

IT-Sicherheits-Forum 2007

Agenda

Montag, 07.05.07 Tutorien - bitte wählen Sie ein Tutorium auf der Folgeseite aus!!

Tutorium 1: Prozessorientiertes

IT-Sicherheitsmanagement mit ITIL

Interaktive Erarbeitung mit den Teilnehmern

IT-Sicherheitsmanagement im Unternehmen

- Ziel, Komponenten, Hindernisse, Nutzen?

ITIL: Die Vorstellung

- Entstehung und Struktur
- Prozesse im Überblick

Der Prozess ITIL Security Management

IT-Sicherheitsmanagement in den ITIL-Kernprozessen

ITIL-Sicherheitsmaßnahmen

- Darstellung der Maßnahmen in den Prozessteilen
- Control
- Plan
- Implement
- Evaluate
- Maintenance
- Report

Koexistenz mit anderen IT-Sicherheitskriterien

- IT-Grundschutz
- ISO 17799 / ISO 27001
- ISO 13335
- CoBIT

Christian Aust,
.consecco

Tutorium 2: Sicheres Netzwerk-Management

Live-Demos und Beispiele aus komplexen Umgebungen

SNMP

- Sicherheitsprobleme und Gegemaßnahmen

SNMPv3

- Architektur und Konfiguration
- Wann SNMPv3 eingesetzt werden muss und wann es nicht eingesetzt werden sollte

Device- Zugriff

- SSH vs. Telnet, Arbeit mit Jumposts, das Problem Web-Interfaces, sicherer Konsolenzugriff

Sichere Konfigurations- und Image-Verwaltung

- Integritätsprüfungen von Konfigs, wichtige Tools (RANCID et.al.)

Logging und Log-Auswertung

- Protokolle & Formate (BSD syslog, syslog-ng, Windows Eventlog), wichtige Tools

Revisionsanforderungen und rechtliche Aspekte

Enno Rey,
ERNW Netzwerke GmbH

Tutorium 3: Information Security Management

von A(udit) bis Z(ertifizierung)

Einführung

- Der Information-Security-Management-Prozess
- Strategie, Konzeption, Umsetzung, Betrieb, Management

Standards

- ISO 27001
- Grundschriftzhandbuch

Security Policy

- Vorgaben, Umfang, Vorgehen bei Erstellung und Umsetzung

Risikoanalyse und Sicherheitskonzept

- Bestandsaufnahme, Schutzbedarfsfeststellung, Bedrohungsanalyse

Business Continuity Management & Emergency Response

- Notfallkonzept und -planung, Sicherheitsvorfälle

Umgang mit Sicherheitsvorfällen

- Management von Vorfällen, organisatorische Umsetzung, Business Continuity

Jörg Völker,
Secorvo Security Consulting GmbH

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

Dienstag, 08.05.07

09:30 Uhr - 09:45 Uhr

Begrüßung / Übersicht

Detlef Weidenhammer,
GAI NetConsult GmbH

09:45 Uhr - 10:30 Uhr

Vista unter Sicherheitsaspekten - Mehrwerte und Risiken?

- User Account Control (UAC) - eine gute Funktionalität, jedoch mit Schwachstellen?
- BitLocker - tatsächlich eine Alternative im Bereich der Festplattenverschlüsselung?
- Gruppenrichtlinien - zentral Sicherheit verbreiten!
- Weitere „Kleinigkeiten“ wie driver signing, Netzwerk, Firewall und Defender, protected mode beim IE7

Michael van Laak,
ComConsult Beratung und Planung GmbH

10:30 Uhr - 11:15 Uhr

Informationsdiebstahl durch Schadsoftware

- Funktionsweise und Infektionswege von Schadsoftware
- Vorbeugende Massnahmen
- Detektionsmechanismen
- Reaktionskonzepte

Tom Fischer,
BfK GmbH

11:45 Uhr - 12:30 Uhr

Neue Gefahren aus der Sicht eines Antivirus-Herstellers

- Derzeitiger Stand der Bedrohungen
- Wie kann man sich vor „Targeted Attacks“ schützen?
- Umgang mit 0-day Exploits
- Wachsende Compliance-Anforderungen bei komplexeren Sicherheitsrisiken

Wolf-Dieter Jahn,
mcAfee

12:30 Uhr - 13:00 Uhr

Podiumsdiskussion „Neue Gefahren durch Malware“

14:30 Uhr - 15:15 Uhr

Netzzugangskontrolle und Desktop Integrity

- Port-basierte Zugangskontrolle mit IEEE 802.1X und EAP
- Rolle von Directory Service und Identity Management
- Zuweisung von VLANs und ACLs über RADIUS
- Cisco NAC und Microsoft NAP in der Analyse
- Was ist von Trusted Network Connect (TNC) zu erwarten?

