# CAk update

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 16 / Januar 2015


**Wir wünschen ein gesundes, erfolgreiches und sicheres Jahr 2015!**

Im neuen Jahr bietet die Cyber-Akademie erstmals das Seminar "Datenschutzbeauftragte(r) im Gesundheitswesen" mit TÜV-Zertifizierung an, das bisher exklusiv bei elf Kassenärztlichen Vereinigungen und der Bundesvereinigung als Inhouse-Seminar angeboten wurde. Die praxisnahe Ausbildung auf Basis der Besonderheiten im Gesundheitswesen mit TÜV Rheinland- Personenzertifizierung geht insbesondere auf

- Besonders sensible personenbezogenen Daten von Patienten ein, die bei einem Missbrauch Betroffene erheblich in ihren Persönlichkeitsrechten beeinträchtigen können.
- das Sozialgesetzbuch (SGB) neben dem Bundes- und den Landesdatenschutzgesetzen (BDSG, LDSG) ein.
- Besonderheiten im Gesundheitswesen neben den allgemeinen Grundlagen für Datenschutzbeauftragte ein.

Die Prüfung wird von der unabhängigen Personenzertifizierungsstelle PersCert TÜV des TÜV Rheinland durchgeführt. Nach erfolgreicher Prüfung erhalten die Teilnehmer das Zertifikat "Datenschutzbeauftragter im Gesundheitswesen mit TÜV Rheinland geprüfter Qualifikation" (siehe auch Certipedia).

Frühjahr 2015

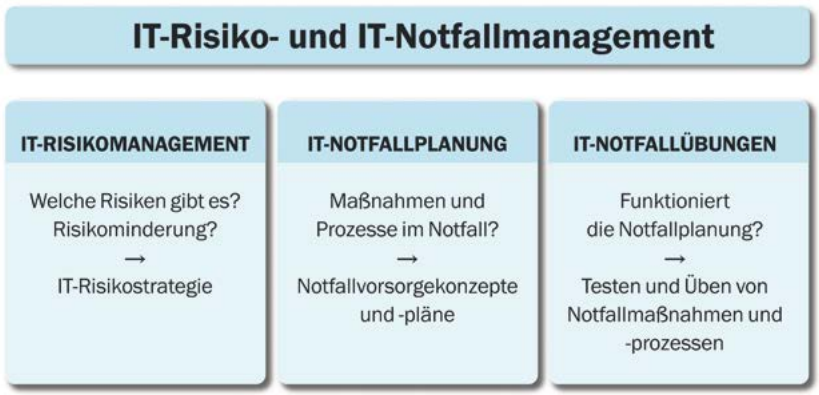
## IT-Risiko und IT-Notfallmanagement

Im März veranstaltet die Cyber Akademie erneut eine IT-Risiko- und IT-Notfallmanagement-Woche, dieses Mal in Düsseldorf. In drei aufeinander abgestimmten Seminaren können Interessierte einen umfassenden, konsistenten Gesamtüberblick über den Themenkomplex erhalten. Die Fortbildungen sind modular konzipiert, so dass auch die Teilnahme an einzelnen Seminaren möglich ist. Alle drei Seminare zusammen können zum Sonderpreis von 1.800,- Euro gebucht werden.

IT-Risikomanagement, IT-Notfallplanung und die Durchführung von IT-Notfallübungen innerhalb einer Organisation sollten aufeinander aufbauen und Hand in Hand gehen.

Die drei Seminare liefern dazu Antworten auf folgende Fragen:

- Welchen Risiken für Informationen und IT ist die eigene Organisation ausgesetzt?
- Welche Konsequenzen können im Krisenfall eintreten und welche Maßnahmen können zur Risikominderung getroffen werden?
- Welche IT-Notfallmaßnahmen sind einzuleiten, um den Geschäftsbetrieb aufrecht zu erhalten?
- Wie stellt man sicher, dass diese im Notfall funktionieren und reibungslos umgesetzt werden?




