Thomas Hetschold (56)
Senior Information Security Consultant
CISSP-ISSMP
PMP

Wilhelmshöher Straße 74
60389 Frankfurt am Main
Tel. 0170/57 29 310
thomas@hetschold.de

Qualifikation

Ausbildung/Studium:

- Diplom Informatiker, J. W. Goethe-Universität, Frankfurt
- Certified Information Systems Security Professional
- Information Systems Security Management Professional
- Project Management Professional
- Cybersecurity Automotive Professional

Erfahrungsfelder

Branchen-know-how:

- Automotive – 6 Jahre
  Koordination der Business Information Security Officer (Daimler/Mercedes-Benz Group)
  Unterstützung bei der Einführung eines Cybersecurity Management Systems (Daimler Truck)
  Erstellen von Sicherheitsprofilen als Information Security Architect (Daimler)
  Unterstützung bei der Einführung eines toolgestützten Cloud Risiko Prozesses (Daimler)
  Durchführung von Spotchecks bei Cloud Projekten (Daimler)
  Unterstützung bei der Steuerung des Cloud Risiko Prozesses (Daimler)
  Erstellung einer IT-Security Policy für den Automotive Bereich (BMW)
  Definition, Aufbau und Betrieb des Center of Competence Automotive Security (BMW)
  Erstellung einer Bedrohungs- und Risikoanalyse für die Fahrzeug Security Architektur (BMW)
  Einführung einer sicheren SAP R/3 Infrastruktur (Volkswagen)
- Aviation – 9,5 Jahre
  Umsetzung des Payment Card Industry Data Security Standards (Lufthansa)
  Mehrfache erfolgreiche Re-Zertifizierung gemäß PCI DSS (Lufthansa)
  Unterstützung bei der Einführung und Umsetzung von IT-Security Prozessen (Lufthansa)
  Durchführung von Risikoanalysen für IT-Systeme mit Aircraftbezug (Lufthansa)
  Konzept zur Flight Operation Information Security (Lufthansa)
- Banken – 3 Jahre
  Entwicklung von Sicherheitsprotokollen für elektronische Geschäftsprozesse (Deutsche Bank, Dresdner Bank, Bank of America, ABN Amro)
  Entwicklung eines sicheren Online-Banking Protokolls (Dresdner Bank)
- Behörden/Öffentlicher Dienst – 2,5 Jahre
  Erstellen einer Bedrohungsanalyse für das automatisierte Fahren (Land Baden-Württemberg)
  Erstellung von IT-Sicherheitskonzepten für den Einsatz der elektronischen Gesundheitskarte (div. Krankenkassen)
  Entwicklung eines signaturgesetzkonformen Bestellwesens (Land Niedersachsen)
  Entwicklung von Sicherheitsprotokollen zum Einsatz der Health Professional Card (ABDA)
- Energie – 1 Jahr
  Entwicklung eines Systems zur sicheren Vorgangssteuerung im Kernkraftwerk (RWE)
  Einführung einer sicheren SAP R/3 Infrastruktur (RWE)
- IT und Telekommunikation – 8 Jahre
  Entwicklung eines Produktes zur Absicherung des SAP R/3 Systems (SAP)

Entwicklung von Security Produkten (Secude, Fillmore Labs)
Entwicklung der Zugriffskontrolle einer OSI Managementplattform nach X.741 (Deutsche Telekom)
- Medien – 1,5 Jahre
  Entwicklung eines Digital Rights Management Systems für eine Internet Tauschbörse (DWS/Bertelsmann)
- Transport – 0,75 Jahre
  Erstellung eines Informationssicherheits-Konzeptes und eines Datenschutzkonzeptes für eine Maut-Plattform (Kapsch)

Erfahrung Fachprozesse, Fachkompetenz:

