Dipl.-Informatiker Hartmut Goebel

Experte für IT-Security-Management

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 14 Jahren 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 14 Jahren im der IT-Security tätig
- Umfangreiche Kenntnisse der einschlägigen IT-Security Standards wie ISO 27001, BSI Grundschutz und zugehöriger Methoden sowie gesetzlicher Anforderungen
- 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
- Weiterbildungen in den Bereichen Moderation, Präsentation, Projektmanagement

Persönliche Stärken

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

Ausgewählte Projekte

seit 2014	Technische Beratung zu Privatsphäre und „Digitaler Selbstverteidigung“	Details >>
seit 2013	Erarbeiten einer neuen Policy für das Umorganisieren des Netzwerks	Details >>
2012	Informationssicherheitsbeauftragter im Projekt	Details >>
	Erstellen von Risikoanalysen	Details >>
	Strategie-Beratung zum Aufbau eines ISMS bei einer agilen Internetplattform	Details >>
2011	Erarbeiten einer Policy für die Reorganisation von Netzwerk-Diensten	Details >>
	Erstellen von Policies und Aufbau eines ISMS incl. Organisation im Mittelstand	Details >>
2010	Software-Audits	Details >>
	Schwachstellen-Test für Massen von Geräten – Design und Implementierung	Details >>
2009	Projektleitung und Konzept zur Beseitigung von „Altlasten“ im Netzwerk	Details >>
	Entlastung des IT Security Offices	Details >>
2008	Einführung verschlüsselter E-Mail für Vorstand und Aufsichtsrat	Details >>
	Risikoanalyse für die Umstellung auf VPN	Details >>
	Sicherheits-Audit und Qualitätssicherung bei 200 Standorten	Details >>
2007	Sicherheits-Audit bei einer Bank	Details >>
	Konzept und Implementierung ipfilter/IPSec für HP-UX	Details >>
	Machbarkeitsstudie: SAP WebAS ohne DMZ	Details >>
2006	Sicherheitsüberprüfung nach BSI-Grundschutz	Details >>
	Sicherheitsüberprüfung eines Windows-Netzwerks	Details >>
2005	Migrationsplanung eines komplexen Netzwerkes	Details >>
	Betriebsübernahme eines Intrustion-Prevention Systems	Details >>
	Studie und Konzept zum Einsatz von VPN (Entscheidungsgrundlage)	Details >>

Systematische Analyse einer komplexen DMZ-Umgebung zur Restrukturierung Details >>

2004 Umstellung und Erweiterung der Mail- und DNS-Infrastruktur im Firewall-Bereich Details >>

Sicherheits-Überprüfung/Spurensicherung auf einem Linux-Server Details >>

2000 - 2003 Aufbau und Leitung der Consulting Abteilung (angestellt) Details >>

Projekte im Detail

2015 Sicherheitsuntersuchung 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.

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.

seit 2014 Technische Beratung für eine NGO

Eine NGO (Nicht-Regierungs-Organisation), das im Bereich Datenschutz, Privatsphäre und Überwachung tätig ist, suchte einen technischen Experten. Es sollen Anwendungen daraufhin untersucht werden, ob die sie Privatsphäre der Benutzer beeinträchtigen. Ich habe bei diesen Untersuchungen mitgearbeitet und daraus Empfehlungen entwickelt, welche die NGO veröffentlich hat.

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

seit 2013 Erarbeiten einer neuen Policy für das Umorganisieren des Netzwerks

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. Au-

ßerdem sollte bislang dezentral Geregeltes in die nächste Version der unternehmensweiten Policy aufgenommen werden und viele technische Richtlinien erstellt werden.

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 - 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

2013 Netzwerkanalyse in einer Privatklinik

In einer Privatklinik musste das bislang undokumentierte Netzwerk analysiert und dokumentiert werden.

Rolle:	Engineer
Aufgaben:	- Alle, auch bislang unbekannte, Geräte im Netz aufspüren - Unbekannte Geräte identifizieren - Erstellen einer Geräteliste

Branche: Healthcare

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

2012 Erstellen von Risikoanalysen

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

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

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

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
Besonderes:	

Firmengröße: ca. 750 Personen

2010 Software-Audits

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)

2010 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)

2009 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 Sichheitsrelevanz überprüft werden. Viele Parameter des Projekts sind 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 Prüf-

konzept: 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

Rolle: Berater

Firmengröße: ca. 150.000 Personen (in D)

2009 Entlastung des IT Security Offices (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.

Rolle: Berater

Firmengröße: ca. 12.000 Personen (in D)

2008 Einführung verschlüsselter E-Mail für Vorstand und Aufsichtsrat

In einem Unternehmen wurden sensible Daten (BWA, Bilanzen, etc.) unverschlüsselt per E-Mail verschickt. Meine Aufgabe war, Vorstand und Aufsichtsrat zu überzeugen, dass solche E-Mails verschlüsselt werden müssen. Danach habe ich einen geeigneten Trustcenter ausgewählt und die Einführung der Verschlüsselung begleitet.

