# Security: Cybersicherheit und Riskmanagement mit PwC Survey

CONNECT INFORMUNITY

**Donnerstag, 8. März 2018**
**9.00–15.00 Uhr**

**PricewaterhouseCoopers (PwC)**
**1030 Wien, Erdbergstraße 200**

- **Präsentation des Global State of Information Security® Survey 2018 von PwC mit einem Schwerpunkt auf Österreich**
- **Vorhersage und nachhaltige Bewältigung von Cyber-Attacken – Threat Intelligence, Threat Prediction mit Security KI und Big Data**
- **AKTUELLER Stand zur Securityforschung aus Sicht des Austrian Institute of Technology – am Beispiel von Quantenkryptographie und andere Themen**
- **DSGVO & Passwortmanagement**
- **DSGVO-AUDIT: Worauf es ankommt!**
- **Die neue Datenschutzgrundverordnung und ihre Umsetzung**
- **Secure Coding**
- **Podiumsdiskussion**

**Referenten:**
**Ulrich Bayer** (SBA Research), **Wolfgang Fiala** (Fiala Informatik), **Dr. Markus Frank, LLM** (Frank Law), **Daniel Holzinger** (colited), **Christian Kurz** (PwC Österreich), **Uwe Maurer** (NTT Security), **Martin Stierle** (AIT – Austrian Institute of Technology)

**Bei freiem Eintritt.**
**Anmeldung erforderlich!**

Mit freundlicher Unterstützung von: AIT Austrian Institute of Technology, fh st.pölten, NTT Security, pwc, SBA Research, Future Network

## AGENDA

**8.30** **Registration**

**9.00** **Global State of Information Security® Survey 2018 mit einem Schwerpunkt auf Österreich**
Christian Kurz (PwC Österreich)

**10.00** **Vorhersage und nachhaltige Bewältigung von Cyber-Attacken – Threat Intelligence, Threat Prediction mit Security KI und Big Data**
Uwe Maurer (NTT Security)

**10.30** **Pause**

**11.30** **Podiumsdiskussion**

**12.20** **AKTUELLER Stand zur Securityforschung aus Sicht des Austrian Institute of Technology – am Beispiel von Quantenkryptographie und andere Themen**
Martin Stierle (AIT – Austrian Institute of Technology)

**12.45** **DSGVO & Passwortmanagement**
Daniel Holzinger (colited)

**13.00** **Pause**

**13.30** **DSGVO-AUDIT: Worauf es ankommt!**
Wolfgang Fiala (Fiala Informatik)

**14.00** **Die neue Datenschutzgrundverordnung und ihre Umsetzung**
Markus Frank (Frank Law)

**14.30** **Secure Coding**
Ulrich Bayer (SBA Research)

**15.00** **Ende der Veranstaltung**

## Global State of Information Security® Survey 2018 mit einem Schwerpunkt auf Österreich

### Vorbereitung auf die Cyberangriffe als Geschäftsanforderung

**Christian Kurz** (PwC Österreich)

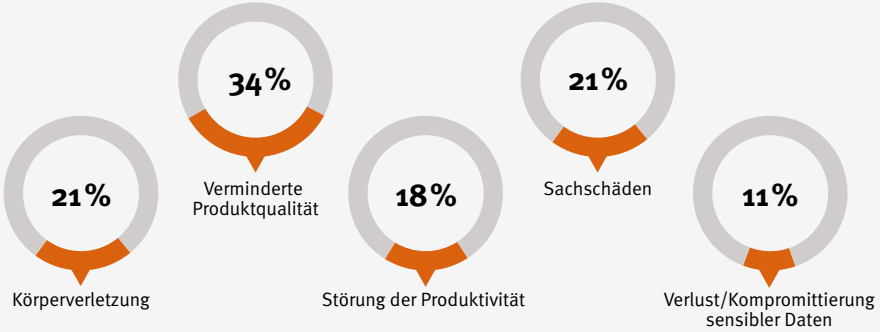
Die Funktion des Chief Information Security Officers (CISO) gewinnt zunehmend an Bedeutung. Der GSISS 2018 zufolge, berichten in Österreich rund 43 % der CISOs (oder CSOs) an den Chief Privacy Officer, 24 % an die Unternehmensleitung und 14 % jeweils an den CIO (Chief Information Officer), den CTO (Chief Technology Officer) bzw. an den COO (Chief Operating Officer).