## CAk-Seminare 2/2015

Webanwendungssicherheit und Penetrationstests
3. März 2015, Hannover

Mobile Device Security – Risiken und Schutzmaßnahmen
3.–5. März 2015, Düsseldorf

Datenschutzbeauftragte(r) im Gesundheitswesen
9.–13. März 2015, Berlin

IT-Risikomanagement – Identifikation, Bewertung und Bewältigung von Risiken
9.–10. März 2015, Berlin

IT-Notfallplanung – Vorausschauende Vorbereitung auf den IT-Notfall
11. März 2015, Berlin

IT-Notfallübungen – In der Krise sicher handeln
12. März 2015, Berlin

Datenschutzbeauftragte(r) in der öffentlichen Verwaltung
13.–17. April 2015, Berlin

Webanwendungssicherheit-Workshop (Live Training)
20.–22. April 2015, Düsseldorf

Informationssicherheit nach BSI-Grundschutz und ISO 27001 im Praxisvergleich
27.–30. April 2015, Frankfurt a.M.

Sichere Webanwendungen in der öffentlichen Verwaltung – Vergabe, Entwicklung, Abnahme
28.-29. April 2015, Bonn

*Alle Seminare und Termine finden Sie unter: www.cyber-akademie.de.*

CAk-Seminare 2/2015

3. März 2015 in Hannover

# Webanwendungssicherheit und Penetrationstests


*Foto: Cak/ © fotomek, fotolia.com*

Die Notwendigkeit Server technisch vor Angriffen zu schützen ist mittlerweile in der freien Wirtschaft und der öffentlichen Verwaltung bekannt und wird von den Administratoren umgesetzt.
Dem gegenüber ist die Sicherheit von Webanwendungen und damit der Schutz der dort verarbeiteten Daten in vielen Fällen unzureichend. Dies zeigen nicht zuletzt die – auch immer häufiger in der breiten Öffentlichkeit – bekannt gewordenen Datenskandale. Fachanwendungen in der öffentlichen Verwaltung und in Unternehmen verarbeiten sehr sensitive, in vielen Fällen personenbezogene Daten. Auch aus Datenschutzgründen muss daher der Sicherheit der Anwendungen ein hoher Stellenwert zukommen.

## Zielsetzung

Das Seminar bietet einen Einstieg in das Thema Webanwendungssicherheit und vermittelt das Verständnis der spezifischen Angriffsmöglichkeiten, welchen Webapplikationen ausgesetzt sind. Die Teilnehmer können anhand von praktischen Beispielen und Demonstrationen die Lücken mit den höchsten Risiken und der größten Verbreitung (OWASP Top 10) nachvollziehen. Aus Zeit- und Effizienzgründen werden keine Hands-On-Übungen durchgeführt. Es werden jedoch praktische Empfehlungen gegeben, wie die Teilnehmer im Nachgang auf Basis kostenfreier Test-Werkzeuge autark entsprechende Penetrations-Übungen selbst durchführen können.

## Zielgruppe

IT-Sicherheitsbeauftragte, CISOs, IT- und IT-Sicherheitsverantwortliche, IT-Administratoren, Entwicklungs-Teamleiter, Webentwickler, Ermittler in Strafverfolgungsbehörden, IT-Dienstleister, Datenschutzbeauftragte

## Preis

490,– Euro zzgl. MwSt.

## Veranstaltungsort

NH-Hotel Düsseldorf City,
Kölner Straße 186-188, 40227 Düsseldorf

## Referent

***Tobias Glemser,*** *Geschäftsführer der secuvera GmbH, verfügt über langjährige Erfahrung im Bereich Sicherheitsüberprüfungen und Penetrationstests. Er ist BSI-zertifizierter Penetrationstester und Certified Ethical Hacker. Darüber hinaus ist er BSI-geprüfter Evaluator und damit berechtigt, Evaluierungen für Zertifizierungen im Rahmen der Common Criteria Compliance durchzuführen.*
*Herr Glemser ist Lead des German Chapters des Open Web Application Security Project (OWASP) und hauptverantwortlich für die Erstellung des OWASP-Whitepapers „Projektierung der Sicherheitsprüfung von Webanwendungen". Seit vielen Jahren ist Herr Glemser sowohl im Rahmen technischer Audits als auch in BSI-Grundschutzprojekten im Behördenumfeld tätig.*

