MICHAEL STRÖDER

Klauprechtstr. 11
D-76137 Karlsruhe
Telefon +49 721 8304316
michael@stroeder.com
http://www.stroeder.com/

ART DER TÄTIGKEIT

Freiberuflich als Berater für Systemintegration und IT-Sicherheit, insbesondere Verzeichnisdienste, Identity & Access Management (IAM), Single Sign-On, Mehrfakor-Authentifizierung, Public-Key-Infrastrukturen (PKI) und verwandte Anwendungen.

KOMPETENZFELDER

- Planung und Implementierung von Architekturen zur sicheren Nutzung von IT-Diensten (PKI, SSL, S/MIME, VPN, LDAP, Identity & Access Management, Single Sign-On, Firewalls)
- Entwurf, Implementierung und automatisierte Installation/Konfiguration (DevOps) sicherer Software (z.B. Web-Applikationen), objektorientierte Programmierung (z.B. Python)
- Systemintegration und Benutzerverwaltung in komplexen und heterogenen Umgebungen (Datenmigration und Datensynchronisation)
- Schulungen und Workshops

PROJEKTE

Internationaler Hersteller Transportsysteme (11/2018..02/2019)

- Konfiguration eines Samba 4 Datei-Servers und sssd integriert mit MS Active Directory auf CentOS
- Implementierung von ansible-Rollen, -Modulen und -Plugins zur automatisierten Konfiguration von CentOS gemäß Sicherheitsrichtlinien des Konzerns (Basis-OS mit automatischer Domänenintegration, Samba, HTTP-Server, DHCP-Server)
- Implementierung eines OpenLDAP-Server als Backend für DHCP mit integrierter Anmeldung basierend auf MS Active Directory
- LDAP-Integration von vCenter Server Appliance (VCSA)

IT Company (10/2018..11/2018)

- Vergleich von vier kommerziellen IAM-Produkten
- Erstellung einer Bewertungsmatrix und einem Dokument mit vergleichender Produktübersicht

Implementierung freies Software-Projekt Æ-DIR (03/2018 bis heute)

- Implementierung verschiedener Komponenten in Python
- Speziell angepasster NSS-/PAM-Dienst *aehostd* für Linux-Logins
- Spezielle Härtungsmassnahmen, u.a. mittels *AppArmor*-Profilen
- *ansible*-Rollen zur automatischen Installation und Konfiguration der Komponenten

Internationaler Internet-Provider (12/2017 bis 02/2018)

- Konzeption und Implementierung eines Dienstes zur sicheren Ausgabe von Kurzzeitzertifikaten für zeitlich begrenzte SSH-Logins
- Integration eines HSMs via PKCS#11 und Mehrfaktorauthentifizierung

Mittelständische IT-Firma im Bereich Data Science (03/2016..12/2017)

- Einführung eines firmenweiten Identity / Access Managements (IAM) als Grundlage für sichere Zugriffe auf die IAAS-Plattform

- Implementierung und kundenspezifische Anpassung von Æ-DIR mit Mehrfaktorauthentifizierung (OATH-LDAP)
- Implementierung diverser komplexer ansible roles zur vollautomatischen Installation/Konfiguration des Systems auch in Microsoft Azure

Internationaler Internet-Provider (04/2012 bis 06/2015)

- Aufbau einer Betriebsinfrastruktur eines proprietären, hochsicheren Messaging-Systems, Dokumentation für Sicherheits-Audit dieses staatlich regulierten Systems gemäß IT-Grundschutzhandbuch (GSHB).
- Installation/Konfiguration/Dokumentation eines öffentlichen Verzeichnisdienstes für Kundendaten basierend auf OpenDJ, spätere Migration auf OpenLDAP.
- Konzeption und Aufbau verschiedener OpenLDAP-Server zur Authentifizierung und Autorisierung der Administratoren, u.a. auch als Backend für Samba- und TACACS+-Server
- Definition eines speziellen LDAP-Schemas und *set*-basierter OpenLDAP-ACLs für die feingranulierte und hochsichere Berechtigung der Benutzer auf Server-Gruppen
- Spezifische Anpassungen für web2ldap zur Pflege der Benutzer-, Gruppen- und SUDO-Einträge, Implementierung der Datensynchronisation von Personen- und Benutzerdaten
- Konzeption und Implementierung verschiedener Verschlüsselungstechnologien, insbesondere Spezifikation eines Austauschformats für provider-übergreifende Mail-Routing-Informationen zur STARTTLS-Nutzung
- Implementierung vollautomatischer Installation und Konfiguration verschiedenster Dienste mit Puppet 2.7
- Implementierung diverser Dienste-Checks für ein Monitoring-System basierend auf check_mk
- Konzeption und Aufbau einer internen PKI basierend auf EJBCA
- Konzeption und Implementierung einer integrierten 2-Faktor-Authentifizierung mit OpenLDAP und yubikey (OATH-HOTP) für Linux-Login und diverse Web-Anwendungen

