Dipl.-Informatiker Hartmut Goebel

Spezialist für Cyber-Security-Management mit starkem technischen Hintergrund

Mein Angebot

- Erstellen von Risikoanalysen
- Erarbeiten von Security-Policies
- Planen und Prüfen von Sicherheitsarchitekturen
- Konzipieren & Aufbauen von Information Security Management Systemen (ISMS)
- Entwickeln von Strategien für Informationssicherheit
- Interims-Management für Informationssicherheit

Für diese Aufgaben stehe ich Ihnen tageweise oder für längere Einsätze zur Verfügung.

Ihr Nutzen

- Sie erhalten konkrete Lösungen, die zu Ihren Bedürfnisse und Ihren Unternehmenszielen passen.
- Ich empfehle Ihnen nur Maßnahmen, die sich umsetzen und in der Praxis betreiben lassen.
- Sie profitieren von meinen Erfahrungen aus anderen Unternehmen.
- Sie sind für zukünftige Anforderungen gerüstet.
- Sie nutzen mein aktuelles Wissen und über 25 Jahre Erfahrung.

Kontakt

Hartmut Goebel
Salamanderweg 5, 84034 Landshut
Mobil: 0175 / 29 78 072
h.goebel@goebel-consult.de

www.goebel-consult.de

Meine Kompetenzen

Erfahrungen

- Seit über 20 Jahren in der IT- und Cyber-Security tätig
- Umfangreiche Kenntnisse der einschlägigen IT-Security Standards wie ISO 27001, BSI IT-Grundschutz und zugehöriger Methoden sowie gesetzlicher Anforderungen (z.B. BSDG, EU-DSGVO)
- Profunde technische Kenntnisse in Netzwerk-Sicherheit, Web-Application, Protokolle & Standards, Datenbanken, Verschlüsselung, Unix
- Langjährige Erfahrung im Programmieren
- Händchen für Prozesse und Organisation
- betriebswirtschaftliche Kenntnisse
- Diverse Vorträge und Veröffentlichungen in renommierten Zeitschriften

Ausbildung

- Diplom-Informatiker (univ.)
- CISSP - Certified Information Systems Security Professional (ISC)²
- CSSLP - Certified Secure Software Lifecycle Professional (ISC)²
- Certified ISO 27001 Lead Implementer (PECB)
- ITIL Foundation Zertifikat
- Fortbildungen zu Management und Personalführung

Persönliche Stärken

- kann sehr gut abstrahieren und strukturieren
- sehe Dinge, die andere nicht sehen
- bin durchsetzungs-, konflikt- und teamfähig
- stelle auch unbequeme Fragen
- habe eine professionelle und zuverlässige Arbeitsweise
- treffe Entscheidungen

Unternehmer

- Aufsichtsratsvorsitzender und langjähriges Aufsichtsratsmitglied in unterschiedlichen Genossenschaften
- (Mit-) Gründer mehrerer Genossenschaften und Aufbau der Unternehmens-IT
- Gründungsberatung von Genossenschaften

Was mich besonders macht

- bin „Überzeugungstäter“ – als Informatiker, Programmierer und System-Admin.
- bin gut vernetzt mit anderen Praktikern der Informationssicherheit: 2010-2018 organisierte ich die Konferenz „IT Security live“ für die ACM (Association of Computing Machinery). Ich bin aktives Mitglied im deutschen Chapter des (ICS)² und beteilige mich an dessen regelmäßigen Treffen.
- weiß, wovon ich rede: Beschäftige mich seit meiner früher Jugend mit Computern und experimentiere noch heute laufend mit Neuem
- akzeptiere nicht jedes „geht nicht“: Ich weiß aus Erfahrung, dass es sehr oft doch eine Lösung gibt.
- bin immer am Ball: Lese regelmäßig mehrere Fachzeitschriften, unzählige Mailinglisten, Newsticker und Blogs und bin damit über die neusten Trends und Techniken auf dem Laufenden.
- bin Praktiker: Ich betreibe meine eignen IT-Systeme und entwickle Open-Source-Software.
- lege ich Hand an: Hilft es dem Kunden, schreibe ich ein paar Makros oder Scripte.
- beschäftige mich mit Auswirkungen der IT in der Gesellschaft: Datenschutz, Schutz der Privatsphäre und Überwachung sind meine Themen. Daher bin ich aktives Mitglied bei Digitalcourage e.V.

