der GKV an den Zahnersatzkosten ist seit dem Jahr 2000 von 46,2 Prozent auf nur noch rund ein Drittel gesunken.“

▶ Seite 4

**Stark & Schön**  
ZrO<sub>2</sub> einer neuen Generation

**DDcubeX<sup>2</sup> HS**  
high strength cubic zirconia system

- Biegefestigkeit > 1000 MPa
- Transparenz > 45%

**COMING SOON** **IDS 2017**

Besuchen Sie uns in Halle 3.1 Stand J-038/H-030

Dental Direkt GmbH Industriestrasse 106 - 108  
12179 Berlin Tel. +49 30 20 80 31 0  
E-Mail: [info@dentaldirekt.de](mailto:info@dentaldirekt.de) [www.dentaldirekt.de](http://www.dentaldirekt.de)

**20 JAHRE** **Dental Direkt**

ZWL

## ZAHNTECHNIK WIRTSCHAFT LABOR

ISSN 1617-5885 · F 47376 · www.oemus.com · Preis 5,- EUR (inkl. zgl. MwSt.) · 16. Jahrgang · Dezember 2016

---

**Funktion**

AB SEITE 18

**WIRTSCHAFT – SEITE 6**  
Praxisfrage – 09 aktuell sehr  
brillante Thema

**TECHNIK – SEITE 18**  
Nachwuchswettbewerb  
Instrumentelle Blutergötterung?

**VERANSTALTUNG – SEITE 48**  
16. Digital Dentale Technologien  
in Hagen 2017

digital

## dentistry

\_ practice & science

ISSN 2102-0716 · Entgelt bezahlt: 2,90 € · Preis: € 10,00 zzgl. MwSt.

---

4

2016

**Fachbeitrag**  
Intraoralscan komplettiert  
digitalen Laborworkflow

**Spezial**  
Konzepte für erfolgreiches  
Praxismarketing

**Interview**  
„Wichtig ist Transparenz  
und Nähe zum Kunden“

## Fax an 0341 48474-290

Ja, ich möchte die Informationsvorteile nutzen und sichere mir folgende Publikationen bequem im günstigen Abonnement:

- ZT Zahntechnik Zeitung 12x jährlich 55,- Euro\*
- ZWL Zahntechnik Wirtschaft Labor 6x jährlich 36,- Euro\*
- digital dentistry 4x jährlich 44,- Euro\*

Widerrufsbelehrung: Den Auftrag kann ich ohne Begründung innerhalb von 14 Tagen ab Bestellung bei der OEMUS MEDIA AG, Holbeinstraße 29, 04229 Leipzig schriftlich widerrufen. Rechtzeitige Absendung genügt. Das Abonnement verlängert sich automatisch um 1 Jahr, wenn es nicht fristgemäß spätestens 6 Wochen vor Ablauf des Bezugszeitraumes schriftlich gekündigt wird.

\* Preise verstehen sich zzgl. MwSt. und Versandkosten. Entsigelte Ware ist vom Umtausch ausgeschlossen.

Name / Vorname \_\_\_\_\_

Telefon / E-Mail \_\_\_\_\_

Unterschrift \_\_\_\_\_

Praxisstempel \_\_\_\_\_

ZT 2/17

OEMUS MEDIA AG

Holbeinstraße 29 · 04229 Leipzig · Tel.: 0341 48474-201 · [grasse@oemus-media.de](mailto:grasse@oemus-media.de)