

Persönliche Daten

Markus Wernig
Schreinerweg 15, CH-3012 Bern
x:fer GmbH – <http://xfer.ch>

Geboren: 16. August 1967
Nationalität: Österreich (Bewilligung C für die Schweiz)
Zivilstand: Ledig
Kontakt: +41 (0)78 743 77 81
markus.wernig@xfer.ch



see [below](#) for English

Verfügbarkeit: Übersicht

auf Anfrage

In über 15 Jahren Projektstätigkeit für namhafte Kunden im **Enterprise-Security-Umfeld** habe ich in Bereichen mit verschiedenen Schwerpunkten gearbeitet und dort entsprechend **vertieftes Know-how** aufbauen bzw. Ausbildungen absolvieren können:

- **Public Key Infrastructure (PKI)**
Architektur, Engineering, Betrieb Infrastruktur, RA Op, CA Op, SSCD, Policies, Prozesse, Tools, Software-Entwicklung
- **Firewalls**
CheckPoint, Phion, StoneGate, PF/IPFW; Planung, Betrieb, Engineering
- **X.509, Verschlüsselung**
SSL, S/MIME, PGP
- **VPN**
SSL, IPsec; CheckPoint, Isakmpd, Kame, SafeNet
- **Intrusion Prevention**
ISS, Snort, TippingPoint, TripWire, OSSEC
- **Netzwerke**
TCP/IP, Routing, Switching
- **OS Tuning und Hardening**
- **Service-Engineering**
Web, Mail, FTP, DNS, LDAP, RADIUS, SSL, Proxy (reverse, forward)

Neben technischen Aufgabenstellungen gab es auch immer wieder organisatorische, die ich – im Rahmen bereits laufender Projekte – in verschiedenen Rollen erfüllt habe:

- **Projektleitung, Architektur**
- **Business Analyse**

Viele Projekte spielten sich im System-Engineering-Umfeld ab, daraus resultiert ein weiterer Schwerpunkt:

- **Server-Administration, Plattform-Engineering, Datenbank**
- **Applikations-Engineering und -Programmierung**
- **Service-Integration, -Einführung, Troubleshooting**

In allen diesen Gebieten verbinde ich analytische und konzeptionelle Fähigkeiten mit technischem Know-how und angewandter Erfahrung.

Ich bin gewohnt, in Teams zu arbeiten, und erfülle dort meine Aufgaben mit Selbstständigkeit. In ITIL-Umgebungen habe ich ebenso gearbeitet wie entsprechende Prozesse entwickelt und umgesetzt.

Ich führe meine eigene Firma, x:fer GmbH, die auch als eigenständige Dienstleisterin für Security, Unix, PKI und Netzwerk auftritt.

Ausbildung

- 1985 Abitur (Österreich)
- 1998-1999 Diplom: "Informatiktechniker TS" (ZbW St.Gallen, Schweiz)
- 2000 Veritas Netbackup (Veritas)
- 2001 Solaris System Administration II (SUN Microsystems)
- 2002 Linux Administration (Brainbench)
- 2002 Network Technical Support (Brainbench)
- 2004 CCSA (CheckPoint)
- 2005 CISSP (ISC)²
- 2006 CCSE (CheckPoint)

Sprachen

- Muttersprache: Deutsch
- Fließend: Englisch (s, m), Italienisch (s, m)
- Gut: Französisch (m)

Auftraggeber/ Kunden

- | | |
|-----------------------------------|--------------------------------|
| Cope AG | Swisscom (Schweiz) AG |
| Mount10 (jetzt SIAG) | ALPIQ |
| SUN microsystems (jetzt Oracle) | Swiss Post Solutions |
| Swiss Post Information Technology | SEPPmail AG |
| Swisscom IT Services | SDMS SA |
| SwissSign AG | Schweizerischer Notarenverband |
| | SNV |