***Mehr Informationen hier***

3. – 5. März 2015 in Düsseldorf

# Mobile Device Security – Risiken und Schutzmaßnahmen


*Foto: Cak/Texelart , fotolia.com; Illustration: Behörden Spiegel-Gruppe*

Smartphones, Tablets und Notebooks bieten hohe Mobilität und Flexibilität, bringen aber auch besondere Sicherheitsrisiken für Behörden und Unternehmen mit sich – vor allem dann, wenn „Bring Your Own Device (BYOD)“ oder „Private Use Of Company Equipment“ ins Spiel kommen. Insbesondere Smartphones sind für Angreifer interessant, da auf diesen eine Vielzahl von Daten bei häufig sehr unzureichendem Schutzniveau zu finden sind.

## Zielsetzung

Das Seminar gibt einen Einblick in die typischen Bedrohungen für mobile Endgeräte (unsichere Apps, gezielte Angriffe, Rooten / Jailbreak, usw.), Authentisierung, Password-Sicherheit, Verschlüsselung, Mobile Device Management und die (Un-)Sicherheit der Übertragungswege. Dabei werden auch die verschiedenen Plattformen (iOS, Android, Blackberry, Windows) verglichen. Die Angriffs- und Schutzmöglichkeiten werden anschaulich in praktischer Form demonstriert.
Die Teilnehmer erkennen, ob und unter welchen Voraussetzungen BYOD in der eigenen Institution ratsam und praktikabel ist und wie mobile Endgeräte verwaltet werden können.

## Zielgruppe

IT-Sicherheitsbeauftragte, CIOs, IT-Leiter, IT-Administratoren, IuK-Verantwortliche, IT-Dienstleister, Ermittler in Strafverfolgungsbehörden, Datenschutzbeauftragte

## Preis

1.250,– Euro zzgl. MwSt.

## Veranstaltungsort

NH-Hotel Düsseldorf City,
Kölner Straße 186-188, 40227 Düsseldorf

## Referent

***Tobias Elsner,*** *IT Security Resulter der @-yet GmbH führt IT-Sicherheitsüberprüfungen bei Behörden und Unternehmen durch. Er verfügt über langjährige Erfahrung als IT-Berater in den Bereichen IT-Infrastruktur, IT-Security und Servervirtualisierung und besitzt die Qualifikation EC Council Certified Ethical Hacker.*

***Mehr Informationen hier***

9.–13. März 2015 in Berlin

# Datenschutzbeauftragte(r) im Gesundheitswesen


*Foto: Cak/Bastian Weltjen , fotolia.com;*

Im Gesundheitswesen kommt dem Datenschutz eine besondere Bedeutung zu, da in verschiedenen Bereichen eine Vielzahl von sensiblen personenbezogenen Daten, vor allem Patientendaten, verarbeitet werden.
In die Zuständigkeit der/des Datenschutzbeauftragten fällt es, entsprechende Datenschutzkonzepte zu erstellen und umzusetzen, die Einhaltung der Datenschutzvorgaben zu kontrollieren, die Leitungsebene sowie die Mitarbeiter in Sachen Datenschutz zu informieren bzw. zu beraten und Awareness-Maßnahmen durchzuführen.

## Zielsetzung

Zur Erfüllung dieser Aufgaben vermittelt das Seminar in kompakter und praxisnaher Form das spezifische „Handwerkszeug" für Datenschutzbeauftragte im Gesundheitswesen. Dazu wird neben dem Bundes- und den Landesdatenschutzgesetzen (BDSG, LDSG) vor allem auf das Sozialgesetzbuch (SGB) eingegangen.
Neben den Grundlagen – wie z. B. Datenschutzmanagement, technisch-organisatorische Maßnahmen, IT-Sicherheitsgrundlagen – werden die Besonderheiten im Gesundheitswesen behandelt.

Die Prüfung wird von der unabhängigen Personenzertifizierungsstelle PersCert TÜV des TÜV Rheinland durchgeführt. Bei Erfolg erhalten die Teilnehmer das Zertifikat „Datenschutzbeauftragter im Gesundheitswesen mit TÜV Rheinland geprüfter Qualifikation".
Hinweis: Im Rahmen des Seminars wurden bereits Datenschutzbeauftragte aus elf Kassenärztlichen Vereinigungen und der Bundesvereinigung ausgebildet und zertifiziert.