Kurz-Vita

seit 2003	Freiberuflicher Spezialist für Informations-Sicherheit	
2000–2003	Aufbau und Leitung der Consulting Abteilung (angestellt)	Details »
1998–2000	Festanstellung als System Engineer, Schwerpunkte Security, Banyan Vines und Unix	
1990er-jahre	Studium: Informatik und Philosophie	

Weiteres

2019-2021	Mitgründer einer SoLaWi-Genossenschaft, Aufsichtsratsvorsitzender und CTO Regionalkollektiv eG (http://regionalkollekitv.de)
2019	Gründungsberatung der Bürgergenossenschaft Landshut; Mitgründer
2006-2013	*Aufsichtsrat* bei 7-it eG, einer IT-Vertriebsgenossenschaft (https://7-it.de)
2010-2018	Mitinitiator und Tagungsleiter der Workshopreihe "IT-Security live" des German Chapter of the ACM
ca. 2004-2010	Mitgründer und Sprecher das Arbeitskreises Selbständige in der Regionalgruppe Nbg. der Gesellschaft für Informatik (GI e.V.)

Projektübersicht

Informationssicherheits-Management – seit 2008

2020-2022 Architekt für Verschlüsselungs-Software	Details »
2018-2019 Patch Management Improvement	Details »
2017 Interner Audit zu „Thread and Vulnerability Management“	Details »
2017 Erstellen von Security-Richtlinien	Details »
2013–2017 Erarbeiten neuer Policies und Technischer Richtlinien	Details »
2015/2016 Erstellen von Risikoanalysen und Cloud-Konzepten für ein DAX-Unternehmen	Details »
seit 2014 Beratung zu Datenschutz, Privatsphäre und „Digitaler Selbstverteidigung“	Details »
2014 Strategie-Workshop für neue Security-Produkte	Details »
2012–2013 Informationssicherheitsbeauftragter im Projekt	Details »
2012 Erstellen von Risikoanalysen für ein DAX-30-Unternehmen	Details »
2012 Strategie-Beratung zum Aufbau eines ISMS bei einer agilen Internetplattform	Details »
2011 Erarbeiten einer Policy für die Reorganisation von Netzwerk-Diensten	Details »
2011 Erstellen von Policies und Aufbau eines ISMS incl. Organisation im Mittelstand	Details »
2009 Entlasten des IT Security Officers (Security Management)	Details »
2008 Konzept für Sicherheits-Audit bei 200 Standorten	Details »

(Technische) IT-Sicherheit – seit 2006

Audits, Schwachstellentests (für bis zu 140.000 Geräten), Sicherheitskonzepte, Architekt, etc.

Liste der Projekte in diesem Bereich »

(Technische) Netzwerk-Sicherheit – 2003-2013

Netzwerkanalysen, Betriebskonzepte, Problemmanagement, Firewalls, IPS/IDS, DNS, Mail, etc.

