

# CAk update

Newsletter der Cyber Akademie zur Informationssicherheit



Nr. 17 / Februar 2015

## Malware-Monat Mai

Im Mai 2015 bietet die Cyber-Akademie zwei besondere Seminare mit dem Schwerpunkt auf technischer Informationssicherheit an, die in diesem Newsletter beschrieben werden. Bereits jetzt machen wir auf das Seminar IT-SiBe in der öffentlichen Verwaltung aufmerksam. Kurztgeschlossene können noch weitere CAk-Seminare im Frühjahr buchen. In diesen Seminaren sind noch **Plätze frei**:

- **Webanwendungssicherheit und Penetrationstests**, 03.03.2015, Hannover
- **Mobile Device Security**, 03.-05.03.2015, Düsseldorf
- **IT-Risiko- und IT-Notfallmanagement-Woche 2015**, 09.-12.03.2015, Düsseldorf

Mai 2015

## Abwehr, Aufdeckung und Aufarbeitung von Cyber-Angriffen und Datendiebstahl

Nicht nur Wirtschaftsunternehmen werden ausspioniert, sondern auch Behörden, Ministerien und Öffentliche Verwaltungen werden gezielt angegriffen, wie die Berichte über Malware mit harmlos klingenden Namen wie "Regin" und "Turla" gezeigt haben. Auch die desaströsen Auswirkungen des Sony-Hacks können keinen IT-Verantwortlichen kalt lassen. Um sich auf Angriffe vorzubereiten muss man verstehen, wie der Gegner denkt und arbeitet. Das kann zum einen dadurch gelingen, dass man verschiedene Angriffsszenarien durchspielt und Abwehrmaßnahmen ergreift. Zum anderen kann man sich auf die Spurensuche nach einem erfolgten Angriff durch forensische Analysen machen.

Mit den beiden Kursen zu Hacking-Methoden und der forensischen Spurensuche auf elektronischen Datenträgern stehen im Wonnemonat Mai zwei besonders technisch ausgelegte Kurse auf dem Programm der Cyber-Akademie, die solide Grundkenntnisse der Informationstechnologie voraussetzen.

## CAk-Seminare 5/2015

IT-Forensik – Spurensuche auf elektronischen Datenträgern  
05.-07. Mai 2015, Frankfurt a.M.

Hacking-Methoden in der Praxis: Vorgehen des Angreifers und Schutzmaßnahmen  
11.-12. Mai 2015, Berlin

IT-Sicherheitsbeauftragte(r) in der öffentlichen Verwaltung  
22.-26. Juni 2015, Nürnberg

[www.cyber-akademie.de](http://www.cyber-akademie.de)



Zentrum für Informationssicherheit

## Besuchen Sie unseren Stand und unsere Partnerforen auf dem 18. Europäischen Polizeikongress

- ▶ Big Data: Analyse unstrukturierter Datenmengen
- ▶ Lagebild: Cyber-Kriminalität 2015 – und Gegenstrategie

**24.–25. Februar 2015, Berlin Congress Center**



Weitere Informationen zu diesen und anderen Seminaren unter: [www.cyber-akademie.de](http://www.cyber-akademie.de)



5. bis 7. Mai 2015 in Frankfurt/Main

# IT-Forensik – Spurensuche auf elektronischen Datenträgern



Foto: CAK/© Orlando Florin Rosu, fotolia.com

Bereits bei dem Verdacht eines Datendiebstahls durch einen Angreifer oder des Missbrauchs Ihres IT-Systems zu kriminellen Zwecken sollte verzugslos gehandelt werden. An dieser Stelle setzt die IT-Forensik an: Entsprechende Spuren müssen gerichtsverwertbar gesichert und ausgewertet werden, um Sicherheitslücken rasch zu identifizieren und den Täter zu ermitteln.

## Zielsetzung

Das Seminar vermittelt technische Begriffe, rechtliche Aspekte, Organisation und Vorgehensweisen zur Planung und Durchführung von IT-forensischen Untersuchungen.

Das technisch orientierte Seminar geht explizit auf die praktische Anwendung der Methoden und Werkzeuge ein, mit welchen elektronische Daten auf verschiedenen Datenträgern – z.B. Festplatten, Smartphones und Server – gerichtsverwertbar gesichert und analysiert werden können.

Live-Demonstrationen mit anonymisierten Falldaten sind ebenso Bestandteil wie Erfahrungsberichte aus der Ermittlungspraxis.

## Zielgruppe

IT-Sicherheitsbeauftragte, IT-Leiter und IT-Administratoren, Ermittler im polizeilichen Bereich, Incident Manager, Datenschutzbeauftragte, Revisoren, IT-Dienstleister.

Voraussetzung für die Teilnahme sind solide IT-Grundkenntnisse.

## Preis

1.520,- Euro zzgl. MwSt.

