Thomas Hetschold (54)
Senior IT-Security Consultant
CISSP-ISSMP
PMP

Wilhelmshoeher Str. 74
60389 Frankfurt am Main
Germany
Tel. +49-(0)170/57 29 310
thomas@hetschold.de

Qualification

Education:

- Diploma in Computer Science, J. W. Goethe-University, Frankfurt, Germany
- Certified Information Systems Security Professional
- Information Systems Security Management Professional
- Project Management Professional

Skills

Professional Know-how:

- Automotive – 5 years
  Support in implementing a cybersecurity management system (Daimler Truck)
  Creation of security profiles as information security architect (Daimler)
  Support in implementing a tool-based cloud risk process (Daimler)
  Conduct spot checks of cloud projects (Daimler)
  Support in governing the cloud risk process (Daimler)
  Design of an IT security policy for the automotive field (BMW)
  Definition, implementation and operation of the Center of Competence Automotive Security (BMW)
  Creation of a threat- and risk-analysis for the vehicle security architecture (BMW)
  Implementation of a secure SAP R/3 infrastructure (Volkswagen)
- Aviation 9,5 years
  Implementation of Payment Card Industry Data Security Standards (Lufthansa)
  Multiple successful re-certification per PCI DSS (Lufthansa)
  Supporting the implementation of IT-security processes (Lufthansa)
  Risk-analysis for IT systems that affect the aircraft (Lufthansa)
  Concept for flight operations information security (Lufthansa)
- Banking – 3 years
  Development of security protocols for electronic business processes (Deutsche Bank, Dresdner Bank, Bank of America, ABN Amro)
  Development of a security online banking protocol (Dresdner Bank)
- Public administration – 2,5 years
  Development of a threat analysis for automated driving (State of Baden-Württemberg)
  Design of IT security concepts for the deployment of the German electronic health card (several health insurance companies)
  Development of a purchase system according to German signature law (Federal State of Lower Saxony)
  Development of security protocols for the deployment of the German Health Professional Card (ABDA)
- Power – 1 year
  Development of a system for the secure operation control in a nuclear power plant (RWE)
  Implementation of a secure SAP R/3 infrastructure (RWE)
- IT and Telecommunication – 8 years
  Development of a product to secure SAP R/3 systems (SAP)
  Development of security products (Secude, Fillmore Labs)
  Development of access control in an OSI management platform according to X.741 (Deutsche Telekom)
- Media – 1,5 years
  Development of a digital rights management system for a peer to peer file sharing service (DWS/Bertelsmann)
- Transport – 0,75 years

Development of an information security concept and a data privacy concept for a tolling platform (Kapsch)

Professional Competence:

- UNECE R155, ISO 21434
- Tolling processess
- Automotive processes
  E/E development processes
  Production processes
  Service processes
  Logistics processes
- Aviation processes
- Processes of financial services
  Money transfer
- Quality management in the pharmaceutical industry
- IT processes
  PCI DSS
  ISO 2700x
  Documentation according to Common Criteria
  Development processes according to ISO-9000
  Quality management
  Documentation according to ITSec

Specialization

- General data protection directive (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- IT security processes
- IT risk management
- Software development
- Integration of security functionality in existing applications
- Design of e-commerce and e-business protocols
- Design of security policies
- Security protocols (SSL/TLS, GSS)
- Smartcards (PKCS#11, PC/SC, ISO 7816)
- Cryptographic standards and algorithms (PKCS, PKIX)
- Digital rights management
- Process analysis and -modelling

Leadership experience:

- CTO Secude GmbH, Management of Development and Consulting with 30 employees, 7 years
- CEO Fillmore Labs GmbH, 7 employees, 2 years

Project management experience:

- Lufthansa, project management, 7 years
- Secude GmbH, program management, 7 years
- Fillmore Labs GmbH, project management, 2 years
- GMD (Fraunhofer Gesellschaft), 2 years

Miscellaneous:

- Development of a private internet website with more than 1000 participants
- Member of Mensa e.V.

