

IT-Sicherheits-Forum 2008

Agenda

ComConsult
Akademie

GAI
NetConsult

Montag, 26.05.08 Tutorien - bitte wählen Sie ein Tutorium auf der Folgeseite aus!!

Alle Tutorien finden parallel statt und starten um 09:30 Uhr und enden gegen 17:00 Uhr

Tutorium 1: Aktueller Stand der IT-Sicherheit Bedrohungen, Technik, Organisation

Detlef Weidenhammer,
GAI NetConsult GmbH

09:30 Uhr - 09:45 Uhr Begrüßung / Übersicht

09:45 Uhr - 10:45 Uhr

IT-Sicherheit zwischen Datenschutz und staatlicher Überwachung

- Entwicklung der Überwachungsbefugnisse des Staates
- Rechtsstaatliche Grenzen staatlicher Eingriffsmöglichkeiten
- Informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität
- Konsequenzen für die IT-Sicherheit im Unternehmen

Dirk Fox,
Secorvo Security Consulting GmbH

10:45 Uhr - 11:30 Uhr

Web 2.0: Techniken, Trends, Risiken

- Typische Sicherheitsrisiken bei Ajax-basierten Anwendungen
- XSS 2.0, Bye Bye Same Origin Policy
- RIA: Sicherheit bei Flash, Silverlight und AIR
- Prüfung und Sicherung von Anwendungen im Web 2.0

Björn Fröbe,
GAI NetConsult GmbH

Tutorium 2: Security Awareness Methoden, Konzepte, Best Practice

12:00 Uhr - 13:00 Uhr

Analyse des „Storm Worm“

- Gefahren durch Botnetze
- Technischer Überblick zu Storm Worm
- Empirische Messergebnisse
- Schutz vor Storm und anderen Botnetzen

Thorsten Holz,
Universität Mannheim

14:30 Uhr - 15:15 Uhr

Frühwarnung und Lagebild -

Neue Herausforderungen für das Incident Management

- Stand aktueller Frühwarnsysteme in der Praxis
- Sensorik und Auswertung verfügbarer Daten
- Bedeutung von Open Source Intelligence
- Notwendigkeit kooperativer Ansätze für eine breite Nutzung

Dr. Klaus-Peter Kossakowski,
PRESECURE Consulting GmbH

15:15 Uhr - 16:00 Uhr

Sicherheitsaspekte virtualisierter Umgebungen

- Threats & Vulnerabilities in virtualisierten Umgebungen
- Definition von Kriterien für „sichere Virtualisierung“
- Virtual Appliances & Virtual Shields - Konzepte & Produkte
- Überblick über Härtings-Maßnahmen

Enno Rey, Roger Klose,
ERNW Netzwerke GmbH

Tutorium 3: Oracle Security Bedrohungen und Schutzmaßnahmen

11:00 - 11:30 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

16:30 Uhr - 17:15 Uhr

SAN Security - Sicherheitsaspekte von Storage Area Networks

- Überblick über gängige SAN-Technologien: Fibre Channel und iSCSI
- Sicherheitsprobleme: Zoning, Authentisierung, TCP-IPSchwächen, Man-in-the-Middle-Angriffe
- Technische Schutzmaßnahmen
- Empfehlungen für sicheres SAN-Management

Dr. Stephan Beirer,
GAI NetConsult GmbH

17:15 - 18:00 Uhr

Sind SIEM-Tools schon produktiv einsetzbar?

- Log- und Eventdaten, eine ungenutzte Ressource
- Die Entwicklung vom Loganalyser zum SIEM-Tool
- Kriterien zur Produktauswahl und Marktübersicht
- Ausblick: wohin geht die Entwicklung?

