GESELLSCHAFT FÜR INFORMATIK E.V.

Workshop der Fachgruppe SECMGT

Aktueller Stand: Cybersecurity Defence und Bekämpfung von Cyber-Kriminalität

21. März 2025
Goethe-Universität Frankfurt am Main

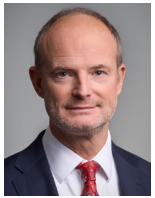
Fachgruppe SECMGT

Wir verstehen uns als **Praktiker-Forum**, das sich mit dem Management von Informationssicherheit, den entsprechenden Risiken und Lösungen für Unternehmen, Behörden und anderen Organisationen beschäftigt.

- wir bieten eine neutrale Plattform „von Spezialisten für Spezialisten“ für Vernetzung, Wissens- und Erfahrungsaustausch,
- wir bringen uns zukunftsorientiert und ergebnisoffen in die aktuelle Fachdiskussion zur Informationssicherheit ein,
- wir sind Teil des GI-Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit“,
- wir veranstalten regelmäßig Workshops, bei denen auch Nichtmitglieder stets willkommen sind,
- wir informieren Sie über: www.secmgt.de und secmgt@gi-fb-sicherheit.de

Leitungsgremium

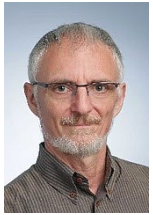
Machen Sie mit!
Neuwahl in 2025



Sprecher der Fachgruppe
Dr. Frank Damm
FTI Consulting

stellv. Sprecher der Fachgruppe
Benedict Voßbein
UIMC Dr. Voßbein
GmbH & Co. KG

Prof. Dr. Alexander Lawall
IU Internationale Hochschule



Prof. Dr.
Ralf Kneuper
IU
Internationale
Hochschule

Isabel Münch
Bundesamt für Sicherheit in der Informationstechnik

Georg Reiss
Stadtwerke Frankfurt am Main

Peer Reymann
ITQS GmbH

Marion Steiner
IT-Security@Work GmbH

Bernhard C. Witt
it.sec GmbH & Co. KG

Hinweise

- Bewegen im Gebäude
- Mittagspause und Mittagessen
- Getränke
- Toiletten

Herzlichen Dank an die Sponsoren!

Ohne externe Unterstützung ist die Durchführung einer solchen Veranstaltung nicht denkbar.

Die Fachgruppe bedankt sich darum bei den Sponsoren:

Goethe-Universität Frankfurt am Main für den Raum.

UIMC DR. VOSSBEIN GmbH & Co KG, Prof. Dr. Ralf Kneuper und Dr. Frank Damm für die Getränke.

Nächste Termine

Sep/Nov 2025	Workshop der Fachgruppe Thema: tbd
Q4 2025	Neuwahl Leitungsgremium Interessierte: bitte meldet Euch!

Aktuelle Informationen zu unseren Aktivitäten finden Sie immer unter https://fg-secmgt.gi.de oder Sie sprechen uns einfach an.

Aktueller Stand: Cybersecurity Defence und Bekämpfung von Cyber-Kriminalität

Es gibt keine 100% Sicherheit, die Frage ist nicht, ob, sondern wann ein Angriff erfolgt“ – dieser Satz wird von Experten treffenderweise sehr häufig zitiert. Ein zentrales Thema der Informationssicherheit ist daher neben Schutz durch präventive Maßnahmen auch die Erkennung und Reaktion auf erfolgte Angriffe. Dazu ist es wichtig zu wissen, wie die verschiedenen Angreifergruppen agieren. Wie kann effektiver Schutz gegen Angriffe von Kriminellen, Nachrichtendiensten und anderer Akteure aussehen? Wie unterscheiden sie sich, und wie kann man sie erkennen? Was kann man daraus ableiten für den Schutz gegen solche Angriffe?

Das BSI hat hierzu bereits in 2022 eine „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=17) herausgegeben, die insbesondere von KRITIS-Unternehmen zu berücksichtigen ist und deren Umsetzung im Rahmen der Prüfung bewertet wird. Diese wurde gerade im November 2024 aktualisiert und kann auch nicht KRITIS-Unternehmen als Hilfestellung dienen, wenn es um die Identifizierung wichtiger Bausteine geht. Und auch der „Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen“ (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/MST_BSI_PD_Version_2_1.pdf?__blob=publicationFile&v=6) für die Infrastrukturen des Bundes wurde parallel aktualisiert.

Was gehört zu einer angemessenen Verteidigung, welche Lösungsansätze gibt es und welche Erfahrungen mit Umsetzungen gibt es in der Praxis?

Mit diesen Fragen wollen wir uns in diesem Workshop befassen. Neben der Sicht von Unternehmen und dem Einsatz von SOC und Threat Intelligence sind dabei auch Präsentationen staatlicher Akteure geplant, die sich mit der Bekämpfung von Cyber-Kriminalität oder dem Schutz gegen Spionage befassen.

Agenda Workshop (1/2)

Uhrzeit	Referent	Titel
10:00	Benedict Voßbein, stellvertretender Sprecher der Fachgruppe Dr. Frank Damm, Sprecher der Fachgruppe	Begrüßung und Vorstellung der Fachgruppe
10:15	Klaus Hunsänger, Bundesamt für Sicherheit in der Informationstechnik (BSI)	Systeme zur Angriffserkennung (SzA)
10:55		Kommunikationspause
11:10	Eric Müller, Polizeioberkommissar, Max Bachon, Polizeioberkommissar, Hessisches Landeskriminalamt, ZAC – Zentrale Ansprechstelle Cybercrime	YOU HAVE BEEN HACKED! Vorstellung der Zentralen Ansprechstelle Cybercrime für die Wirtschaft
11:50		Kommunikations- und Mittagspause
13:30	Thomas Wallutis, (externer) ISB, IHK-GfI GmbH	Zwei Jahre nach dem Vorfall – ein Erfahrungsbericht

Agenda Workshop (2/2)

Uhrzeit	Referent	Titel
14:10		Kommunikationspause
14:25	Christopher Brumm, Security Architekt, glueckkanja AG	Clickbait vs. Reality: Die Cyber Threats, um die Sie sich wirklich sorgen sollten
15:05		Kommunikationspause
15:20	Dr. Philipp Trinius, Deutsche Telekom Security GmbH, Leiter Cyber Defense und Cloud Security	Security Operations Center (SOC) als Managed Security Service (MSS)
16:00	Diskussion/Open Panel	Erfahrungen & Best Practices der Workshopteilnehmer
17:00		Ende der Veranstaltung
18:00	Gemeinsames Abendessen	Ristorante Isoletta, Feldbergstr. 31

Nach dem Workshop

Teilnahmenachweis/continuing professional education

Diese Veranstaltung dient auch der continuing professional education. Um CPE-Punkte zu sammeln, nutzen Sie eines der vorbereiteten CPE Formulare. Tragen Sie dort Ihren Namen und Ihre Zertifizierung ein. Eine/r der anwesenden Leitungsgremiumsmitglieder bestätigt gegen Ende der Veranstaltung Ihre Teilnahme durch Unterschrift auf dem Formular.

Präsentationen vom Workshop

finden Sie kurz nach der Veranstaltung unter:
https://fg-secmgt.gi.de/veranstaltung,
sofern sie uns zur Verfügung gestellt werden.

Wir freuen uns auf den fachlichen Austausch mit Ihnen!