Former Employments

- Since 2004 freelancer (senior security consultant, process design)
- 2003 – 2004 Secude GmbH (CTO)
- 2001 – 2003 Fillmore Labs GmbH (CEO)
- 1996 – 2001 Secude GmbH (CTO)
- 1993 – 1997 GMD – German national research center for information technology GmbH (scientific employee, project manager)
- 1990 – 1993 self-employed (IT consultant, software developer)

Languages

- German
- English (Certificate in Advanced English)

IT Knowledge

- Applications:
  MS Office, MS Project, MS Visio, Confluence, Jira, Service Now, Doors
- Programming languages:
  C++, C, Java, HTML, XML, SOAP, SQL, Pascal, Modula, PLI, Lisp, Prolog
- System software:
  GIT, CVS, Quality Center, Gauss VIP, SAP Basis, Subversion
- Development environments:
  Visual Studio, Eclipse
- Databases:
  DBase III, DBase IV, MySQL, Microsoft Access, Paradox
- Operating systems:
  AIX, FreeBSD, HP UX, Linux, Mac OS, Microsoft Windows, Solaris

Further Education

- Information Security Architect (Daimler)
- PCI SSC Standards Training
- ITIL-Foundation
- Project management of IT projects (CSC Ploenzke)

Projects

Since 01/2021	**Support in implementing a Cybersecurity Management Systems (CSMS)**
Role:	Senior Car Information Security Architect
Customer:	Daimler TSS / Daimler Truck
Site:	Ulm
Tasks:	According to UN Regulation 155 OEMs are required to implement a cybersecurity management system in the future for type approval. This requires them to comply to ISO/IEC 21434. Determine status quo of all vehicle types affected. Extend the vehicle development process to follow the requirements of ISO 21434. Create vehicle TARAs (Threat Analysis and Risk Analysis).
09/2020 – 12/2020 4 months (50%)	**Creation of security profiles as Information Security Architect (ISA)**
Role:	Information Security Architect
Customer:	Daimler
Site:	Stuttgart
Tasks:	Creation of a C4 model and data flow model during analysis of IT systems to identify possibly vulnerabilities and threats as well as determine cloud specific threats. Evaluate threats and risks. Develop appropriate countermeasures to mitigate risks to an acceptable level. Discuss the results with the project team.
07/2020 – 12/2020 3 months (50%)	**Threat Analysis IT security and autonomous Driving**
Role:	Senior Information Security Consultant
Customer:	State of Baden-Württemberg
Site:	Stuttgart
Tasks:	Analysis and identification of new threats through networked and automated driving.

	Preventive measures and the detection of attacks and appropriate countermeasures shall be proposed. Especially new ways to detect criminal offenses shall be considered and also procedures for the traceability of decisions of the automated driving system that are based on machine learning.
10/2018 – 03/2020 18 months	**Sub-project Management Development and Introduction of a tool-based Cloud Risk Process**
Role:	Senior Information Security Consultant
Customer:	Daimler AG
Site:	Stuttgart
Tasks:	Create and implement a concept for the support incl. provider selection. Create and implement a concept to establish a world-wide multiplier structure to complement the support. Create and implement a concept for spot checks to validate projects have complied to the process and have identified and mitigated risks correctly. Support the work package communication.
04/2018 – 12/2019 21 months	**Support in Governance of the Cloud Risk Process**
Role:	Senior Information Security Consultant
Customer:	Daimler AG
Site:	Stuttgart
Tasks:	Validate project documentation for cloud usage. Align risk assessments with IT and legal. Validate that mitigating measures have been implemented in a project (spot checks). Propose process improvements for the cloud risk process and align with the responsible stakeholders. Deploy a tool for governing the cloud risk process.
07/2017 – 03/2018 9 months	**Preparation of a Concept Information Security, Data Privacy**
Role:	Project Information Security Manager
Customer:	Kapsch TrafficCom
Site:	Vienna
Tasks:	Understand the enterprise architecture to be able to deliver an information security concept for the program. Align the security concept with the responsible business stakeholders. Ensure that the information security concept complies with the information security strategy as well as the existing ISMS. Develop an information security risk management approach. Derive from the security concept a security operations concept.