Internationaler Logistikkonzern (01/2011 bis 03/2013)

- Konzeption/Konfiguration eines OpenLDAP-basierten Verzeichnisdienstes für die projektinterne Mitarbeiter- und Benutzerverwaltung
- Entwicklung von div. Werkzeugen und Web-Applikationen in Python, Customizing von web2ldap für die Pflege der Benutzer-, Gruppen- und Orga-Einträge
- LDAP-Integration diverser Systeme und Anwendungen (Jira, Confluence, Mediawiki, SharePoint, SVN)

Bank in Frankfurt (06/2011..01/2012)

- Konzeption und Installation OpenLDAP-Server als Basis für LDAP-basierte Anmeldung via CAS
- Implementierung eines Delta-Synchronisationsprozesses von einer Oracle DB zu OpenLDAP in Python

Bundesbehörde in Deutschland (12/2010 bis 07/2011)

- Konzeption und Installation für eine Migration eines bestehenden Systems von Novell eDirectory und DirXML hin zu einer Open-Source-Lösung
- Implementierung eines Delta-Synchronisationsprozesses von eDirectory zu OpenLDAP in Python

Internationaler Logistikkonzern (10/2009 bis 06/2011)

- Sicherheitsberatung hinsichtlich Design, Entwicklung und Betrieb eines proprietären Messaging-System mit Nachrichtenverschlüsselung und digitaler Signatur
- Coaching von Entwicklern, Software-Reviews
- Konfiguration nCipher HSMs

Bundesbehörde in Deutschland (06/2009 bis 10/2009)

- Konzeption für eine Migration eines bestehenden Systems von Novell eDirectory und DirXML hin zu einer Open-Source-Lösung
- Pilotimplementierung der Synchronisation von MS AD zu OpenLDAP in Python

Mittelständische Bank in Stuttgart (10/2007 bis 03/2009)

- Konzeption für ein Single Sign-On für Web-Applikationen
- Pilotinstallation von Central Authentication Service (CAS) mit wahlweiser Authentifizierung gegen MS AD mit SPNEGO/Kerberos oder LDAP
- Implementierung einer Benutzerdatensynchronisation zwischen einer PostgresQL-Datenbank, MS Active Directory und Lotus Domino

Landesbehörde in Baden-Württemberg (12/2005 bis heute)

- Konzeption, Pilotinstallation und Dokumentation eines OpenLDAP-basierten Verzeichnisdienstes zur zentralen Speicherung von abstrakten Rollen und anwendungsspezifischen Autorisierungsmerkmalen
- Beschreibung/Entwurf von Prozessen, Schnittstellen und Use-Cases für eine delegierte Benutzerverwaltung

Internationaler Pharmakonzern (02/2006 bis 11/2007)

- Konzeption einer stark mit Lotus Notes integrierten PKI zur Nutzung verschlüsselter E-Mail gemäß S/MIME-Standard
- Vorstudie für eine konzernweite PKI als Basis für Windows Smartcard Logon und Dateiverschlüsselung. Arbeitsergebnis umfasste Kostenschätzung, Meilensteine für Projektplanung etc.
- Konzeption und Installation einer konzernweiten PKI (s.o.), Integration mit Konzernverzeichnisdienst
- Erstellung eines Certification Practice Statements (CPS) gemäß RFC 3647 für öffentlichen Teil der PKI

Luftfrachtunternehmen (02/2007 bis 04/2007)

- Vorstudie inkl. Konzeption und Kostenschätzung einer Lösung für Single Sign-On an web-basierten B2B-Applikationen
- Dokumentation von bestehenden Anwendungen

Internationaler Telekommunikationskonzern (09/2005 bis 04/2006)

- Neukonzeption und Pilotimplementierung der Datensynchronisation für den konzernweiten Verzeichnisdienst
- Evaluierung verschiedener LDAP-Server-Produkte (Interoperabilitäts- und Performance-Tests)

Internationaler Logistikkonzern (09/2003 bis 06/2005)