## Veranstaltungsort

Novotel Frankfurt City,

Lise-Meitner-Straße 2, 60486 Frankfurt am Main

## Referenten



**Hakan Özbek**, Direktor Analytic Forensic Technology, Deloitte Deutschland, Certified Fraud Examiner, Certified Information System Auditor



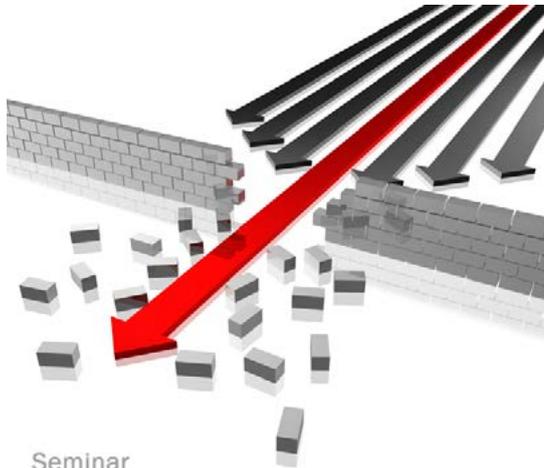
**Sven Bursch-Osewold**, Manager Analytic Forensic Technology, Deloitte Deutschland, Encase Certified Examiner

Beide Referenten verfügen über langjährige Erfahrung im Einsatz IT-forensischer Methoden und Technologien im Auftrag von Ermittlungsbehörden sowie im gutachterlichen Umfeld.

**Mehr Informationen hier**

11. – 12. Mai 2015 in Berlin

# Hacking-Methoden in der Praxis: Vorgehen und Schutzmaßnahmen



Seminar

## Hacking-Methoden in der Praxis: Vorgehen des Angreifers und Schutzmaßnahmen

Foto: Cak/© nali, fotolia.com

„Man muss den Feind kennen, um ihn schlagen zu können“

(Sunzi, chinesischer Strategie)

Wirkungsvolle IT-Sicherheitsmaßnahmen können nur dann getroffen werden, wenn man die Hacking-Methoden und -Mittel des Angreifers kennt. Deren Bandbreite wächst mit Fortschreiten der technologischen Entwicklung ständig. Selbst technisch wenig versierte Personen können mittlerweile leistungsfähige Angriffstools inkl. Supportleistungen (illegal) käuflich erwerben und einsetzen.

### Zielsetzung

Die Teilnehmer des Seminars werfen einen Blick hinter die Kulissen und erleben nachvollziehbar in Live-Demonstrationen, auf welche Weise und mit welcher Motivation Angreifer aktuell in eine IT-Umgebung eindringen und welche Schäden daraus entstehen können. Sie erhalten einen umfassenden Überblick über die gängigen Angriffsmethoden und -mittel (SQL-Injection, Man-in-the-Middle-Angriffe, Netzwerkenumeration, Keylogger, Netzwerksniffer, Session Hijacking usw.) und entsprechende organisatorische und technische Gegenmaßnahmen.

### Zielgruppe

IT-Sicherheitsbeauftragte, IT- bzw. IuK-Verantwortliche, -Architekten und -Administratoren, CERT-Personal, Ermittler in Strafverfolgungsbehörden. Teilnahmevoraussetzung: solide IT-Grundkenntnisse, unter anderem über gängige Netzwerktechnik sowie Betriebssystem- und Anwendungsarchitektur.

### Preis

990,- Euro zzgl. MwSt.

### Veranstaltungsort

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

### 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**

22.–26. Juni 2015 in Nürnberg

# IT-Sicherheitsbeauftragte(r) in der öffentlichen Verwaltung



## Gegenstand des Seminars

Ohne die Verfügbarkeit von digitalen Informationen und Prozessen geht in vielen Bereichen nichts mehr. Für deren Sicherheit spielt der IT-Sicherheitsbeauftragte eine wesentliche Rolle, indem er vor allem folgende Aufgaben wahrnimmt:

- Beratung der Leitungsebene,
- Erstellung einer Leitlinie zur Informationssicherheit,
- Gesamtkoordination des Informationssicherheitsprozesses,
- Initiierung von Sensibilisierungsmaßnahmen,
- Erstellung von IT-Sicherheits- und IT-Notfallkonzepten,
- Untersuchung von Sicherheitsvorfällen.

## Zielsetzung

Das Seminar vermittelt das „Handwerkszeug“ zur Erfüllung der Aufgaben eines behördlichen IT-Sicherheitsbeauftragten. Die Teilnehmer eignen sich Fachwissen in folgenden Themenbereichen an: technische Computer- und Netzwerksicherheit, Kryptographie, organisatorische und physische IT-Sicherheit, rechtliche Grundlagen, ISM nach IT-Grundschutz des BSI. Die Prüfung wird durch die Personenzertifizierungsstelle PersCert TÜV des TÜV Rheinland durchgeführt, bei Erfolg erhalten die Teilnehmer das Zertifikat „IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung mit TÜV Rheinland geprüfter Qualifikation“.

## Zielgruppe

IT-Sicherheitsbeauftragte und -koordinatoren, IT-Dienstleister, IT- und IT-Sicherheitsverantwortliche, Datenschutzbeauftragte.

## Preis

### Seminarpreis:

2.100,- 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

NH-Hotel Nürnberg City Center,  
Bahnhofstraße 17-19, 90402 Nürnberg



## 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**

## IMPRESSUM

Herausgeber: Cyber Akademie GmbH, Geschäftsführer: 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](http://www.cyber-akademie.de)

Registrierungsgericht: HRB 148255 AG Berlin (Charlottenburg)

Redaktionelle Leitung: R. Uwe Proll; Redaktion: 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. Bundesministerium 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