Key Words

- Security-Engineering und -Consulting, PKI-Architektur und -Betrieb
- Planung, Umsetzung von gesicherten Netzwerkumgebungen: VPN/ IPsec, X.509, SSL, Firewalls, Authentisierung, Routing, Architektur
- Firewalls (Checkpoint FW-1/Provider-1, Nokia, StoneGate, Phion, Open-Source-Produkte), VPN (VPN-1, FreeS/Wan, Racoon/Kame, Isakmpd) und IDS
- TCP/IP Netzwerke, Oracle, VMWare Server, Nagios
- UNIX System-Engineering und -administration (Solaris, Linux, BSD)
- Server-Technologien and -Protokolle: HTTP/S, SMTP, DNS, POP/IMAP, SQL, DHCP, SSL, LDAP, RADIUS; Virus- und Spam-Filter, Forward und Reverse Security Proxies (Airlock, Apache, Squid, Nevis), S/MIME
- Programmierung: C, C++, Perl, Shell (Bash, Ksh), Web-Applikationen (PHP, JavaScript, Perl. AJAX), Java
- System-Architektur und -Design
- Open-Source, Grundlagen Windows-Administration
- "Anything Unix"

«Vor der IT»

- 1987 - 1988 Studium Anglistik/Publizistik, Universität Wien
- 1988 - 1997 "Die Ostschweiz", St.Gallen, Schweiz

Desktop Publishing, Support (Macintosh), Korrekturlesen

Hobbies

- Literatur, internationale Küche, Reiten

Projekte (Auszug)

- 07.2014 (aktuell) **Entwickler/Engineer Register-Software**
- Entwicklung/Erweiterung des X.509-Signatur-Registers des Schweizerischen Notarenverbands
 - Entwicklung des Zentralen Eidgenössischen Testamentenregisters und -Portals
 - SuisseID-Integration
 - Verwendete Technologien: Perl, Java, AJAX, CSS, SSL, PKCS#7, X.509, Mysql, XMLRPC, Apache, mod_perl
- 04.2012 – 06.2015 **Network Security Engineer**
- Management komplexer Firewall-Infrastrukturen für Outsourcing-Plattformen (ca. 500 Firewall-Cluster/200 CMA)
 - Verwendete Technologien: StoneGate FW, CheckPoint Provider-1
- 07.2010 (aktuell) **Entwickler/Engineer E-Mail Verschlüsselungs-Gateway**
- Entwicklung/Erweiterung eines E-Mail Verschlüsselungs- und Signatur-Gateways
 - Secure Webmail Interface
 - SuisseID-Integration
 - Nachvollziehbarkeit, Nicht-Abstreitbarkeit, Abrechnung
 - System-Engineering der Sicherheitsplattform (OpenBSD)
 - Verwendete Technologien: Perl, SSL, RSA, ASN.1, PKCS#1, PKCS#7, PKCS#10, X.509, S/MIME, PGP; LDAP, Apache
- 01.2010 – 07.2010 **Enterprise Security Engineer**
- Entwurf einer neuen konzernweiten, hochverfügbaren Firewall-Plattform, verteilt auf mehrere Standorte in der Schweiz
 - Entwurf und Einführung einer neuen Leitstellenkopplung
 - Security-Engineering für interne Netzwerkprojekte (Video Conferencing, Corporate Communication Services, Strom-Verteilnetz-Messungen und -Alarmierungen)
 - Redesign der Corporate Remote Access Services
- 09.2009 – 12.2011 **Entwickler/Engineer eHealth PKI**
- Software-Entwicklung einer Certificate Authority für Card verifiable Certificates nach ISO-7816, CEN-CWA-14890-1
 - Online-Schnittstelle für automatisches Zertifikats-Enrollment
 - System Engineering PKI Security Platform (Linux, Solaris)
 - Spezifikation Karten-, Zertifikats- und Requestformate
 - Koordination Integrationsarbeiten Middleware
 - Verwendete Technologien: Perl, SSL, RSA, ASN.1, PKCS#1, PKCS#7, PKCS#10, X.509; MySQL, Apache
 - Betrieb und Betriebssupport PKI
- 01.2009 – 06.2009 **Engineer Managed Security Services**
- Operations und Engineering gemanagter Security-Plattformen (international)
 - CheckPoint VPN-1, SecurePlatform, Edge, Connectra,
 - Phion Netfence, Phion/Visonys Airlock, Solaris
 - RADIUS, LDAP, Cisco ASA, WebWasher, ...
- 06.2006 – 12.2008 **Unix Security Systems/PKI Engineer**
- System Engineering der PKI Plattform
 - Update der Infrastruktur auf ZertES-Anforderungen (KPMG-Audit)
 - Planung und Design neuer, ETSI-konformer Infrastruktur