- UNECE R155, ISO 21434
- Maut Prozesse
- Automotive Prozesse
  E/E-Entwicklungsprozesse
  Fertigungsprozesse
  Serviceprozesse
  Logistikprozesse
- Aviation Prozesse
- IT-Prozesse
  PCI DSS
  ISO 2700x
  OWASP
  Dokumentation nach Common Criteria
  Dokumentation nach ITSec

Spezialisierungen / Schwerpunkte

- Aufbau eines CSMS nach ISO 21434
- Datenschutzgrundverordnung (DSGVO)
- Payment Card Industry Data Security Standard (PCI DSS)
- IT-Sicherheitsprozesse
- IT-Risikomanagement
- Prozessanalyse und -modellierung

Führungserfahrung:

- CTO Secude GmbH, Leitung Entwicklung und Consulting mit 30 Mitarbeitern, 7 Jahre
- Geschäftsführer Fillmore Labs GmbH, 7 Mitarbeiter, 2 Jahre

Projektleitungserfahrung:

- Daimler, Teilprojektleitung, 1,5 Jahre
- Lufthansa, Projektmanagement, 7 Jahre
- Secude GmbH, Programmmanagement, 7 Jahre
- Fillmore Labs GmbH, Projektmanagement, 2 Jahre
- GMD (Fraunhofer Gesellschaft), 2 Jahre

Sonstiges:

- Mensa-Mitglied

Weiteres zur Person

- seit 2004 selbstständig (Senior Ìnformation Security Consultant, Prozessmodellierung)
- 2003 – 2004 Secude GmbH (CTO)
- 2001 – 2003 Fillmore Labs GmbH (Geschäftsführer)
- 1996 – 2001 Secude GmbH (CTO)
- 1993 – 1997 GMD – Forschungszentrum Informationstechnik GmbH (Wissenschaftlicher Mitarbeiter, Projektleiter)
- 1990 – 1993 selbstständig (IT Consultant, Software Entwickler)

Sprachkenntnisse

- Deutsch
- Englisch (Certificate in Advanced English)

Fortbildungen

- Information Security Architect (Daimler)
- PCI SSC Standards Training
- ITIL-Foundation
- Projektleitung IT Projekte bei CSC Ploenzke

Projekte

Ab 01/2022	**Koordination der Business Information Security Officer (BISO)**
Rolle:	Senior Information Security Consultant
Kunde:	Daimler / Mercedes-Benz Group
Einsatzort:	Stuttgart
Aufgaben:	Unterstützen bei der Definition und Entwicklung geeigneter, konzernweit gültiger Zielstrukturen und Prozesse für die Information Security in den Geschäfts- und den Zentralbereichen. Weiterentwicklung konzernweit gültiger Rollen-, Gremien- und Zusammenarbeitsmodelle im sehr komplexen Umfeld der Information Security. Steuerung und Weiterentwicklung des neuen Gremiums der Information Security Verantwortlichen der Geschäftsbereiche.
01/2021 – 12/2021	**Unterstützung bei der Einführung eines Cybersecurity Management Systems (CSMS)**
Rolle:	Senior Car Information Security Architect
Kunde:	Daimler TSS / Daimler Truck
Einsatzort:	Ulm
Aufgaben:	Gemäß UN Regulierung 155 müssen Automobilhersteller zukünftig die Umsetzung eines Cybersecurity Management Systems nachweisen, um eine Typzulassung zu erhalten. Dazu ist die Einhaltung der ISO/IEC 21434 notwendig. Ermitteln des Status Quo bei allen betroffenen Fahrzeugtypen. Erweitern des Fahrzeugentwicklungsprozesses, so dass die Anforderungen der ISO zukünftig berücksichtigt werden. Erstellen von Fahrzeug-TARAs (Threat Analysis and Risk Analysis).
09/2020 – 12/2020 4 Monate (50%)	**Erstellen von Sicherheitsprofilen als Information Security Architect (ISA)**
Rolle:	Information Security Architect
Kunde:	Daimler
Einsatzort:	Stuttgart
Aufgaben:	Erstellen eines C4-Modells und Data Flow Modells im Rahmen der Analyse von IT-Systemen zur Ermittlung möglicher Schwachstellen und Bedrohungen sowie ermitteln von Cloud-spezifischen Bedrohungen. Bewertung der Bedrohungen und Risiken. Entwickeln von angemessenen Gegenmaßnahmen, um Risiken auf ein akzeptables Maß zu reduzieren. Abstimmen der Ergebnisse mit dem Projekt.