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

15:15 Uhr - 16:00 Uhr

MPLS Sicherheit

- Sicherheitsaspekte beim Einsatz von MPLS (eigener Betrieb oder „Kauf eines VPN-Produkts“)

- Rahmenparameter und mögliche Sicherheitsmassnahmen
- neue (Ethernet-) Dienste und Sicherheitsprobleme
- Vorstellung einer Checkliste zur Bewertung

Enno Rey,
ERNW Netzwerke GmbH

16:30 - 17:15 Uhr

Sicherheit sensibler Daten

- Bedrohungen für sensible Daten im Unternehmen
- Verschiedene Lösungsansätze
- Vor- und Nachteile der vorgestellten Lösungsansätze
- Handlungsempfehlungen

Stefan Strobel,
cirosec GmbH

17:15 - 18:00 Uhr

Sicherheitsfaktor Mitarbeiter: Aufbau eines Personnel Security Lifecycle

- Bedeutung des Mitarbeiters für die IT-Sicherheit
- Steuerung, Motivation, Maßnahmen
- Bestandteile des Personnel Security Lifecycle
- Projektbeispiele

Christian Aust,
.consecco

11:15 - 11:45 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Mittwoch, 09.05.07 Praxis-Workshops - bitte wählen Sie 2 Workshops auf der Folgeseite aus!!

9:00 Uhr - 12:30 Uhr

Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?

Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen

Workshop 3: Interne Compliance Audits

Workshop 4: Rechtliche Aspekte der Mobile Security

14:00 Uhr - 17:30 Uhr

Workshop 1n: Was leisten Herstellerlösungen zur Netzzugangskontrolle?

Workshop 2n: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen

Workshop 5: IT-Security Best Practice Top-10 Tips und Tricks in der Diskussion

Workshop 6: Neues über VoIP-Sicherheit

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

Donnerstag, 10.05.07

9:00 Uhr - 11:00 Uhr

SCADA- und Automatisierungssysteme: Neue Bedrohungen durch fortschreitende Vernetzung

- Bedrohungen durch Konvergenz von Prozessleittechnik und klassischer IT
- ISMS-Ansatz für SCADA- und Automatisierungssysteme
- Richtlinienbeispiele, kommende Standards (IEC-62443, ISA SP99,...)
- Schutzmaßnahmen bei der Kopplung mit Office- und externen Netzen

Stephan Beirer,
GAI NetConsult GmbH

10:00 Uhr - 11:00 Uhr

IT-Sicherheit in der Produktion: Der Status quo in deutschen Industrieunternehmen

- Schutzziele und Schadenspotenziale in der Produktion
- Die tatsächlichen Bedrohungen

- Der Sicherheitsstand heutiger Automatisierungssysteme
- Ausblick: Was muss getan werden, um den Zustand zu verbessern?

Ralph Langner,
Langner Communications AG

11:30 Uhr - 12:30 Uhr

Bluetooth - Ein Risiko für das Unternehmen?

- Bluetooth Usage scenario
- Risiko für das Unternehmen? Mythen und Fakten
- Live-Demo einer Attacke
- Pin cracking

Thierry Zoller,
n.runs AG

13:45 Uhr - 14:45 Uhr

Ermittlungsstrategien nach Systemenbrüchen (IT-Forensik)

- Grundregeln und Abläufe bei der Ermittlung
- Analyseansätze für die Ermittlung

- Sicherstellung und Umgang mit Beweismitteln
- Werkzeuge für die Beweismittelsicherung und Analyse

Sebastian Krause,
HiSolutions AG

14:45 Uhr - 15:45 Uhr

Notfallplanung unter dem Gesichtspunkt der Beschlagnahme

- Fälle von IT-Beschlagnahme in Unternehmen
- Rechtliches: Der Durchsuchungs- und Beschlagnahmebeschluss
- Integration in das Notfallkonzept (Merkblätter, technische Vorsorge, usw.)
- Folgen bei vorgenommener Beschlagnahme

Holm Diening,
GAI NetConsult GmbH

15:45 Uhr - 16:00 Uhr

Zusammenfassung und Schlusswort

Detlef Weidenhammer,
GAI NetConsult GmbH

IT-Sicherheits-Forum 2007

Agenda - Bitte treffen Sie hier Ihre Wahl!



Faxantwort an: 030/417898-300

Firma: _____

Name: _____

Tutorien: Bitte kreuzen Sie ein Tutorium-Thema an!

1

Tutorium 1: Prozessorientiertes IT-Sicherheitsmanagement mit ITIL - Interaktive Erarbeitung mit den Teilnehmern

2

Tutorium 2: Sicheres Netzwerk-Management - Live-Demos und Beispiele aus komplexen Umgebungen

3

Tutorium 3: Information Security Management von A(udit) bis Z(ertifizierung)

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

9:00 - 12:30 Uhr

1

Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?