Rolle: Berater

2008 Risikoanalyse für die Umstellung auf VPN (nach 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 Inte-

grität 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 entwicklet

2008 Sicherheits-Audit und Qualitätssicherung bei 200 Standorten

Anforderung des Kunden: Nach dem kompletten Neuaufbau eines komplexen Netzwerks mit cirka 200 Standorten sollte eine Sicherheitsprüfung für die Endabnahme der Neuinstallation 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.

Zu diesen Aufgaben kam noch die Qualitätssicherung der Konfig-DB sowie des DNS hinzu. Da diese vom zuständigen Projektteam nicht zuverlässig gepflegt wurden, mussten Fehler und Inkonsistenzen gefunden werden.

Um sicher zu stellen, ob auch wirklich alle Daten vollständig, konsistent und korrekt vorliegen, habe ich Skripts erstellt, die diese Aufgabe zuverlässig und fehlerfrei durchführen - bei mehreren tausend Geräten ist dies nicht mehr manuell möglich.

Dies ist ein Folgeauftrag im gleichen Projekt "Produktivitätssteigerung durch Automatisierung" vom Herbst 2007.

Rolle: Berater

Firmengröße: bis 50.000 Personen, Abteilungsgröße: bis 50 Personen

2007 Sicherheits-Audit bei einer Bank

In einer Bank sollten ausgewählte Aspekte der IT-Sicherheit überprüft wurden. Die Prüfung orientierte sich am BSI-Grundschutz-Handbuch. Schwerpunkte waren

- Organisatorische Mängel bei der Dokumentation (K-Fall-Handbuch, Orga-Handbuch)
- Sicherheit Mobile Clients (Notebooks, etc.)
- Möglichkeiten, von außen in das PC-Netz einzudringen (Penetrationstest).

Mit dem von mir erstellten Abschlussbericht erhielt der Vorstand der Bank Gewissheit über die Sicherheitslage der IT in seinem Hause.

Rolle: Berater

2007-2008 Konzept und Implementierung ipfilter/IPSec für HP-UX

Benötigt wurde ein Konzept für den Betrieb von ipfilter und IPSec unter HP-UX. Dieses sollte eine möglichste einfache Administration dieser komplexen Materie ermöglichen, ausbaufähig sein und die Security-Anforderungen erfüllen. Die bestehenden Prozesse sollte möglichst unverändert bleiben.

Ich erstellte das Konzept, kläre die sicherheitsrelevanten Fragen mit dem ISO und implementierte die benötigten Lösung. Er schulte die Administratoren und half bei der Inbetriebnahme und erstellte das Betriebshandbuch (in Form eines Cookbooks). Für die Absicherung der Konfigurationen werden X.509-Zertifikate verwendet. Technisch werden bei dieser Lösung mehreren Open Source Programmen mit ausgeklügelten Skripten verbunden.

Die Herausforderung bei diesem Projekt war, auf mehreren Ebenen komplexe Vorgänge zu berücksichtigen, die sich gegenseitig beeinflussen: Sicherheit, Prozess, Technik, Know-How der Mitarbeiter, zukünftige Planung. Dies ist mir gelungen.

Firmengröße: ca. 38.000 Personen

Rolle: Berater

2007 Produktivitätssteigerung durch Automatisierung

In circa 200 Sites mussten Cisco-Komponenten (um-)konfiguriert und die Qualität gesichert werden. Hierzu habe ich einige Skripte erstellt, die die Aufgabe schnell und

mit weniger Fehlern erledigten. Damit habe ich auch die Produktivität der anderen Projektmitarbeiter erhöht und die Fehlerquote reduziert. Die gewonnene Zeit habe ich genutzt, um weiter Skripte zur Qualitätsicherung zu erstellen. Beispielsweise zu einem Abgleich der Konfig-DB mit dem Konzept. Die Skripte wurden auch nach meinen Weggang bis zum Projektende (März 2008) eingesetzt.

Mein Lösungsvorschlag sparte bereits in der ersten Projektwoche ca. 200.000 €, da die Anfahrten zu den 200 Sites eingespart werden konnten.

Rolle: Berater
Aufgaben: - Automatisierung und Qualitätssicherung
Firmengröße: Bis 50.000 Personen; Abteilungsgröße: Bis 50 Personen

2007 Machbarkeitsstudie: SAP WebAS ohne DMZ, IPSec/ipfilter

Bei einem SAP-System mit Web-Frontend sollte der externe ITS (AGate/WGate) entfernt werden und der Zugriff direkt auf das SAP-System im LAN erfolgen. Die Komponenten in der DMZ sollten komplett entfallen und durch eine Absicherung durch IPSec/ipfilter ersetzt werden.

Meine Aufgabe in diesem Projekt war, die geänderte Sicherheitsarchitektur zu bewerten. Der SAP-Bereich wurde durch ein anderes Team-Mitglied beigesteuert. Weitere Aufgaben: abteilungsübergreifende Interviews durchführen, Architektur erarbeiten, Machbarkeit prüfen, Risikobewertung abgeben, Projektplan erstellen, Review des Berichts.

