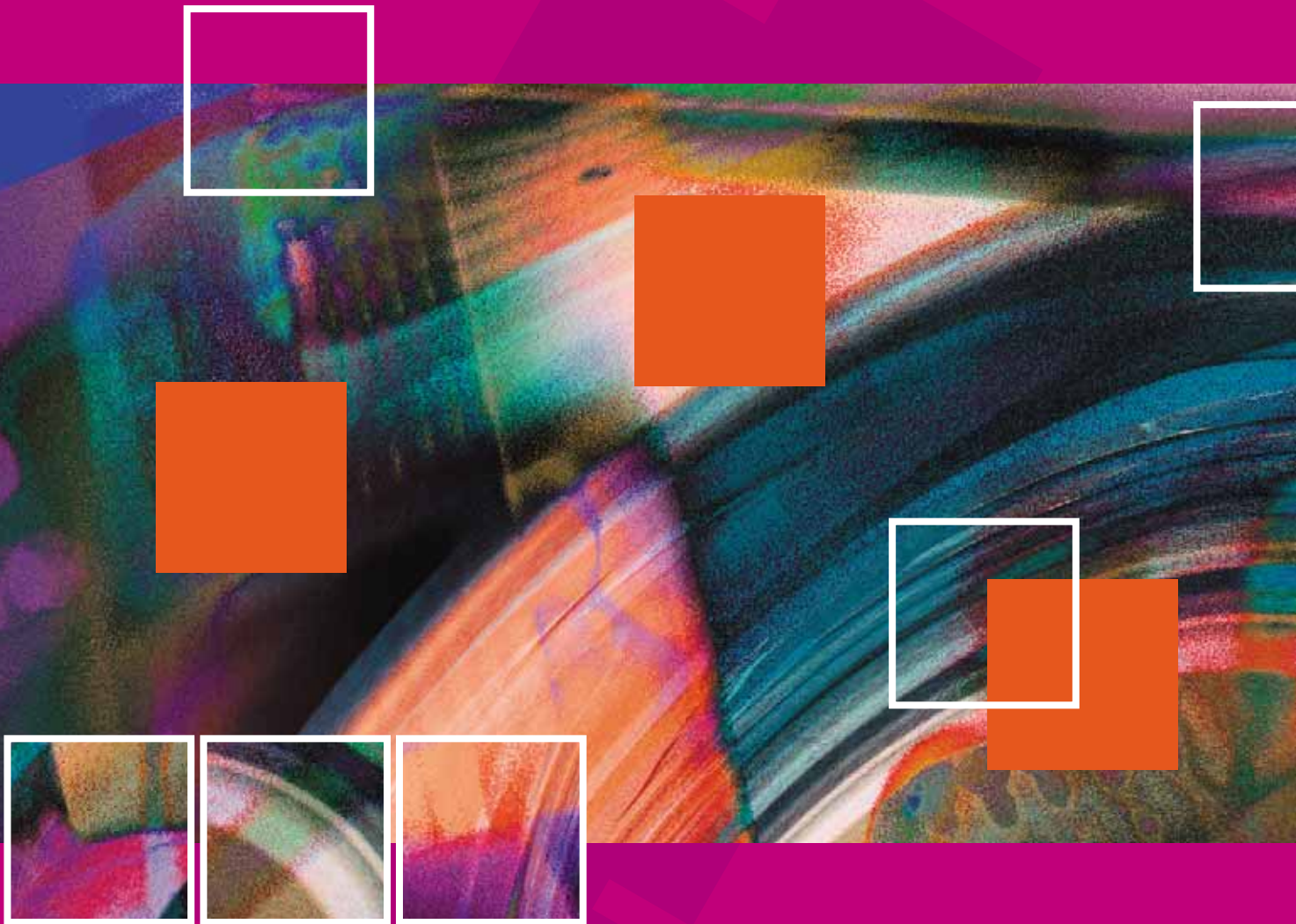


# IT SECURITY

2 0 0 6



## Managing Enterprise Security

Konferenz: 30. - 31.5.2006 – Schrammehalle München



### Referenten



Jörg Altmeier,  
wikima4 AG



Stefan Bumerl,  
cryptas GmbH



Peter Dölling,  
Defense AG



Alexander Geschonneck,  
HiSolutions AG



Frederik Humpert,  
Humpert & Partner



Lukas Grunwald,  
DN-Systems Enterprise  
Internet Solutions GmbH



Tobias Kirchhoff,  
TÜV Secure IT GmbH



Timo Kob,  
HiSolutions AG



Klaus Lenssen,  
Cisco Systems GmbH

### Die Themen im Überblick

#### Enterprise Security Management – from Real-time to Forensic

Der Bereich Security hat sich in den letzten Jahren stark verändert. Die Security ist genauso komplex wie alle anderen IT-Prozesse, wenn nicht sogar komplexer. Ein alleiniges Management von Security reicht nicht mehr aus. Das Ziel von Enterprise Security Management ist es, Organisationen und Unternehmen Tools zur Verfügung zu stellen, die wirkliche Bedrohungen ihrer Services in Echtzeit aufzeigt, den Ursprung solcher Attacken und wie die einzelnen Geschäftsbereiche davon betroffen sind, vollumfängliche Integration in die existierenden IT-Prozesse etwa ITIL, die Möglichkeit des Reportings für die Befolgung von Vorgaben (intern und extern) sowie als Unterstützung während gerichtlichen Untersuchungen. Wir zeigen die Prozesse, Technologien und mögliche Lösungen auf, die aus unserer Sicht für das Enterprise Security Management notwendig sind.

