



Mit Sicherheit weiter kommen.



ANDREA KLENK Leiterin Security Solutions



„Sicherheit ist
der Schlüssel
zum Erfolg in
einer globalen
und vernetzten
Welt.“

Gestern. Heute. Morgen.

Bei unserer Gründung im Jahr 1995 haben wir uns das ehrgeizige Ziel gesetzt, die Schlüsseltechnologien für die Märkte der Zukunft zu beherrschen und zu kreativen und kommerziell erfolgreichen Lösungen zu verbinden. Inzwischen haben viele zufriedene Kunden und Partner unsere Kompetenz und langjährige Projekterfahrung in Beratung, Softwareentwicklung und Systemintegration zu schätzen gelernt.

Drei Kernbereiche stehen im Mittelpunkt unserer Arbeit:

- > **Sicherheitstechnologie**
- > **Multimedia-Anwendungen**
- > **Telekommunikation**

Viele unserer Mitarbeiter sind mit den Themen Telekommunikation und Betriebssysteme groß geworden und haben seit Mitte der 80er Jahre in der internationalen Standardisierung von Kommunikationsprotokollen (ITU-T, ETSI, ISO, ...) gearbeitet und diese in Entwicklungen umgesetzt.

Die sich seitdem vollziehenden Neuerungen haben wir aktiv miterlebt und -gestaltet. Dramatische Verbesserungen hinsichtlich Speicherkapazitäten, Rechengeschwindigkeiten und Netzbandbreiten haben den Weg zu multimedialen und interaktiven Anwendungen geebnet. Doch nur in Verbindung

mit fundierten Kenntnissen der Netzwerktechnologie und Telekommunikation sind effiziente und sichere e-Commerce Lösungen wie unsere möglich.

Durch das breite Spektrum und die Fähigkeit zur sinnvollen Verknüpfung der angewandten Technologien sind wir in der Lage, zukunftsorientierte und zugleich praxisnahe Lösungen aus einer Hand anzubieten.



Mit Brief und Siegel.

mtG wurde als eines von nur 12 deutschen Unternehmen als **Prüfstelle für IT-Sicherheit** im Bereich der Common Criteria akkreditiert. Das anspruchsvolle Zulassungsverfahren beim Bundesamt für Sicherheit in der Informationstechnik (BSI) dauerte über ein halbes Jahr. Damit bewies mtG nachdrücklich die fachliche Kompetenz seiner Mitarbeiter und die Wirksamkeit des firmeneigenen Qualitätsmanagements.

Thomas Martin, Leiter der mtG Prüfstelle, und sein Team unterstützen Sie kompetent bei der Evaluierung und anschließenden Zertifizierung Ihrer IT-Komponenten.

Die weltweit abgestimmten Common Criteria (CC) sind internationaler Standard (ISO/IEC 15408) und machen die IT-Sicherheit von Produkten und Systemen bewertbar und vergleichbar. IT-Sicherheitszertifikate nach Common Criteria werden international anerkannt, erhöhen die Vertrauenswürdigkeit von Produkten und werden beispielsweise beim Einsatz im eGovernment Umfeld häufig gefordert.

Die mtG Prüfstelle arbeitet in den folgenden Themenschwerpunkten:

- > **Public Key Infrastrukturen, (z. B. CA-Systeme, Signatur-Anwendungs-Komponenten, PKI-basierende Anwendungen, Identity Management)**
- > **Datenübertragung (z. B. IPSec, VPN-, Application-Server-, WLAN- und VoiceOverIP-Lösungen)**
- > **DRM-Systeme**
- > **Datenbanken**
- > **Firewalls**
- > **Betriebssysteme (z. B. Unix/Linux)**
- > **PC-Sicherheit**

Wenige Schritte zu mehr Sicherheit.

Wo steht Ihr Unternehmen in puncto Common Criteria?

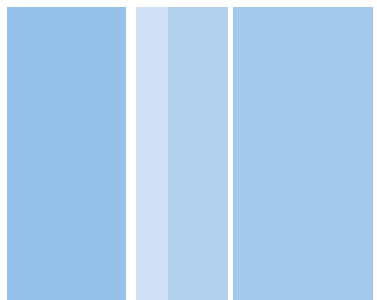
- > Wir informieren und beraten Sie bei allen Fragen zu CC und zum Evaluierungs- und Zertifizierungsverfahren.
- > Wir bieten Schulung und Training im Kontext der CC.
- > Wir helfen Ihnen beim Ermitteln Ihres speziellen „CC-Status“.

So machen Sie sich fit für Common Criteria!