## Zielgruppe

Angehende oder bereits tätige Datenschutzbeauftragte im Gesundheitswesen
Vorkenntnisse sind nicht erforderlich

## Preis

**Seminarpreis:** 1.900,– Euro zzgl. MwSt.

**Prüfungsgebühr:** 250,– Euro zzgl. MwSt.

## Veranstaltungsort

InterCityHotel Berlin Hauptbahnhof,
Katharina-Paulus-Straße 5, 10557 Berlin

## Referent

***Michael Redey*** *ist Senior Consultant für Datenschutz, Internal Audit, Revision sowie Informationssicherheit bei der Loomans & Matz AG. Die Schwerpunkte seiner Tätigkeit sind Beratung und Begleitung von Kunden im Rahmen von Audits und Revisionen. Zudem betreut er mittelständische Unternehmen und Behörden als externer Datenschutzbeauftragter.*

***Mehr Informationen hier***

9.–10. März 2015 in Düsseldorf

# IT-Risikomanagement – Identifikation, Bewertung und Bewältigung von Risiken IT-Notfallplanung – VorausIT-


*Foto: Cak/Orlando Florin Rosu , fotolia.com;*

Angesichts der zunehmenden Bandbreite von Gefahren für die IT-Sicherheit ist es von elementarer Bedeutung, die für eine Organisation maßgeblichen Risiken zu identifizieren, mögliche Konsequenzen zu bewerten und Maßnahmen zur Risikominderung zu beschreiben und umzusetzen. Das Seminar gibt eine praktische Anleitung zur Durchführung von IT-Risikoanalysen und zur Definition von risikomindernden Maßnahmen und IT-Risikostrategien

## Zielsetzung

Die Seminarteilnehmer erhalten einen umfassenden Überblick über die Anforderungen eines IT-Risikomanagements sowie die unterschiedlichen Ansätze und Methoden. Sie werden in die Lage versetzt:

- Gefährdungen im Rahmen einer Business Impact Analyse zu ermitteln,
- Kosten-Nutzen-Analysen durchzuführen,
- geeignete Maßnahmen im Rahmen einer IT-Risikostrategie zu planen und umzusetzen,
- die Wirksamkeit der Maßnahmen zu prüfen.

Die Teilnehmer lernen, Risikostrategien zu entwickeln und dabei die Balance zwischen Aufwendungen für risikomindernde Maßnahmen und Rest-Risiken zu finden.

## Zielgruppe

IT-Sicherheitsbeauftragte,CISOs, IT- und IT-Sicherheitsverantwortliche, Business-Continuity-Manager, Risikomanager, Notfallmanager, Mitarbeiter aus Compliance und Controlling sowie Revision und Prüfungsämtern.

## Preis

950,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

## Veranstaltungsort

NH Düsseldorf City,
Kölner Straße 186-188, 40227 Düsseldorf

## Referent

***Björn Schmelter*** *ist Managing Consultant und Product Manager bei der HiSolutions AG mit langjähriger Erfahrung im Bereich Risikomanagement. Als Schwerpunkt seiner Tätigkeit begleitet er Unternehmen und Behörden bei der Einführung von Informationssicherheits-, Business Continuity- sowie Compliance Managementsystemen. Björn Schmelter ist u. a. Certified Lead Auditor für Managementsysteme nach ISO27001 und BS 25999, CISA, Enterprise Risk Manager (Univ.) und Mitautor des BSI-Standards 100-4 Notfallmanagement.*

***Mehr Informationen hier***

11. März 2015 in Düsseldorf

# Notfallplanung – Vorausschauende Vorbereitung auf den IT-Notfall


*Foto: Cak/ Orlando Florin Rosu, fotolia.com*

## Zielgruppe

IT-Sicherheitsbeauftragte, CISOs, IT- und IT-Sicherheitsverantwortliche, Business-Continuity-Manager, Notfallmanager

