ISACA EURO CACS 2017 conference Munich (29.-31. Mai 2017)

Review aus der Sicht eines Teilnehmers

Dr. Gregor Kuznik

Table of Content

Cybersecurity Fundamentals Workshop: timeline

Saturday May, 27th / Sunday May, 28th Cybersecurity Fundamentals Workshop

Rolf von Roessing (President, Forfa AG)

08:00 AM - 09:00 AM	*Coffee/tea service* (Saturday starting at 07:30 AM)*
09:00 AM - 10:30 AM	*Session*
10:30 AM - 11:00 AM	*Break*
11:00 AM - 12:30 PM	*Session*
12:30 PM - 13:30 PM	*Lunch*
13:30 PM - 15:00 PM	*Session*
15:00 PM - 15:30 PM	*Break*
15:30 PM - 17:00 PM	*Session*

Cybersecurity Fundamentals Workshop: abstract

"Cyber security is rapidly evolving and spreading to impact every sector of global commerce and technology. As a result, it is more and more crucial that professionals involved in almost all areas of information systems understand the central concepts that frame and define this increasingly pervasive field. The Cybersecurity Fundamentals Workshop is ideal for information systems professionals wishing to advance their knowledge in or transfer to cyber security, and for recent college/university graduates looking to start a career in this in-demand, fiercely competitive field.

The Cybersecurity Fundamentals Workshop is designed to enhance the knowledge of beginning learners and prepare those who wish to obtain a globally recognized credential for the Cybersecurity Fundamentals Certificate Exam which can be taken online at a later date.

This workshop will cover four key areas of cyber security:

- *Cyber security architecture principles*
- *Security of networks, systems, applications and data*
- *Incident response*
- *The security implications of the adoption of emerging technologies."*

Cybersecurity Fundamentals Workshop: goals

"After completing this workshop, you will be able to:

- *Understand basic cyber security concepts and definitions*
- *Define network security architecture concepts*
- *Recognise malware analysis concepts and methodology*
- *Identify computer network defense (CND) and vulnerability assessment tools, including open source tools and their capabilities*
- *Explain network systems management principles, models, methods, and tools*
- *Distinguish system and application security threats and vulnerabilities*
- *Classify types of incidents (categories, responses, and timelines for responses)*
- *Outline disaster recovery and business continuity planning*
- *Comprehend incident response and handling methodologies*
- *Understand security event correlation tools, and how different file types can be used for atypical behavior*
- *Be aware of the basic concepts, practices, tools, tactics, techniques, and procedures for processing digital forensic data*
- *Recognise new and emerging information technology and information security technologies"*

ISACA EURO CACS 2017

Track 1—Audit & Assurance

Track 2—Security/Cyber Security

Track 3—Security/Cyber Security

Track 4—GRC/COBIT

Track 5—Data Analytics & Information Management/Industry Trends & Insights

ISACA EURO CACS 2017

“[Beginner] Beginner
Attendee has limited or no prior knowledge or experience or are new to the subject matter. Beginner sessions are geared toward attendees who are new to the field and seeking to learn basic concepts. Beginner’s sessions are intended to help attendees who seek to build foundational knowledge in an effort to gain a working knowledge of the topic.”

“[Intermediate] Intermediate
Attendee has a working knowledge of the topic covered but is not yet an advanced practitioner. Intermediate sessions are geared toward delegates who have some competence in the subject under discussion resulting from prior training, education and/or work experience. Delegates who seek to build upon foundational knowledge, refine and better hone their skills, and advance their understanding of the topic may wish to consider intermediate-level sessions.“

ISACA EURO CACS 2017

“[Advanced Technical] Advanced Technical
Attendee has a high level of technical understanding of the topic under discussion. Advanced technical sessions are geared toward delegates that have already achieved a high degree of technical competence in the subject of discussion resulting from extensive training in the area and supplemental work experience. Delegates, who wish to build upon intermediate knowledge, achieve mastery in a specific technical area, or build upon existing technical skills may wish to consider advanced technical sessions.”

“[Advanced Managerial] Advanced Managerial
Attendee has a high level of understanding of managerial concepts. Advanced managerial sessions are geared toward attendees that have already achieved a high degree of leadership competence in the subject of discussion resulting from extensive training in the area and several years of work experience. Attendees, who wish to build upon intermediate knowledge, achieve mastery in a specific managerial area, or build upon existing leadership skills may wish to consider advanced managerial sessions.”

