# JENS HENNIG

CYBERSECURITY EXPERT

h-its.info
kontakt@h-its.info
+49 211 15838091

## Kurzvita

Jens Hennig ist ein erfahrener Cybersecurity-Experte mit einer einzigartigen Kombination aus militärischer Führungsverantwortung und tiefgehender technischer Expertise in IT- und Netzwerksicherheit. In leitenden Positionen bei der Bundeswehr verantwortete er unter anderem die Implementierung sicherer Kommunikationsinfrastrukturen, die Koordination multinationaler IT-Projekte und die Einführung moderner Technologien wie DigiFu BOS und SatComBw. Mit fundiertem Wissen in Bereichen wie IT-Governance, Netzwerksicherheit und Kryptografie sowie einer soliden akademischen Grundlage aus einem laufenden M.Sc. in Cyber Security und früheren Ingenieurstudiengängen ist er bestens aufgestellt, um komplexe Herausforderungen in der Cybersicherheit zu lösen. Sein Ansatz kombiniert strategische Planung, operative Umsetzung und die kontinuierliche Verbesserung sicherheitskritischer IT-Systeme.

## Erfahrung

IT-Offizier, Bundeswehr BAMAD, Köln, NRW — August 2018 – Januar 2023

- Analysierte und spezifizierte Anwenderanforderungen für organisationsspezifische IT-Verfahren mit Schwerpunkt auf Schnittstellenmanagement und Cyber-Sicherheitsanforderungen.
- Erarbeitete funktionale Anforderungen zur Weiterentwicklung von IT-Systemen und stellte die Einhaltung von BSI IT-Grundschutz und weiteren IT-Sicherheitsvorgaben sicher.
- Koordinierte und implementierte DigiFu BOS (Digitalfunk für Behörden und Organisationen mit Sicherheitsaufgaben) mit besonderem Schwerpunkt auf Netzwerksicherheit, Verschlüsselung und interoperable Systemintegration.
- Koordinierte und implementierte sichere Videokonferenzsysteme in heterogenen Netzwerken, um den geschützten Austausch zwischen Organisationen zu ermöglichen.
- Modernisierte die Kommunikationsinfrastruktur durch die Begleitung des Projekts ALLIP zur Migration von ISDN auf IP, einschließlich der Implementierung sicherer Netzwerkschnittstellen und der Einhaltung von IT-Sicherheitsrichtlinien.
- Konfigurierte und administrierte SIP-Telefonanlagen mit Fokus auf verschlüsselte Kommunikation, sichere Authentifizierung und den Schutz vor Netzwerkangriffen.
- Implementierte und verwaltete Mobile Device Management (MDM)-Lösungen, um mobile Endgeräte vor Datenlecks und unbefugtem Zugriff zu schützen.
- Vertrat den MAD in behördenübergreifenden Arbeitsgruppen, um IT-Sicherheitsanforderungen zu koordinieren und organisationsübergreifende Zusammenarbeit zu fördern.
- Verwaltete Datensätze zur alternativen Identifikation und implementierte Schutzmaßnahmen zur Sicherstellung von Datenintegrität und Vertraulichkeit.

IT-Sicherheitsbeauftragter, Bundeswehr,Sanitätsregiment 2, Rennerod Juli 2015 – August 2018

- Erstellte ein IT-Sicherheitskonzept für das Sanitätsregiment 2 auf Basis des BSI IT-Grundschutzes, mit Fokus auf Risikoanalyse, Schutzbedarfsfeststellung und der Implementierung von Maßnahmenkatalogen gemäß Vorschrift A960/1.
- Führte eine Kryptoverwaltungsprüfung unter Berücksichtigung der BSI-Anforderungen an Schlüsselmanagement und Verschlüsselungsprozesse durch, um Compliance sicherzustellen und Angriffsvektoren zu minimieren.
- Bereitete das Sanitätsregiment 2 auf eine IT-Sicherheitsprüfung durch die übergeordnete Ebene vor, einschließlich der Dokumentation und Umsetzung von Maßnahmen gemäß BSI-Grundschutz-Kompendium.
- Implementierte eine IT-Sicherheitsstrategie und überwachte deren Umsetzung gemäß BSI-Vorgaben.

Zugführer(Bereichsleiter), Bundeswehr,IT-Battalion 281, Gerolstein Januar 2014 – Juli 2015

• Auslandseinsatz „Active Fence Turkey“ (AFTUR): Führte ein Team, das als IT-Serviceprovider für NATO-Operationen agierte. Verantwortete den Einsatz und Betrieb von Technologien wie SATCOMBw, VLAN, VPN, Videokonferenzsystemen und TETRAPOL, um sichere, verschlüsselte und hochverfügbare IT-Dienste zu gewährleisten. Implementierte Sicherheitsmechanismen, um die Infrastruktur vor Cyber-Bedrohungen zu schützen und die Integrität kritischer Kommunikationskanäle sicherzustellen.