07/2020 – 12/2020 3 Monate (50%)	**Bedrohungsanalyse** **IT-Sicherheit und autonomes Fahren**
Rolle:	Senior Information Security Consultant
Kunde:	Land Baden-Württemberg
Einsatzort:	Stuttgart
Aufgaben:	Analyse und Identifikation neuer Bedrohungen durch das vernetzte und automatisierte Fahren Es sollen sowohl präventive Maßnahmen als auch die Erkennung von Angriffen sowie die Ergreifung geeigneter Gegenmaßnahmen erforscht werden. Dabei sollen unter anderem neue Ansätze zur Erkennung von Straftaten sowie Verfahren für die Nachvollziehbarkeit von Entscheidungen automatisierter Fahrfunktionen, die auf maschinellen Lernverfahren beruhen, berücksichtigt werden.
10/2018 – 03/2020 18 Monate	**Teilprojektleitung Entwicklung und Einführung eines toolgestützten Cloud Risiko Prozesses**
Rolle:	Senior Information Security Consultant
Kunde:	Daimler AG
Einsatzort:	Stuttgart
Aufgaben:	Erstellen und umsetzen eines Konzepts für den Support inkl. Providerauswahl. Erstellen und umsetzen eines Konzepts für eine weltweite Multiplikator-Struktur zur Ergänzung des Supports. Erstellen und umsetzen eines Konzepts für Spotchecks zur Prüfung, ob Projekte die Prozessvorgaben eingehalten haben sowie Risiken richtig erkannt und mitigiert haben. Unterstützen des Arbeitspakets Kommunikation.
04/2018 – 12/2019 21 Monate	**Unterstützung Steuerung** **Cloud Risiko Prozess**
Rolle:	Senior Information Security Consultant
Kunde:	Daimler AG
Einsatzort:	Stuttgart
Aufgaben:	Prüfen von Projektunterlagen für die Cloudnutzung. Abstimmen der Risiko-Assessments mit IT und Legal. Prüfen, ob mitigierende Maßnahmen vom Projekt umgesetzt wurden (Spotchecks). Verbesserungen am Cloud Risiko Prozess vorschlagen und mit den verantwortlichen Stakeholdern abstimmen. Einführen eines Tools zur Steuerung des Cloud Risiko Prozesses.
07/2017 – 03/2018 9 Monate	**Konzepterstellung** **Informationssicherheit, Datenschutz**
Rolle:	Project Information Security Manager
Kunde:	Kapsch TrafficCom
Einsatzort:	Wien
Aufgaben:	Verstehen der Systemarchitektur des Mautprogrammes.

Abstimmen des Sicherheitskonzeptes mit den verantwortlichen Stakeholdern.

Sicherstellen, dass das Sicherheitskonzept mit der Informationssicherheits-Strategie des ISMS zusammenpasst.

Entwickeln einer Informationssicherheits-Risikomanagement Vorgehensweise.

Ableiten eines Betriebskonzepts aus dem Sicherheitskonzept.

01/2017 – 06/2017 **Prozessgestaltung Schwachstellenmanagement**
6 Monate

Rolle: Projektleiter

Kunde: Lufthansa Airlines

Einsatzort: Frankfurt

Aufgaben: Einführen von Prozessen zum Durchführen und Monitoren von:

- Regelmäßigen Schwachstellen-Scans
- Einspielen von Sicherheitspatches
- Austauschs von nicht mehr Hersteller-unterstützen Softwarekomponenten
- Austausch nicht mehr sicheren Verschlüsselungsprotokollen für den Datentransport (speziell Einführung von TLS 1.2)

11/2016 – 12/2016 **Konzepterstellung**
2 Monate (50 %) **„Aircraft affecting Information Security“**

Rolle: Projektleiter

Kunde: Lufthansa AG

Einsatzort: Frankfurt

Aufgaben: Erstellen eines Konzeptes wie das Thema „Aircraft affecting Information Security“ im Konzern umgesetzt werden kann.