Viele Organisationen könnten proaktiver mit Cyberrisiken umgehen. Nur 19 % der Befragten geben an, dass ihre Organisation Background Checks durchführt. Nur ein Viertel der Studienteilnehmer (25 %) hat Schlüsselprozesse zur Aufdeckung von Cyberrisiken in Geschäftssystemen eingeführt – darin inbegriffen Penetration Tests, Threat Assessments, Monitoring von Sicherheitsinformationen sowie Sicherheits- und Schwachstellenanalysen.

Es bedarf mehr Informationsaustausch und Koordination zwischen den Stakeholdern. Nur 49 % der Studienteilnehmer geben an, dass sie formell mit anderen in ihrer Branche, einschließlich Mitbewerbern, zusammenarbeiten, um die Sicherheit zu erhöhen und potentielle zukünftige Bedrohungen zu verringern

### 22 % geben an, dass ihre Organisationen planen, IoT-Risiken quer über das Geschäftsfeld zu erfassen.

Erwartete Ergebnisse einer erfolgreichen Cyberattacke gegen Automatisierungs- bzw. Robotersysteme




*Quelle: PwC, CIO und CSO, The Global State of Information Security® Survey 2018, 18. Oktober 2017. Basis: 9500 Befragte*

## Vorhersage und nachhaltige Bewältigung von Cyber-Attacken – Threat Intelligence, Threat Prediction mit Security KI und Big Data

**Uwe Maurer**
(NTT Security)

NTT überwacht laufend die globale Bedrohungssituation und konkrete kritische Bedrohungen. Gleichzeitig werden neue Technologien im Bereich Cyber Defense kontinuierlich weiterentwickelt. Für die Vorhersage von Cyber-Attacks aus dem Internet setzt NTT Security stark auf Threat Intelligence, Threat Prediction mittels Techniken der künstlichen Intelligenz und Big-Data-Analyse.

Für die Erkennung von Angreifern, die bereits im Netz sind, von Verstößen gegen die Richtlinien und von Fehlern bei den Sicherheitseinrichtungen werden Überwachungsregeln aus den Libraries und den Erfahrungen der NTT bei Compromize-Analysis und Forensik eingesetzt. Zudem werden die Daten in Security-Metriken und Schwellwerten verwendet, um laufend die Prevention und die Incident-Response zu verbessern.

Wir zeigen auf, wie mit unseren Experten, auch auf Grundlage von bestehenden Log-Systemen, bei Ihnen ein Intrusion-Detection und Incident-Management nach State-of-the-Art aufgebaut und betrieben werden kann.

## AKTUELLER Stand zur Securityforschung aus Sicht des Austrian Institute of Technology – am Beispiel von Quantenkryptographie und andere Themen

**Martin Stierle**
(AIT – Austrian Institute of Technology)

## DSGVO & Passwortmanagement

**Daniel Holzinger**
(colited)

Eine Passwortmanagement-Lösung unterstützt bei der Umsetzung einiger Regularien der DSGVO. So erfordert der Artikel 32 DSGVO beispielsweise, dass es Systeme und Prozesse gibt, die das Risiko von undichten Stellen in Bezug auf persönliche Daten minimieren. Mit dem Einsatz einer Passwortmanagement-Lösung können verantwortliche Personen belegen, dass Zugriffe nur bestimmten Personen oder Gruppen erlaubt werden. Darüber hinaus können Zugriffsrechte sofort entfernt werden, wenn diese nicht mehr gebraucht werden (Mitarbeiterkündigung, Veränderungen im Team etc.).