## Preis

530,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

## Veranstaltungsort

NH Düsseldorf City,
Kölner Straße 186-188, 40227 Düsseldorf

## Gegenstand des Seminars

Trotz bestmöglicher IT-Schutzmaßnahmen besteht immer ein Restrisiko. Für eine vorausschauende IT-Notfallplanung sollten deshalb die Maßnahmen beschrieben werden, die bei Eintreten eines IT-Notfalls einzuleiten sind, um den Schaden zu begrenzen und schnellstmöglich wieder zum Normalbetrieb zurückzukehren.
Die im Seminar vermittelten Best Practices zur Erstellung von IT-Notfallvorsorgekonzepten und -plänen befähigen dazu, im Notfall schnell und gezielt zu reagieren.

## Zielsetzung

Die Seminarteilnehmer erhalten einen vertiefenden Einblick in Struktur und Wirkungsweise von Notfallvorsorgekonzepten und die Funktion der IT-spezifischen Anteile.
Die Erstellung, Beurteilung und Umsetzung von IT-Notfallplänen wird in allen Schritten praxisorientiert vermittelt. Dabei wird die Koordination der IT-Notfallplanerstellung mit den Fachbereichen außerhalb der IT und deren unterschiedlichen Anforderungen erläutert.
In praktischen Übungen erörtern die Teilnehmer Notfallvorsorgekonzepte und erlernen die Erstellung von IT-Notfallplänen.

## Referent

***Stephan Kurth*** *ist Consultant bei der HiSolutions AG. Der Schwerpunkt seiner Tätigkeit liegt in den Bereichen Business Continuity Management, Krisenmanagement, IT-Notfallmanagement und IT-Risikomanagement. Er hat zahlreiche Unternehmen und Behörden bei der Einführung, Überprüfung und Optimierung von Business Continuity Management-Systemen betreut. Herr Kurth ist Certified ISO 22301 Lead Auditor und ITIL-zertifiziert sowie Mitautor des Umsetzungsrahmenwerks zum Standard BSI 100-4 „Notfallmanagement" (UMRA BSI 100-4).*

***Mehr Informationen hier***

12. März 2015 in Düsseldorf

# IT-Notfallübungen – In der Krise sicher handeln


*Foto: Cak/ Orlando Florin Rosu, fotolia.com*

## Zielgruppe

IT-Sicherheitsbeauftragte, CISOs, IT- und IT-Sicherheitsverantwortliche, Notfall- und Krisenmanager, Business-Continuity-Manager

## Preis

530,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

## Veranstaltungsort

NH Düsseldorf City,
Kölner Straße 186-188, 40227 Düsseldorf

## Gegenstand des Seminars

IT-Notfallpläne greifen nur dann, wenn im Krisenfall alle Beteiligten mit den vorgesehenen Maßnahmen und ihren jeweiligen Aufgaben vertraut sind und das Zusammenspiel vorher trainiert wurde. IT-Notfallübungen sollten deshalb in regelmäßigen Abständen und auf allen Ebenen durchgeführt werden. In einer solchen Übung kann zudem überprüft werden, wie wirkungsvoll die Pläne zur Notfall- bzw. Krisenbewältigung sind.

## Zielsetzung

In diesem Seminar werden die Teilnehmer mit den unterschiedlichen Übungsarten und deren Einsatzbereichen vertraut gemacht:

- technische Tests,
- Plan-Review,
- Planbesprechung,
- Stabsübungen,
- Stabsrahmenübungen,
- Kommunikations- und Alarmierungsübung,
- Simulation von Szenarien,
- Ernstfall- oder Vollübung.

In Workshops wenden die Teilnehmer die Methoden und Werkzeuge an und werden befähigt, IT-Notfallübungen in ihrer Institution selbst anzulegen, durchzuführen und auszuwerten.