Liste der Projekte in diesem Bereich »

Softwareentwicklung

seit ca. 2000	Entwickler diverser kleinerer und größerer Open-Source-Projekte– eigenen und fremde, bevorzugt in Python. Diese Tools setze ich immer wieder in meinen technischen Projekten ein.
2011—2019	Maintainer der Software PyInstaller (www.pyinstaller.org)
1990er-Jahre	Compilerbau Modula-2 und Oberon (kommerziell, Industriequalität)
1980er-Jahre	Softwareentwicklung und Hardwarebasteleien mit Commodore 3032, C-64, Amiga

Projekte im Detail

2020-2022 Architekt für Verschlüsselungs-Software

Für einen Anbieter einer neuartigen Verschlüsselungs-Software war ich als Architekt für das Banking Produkt tätig. Die Aufgabe umfasste die Software-Architektur, Deployment, Dokumentation, Kundenbetreuung. Zudem war ich zuständig für Design und Entwicklung der Softwarekomponente „Enterprose Toolkit“ sowie

Rolle:	Architekt, Entwickeln, Berater Erfahrung von 30 Jahren IT und Software-Entwicklung einbringen
Besonderes:	IBM MQ, Swift, ISO 20022, MT FIN (ISO 15022), Crypto

Branche: Software ↑Projektübersicht

2018-2019 Patch Management Improvement

Ein DAX-30-Unternehmen wollte die Patch-Management-Prozesse in den einzelnen Bereichen verbessern. Innerhalb des Projektteams aus zwei, teilweise auch vier, Beratern war ich zuständig für: Best-practice evaluieren, Marktübersicht Patch-Produkte erstellen und Produkt analysieren, Greenfield-Studies erstellen, Ist-Analysen der bestehenden Prozesse erstellen, Verbessungsvorschläge erarbeiten, neues Prozessdesign und deren Bescheibung, Traininsmaterial erstellen, Trainings durchführen, etc.

Rolle:	Berater
Besonderes:	Weltweite, heterogene Landschaft, > 350.000 Clients, > 40.000 Server Als einziger von fünf Beratern während der gesamten Projektlaufzeit dabei

Branche: Industrie ↑Projektübersicht

2017 Interner Audit zu „Thread and Vulnerability Management“

Für ein Unternehmen der Supply-Chain habe ich einen internen Audit des „Thread and Vulnerability Management“ Prozesses erstellt, Verbesserungsvorschläge erarbeitet und die Ergebnisse dem CISO präsentiert.

Rolle:	Berater / Auditor

Branche: Supply-Chain, Handel, Dienstleitung ↑Projektübersicht

2017 Erstellen von Security-Richtlinien

Als Vorbereitung für den ISO-27001-Audit habe ich für ein Unternehmen der Supply-Chain Security-Richtlinien erstellt. Da der bisherige Berater ausgefallen war, musste ich binnen weniger Tage etwas brauchbares „aus dem Hut zaubern“ – was mir gelungen ist.

Rolle:	Berater
Besonderes:	Nur wenige tage Zeit

Branche: -Chain, Handel, Dienstleitung ↑Projektübersicht

2013–2017 Erarbeiten neuer Policies und Technischer Richtlinien

Das genossenschaftliches Rechenzentrum, für das ich schon 2011/2012 gearbeitet habe, stellt seine bestehende Netzstruktur komplett um. Das Ziel ist, viele „Mikro-Perimeter“ aufzubauen. Hier gilt es, sinnvolle Regeln zu erarbeiten, nach denen die Netzaufteilung gestaltet werden soll, und deren Begründung zu dokumentieren. Außerdem sollte bislang dezentral Geregeltes in die nächste Version der unternehmensweiten Policy aufgenommen werden und viele technische Richtlinien erstellt werden.

Im Laufe des Projekts wurde ich dann beauftragt, Policies für andere Themen sowie technische Richtlinien zu entwickeln. Für Teilaufgaben berichtete ich direkt an den CISO.