- > Wir helfen Ihnen, existierende Schutzprofile zu interpretieren und für Ihre IT-Produkte oder IT-Systeme zu nutzen.
- > Wir unterstützen Sie beim Erstellen neuer Schutzprofile für Ihre IT-Produkttypen.
- > Wir führen für Ihre IT-Komponenten Vor-Evaluierungsverfahren zu CC durch.

Sichern Sie Ihren Unternehmenserfolg nachhaltig durch international zertifizierte IT-Produkte und IT-Systeme nach Common Criteria!

- > Wir bieten Ihnen Beratung im Evaluierungsprozess an.
- > Wir übernehmen die Evaluierung Ihrer IT-Komponenten.
- > Wir unterstützen Sie beim Zertifizierungsverfahren.



Die Schlüssel zur Sicherheit.

X.509-Zertifikate und Public Key Infrastrukturen (PKI) bilden die technische Grundlage für die sichere Nachbildung traditioneller Geschäfts- und Verwaltungsprozesse in elektronischen Medien.

Konzeption und Realisierung von PKI

Wir sind spezialisiert auf die Bereitstellung und Pflege von Certification Authority (CA)- und Verzeichnisdiensttechnologie, sowie deren begleitende Infrastruktur. Wir haben beispielsweise im Auftrag der Deutschen Telekom deren CA-Plattform festgelegt und die dafür erforderliche Hardware- und Software-Infrastruktur im Trust Center aufgebaut. In unseren Räumen betreiben wir zudem die Entwicklungs- und Testumgebung dieser Plattform.

Zur nahtlosen Integration von X.509 Zertifikaten in Anwendungen und Unternehmensprozesse bietet sich unser Produkt mtG-CARA (mtG Certification Authority und Registration Authority) mit entsprechenden Schnittstellen an. Alle notwendigen Registrierungs-, Veröffentlichungs-, Verwaltungs- und Abrechnungsprozesse einer Unternehmens-PKI können damit flexibel, effizient und benutzerfreundlich abgebildet werden.

Die Bausteine unserer Erfolge sind Standardkonformität, Interoperabilität und Kundenorientierung.

Auf Grund dieser Strategie können wir – wie kaum eine andere Firma in Deutschland – auf eine große Anzahl von PKI-Projekte zurückblicken. Dabei sind wir zu Recht stolz darauf, dass unsere Lösungen nicht im Stadium von Studien, Pilotversuchen, Demoversionen oder Showcases steckengeblieben sind, sondern sich durchweg in der Praxis bewährt haben und in den Wirkbetrieb überführt werden konnten.

Unser im Bereich PKI erworbenes Fachwissen bringen wir in die Arbeit des TeleTruST Deutschland e.V.* und des CAST-Forums** ein.

* TeleTruST Deutschland e.V. (Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik) befasst sich mit Standardisierung, Harmonisierung und Öffentlichkeitsarbeit in Bezug auf sicherheitsrelevante Themenstellungen. **Siehe auch www.teletrust.de**

** Das in Darmstadt ansässige CAST-Forum (Competence Center for Applied Security Technology) ist eine Kooperation von Hochschuleinrichtungen, Forschungsinstituten und Firmen zur Förderung von Technologietransfer, Aus- und Weiterbildung im Bereich der Sicherheitstechnologien. **Siehe auch www.cast-forum.de**

Risiken rechtzeitig erkennen und ausschalten.

Für jedes zukunftsorientierte Unternehmen ist es absolut notwendig, in regelmäßigen Abständen Schwachstellenanalysen durchzuführen, da ein IT-System keine feste, unveränderliche Größe ist, sondern laufenden Veränderungen unterliegt, die Auswirkungen auf die Sicherheit des Systems haben können.

Aktuellen Studien und Umfragen zufolge nennen deutsche Unternehmen als Hauptgefahren für ihre IT-Sicherheit:

- > **Irrtum und Nachlässigkeit der eigenen Mitarbeiter (unbeabsichtigte Fehler)**
- > **Gefährdung durch Malware (Viren, Würmer, etc.)**
- > **Softwaremängel**
- > **gezielte Angriffe**

Auch unvermeidliche Systemänderungen durch Einsatz neuer Technologien, Upgrades vorhandener Software, Erweiterungen der Funktionalität, Reaktionen auf Sicherheitsvorfälle und vieles mehr machen eine regelmäßige Überprüfung notwendig.

Die Folgen von Sicherheitslücken können in vielfacher Hinsicht sehr schwerwiegend sein und reichen von der Möglichkeit der Datenmanipulation durch Angreifer bis hin zu Produktionsausfällen und rechtlichen sowie finanziellen Konsequenzen (KonTraG, Basel-II).