ISACA EURO CACS 2017

Monday May, 29th EURO CACS 2017

09:00 AM - 10:00 AM	Opening Session & Keynote: Lessons Learned from Google Dan Cobley	****
10:30 AM - 11:30 AM	112 - Sun Tzu: The Art of War for IT Security Tom Madsen (CISM; IT Specialist, United Nations Development Programs)	****
12:00 PM - 01:00 PM	124 - The Enterprise Immune System Sam Alderman-Miller (Senior Account Manager, Darktrace)	***
02:15 PM - 03:30 PM	133 - The End of Cryptography as We Know It Mike Brown (CTO, ISARA Corporation)	*****
04:00 PM - 05:00 PM	141 - Rational Assessment of Controls Viability Jacques Duret (CISA; Principal - Lifesciences, Antaes SA)	*

ISACA EURO CACS 2017

Tuesday May, 30th EURO CACS 2017 (AM)

08:30 AM - 09:30 AM	214 - Embedding Data Analytics in Fraud Auditing Rolf von Roessing (President, Forfa AG)	*****
10:00 AM - 11:00 AM	223 - Wearable Botnets & Happy Hacked Drivers Andrea Pompili (Cy4GAte)	*****
11:15 AM - 12:15 PM	233 - IoT & AI: New Threats & Mitigations Steve Williamson (CEng)	***

ISACA EURO CACS 2017

Tuesday May, 30th EURO CACS 2017 (PM)

01:30 PM - 02:30 PM	242 - Bridging the Cyber Skills Gap from Within Steve Mair (CISM; Senior Cyber Security Consultant, PGI Cyber)	***
02:45 PM - 03:45 PM	251 - Auditing ITSM Philip Green (CISA, CISM, CRISC; Director, G3 Service Solutions Limited)	*****
04:00 PM - 05:00 PM	263 - The Art of Cyber Risk Management Asaf Weisberg (CEO, introSight)	**
05:15 PM - 05:45 PM	SS1 - Spotlight Session Compliance on Z/OS using Multifactor Authentication Brian Marshall (Vice President, Research & Development, Vanguard)	****
06:30 PM - 09:00 PM	Bavarian Fest Social Event	*****

ISACA EURO CACS 2017

Wednesday May, 31st EURO CACS 2017

08:30 AM - 09:30 AM	312 - Building a "Global Cybersecurity" Framework David Inaneishvili (CISA, CISM, CRISC; Global Director of Information Security, FINCA International)	***
09:45 AM - 10:45 AM	322 - Deep & Dark Web Prof. Claudio Cilli (University of Rome)	****
11:15 AM - 12:30 PM	Closing Keynote Address: Can Technology Solve Everything?	

ISACA EURO CACS 2017

[---] Opening Session & Keynote Lessons Learned from Google

Was die digitale Transformation von Organisationen verlangt.

Wichtigste Erkenntnisse:

- *Seven Recommendations:*
    - *Have a clear, aligned mission*
    - *Give people real autonomy*
    - *Embrace learning through failure*
    - *Use data, kill the hippo*
    - *Be terrifyingly open*
    - *Cannibalize yourself*
    - *Innovate 10x*
- *"Real autonomy" for employees is mandatory*
- *Empowerment and freedom of decision-making is crucial to be successful and "failure" is necessary to learn*

Quellen:

- https://www.isaca.org/Education/Conferences/Documents/2017-CACS-Conference-Report_mkt_eng_0617.pdf

ISACA EURO CACS 2017

[112] Sun Tzu: The Art of War for IT Security

Zeigt Parallelen zwischen den vor 2500 Jahren von Sun Tzu veröffentlichten Überlegungen zur (taktischen) Kriegsführung und der heutigen Strategie für "Cyber War" (Attack & Defense) auf.

Wichtigste Erkenntnisse:

- jeder Angriff ist einzigartig, wobei das Überraschungsmoment entscheidend sein kann
- wer den Feind besiegen will, muss sich selbst richtig (und umfassend) einschätzen (können)
- Fokussierung auf die wichtigen zu schützenden Bereiche ("Kronjuwelen")
- auch Angreifer handeln nur nach Aufwand-Nutzen-Kalkulation
- nicht jeder Angriff kann abgewehrt werden, aber die Kosten für den Angreifer können so hoch getrieben werden, dass der Angreifer andere Ziele vorzieht

Quellen:

- https://www.zenedge.com/blog/the-art-of-cyber-war-sun-tzus-wisdom-still-applies-2500-years-later
- https://blogs.microsoft.com/microsoftsecure/2016/04/11/whats-the-art-of-war-got-to-do-with-cybercrime-quite-a-bit-actually/
- https://www.giac.org/paper/gsec/601/sun-tzu-art-cyber-war-ancient-advice-developing-information-security-program/101438
- https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf
- http://www.envistacom.com/art-war-cybersecurity-take/
- https://www.itnews.com.au/news/sun-tzus-13-lessons-to-combat-hackers-230430/page0

ISACA EURO CACS 2017

[124] The Enterprise Immune System

Selbst-lernende Verteidigung mittels Maschinen-Lernen.

Wichtigste Erkenntnisse:

- bereits bekanntes aus der Art und Weise wie (Groß)Konzerne ihre Infrastruktur bewerten
- keine Präsentation verfügbar

Quellen:

- ---

ISACA EURO CACS 2017

[133] The End of Cryptography as We Know It

Kryptographie ohne Berücksichtigung des Einsatzes von Quantentechnologie hat keine Zukunft. Welche Methoden auch weiterhin hohe Sicherheit gewährleisten können und was es dabei zu berücksichtigen gilt, war Thema dieses Vortrags.

Wichtigste Erkenntnisse:

- heutige Kryptographie basiert auf komplexen mathematischen Gleichungen, deren Ergebnisse nur in einer Richtung mit vertretbarem Zeitaufwand berechnet werden können
- Quantencomputer verändern die Sachlage, da sie in der Lage sind, alle Zustände einer Gleichung gleichzeitig zu berechnen, d.h. die benötigte Rechenzeit sinkt dramatisch
- Lösungen bieten u.a. Hash-basierte Signaturen (z.B. one-time Signaturen oder sehr große private Schlüssel bei minimalen öffentlichen Schlüsseln) oder Merkle-Tree basierte Signaturen oder . . .

Quellen:

- www.isara.com

ISACA EURO CACS 2017

[141] Rational Assessment of Controls Viability

Die Komplexität nimmt stetig zu und damit auch die Kosten der Regulierung.

Wichtigste Erkenntnisse:

- eine Firma ist ein sozio-technologisches System
- die (Anzahl der) stabilen Zustände zu bestimmen, erfordert hohen Aufwand und tiefe Sachkenntnisse, ist aber für eine vernünftige Regulierung unabdingbar
- wenn ein System stabil sein soll, muss die Anzahl stabiler Zustände der Kontrollmechanismen gleich oder größer als die Anzahl Zustände des kontrolllierten Systems sein
- jeder gute Regulator eines System muss ein (vereinfachtes) Modell des Systems sein
- jeder Kontrollmechanismus / Regulierungsprozess muss einem Entwicklungsprozess unterworfen sein und angepasst werden können

Quellen:

- http://supply-chain-mapping.blogspot.fr

ISACA EURO CACS 2017

[214] Embedding Data Analytics in Fraud Auditing

Worauf kommt es im betrugsrelevanten Umfeld an und wie erfolgt die Beweissicherung? Und wie läßt sich die Analyse großer Datenmengen (big data) darin einbinden? Eine Antwort auf diese und weitere Fragestellungen lieferte dieser Vortrag.

Wichtigste Erkenntnisse:

- traditionelle Vorgehensweisen oder Abläufe helfen oft nicht (z.B. Zeitverzug zwischen Vergehen und Entdeckung oder neue Medien VoiceOverIP)
- welche Methoden gibt es, worin unterscheiden sie sich und wann kann man sie anwenden
- systematische Herangehensweise notwendig zur Beweiskraftsicherung (chain of custody / chain of evidence)

Quellen:

- ---

ISACA EURO CACS 2017

[223] Wearable Botnets & Happy Hacked Drivers

Der Teufel steckt oft im Detail und Zeitnot oder Bequemlichkeit führt oft zu haarsträubenden Problemlösungen. Der Bezug auf durchaus bedrohliche Beispiele aus der realen Welt sollte jedem klarmachen, dass Handlungsbedarf besteht.