- Aufbau der kompletten Linux-Server-Plattform (inkl. Install-Server, Backup, Config-Management etc.)
- Business Analyse, Engineering und Support Lösungsintegration Partner und Endkunden
- Perimeter-Sicherheit mit stateful HA-Firewall-Clusters (OpenBSD)
- Teilprojektleitung SSCD-Framework, Schnittstellenfunktion Lieferant – Middleware, PKI (inhouse) – Integrator; Troubleshooting
- Linux Server Hardening auf B1-kompatibles Niveau
- Enterprise Remote Access (IPSec, OpenBSD)
- Verantwortlicher für Change, Incident und Problem Management (Prozesse und Tools, ITIL)
- Projektleitung und Überwachung PKI-Software-Entwicklung
- Entwicklung PKI-Software-Module (Perl, C)
- Migration/Redesign best. Applikationen in die neue Infrastruktur
- Betrieb Firewalls und Unix Server (Linux, Solaris, OpenBSD)

01.2006 – 12.2006

Security Engineering / Security Architecture

- Enterprise compliance testing
- Engineering einer Trading Floor Sicherheitsarchitektur
- Erstellung konzernweiter VPN-Site-to-Site-Policy
- Erstellung PKI-Zertifikats-Spezifikationen
- Projektleitung Security Management Workflow
- Redesign RAS Infrastruktur

Network Architecture Consulting

- Erstellung Log Management Policy
- Konsolidierung DNS-Daten für Netzwerk-Management

2003 – 2005

Entwicklung neue Netzwerk-Sicherheits-Infrastruktur

- Entwurf der Firewall-Infrastruktur für eine neue Netzwerk-Sicherheits-Plattform (Ziel: Konsolidierung einer Umgebung mit 50 Firewalls, 200 DMZs und ca. 1000 Servern). (CheckPoint FW-1, Provider-1, Nokia, OpenBSD)
- IP-Routing-Konzept, IP-Adress-Schema.
- Erstellung und Pflege der Network Security Policy.
- Installation, Konfiguration und Inbetriebnahme der Firewalls.
- Techn. Unterstützung Netzwerkabteilung während der Einführung.
- Migrationsberatung für Kunden.
- Integration neuer Projekte in die Plattform.
- Sicherheitsaspekte eingeführter Services analysieren und bei Bedarf Massnahmen erarbeiten.
- Entwicklung von Administrationswerkzeugen (Bash, Perl).

2005

Entwicklung eines Online-Dokumentationssystems

- Perl/Bash
- Linux/Apache/MySQL

2004

Entwicklung eines Alarming Agent mit HP OVO Interface

- Perl
- Solaris, Linux

2002 – 2003

Entwurf, Entwicklung, Einführung und Pflege einer Log- und Verbindungs-Datenbank

- Definition der Logging-Richtlinien.
- Entwicklung von Programmen zur Erfassung und Konsolidierung von Server- und Netzwerk-Logs (Bash, Perl).
- Definition der Datenbankstrukturen.
- Installation, Konfiguration und Einsatz der benötigten Komponenten.