Rolle:	Berater
Aufgaben:	- Inhalte der neuen Sicherheitsrichtlinie entwickeln (gemeinsam mit dem intern Verantwortlichen) - Erstellen und Abstimmen der Sicherheitsrichtlinie und der technischen Richtlinien - Erstellen eines neuen Prüf-Fragebogens zur Risikobewertung - Erstellen eines neuen Administrations-Konzepts - Erweitern und überarbeiten der alten Policy für die Reorganisation von Netzwerk-Diensten - Unterstützung bei Sicherheitsprüfungen - Mitarbeit beim Audit-Konzept
Besonderes:	- intensive 2-Tages-Workshops zu Zweit - Mindmaps als Werkzeug zum Erstellen unterschiedlicher „Sichten“ der Dokumente

Firmengröße: ca. 5900 Personen; Branche: Informationstechnik ↑Projektübersicht

2015/2016 Erstellen von Risikoanalysen und Cloud-Konzepten für ein DAX-Unternehmen

Das Unternehmen suchte Unterstützung für das Risk-Management-Team. Ich habe Analysen erstellt, unter welchen Voraussetzungen streng vertrauliche Daten in Cloud-Services verarbeitet werden könnten und welche Maßnahmen dafür nötig wären. Hierzu habe ich einen Anforderungen und einen Fragebogen für Lieferanten erstellt. Zusammen mit der Vertragsabteilung habe ich die Anforderungen in einen Vertragsanhang gegossen.

Rolle:	Berater
Aufgaben:	- Risikoanalysen, insb. zu Cloud-Diensten - Erarbeiten von Anforderungen an Cloud-Provider für verschiedenen Vertraulichkeitsstufen von Daten - Erarbeiten eines Fragebogens an Cloud-Provider - Erarbeiten der Vertragsbestandteile für Cloud-Services - Überarbeiten des automatischen Reportings

Firmengröße: ca. 8.500 Personen (in D); Branche: Halbleiterindustrie ↑Projektübersicht

seit 2014 Beratung zu Datenschutz, Privatsphäre und „Digitaler Selbstverteidigung“

Seit 2014 bin ich für Digitalcourage e.V. als technischer Experte ehrenamtlich tätig. Digitalcourage setzt sich ein für Datenschutz, Privatsphäre und gegen Überwachung. Wir untersuchen Anwendungen daraufhin, ob die sie Privatsphäre der Benutzer beeinträchtigen und Entwickeln daraus Empfehlungen zur „Digitalen Selbstverteidigung“.

In diesem Zusammenhang beschäftige ich mich auf immer wieder mit gesetzlichen Regelungen, z.B. der EU Datenschutzgrundverordnung (EU-DSGVO, engl. General Data Protection Regulation, GDPR).

Besonderes:
- NGO (Nicht-Regierungs-Organisation)
- viele, auch mobile Plattformen
- Zielgruppe: NGOs und Endverbraucher

↑Projektübersicht

2014 Strategie-Workshop für neue Security-Produkte

Ein mittelständisches Unternehmen suchte Ideen, weitere IT-Security-Produkte zu entwickeln, die zum bestehenden Portfolio und zur Unternehmenskultur passen. Im Rahmen eines Workshops mit vier anderen Experten stellte ich mein Know-How und meine Kenntnisse über Markt und Kunden bereit.

↑Projektübersicht

2012–2013 Informationssicherheitsbeauftragter im Projekt

Für eine neue Forschungsabteilung in China werden die IT-Infrastruktur und die Anwendungen aufgebaut. Dabei sollen der Informationsschutz und die IT-Sicherheit früh berücksichtigt werden, ehe Strukturen in Stein gegossen werden. Zudem ist ein bestehender Freigabeprozess zu verbessern, und für die Beteiligten transparent darzustellen.

Rolle: Berater, Sicherheitsbeauftragter

Aufgaben:
- Beraten der Teil-Projekte und Anwendungsentwicklung zur IT-/Info-Sicherheit
- Erstellen von Schutzbedarfsfestellungen, Risiko- und Sicherheitsanalysen sowie Sicherheitskonzepten
- Durchdringen und Überarbeiten des Freigabeprozesses

Besonderes:
- neu strukturieren des Genehmigungs-Prozesses
- Sicherheit bei UCS/Siemens Teamcenter

Firmengröße: Konzern; im Projekt ca. 200; Branche: Automotive

↑Projektübersicht

2012 Erstellen von Risikoanalysen für ein DAX-30-Unternehmen

Unterstützung beim Erstellen von Risikoanalysen mit ISF IRAM für Bedrohungen und Schwachstellen und FMEA für die Bewertung der Maßnahmen..

Rolle: Berater

Aufgaben:
- Erstellen von Risikoanalysen (mit ISF IRAM und FMEA)
- Vergleichende Bewertung von Maßnahmen mit anderen Unternehmen

Firmengröße: ca. 8.500 Personen (in D); Branche: Halbleiterindustrie ↑Projektübersicht

2012 Strategie-Beratung zum Aufbau eines ISMS bei einer agilen Internetplattform

Das Unternehmen betreibt einen Internetplattform und plant einen Release-Zyklus von wenigen Stunden. Als Konzerntochter unterliegt es harten Vorgaben, die für dieses Unternehmen angepasst werden müssen. In einem Workshop erarbeitete ich mit dem IT-Leiter eine Strategie zum Aufbau eines ISMS, das zur Unternehmenskultur passt und gleichzeitig den Anforderungen der Konzernmutter gerecht wird.

Rolle: Strategie-Berater

Aufgaben:
- Strategie zum Aufbau eines ISMS entwerfen
- Meilensteinplan und Aufwandsschätzung erstellen

Firmengröße: ca. 100 Personen, Konzerntochter; Branche: Internetplattform ↑Projektübersicht

2011 Erarbeiten einer Policy für die Reorganisation von Netzwerk-Diensten

Ein genossenschaftliches Rechenzentrum plante Netzwerk-Dienste zu zentralisieren. Hier galt es, die „aus dem Bauch“-Regeln in eine Policy zu überführen, um die Entscheidungen nachvollziehbar und besser begründbar zu machen.

Rolle: Berater

Aufgaben:
- Workshops vor- und nachbereiten
- Inhalte der Policy entwickeln (gemeinsam mit dem intern Verantwortlichen)
- Ergebnisse strukturieren und als Policy-Dokument formulieren

Besonderes:
- intensive 2-Tages-Workshops zu Zweit

Firmengröße: ca. 5900 Personen; Branche: Informationstechnik ↑Projektübersicht

2011 Erstellen von Policies und Aufbau eines ISMS incl. Organisation im Mittelstand

Für ein mittelständisches Unternehmen sollte anfänglich lediglich eine IT-Security-Policy erstellt werden. Es stellte sich aber schnell heraus, das auch das Leitbild, die Strategie und die Organisation der Informationssicherheit nicht geklärt sind. Hierzu gehörte auch, die Rolle des Informationssicherheitsbeauftragten (ISO) zu definieren, dessen Rechte und Aufgaben und die Zusammenarbeit innerhalb des Unternehmens festzulegen.

Rolle: Berater

Aufgaben:
- Bestandsaufnahme bereits gelebter Security-Maßnahmen
- Erarbeiten der Security-Policy auf dieser Basis
- Einbinden unterschiedlichen Stakeholder
- Entwerfen des Leitbild, der Security-Strategie und der Organisation
- Entscheidung der Geschäftsführung herbeiführen

Firmengröße: ca. 750 Personen; Branche: Telekommunikation ↑Projektübersicht

2009 Entlasten des IT Security Officers (Security Management)

Der IT Security Officer benötigte Entlastung, um das neu zusammengestellte Team aufbauen zu können. Ich übernahm binnen weniger Tagen eigenverantwortlich alle typischen Aufgaben eines Security Officers. Dazu gehörten Erstellen von Konzepten und Präsentationen, Neugestalten von Prozessen, Bearbeiten von Security Incidents, Beratung der Projektteams im Fachbereich, Durchführen von Projekt- oder Vertragsreviews sowie der Know-how-Transfer zu den neuen Teammitglieder.

Ich arbeitete an Themen wie einem neuen Schwachstellen- und Patch-Prozess, der Fortschreibung der Security-Policy, der Schwachstellen-Bewertung (CVSS), der Benutzer-Anleitung für Verschlüsselung, der Team-Organisation, einem Blueprint für Java-Anwendungen, Kerberos u.a.

Firmengröße: ca. 12.000 Personen (in D); Branche: Finance/Versicherung ↑Projektübersicht

2008 Risikoanalyse für die Umstellung auf VPN (nach BSI-Grundschutz)

Eine Bank will die Anbindung der Filialen nicht mehr über das MPLS-Netz des Rechenzentrums anbinden, sondern kostengünstig über DSL und IPSec-VPN. Die Risikoanalyse sollte dem Vorstand Gewissheit geben, ob Vertraulichkeit, Verfügbarkeit und Integrität erhalten bleiben. Ich führte dieses Projekt in Eigenverantwortung durch. Der Vorstand erhielt hiermit eine Entscheidungsgrundlage und die Administratoren einen priorisieren Maßnahmenkatalog.

Rolle: Berater
Aufgaben:
- Erstellen der Risikoanalyse
- Abgeben einer Empfehlung als Entscheidungsgrundlage

Besonderes:
- Baustein für das BSI Grundschutzhandbuch/Grundschutzkataloge entwickelt

Branche: Banken/Finance ↑Projektübersicht

2008 Konzept für Sicherheits-Audit bei 200 Standorten

Nach dem kompletten Neuaufbau eines komplexen Netzwerks mit circa 200 Standorten sollte eine Sicherheitsprüfung durchgeführt werden. Die besondere Herausforderung dieser Sicherheitsprüfung bestand darin, dass jeder Standort von einer Firewall sowie einem IPS abgesichert ist, was die Ergebnisse stark verzerren kann. Die Sicherheitstests mussten demnach so konzipiert werden, dass sie sinnvolle und aussagekräftige Ergebnisse lieferten.

Ich entwickelte die Sicherheitsprüfung und die Vorgehensweise und dokumentierte beides. Der Endkunde war damit in der Lage, die Endabnahme selbst durchzuführen.

Firmengröße: bis 50.000 Personen, Abteilungsgröße: bis 50 Personen ↑Projektübersicht

Projekte zu (technischer) IT-Sicherheit – seit 2006

- **2015 Sicherheitsanalyse/Audit bei einer Volks- und Raiffeisenbank**

  Eine Bank betreibt ein CRM-System, auf das einige Benutzer sehr viele Rechte haben. Ich sollte untersuchen, ob das Linux-System nach dem Stand der Technik installiert ist und betreiben wird und ob z.B. Tätigkeiten revisionssicher protokolliert werden. Hierzu habe ich das System und dessen Konfiguration untersucht und die Ergebnisse in einem Bericht zusammengestellt.

  Firmengröße: 1.000; Branche: Banken/Finance ↑Projektübersicht

- **Software-Audits für Abnahmetests**

  Im Rahmen des Abnahmetests von Anwendungen war unter anderem die „Sicherheit“ zu testen. Dies reichte vom Prüfen der Sicherheits- und Datenschutzkonzepte über Prüfen der korrekten Installation (nach Konzernvorgaben und best-practice) bis zur Suche von Lücken in der Anwendung.

  Rolle: Pen-Tester und Wissensvermittler
  Aufgaben:
  - Sicherheitsanalysen und Pen-Tests durchführen
  - Grundlagen und Tests für Webshere MQ erarbeiten.
  - Dem Team Ideen und Wissen liefern.

  Firmengröße: Konzern (in D); Branche: Telekomunikation ↑Projektübersicht

- **Schwachstellen-Test für Massen von Geräten – Design und Implementierung**

  In einem Netzwerk sollen rund 80.000 Geräte auf Schwachstellen untersucht werden. Wegen der Größe des Netzes schied ein kommerzieller Anbieter aus. Ich entwickelte ein datenbankgestütztes System, um Geräte(-klassen) für Scan-Aufträge auszuwählen. Scan-Aufträge werden dann automatisch an entfernte Sensoren (Slave-Scanner) zu übermitteln, die Ergebnisse eingesammelt und ausgewertet. Bei Bedarf werden ebenfalls automatisch Tickets im Trackingtool angelegt, die alle nötigen Informationen und Links auf den Report enthalten.

  Rolle: Architekt und Entwickler; Firmengröße: ca. 150.000 Personen (in D); Branche: Logistik ↑Projektübersicht

- **Projektleitung und Konzept zur Beseitigung von „Altlasten“ im Netzwerk**

  In einem Netzwerk mit rund 140.000 Geräten sollen alle Geräte, die bislang nicht in den obligatorischen Sicherheitsprozesse eingebunden waren, identifiziert und auf ihre Sicherheitsrelevanz überprüft werden. Viele Parameter des Projekts waren hierbei unklar: Etwa die auch nur ungefähre Größenordnung der bekannten und unbekannten Systeme im Netz oder die möglichen Datenquellen für Bestands- und Live-Daten.

  Ich erstellte ein Konzept, um die betroffenen Geräte im Netz ausfindig zu machen. Daran anschließend entwickelte er aus den gesammelten Daten ein dreistufiges Prüfkonzept: Es beschreibt die Methodik und Vorgehensweise, die benötigte Projekt-Infrastruktur und einen Projektplan. Anhand dieser Vorgaben ist der Kunde in der Lage, das Hauptprojekt zu budgetieren und selbständig durchzuführen.

  Rolle: Teilprojektleiter; Firmengröße: ca. 150.000 Personen (in D); Branche: Logistik ↑Projektübersicht

- **Sicherheits-Audit bei einer Bank, orientiert am BSI-Grundschutz-Handbuch (BSI GSHB), incl. Penetrationstest**

  Branche: Finance/Banken ↑Projektübersicht

- **Machbarkeitsstudie: SAP WebAS ohne DMZ, IPSec/ipfilter**

  Meine Aufgaben in diesem Projekt waren: die geänderte Sicherheitsarchitektur bewerten, Architektur erarbeiten, Machbarkeit prüfen, Risikobewertung abgeben, Projektplan erstellen, und ein Review des Berichts.

  Firmengröße: ca. 38.000 Personen; Branche: Finance/Versicherung ↑Projektübersicht

- **Sicherheitsüberprüfung nach BSI-Grundschutzhandbuch (BSI 100-1)**

  Rolle: Projektleiter und Teamleiter des Audit-Teams; Branche: Finance/Banken

- **Rechtekonzept für ein Content-Management-System**

  Für das Redaktionssystem des Online-Auftritt einer Zeitschrift entwickelte ich ein rollenbasiertes Rechtekonzept.

  Branche: Verlag ↑Projektübersicht

- **Sicherheitsüberprüfung eines Windows-Netzwerks**

- **Sicherheitsüberprüfungen/Audits auf GNU/Linux und Unix-Servern, incl. Suche nach schwachen Passwörtern**

Projekte zu (technischer) Netzwerk-Sicherheit – 2003–2013

- **Trainer für IT-Sicherheit und Netzwerksicherheit (2003 – 2010)**

  Ich vermittelte Wissen zu Netzwerk-Grundlagen, Hacking, Angriffstechniken und Verteidigungsmöglichkeiten, etc. Ein Teil der Kurse war von mir selbst entwickelt.

  ↑Projektübersicht

- **Netzwerkanalyse in einer Privatklinik**

  In einer Privatklinik musste das bislang undokumentierte Netzwerk analysiert und dokumentiert werden, Alle, auch bislang unbekannte, Geräte im Netz waren aufzuspüren, unbekannte Geräte identifizieren, und eine Geräteliste zu erstellten. Hierfür nutzte ich die Tools, die ich bereits für frühere Projekte (siehe unten) entwickelt hatte.