Wichtigste Erkenntnisse:

- je mehr Vernetzungsmöglichkeiten, desto größer die Bandbreite an Angriffsvektoren
- alte Hardware war nicht für den Einsatz in vernetzten Umgebungen gedacht
- wenn es Lücken gibt, ist es nur eine Frage der Zeit , bis diese ausgenetzt werden
- es ist keine Frage ob, sondern nur wann und wie ein System gehackt wird

Quellen:

- http://deadhacker.com/2010/02/03/jtag-enumeration/
- http://openocd.org/doc/html/Debug-Adapter-Hardware.html
- https://github.com/synthetos/PiOCD/wiki/Using-a-Raspberry-Pi-as-a-JTAG-Dongle
- http://www.dataman.com
- http://www.limpkin.fr/index.php?post/2012/04/30/Hacking-a-laundry-machine-in-one-day-%28SLE4442%29
- https://www.freedesktop.org/wiki/Software/dbus/
- https://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf
- https://www.robtex.com/

ISACA EURO CACS 2017

[233] IoT & AI: New Threats & Mitigations

Grundlegende Betrachtungen zu IoT und AI. Für eigene Risikobewertungen können die vorgestellten Klassifizierungen hilfreich sein.

Wichtigste Erkenntnisse:

- OWASP Top 10 IoT Vulnerabilities als Basis einer Controls and Assurance Checklist der IoT Security Foundation
- eine ACP Bewertung der Daten ist auch im IoT Umfeld unerlässlich
- durch den Einsatz von AI lassen sich nicht nur Analysen automatisieren sondern auch Attacken

Quellen:

- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main (OWASP IoT project)
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities (IoT vulnerabilities)
- https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf (IoT Compliance Framework)
- https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf (basic considerations)

ISACA EURO CACS 2017

[242] Bridging the Cyber Skills Gap from Within

Es ist ökonomischer, die eigenen Angestellten im Unternehmen aus- und weiterzubilden als ständig neue Mitarbeiter anzuwerben und anzulernen.

Wichtigste Erkenntnisse:

- *"There are risks and costs to a program of action – but they are far less than the long range costs of comfortable inaction. John F. Kennedy, US President"*
- "*What if train people and they leave? – CEO*
  What if don't, and the stay? – CFO"
- Weiterbildung behält das Wissen im Unternehmen und sichert langfristig die Attraktivität des Unternehmens für neue Talente

Quellen:

- https://pgicyber.com

ISACA EURO CACS 2017

[251] Auditing ITSM

Grundlegende Betrachtungen zum Ansatz des IT Service Management Gedankens und darauf aufbauend, wie die Bewertung (der Qualität) des Services erfolgt. Kurzer, prägnanter Überblick über die Begrifflichkeiten des Service Managements.

Wichtigste Erkenntnisse:

- Standards gibt es viele (ITL V3, ISO/IEC 20000, COBIT 5), wichtig ist die konsequente Umsetzung und Dokumentation (insbesondere von Ausnahmen) eines Standards auch im Hinblick auf spätere Auditierbarkeit
- die Ziele des Audits müssen vorher definiert werden
- das IT Audit sollte immer abgestimmt mit breiter angelegten Audits des Unternehmens sein

Quellen:

- ---

ISACA EURO CACS 2017

[263] The Art of Cyber Risk Management

Grundlegende Beschreibung des Risiko Managements. Die Ansätze sind nicht neu, nur der Scope reduziert sich auf die digitale Welt. Die Begriffe sollten allen grundsätzlich bekannt sein.

Wichtigste Erkenntnisse:

- im Mittelpunkt aller Betrachtungen sollte stets das zu schützende Gut (= *Asset*) stehen
- alle möglichen Risiken sind hinsichtlich Auswirkung (*Impact*) und Wahrscheinlichkeit (*Likelihood*, manchmal auch *Probability*) einzuteilen und auf den eigenen Anwendungsfall zu spiegeln
- ein Risiko zu akzeptieren, ist eine legitime Möglichkeit (Risiken immer nur adequat absichern)

Quellen:

- ---

ISACA EURO CACS 2017

[312] Building a "Global Cybersecurity" Framework

Grundlegende Betrachung zu Aufbau und Funktionsweise einer Informationssicherheitsorganisation.