2002 · Entwicklung eines Web-basierten GUI für die Auswertung.
Entwicklung eines Load balancing agent für UNIX-Server
und Checkpoint FW-1 (Sprache: C; System: Solaris, Linux, HP-UX)

2001 **Entwicklung einer Intrusion-Detection-Infrastruktur**
· Analyse der möglichen Angriffsszenarien in einem Umfeld von ca. 600
Servern (Finanzapplikationen).
· Produktevaluation.
· Installation, Konfiguration und Einsatz der technischen IDS-Infrastruktur
(Sensor und zentrale Datenbanken).
· Definition der Incidence-Response-Prozeduren .
· Durchführung von Incidence-Response-Massnahmen.

Weitere Skills:
· Nokia IP Series Plattform
· Entwicklung verschiedener administrativer Tools/Applikationen (Monitoring,
Remote Management, konsistente Datenverteilung, Backup ...) für UNIX-
Systeme (Perl, Bash; SSH)
· DNS, Proxies

x:fer Services Mit der **x:fer GmbH** betreibe ich für Kunden u.a. die **folgenden Services:**
· Mail hosting (Firmen und Private)
· Web hosting
· DNS
· Engineering-Leistungen in jedem der obigen Gebiete.
· Die Services basieren auf einer Solaris 11 hot-standby Cluster Lösung und gut
integrierten Open-Source-Software-Lösungen (sendmail, apache, bind, cyrus-
imap, mysql, perl, php, clamAV, spamassassin, openldap).

Personal Details Markus Wernig
Schreinerweg 15, CH-3012 Bern
x:fer GmbH – <http://xfer.ch>

Date of birth: August 16th 1967
Nationality: Austrian (Swiss Work Permit C)
Status: Unmarried
Contact: +41 (0)78 743 77 81
markus.wernig@xfer.ch

Availability: upon request

Abstract

In over 15 years of **Enterprise Security** project business for notable customers I have worked in fields of various focus in which I was able to acquire **in-depth know-how** and education:

- **Public Key Infrastructure (PKI)**
Architecture, Engineering, Operations, Infrastructure, RA Op, CA Op, SSCD, Policies, Processes, Tools, Software engineering
- **Firewalls**
CheckPoint, Phion, StoneGate, PF/IPFW; Planning, Operations, Engineering
- **X.509, Encryption**
SSL, S/MIME, PGP
- **VPN**
SSL, IPSec; CheckPoint, Isakmpd, Kame, SafeNet
- **Intrusion Prevention**
ISS, Snort, TippingPoint, TripWire, OSSEC
- **Networking**
TCP/IP, Routing, Switching
- **OS Tuning and Hardening**
- **Service Engineering**
Web, Mail, FTP, DNS, LDAP, RADIUS, SSL, Proxy (reverse, forward)

Apart from the technical tasks there have always been organizational ones, which I have carried out – within the context of an ongoing project – in various roles:

- **Project management, Architecture**
- **Business analysis**

Many projects had a strong system engineering background or objective, from which another skill focus results:

- **Server administration, Platform engineering, Databases**
- **Application engineering and programming**
- **Service integration, deployment, troubleshooting**

In all of those fields I combine analytical and conceptual abilities with in-depth technical expertise and hands-on experience.

A freelancer in IT since 1999, I am used to working in teams, independently fulfilling my tasks. I have worked in ITIL environments, where I have also developed and deployed the corresponding processes.

I run my own company, x:fer GmbH, who is also acting as an independent service provider for Security, Unix, and Networking.

Education

- 1985 Abitur (High school graduation; Austria)
- 1998-1999 Diploma: "Informatiktechniker TS" (Information Technology Engineer)(ZbW St.Gall, Switzerland)
- 2000 Veritas Netbackup (Veritas)
- 2001 Solaris System Administration II (SUN Microsystems)
- 2002 Linux Administration (Brainbench)
- 2002 Network Technical Support (Brainbench)
- 2004 CCSA (CheckPoint)
- 2005 CISSP (ISC)²
- 2006 CCSE (CheckPoint)

Languages

Native: German
Fluent: English (w, s), Italian (w, s)
Good: French (s)

