Gesellschaft
für Informatik

Management von Informationssicherheit auf Level 31

GI-Fachgruppe
Management von Informationssicherheit
(SECMGT)

Gesellschaft
für Informatik

AGENDA

- **Überblick - Die Gesellschaft für Informatik e.V.**
- **Einblick - Der Fachbereich Sicherheit und die Fachgruppe SECMGT**
- **Rückblick – Motivation und bisherige Tätigkeiten**
- **Ausblick - kommende Veranstaltungen der Fachgruppe**
- **Anblick – Einladung, teilzunehmen und/oder mitzumachen**

Gesellschaft
für Informatik

Über die Gesellschaft für Informatik e.V.

- **Informatik leben** – durch Zusammenarbeit in Fachbereichen, -gruppen, Regionalgruppen und vielen Tagungen, Workshops, Social Media Plattformen, etc.
- **Informatik bewerben** – durch aktive Nachwuchsförderung wie den Bundeswettbewerb Informatik, Informatiktage, InformatiCup oder Informatik-Biber
- **Informatik öffentlich machen** – durch das Aufzeigen des Nutzens und die politische Einflussnahme – bildungs- und forschungspolitisch

Gesellschaft
für Informatik

Was ist die GI?

- Eine Gesellschaft zur Förderung der Informatik in allen gesellschaftlichen Bereichen, sei es in **Studium, Ausbildung, Beruf, Lehre oder Forschung**
- Eine Vertretung von Menschen, die sich mit Informatik beschäftigen, sei es in **Anwendung, Forschung, Lehre oder Weiterbildung**
- Ein Netzwerk von über 22.000 Mitgliedern, die sich mit Informatik beschäftigen

Gesellschaft
für Informatik

Woraus besteht die GI?

- Die GI ist eine Gesellschaft von Menschen:
  Persönliche Mitglieder sind Einzelpersonen in allen Altersgruppen und Tätigkeitsfeldern.
- Die GI ist eine Gesellschaft von Firmen:
  Korporative Mitglieder sind Firmen oder Einrichtungen, die sich als Institution zu den Zielen der GI bekannt haben und diese fördern.
- Die GI ist ein lebendiges Netzwerk:
  Assoziierte Mitglieder sind Mitglieder von Schwestergesellschaften und/oder Mitglieder in einer der Fachgruppen.

Gesellschaft
für Informatik

Themen der GI

Unsere Gesellschaft bearbeitet eine Vielfalt von Themen

aus Forschung und Praxis wie z.B.:

- Softwaretechnik, Grundlagen der Informatik, Wirtschafts-informatik, KI, Technische Informatik, Datenbanken, Sicherheit, Datenschutz, Informationssysteme, Automotive IT, Informatik in den Lebenswissenschaften, Recht/ Öffentliche Verwaltung,...

  aber auch: Gesellschaftliche Fragen wie z.B.

- Ethik, Geistiges Eigentum, Arbeitswelt und Ausbildung,..

Gesellschaft
für Informatik

Fachliche Aktivitäten der GI

- Unterstützung der Arbeit unserer Mitglieder in Ausbildung, Lehre, Forschung und Berufstätigkeit durch
  - Tagungen, Fortbildungen und Seminare
  - Seminare durch eigene – spezialisierte – Tochterfirma
  - Veröffentlichung von Fachpublikationen
- Förderung der Weiterentwicklung von Informatik
- Herausgabe von Empfehlungen und Stellungnahmen zu relevanten Informatik-Fragestellungen

Gesellschaft
für Informatik

Gesellschaftspolitische Aktivitäten der GI

- Lobbyarbeit für Informatik in Politik und Wirtschaft
- Mitwirkung im Prozess der politischen Planung und Gesetzgebung informatiknaher Themen
- Positionierung pro Informatik durch Empfehlungen und Stellungnahmen
- Durchsetzung der faktischen Gleichstellung von Frauen in der Informatik

Gesellschaft
für Informatik

Ihr Engagement...

- aktive Mitarbeit in Fach- und Regionalgruppen, den Beiräten und Arbeitsgruppen
- Pflege des fachlichen und menschlichen Austauschs
- Nutzung der Fortbildungsangebote
- Netzwerken

Gesellschaft
für Informatik

...in einer vielgestaltigen Community

- Weltweit/Europa, z.B.

  CEPIS, IFIP, ACM, IEEE/CS, OCG, SI, I-12...