Abstimmung mit den relevanten Stellen.

Erstellen einer Präsentation der wichtigsten Ergebnisse als Grundlage für die Erstellung einer Vorstandsvorlage.

01/2016 – 12/2016 **Umsetzung PCI DSS 3.2**
1 Jahr

Rolle: Projektleiter

Kunde: Lufthansa Airlines

Einsatzort: Frankfurt

Aufgaben: Der aktualisierte Standard macht die Implementierung von TLS 1.2 notwendig. Dazu müssen rund 120 IT Systeme angepasst werden.

Gesamtkoordination der notwendigen Einzelmaßnahmen.

Kostenmanagement.

Auditbegleitung.

01/2015 – 12/2015 **Projektleitung PCI DSS 3.0**
1 Jahr

Rolle: Projektleiter

Kunde:	Lufthansa Passage
Einsatzort:	Frankfurt
Aufgaben:	Umsetzung der erweiterten Anforderungen aus PCI DSS 3.0.
	Auditbegleitung.

07/2011 – 12/2014 **Projektleitung PCI DSS**
3 Jahre 6 Monate

Rolle:	Projektleiter
Kunde:	Lufthansa Passage
Einsatzort:	Frankfurt
Aufgaben:	Aufwands-, Termin-, Meilenstein- und Kostenmanagement.
	Budgetverantwortung.
	Risikomanagement.
	Stakeholder-Management.
	Gesamtkoordination der zur Projekterreichung notwendigen Einzelmaßnahmen.
	Inhaltliche Prüfung der umzusetzenden Sicherungsmaßnahmen auf PCI DSS Compliance.
	Erstellen des Projektauftrags, Erstellen des Projektabschlussberichts.
	Auditbegleitung.

01/2009 – 06/2011 **Umsetzung PCI DSS**
2 Jahre 6 Monate

Rolle:	Senior Security Consultant
Kunde:	Lufthansa Passage
Einsatzort:	Frankfurt
Aufgaben:	Das im Vorprojekt erarbeitete Konzept zur Umsetzung von PCI DSS sollte angewendet werden. Dabei musste flexibel auf neue Anforderungen reagiert werden.
	Es wurden Lösungen erarbeitet, um Systemfamilien out-of-scope zu bringen.
	Abstimmung mit den Systemverantwortlichen.
	Vorbereitung von Review Boards.
	Kostenmanagement.

12/2007 – 12/2008 **Vorprojekt PCI DSS**
1 Jahr 1 Monat

Rolle:	Senior Security Consultant
Kunde:	Lufthansa Passage
Einsatzort:	Frankfurt
Aufgaben:	Evaluation von Aufwand und Kosten, um den Sicherheitsstandard PCI DSS (Payment Card Industry Data Security Standard) der Kreditkartenunternehmen bei Lufthansa Passage vollständig zu implementieren.
	Erstellung einer Vorstandsvorlage zur Implementierung des PCI DSS.