## Referenten

***Stefan Riegel** und **Kai Mettke-Pick** sind Managing Consultants bei der HiSolutions AG. Beide weisen langjährige Erfahrungen in der Beratung zu Krisen,- Notfall- und IT-Notfallmanagement, IT-Risikomanagement sowie Informationssicherheit auf. Ihre Tätigkeitsschwerpunkte liegen zudem im Aufbau von Übungs- und Testprogrammen für Notfall- und Krisenmanagement. Stefan Riegel ist Mitautor des Umsetzungsrahmenwerkes zum BSI-Standard 100-4. Kai Mettke-Pick war viele Jahre als Konzernkoordinator für Business Continuity Management bei einer großen deutschen Bank tätig.*

***Mehr Informationen hier***

13.–17. April 2015 in Berlin

# Datenschutzbeauftragte(r) in der öffentlichen Verwaltung – Behördliche(r) Datenschutzbeauftragte(r)


*Foto: Cak/ Bastian Weltjen, fotolia.com*

## Gegenstand des Seminars

Das Bundesdatenschutzgesetz (BDSG) sowie die jeweiligen Landesdatenschutzgesetze (LDSG) schreiben die Benennung von Datenschutzbeauftragten in Behörden zur Umsetzung des Datenschutzes vor. Um diese Aufgaben ordnungsgemäß erfüllen zu können, sind sowohl umfassende rechtliche, technische und organisatorische Kenntnisse und Fähigkeiten erforderlich, die in diesem Seminar vermittelt werden.

## Zielsetzung

Das Seminar stellt in kompakter und praxisnaher Form das „Handwerkszeug" für Datenschutzbeauftragte bereit und behandelt folgende Themen: Rechtsgrundlagen, Zulässigkeit der Datenverarbeitung, bereichsspezifischer Datenschutz, Beschäftigtendatenschutz, Auftragsdatenverarbeitung, Datenschutzmanagement, technische und organisatorische Maßnahmen, BSI-Standards, Risikoanalysen und Kontrollen, IT-Sicherheit-Grundlagen.
Neben dem Bundesdatenschutzgesetz wird auch auf die Landesdatenschutzgesetze der jeweiligen Teilnehmer eingegangen.
Die Prüfung wird von der unabhängigen Personenzertifizierungsstelle PersCert TÜV von TÜV Rheinland durchgeführt. Bei Erfolg erhalten die Teilnehmer das Zertifikat „Datenschutzbeauftragter in der öffentlichen Verwaltung mit TÜV Rheinland geprüfter Qualifikation".

## Zielgruppe

Angehende oder bereits tätige Datenschutzbeauftragte in Behörden und bei Dienstleistern
Vorkenntnisse sind nicht erforderlich.

## Preis

**Seminarpreis:** 1.990,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

**Prüfungsgebühr:** 297,50 Euro inkl. MwSt.

## Veranstaltungsort

InterCityHotel Berlin Hauptbahnhof,
Katharina-Paulus-Straße 5, 10557 Berlin

## Referenten

***Thomas Fischer,*** *Senior Consultant für Informationssicherheit und Business Continuity bei der Loomans & Matz AG*

***Michael Redey,*** *Senior Consultant für Datenschutz, Internal Audit, Revision sowie Informationssicherheit bei der Loomans & Matz AG*

***Dagobert Brauburger,*** *Senior Consultant für Informationssicherheit bei der Loomans & Matz AG mit Schwerpunkt IT-Grundschutz nach BSI*

***Mehr Informationen hier***

20.–22. April 2015 in Düsseldorf

# Webanwendungssicherheit-Workshop

***Sage es mir, und ich vergesse es.***
***Zeige es mir, und ich erinnere mich.***
***Lass es mich tun, und ich verstehe es.***
*(nach Konfuzius, chines. Philosoph)*

**WEB SECURITY LIVE**
Die Teilnehmer dieses Workshops sammeln unter Anleitung von Experten praktische Erfahrungen zu Angriffsmöglichkeiten und Schutzmaßnahmen und führen Penetrationstests selbst durch.

Nach einem kurzen Überblick zu Webtechnologien erfahren die Teilnehmer anhand praktischer Beispiele und Demonstrationen, welchen Angriffsmöglichkeiten und Risiken Webapplikationen ausgesetzt sind. Mittels entsprechender Tools führen die Teilnehmer selbst an bereitgestellten PC-Arbeitsplätzen Penetrationstests durch, erlernen auf praktische Weise das Erkennen von Lücken sowie Angriffsvektoren und kennen nach dem Workshop die technischen Möglichkeiten zur Absicherung von Webanwendungen.