#### Computer Forensik

Dieses Teilgebiet der IT-Security beschäftigt sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen etwa durch Analyse von digitalen Spuren. Die Ziele einer forensischen Analyse (etwa nach internen Attacken, Datenlöschungen, Sabotage, Datendiebstahl, anderen Sicherheitsvorfällen) sind in der Regel die Identifikation des/r Angreifer/Täter, das Erkennen der Methode oder der Schwachstelle, die zum Vorfall oder der Straftat geführt haben, die Ermittlung des Schadens und die Sicherung der Beweise für weitere juristische Aktionen. Hilfreich sind dazu in einem zweiten Schritt Tools, deren es viele auch aus dem Open Source-Bereich gibt. Wir zeigen exemplarisch auf, welchen Tools Sie vertrauen können.

#### Live Hacking

In diesem Vortrag zeigen wir, wie einfach es ist, vermeintlich sichere Technologien zu knacken. Anhand des „VPN-Hijacking“ stellen wir dar, wie schnell und einfach Sitzungen im Virtual Private Network (VPN) als Königsweg der sicheren Verbindung zu entführen sind. In dem Kapitel „VoIP - Mithören leicht gemacht“ schneiden wir ein Telefonat via Voice over IP (VoIP) mit. Ferner stellen wir den Hacker-Baukasten Metasploit dar und sensibilisieren auch damit die Sinne für Attacken gegen das eigene Netz oder Systeme. Dabei gehen wir immer auf mögliche Gegenmaßnahmen und Voraussetzungen ein.

#### Identity Management

Ein Werkzeugkasten für das Identity Management (IdM) ist wünschenswert. Gibt es den? Die Liste der Wünsche für den Einsatz eines IdM-Systems sind lang: Redundante Benutzerdaten eliminieren; Legacy-Applikationen einfach integrieren; Benutzer, Kunden, Services, Maschinen etc. managen; einfach administrieren; Access Management übernehmen; Globales SSO realisieren; Security Policies automatisch umsetzen; User Help Desk entlasten, alte Accounts automatisch mappen; Passwörter und Profile synchronisieren und und und... Am Beginn aber stehen immer die Prozessarbeiten!