- Deutschland, z.B.

  BWINF, CERT-IT, DGRI, DIA, DLGI, FIZ Karlsruhe, GIL, Leibniz-Zentrum für Informatik (Schloss Dagstuhl), VDE ITG,…

Gesellschaft
für Informatik

Angebote und Vorteile

- für Vernetzung und lebenslanges Lernen,
- speziell für Studierende,
- fachliche und auch nicht-fachliche Angebote

auf www.gi.de/service/

Gesellschaft
für Informatik

AGENDA

- Überblick - Die Gesellschaft für Informatik e.V.
- **Einblick - Der Fachbereich Sicherheit und die Fachgruppe SECMGT**
- Rückblick – Motivation und bisherige Tätigkeiten
- Ausblick - kommende Veranstaltungen der Fachgruppe
- Anblick – Einladung, teilzunehmen und/oder mitzumachen

Gesellschaft
für Informatik

Vorstellung des Fachbereichs Sicherheit

Der GI-Fachbereich Sicherheit – Schutz und Zuverlässigkeit

Die inhaltliche Arbeit erfolgt in den Fachgruppen

- ADA – Zuverlässige Software-Systeme
- BIOSIG – Biometrik und elektronische Signaturen
- ECOM – E-Commerce, E-Government und Sicherheit
- ENCRESS – Zuverlässigkeit und Sicherheit softwarebasierter Systeme
- EZQN – Evaluation, Zertifizierung, Qualitätssicherung, Normung
- FERS – Fehlertolerierende Rechensysteme
- FoMSESS – Formale Methoden und Software Engineering für Sichere Systeme
- KRYPTO – Angewandte Kryptologie
- NETSEC – Sicherheit in Mobil- und Festnetzen
- PET – Datenschutzfördernde Technik (Privacy Enhancing Technologies)
- **SECMGT – Management von Informationssicherheit**
- SIDAR – Erkennen und Beherrschen von Vorfällen der Informationssicherheit

Gesellschaft
für Informatik

Vorstellung der GI-FG SECMGT

Die GI-Fachgruppe Management von Informationssicherheit

- bietet den im Bereich des Managements von Informationssicherheit tätigen Personen eine *neutrale Plattform*, um sich miteinander zu vernetzen sowie *Wissen und Erfahrungen auszutauschen*.
- ist Teil der Gesellschaft für Informatik e.V., Fachbereich Sicherheit
- vertritt praxisorientierte Themen zu Management, Konzeption, Betrieb und Fortentwicklung von Informationssicherheit
- veranstaltet mehrere Workshops pro Jahr (auch Nichtmitglieder sind stets willkommen); durch Teilnahme können CPEs erworben werden
- ist erreichbar unter www.fg-secmgt.gi.de (dort sind auch die Folien zu den Workshops downloadbar)

Gesellschaft
für Informatik

Leitungsgremium der Fachgruppe

Folgende Personen sind aktuell im **LG der GI-FG SECMGT**:

- Peer Reymann (ITQS GmbH) als Sprecher
- Bernhard C. Witt (it.sec GmbH & Co. KG) als Stellvertreter
- Dr. Frank Damm (DB Systel GmbH)
- Ingrid Dubois (dubois it-consulting gmbh)
- Prof. Dr. Dirk Koschützki (Hochschule Furtwangen)
- Kirsten Messer-Schmidt (excepture)
- Isabel Münch (Bundesamt für Sicherheit in der Informationstechnik)
- Claus Stark (Citigroup Global Markets Deutschland AG)
- Dr. Jörn Voßbein (UIMC Dr. Vossbein GmbH & Co KG)

Gesellschaft
für Informatik

Arbeitskreise und Kooperationen

- Arbeitskreis kritischen Informations- und Kommunikationsinfrastrukturen (**AK KRITIS)**
- Dauerhafte **Kooperationen** mit
  - D-A-CH Security → SECMGT-Workshop auf jährlicher Tagung
  - CAST e.V. → gemeinsamer Workshop zur Enterprise Security
  - GI-FG PET → gemeinsamer Workshop auf GI-Jahrestagungen