## Zielgruppe
IT-Administratoren, Entwicklungs-Teamleiter, Webentwickler, Ermittler in Strafverfolgungsbehörden, IT-Dienstleister, CERT-Personal, IT-Sicherheitsbeauftragte

Grundkenntnisse im Bereich HTTP bzw. Webtechnologien werden vorausgesetzt.

## Preis
1.420,– Euro zzgl. MwSt.

## Veranstaltungsort
In den Schulungsräumen der Lanworks AG,
Lippestrasse 4, 40221 Düsseldorf

## Trainer
***Tobias Elsner,*** *IT Security Resulter der @-yet GmbH führt IT-Sicherheitsüberprüfungen bei Behörden und Unternehmen durch. Er verfügt über langjährige Erfahrung als IT-Berater in den Bereichen IT-Infrastruktur, IT-Security und Servervirtualisierung und besitzt die Qualifikation EC Council Certified Ethical Hacker.*

***Mehr Informationen hier***

27.–30. April 2015 in Frankfurt a. M.

# Informationssicherheit nach BSI-Grundschutz und ISO 27001 im Praxisvergleich


*Foto: Cak/ Orlando Florin Rosu, fotolia.com*

## Gegenstand des Seminars

In Deutschland gebräuchliche Informationssicherheitsmanagement-Standards sind der IT-Grundschutz des BSI und die ISO 27001. Das Seminar behandelt folgende Aspekte:

- Anwendung der beiden Standards in der Praxis
- Unterschiede der Standards und Eignung für die jeweilige Institution
- Kombination von Elementen beider Standards?
- Bedeutung eines Umstiegs von einem Standard auf den anderen

## Zielsetzung

Die Seminarteilnehmer eignen sich Praxiserfahrung zur Anwendung der beiden Standards an. Anhand einer realitätsnahen (fiktiven) „Modell-Organisation" erstellen sie

- im Teil 1 (Tag 1 und 2) ein IT-Sicherheitskonzept nach IT-Grundschutz des BSI,
- im Teil 2 (Tag 3 und 4) ein IT-Sicherheitskonzept nach ISO 27001.

Die Teilnehmer erkennen auf diese Weise die Unterschiede im Vorgehen und können einen Vergleich der Ergebnisse beider Methoden anstellen. Wenn Sie beabsichtigen in Ihrer Institution ein Informationssicherheitsmanagement (neu) aufzubauen, hilft Ihnen dieses Praxisseminar die für Sie angemessene Vorgehensweise zu ermitteln. Aufgrund des modularen Seminaraufbaus ist auch die Teilnahme an nur einem der beiden Teile möglich.

## Zielgruppe

IT-Sicherheitsbeauftragte, CIOs, verantwortliche Personen aus den Bereichen Informationssicherheit, Netz- und Systemadministration, IT-Organisation, IT-Beratung, Revision und Risikomanagement.
Die Teilnehmer sollten die Grundbegriffe der beiden Standards kennen.

## Preis

**Praxis-Workshop gesamt**
(Teile 1 und 2): 1.790,– Euro zzgl. MwSt.
**Alternativ:**
Teil 1 oder Teil 2 einzeln: je 990,– Euro zzgl. MwSt

## Veranstaltungsort

Novotel Frankfurt City
Lise-Meitner-Straße 2, 60486 Frankfurt am Main

## Referenten

***Thomas Fischer,*** *Senior Consultant für Informationssicherheit und Business Continuity bei der Loomans & Matz AG*

***Michael Redey,*** *Senior Consultant für Datenschutz, Internal Audit, Revision sowie Informationssicherheit bei der Loomans & Matz AG*

***Dagobert Brauburger,*** *Senior Consultant für Informationssicherheit bei der Loomans & Matz AG mit Schwerpunkt IT-Grundschutz nach BSI*

***Mehr Informationen hier***

28.–29. April 2015 in Bonn

# Sichere Webanwendungen in der öffentlichen Verwaltung – Vergabe, Entwicklung, Abnahme


*Foto: Cak/Pure Solution, fotolia.com*

## Gegenstand des Seminars

Über Webanwendungen können Behörden und Unternehmen moderne Dienstleistungen für Bürger und Kunden bereitstellen. Um aber auch dem spezifischen Schutzbedarf gerecht zu werden, sollten entsprechende IT-Sicherheitsvorgaben zur Konzeption, Umsetzung und zum Betrieb von Webanwendungen rechtzeitig im Rahmen der Vergabe oder des Entwicklungsprojekts eingebracht werden.