Detlef Weidenhammer,
GAI NetConsult GmbH

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Dienstag, 27.05.08

09:30 Uhr - 09:45 Uhr Begrüßung / Übersicht

09:45 Uhr - 10:45 Uhr

IT-Sicherheit zwischen Datenschutz und staatlicher Überwachung

- Entwicklung der Überwachungsbefugnisse des Staates
- Rechtsstaatliche Grenzen staatlicher Eingriffsmöglichkeiten
- Informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität
- Konsequenzen für die IT-Sicherheit im Unternehmen

Dirk Fox,
Secorvo Security Consulting GmbH

10:45 Uhr - 11:30 Uhr

Web 2.0: Techniken, Trends, Risiken

- Typische Sicherheitsrisiken bei Ajax-basierten Anwendungen
- XSS 2.0, Bye Bye Same Origin Policy
- RIA: Sicherheit bei Flash, Silverlight und AIR
- Prüfung und Sicherung von Anwendungen im Web 2.0

Björn Fröbe,
GAI NetConsult GmbH

12:00 Uhr - 13:00 Uhr

Analyse des „Storm Worm“

- Gefahren durch Botnetze
- Technischer Überblick zu Storm Worm
- Empirische Messergebnisse
- Schutz vor Storm und anderen Botnetzen

Thorsten Holz,
Universität Mannheim

14:30 Uhr - 15:15 Uhr

Frühwarnung und Lagebild -

Neue Herausforderungen für das Incident Management

- Stand aktueller Frühwarnsysteme in der Praxis
- Sensorik und Auswertung verfügbarer Daten
- Bedeutung von Open Source Intelligence
- Notwendigkeit kooperativer Ansätze für eine breite Nutzung

Dr. Klaus-Peter Kossakowski,
PRESECURE Consulting GmbH

15:15 Uhr - 16:00 Uhr

Sicherheitsaspekte virtualisierter Umgebungen

- Threats & Vulnerabilities in virtualisierten Umgebungen
- Definition von Kriterien für „sichere Virtualisierung“
- Virtual Appliances & Virtual Shields - Konzepte & Produkte
- Überblick über Härtings-Maßnahmen

Enno Rey, Roger Klose,
ERNW Netzwerke GmbH

16:30 Uhr - 17:15 Uhr

SAN Security - Sicherheitsaspekte von Storage Area Networks

- Überblick über gängige SAN-Technologien: Fibre Channel und iSCSI
- Sicherheitsprobleme: Zoning, Authentisierung, TCP-IPSchwächen, Man-in-the-Middle-Angriffe
- Technische Schutzmaßnahmen
- Empfehlungen für sicheres SAN-Management

Dr. Stephan Beirer,
GAI NetConsult GmbH

17:15 - 18:00 Uhr

Sind SIEM-Tools schon produktiv einsetzbar?

- Log- und Eventdaten, eine ungenutzte Ressource
- Die Entwicklung vom Loganalyser zum SIEM-Tool
- Kriterien zur Produktauswahl und Marktübersicht
- Ausblick: wohin geht die Entwicklung?

Detlef Weidenhammer,
GAI NetConsult GmbH

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Mittwoch, 28.05.08 Praxis-Workshops - bitte wählen Sie 2 Workshops auf der Folgeseite aus!!

vormittags

9:00 Uhr - 12:30 Uhr

Workshop 1: Aktuelle Produktübersicht „Web Application Firewalls (WAF)“

Workshop 2: VMware - Angriffe und Sicherheits- Maßnahmen mit Live-Demos von Angriffen

Workshop 3: BSI IT-Grundsicherung in der Praxis incl. neuer Bausteine und Tools

nachmittags

14:00 Uhr - 17:30 Uhr

Workshop 4: Vergleich von SIEM-Lösungen Moderierter Produktvergleich mit Liveszenarien

Workshop 5: Praxis der IP-Telefonie-Sicherheit am Bsp. von Cisco Unified Communications Manager (Live-Demos)

Workshop 6: Aktuelle rechtliche Aspekte des E-Mail-Managements

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause

Donnerstag, 29.05.08

9:00 Uhr - 10:00 Uhr

Fixed Mobile Convergence: Gefährdungen und Sicherheitsmaßnahmen

- Techniken zur Integration mobiler Endgeräte in TK-Anlagen und resultierende Gefährdungen
- Seiteneffekte für die IT-Sicherheit durch Roaming zwischen GSM/UMTS und WLAN
- Generic Access Network in UMTS/GSM: Mehrwert für die IT-Sicherheit?
- Absicherung von Smartphones: Was ist überhaupt möglich?
- Konsequenzen für das Netzdesign