Gesellschaft
für Informatik

Veranstaltungen der GI-FG SECMGT 2011

Datum	Thema	Ort
25.02.2011	Data Leakage	Frankfurt/Main
10.06.2011	Management von Informationssicherheit kritischer Infrastrukturen	Frankfurt/Main
06.10.2011	Sicherheitsmanagement und Datenschutz in Anwendung und Praxis (GI-Jahrestagung 2011; m. GI-FG PET)	Berlin
11.11.2011	Outsourcing und Vendor Security	Frankfurt/Main
12.11.2011	AG KRITIS – Interessenskonflikte im Kontext kritischer Infrastrukturen (FIfF-Jahrestagung 2011)	München

Gesellschaft
für Informatik

Veranstaltungen der GI-FG SECMGT 2012

Datum	Thema	Ort
27.01.2012	*AK KRITIS*	*Karlsruhe*
03.02.2012	Praxis-Probleme und Erfahrungen zur Informationssicherheit	Frankfurt/Main
20.04.2012	*AK KRITIS*	*Frankfurt/Main*
15.06.2012	Digitale Identitäten / Identitätsmanagement	Frankfurt/Main
27.07.2012	*AK KRITIS*	*Wiesbaden*
17.09.2012	Sicherheit, Datenschutz, Management und Interoperabilität medizinischer Daten (GI-Jahrestagung 2012; m. GI-FG PET & GMDS-AG DGI)	Braunschweig
26.09.2012	Ganzheitliches Management von Informationssicherheit (D-A-CH Security 2012)	Konstanz
19.10.2012	*AK KRITIS*	*Frankfurt/Main*
09.11.2012	Organisatorische Sicherheit – Zur Rolle des CISO / IT-Sicherheitsbeauftragten	Frankfurt/Main

Gesellschaft
für Informatik

Veranstaltungen der GI-FG SECMGT 2013

Datum	Thema	Ort
25.01.2013	*AK KRITIS*	*Frankfurt/Main*
28.02.2013	Enterprise Security im Wandel der Zeit: das Risikomanagement (CAST-Forum; m. CAST)	Darmstadt
19.04.2013	*AK KRITIS*	*Bonn*
07.06.2013	Wert von Zertifizierungen	Frankfurt/Main
14.06.2013	Cyber Security Normung (m. DIN & GI-FGn EZQN + FoMSESS)	Berlin
26.07.2013	*AK KRITIS*	*Frankfurt/Main*
18.09.2013	Management von Informationssicherheit für KMUs (D-A-CH Security 2013)	Nürnberg
11.10.2013	*AK KRITIS*	Bonn
08.11.2013	Sicherheitsmanagement für mobile Geräte	Frankfurt/Main

Gesellschaft
für Informatik

Veranstaltungen der GI-FG SECMGT 2014

Datum	Thema	Ort
07.02.2014	*AK KRITIS*	Bonn
10.04.2014	Enterprise Security - Kennzahlen und Indikatoren zur Steuerung von Management Systemen (CAST-Forum; m. CAST)	Darmstadt
25.04.2014	*AK KRITIS*	Bonn
09.05.2014	Lessons Learnt? Informationssicherheit in Zeiten staatlicher Überwachung	Frankfurt/Main
04.07.2014	*AK KRITIS*	Bonn
17.09.2014	Ganzheitliches Management von Informationssicherheit (D-A-CH Security 2014)	Graz
26.09.2014	Risikokommunikation im Kontext von IT-Sicherheit und Safety (GI-Jahrestagung 2014; m. GI-FG ECOM)	Stuttgart
17.10.2014	*AK KRITIS*	*Wettenberg*
28.11.2014	Neuerungen und Anpassungen rund um ISO/IEC 27001:2013	Frankfurt/Main

Gesellschaft
für Informatik

AK KRITIS Steckbrief

++++ 2011 Die GI-Fachgruppe SECMGT gründet einen Arbeitskreis zu kritischen Informations- und Kommunikationsinfrastrukturen (AK KRITIS). ++++ Der AK wird durch ein eigenes Leitungsgremium gesteuert. ++++ 2012 Der AK wählt sein erstes Leitungsgremium und nimmt die Arbeit auf. ++++ Seit Anfang 2012 finden alle drei Monate Experten-Workshops zur Bearbeitung von KRITIS-relevanten Themen statt. ++++

Leitungsgremium 2014:

- Sprecherin: Kirsten Messer-Schmidt, *excepture*
- Stellv. Sprecher: Klaus Kirst, *PTLV Hessen*
- Dr. Heinrich Seebauer, *Dr. Seebauer ITC*
- Dr. Steffen Wendzel, *Fraunhofer FKIE*
- Michael Wiesner, *CTNS Security GmbH*