Customer/ Employer list

Cope AG	Swisscom (Switzerland) AG
Mount10 (now SIAG)	ALPIQ
SUN microsystems (now Oracle)	Swiss Post Solutions
Swiss Post Information Technology	SEPPmail AG
Swisscom IT Services	SDMS SA
SwissSign AG	Swiss Notary Association SNV

Key Words

- UNIX system engineering and administration (Solaris, Linux, BSD)
- Server technologies and protocols: HTTP/S, SMTP, DNS, POP/IMAP, SQL, DHCP, SSL, LDAP, RADIUS; Virus and Spam controls; Forward & Reverse Security Proxies (Airlock, Apache, Squid, Nevis), S/MIME
- Programming: C, C++, Perl, Shell (Bash, Ksh), Web applications (PHP, JavaScript, Perl, AJAX), Java
- System architecture design
- Security engineering and consulting, PKI architecture and operations
- Design and deployment of secured network environments: VPN/ IPSec, X.509, SSL, Firewalls, Authentication, Routing, Architecture
- Checkpoint FW-1/Provider-1, StoneGate, Nokia, Phion, Open source firewalls, VPN-1, FreeS/Wan, Racoon/Kame, Isakmpd, IDS
- TCP/IP networking, Nagios
- Oracle, VMWare Server, Open Source, Basic Windows administration
- "Anything Unix"

«Before IT»

1987 - 1988 Study Anglistics/Publicistics, University of Vienna
1988 - 1997 "Die Ostschweiz", St.Gall, Switzerland

Desktop Publishing, Support (Macintosh), proof reading

Hobbies

Literature, international cuisine, riding

Projects (excerpt)

- 07.2014 (ongoing) **Developer/Engineer Registry Software**
- Development/extension of the X.509 signature register of the Swiss Notary Association
 - Engineering/Development of the Central Swiss Testament Register and Portal
 - SuisseID smartcard integration
 - Technology: Perl, Java, AJAX, CSS, SSL, PKCS#7, X.509, Mysql, XMLRPC, Apache, mod_perl
- 04.2012 – 06.2015 **Network Security Engineer**
- Management of complex Firewall infrastructures for outsourcing platforms (ca. 500 firewall cluster/200 CMA)
 - Technology: StoneGate FW, CheckPoint Provider-1
- 07.2010 (ongoing) **Developer/Engineer E-Mail Encryption Gateway**
- Development/extension of an E-Mail Encryption/Signature Gateway
 - Secure Webmail Interface
 - SuisseID integration
 - Traceability, non-repudiation, accounting, billing
 - System Engineering of the underlying Security Platform (OpenBSD)
 - Technology: Perl, SSL, RSA, ASN.1, PKCS#1, PKCS#7, PKCS#10, X.509, S/MIME, PGP; LDAP, Apache
- 01.2010 – 07.1010 **Enterprise Security Engineer**
- Design of a new corporate, highly available Firewall platform spanning multiple locations in Switzerland
 - Design and deployment of Power Grid Control Center Interconnection
 - Security Engineering for internal network projects (Video Conferencing, Corporate Communication Services, power grid metering and alerting)
 - Redesign of Corporate Remote Access Services
- 09.2009 – 12.2011 **Developer/Engineer eHealth PKI**
- Development of a Certificate Authority Software for Card verifiable Certificates acc. to ISO-7816, CEN-CWA-14890-1
 - Online Interface for automatic Certificate Enrollment
 - System Engineering of the PKI Security Platform (Linux, Solaris)
 - Specification of card, certificate and request formats
 - Coordination of Middleware integration
 - Technology: Perl, SSL, RSA, ASN.1, PKCS#1, PKCS#7, PKCS#10, X.509; MySQL, Apache
 - PKI Operations and Operations support
- 01.2009 – 06.2009 **Engineer Managed Security Services**
- Operations and Engineering of managed security platforms (international)
 - CheckPoint VPN-1, SecurePlatform, Edge, Connectra
 - Phion Netfence, Phion/Visonys Airlock, Solaris
 - RADIUS, LDAP, Cisco ASA, WebWasher
- 06.2006 – 12.2008 **Unix Systems/PKI Engineer**
- System Engineering of PKI infrastructure
 - Update infrastructure to ZertES requirements (KPMG audit)
 - Plan and design new, ETSI-compliant PKI infrastructure
 - Setup of a complete Linux server platform (incl. Install server, Backup, Configuration management etc.)
 - Engineering and support of solution integration with partners and end

