Lebenslauf

Marl Joos

mail@m-a-r-l.de

*18. Oktober 1994, Engen

Deutsch

sec6.de

Berufliche Erfahrung

05/2021 – 07/2024 ICS/OT Security Consultant bei GAI NetConsult GmbH
(Für eine detaillierte Projektliste siehe Anhang 1 auf Seite 4.)

- Sicherheitsaudits auf Basis von ISO/IEC 27001/2/19, IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG und anderen Standards
  - Dokumentensichtung, Interviews, Berichtserstellung, Ableitung von Empfehlungen
- Security-Assessments auf Basis des NIST Cybersecurity Frameworks
  - OT Security Architecture Review
  - Supply Chain Security Assessments
  - ICS Readiness Assessments
- Fachliche Beratung und Unterstützung zur Entwicklung der Version 3.0 (09/2024) des BDEW/OE/VSE-Whitepapers[1]
- Systemspezifische Risikoanalysen (z. B. auf Basis des BDEW/OE-Whitepapers oder kundenspezifischer Risikoanalysemethoden)
- Sicherheitstechnische Bewertung von Pflichtenheften / Design-Spezifikationen in der Ausschreibungs- oder Design-Phase
- BSI-IT-Grundschutz-Baustein-basierte Audits

10/2019 – 02/2021 Masterand bei secunet Security Networks AG

09/2019 – 09/2020 Werkstudent bei secunet Security Networks AG

[1] Siehe Seite 2 des Dokumentes als Nachweis.

- Softwareentwicklung im Bereich eingebette Systeme im Software Development and Verification Team
- Portierung eines Linux-Treibers in C in Ada/SPARK
- Treiberentwicklung in Ada/SPARK
- Allgemeine Arbeiten im Build-System, Compiler-Updates und Compiler-Bug Reporting

12/2017 – 09/2018 Technology Specialist (Industrial Security / Cyber Defense) bei Computacenter AG & Co. oHG

- Entwicklung von Informationssicherheitsrichtlinien für die Produktion eines DAX30-Unternehmens
- Erweiterung eines Demokoffers mit industriellen Steuergeräten und Netzwerk(sicherheits)geräten
- Teilnahme an zahlreichen IT-Sicherheitsschulungen

10/2017 – 11/2017 Geringfügige Beschäftigung bei P3 communications GmbH

09/2016 – 09/2017 Werkstudententätigkeit bei P3 communications GmbH

- Technische Sicherheitstests an (industriellen) eingebetten Systemen[1] und Entwicklung eines Sicherheitstestskataloges
- Forschungsprojekte:
  - SEnCom: "Systemsicherheit von Energieversorgungsnetzen bei Einbindung von Informations- und Kommunikationstechnologien"
  - BERCOM: "Blueprint for Pan-European Resilient Critical Infrastructures based on LTE Communications"

04/2015 – 07/2015 Werkstudententätigkeit bei DGI Deutsche Gesellschaft für Informationssicherheit AG

02/2015 – 04/2015 Berufspraktikum bei DGI Deutsche Gesellschaft für Informationssicherheit AG

Ausbildung

2017 – 2021 Studium der Informatik (M.Sc.), Technische Universität Berlin, Abschlussnote 1,2

- Spezialisierung: Embedded Systems and Computer Architectures

[1] https://cert-portal.siemens.com/productcert/pdf/ssa-507847.pdf

- Persönliche Schwerpunkt auf IT-Sicherheitsmodulen aus sämtlichen Studiengebieten
- Masterarbeit: “Mitigation of Cache Side Channel Attacks with Logic Programming“

2013 – 2017 Studium der Informatik (B.Sc.), Freie Universität Berlin, Abschlussnote: 2,0

- Bachelorarbeit: “Entwicklung einer Lösung zur automatisierten Änderung von Passwörtern“

2010 – 2013 Technisches Gymnasium, Hohentwiel-Gewerbeschule Singen, Abschlussnote: 1,8

2005 – 2010 Friedrich-Wöhler Gymnasium Singen

Zertifikate und Schulungen[2]

07.03.24 SecOps: Operative Informationssicherheit

- https://www.comconsult.com/secops-operative-sicherheit/

05.10.23 ISO/IEC 27001:2022 Transition Training for Auditors

12.06.21 - 16.07.21 ISO/IEC 27001:2013 Lead Auditor

- Credential ID: 337221

31.07.19 ISTQB® Certified Tester Foundation Level

- Zertifikatsnummer: 19-CTFL-161736-01
- https://zertdb.isqi.org/de/download/certificate/token/RjQJXrZA15VE6Th3