Gesellschaft
für Informatik

AK KRITIS: Ziel, Inhalte, Beteiligte

Ziel: Beschäftigung mit Anforderungen, Vorgehensweisen im Umgang mit kritischen ITK-Infrastrukturen unter Einbezug praktischer Erfahrungen

Arbeitsinhalte: Entwicklung von Methoden und Verfahren, die IT-Entscheidern, Technologen und Fachabteilungen bei der Identifikation kritischer ITK-Systeme und der Einschätzung von ITK-Kritikalität helfen sollen.

Schwerpunkt der laufenden Workshops: Konzeption eines Vorgehensmodells (für KMU) zur Vorbereitung, Planung, Entwicklung und Betrieb kritischer Informations- und Kommunikationstechnologie

Beteiligte: engagierte Vertreter aus Wirtschaft, Beratung, Behörden und Forschungsinstituten

Gesellschaft
für Informatik

AK KRITIS: Austausch und Kontakt

Aufgrund der Komplexität des Themas sind Vernetzung und Austausch mit anderen Gremien, Arbeitskreisen, betroffenen Unternehmen oder sonstigen Interessensvertretern im KRITIS-Umfeld jederzeit herzlich willkommen.

Wenn Sie als Experte Interesse an der Arbeit des AK KRITIS haben oder an unserer Fachdiskussion teilnehmen möchten, nehmen Sie bitte Kontakt auf über: info-ak-kritis@secmgt.de.

Informationen über die Inhalte vergangener und geplanter Workshops finden Sie auf der Webseite der Fachgruppe „Management für Informationssicherheit.

Gesellschaft
für Informatik

AGENDA

- Überblick - Die Gesellschaft für Informatik e.V.
- Einblick - Der Fachbereich Sicherheit und die Fachgruppe SECMGT
- **Rückblick – Motivation und bisherige Tätigkeiten**
- Ausblick - kommende Veranstaltungen der Fachgruppe
- Anblick – Einladung, teilzunehmen und/oder mitzumachen

Gesellschaft
für Informatik

Motivation für Informationssicherheit

- Einhalten von Gesetzen, Vorschriften und Verträgen
- Erfüllen von Anforderungen (und Erwartungen) von Internen und Externen
- Schützen vor Gefahren und Angriffen
- Vermeiden von Schäden
- Nutzen von Potentialen zur Optimierung

Gesellschaft
für Informatik

Ziele von Informationssicherheit

- Compliance – Erfüllen von Anforderungen
- Zufriedenheit – von Bürgern, Geschäftspartnern und Mitarbeitern
- Angemessenen Schutz – **Vertraulichkeit, Integrität, Verfügbarkeit**
- Effizienz – Verbessern der Prozesse
- Vorteile auf dem Markt – bei Kunden und Lieferanten
- …

Informationssicherheit – Themen/Stichworte

- Organisation: CISO/(IT-)Sicherheitsbeauftragter, Haftungsrisiken, ...
- Praxisprobleme: Identitätsmanagement, Mobile Geräte, Passworte, ...
- Katastrophenvorsorge: BCM, Schutz kritischer Infrastrukturen, LüKEx, ...
- Standards: BSI IT-Grundschutz, ISO/IEC 27001, CObIT, ITIL, ...
- Juristische Bedeutung: Data Leakage, Datenschutz, Jahresabschlussprüfung, ...
- Risiko-Management: Methoden, Herausforderungen, Tools, ...
- IT-Governance: Outsourcing, Vendor Security, Cloud Services, ...
- Schulung: Awareness, Social Engineering, Personenzertifizierung, ...
- Effizienz und Effektivität: Wirksamkeit von Maßnahmen, Rentabilität, ...
- Zertifizierung: Durchführung, Wert von Zertifizierung, Datenschutz-Audits, ...
- Neues, Aktuelles, Änderungen: NSA-Skandal, Datenschutzreform, ...
- ...