- Konzeption zur Nutzung archivfester digitaler Signatur mit einer X.509-basierten PKI in Filialkassensystemen und den beteiligten Backend-Systemen
- Konzeption für persönliche, offline-fähige Anmeldung und Single Sign-On an Filialkassensystemen basierend auf Smartcards
- Konzeption zur Verwaltung der Benutzer der Filialkassensysteme mit automatischem Abgleich der Benutzerstammdaten mit Personaldatenbank
- Abstimmung und Koordination mit Wirtschaftsprüfern hinsichtlich GOB/GOBS-relevanter Sicherheitsthemen bei Filialkassensystemen und den beteiligten Backend-Systemen

Internationaler Telekommunikationskonzern (11/2002 bis 09/2003)

- Konzeptionelle Arbeiten für Entrust-basierte PKI-Architektur (Registrierungsprozeduren, Selbst-Administrierung, etc.)
- Dokumentation für Integration der Entrust-basierten PKI-Architektur in Web- und Desktop-Anwendungen

- Konzeption für die Integration einer X.509-basierten Single Sign-On-Lösung (Entrust TruePass) und eines LDAP-Verzeichnis (Siemens Dir/X) in eine web-basierte Anwendung
- Coaching der Java-Entwickler
- Workshops für Administratoren

Internationaler Pharmakonzern (09/2001 bis 05/2003)

- Entwurf, Implementierung und Pilottests eines konzernweiten, LDAP-basierten Verzeichnisdienstes (iPlanet Directory Server) zur Benutzerauthentifizierung als Single-Password-Lösung. Das System wurde konzeptioniert als zentrale Benutzerdatenbank für interne und externe Nutzer von Web-basierten Anwendungen und anderen Systemen.
- Konzeption und Implementierung der Synchronisation der LDAP-Benutzerdaten mit einer Datenbank auf Host-Systemen (DB2 auf S/390, Einsatz von DB2 Connect unter Linux)
- Entwurf einer Public-Key-Infrastruktur (PKI) zur Ausgabe von X.509-Zertifikaten für Computersysteme (z.B. SSL-Server, IPSec-Router). Diese Arbeit umfaßte die Definition des Zertifikatprofils, Schreiben einer PKIX-konformen Zertifizierungsrichtlinie (CP und CPS gemäß RFC 2527) und Unterstützung beim Entwurf der Java-basierten Software.
- Evaluierung von PKI-Produkten (Entrust und RSA Keon) in einer Pilotumgebung für VPN, Single Sign-on, S/MIME-basierte E-mail.
- LDAP-Integration/-Konfiguration für das Profil-Verzeichnis eines Web-Portal-Produkts, Implementierung eines Prozesses für die Synchronisation der Benutzerdaten gegen Domino/LDAP
- Tiefgehende Analyse der Sicherheitsmechanismen von Netegrity Siteminder und Integration mit LDAP-Verzeichnisdienst der Benutzerverwaltung gemäß fachlicher Vorgaben

Verschiedene Aktivitäten (von 04/2001bis 2002)

- Einführungsschulung, Workshops und Beratung bzgl. einheitlicher Benutzeradministration und zentralem LDAP-Verzeichnis für interne und externe Benutzer bei einem internationalen Textilunternehmen
- Entwurf und Realisierung eines zentralen, LDAP-basierten Adressbuchs für die Stadtverwaltung Karlsruhe, Anbindung des Web-Content-Management-Systems (ZOPE) an Domino/LDAP

emagine GmbH, Eschborn (10/2000 bis 04/2001)

- Entwurf von PKI-bezogener Software zur Bereitstellung von Mehrwertdiensten im Bankenbereich (basierend auf Identrus)
- Erstellung eines Konzepts für einen generalisierten Zertifizierungsablauf zur Integration mehrerer Zertifizierungsdienstleister in den sog. Registration Authority (RA) Server

Propack Data GmbH, Karlsruhe (05/1996 bis 09/2000)

- Einführung, Planung, Installation und Administration verschiedenster Internet- und Intranet-Dienste basierend auf offenen Standards.
- Entwurf und Realisierung Firewall zur Gewährleistung einer sicheren Internet-Anbindung basierend auf Linux mit diversen Proxy-Diensten (Squid, postfix, dnscache).
- Entwurf, Implementierung und Einführung einer Public-Key-Infrastruktur (PKI) zur Ausgabe von X.509-Zertifikaten an alle Mitarbeiter. Die X.509-Zertifikate wurden hautpsächlich für S/MIME-basierte E-Mail (Verschlüsselung und digitale Signatur) und zur Benutzerauthentifizierung mobiler Benutzer eingesetzt (VPN, IMAP via SSL, SMTP mit StartTLS und X.509-Client-Zertifikaten für die Relaying-Regeln).
- Installation IPSec-basierter VPN-Verbindungen zur kostengünstigen Anbindung international verteilter Geschäftsstellen basierend auf Linux und FreeS/WAN.
- Einführung und Einsatz eines LDAP-Verzeichnisdienstes (OpenLDAP) als zentrales Adreßbuch und PKI-Repository.
- Integration von Domino/LDAP und die PKI.