Im Vortrag erfahren Sie:

- Warum ein großer Teil der Datenschutzverletzungen auf schwache Passwörter zurückzuführen ist
- Wie Sie den Zugriff auf Unternehmensanwendungen sicher gestalten
- Wie Sie die konkurrierenden Prioritäten der Endanwender und der Unternehmens-IT lösen
- Wie Sie ein zentrales Management in Ihrem Unternehmen aufbauen
- Wie Sie einfach Richtlinien kontrollieren und Berichte erstellen
- Wie Sie Single Sign-On und eine Zwei-Faktor-Authentifizierung integrieren

## DSGVO-AUDIT: Worauf es ankommt!

**Wolfgang Fiala**
(Fiala Informatik)

Zu den Aufgaben eines Datenschutz-Beauftragten gehört die Überwachung der Einhaltung der DSGVO. Dabei wird auf externe Audits zurückgegriffen, damit die Unabhängigkeit und ausreichende fachliche Kompetenz gesichert ist. Wird das volle Potenzial solcher Audits ausgeschöpft, wird auch der Datenschutzreifegrad kontinuierlich erhöht. Ein Zertifikat bestätigt die DSGVO-Compliance.

Folgende Fragestellungen werden beantwortet:

- Worauf kommt es beim DSGVO-Audit an?
- Warum sind externe Audits wichtig?
- Wann bzw. wie oft sollte ein Audit stattfinden?
- Wer kann so einen DSGVO-Audit durchführen?

## Die neue Datenschutzgrundverordnung und ihre Umsetzung

**Markus Frank**
(Frank Law)

EU-Datenschutz: die größten Fragezeichen vor der Umsetzung – von hohen Geldbußen bis zu unsicheren Pflichten

Die neue EU-Datenschutz-Grundverordnung wirft für die Unternehmen derzeit fast mehr Fragen auf, als sie Sicherheit gibt. Nationale Ausformungen und die Ausjudizierung bleiben abzuwarten. Jedenfalls werden anerkannte Datenschutz-Zertifizierungen – als ›Sicherheitsnetz‹ – zu einem zentralen Thema der kommenden Jahre. So lautet das Fazit von Wirtschaftsjurist und Rechtsanwalt Dr. Markus Frank, der in seinem Vortrag das jüngste EU-Regelwerk beleuchtet. Extrem hohe Bußgelder bis zu 20 Mio. Euro oder vier Prozent des weltweiten Konzernumsatzes sowie die Tatsache, dass der Schädiger bei Verstößen seine Nicht-Verantwortlichkeit im Sinne der Beweislastumkehr belegen muss, machen aus dem einst zahnlosen Papiertiger ein messerscharfes Datenschutz-Instrument. In seinem Vortrag geht Markus Frank auf wesentliche Neuerungen ein wie: Bestellung eines Datenschutzbeauftragten, Risikoabschätzung oder Datenschutz-Folgeabschätzung insbesondere im Zusammenhang mit sensiblen Mitarbeiterdaten oder Profiling, technische und organisatorische Schutzmaßnahmen wie Verschlüsselung und Pseudonymisierung, Haftungsminimierung und Nachweise durch anerkannte Zertifizierungen u. a.

## Secure Coding

**Ulrich Bayer**
(SBA Research)

Über reine Wissensvermittlung hinaus steht das Schärfen des Sicherheitsbewusstseins in der Softwareentwicklung im Vordergrund. Über welche notwendigen Kenntnisse die Mitarbeiter bei der Prüfung sicherheitsrelevanter Anwendungen verfügen sollten wird anhand von Einblicken in die typische Arbeitsweise von Hackern gewährt, was in modernen Web-Applikationen – lt. OWASP Organisation – die gefährlichsten Sicherheitsschwachstellen sind.

## Referenten

**Dr. Ulrich Bayer** *arbeitet als Senior Security Analyst bei Secure Business Austria und ist dort unter anderem für die Durchführung von Sicherheitsüberprüfungen sowie das Abhalten von Security-Schulungen verantwortlich. Davor arbeitete er als Projektassistent auf der TU Wien und forschte und programmierte auf dem Gebiet der Malware-Analyse. Zudem besitzt er zahlreiche Qualifikationen wie CISSP, Certified Ethical Hacker und CSSPL und ist akkreditierter ÖNORM A7700-Auditor. Er ist auch Mitglied bei Usenix und OCG.*

**Dipl.-Ing. Wolfgang Fiala** *gründete die Fiala Informatik Ziviltechniker GmbH 2003 in Wien. Zu den Schwerpunkten gehören Systemplanungen, Audits, Projektkalkulationen, Prüfung auf Preisangemessenheit, Messungen, Fehlerprüfung etc. sowie zahlreiche Gutachten. In den letzten Jahren ist er schwerpunktmäßig im Public Sector aktiv sowie Mitwirkung bei Ausschreibungen nach BVergG. Er verfügt über umfangreiches Wissen in öffentlichnahen Bereichen (Ministerien, BRZ, Asfinag, etc).*

**Dr. Markus Frank, LLM,** *ist als Rechtsanwalt spezialisiert auf interdisziplinäre Untersuchungen von Schadenursachen bei Wirtschaftsdelikten und Vertragsverletzungen. Vor diesem Hintergrund ist er als Rechtsexperte im Beirat der Zertifizierungsorganisation CIS vertreten und fungiert im Rahmen der CIS-Zertifikatslehrgänge als Trainer für ISO 27001.*

**Daniel Holzinger** *blickt auf rund 20 Jahre Erfahrung in der Informationstechnologie zurück. Er bekleidete internationale Managementpositionen in den Bereichen Vertrieb, Marketing, Public Relations, Partnermanagement und Business Development. Darüber hinaus war er mehrere Jahre als Lektor für Marketing- und Vertriebscontrolling an der FH Wien tätig. Zuletzt war der colited Gründer bei Netviewer/Citrix Online als Geschäftsführer für Österreich und international als Vice President für die Webinar-Strategie verantwortlich.*

**Christian Kurz** *arbeitet seit 2012 für PwC und war davor 7 Jahre in der IT-Beratung und 5 Jahre in der Forschung tätig. Parallel dazu unterrichtet er an Fachhochschule St. Pölten im Masterstudiengang Information Security. Seine fachlichen Schwerpunkte liegen in den Bereichen Computer-Forensik, Electronic Discovery und Untersuchungen im Bereich Cyberforensics. Er ist Certified Cyber Forensic Professional – European Union von (ISC)².*

**Uwe Maurer** *arbeitet als Chief Architect Cyber Defense EMEA bei der Gestaltung von SIEM und SOC Lösungen der NTT Security mit. Er wirkt als Principal Security Consultant daneben in wichtigen Projekten aktiv mit.*

CONECT
BUSINESS ACADEMY

# CISSP (Certified Information Systems Security Professional Training)

**Referenten: Philipp Reisinger** oder **Christoph Falta** (SBA Research)

**Termine: 16.–20. April 2018, 13.–23. November 2018, alle Wien**

- tiefgehende Kenntnisse in Sicherheitskonzepten, Umsetzung und Methodologie
- ISC²
- Entwicklung von Sicherheitsrichtlinien
- Sicherheit in der Softwareentwicklung
- Angriffsarten und die korrespondierenden Gegenmaßnahmen
- kryptographische Konzepte und deren Anwendung
- Notfallplanung und -management
- Risikoanalyse
- forensische Grundlagen

**Teilnahmegebühr:** € 3.000,–, Prüfungsgebühr: € 520,– (Alle Preise +20 % MwSt.)

**Information und Anmeldung: www.conect.at**

CONECT
BUSINESS ACADEMY

# CSSLP (Certified Secure Software Lifecycle Professional)

**Referent: Thomas Konrad** (SBA Research)

**Termine: 16.–20. April 2018, 17.–21. September 2018, alle Wien**

Die TeilnehmerInnen dieses Kurses werden nach Abschluss gut für die CSSLP-Prüfung vorbereitet sein. Unabhängig davon, ob sie die Prüfung nun wirklich ablegen, werden gewonnene Erfahrung und das profunde Wissen für die Sicherheit Ihres gesamten Softwareentwicklungsprozesses von entscheidender Bedeutung sein.

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance and Disposal
- Supply Chain & Software Acquisition

**Teilnahmegebühr:** € 3.000,–; Prüfungsgebühr: € 480,– (Alle Preise + 20 % MwSt.)

**Information und Anmeldung: www.conect.at**

CONECT
BUSINESS ACADEMY

# DSGVO 2018 – praktische Herausforderungen bei der Umsetzung

**Referenten: DI Wolfgang Fiala** (Fiala Informatik Ziviltechniker GmbH), **DI Dr Peter Gelber** (ZT Gelber)

**Termin: 22. März 2018, Wien**

Den Teilnehmern soll ein umfassender Überblick und nötige Hilfestellungen gegeben werden, um für die Umsetzung der DSGVO gerüstet zu sein. Hier werden ausdrücklich keine juristischen Themen behandelt, sondern praktische Aspekte beleuchtet.

- **Startphase**
  Wie startet man das Projekt? Vorbereitung DSMS (Datenschutz-Management-System)
- **Umsetzungsphase**
  Risiko-Analyse, Datenschutz-Folgeabschätzung
  Technisch-Organisatorische Maßnahmen
  DSGVO-Audit
- **Beispiele aus der Praxis**
- **Lfd. Aktivitäten nach dem 25. 5. 2018**
  Kommunikation mit Betroffenen, Workflow und Dokumentation, Statistiken

**Teilnahmegebühr:** € 650,–; Frühbucher: € 590,– (Alle Preise + 20 % MwSt.)

**Information und Anmeldung: www.conect.at**

**An**
**CON•ECT Eventmanagement**
**1070 Wien, Kaiserstraße 14/2**

**Tel.: +43 / 1 / 522 36 36-36**
**Fax: +43 / 1 / 522 36 36-10**
**E-Mail: registration@conect.at**
**http://www.conect.at**

**Zielgruppe: Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand, IT-EntscheiderInnen, IT-Verantwortliche sowie VertreterInnen von Medien und Wissenschaft.**

**ANMELDUNG:** Nach Erhalt Ihrer Anmeldung senden wir Ihnen eine Anmeldebestätigung. Diese Anmeldebestätigung ist für eine Teilnahme am Event erforderlich.

**STORNIERUNG:** Sollten Sie sich für die Veranstaltung anmelden und nicht teilnehmen können, bitten wir um schriftliche Stornierung bis 2 Werktage vor Veranstaltungsbeginn. Danach bzw. bei Nichterscheinen stellen wir eine Bearbeitungsgebühr in Höhe von € 50,– in Rechnung. Selbstverständlich ist die Nennung eines Ersatzteilnehmers möglich.

**ADRESSÄNDERUNGEN:** Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

CON•ECT EVENTMANAGEMENT

## Anmeldung

- ☐ Ich melde mich zu »Security: Cybersicherheit und Riskmanagement mit PwC Survey« am 8. 3. 18 kostenfrei an.
- ☐ Ich möchte Zugriff auf die Veranstaltungspapers zu € 99,– (+ 20 % MwSt.)
- ☐ Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

Firma:

Titel: | Vorname:

Nachname:

Funktion:

Straße:

PLZ: | Ort:

Telefon: | Fax:

E-Mail:

Datum: | Unterschrift/Firmenstempel:

● Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.

● Ich bin mit der Zusendung von Veranstaltungsinformationen per E-Mail einverstanden.

(Nichtzutreffendes bitte streichen)

1801D Layout: Gerhard Krill