#### ITIL & IT-Security

Sicherheit muss in IT-Prozesse integriert werden. Dazu gehört es, die Aufgaben, Rollen und Key Performance Indicators zu kennen, die implementiert werden müssen, um ein erfolgreiches IT-Security Management aufzubauen. Durch ITIL-Konformität wird der Bezug zu den weiteren IT-Prozessen hergestellt, so dass die Sicherheit nicht nur theoretisch besteht.

#### Sicherheit für Enterprise J2EE-Applikationen

Dieser Vortrag gibt einen Überblick auf Angriffsstrategien und Verteidigungsmöglichkeiten für J2EE-Applikationen (JSP, Servlets, EJBs, JMS und JDBC). Wichtige Themen wie Single-Sign-On, Datenbanken, Integration mit PKI-Systemen und andere werden behandelt. Der Vortrag wird praxisnah und mit Beispielen gestaltet.

#### Service-orientierte Netzwerkkonstrukturen

Mit der wachsenden Bedeutung von Basel II, SOX oder anderen Regularien rückt das Riskmanagement und letztlich die IT-Sicherheit für Unternehmen noch mehr in den Fokus. Während die Geschäftsprozessoptimierung zur Einführung von SOA führt, stellt sich gleichzeitig die Frage, wie kann man die Prozesse absichern ohne zusätzlich die Komplexität zu erhöhen. Die Antwort hierauf ist die konsequente Anwendung des SOA-Gedankens und die Abbildung der Konzepte auf der Netzwerkebene. So wird ein holistischer Ansatz möglich, der nicht nur das Netzwerk als solches, sondern die gesamte Prozesskette absichert.



### Referenten

#### Monitoring Enterprise Security

Um Attacken auf die IT-Infrastruktur zu entdecken und richtig darauf zu reagieren, muss ein Security Management und Monitoring System implementiert sein, welches genau auf die Sicherheitsbedürfnisse der Unternehmung abgestimmt ist. Zusätzlich ist das Compliance Reporting, das nachweisbare Einhalten der gesetzlichen und regulatorischen Rahmenbedingungen, ein wichtiger Indikator für das IT Security Risk Management.

#### Prozessorientiertes IT-Security Managementsystem

Um den Status der IT-Sicherheit im Unternehmen ermitteln zu können, sind Kennziffern unerlässlich. Zunächst ist der Aufbau eines umfassenden und vollständigen IT-Sicherheitsprozesses zwingend, dann geht es im zweiten Step um die Erweiterung und/oder Optimierung bestehender Prozesse. Wir stellen ein IT-Security Prozessmodell auf Basis des internationalen Standards ISO 27001 vor sowie ein Security Process Framework (SPF). Dabei handelt es sich um ein umfassendes IT-Security Rahmenwerk, bestehend aus definierten und bewährten Methoden, Verfahren und Best Practices.

#### SAP-Security

Die Anforderungen an die Sicherheit von SAP-Systemen steigen mit der Komplexität der eingesetzten Funktionalitäten. Zahlreiche Unternehmen sind noch nicht genügend vor möglichen Bedrohungen geschützt. Eine aktuelle Studie zum Status Quo ergibt eine Liste der wichtigsten Verbesserungen und zeigt überraschende Ergebnisse. Bei den Verantwortlichen steigt die Erkenntnis, dass es Zeit zum Handeln ist. Eine Roadmap gibt Hilfestellung bei der Umsetzung der wichtigsten Schritte.

#### SOA und Security

Die Einführung und die Absicherung service-orientierter Architekturen ist für viele Unternehmen eine Herausforderung. Die Sicherheitsanforderungen sind deutlich höher als in herkömmlichen monolithischen Strukturen. Dabei kann man vieles falsch machen. Ein Weg wäre die Implementierung für den Enterprise Service Bus (ESB) und andere Service-orientierte Architekturen selbst konsequent als service-orientierte Lösung zu implementieren.