## Zielsetzung

Das Seminar zeigt die spezifischen Sicherheitslücken in Webanwendungen auf. Anhand von Praxisbeispielen werden die Grundlagen für Beauftragung, Projektierung, Entwicklung und Abnahme sicherer Webanwendungen vermittelt. Die Teilnehmer werden befähigt,

- IT-Sicherheitsanforderungen nach dem Stand der Technik in Projektplanungen und Vergabeunterlagen zu integrieren,
- die Eignung potentieller Auftragnehmer anhand von Leistungskriterien bereits vor dem Projektstart zu bewerten,
- die Leistungen von Auftragnehmern während Vergabe und Projektumsetzung anhand von Quality Gates zu bewerten,
- IT-Sicherheitsanforderungen im Entwicklungsprozess zu implementieren und umzusetzen,
- den Reifegrad des Prozesses zu bestimmen und zu erhöhen,
- den Abnahmeprozess für Webanwendungen durchzuführen.

Die Seminarinhalte orientieren sich dabei an den entsprechenden Leitfäden des BSI.

## Zielgruppe

Auftraggeber in der öffentlichen Verwaltung (technischer Einkauf, Projektmanager, QS), Projekt-, Fach- und IT-Sicherheitsverantwortliche in Behörden, Unternehmen, die im Auftrag Webanwendungen entwickeln (Projektmanager, SW-Entwickler, …)

## Preis

890,– Euro zzgl. MwSt.

## Veranstaltungsort

Gustav-Stresemann-Institut Bonn,
Langer Grabenweg 68, 53175 Bonn

## Referent

***Amir Salkic,*** *MSc „Informationsmanagement und Computersicherheit", ist Security Consultant bei der SEC Consult Unternehmensberatung GmbH und berät nationale wie internationale Kunden in den Themen Informationssicherheit, Awareness und Applikationssicherheit. Herr Salkic verfügt über umfangreiche Erfahrungen aus Projekten für Behörden und Unternehmen und hat an den BSI-Leitfaden zur Entwicklung sicherer Webanwendungen mitgewirkt.*

***Mehr Informationen hier***

**IMPRESSUM**

**Herausgeber:** Cyber Akademie GmbH, Geschäftsführer: Ralf Kaschow, R. Uwe Proll; **Presserechtlich Verantwortlicher:** R. Uwe Proll
**Geschäftsstelle:** Friedrich-Ebert-Alle 57, 53113 Bonn, Telefon: 0049-228-97097-0, Telefax: 0049-228-97097-75, ↗ *www.cyber-akademie.de*
Registergericht: HRB 148255 AG Berlin (Charlottenburg)
**Redaktionelle Leitung:** R. Uwe Proll; **Redaktion:** Ralf Kaschow, Sven Schuberth; **Redaktionsassistenz:** Angelina Meyer (Bonn), Kerstin Marmulla , Angela Götze (Berlin)
**Programmbeirat:** Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Troels Oerting, Assistant Director Europol, Head of European Cybercrime Centre (EC3); Dr. August Hanning, Staatssekretär a.D. Bundeministerium des Innern, Präsident des Bundesnachrichtendienstes a.D.; Reinhold Harnisch, Geschäftsführer Kommunales Rechenzentrum Minden-Ravensberg/Lippe; Hans-Jürgen Hohnen, Staatssekretär a.D. Innenministerium Brandenburg; Prof. Dr. Radu Popescu-Zeletin, ehem. Leiter des Fraunhofer Instituts für Offene Kommunikationssysteme; Dieter Schneider, LKA-Präsident Baden Württemberg; Andreas Schuster, Landesbezirksvorsitzender Brandenburg der Gewerkschaft der Polizei (GdP); Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW