Gesprächsprotokoll 38. Sitzung des CMG Themenpanels „Sicherheit Sensibler Systeme“ am Montag 10.9.2020 als Zoom Online Meeting.

Dabei waren: Dominique Meixner, Roland Pucher, René Pfeiffer, Hermann Bühler, Uwe Schimon, Jürgen Schmid, Christian Ungerböck, Evangelos Lianos, Manfred Wöhrl, Michael Wagner, Andreas Schuster

Unsere Agenda für den 10.9.2020

- Fachvortrag "Whistleblowing - Praktische Tipps zur Einführung von Hinweisgebersystemen", Roland Pucher, BDO
- Erfahrungsaustausch – aktuelle Bedrohungen – EU-Kommission: Ende der Ende-zu-Ende Verschlüsselung?
- Letzte Abstimmung zum Draft: CMG Leitfaden "Sichere Softwareentwicklung - Secure Coding und Design"
- Arbeiten an der Agenda für unseren Event am Dienstag den 20. Oktober 2020

1. Wissenstransfer "Whistleblowing - Praktische Tipps zur Einführung von Hinweisgebersystemen", Dominique Meixner und Roland Pucher, BDO

Vorstellung Dominique Meixner:

Dominique Meixner ist seit 2013 im Bereich Governance, Risk & Compliance tätig und begleitete in dieser Zeit eine Vielzahl verschiedener Projekte im In- und Ausland. Sie leitet den Fachbereich Forensic Services bei BDO Austria und unterstützt Kunden bei der Durchführung von forensischen Sonderuntersuchungen sowie bei der Aufklärung von wirtschaftskriminellen Handlungen. Zudem ist sie auf die Präventionsberatung zur Vermeidung doloser Handlungen und auf die Überprüfung compliancerelevanter Geschäftsprozesse spezialisiert.

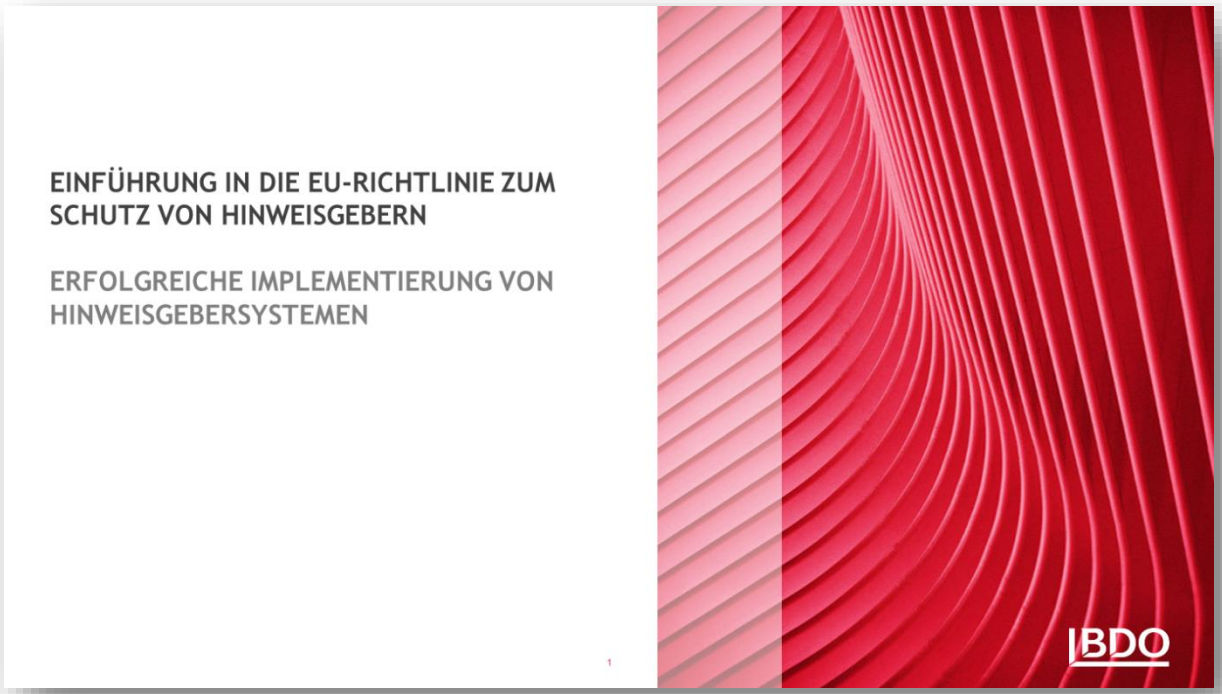
Dominique Meixner berichtet über die EU Richtlinie 2019/1939 vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. Die Richtlinie ist veröffentlicht und unter dem folgenden Link einsehbar: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L1937&from=en

Aus der Richtlinie:

> Personen, die für eine öffentliche oder private Organisation arbeiten oder im Rahmen ihrer beruflichen Tätigkeiten mit einer solchen Organisation in Kontakt stehen, nehmen eine in diesem Zusammenhang auftretende Gefährdung oder Schädigung des öffentlichen Interesses häufig als Erste wahr. Indem sie Verstöße gegen das Unionsrecht melden, die das öffentliche Interesse beeinträchtigen, handeln diese Personen als Hinweisgeber und tragen entscheidend dazu bei, solche Verstöße aufzudecken und zu unterbinden. Allerdings schrecken potenzielle Hinweisgeber aus Angst vor Repressalien häufig davor zurück, ihre Bedenken oder ihren Verdacht zu melden. In diesem Zusammenhang wird sowohl auf Unionsebene als auch auf internationaler Ebene zunehmend anerkannt, dass es eines ausgewogenen und effizienten Hinweisgeberschutzes bedarf.

Dominique Meixner erklärt, dass es bei der Richtlinie primär um den Schutz von Personen geht, Hinweise geben und Verstöße aufdecken. Wobei es bei den aufzudeckenden Verstößen immer um den Firmenkontext geht.

Vortragsfolien



STATUS QUO ZUM THEMA WHISTLEBLOWING

BUSINESS INSIDER

HOME » WIRTSCHAFT » FINANZEN » WIRECARD: WHISTLEBLOWER WARNTE SCHON 2019 VOR UNREGELMÄSSIGKEITEN

Wirecard: Whistleblower warnte offenbar schon Anfang 2019, doch die Behörden reagierten nur langsam

Süddeutsche Zeitung

26. April 2016, 07:37 Uhr Antoine Deltour

Lux-Leaks-Whistleblower droht Gefängnisstrafe

Die durch ihn enthüllten Dokumente hatten gezeigt, wie Luxemburg die Steuerflucht für mehr als 300 Unternehmen organisiert hatte.

KURIER

Causa Commerzialbank: Whistleblower verriet Illedits-Geschenk

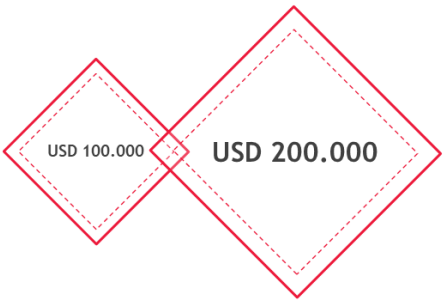
Handelsblatt

ABGASSKANDAL

VW-Whistleblower steckt hinter neuen Enthüllungen

STATUS QUO ZUM THEMA WHISTLEBLOWING

Relevanz von Hinweisgebersystemen



Durchschnittlicher Verlust mit und ohne Möglichkeit zur Meldung*

Hinweise, z.B. von Hinweisgebern, sind mit Abstand die **häufigste Methode**, um dolose Handlungen aufzudecken.

Am häufigsten werden Meldungen von Hinweisgebern via **Telefon, E-Mail oder web-basierten Tools** erstattet.

Möglichkeiten zur Meldung werden oftmals nur **innerhalb des Unternehmens** an Mitarbeiter kommuniziert. Zur Abdeckung eines breiteren Feldes sollte diese Möglichkeit auch an Geschäftspartner kommuniziert werden.

**Quelle: ACFE Report to the Nations 2018, https://www.acfe.com/report-to-the-nations/2018/*

GESETZLICHE GRUNDLAGEN

EU-Richtlinie zum Schutz von Hinweisgebern (Umsetzungsfrist für die Mitgliedstaaten: 17.12.2021)

Hinweisgeber

- Personen, die Informationen über Verstöße im Zusammenhang mit ihren Arbeitstätigkeiten melden bzw. offenlegen

Ausgangssituation

- Keine einheitlichen Regelungen zum Schutz von Hinweisgebern
- Nur wenige Rechtsvorschriften auf EU-Ebene

Ziel

- Festlegung von Mindeststandards, die einen umfassenden Schutz von Hinweisgebern und ihren Unterstützern in der EU sicherstellen

Abhängig von der konkreten Umsetzung des nationalen Gesetzgebers können Ausnahmen bzw. Erweiterungen in der nationalen Gesetzgebung vorgesehen werden. Die Richtlinie legt lediglich die Mindestanforderungen auf EU-Ebene fest.

GESETZLICHE GRUNDLAGEN

EU-Richtlinie zum Schutz von Hinweisgebern (Umsetzungsfrist für die Mitgliedstaaten: 17.12.2021)

Anwendungsbereich

Die EU-Richtlinie zum Schutz von Hinweisgebern legt Mindeststandards für den **Schutz von Personen** fest, die **Verstöße gegen das Unionsrecht**, unter anderem aus den folgenden Bereichen, melden:

- Öffentliches Auftragswesen
- Finanzdienstleistungen, Finanzprodukte und Finanzmärkte
- Verhinderung von Geldwäsche und Terrorismusfinanzierung
- Produktsicherheit und -konformität
- Verkehrssicherheit
- Umweltschutz
- Verbraucherschutz
- Schutz der Privatsphäre und personenbezogener Daten

GESETZLICHE GRUNDLAGEN

EU-Richtlinie zum Schutz von Hinweisgebern (Umsetzungsfrist für die Mitgliedstaaten: 17.12.2021)

Einrichtung eines internen Meldekanals für Hinweisgeber

- Privatrechtliche Unternehmen **ab 50 Mitarbeitern**
- **Alle juristischen Personen des öffentlichen Sektors**, wie z.B. Gemeinden, Landes- und Regionalverwaltungen
- **Ausnahmen** können in der Umsetzung der Richtlinie durch den österreichischen Gesetzgeber vorgesehen werden
- Ausnahme von der allgemeinen Umsetzungsfrist für die Mitgliedstaaten hinsichtlich der Einrichtung interner Meldekanäle für juristische Personen mit **50 bis 249 Arbeitnehmern**: 17.12.2023

Meldemöglichkeiten von Verstößen durch die Hinweisgeber

- **Interner Meldekanal** des privatrechtlichen Unternehmens oder der juristischen Person des öffentlichen Sektors
- **Externer Meldekanal** von Behörden, die von den EU-Mitgliedstaaten zu bestimmen sind
- **Offenlegung** direkt an die Öffentlichkeit bzw. Medien unter bestimmten Voraussetzungen

Voraussetzungen für den internen Meldekanal

- Meldungen müssen entweder **schriftlich** (z.B. webbasiertes System) oder **mündlich** eingebracht werden können
- **Schutz der Identität des Hinweisgebers** (keine verpflichtende Anonymität, aber empfohlen)
- **Eingangsbestätigung** der Meldung und **Information** über getroffene Maßnahmen (innerhalb einer bestimmten Frist)
- **Zusätzliche Voraussetzungen** für die Handhabung von Meldungen (z.B. Benennung einer unparteiischen Person oder Abteilung)

GESETZLICHE GRUNDLAGEN

EU-Richtlinie zum Schutz von Hinweisgebern (Umsetzungsfrist für die Mitgliedstaaten: 17.12.2021)

Geschützte Personen

- Die Richtlinie schützt unter anderem die folgenden Personen aus dem **privaten und öffentlichen Sektor**, die im **beruflichen Kontext** Informationen über Verstöße erlangt haben:
  - Arbeitnehmer
  - Beamte
  - Selbstständige
  - Anteilseigner sowie Verwaltungs-, Leitungs- und Aufsichtsorgane und nicht geschäftsführende Mitglieder
  - Freiwillige
  - Praktikanten
  - Auftragnehmer und Zulieferer
  - Ehemalige Arbeitnehmer und Bewerber
  - Mittler

Schutz vor Repressalien

- Hinweisgeber müssen unter anderem vor den folgenden **Repressalien** sowie vor der **Androhung** und dem **Versuch** dieser geschützt werden:
  - Suspendierung, Kündigung
  - Herabstufung oder Versagung einer Beförderung
  - Aufgabenverlagerung, Änderung des Arbeitsortes, Gehaltsminderung, Änderung der Arbeitszeit
  - Versagung der Teilnahme an Weiterbildungsmaßnahmen
  - negative Leistungsbeurteilung oder Ausstellung eines schlechten Arbeitszeugnisses
  - Disziplinarmaßnahme, Rüge oder sonstige Sanktion einschließlich finanzieller Sanktionen
  - Nötigung, Einschüchterung, Mobbing oder Ausgrenzung
  - Diskriminierung
  - Vorzeitige Kündigung oder Aufhebung eines Vertrags über Waren oder Dienstleistungen

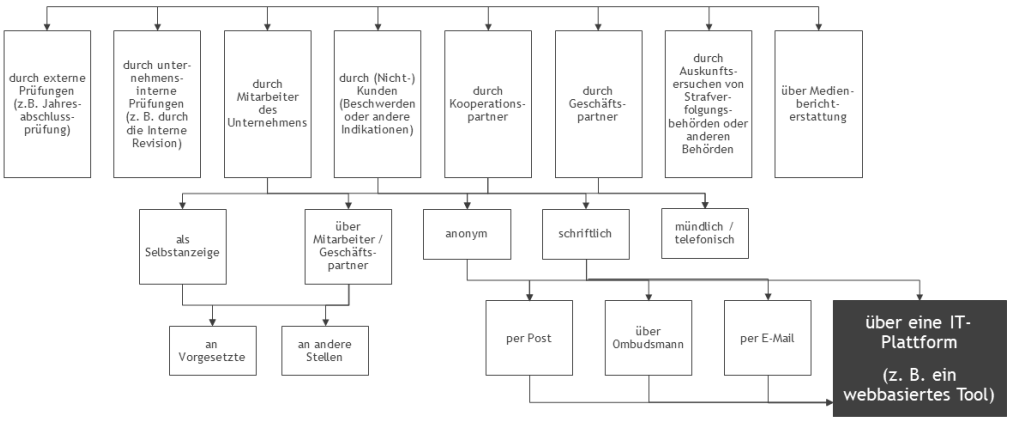
EINFÜHRUNG IN DIE EU-RICHTLINIE ZUM SCHUTZ VON HINWEISGEBERN

ERFOLGREICHE IMPLEMENTIERUNG VON HINWEISGEBERSYSTEMEN

MELDEKANÄLE UND VERFAHREN

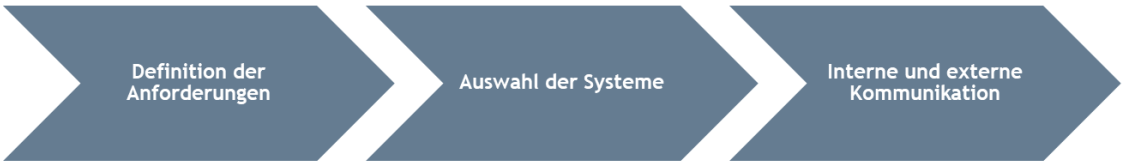
Meldekanäle für Informationen und Hinweise auf Unregelmäßigkeiten

- Informationen, die ein Unternehmen über Unregelmäßigkeiten erhält, können über verschiedene Informationskanäle empfangen werden:



IMPLEMENTIERUNG EINES HINWEISGEBERSYSTEMS

- Die erfolgreiche Implementierung eines Hinweisgebersystems im Unternehmen umfasst im Wesentlichen drei Schritte. Jeder Prozessschritt umfasst unterschiedliche Fragestellungen, die essentiell für ein durchdachtes Hinweisgebersystem als Teil des Compliance Management Systems sind.



IMPLEMENTIERUNG EINES HINWEISGEBERSYSTEMS

Definition der Anforderungen

- Bestehende Systeme
- Betreiber des Hinweisgebersystems
- Sprachen
- Stakeholder
- Mögliche Hinweisgeber
- Bearbeitung der Hinweise
- Richtlinien im Unternehmen
- Kommunikationskanäle
- Verstöße
- Rechtliche Anforderungen

IMPLEMENTIERUNG EINES HINWEISGEBERSYSTEMS

Definition der Anforderungen | Auswahl der Systeme | Interne und externe Kommunikation

Auswahl der Systeme

- Prozesse
- Systeme
- Funktionsweise
- Zuständigkeiten

IMPLEMENTIERUNG EINES HINWEISGEBERSYSTEMS

Definition der Anforderungen | Auswahl der Systeme | Interne und externe Kommunikation

Interne und externe Kommunikation

- Kommunikationskanäle innerhalb und außerhalb des Unternehmens
- Relevante Informationen
- Positive Kommunikation des Hinweisgebersystems

KEY FACTS ZU WEBBASIERTEN HINWEISGEBERPLATTFORMEN

IT-Sicherheit und Datenschutz stehen an erster Stelle

Sicherheit & Schutz

Webbasierte Hinweisgeberplattform erfüllen höchste Sicherheitsstandards und gewährleistet die Anonymität der Hinweisgeber.

Die Vertraulichkeit und Integrität der Daten wird durch umfassende Kontrollen sichergestellt.

Durch den Einsatz von redundanten Servern profitieren die Unternehmen von höchster Verfügbarkeit.

Umfassendes Berechtigungskonzept nach dem Need-to-know Prinzip

Regelmäßige ISO 27001 Zertifizierung der IT-Infrastruktur

DSGVO-konformes Datenmanagement

Rechenzentren in der EU, EWG und in Drittstaaten mit angemessenem Schutzniveau

Erfüllung geltender Gesetze und Verordnungen (z.B.: MAR, MiFID, etc.)

Durchführung von Penetration Tests nach OWASP Standards

VORTEILE EINES WEBBASIERTEN HINWEISGEBERSYSTEMS

Mit einer webbasierten Hinweisgeberplattform genießen Sie die folgenden Vorteile

Anonymität

- Hinweisgeber können Meldungen anonym abgeben
- Verschlüsselte Zwei-Wege Kommunikation zwischen dem Hinweisgeber und dem (Compliance-) Verantwortlichen
- Trotz Anonymität kann der Hinweisgeber über den Status informiert werden

Dokumentation

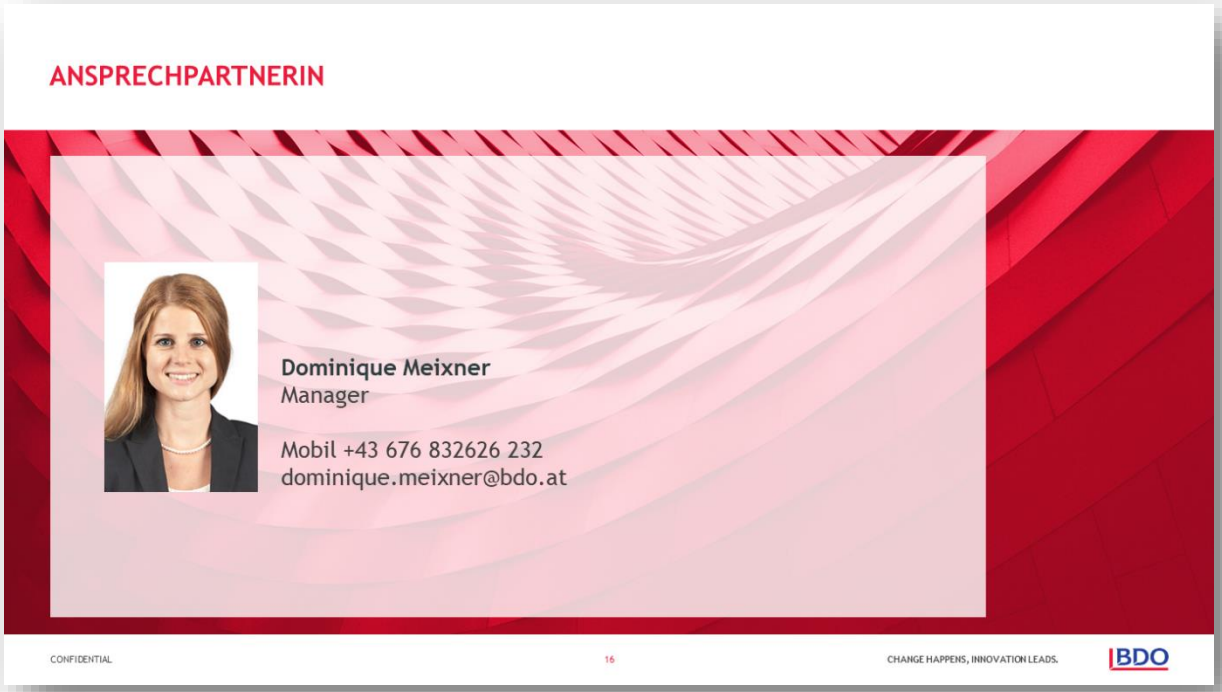
- Meldungen werden innerhalb der Plattform gespeichert
- Umfassende Dokumentation der Fälle
- Möglichkeit zur pseudonymisierten Archivierung
- Möglichkeit zur Erstellung umfassender Compliance-Statistiken (Reporting)

Erreichbarkeit

- Die Plattform ist rund um die Uhr erreichbar (24/7)
- Meldungen können auch außerhalb der Geschäftszeiten abgegeben werden
- Hohe Flexibilität für die Hinweisgeber

Schutz

- Hinweisgebersysteme sind Teil eines funktionsfähigen Compliance Management Systems (CMS)
- Unterstützung bei der Vermeidung bzw. Eindämmung von wirtschaftlichen und rechtlichen Schäden



Frage die geklärt wurden:

Die Richtlinie ist für alle Firmen ab 50 MA verpflichtend. Bis wann die Fristen der Umsetzung gelten kann man erst sagen, wenn das österreichische Gesetz zumindest als Draft existiert. Der ursprüngliche Plan Unternehmen mit 17.12.2021 zu verpflichten ist aufgrund von COVID-19 eventuell aufgeweicht.

Das Gesetz wird für öffentliche Unternehmen und die Privatwirtschaft gelten, die 50 MA überschreiten, jedoch kann es für Unternehmen die kleiner als 250 MA sind eventuell auch eine um rd. 2 Jahre längere Umsetzungsfrist geben. Ebenso können Gemeinden mit unter 10.000 Einwohner ausgenommen werden.

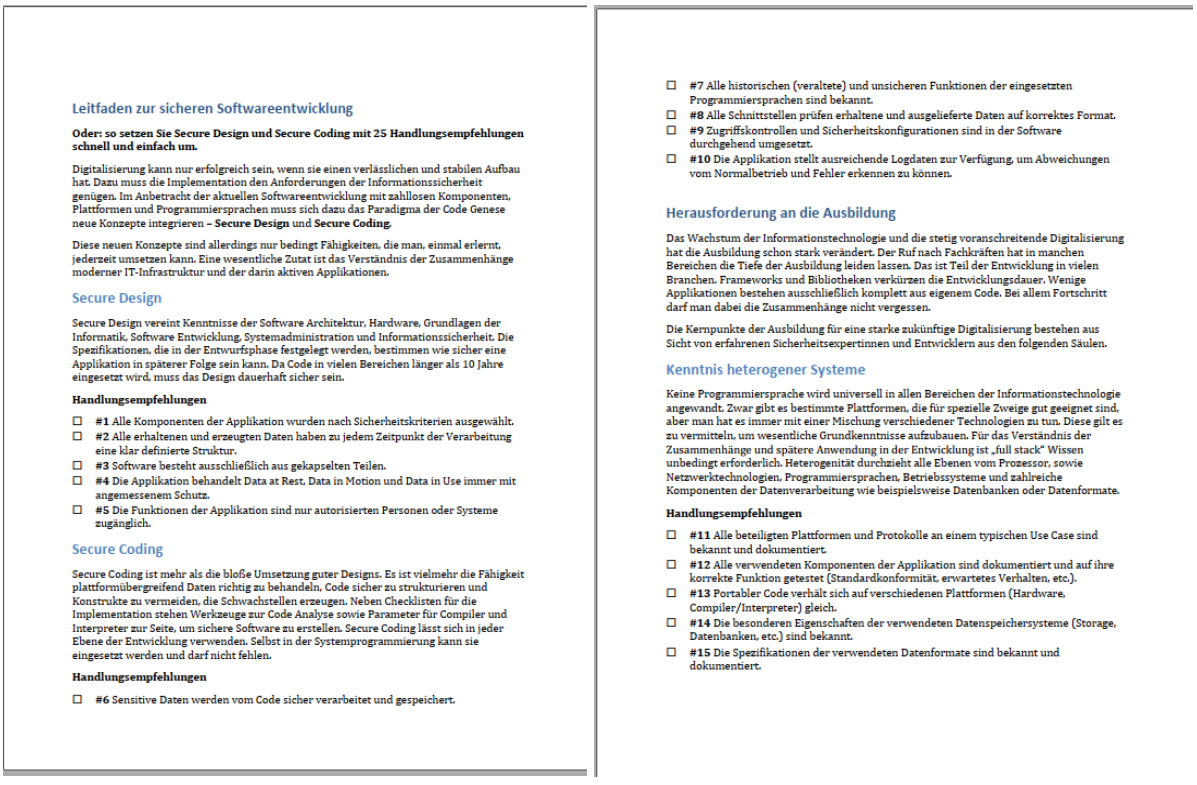
BDO sieht einen erhöhten Handlungsbedarf beim Thema Whistleblowing und berät Unternehmen bei der Umsetzung.

Kontaktdaten:

Mag. Dominique Meixner
Manager, Forensic Services
Tel: +43 676 832626232
Email: dominique.meixner@bdo.at
BDO Consulting GmbH
Gewerbepark Urfahr 6
4040 Linz

2. Letzte Abstimmung zum Draft: CMG Leitfaden "Sichere Softwareentwicklung - Secure Coding und Design"

Aktueller Dokumentenstand:



Leitfaden zur sicheren Softwareentwicklung

Oder: so setzen Sie Secure Design und Secure Coding mit 25 Handlungsempfehlungen schnell und einfach um.

Digitalisierung kann nur erfolgreich sein, wenn sie einen verlässlichen und stabilen Aufbau hat. Dazu muss die Implementation den Anforderungen der Informationssicherheit genügen. Im Anbetracht der aktuellen Softwareentwicklung mit zahllosen Komponenten, Plattformen und Programmiersprachen muss sich dazu das Paradigma der Code Genese neue Konzepte integrieren – **Secure Design** und **Secure Coding**.

Diese neuen Konzepte sind allerdings nur bedingt Fähigkeiten, die man, einmal erlernt, jederzeit umsetzen kann. Eine wesentliche Zutat ist das Verständnis der Zusammenhänge moderner IT-Infrastruktur und der darin aktiven Applikationen.

Secure Design

Secure Design vereint Kenntnisse der Software Architektur, Hardware, Grundlagen der Informatik, Software Entwicklung, Systemadministration und Informationssicherheit. Die Spezifikationen, die in der Entwurfsphase festgelegt werden, bestimmen wie sicher eine Applikation in späterer Folge sein kann. Da Code in vielen Bereichen länger als 10 Jahre eingesetzt wird, muss das Design dauerhaft sicher sein.

Handlungsempfehlungen

- ☐ **#1** Alle Komponenten der Applikation wurden nach Sicherheitskriterien ausgewählt.
- ☐ **#2** Alle erhaltenen und erzeugten Daten haben zu jedem Zeitpunkt der Verarbeitung eine klar definierte Struktur.
- ☐ **#3** Software besteht ausschließlich aus gekapselten Teilen.
- ☐ **#4** Die Applikation behandelt Data at Rest, Data in Motion und Data in Use immer mit angemessenem Schutz.
- ☐ **#5** Die Funktionen der Applikation sind nur autorisierten Personen oder Systeme zugänglich.

Secure Coding

Secure Coding ist mehr als die bloße Umsetzung guter Designs. Es ist vielmehr die Fähigkeit plattformübergreifend Daten richtig zu behandeln, Code sicher zu strukturieren und Konstrukte zu vermeiden, die Schwachstellen erzeugen. Neben Checklisten für die Implementation stehen Werkzeuge zur Code Analyse sowie Parameter für Compiler und Interpreter zur Seite, um sichere Software zu erstellen. Secure Coding lässt sich in jeder Ebene der Entwicklung verwenden. Selbst in der Systemprogrammierung kann sie eingesetzt werden und darf nicht fehlen.

Handlungsempfehlungen

- ☐ **#6** Sensitive Daten werden vom Code sicher verarbeitet und gespeichert.
- ☐ **#7** Alle historischen (veraltete) und unsicheren Funktionen der eingesetzten Programmiersprachen sind bekannt.
- ☐ **#8** Alle Schnittstellen prüfen erhaltene und ausgelieferte Daten auf korrektes Format.
- ☐ **#9** Zugriffskontrollen und Sicherheitskonfigurationen sind in der Software durchgehend umgesetzt.
- ☐ **#10** Die Applikation stellt ausreichende Logdaten zur Verfügung, um Abweichungen vom Normalbetrieb und Fehler erkennen zu können.

Herausforderung an die Ausbildung

Das Wachstum der Informationstechnologie und die stetig voranschreitende Digitalisierung hat die Ausbildung schon stark verändert. Der Ruf nach Fachkräften hat in manchen Bereichen die Tiefe der Ausbildung leiden lassen. Das ist Teil der Entwicklung in vielen Branchen. Frameworks und Bibliotheken verkürzen die Entwicklungsdauer. Wenige Applikationen bestehen ausschließlich komplett aus eigenem Code. Bei allem Fortschritt darf man dabei die Zusammenhänge nicht vergessen.

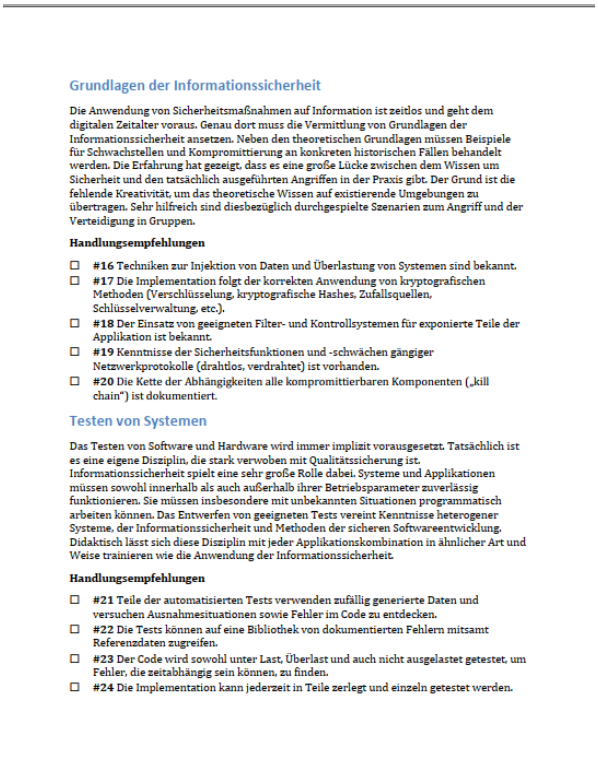
Die Kernpunkte der Ausbildung für eine starke zukünftige Digitalisierung bestehen aus Sicht von erfahrenen Sicherheitsexpertinnen und Entwicklern aus den folgenden Säulen.

Kenntnis heterogener Systeme

Keine Programmiersprache wird universell in allen Bereichen der Informationstechnologie angewandt. Zwar gibt es bestimmte Plattformen, die für spezielle Zweige gut geeignet sind, aber man hat es immer mit einer Mischung verschiedener Technologien zu tun. Diese gilt es zu vermitteln, um wesentliche Grundkenntnisse aufzubauen. Für das Verständnis der Zusammenhänge und spätere Anwendung in der Entwicklung ist „full stack" Wissen unbedingt erforderlich. Heterogenität durchzieht alle Ebenen vom Prozessor, sowie Netzwerktechnologien, Programmiersprachen, Betriebssysteme und zahlreiche Komponenten der Datenverarbeitung wie beispielsweise Datenbanken oder Datenformate.

Handlungsempfehlungen

- ☐ **#11** Alle beteiligten Plattformen und Protokolle an einem typischen Use Case sind bekannt und dokumentiert.
- ☐ **#12** Alle verwendeten Komponenten der Applikation sind dokumentiert und auf ihre korrekte Funktion getestet (Standardkonformität, erwartetes Verhalten, etc.).
- ☐ **#13** Portabler Code verhält sich auf verschiedenen Plattformen (Hardware, Compiler/Interpreter) gleich.
- ☐ **#14** Die besonderen Eigenschaften der verwendeten Datenspeichersysteme (Storage, Datenbanken, etc.) sind bekannt.
- ☐ **#15** Die Spezifikationen der verwendeten Datenformate sind bekannt und dokumentiert.



Grundlagen der Informationssicherheit

Die Anwendung von Sicherheitsmaßnahmen auf Information ist zeitlos und geht dem digitalen Zeitalter voraus. Genau dort muss die Vermittlung von Grundlagen der Informationssicherheit ansetzen. Neben den theoretischen Grundlagen müssen Beispiele für Schwachstellen und Kompromittierung an konkreten historischen Fällen behandelt werden. Die Erfahrung hat gezeigt, dass es eine große Lücke zwischen dem Wissen um Sicherheit und den tatsächlich ausgeführten Angriffen in der Praxis gibt. Der Grund ist die fehlende Kreativität, um das theoretische Wissen auf existierende Umgebungen zu übertragen. Sehr hilfreich sind diesbezüglich durchgespielte Szenarien zum Angriff und der Verteidigung in Gruppen.

Handlungsempfehlungen

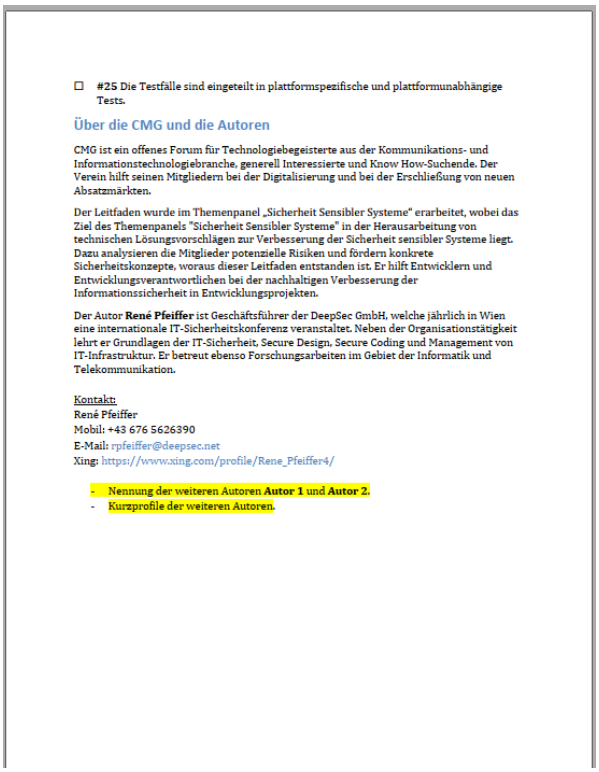
- ☐ **#16** Techniken zur Injektion von Daten und Überlastung von Systemen sind bekannt.
- ☐ **#17** Die Implementation folgt der korrekten Anwendung von kryptografischen Methoden (Verschlüsselung, kryptografische Hashes, Zufallsquellen, Schlüsselverwaltung, etc.).
- ☐ **#18** Der Einsatz von geeigneten Filter- und Kontrollsystemen für exponierte Teile der Applikation ist bekannt.
- ☐ **#19** Kenntnisse der Sicherheitsfunktionen und -schwächen gängiger Netzwerkprotokolle (drahtlos, verdrahtet) ist vorhanden.
- ☐ **#20** Die Kette der Abhängigkeiten alle kompromittierbaren Komponenten („kill chain") ist dokumentiert.

Testen von Systemen

Das Testen von Software und Hardware wird immer implizit vorausgesetzt. Tatsächlich ist es eine eigene Disziplin, die stark verwoben mit Qualitätssicherung ist. Informationssicherheit spielt eine sehr große Rolle dabei. Systeme und Applikationen müssen sowohl innerhalb als auch außerhalb ihrer Betriebsparameter zuverlässig funktionieren. Sie müssen insbesondere mit unbekannten Situationen programmatisch arbeiten können. Das Entwerfen von geeigneten Tests vereint Kenntnisse heterogener Systeme, der Informationssicherheit und Methoden der sicheren Softwareentwicklung. Didaktisch lässt sich diese Disziplin mit jeder Applikationskombination in ähnlicher Art und Weise trainieren wie die Anwendung der Informationssicherheit.

Handlungsempfehlungen

- ☐ **#21** Teile der automatisierten Tests verwenden zufällig generierte Daten und versuchen Ausnahmesituationen sowie Fehler im Code zu entdecken.
- ☐ **#22** Die Tests können auf eine Bibliothek von dokumentierten Fehlern mitsamt Referenzdaten zugreifen.
- ☐ **#23** Der Code wird sowohl unter Last, Überlast und auch nicht ausgelastet getestet, um Fehler, die zeitabhängig sein können, zu finden.
- ☐ **#24** Die Implementation kann jederzeit in Teile zerlegt und einzeln getestet werden.



- ☐ **#25** Die Testfälle sind eingeteilt in plattformspezifische und plattformunabhängige Tests.

Über die CMG und die Autoren

CMG ist ein offenes Forum für Technologiebegeisterte aus der Kommunikations- und Informationstechnologiebranche, generell Interessierte und Know How-Suchende. Der Verein hilft seinen Mitgliedern bei der Digitalisierung und bei der Erschließung von neuen Absatzmärkten.

Der Leitfaden wurde im Themenpanel „Sicherheit Sensibler Systeme" erarbeitet, wobei das Ziel des Themenpanels "Sicherheit Sensibler Systeme" in der Herausarbeitung von technischen Lösungsvorschlägen zur Verbesserung der Sicherheit sensibler Systeme liegt. Dazu analysieren die Mitglieder potenzielle Risiken und fördern konkrete Sicherheitskonzepte, woraus dieser Leitfaden entstanden ist. Er hilft Entwicklern und Entwicklungsverantwortlichen bei der nachhaltigen Verbesserung der Informationssicherheit in Entwicklungsprojekten.

Der Autor **René Pfeiffer** ist Geschäftsführer der DeepSec GmbH, welche jährlich in Wien eine internationale IT-Sicherheitskonferenz veranstaltet. Neben der Organisationstätigkeit lehrt er Grundlagen der IT-Sicherheit, Secure Design, Secure Coding und Management von IT-Infrastruktur. Er betreut ebenso Forschungsarbeiten im Gebiet der Informatik und Telekommunikation.

Kontakt:
René Pfeiffer
Mobil: +43 676 5626390
E-Mail: rpfeiffer@deepsec.net
Xing: https://www.xing.com/profile/Rene_Pfeiffer4/

- Nennung der weiteren Autoren **Autor 1** und **Autor 2**.
- Kurzprofile der weiteren Autoren.

Der Draft des Dokumentes wird mit den Teilnehmern des AK gesichtet und es ergeben sich folgende Rückmeldungen zum Inhalt:

1. **Zu überprüfen ist, ob die kurzfristig kommende ÖVE/ÖNORM 17529 (diese nimmt Einfluss auf europäischer Ebene auf die CE Kennzeichnung) auch in dem Leitfaden berücksichtigt werden soll.**

Einschätzung René Pfeiffer und Andreas Schuster:

> Die ÖVE/ÖNORM 17529 beschäftigt sich mit dem „Datenschutz by Design und als Grundeinstellung" und bietet eine sehr interessante Methodik der Zerlegung von Produkte und Diensten in eine Vielzahl an technischen Produktschichten (Komponenten, Geräte, Betriebssystem, Kommunikation, Speicher, Benutzerschnittstellen, usw.) sowie Diensteschichten (Management, Self-Service, Integration, Übertragungsschickt, Aktualisierung, Client-Dienste, usw.) die man einzeln mit einem Zielerreichungsgrad von A-Z bewerten kann.
>
> Die Norm fokussiert sich jedoch auf den Datenschutz, und unser Leitfaden steht mehr im Licht der Informationssicherheit / IT-Security bei der Softwareentwicklung. Daher werden wir das Thema Datenschutz nicht entsprechend der Norm ausbauen.

2. **Ebenfalls ein Vorschlag ist das Thema RED (Radio Equipped Devices) und IOT mehr einzubringen. Hierzu gibt es eine EU Direktive 2014/53/EU (RED) siehe https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053 die für Radio Equipment gilt und durchaus auch für andere IoT Hardware mit Funkverbindung interessant ist.**

Einschätzung René Pfeiffer und Andreas Schuster:

Die Direktive ist sehr speziell für die Harmonisierung von Radio Equipment entwickelt und wenig für einen Software-Entwickler geeignet, der sich nur in den seltensten Fällen mit einer Funkfrequenz seiner Devices beschäftigt. Daher werden wir diesen Funkt / IoT Aspekt nicht in unserem Leitfaden aufnehmen.

3. **So wie heutige Normen es vorsehen ist die Überlegung ein Managementsystem für die sichere Softwareentwicklung zu betreiben. Hierbei ist sowohl der KVP Prozess der Entwicklung zu berücksichtigen als auch wie die Produkte nach der Markteinführung sicher betrieben und weiterentwickelt werden.**

Einschätzung René Pfeiffer und Andreas Schuster:

Die Nachhaltigkeit der sichern Softwareentwicklung hat im Leitfaden gefehlt, es wurde daher ein Absatz „Softwarepflege und Wartung“ erstellt, der Tipps für eine qualitätsorientierte Produktpflege gibt. Das wir das Ziel von 25 Handlungsempfehlungen für den Leitfaden bereits erreicht haben, hat dieser Abschnitt keine weiteren Handlungsempfehlungen als Checkbox.

3. Erfahrungsaustausch – aktuelle Bedrohungen – EU-Kommission: Ende der Ende-zu-Ende Verschlüsselung?

Aus aktuellem Anlass diskutiert der AK über eine Ankündigung in der die EU-Regulation sich gegen eine sichere Ende-zu-Ende Verschlüsselung positioniert und angekündigt wird, das Kommunikationsmittel mit einer E2E Verschlüsselung zukünftig reguliert werden. Reguliert heißt in diesem Zusammenhang entweder verboten oder mit einem Backdoor für staatliche Stellen ausgerüstet. Hier ein Screenshot der Meldung auf ORF.at:

Im Arbeitskreis haben wir darüber gesprochen, dass ein solches Verbot kriminelle oder terroristische Aktivitäten nicht ausbremsen kann und es zahlreiche inoffizielle Dienste gibt, die keiner Kontrolle

unterliegen. Daher bewerten die Mitglieder des AK diese Ankündigung als Kettenrasseln und nicht als eine akute Bedrohung der Verschlüsselungsdienste.

4. Arbeit an der Agenda für den 22. Oktober Event unseren Themenpanels

Folgender Ideenpool wurde diskutiert:

- Umgang mit Authentisierung und vertraulichen Daten in Home-Office / Office Mischbetrieb. - ??
- Verschlüsselung ist nicht das große Thema
- Mehr die organisatorischen Herausforderungen mit über die Schulter schauen, Besucher, Mithören in öffentlichen Räumen, Regelungen welche Arbeit On-Prem und welche Arbeiten auch im Homeoffice erledigt werden können.
- Auch Drucker und Ausdrucke, dabei auch der unsicher Transport von physischen Informationen in öffentliche Verkehrsmittel.
- Arbeit vom Privatgerät mit Privatdrucker per VDI Session
- Herausforderungen Homeoffice
- Ev. als Ausblick: Cyber Security Act – Regulativa die kommen

Die Fa. BDO hat einen guten Vortrag zum Thema IT und COVID-19 Krise. Diesen werden wir in die den Vormittag einbauen. Danke Roland Pucher von der BDO für deinen Vorschlag!

Im Nachgang zu dem Arbeitskreis wurde gemeinsam mit Irmgard Kollmann folgender Eventtitel und die die Agenda fixiert:

CMG

5. CMG Security KONKRET

zum Thema:

Wie Sie nach der Krise die Kontrolle Ihrer IT zurückgewinnen

ONLINE KONFERENZ

22.Oktober 2020, 9.00 – 12.00 Uhr

Sehr geehrte Damen und Herren,

liebe Mitglieder der CMG!

In vielen Unternehmen wurde im Zuge der COVID-19 Krise die **Informationssicherheit** rasch angepasst und Arbeitsmethoden für **Remote-Zugriff** und **Homeoffic**e adaptiert. Obwohl wir uns alle schnell an die neue Arbeitsweise angepasst haben**,** stellt uns die regelmäßige Heimarbeit vor einen nie dagewesenen Kontrollverlust der IT-Sicherheit.

Speziell im Homeoffice steigende Gefahr von **Computerkriminalität** durch E-Mail-Fälschung oder Telefonbetrug rasant und so muss das **Sicherheitsbewusstsein** aller Mitarbeiter geschärft werden. Zur Prävention von Cyberangriffen müssen aber auch bei der Heimarbeit große **Systemaktualisierungen und Sicherheitsupdates** zügig auf die Clients verteilt werden.

Obwohl uns **Verschlüsselung** und **Cloud-Anwendungen** trotz dezentraler Speicherung helfen die Kontrolle über Daten zu behalten**,** müssen wir auf weitere Krisen durch eine Optimierung unseres **Notfallmanagements** vorbereiten.

In der CMG Veranstaltung präsentieren Experten praxisorientiert wie Unternehmen die Kontrolle über die IT und die Unternehmensdaten zurückerlangen und sich gleichzeitig für die Zukunft rüsten können.

Moderation: Ing. Andreas Schuster, Leiter Themenpanel Sicherheit Sensibler Systeme, CMG

8.45	*Einlaß in den virtuellen Conference Room*
09.00	***Begrüßung*** *Ing. Andreas Schuster, Leiter Themenpanel Sicherheit Sensibler Systeme, CMG*
09.10	***Was tun bei einem Security Incident?*** *Michael Karl, Geschäftsführer, SnapSec GmbH*
9.50	***Security Awareness – The Human Firewall – Schutz in letzter Instanz!*** *Thomas Riedl, Geschäftsführer, R4C GmbH*
10.20	*Bio Break*
10.30	***Cyber Security & Homeoffice – Nach der Krise ist vor der Krise*** *Thomas Simon, Senior Manager und Prokurist, BDO Austria GmbH* *Roland Pucher, Senior Manager-Cyber Security & Digital Forensics, BDO Austria GmbH*
11.00	***Cloud Compliance – Anleitung zur operativen Umsetzung einer sicheren Cloud*** *Dr. Tobias Höllwarth, Executive Partner, Sourcing International GmbH*
11.30	***IT Herausforderungen im COVID-19 Krisenstab – Lessons Learned*** *DI Gerhard Reismüller, Geschäftsführer, BC Consulting GmbH*
12.00	***Zusammenfassung und Ausblick*** *Ing. Andreas Schuster, Leiter Themenpanel Sicherheit Sensibler Systeme, CMG*
12.15	*Ende der Veranstaltung*

5. Organisatorisches

Nächster Termin Do. 15.10 @ 16:00 = 1 Woche vor unserem Security Event.