  Branche: Healthcare ↑Projektübersicht

- **Scripte für automatische Konfiguration und Qualitätssicherung**

  In ca. 200 Standorten mussten Cisco-Komponenten (um-)konfiguriert und die Qualität gesichert werden. Hierzu habe ich einige Scripte erstellt, die dies schnell erledigten und die Fehlerquote reduzieren, sowie weitere Scripte zur Qualitätssicherung, beispielsweise um die Ist-Daten, die Konfig-DB und den DNS mit dem Konzept abzugleichen.

  Firmengröße: Bis 50.000 Personen; Abteilungsgröße: Bis 50 Personen ↑Projektübersicht

- **Konzept und Implementierung ipfilter/IPSec für HP-UX**

  Ich erstellte das Konzept und klärte die sicherheitsrelevanten Fragen mit dem Information Security Office (ISO). Als Lösung implementierte ich ausgeklügelte Scripte, die mehre Open-Source-Programme verbinden und sicherstellen, das Änderungen revisionssicher vorgenommen werden.

  Firmengröße: ca. 38.000 Personen; Branche: Finance/Versicherung ↑Projektübersicht

- **Problemmanagement bei einem Log-Analyse-System (SIEM)**

  Das SIEM lieferte nicht die gewünschte Performance . Ich kreiste die Probleme ein und versuchte, sie zusammen mit dem Hersteller zu lösen.

- **Migrationsplanung eines komplexen Netzwerkes**

  Ich implementierte ein Tool, um alle erreichbaren Komponenten automatisch zu inventarisieren. Die Daten Geräte werden per SNMP, Telnet- und SSH-Login abgefragt.

- **Betriebsübernahme eines Intrustion-Prevention Systems (IDS/IPS)**
- **Studie und Konzept zum Einsatz von VPN (Entscheidungsgrundlage)**
- **Systematische Analyse einer komplexen DMZ-Umgebung**
- **Umstellung und Erweiterung der Mail- und DNS-Infrastruktur im Firewall-Bereich**

↑Projektübersicht

Aufbau und Leitung der Consulting Abteilung – 2000–2003, angestellt

Meine Aufgabe in dieser Festanstellung war es, eine Consulting-Abteilung mit Schwerpunkt IT-Security aufzubauen und zu leiten. Die beinhaltet konzeptionelle, strategische Planungen ebenso wie Personalführung und Engineering.

Weitere Themen waren:

- Entwickeln eines Businessplans (Marktanalyse, Konkurrenz-Analyse, Marketing, Strategie-Entwicklung, etc.)
- Entwicklung und Fortschreibung von Qualitätsstandards für Firewall-Projekte (Checklisten, etc.)
- Produktentwicklung "Managed VPN"
- Einführung eines webbasierten Dokumenten-Management-Systems (incl. Konzeption der Ablage- und Rechte-Struktur)
- Vorträge und Workshops zu Themen Rund um IT-Sicherheit

↑Projektübersicht

Ältere Projekte

Seit ca. 2000	Entwickler und Maintainer diverser Python-Bibliotheken und Tools
1998—2000	Festanstellung als System Engineer, Schwerpunkte Security, Banyan Vines und Unix
1990er	Compilerbau Modula-2 und Oberon (kommerziell, Industriequalität)
	Neben den Studium habe ich viel mit den spannenden neuen Techniken Web, Internet, E-Mail, UUCP, etc. ausprobiert. Erste Erfahrungen mit Verschlüsselung und PGP.
1980er	Softwareentwicklung und Hardwarebasteleien mit Commodore 3032, C-64 und Amiga
	Die Debatte um die Volkszählung 1987 sensibilisiert mich für Datenschutz..
1979	kam der erste Computer in unser Haus, ein Commodore 3008, getarnt als PET – der schon bald aufgerüstet wurde :-)

↑Projektübersicht