#### Standardisierungen erfolgreich umsetzen

Immer wieder stehen Anwender vor dem Problem, neue Standards umzusetzen. Am Beispiel von SSE-CMM als Basis zur Etablierung und Bewertung eines ISMS zeigen wir, wie dies funktioniert. Hilfreich ist auch der Einsatz erfolgreiche Methoden. Ziel ist es die Risiken und Sicherheitsbedürfnisse im Unternehmen zu erkennen und zu analysieren. Wir demonstrieren dies am Beispiel der Octave-Methode, die an der Carnegie-Mellon-Universität entwickelt wurde und im IT-Bereich zunehmend zur Anwendung kommt. Im Unterschied zu herkömmlichen Verfahren wird hier die gesamte IT-Struktur mit ihren vielfältigen Verknüpfungen technischer und organisatorischer Art als Gesamtsystem betrachtet.

#### Web Application Security

Angriffe auf Web-Anwendungen wie etwa das Phishing haben sich in den letzten Monaten zu einem Kernthema im Bereich IT-Sicherheit entwickelt. Herkömmliche IT-Sicherheitslösungen wie Firewalls oder IDS/IPS bieten keinen ausreichenden Schutz gegen derartige Angriffe. Das Web, speziell das HTTP-Protokoll, wurde nicht für komplexe Anwendungen konzipiert, die heute aber im e-Business aus wirtschaftlichen Gründen eine Notwendigkeit geworden sind. Die daraus resultierenden Schwachstellen von Web-Anwendungen werden noch verstärkt durch die hohe Komplexität, verursacht von der Vielzahl von Web-Scripts, Frameworks und Web-Technologien. Letztlich erfordert deshalb jede Web-Anwendung ein eigenes, auf ihre jeweilige Logik zugeschnittenes Schutzprofil.

#### Sicherheit für Web Services und SOA

Die Sicherheit von SOA mit Web-Services wird ausführlich behandelt. Themen sind: Security Design Pattern für SOA, die Benutzung von SAML, die Behandlung von Identitäten, konkrete Maßnahmen für Authentication mit Web Services, Verschlüsselung von Messages und die Integration mit PKI-Systemen. Außerdem werden einige Schwachstellen von Web Services anhand von praxisnahen Beispielen aufgezeigt.

#### Vulnerability Management

Gute Lösungen sollten sich nicht nur durch die Informationen zu den identifizierten Schwachstellen und relevanten Applikationen auszeichnen, sondern auch Router-Konfigurationen und Firewall-Regeln in einem integrierten Sicherheitsmodell darstellen und verknüpfen. Zum Leistungsumfang sollten auch simulierte Angriffe gehören. Diese sollen aus den gefundenen Schwachstellen die ca. 1 bis 2% wirklich kritischen IT-Schwachstellen identifizieren und aufzeigen. Auf Basis solcher Ergebnisse wird berechnet, welches Risiko die einzelnen Schwachpunkte für Geschäftsapplikationen bedeuten und Schutzmaßnahmen vorgeschlagen.



Fabian Libeau,  
Arcsight



Marco Lorenz,  
cirosec GmbH



Georg Markowski,  
Media@Net



Dr. Dieter Masak,  
plenum AG



Alexander Meisel,  
art of defence GmbH



Ulrich Parthier,  
Publisher IT SECURITY



Heiko Rudolph,  
admeritia



Dr. Bruce J. Sams,  
Optima bit GmbH



30. Mai 2006

08:30 – 09:00 **Registrierung & Second Breakfast**

**Block 1: SAP Security**

**09:00 – 09:45 Risk Management in SAP-Systemen**  
*Alexander Geschonneck, HiSolutions AG*

- SAP-Server, das vergessene Risiko
- Absicherung der User
- Logging und Auditing
- Sicherheit bei Webschnittstellen

**09:45 – 10:30 Roadmap zur erfolgreichen Umsetzung von Sicherheit in SAP-Systemen**  
*Jörg Altmeier, wikima4 AG*

- Studie zum Status Quo der Sicherheit von SAP-Systemen
- Von der Sicherheit der Verfügbarkeit zur Regulatory Compliance
- SAP Security Framework zur Strukturierung
- Roadmap zur Umsetzung von Best Practices

10:30 – 11:00 **Kommunikationspause**

**BLOCK 2: Monitoring Enterprise Security**

**11:00 – 11:45 Frühwarn- und Überwachungssysteme für Administratoren**  
*Georg Markowski, Media@Net*

- System-Sicherheit und -Kontrolle
- Erkennen von wichtigen Parametern
- Produkte am Markt & Linux-Alternativen
- Live-Demo

**11:45 – 12:30 Monitoring: Von Prozessen zur toolüberwachten Unterstützung**  
*Peter Dölling, Defense AG*

- Prozesse definieren
- Produkt evaluieren
- Kosten und Nutzen klären
- Security Monitoring „out of the box“

12:30 – 13:30 **Business Lunch**





30. Mai 2006

### BLOCK 3: Workshops (bitte zwischen A - B - C wählen)

13:30 – 15:00

#### **A: ITIL & IT-Security**

*Timo Kob, HiSolutions AG*

- Vorstellung der BSI-Studie „ITIL & Informationssicherheit“
- Wo kann ein Security Manager ITIL-Prozesse nutzen?
- Wie kann ein Security Manager ITIL-Prozess unterstützen?
- Synergie-Effekte nutzen

#### **B: Live Hacking**

*Heiko Rudolph, admeritia*

- VPN-Hijacking – Wenn der Königsweg unsicher wird
- Metasploit – Ein Baukasten für Hacker und die Folgen für Sie
- VoIP-Hacking: Mithören leicht gemacht
- Strategien gegen Hacking-Attacken

#### **C: Antizipation von Security-Gefahren: Die Simulation von Angriffsszenarien**

*Marco Lorenz, cirosec GmbH*

- Sicherheitslücken
- Strategien im Vulnerability Management
- Benefits
- Tools im Vergleich (Skybox, Lumeta, Foundstone, Qualys u.a.)

15:00 – 15:30

**Kommunikationspause**

### BLOCK 4: Internet & Netzwerk – Live Szenarien

15:30 – 16:15

#### **Verschlüsselung in der Praxis**

*Stefan Bumerl, cryptas GmbH*

- Absicherung von Festplatten, E-Mails, PDAs und anderer Daten
- Unterschiedliche Ansätze auf dem Prüfstand
- Möglichkeiten für das Recovery
- Deployment und Management einer Lösung

16:15 – 17:00

#### **Security-Management**

*Fabian Libeau, Arcsight*

- Enterprise Security Management im Überblick
- Integration von ESM in bestehende IT-Prozesse
- Unterstützung und Umsetzung von Sicherheitsstandards wie etwa ISO 17799
- Praxisbeispiel CERT

17:00 – 17:30

#### **Paneldiskussion**

#### **Werkzeugkasten für das Identity Management**

*Diskussionsrunde mit Ulrich Parthier*

Ab 19:00

**Festliches Dinner**



### 31. Mai 2006

#### BLOCK 5: Computer Forensik

**09:00 – 09:45**     **Praktische Aspekte der Computer Forensik**

*Lukas Grunwald, DN-Systems Enterprise Internet Solutions GmbH*

- Managementrahmen der forensischen Analyse
- Organisationssteuerung/Bewusstseinssteuerung
- Technische Umsetzung/Techniksteuerung
- Anti-Forensik

**09:45 – 10:30**     **Tooleinsatz in der Computer Forensik**

*Alexander Geschonnek, HiSolutions AG*

- Der Ermittlungsprozess
- Der Nutzen von Forensik-Tools
- Kriterien für die Toolauswahl
- Der ideale Werkzeugkasten

**10:30 – 11:00**     **Kommunikationspause**

#### BLOCK 6: Standardisierungen erfolgreich umsetzen

**11:00 – 11:45**     **SSE-CMM als Basis zur Etablierung und Bewertung eines ISMS**

*Timo Kob, HiSolutions AG*

- SSE-CMM/ISO21827 - der vergessene Standard
- Den Reifegrad der Security-Prozesse ermitteln
- ISO27001 sagt, was nicht funktioniert – SSE-CMM ergänzt, warum es nicht funktioniert
- SSE-CMM als Framework für die Prozess-Gestaltung