07/2007 – 11/2007 5 Monate	**Unterstützung CC-Evaluierung Signaturanwendungskomponente gemäß SigG**
Rolle:	Security Consultant
Kunde:	Authentidate
Einsatzort:	Düsseldorf
Aufgaben:	Die Signaturanwendungskomponente gemäß Signaturgesetz/Signaturverordnung zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen wurde gemäß Common Criteria EAL 4 evaluiert. In diesem Zusammenhang wurden in Java Unit-Tests erstellt, um die Korrektheit der Anwendung nachzuweisen. Außerdem musste die Vollständigkeit der Testabdeckung nachgewiesen werden.
04/2007 – 06/2007 3 Monate	**Erstellung von Sicherheitskonzepten für den Einsatz der elektronischen Gesundheitskarte**
Rolle:	Security Consultant
Kunde:	Authentidate
Einsatzort:	Düsseldorf
Aufgaben:	Erstellung von Sicherheitskonzepten auf Basis ISO 2700x Evaluation diverser Hardware Security Module.
03/2006 – 03/2007 1 Jahr 1 Monat	**Betrieb des Center of Competence Automotive Security**
Rolle:	Senior Security Consultant
Kunde:	BMW AG
Einsatzort:	München
Aufgaben:	Monatliche Durchführung des Steuerkreises CoC Automotive Security. Erstellung von Entscheidungsvorlagen für das Hauptabteilungsleiter-Gremium gemäß den Vorgaben des Auftraggebers. Kommunikation des Automotive Security Know-How an alle beteiligten Abteilungen. Fortschreibung des BMW Gefährdungskatalogs in Abstimmung mit der Stabsstelle für Informationsschutz. Definition des Standardschutzes für Automotive Security in Abstimmung mit der Stabsstelle für Informationssicherheit. Review vorhandener Security-Maßnahmen der Steuergeräteverantwortlichen. Anforderungsmanagement für Security-Maßnahmen der Automotive Security.
08/2005 – 02/2006 7 Monate	**Aufbau des Center of Competence Automotive Security**
Rolle:	Projektleiter
Kunde:	BMW AG
Einsatzort:	München
Aufgaben:	Identifikation und Analyse der Anforderungen an ein CoC Automotive Security.

	Definition der Aufgaben und Beschreibung der Rollen und Prozesse des CoC Automotive Security. Abstimmung mit allen relevanten Ansprechpartnern der beteiligten Abteilungen. Erstellung eines Maßnahmenplans zur Umsetzung des CoC Automotive Security. Umsetzung des Maßnahmenplans und Integration des CoC Automotive Security in die Prozesslandschaft des Auftraggebers. Unterstützung der Projektleitung bei der Implementierung des CoC Automotive Security inklusive Koordination aller beteiligten Stellen.
07/2005 – 07/2005 1 Monat	**Schwachstellenanalyse Fahrzeug Security**
Rolle:	Projektleiter
Kunde:	BMW AG
Einsatzort:	München
Aufgaben:	Durchführung einer Schwachstellenanalyse bezüglich der Sicherheit der derzeit implementierten Lösung "Fahrzeug Security". Skizzierung von Angriffsszenarien. Bewertung der Wirksamkeit der implementierten Sicherheitsfunktionen. Durchführung einer Restrisikoanalyse.
05/2005 – 06/2005 2 Monate	**Steuerung des Projektes Grobkonzept HDD-Update**
Rolle:	Projektleiter
Kunde:	BMW AG
Einsatzort:	München
Aufgaben:	Gesetzlichen Anforderungen bestimmen und Security Anforderungen ableiten. Abstimmung mit allen relevanten Abteilungen.
11/2004 – 04/2005 6 Monate	**Bedrohungs- und Risikoanalyse Fahrzeug Security**
Rolle:	IT Security Consultant
Kunde:	BMW AG
Einsatzort:	München
Aufgaben:	Entwicklung und Erstellung einer Bedrohungs- und Risiko-Analyse auf Basis der VIVA Kriterien (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) für die Security-Architektur des neuesten Fahrzeug-Modells sowohl für die Fahrzeugseite, als auch für die Infrastrukturseite. Mit den relevanten Ansprechpartnern das Risikoprofil der jeweiligen Kunden- und Systemfunktion diskutieren und priorisieren (Schutzbedarfsfeststellung). Das Gesamtrisiko für das Fahrzeug aus den Einzelrisiken der Kunden- und Systemfunktionen ableiten. Das Gesamtrisiko für die Infrastruktur aus den Einzelrisiken der jeweiligen Kundenfunktionen ableiten Festlegung von

Security-Bausteinen, die geeignet sind, die Bordnetzarchitektur abzusichern.