01/2017 – 06/2017 **Process Design Vulnerability Management**
6 months

Role: Project manager

Customer: Lufthansa Airlines

Site: Frankfurt

Tasks: Launch of processes to perform and monitor:

- Regular vulnerability scans
- Installation of security patches
- Exchange of software components no longer supported by the manufacturer
- Exchange of encryption protocols for data transport that are no longer secure (especially introduction of TLS 1.2)

11/2016 – 12/2016 **Preparation of a Concept**
2 months (50 %) **„Aircraft affecting Information Security“**

Role: Project manager

Customer: Lufthansa AG

Site: Frankfurt

Tasks: Preparation of a concept about how „Aircraft affecting Information Security“ can be implemented within the company.

Coordination with all relevant departments.

Preparation of a presentation of the main results as basis for the creation of a board paper.

01/2016 – 12/2016 **Implementation PCI DSS 3.2**
1 year

Role: Project manager

Customer: Lufthansa Airlines

Site: Frankfurt

Tasks: The revised standard requires the implementation of TLS 1.2. Adaption of roughly 120 IT systems is therefore necessary.

Overall coordination of all required individual measures.

Cost management.

Audit support.

01/2015 – 12/2015 **Project Management PCI DSS 3.0**
1 year

Role: Project manager

Customer: Lufthansa Passage

Site: Frankfurt

Tasks: Implementation of the new requirements of PCI DSS 3.0.

Audit support.

07/2011 – 12/2014 **Project Management PCI DSS**
3 years 6 months

Role: Project manager

Customer: Lufthansa Passage

Site: Frankfurt

Tasks:	Scope-, time-, milestone- and cost management. Budget responsibility. Risk management. Stakeholder management. Overall coordination of all required individual measures to fulfil the project objective. Review of the security measures to be implemented regarding PCI DSS compliance. Creation of the project charter, creation of the project closure report. Audit support.

01/2009 – 06/2011 **Implementation of PCI DSS**
2 years 6 months

Role:	Senior Security Consultant
Customer:	Lufthansa Passage
Site:	Frankfurt
Tasks:	Implementation of the concept created within the feasibility analysis regarding PCI DSS. Thereby reacting flexible to new requirements. Solutions were developed to get whole families of systems out-of-scope of PCI DSS. Coordination with system managers. Preparation of review board meetings. Cost management.

12/2007 – 12/2008 **Feasibility Analysis PCI DSS**
1 year 1 month

Role:	Senior Security Consultant
Customer:	Lufthansa Passage
Site:	Frankfurt
Tasks:	Evaluation of effort and cost to implement the security standard PCI DSS (Payment Card Industry Data Security Standard) entirely within Lufthansa Passage. Preparation of a board paper to implement PCI DSS.

07/2007 – 11/2007 **Support the CC-Evaluation of a Signature Application Component according to SigG**
5 months

Role:	Security Consultant
Customer:	Authentidate
Site:	Düsseldorf
Tasks:	The Signature application component fulfilling the German Signature Law to create and verify qualified electronic signatures was evaluated according to Common Criteria EAL 4. In this context, Java unit tests were created to verify the correctness of the application. Furthermore, the completeness of the test coverage had to be proven.

04/2007 – 06/2007 3 months	**Development of Security Concepts for the Deployment of the German Electronic Health Card**
Role:	Security Consultant
Customer:	Authentidate
Site:	Düsseldorf
Tasks:	Development of security concepts according to ISO 2700x.
	Evaluation of several hardware security modules.
03/2006 – 03/2007 1 year 1 month	**Operation of Center of Competence Automotive Security**
Role:	Senior Security Consultant
Customer:	BMW AG
Site:	München
Tasks:	Monthly organization of the steering committee CoC Automotive Security.
	Preparation of decision memos for the board of heads of departments according to the guidelines of the client.
	Communication of the know-how of automotive security to all involved departments.
	Amendment of the BMW threat catalogue in collaboration with the administrative department for information protection.
	Definition of the base protection profile for automotive security in collaboration with the administrative department for information security according to ISO 2700x.
	Review of existing security measures of the responsibles for electronic control units.
	Requirements management for security measures of automotive security.
08/2005 – 02/2006 7 months	**Definition and Implementation of Center of Competence Automotive Security**
Role:	Project manager
Customer:	BMW AG
Site:	München
Tasks:	Identification and analysis of requirements of a CoC Automotive Security.
	Definition of the tasks and description of roles and processes of the CoC Automotive Security.
	Coordination with all relevant contact persons of the involved departments.
	Preparation of an action plan to implement the CoC Automotive Security.
	Enforcement of the action plan and integration of the CoC Automotive Security in the process landscape of the client.
	Support of the project management to implement the CoC Automotive Security and coordination of all involved departments.

07/2005 – 07/2005 1 month	**Vulnerability Analysis of Vehicle Security**
Role:	Project manager
Customer:	BMW AG
Site:	München
Tasks:	Implementation of a vulnerability analysis regarding the security of the currently implemented solution of “Vehicle Security”. Outline of attack scenarios. Evaluation of the effectiveness of the implemented security functions. Implementation of a residual risk analysis.
05/2005 – 06/2005 2 months	**Management of the Project Main Concept HDD-Update**
Role:	Project manager
Customer:	BMW AG
Site:	München
Tasks:	Determine the legal requirements and derive the necessary security requirements. Coordination with all relevant departments.
11/2004 – 04/2005 6 months	**Threat and Risk Analysis of Vehicle Security**
Role:	IT Security Consultant
Customer:	BMW AG
Site:	München
Tasks:	Design and development of a threat- and risk analysis based on CIA criteria (confidentiality, integrity, availability) for the security architecture of the newest vehicle model as well for the vehicle side as for the infrastructure side. Discussion and prioritization of the risk profile with the relevant contact persons of the respective consumer and system functions (security requirements analysis). Derive the overall risk for the vehicle from the single risks of the consumer and system functions. Derive the overall risk for the infrastructure from the single risks of the respective consumer functions. Definition of security components appropriate to secure the bordnet architecture. Determination of the residual risk according to the specifications of BMW.

Older Projects

- Digital Rights Management for Napster
  Design and development of a high performant PKI system for 50 millions of users for Napster
  Design and integration of brand-new obfuscation techniques into the Napster software to enforce digital rights management
- Security for SAP R/3
  Design and development of a product to secure the client/server communication of SAP R/3

Because of export restrictions it was necessary for SAP, to integrate an interface into the R/3 system in a way, that third party products could realize the encryption of the communication channel without the need for SAP to implement the security functionality by themselves
The protocol had to ensure strong authentication of the users and the encryption of the communication channel
The use of hardware to enhance security should be possible

- BaanERP Security
  Design and development of a client/server system that uses signature law compliant hardware components for the secure login to a Baan ERP system for the Federal State of Lower Saxony
  It was not possible to integrate the security functionality directly into the Baan ERP system
  Realization was accomplished as middleware as well on the client side as on the server side
  On the client side the Microsoft protocol stack was extended and on the server side the middleware acts as a proxy which allows the connection to the BaanERP server only after a successful user authentication
  As hardware components signature law comliante smartcards of Deutsche Telekom were used
- Identrus
  Identrus was an initiative of international major banks to establish a public key infrastructure for business-to-business to suport e-commerce
  New security protocols for electonic business processes were designed together with Identrus
  The software developed was being used as reference to test third party software for compliance to the protocols
  Patent submissions:
  20020165827: System and method for facilitating signing by buyers in electronic commerce
  20020112156: System and method for secure smartcard issuance
- Secure Online Banking
  Design and development of a secure online banking protocol for Dresdner Bank
  At the time of the project common online banking implementations used only PIN/TAN techniques for authentication and transaction security
  Digital signatures are still not very common in this area but they are ideally suited to provide this functionality
  In co-operation with several companies an online banking protocol was designed based on digital signatures. This protocol models the entire process from certificate issuing to online transactions
- Security in OSI-Management
  Design of specifications to integrate access control into an existing X.700 OSI management platform
  Implementation of access control for OSI Management (X.741)
  Development of scientific publication about security policies and their representation
  Design of specifications to integrate security policies into an existing OSI management platform
  Implementation of security policies into an existing OSI management platform