19.03.18 - 22.03.18 Incident Analysis-Schulung von ERNW INSIGHT Training

26.02.18 - 28.02.18 Security Monitoring-Schulung von ERNW INSIGHT Training

14.02.18 - 16.02.18 Hacking Fundamentals-Schulung von ERNW INSIGHT Training

17.03.15 ITIL® Foundation Certificate in IT Service Management

IT-Kenntnisse

GNU/Linux (Serveradministration), QubesOS, Separation Kernel (Muen), Windows-Sicherheit

C, Ada/SPARK, Python, Shell-Skrpting, Java, LaTeX, HTML, CSS, PHP, Haskell, R, x86/x64/ARM-Assembler

[2]Nachweise gerne auf Anfrage

Sicherheitsanalysen (u. a. Schwachstellenanalysen), OWASP, Firmwareanalysen

Fremdsprachen

Gute Englisch-Kenntnisse in Wort und Schrift

Grundkenntnisse in Französisch

Grundkenntnisse in Chinesisch

Sonstige Aktivitäten

Seit 10/2017	AG Rechnersicherheit der TU Berlin - ehemalig: Beteiligung an CTFs, derzeit: unregelmäßige Teilnahme an den Treffen und Diskussionen
Seit 01.06.2019	Gesellschaft zur wissenschaftlichen Untersuchung von Parawissenschaften e. V. - Teilnahme an regionalen Veranstaltungen
01.01.2019 - 2023	Gesellschaft für Informatik e. V. - passives Mitglied
Seit 01.06.2016	Wikimedia Deutschland e.V. - passives Fördermitglied
18.03.18	Teilnahme an der TROOPERS18 IT-Sicherheitskonferenz
Ehemalig:	Mitglied der SCADACS-Gruppe (SCADA & Computer Security) am Fachbereich Informatik, Arbeitsgruppe Sichere Identität, Freie Universität Berlin. Themengebiet: Sicherheit von Industrieanlagen. http://scadacs.org
Ehemalig:	Durchführung von Schulungen über verschlüsselte Kommunikation (OpenPGP, XMPP+Off-The-Record-Messaging) am Institut für Informatik. http://krypto.mi.fu-berlin.de http://crypto.spline.de
Ehemalig:	Mitglied von spline (Studentisches Projekt Linux und Netzwerke), Vereinigung von Freunden des Linux-Kernels und freier Software. Serveradministration. http://spline.de
Ehemalig:	“Kryptografie unter GNU/Linux“-Vorlesung der von spline organisierten Vorlesungsreihe über GNU/Linux. http://linuxkurs.spline.de/

Anhang 1: Auszug Projektliste

Zurück zur beruflichen Erfahrung

Im Folgenden werden Aktivitäten und Projekte zusammengefasst und aufgeführt, bei denen

ich besonders mitgewirkt habe. Die Projekte wurden üblicherweise im Team durch zwei Personen durchgeführt:

- **Informationssicherheitsaudits auf Basis ISO/IEC 27001 und anderen Standards**
  Durchführung von mehreren Informationssichereitsaudits bei Übertragungsnetzbetreibern auf Basis des Anhang A der ISO/IEC 27001 und weiteren Standards und IT/OT-Sicherheitsanforderungen wie ISO/IEC 27002, 27019, OPDE (Operational Planning Data environment) sowie unternehmensinterner Vorgaben und Vorgaben des IT-Sicherheitskatalogs gemäß § 11 Abs. 1a EnWG. Zum Auditgeltungsbereich gehörten Netzleitsysteme, Energiemarktapplikationen, PDV-Infrastrukturen, Schutz- und Leittechnik, Betriebstelefonie und Rechenzentren. Das Standardvorgehen beinhaltete die Dokumentensichtung, Interview-Termine und ggf. Vor-Ort-Begehungen sowie die Berichtserstellung.

- **IT/OT-Sicherheitsberatung in der Ausschreibe- und Entwurfsphase**
  Mehrere Übertragungsnetzbetreiber wurden bei der Ausschreibe- und/oder der Entwurfsphase für elektrische Einrichtungen wie zum Beispiel Offshore-Umspannstationen oder STATCOM-Anlagen unterstützt. Dazu gehörte die Definition von IT/OT-Sicherheitsanforderungen nach dem Stand der Technik und anerkannter Standards wie dem BDEW/OE Whitepaper. Gemäß der Anforderungsgrundlage und den Angeboten bzw. Pflichtenheften wurden die Bieter und ihre angebotenen Lösungen kommentiert und beurteilt. Dabei wurden regelmäßige Interviews mit dem Kunden und den Bietern zur Abstimmung und Klärung von Rückfragen durchgeführt.

- **OT-Security-Assessments auf Basis von NIST CSF und MITRE ATT&CK®**
  Auf Basis ausgewählter Funktionen und Subkategorie des NIST Cybersecurity Frameworks und den ICS Mitigations nach MITRE ATT&CK® wurden mehrere Technologiebereiche sogenannten Architecture-, Supply-Chain-Security-Review oder ICS Readiness Assessments bewertet. Im Rahmen dieser Untersuchungen wurden mehrere Workshop-Termine organisiert, Dokumente (unternehmensinterne Vorgaben und auch alle relevante technische Dokumentation) gesichtet, Fragenkataloge entwickelt und ggf. unter Hinzuziehung externer Zulieferer und Dienstleister des Kunden Interviews durchgeführt.

  Bei den Architecture-Reviews handelte es sich um IT/OT-Sicherheitsüberprüfungen, die überwiegend auf NIST-Subkategorie der Funktionen “Protect“ und “Detect“ basierten. Zu den überprüften Themen gehörte zum Beispiel der Einsatz sicherer Authentifizierungsverfahren, Härtungsmaßnahmen, Update-, Patch- und Schwachstellenmanagement.

  In den Supply-Chain-Security-Reviews wurden Infrastrukturen und Betriebsprozesse auf die Berücksichtigung von Sicherheitsanforderungen in der Lieferkette untersucht. Hierbei wurden unternehmensinterne Vorgaben, Beschaffungsprozesse, Wartungsverträge sowie relevante Prozesse mit Bezug zur Dienstleistungserbringung durch Befragung der Zulieferer untersucht.

Im Rahmen der ICS-Readiness-Assessments wurden auf Basis der NIST-CSF-Funktionen “Respond“ und “Recovery“ die Fähigkeiten zur Wiederherstellung von Systemen und Prozessen sowie zur Sicherheitsvorfallsreaktion des Kunden und seine Zulieferer untersucht.

Abschließend wurden die Ergebnisse dokumentiert, nach definierten Kriterien bewertet und Maßnahmenempfehlungen abgeleitet. Das Gesamtergebnis wurde in einem Abschlussbericht dokumentiert.

- **Sonstige Beratungsprojekte**
  Weitere Projekte, in denen ich mitgewirkt habe, waren die Erstellung eines Zonenkonzepts für den OT-Bereich eines Netzbetreibers, eigens entwickelte Ransomware-Readiness-Assessments, Bewertungen von auf OT spezialisierte IDS-Lösungen, fachliche Beratung bei der Entwicklung eines IT/OT-Sicherheitsstandards der Energiebranche, BSI-IT-Grundschutz-basierte Audits (z. B. Webserver, Verzeichnisdienste, Firewalls), eine OT-Incident-Response-Übung, Rechenzentrumsprüfung (auf Basis der BSI-IT-GS Bausteine INF.2 und INF.5) sowie der Bewertung der Architektur und des Konzepts eines SIEM.

Zurück zur beruflichen Erfahrung

Anhang 2: Absolvierte Hochschulmodule im Bereich Informationssicherheit[2]

- Freie Universität Berlin (Bachelor)
  - Grundlagen der Rechnersicherheit
  - SCADA / ICS Security Praktikum (Hacking-Lab)
  - Proseminar Theoretische Informatik, Vortrag: "Komplexitätstheorie und Kryptographie": http://www.inf.fu-berlin.de/lehre/WS15/PSThInf/notes/12_crypto.pdf
  - Softwareprojekt: Entwicklung eines Cryptophones in C im Team

  Technische Universität Berlin (Master)
  - Hardware Security Lab
  - Computer Security Specialization Small
    - Internet Security
    - Telecommunication Security
  - Computer Security Specialization Large
    - Computer Security Seminar
    - Cryptography
    - Quantum Computing
  - Network Protocols and Architecture
  - Security Lab
  - Analysis and Optimization of Embedded Systems
    - Inhalt: u. a. statische und dynamische Programmanalysetechniken zur Verifikation von Sicherheitseigenschaften (information flow security)

Berlin, den 2. Oktober 2024

[2]Nachweise gerne auf Anfrage