Rolle: Berater
Firmengröße: ca. 38.000 Personen

2006 Sicherheitsüberprüfung nach BSI-Grundschutzhandbuch, BSI 100-1

In einer Bank sollten ausgewählte Aspekte der IT-Sicherheit überprüft wurden. Die Prüfung orientierte sich am BSI-Grundschutz-Handbuch. Schwerpunkte waren

- Organisatorische Mängel bei der Dokumentation (K-Fall-Handbuch, Orga-Handbuch)
- Sicherheit Mobile Clients (Notebooks, etc.)
- Möglichkeiten, von außen in das PC-Netz einzudringen (Penetrationstest).

Ich war Projektleiter und Teamleiter des Audit-Teams. Mit dem mir erstellten und präsentierten Abschlussbericht erhielt der Vorstand der Bank Gewissheit über die Sicherheitslage der IT in seinem Hause.

Rolle: Berater

2006 Rechtekonzept für ein Content-Management-System

Für den Online-Auftritt einer Zeitschrift (living-technology) entwickelte der Consultant ein Rechtekonzept. Die Steuerung der Rechter erfolgt über Rollen. Es gibt interne und externe Autoren, leitende Redakteure, eine Chefredaktion, "Heftpfleger" und eine Rolle für den "Webmaster". Der "Zustand" einer Artikels wird über Workflows gesteuert.

Die (technische) Struktur der Website musste mit dem Rechtekonzept zusammenpassen. Hier war eine enge Zusammenarbeit mit dem Webmaster und Web-Programmierer nötig.

Der Consultant zeigte gutes Verständniss der Prozesse in einem (Zeitschriften-)Verlag und für die Belange eines Online-Systems/Sebsite.

Rolle: Berater

2006 Sicherheitsüberprüfung eines Windows-Netzwerks

In einem Windows-Netzwerk sollten die schlimmsten Schwachstellen gefunden werden. Dem Kunden konnten etliche Wege genannt werden, über die ein Angreifer sensible Daten anziehen oder manipulieren kann. Berücksichtigt wurde auch die Sicherheit der Notebooks, da fast alle Mitarbeiter mobile Arbeitsplätze haben.

Rolle: Berater

2006 Problemmanagement bei einem Log-Analyse-System

Ein mehrstufiges Log-Analyse-Tool fiel einmal die Woche aus. Die vom Lieferanten genannten Lösungen halfen nicht. Der Consultant analysierte die Fehlerursachen (soweit möglich) und verhandelte mit dem Lieferanten über weitere Optimierungsmöglichkeiten. Um das Log-Analye-Tools in das bestehende Monitoring des Unternehmens einzubinden, wurden mit dem Lieferanten geeignete Messpunkte definiert und Sensoren erstellt.

Rolle: Projektleiter

2005 - 2006 Migrationsplanung eines komplexen Netzwerkes

Die redundanten Komponenten eines komplexen Netzwerkes sollten in unterschiedliche Brandabschnitte verteilt werden. Ein aktuelle Dokumentation der Verkabelung und Komponenten existierte nicht. Im Projektteam übernahm der Consultant die Aufgabe, alle erreichbaren Komponenten automatisch zu inventarisieren. Durch die automatische Auswertung bleibt die Liste immer aktuell. Die Daten Geräte werden per SNMP, Telnet- und SSH-Login abgefragt.

Die Auswertungen helfen, unbekannt Geräte aufzuspüren ("Da muss noch ein Switch dazwischen sein, den wir noch nicht kennen") und Leitungen zwischen den Geräten zu finden.

Rolle: Berater

2005 Betriebsübernahme eines Intrustion-Prevention Systems

Die Tippingpoint IPS mit 2x2 Sensoren wurde nach der Installation in den Betrieb übergeführt. Der Consultant analysierte die Möglichkeiten für Monitoring, Betrieb und Troubleshooting und integrierte die Systeme in die bestehenden Prozesse. Wichtig waren a) möglichst viele Standard-Aufgaben automatisch zu erledigen, z.B. das Reporting und b) die Integration in die Change-Prozesse (Patches, etc.) Nach dem Erstellen des Betriebshandbuches wurden die Administratoren eingewiesen.

2005 Studie und Konzept zum Einsatz von VPN (Entscheidungsgrundlage)

2005 Systematische Analyse einer komplexen DMZ-Umgebung zur Restrukturierung

2004 Umstellung und Erweiterung der Mail- und DNS-Infrastruktur im Firewall-Bereich

2004 Sicherheitsüberprüfung von Unix-Servern, incl. Suche nach schwachen Passwörtern

2004 Sicherheits-Überprüfung/Spurensicherung auf einem Linux-Server

2000 - 2003 Security-Consultant sowie Aufbau und Leitung der Consulting Abteilung (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

Ältere Projekte

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, 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 3032