Wichtigste Erkenntnisse:

- Vortrag orientiert sich an den Standardwerken
- Wiederholung bereits umgesetzter oder initiierter Strukturen

Quellen:

- ---

ISACA EURO CACS 2017

[322] Deep & Dark Web

Geschätzt werden nur etwa 0,0034% aller im Internet verfügbaren Daten / Seiten durch die gängigsten Suchmaschinen indexiert, der Rest bildet das sogenannte Deep Web. Den kleinsten Teil davon wiederum bildet “das Dark Web", dessen Inhalte zwar nicht durchsucht, aber bei Kenntnis der genauen URL trotzdem zugreifbar sind (zunächst unabhängig davon, ob mit Zugriffsschutz oder ohne).

Wichtigste Erkenntnisse:

- für das Deep Web existieren eigene Suchmaschinen (die z.B. die robots.txt Dateien ignorieren)
- es gibt nicht ein, sondern beliebig viele Dark Webs; ONION (über TOR) ist nur das bekannteste (I2P, Freenet, anoNET, . . .)
- auch TOR (und alle anderen Dark Webs) haben Grenzen der Anonymität

Quellen:

- www.brandpowder.com (Illustration)
- https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet
- http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf

ISACA EURO CACS 2017

[SS1] Spotlight Session Compliance on Z/OS using Multifactor Authentication

Multi-Faktor-Authentisierung sollte der Standard, Kennung / Kennwort nur die Ausnahme sein. Basierend auf dieser These wird deutlich, warum gerade auch im Bereich der Großrechner eine eindeutige Zuordnung angemeldeter Benutzer essentiell für die Sicherheit ist.

Wichtigste Erkenntnisse:

- nicht alle Methoden sind gleich gut geeignet
- für jeden Anwendungsfall sollte geprüft werden, was genau mit der multi-Faktor-Authentisierung erreicht werden soll
- starke Authentisierung allein löst keine grundlegenden Sicherheitsprobleme
- keine Präsentation verfügbar

Quellen:

- ---

ISACA EURO CACS 2017

[---] Bavarian Fest Social Event

Am zweiten Abend der Konferenz war bei bayerischen Spezialitäten Netzwerken bzw. Kontakte pflegen angesagt.

Wichtigste Erkenntnisse:

- die meisten Konferenzteilnehmer waren auch beim bayerischen Abend anwesend
- Anfangs- und Endzeitpunkt waren genau festgelegt und wurden auch sehr genau eingehalten
- Bustransfer zwischen Hotel und Lokal
- Essen mehr als genug vorhanden und sehr gut

Quellen:

- ---

ISACA EURO CACS 2017

[---] Closing Keynote Address: Can Technology Solve Everything?

Die klare Antwort lautet NEIN, aber Technologie kann uns helfen, Aufgabenstellungen besser und schneller zu verstehen und zu bearbeiten.

Wichtigste Erkenntnisse:

- Technologie hat ihre Grenzen (z.B. Gesichtserkennung, ethische Fragestelllungen)
- Technologie kann den menschlichen Horizont erweitern (z.B. Verarbeitung bzw. Auswertung großer Mengen an Daten wie Log-Dateien, Support-Anfragen)
- Technologie wird immer weiter in Bereiche des heute Menschen vorbehaltenen Lebens vordringen (z.B. autonomes Autofahren, Simultanübersetzung), aber es muss klar definierte Regeln des Menschen für Extremsituationen geben
- keine Präsentation verfügbar

Quellen:

- ---

ISACA EURO CACS 2017

[---] Location

Westin Grand

Wichtigste Erkenntnisse:

- sehr gut mit öffentlichen Verkehrsmitteln erreichbar (U-Bahn Station Arabellapark)
- Klimaanlage funktionierte gut (während des Cybersecurity Workshops sogar zu gut J)
- Bewirtung sehr gut
- Verteilung der Konferenzzone über drei Ebenen (Keller, Erdgeschoss, erster Stock) sorgt für Bewegung und bietet zugleich ausreichend Gelegenheit zum Kontakte knüpfen und vertiefen

Glossar

ISACA	Information Systems Audit and Control Association	Organisation
CACS	Computer Audit, Control and Security	Conference
	Westin Grand	Hotel

References:

- http://www.isaca.org/about-isaca/Pages/default.aspx (abbreviation)
- http://www.isaca.org/About-ISACA/Licensing-and-Promotion/Pages/IP-Guidelines.aspx (trademarks)
- https://www.isaca.org/ecommerce/Pages/european-cacs-europe.aspx (EuroCACS)
- http://www.westingrandmunich.com/en (home)
- http://www.westingrandmunich.com/meetings/en/search (meeting rooms)