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

10:00 Uhr - 11:00 Uhr

Oracle Security 2008 - Letzte Trends in Oracle Security

- Einführende Übersicht zur Oracle Security
- Warum sind Datenbanken auch 2008 noch unsicher?
- Typische Probleme und Lösungen in großen, mittleren und kleinen Unternehmen
- Toolgestützte vs. manuelle Auditierung
- Ausblick in die Zukunft

Alexander Kornbrust,
Red Database Security GmbH

11:30 Uhr - 12:30 Uhr

Sicherheitslücken durch Unified Communications

- Sicherheitsaspekte in CTI, Unified Messaging, Präsenz und Instant Messaging
- Einfallstore TAPI, TSAPI, JTAPI und CSTA
- Unterschätzte Anwendungsschnittstellen ODBC, LDAP und andere
- Sicherheitsmechanismen in den verschiedenen Herstellerlösungen (u.a. MS OCS, Cisco, Siemens) und weitergehende Maßnahmen

Dr. Michael Wallbaum, Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

13:45 Uhr - 14:45 Uhr

Compliance Anforderungen in der IT

- Überblick zu aktuellen Compliance Themen wie SOX, BASELII, Euro-SOX
- Prüfungsstandards und Anforderungen der Prüfer an ein internes Kontrollsystem aus IT-Sicht
- Implementierung der IT-Aspekte des internen Kontrollsystems durch COBIT, ITIL und ISO 27001
- Neue Anforderungen an die Compliance im eCommerce: PCI DSS

Holm Diening,
GAI NetConsult GmbH

14:45 Uhr - 15:45 Uhr

ISO 27001 - kompatible Risikoanalyse mit OCTAVE bei der DAK

- Vorstellung der Methode OCTAVE
- Die DAK und das Projektumfeld
- Planung und Durchführung der Risikoanalyse
- Ergebnisse und Erfahrungen

Christian Aust,
.consecco

15:45 Uhr - 16:00 Uhr

Zusammenfassung und Schlusswort

Detlef Weidenhammer,
GAI NetConsult GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 13:45 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

IT-Sicherheits-Forum 2008

Agenda

ComConsult
Akademie



Faxantwort an: 030/417898-300

Firma: _____

Name: _____

Tutorien: Bitte kreuzen Sie ein Tutorium-Thema an!

1

Tutorium 1: Aktueller Stand der IT-Sicherheit Bedrohungen, Technik, Organisation

IT-Sicherheit heute

- Schwachstellen und Verwundbarkeiten
- Die aktuelle Bedrohungssituation
- Neue Trends bei Schadsoftware
- Zunehmende Risiken durch Spam und Phishing

Die technische Entwicklung

- Risiken durch Funknetze: WLAN, Bluetooth
- Gefährdungen durch Verteilung und Virtualisierung
- Sicherheitsaspekte des Web 2.0
- Multi Level Security in Windows Vista

Neue Anforderungen an das Management

- Vorgaben durch Basel II, KonTraG, MaRisk und andere Vorschriften
- Haftung für Folgen nicht abgedeckter Risiken

Normen der IT-Sicherheit

- Prinzipien der Norm ISO 27001
- IT-Grundschutz-Methodik
- Ergänzende Sicherheitsanalyse und Risikoanalyse
- ISO 27001 Zertifikat auf der Basis von IT-Grundschutz
- Ablauf und Aufwände der Zertifizierung

Dr. Gerhard Weck,
INFODAS GmbH

2

Tutorium 2: Security Awareness Methoden, Konzepte, Best Practice

Konzeptionelle Grundlagen der Awareness

- Zielsetzung, Zielgruppen, Kommunikationswege, Hindernisse

Phasen einer Awarenesskampagne

- Die 5 Schritte zu einer erfolgreichen Kampagne

Führungskräfte mobilisieren

- Relevanz, erfolgreiche Argumentation, Informationsbeschaffung

Praxiserprobte Kampagnenelemente

- Interaktion - die Mitarbeiter erfolgreich packen

Erfolgsmessungen

- Benchmarks für Awarenessmaßnahmen

Natalie Mareth,
Secorvo Security Consulting GmbH

3

Tutorium 3: Oracle Security Bedrohungen und Schutzmaßnahmen

Grundlagen der Oracle Security

- Härten von Oracle Datenbanken (9.2, 10.2, 11g)
- Passworte in der Oracle Datenbank

Bedrohungen der Oracle Security

- Informationsgewinnung über SQL Injection
- Privilegieneskalation über SQL Injection
- Angriffe über / gegen Clients

Typische Angreifer

- externe Hacker, unzufriedene Mitarbeiter (MA), kriminelle MA, neugierige MA

Schutzmaßnahmen

- Verschlüsselung von Daten in der Datenbank (dbms_crypto, Transparent Data Encryption)
- Oracle Zusatzprodukte (Database Vault, Audit Vault)

Alexander Kornbrust,
Red Database Security GmbH

Praxis-Workshops: Bitte kreuzen Sie zwei Workshops an (einen vormittags, einen nachmittags)

9:00 - 12:30 Uhr

1

Workshop 1: Aktuelle Produktübersicht „Web Application Firewalls (WAF)“

Moderierter Produktvergleich mit Liveszenarien

- Sind WAFs inzwischen reif für den Einsatz in der Fläche?
- Wie hoch ist der Konfigurations- und Betriebsaufwand pro Anwendung?
- WAF-Speziallösung oder integrierte Application Delivery Lösung?
- Lässt sich mit WAFs auch im Web 2.0 noch ein ausreichender Schutz realisieren?

Frank Breitschaft,
GAI NetConsult GmbH

2

Workshop 2: VMware - Angriffe und Sicherheits- Maßnahmen mit Live-Demos von Angriffen

- Übersicht über Angriffswege in VMware-Umgebungen (insbesondere VMware ESX)
- Diskussion von Angriffen vom Gast aus
- Demo Escape-Szenarien und „VM Backdoor“ Angriffe gegen Management-Interfaces
- Demo-Angriffe auf Netzwerk-Ebene
- Klassifizierung von Mitigating Controls (Network, Storage, Management)
- Risiko-Analyse & Bewertung von Maßnahmen

Roger Klose,
ERNW GmbH

3

Workshop 3: BSI IT-Grundschutz in der Praxis incl. neuer Bausteine und Tools

- IT-Grundschutz im Überblick
- Anwendung der BSI-Methodik und IT-Grundschutz-Kataloge
- Vorgehensweise beim Aufbau von Sicherheitskonzept und Sicherheitsprozess anhand konkreter Beispiele
- Umgang mit Bausteinen und Maßnahmen
- Vorstellung und Analyse der neuen Bausteine der IT-Grundschutzkataloge
- Einsatz von Tools (BSI Grundschutztool und Verinice)

Oliver Flüs, Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

14:00 - 17:30 Uhr

4

Workshop 4: Vergleich von SIEM-Lösungen

Moderierter Produktvergleich mit Liveszenarien

- Basiskonzepte der vorgestellten Lösungen
- Verschiedene Typen der Event-Collection
- Normalisierung und Aggregation
- Welche Security-Operations werden angeboten?
- Sind die angebotenen Compliance-Reports nutzbar?
- Bewertung von GUI und Real-Time-Monitoring

Detlef Weidenhammer,
GAI NetConsult GmbH

5

Workshop 5: Praxis der IP-Telefonie-Sicherheit am Beispiel von Cisco Unified Communications Manager mit Live-Demos

- Verschlüsselung: wie aufwändig ist die Einrichtung, was bringt sie?
- Härtung des Telefoneservers
- Härtung der Endgeräte
- Worauf muss im Netz geachtet werden?

Dr. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH

6

Workshop 6: Aktuelle rechtliche Aspekte des E-Mail-Managements

- E-Mail-Überwachung nach dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung vom 27.02.2008
- E-Mail-Filterung (Spam/Viren/Content Filter/Data Leakage Protection)
- Vorratsdatenspeicherung bei E-Mails ab 1.1.2009
- E-Mail-Archivierung nach Handels- und Steuerrecht unter Beachtung von GoBS, GdPDU, Datenschutzrecht und den neuen Richtlinien für Wirtschaftsprüfer („EuroSOX“ vom 6.9.2007)
- Information Lifecycle Management

Ulrich Emmert,
esb Rechtsanwälte