- customers
 - Part. project lead SSCD Framework, interface function supplier – middleware, PKI (inhouse) – integrator; troubleshooting
 - Responsibility for Change, Incident and Problem Management (Processes and Tools)
 - Perimeter security with stateful HA-Firewall-Clusters (OpenBSD)
 - Linux Server hardening to B1-compatible level
 - Enterprise Remote Access (IPSec, OpenBSD)
 - Project management and supervision of PKI software development
 - Development of PKI software modules (Perl, C)
 - Migration/redesign of existing applications into new infrastructure
 - Firewall and Unix server operations (Linux, Solaris)
- 01.2006 – 12.2006
- Security Engineering / Security Architecture**
- Enterprise compliance testing
 - Engineering of a Trading Floor Secure Architecture
 - Definition of the enterprise VPN-Site-to-Site-Policy
 - Definition of PKI Certificate specifications
 - Projekt management for Security Management Workflow
 - Redesign of RAS infrastructure
- Network Architecture Consulting**
- Definition of Log Management Policy
 - Consolidation of DNS data for Network Management
- 2003 – 2005
- Development of a new network security infrastructure**
- Design of the firewall infrastructure for a new network security platform (Consolidation 50-firewall environment with 200 DMZs & 1000 Servers). (CheckPoint FW-1, Provider-1, Nokia, OpenBSD)
 - IP routing design, IP addressing scheme design.
 - Definition and maintenance of the Network Security Policy.
 - Install, configure and deploy the firewalls.
 - Provide technical engineering support during implementation to network department.
 - Migration support for customers.
 - Integration of new projects into the platform.
 - Assess and analyze possible threats to the deployed services under network security aspects. Define countermeasures.
 - Development of administrative tools (Bash, Perl).
- 2005
- Development of an Online Documentation System**
- Perl/Bash
 - Linux/Apache/MySQL
- 2004
- Development of an Alarming Agent with HP OVO interface**
- Perl;Solaris, Linux
- 2002 – 2003
- Design, deployment and maintenance of internal Log and Connection Tracking Database**
- Define network traffic logging policies.
 - Develop tools to collect and consolidate traffic logs (Bash, Perl)
 - Define database structure.
 - Install, configure and deploy the necessary components.
 - Develop a web-based GUI for reporting and assessment.
- 2002
- Development of a Load balancing agent for UNIX servers**
- for use with FW-1 (written in C; systems: Solaris, Linux, HP-UX)

2001

Design, deployment and maintenance of an intrusion detection infrastructure

- Define the “hot spots” in a network of about 600 servers with mostly banking applications.
- Evaluate IDS products.
- Install, configure and deploy the technical IDS infrastructure (sensors and central database).
- Provide support to Service Planning in defining incident response procedures.
- Participate in incident response measures.

Further Skills

- Nokia IP Series Firewall platform
- Development of various administrative tools/applications (monitoring, remote management, consistent data distribution, backup ...) for UNIX systems (Perl, Bash; SSH)
- DNS, Proxies

x:fer Services

With **x:fer gmbh**, I operate the **following services**, among others, for customers:

- Mail hosting (corporate and private)
- Web hosting
- DNS
- Engineering services in any of the above fields.
- The services are based on a Solaris 11 hot-standby cluster solution and well-integrated open source software solutions (sendmail, apache, bind, cyrus-imap, mysql, perl, php, clamAV, spamassassin, openldap)