Bestimmen des Restrisikos gemäß der Kundenvorgaben.

Ältere Projekte

- Digital Rights Management for Napster
  Entwurf und Entwicklung einer hochperformanten PKI für 50 Millionen Napster-Nutzer
  Entwurf von ganz neuen Obfuscation Techniken und Integration in die Napster Software, zur Durchsetzung von Digital Rights Management
- Security für SAP R/3
  Entwurf und Entwicklung eines Produktes zur Absicherung der Client/Server Kommunikation von SAP R/3
  Exportrestriktionen machten es für SAP notwendig, eine Schnittstelle in das R/3 System so zu integrieren, dass Drittprodukte die Kommunikationsverschlüsselung realisieren konnten, ohne dass SAP selbst Sicherheitsfunktionalität implementieren würde
  Das Protokoll musste die starke Authentifikation der Anwender gewährleisten und die Client-Server-Verbindung verschlüsseln
  Der Einsatz von Hardware zur Erhöhung der Sicherheit musste möglich sein.
- BaanERP Security
  Entwurf und Entwicklung eines Client-Server-Systems unter Verwendung von signaturgesetzkonformen Hardwarekomponenten zur sicheren Anmeldung an ein Baan ERP-System für das Land Niedersachsen
  Anders als im SAP Fall konnte hier die Integration der Sicherheitsfunktionalität nicht direkt im Baan ERP-System erfolgen
  Die Realisierung wurde sowohl client- als auch serverseitig a ls Middleware ausgeführt
  Clientseitig wurde der Microsoft Protokollstack erweitert und serverseitig agiert die Middleware als Proxy, der erst nach erfolgreicher Benutzerauthentifikation die Verbindung zum BaanERP-Server erlaubt
  Als Hardwarekomponente wurde die SigG-konforme Smartcard der Deutschen Telekom eingesetzt
- Identrus
  Identrus war eine Initiative international agierender Großbanken zum Aufbau einer Public-Key-Infrastruktur im Business-2-Business Umfeld, um den E-Commerce zu fördern
  Zusammen mit Identrus wurden neue Sicherheitsprotokolle für elektronische Geschäftsprozesse entwickelt
  Die dafür entwickelte Software wurde als Referenzsoftware eingesetzt, um wiederum Software von Drittanbietern auf ihre Kompatibilität zu testen
  Patenteinreichungen:
  20020165827: System and method for facilitating signing by buyers in electronic commerce
  20020112156: System and method for secure smartcard issuance
- Secure Online Banking
  Entwurf und Entwicklung eines sicheren Online-Banking-Protokolls für die Dresdner Bank
  Zum Zeitpunkt des Projektes setzten gängige Online-Banking Implementierungen ausschließlich auf PIN/TAN-Verfahren zur Authentifikations- und Transaktionssicherheit
  Digitale Signaturen sind noch heute in diesem Bereich unüblich, dabei eignen sie sich hervorragend um genau diese Funktionalität sicher zu stellen
  In Kooperation mit verschiedenen Firmen wurde auf Basis von digitalen Signaturen ein Online-Banking Protokoll entwickelt, das den kompletten Prozess modelliert, von der Zertifikatsausstellung bis zur Online-Transaktionsabwicklung
- Security in OSI-Management
  Entwurf von Spezifikationen um Zugriffskontrolle in eine bestehende X.700 OSI Managementplattform zu integrieren
  Implementierung von Zugriffskontrolle für OSI Management (X.741)
  Veröffentlichung wissenschaftlicher Papiere über Sicherheitspolitiken und ihrer Repräsentation
  Entwurf von Spezifikationen um Sicherheitspolitiken in eine bestehende OSI Ma-

nagementplattform zu integrieren
Implementierung von Sicherheitspolitiken in eine bestehende OSI Management Plattform