Gesellschaft
für Informatik

AGENDA

- Überblick - Die Gesellschaft für Informatik e.V.
- Einblick - Der Fachbereich Sicherheit und die Fachgruppe SECMGT
- Rückblick – Motivation und bisherige Tätigkeiten
- **Ausblick - kommende Veranstaltungen der Fachgruppe**
- Anblick – Einladung, teilzunehmen und/oder mitzumachen

Gesellschaft
für Informatik

Nächste Veranstaltung der Fachgruppe

Freitag, 28.11.2014 ab 10:15 in Frankfurt am Main

Thema: **Neuerungen und Anpassungen rund um ISO/IEC 27001:2013**

- Was hat sich geändert? Was ist bei einem Wechsel zu beachten?
- Praxisbericht einer zertifizierten Organisation
- Aufgaben und Aufwände aus Sicht einer Zertifizierungsstelle
- Erfahrungsbericht eines Auditors

Gesellschaft
für Informatik

Wesentliche Neuerungen und Änderungen im Standard

- Standard umgeschrieben (Aufbau nun in Anlehnung an ISO Direktive, Annex SL)
- stärkerer Fokus auf die Integration von Informationssicherheit in die Unternehmensprozesse und Festlegen von ISMS-Zielen
- Plan-Do-Check-Act nicht mehr im Standard (aber immer noch relevant)
- Definitionen wichtiger Fachbegriffe nur noch in ISO/IEC 27000:2014
- Fokus auf externe und interne Belange
  - Verständnis der Organisation und ihres Kontexts
  - Verständnis der Bedürfnisse und Erwartungen interessierter Parteien
- Vorgaben für Risikobewertung und –behandlung sind weniger strikt
- Risikobewertung fokussiert nun auf Informationen (nicht mehr Assets)
- Wirksamkeitsbewertung beschränkt sich nicht auf Maßnahmen
- Annex A wurde komplett überarbeitet

Wesentliche Anforderungen an ein ISMS (Kap. 4-10)

- **Kontext der Organisation**
  Externe und interne Einflussfaktoren ermitteln, Scope
- **Führung**
  Führung, Leitlinie, organisatorische Zuständigkeiten/Befugnisse
- **Planung**
  Maßnahmen zum Umgang mit Risiken und Chancen, Informationssicherheitsziele
- **Unterstützung**
  Ressourcen, Kompetenz, Awareness, Kommunikation, Dokumentierte Information
- **Betrieb**
  Einsatzplanung und –kontrolle, Risikoeinschätzung und –behandlung
- **Leistungsauswertung**
  Überwachen, Messen, Auswerten, interne Audits, Bewertung durch das Management
- **Verbesserung**
  Fehler- und Korrekturmaßnahmen, fortlaufende Verbesserung

Wesentliche Neuerungen und Änderungen: Anhang A

ISO/IEC 27001:2013: 14 Bereiche, 114 Maßnahmen (bisher in ISO/IEC 27001:2005: 11 Bereiche, 133 Maßnahmen)

- **neue Kapitel, Bereiche und Maßnahmen**
  - **A.6.1.5 Informationssicherheit im Projektmanagement**
  - **A.12.6.2 Beschränkungen der Software-Installation**
  - **A.14.2.1 Leitlinie für die sichere Entwicklung von Software und Systemen**
  - **A.14.2.5 Grundsätze für sicheres Systemengineering**
  - **A.14.2.6 Sichere Entwicklungsumgebung**
  - **A.14.2.8 Systemsicherheitsprüfungen**
  - **A.15 Lieferantenbeziehungen**
  - **A.15.1.1 Informationssicherheitsleitlinie für Lieferantenbeziehungen**
  - **A.15.1.3 IKT-Lieferkette (Anforderungen für den Umgang mit Risiken)**
  - **A.16.1.4 Bewertung und Einstufung von Informationssicherheitsereignissen**
  - **A.16.1.5 Reaktion auf Informationssicherheitsvorfälle**
  - **A.17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen**

Gesellschaft
für Informatik

Wesentliche Neuerungen und Änderungen: Anhang A

- **Wesentliche Änderungen**
  - **A.6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten**
  - **A.8.2.2 Kennzeichnen von Informationen**
  - **A.8.2.3 Handhabung von Werten (Handling of assets)**
  - **A.9.2 Benutzerzugriffsverwaltung (User access management)**
  - **A.9.4.2 Sichere Anmeldeverfahren (Secure log-on procedures)**
  - **A.12.1.2 Änderungssteuerung (Change management)**
  - **A.12.2.1 Maßnahmen gegen Schadsoftware (Controls against malware)**
  - **A.12.4.1 Ereignisprotokollierung (Event logging)**
  - **A.12.4.3 Administrator- und Betreiberprotokolle (Administrator and operator logs)**
  - **A.14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzen**
  - **A.14.2.8 Systemsicherheitsprüfungen (System security testing)**
  - **A.14.2.9 Systemabnahmeprüfung**
  - **A.16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen**
  - **A.17.1.1 Planung der Kontinuität der Informationssicherheit**
  - **A.17.1.2 Implementieren der Kontinuität der Informationssicherheit**

