Thomas Hetschold (50)
Senior IT-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

Erfahrungsfelder

Branchen-know-how:

- Automotive – 2,5 Jahre
  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 Jahre
  Umsetzung des Payment Card Industry Data Security Standards (Lufthansa)
  Unterstützung bei der Einführung und Umsetzung von IT-Security Prozessen (Lufthansa)
  Durchführung von Risikoanalysen für IT-Systeme mit Aircraftbezug (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
  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)

Erfahrung Fachprozesse, Fachkompetenz:

- Automotive Prozesse
  E/E-Entwicklungsprozesse
  Fertigungsprozesse
  Serviceprozesse
  Logistikprozesse
- Aviation Prozesse

- Finanzdienstleistungsprozesse
  Geldtransfer
- Qualitätsmanagement in der Pharmaindustrie
- IT-Prozesse
  PCI DSS
  ISO 2700x
  Dokumentation nach Common Criteria
  Entwicklungsprozesse nach ISO-9000
  Qualitätssicherung
  Dokumentation nach ITSec

Spezialisierungen / Schwerpunkte

- Payment Card Industry Data Security Standard (PCI DSS)
- IT-Sicherheitsprozesse
- IT-Risikomanagement
- Softwareentwicklung
- Integration von Sicherheitsfunktionalität in bestehende Anwendungen
- Design von E-Commerce und E-Business Protokollen
- Entwurf von Sicherheitspolitiken
- Sicherheitsprotokolle (SSL/TLS, GSS)
- Smartcards (PKCS#11, PC/SC, ISO 7816)
- SAP R/3 Sicherheit (SNC, SSF)
- Kryptographische Standards und Algorithmen (PKCS, PKIX)
- Datenschutz
- Digital Rights Management
- 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:

- Secude GmbH, Programmmanagement, 7 Jahre
- Fillmore Labs GmbH, Projektmanagement, 2 Jahre
- GMD (Fraunhofer Gesellschaft), 2 Jahre

Sonstiges:

- Entwicklung einer privaten Internet-Spieleseite mit über 1000 Teilnehmern
- Mensa-Mitglied

Weiteres zur Person

- seit 2004 selbstständig (Senior Security Consultant, Prozessgestaltung)
- 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)

IT-Kenntnisse

- Anwendungen:
  MS Office, MS Project, Doors
- Programmiersprachen:
  C++, C, Java, HTML, XML, SOAP, SQL, Pascal, Modula, PLI, Lisp, Prolog
- Systemsoftware:
  CVS, Quality Center, Gauss VIP, SAP Basis, Subversion
- Entwicklungsumgebungen:
  Visual Studio, Eclipse
- Datenbanken:
  DBase III, DBase IV, MySQL, Microsoft Access, Paradox
- Betriebssysteme:
  AIX, FreeBSD, HP UX, Linux, Mac OS, Microsoft Windows, Solaris

Fortbildungen

- PCI SSC Standards Training
- ITIL-Foundation
- Projektleitung IT Projekte bei CSC Ploenzke

Projektbeispiele

- Projektleitung bei der Konzeption und Umsetzung der Anforderungen aus dem Payment Card Industry Data Security Standard (PCI DSS) für die Lufthansa Airlines. Durchführung der Budgetplanung. Erfolgreiche Zertifizierung gemäß PCI DSS sowie Re-Zertifizierung. Erstellen von Schutzbedarfsfeststellungen und Risikoanalysen. Prozessberatung für die Erstellung von Schutzbedarfsfeststellungen, Risikoanalysen und die Umsetzung des Identity Management in Anlehnung an ISO 2700x. Unterstützung bei der Einführung eines Security Monitoring
- Erstellung von Sicherheitskonzepten für den Einsatz der elektronischen Gesundheitskarte
  Erstellung von Sicherheitskonzepten auf Basis ISO 2700x
  Evaluation diverser Hardware Security Module
- Betrieb des Center of Competence Automotive Security
  Erstellung einer IT-Security Policy für den Automotive Bereich
  Monatliche Durchführung des Steuerkreises CoC Automotive Security
  Erstellung von Entscheidungsvorlagen für das Hauptabteilungsleiter-Gremium gemäß der Vorgaben des Auftraggebers
  Kommunikation des Automotive Security Know-hows 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 auf Basis ISO 2700x
  Review vorhandener Security-Maßnahmen der Steuergeräteverantwortlichen
  Anforderungsmanagement für Security-Maßnahmen der Automotive Security
- Definition und Aufbau des Center of Competence Automotive Security
  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
- Bedrohungs- und Risikoanalyse Fahrzeug Security
  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 BMW Vorgaben
- 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 als 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 Managementplattform zu integrieren
  Implementierung von Sicherheitspolitiken in eine bestehende OSI Management Plattform