• NATO-Auslandsübung in Ungarn: Führte ein Team, das als Network Access Provider agierte, und verantwortete die Bereitstellung und Verwaltung sicherer Netzwerkzugänge in einem multinationalen Umfeld. Schwerpunkt lag auf der Implementierung von Maßnahmen zur Netzwerksicherheit und der Unterstützung einer robusten Kommunikationsinfrastruktur.

• Leitete ein Team im Aufbau und Betrieb einer transportablen Netzwerkinfrastruktur für Auslandseinsätze, mit Fokus auf Netzwerksicherheit und Kommunikation.

## Ausbildung

**M.Sc**. in Cyber Security, IU Internationale Hochschule Abschluss geplant August 2025

• Verfasste eine Seminararbeit zur Verbesserung der Sicherheit webbasierter Lösungen durch den Einsatz von FIDO2, bei der die Schwachstellen passwortbasierter Authentifizierung analysiert und durch eine implementierte Multi-Faktor-Lösung adressiert wurden.

• Hielt Fachvorträge über Elliptic Curve Cryptography (ECC) mit Schwerpunkt auf deren Effizienz und Sicherheit im Vergleich zu traditionellen Verschlüsselungsverfahren, sowie über die OWASP Top 10, mit Fokus auf präventive Maßnahmen gegen die häufigsten Sicherheitsrisiken in Webanwendungen.

• Erwarb fundierte Kenntnisse in IT-Governance, -Compliance und -Recht, einschließlich der Implementierung und Überwachung von Governance-Strategien und der Einhaltung rechtlicher Vorgaben für Datenschutz und IT-Sicherheit.

• Vertiefte das Verständnis von Kryptologie, insbesondere Verschlüsselungstechniken und deren Anwendungen zur Sicherstellung der Informationssicherheit in IT-Systemen.

• Führte Cyber Risk Assessments durch und entwickelte Risikomanagementstrategien, um potenzielle Bedrohungen zu analysieren und zu mitigieren.

• Spezialisierte sich auf Netzwerksicherheit, mit Fokus auf Schutzmaßnahmen gegen interne und externe Bedrohungen durch fortschrittliche Architekturen und Technologien.

• Erlangte zusätzliche Expertise in Netzwerkforensik und Cybersystemen, durch die Anwendung forensischer Techniken zur Untersuchung von Cyberangriffen und Sicherheitsvorfällen.

**M.Sc**. in Mathematical Engineering September 2013

• Entwickelte im Rahmen der Masterarbeit die Hardware und Software für eine Plasmasteuerung, basierend auf einem Embedded-PC-System, und setzte diese erfolgreich um, um präzise Steuerungs- und Regelungsaufgaben in Plasmaanwendungen zu realisieren.

**B.Sc**. in Mathematical Engineering Oktober 2012

- Erstellte im Rahmen der Bachelorarbeit ein grafisches Benutzerinterface für Optimierungsprobleme, das die Visualisierung und Anwendung verschiedener Lösungsalgorithmen erleichterte und die Benutzerfreundlichkeit solcher Anwendungen deutlich verbesserte.
- Erwarb die Berechtigung zur Führung der Berufsbezeichnung „Ingenieur“.

## Qualifikationen

**Cyber Security:** Cyber Risk Assessment/Management, IT-Governance, -Compliance und -Recht, Datenschutz, Cyber Risk Assessment/Management, Netzwerksicherheit, Netzwerkforensik, Computerforensik, OWASP Top 10, FIDO2, Passkeys
**Virtualisierung:** QEMU, LXC, Docker
**Programmiersprachen und Skripting:** C, Java, Python;PHP, SQL, Bash, Powershell,
**Sicherheitsüberprüfung:** Ü3 gemäß §1 SÜ-Gesetz (2018, abgelaufen 2023; erneuerbar bei Bedarf)
**Zertifizierungen:** Pro Scrum® Master I, Pro Scrum® Product Owner I, COBIT® 5 Foundation, ITIL3
**Sprachen:** Deutsch Muttersprachler, Englisch (NATO-SLP) 3332 entspricht C1

## Verfügbarkeit und Konditionen

- Vertragliches Beschäftigungsverhältnis: Freiberuflich
- Verfügbar auf Anfrage
- Einsatzort: Primär remote, mit Bereitschaft zu kurzfristigen Vor-Ort-Einsätzen, einschließlich Onboarding-Phasen oder spezifischer Projektanforderungen.