Auswirkungen hinsichtlich Zertifizierung / Zertifikaten

- **Auditoren müssen Qualifizierung für 2013er Version nachweisen**
- **Übergangszeiten für eine bestehende Zertifizierung**
  Umstellung bis spätestens 31.09.2015 abgeschlossen (sonst Neu-Zertifizierung)
- **Transition / Umstellung**
  - **Überprüfung im Rahmen eines Audits notwendig (Transition Audit)**
    im Rahmen eines der anstehenden Audits oder in extra beauftragtem Audit
  - **Bis Ende der Umstellungsfrist müssen alle Abweichungen, die aufgrund der geänderten Anforderungen festgestellt werden, behoben sein.**
  - **Empfehlungen**
    - **Transition-Audit bis spätestens in Q2/2015 durchführen.**
      Die Zertifizierungsstellen müssen den Bericht zur Umstellung prüfen. Bei Erfolg wird ein Zertifikat für die 2013er-Version erteilt.
    - **Ggf. eingeschränkte Verfügbarkeit der Auditoren berücksichtigen**
      erhöhte Nachfrage nach Audits möglich, da alle Zertifikatsinhaber umstellen müssen oder das bestehende Zertifikat nach Ablauf der Umstellungsfrist automatisch ungültig wird

Gesellschaft
für Informatik

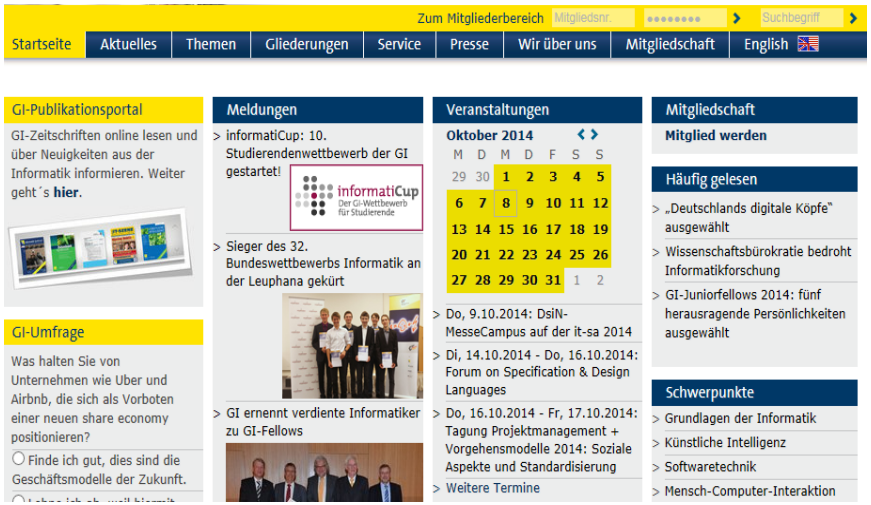
AGENDA

- Überblick - Die Gesellschaft für Informatik e.V.
- Einblick - Der Fachbereich Sicherheit und die Fachgruppe SECMGT
- Rückblick – Motivation und bisherige Tätigkeiten
- Ausblick - kommende Veranstaltungen der Fachgruppe
- **Anblick – Einladung, teilzunehmen und/oder mitzumachen**

Informieren, Teilnehmen, Mitmachen

Im Internet

- www.gi.de
- http://fg-secmgt.gi.de/



E-Mail Verteilerliste / Mailingliste

- https://mail.gi-fb-sicherheit.de/.

Persönlich

- jetzt und hier während der it-sa
- 28.11.2014 in Frankfurt, Workshop zu ISO/IEC 27001:2013
- bei einer der für 2015 geplanten Veranstaltungen (Wirksamkeit, Cyber-??, Privacy, o.ä.)

Gesellschaft
für Informatik

Management von
Informationssicherheit auf Level 31

GI-Fachgruppe
Management von Informationssicherheit
(SECMGT)