Wir spüren Sicherheitslücken in Extranet und Intranet unserer Kunden auf und geben wertvolle Unterstützung bei der Beseitigung der Schwachstellen.

Bei der Durchführung von Tests und Analysen fungieren wir als neutrale externe Instanz und unterliegen nicht der Gefahr der „Betriebsblindheit“. Hohe Effizienz durch unser spezifisches Fachwissen und unsere langjährige Erfahrung sowie Diskretion und eine enge, vertrauensvolle Zusammenarbeit mit IT- oder Fachabteilung unserer Kunden sind dabei selbstverständlich.

Unsere Leistungen umfassen unter anderem:

- > **Penetrationstests**
- > **Sicherheitsprüfung kundenspezifischer Webanwendungen**
- > **White-Box-Analysen und -Tests**



Wir profitieren von unseren fachlichen Wurzeln.

Unser fundiertes Wissen im Bereich der Telekommunikation verbindet sich in sehr naheliegender Weise mit fundierter Security-Expertise im Bereich der Virtual Private Network (VPN) Technologie.

Die IPSec-Protokollserie hat sich als wichtigster Standard zur Realisierung von VPNs herausgebildet, bei denen auf der Basis öffentlicher, unsicherer Netze private und sichere Netze zum Austausch sensibler Daten etabliert werden.

IPSec garantiert Verschlüsselung und zuverlässige Authentifizierung auf der Netzwerkebene, lässt sich also sehr vielfältig für alle IP-basierten Anwendungen einsetzen.

> Konzeption und Aufbau von VPNs:

ENX (European Network eXchange)

Dieses einheitliche, europaweite Branchennetzwerk für die Automobilindustrie unterscheidet sich vom öffentlichen Internet durch besondere Qualitätsmerkmale in Bezug auf Leistungsfähigkeit, Verfügbarkeit sowie Sicherheit. Die Sicherheit in diesem Netz gewährleisten IPSec und die PKI.

mtG ist ein strategischer Partner der ENX-Organisation. Jürgen Ruf, PKI-Experte, hat von Beginn an die PKI für das ENX konzipiert, die später von mtG zusammen mit der Deutschen Telekom AG realisiert wurde.

SNX (Siemens Network Exchange)

Siemens baut im Rahmen des Projekts NGNI (Next Generation Network Infrastructure) ein weltweites VPN SNX auf, um alle Standorte seiner Bereiche und Beteiligungen anschließen zu können. Das SNX ist vergleichbar mit dem ENX, allerdings nur als Extranet für Siemens ausgelegt. mtG berät Siemens beim Einsatz der Sicherheitstechnologie (PKI und IPSec) im SNX.

> IPSec Multicast Gateway

Die Telekom-Tochter T-Systems GmbH hat gemeinsam mit mtG ein Verfahren entwickelt, das es Anbietern von Filmen, Musik, News und ähnlichen, attraktiven Inhalten erstmals ermöglicht, ihre Daten, die im sogenannten „Multicast“-Verfahren übertragen werden, sicher zu verschlüsseln. Die neue Verschlüsselungstechnik gilt unter Fachleuten als „Missing Link“ des Pay-TV im Internet.

Das Multicast-Verfahren spart Bandbreite bei der Übertragung des gleichen Inhalts an viele Teilnehmer. Für Internet-Anwendungen wie Pay-TV, Pay-per-View, Business TV und auch andere, nicht-videoorientierte Anwendungen ist es damit die optimale Übertragungsweise.

Ein Problem blieb allerdings bis vor kurzem ungelöst: Bisher mussten sich Anbieter zwischen effizienter Datenübertragung (Multicast) und Sicherheit entscheiden, denn es gab kein sicheres Verschlüsselungsverfahren. Die Lösung kam von mtG: Mit der neuen Technologie ist es weltweit erstmals gelungen, das standardisierte und erprobte Sicherheitsprotokoll IPSec um die Unterstützung von Multicast-Datenströmen zu erweitern. Das Konzept wurde vom Internet-Standardisierungsgremium IETF unter dem Namen „Group Key Management Architecture“ veröffentlicht.

> IPSec-TestLAB

Testen ist besser als probieren – deshalb haben unsere Testingenieure ein klares Ziel: möglichst viele Interoperabilitätsprobleme in IPSec-Produkten aufzuspüren. Das IPSec-TestLab der mtG hat sich hierfür europaweit einen hervorragenden Ruf erworben.