- Implementierung verschiedenster LDAP-Clients zur Integration bestehender Anwendungen mit dem LDAP-Verzeichnis (z.B. Kennwortprüfung am Web-Proxy Squid).

OPEN SOURCE

Verschiedene freie Software-Projekte werden ggf. auch in Projekten bei Kunden eingesetzt:

- Æ-DIR - Authorized Entities Directory (siehe https://ae-dir.com/)
  Entwurf und Implementierung einer hochsicheren Benutzer- und Berechtigungsverwaltung insbesondere für privilegierte Zugriffe (IAM, PIM, PAM) basierend auf OpenLDAP
- web2ldap (siehe https://web2ldap.de/)
  Entwurf und Implementierung eines komfortablen, web-basierten LDAPv3-Clients mit Unterstützung für LDAPv3-Schema, StartTLS/LDAPS, Referrals, Root Naming Context, DNS SRV Records, Gruppenadministration, etc..
- OATH-LDAP (siehe https://oath-ldap.stroeder.com/)
  Entwurf und Implementierung eines OATH-basierten Authentifizierungssystems mit LDAP als Backend-Datenbank für HOTP / TOTP
- python-ldap (siehe https://python-ldap.org) bis 12/2017
  Langjährige Weiterentwicklung und Wartung eines Modulpaketes zur objektorientierten Programmierung von LDAP-Applikationen mithilfe der Programmiersprache Python

AUSBILDUNG

Abschluß als Dipl.-Inform. an der Universität Karlsruhe (Januar 1999)

- Diplomarbeit:
  "Einführung kryptographischer Techniken zur gesicherten Nutzung des Internet bei der Propack Data GmbH"
- Vertiefende Ausrichtung: Telematik (Computer-Netzwerke, Verteilte Systeme), Interaktive Systeme, Leistungsanalyse von Rechensystemen, Automatisierungstechnik

FACHKENNTNISSE

Verschlüsselungs- und PKI-Standards:
SSL, TLS, S/MIME, X.509, PKIX, IPSec, OpenPGP, DKIM, DNSSEC/DANE

Authentifizierungsmechanismen:
Passwortmechanismen/-synchronisation, OATH-HOTP/TOTP, Kerberos, SPNEGO, SASL, X.509-Client-Zertifikate, PAM unter Linux, RADIUS, TACACS+

Sicherheitsprodukte:
Entrust Authority, Cybertrust UNICERT (früher Baltimore UNICERT), Windows Certificate Services, Lotus Domino CA, RSA Keon CA, Netegrity Siteminder, OpenSSL, OpenSSH, Central Authentication Service (CAS der JA-SIG), Thales nCipher nShield/netHSM, EJBCA, FreeRADIUS, FreeIPA, AppArmor

Verzeichnisdienste:
OpenLDAP, OpenDJ (OpenDS), iPlanet/Netscape/SunONE Directory Server, Novell eDirectory, MS Active Directory, MS ADAM, IBM/Tivoli Directory Server, CA eTrust Directory, Critical Path, Siemens DirX, Lotus Domino/LDAP, Fedora Directory Server

E-Mail-Dienste: postfix, sendmail, qmail, fetchmail, dovecot

Web-Technologien: Apache, Tomcat, nginx, Squid, uwsgi, FastCGI, SCGI, WSGI

Datei-Server: Samba (SMB/CIFS), NFS

DNS & DHCP: PowerDNS, bind9, nsd, unbound, isc-dhcpd

Betriebssysteme:
Linux (openSUSE, SLES, RHEL, Debian etc.), Windows NT/2000/XP/2003/2008/2012, Solaris, OS/2, MS-DOS

Softwareentwicklung und Betriebsautomation:
Python, Pascal, Modula-2, Shell-Scripting, HTML/CSS, Versionskontrolle mit git, Subversion und CVS, Jira, Bugzilla, Trac, DevOps mit Puppet, ansible

Dokumentationswerkzeuge: Confluence, Mediawiki, Trac, T-Wiki, Foswiki

Hardware: PC-Hardware und Grundlagen von Embedded-Systemen

Virtualisierung: VMWare workstation, Virtual Box, QEMU/KVM, libvirt

REFERENZEN

Details zu den oben genannten Kunden auf Anfrage.