**11:45 – 12:30**     **Octave: Methodik zur Risikoanalyse**

*Frederik Humpert, Humpert & Partner*

- Methodik
- Techniken
- Ziele
- Phasenmodell

**12:30 – 13:30**     **Business Lunch**

#### BLOCK 7: Workshops – Teil 1

**13:30 – 15:00**     **A: Online-Test von Web-Applikationen**

*Alexander Meisel, art of defence GmbH*

- Authentifizierung und Session Handling
- Command Injection & Input Validation
- XSS – Indirekte Angriffe
- Secure Application Design & Programming



31. Mai 2006

**B: Einführung eines prozessorientierten IT-Security Managementsystems**

*Tobias Kirchhoff und Bruno Tenhagen, TÜV Secure IT GmbH*

- Organisationsstruktur von wirksamen Prozessen (Top-Down-Ansatz)
- Geeignete Standards und Best Practices zur Einführung und Etablierung
- Umsetzung im Hinblick auf die individuelle Unternehmenskultur
- Prozessmodell

**C: Sicherheit für Enterprise J2EE-Applikationen**

*Dr. Bruce Sams, Optima bit GmbH*

- Vor/Nachteile des J2EE Sicherheitsmodells
- Single-Sign-On
- Application Integration (TIBCO, MQ-Series, usw.)
- PKI mit J2EE Applikationen

15:00 – 15:30 **Kommunikationspause**

**BLOCK 8: Workshops – Teil 2**

**15:30 – 17:00 A: Sicherheit für Web Services und SOA**

*Bruce J. Sams, Optima bit GmbH*

- Besondere Schwachstellen bei Web Services
- Sicheres Design in der SOA-Architektur (SSO, XML Gateways)
- Nachrichtensicherheit
- WS-Security, SAML und andere Sicherheitsstandards

**B: Service-orientierte Netzwerkarchitekturen**

*Klaus Lenssen, Cisco Systems GmbH*

- Wandel der Rolle des Netzwerkes im Unternehmen – IIN
- Evolution der Bedrohungen
- Vorteile einer SONA aus Security-Sicht
- Zeitrahmen

**C: SOA und Sicherheit**

*Dr. Dieter Masak, plenum AG*

- Service-orientierte Architekturen: Struktur und Einsatz
- Sicherheitsarchitekturen
- Web Service-Lücken
- Sicherheitsattacken

**17:00 – 17:30 Paneldiskussion**

**Mobile, Inter- und Intranet-Security: Wie sieht ein proaktiver Schutz aus?**

*Diskussionsrunde mit Ulrich Parthier*





## Anmeldung

**Faxantwort + 49 8104 649422**

Veranstaltungsort:  
Schrannenhalle München  
Viktualienmarkt 15  
80331 München  
U/S-Bahnstation Marienplatz

Name

Firma

Funktion

Straße

PLZ/Ort

Tel.-Nr.

Fax-Nr.

E-Mail

### Teilnahmebedingungen

- Hiermit melde ich mich verbindlich zur Konferenz „Managing Enterprise Security“ in München an.
- Frühbucherrabatt bis 30. April 2006                      690.– Euro zzgl. MwSt. inklusive Apple iPod nano.
- Ab dem 1. Mai 2006    790.– Euro zzgl. MwSt.

Alle Preise verstehen sich zzgl. der zum Zeitpunkt der Rechnungsstellung gesetzlichen MwSt.

Rechnungsanschrift (falls abweichend)

Es gelten die AGBs des IT Verlag für Informationstechnik GmbH. Diese sind mir bekannt und jederzeit unter [www.it-verlag.de](http://www.it-verlag.de) einsehbar.

Datum

Stempel/rechtsverbindliche Unterschrift