IPSec ist zwar als RFC für IP Security schon längere Zeit verabschiedet, jedoch lassen fehlende Definitionen, Optionen

und Interpretationen im Standard immer noch Spielraum für unterschiedliche Implementierungen zu, die dann zu Interoperabilitätsproblemen führen.

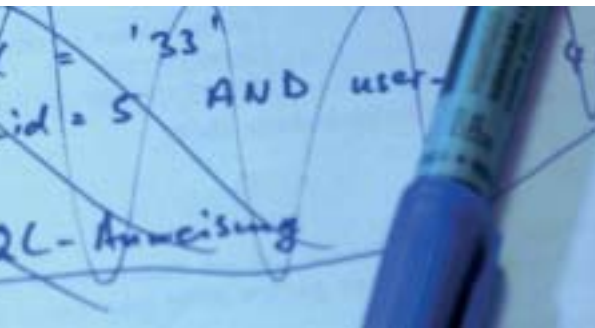
Im IPSec-TestLab werden IPSec Devices verschiedener Hersteller von Erik Neumann und seinem Team auf deren Interoperabilität untereinander getestet. Alle Tests laufen automatisiert ab und entsprechende Logdateien werden generiert, die die Basis für die Dokumentation der Testfälle bilden. Die IPSec Testsuites sind derart gestaltet, dass sie typische Anwendungen simulieren.

Die Leistungen des IPSec-TestLab können mittels Remote Access genutzt werden. Diese Möglichkeit bietet sich vor allem an, wenn Hersteller bereits entwickelte oder sich in der Entwicklung befindende IPSec Devices gegen vorhandene Devices testen möchten.

Unser Testlabor erlaubt es, nahezu beliebige Netzwerktopologien aufzubauen. Wir können damit die IPSec Devices relativ nahe an der Netzwerkconfiguration des Kunden testen.

Neben Interoperabilitäts-Tests führen wir auch Performance-Tests durch, die zuverlässige Aussagen hinsichtlich des Durchsatzes der eingesetzten Devices ermöglichen.

Im Auftrag der ENX Association (www.enxo.com) betreiben wir deren offizielles IPSec Testlabor, in dem IPSec Devices verschiedener Hersteller (z. B. Nokia, TimeStep, Checkpoint, Cisco, BinTec, Alcatel, usw...) auf deren Konformität zu den im ENX festgelegten Profilen getestet und zertifiziert werden. Nur mit dem von mtG vergebenen Prüfsiegel „ENX-IPSec certified“ dürfen die Devices im ENX Netz eingesetzt werden.



Keine Praxis ohne Theorie.

Jede neue Technologie muss verstanden und sinnvoll in die jeweiligen Arbeits- und Produktionsprozesse eingebunden werden. Den zunehmenden Sicherheitsrisiken in einer vernetzten Welt muss mit effizienten Maßnahmen begegnet werden.

SICHERHEITSKONZEPTE

Wir erstellen Sicherheitskonzepte, beraten bei der Formulierung der notwendigen Verhaltensrichtlinien und planen deren Umsetzung unter den unterschiedlichsten Aspekten.

Technik:

- > Netzwerksicherheit (Firewalls, Router, Protokolle, VPNs, IPSec)
- > Betriebssystemeicherheit
- > Datensicherheit

Personelle und organisatorische Gesichtspunkte:

- > Sensibilisierung der handelnden Personen für sicherheitsrelevante Aspekte
- > stetige Information und Weiterbildung des Personals eines Unternehmens zum Thema Sicherheit
- > notwendige Zusammenarbeit mit wichtigen Sicherheitsgremien (BSI, CERT, ...)

Zusätzlich muss vermittelt werden, dass die Umsetzung des Sicherheitskonzepts – das Sicherheitsmanagement – ein permanenter Prozess ist, der stetig sich ändernden Anforderungen in der Infrastruktur eines Unternehmens angepasst werden muss.

Ein funktionierendes Sicherheitsmanagement signalisiert Professionalität und ist ein Qualitätsmerkmal. Es erzeugt Vertrauen bei Auftraggebern, Lieferanten und Kunden und stellt dadurch einen nicht zu unterschätzenden Wettbewerbsvorteil dar.

media transfer AG
Dolivostr. 11
D-64293 Darmstadt

Tel +49 6151 8193-0
Fax +49 6151 8193-43
e-Mail contact@mtg.de

www.mtg.de

media transfer AG
Dolivostr. 11
D-64293 Darmstadt

Tel +49 6151 8193-0
Fax +49 6151 8193-43
e-Mail contact@mtg.de

www.mtg.de