- Freiheitsgrade in IEEE 802.1X: Wo unterscheiden sich die Hersteller?
- Was ändert sich bei Microsoft Vista, Longhorn hinsichtlich IEEE 802.1X?
- Herstellerkonzepte zur Prüfung der Desktop Integrity
- Migrationskonzepte für IEEE 802.1X
- Aufbau von Sicherheitszonen
- Umgang mit Geräten, die IEEE 802.1X nicht unterstützen
- Behandlung von Gastzugängen

Dr. Simon Hoff, ComConsult Beratung und Planung

2

Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen

- Einführung
 - Buzzword Bingo: Ajax, RIA, Mashups und Co.
- Angriffe im Web 2.0 Umfeld
 - Typische Sicherheitslücken in Ajax-Webanwendungen
- Cross-Site-Scripting 2.0
 - Verfall der Same Origin Policy
 - Javascript Malware
 - Umgehen von DNS-Pinning
 - Cross-Site-Request-Forging
 - Zugriff auf das Intranet aus dem Internet
- Prüfung und Sicherung moderner Anwendungen
 - Sind Ajax-Anwendungen über WAFs zu sichern?
 - Wie verhalten sich klassische Web-Scanner bei Ajax-Anwendungen?

Björn Fröbe, GAI NetConsult

3

Workshop 3: Interne Compliance Audits

- Einführung
 - Arten von Audits
 - Anwendungsgebiete von internen Audits
 - Erfüllung gesetzlicher Auflagen
 - Interne Audits im Rahmen der ISO 27001/17799
 - Erhebung von Security Metrics
- Grundlagen
 - Nachvollziehbarkeit, Vergleichbarkeit • RIDE und DRIVE Ansatz
- Vorgehensweisen
 - Erhebung durch Fragebögen
 - Gestaltung und Auswertung der Fragebögen
 - Anwendungsgebiete
 - Durchführung von Audits vor Ort
 - Objektivitätsgrundsatz, Rolle des Auditor
 - Erstellung eines Auditplans, Bestimmung von Stichproben
 - Verfolgung von Audit-Trails • Audit-Bericht
- Fazit

Holm Diening, GAI NetConsult

4

Workshop 4: Rechtliche Aspekte der Mobile Security

- Datenschutz bei Smartphones und PDAs
 - Schutz von Betriebsgeheimnissen
- Verschlüsselungspflicht
 - bei Speicherung auf mobilen Geräten?
 - bei E-Mail-Kommunikation auf mobilen Geräten?
- Virenschutz auf mobilen Geräten
- Schutz gegen Bluejacking und Hacking von mobilen Geräten
- Aufbewahrungspflichten mobil gespeicherter Inhalte
- Neue Impressumspflichten bei SMS und Mail?
- Gefahren von mobilen Bezahlsystemen
- Überwachungsmöglichkeiten
 - des Inhalts mobiler Geräte
 - des Ortes mobiler Geräte

Ulrich Emmert, esb Rechtsanwälte

14:00 - 17:30 Uhr

1n

Workshop 1n: Was leisten Herstellerlösungen zur Netzzugangskontrolle?

- Freiheitsgrade in IEEE 802.1X: Wo unterscheiden sich die Hersteller?
- Was ändert sich bei Microsoft Vista, Longhorn hinsichtlich IEEE 802.1X?
- Herstellerkonzepte zur Prüfung der Desktop Integrity
- Migrationskonzepte für IEEE 802.1X
- Aufbau von Sicherheitszonen
- Umgang mit Geräten, die IEEE 802.1X nicht unterstützen
- Behandlung von Gastzugängen

Dr. Simon Hoff, ComConsult Beratung und Planung

2n

Workshop 2n: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen

- Einführung
 - Buzzword Bingo: Ajax, RIA, Mashups und Co.
- Angriffe im Web 2.0 Umfeld
 - Typische Sicherheitslücken in Ajax-Webanwendungen
- Cross-Site-Scripting 2.0
 - Verfall der Same Origin Policy
 - Javascript Malware
 - Umgehen von DNS-Pinning
 - Cross-Site-Request-Forging
 - Zugriff auf das Intranet aus dem Internet
- Prüfung und Sicherung moderner Anwendungen
 - Sind Ajax-Anwendungen über WAFs zu sichern?
 - Wie verhalten sich klassische Web-Scanner bei Ajax-Anwendungen?

Björn Fröbe, GAI NetConsult

5

Workshop 5: IT-Security Best Practice Top-10 Tips und Tricks in der Diskussion

- Vorgesehene Themen sind:
 - Zentrale Lösungen zur Content-Security
 - Durchführung von Security Audits
 - Aufbau einer Notfallplanung
 - Aufbau einer ISMS-Lösung
 - Rechtsaspekte zur Archivierung von E-Mail
 - Rechtsaspekte zu VoIP

Holm Diening, GAI NetConsult
Detlef Weidenhammer, GAI NetConsult
Ulrich Emmert, esb Rechtsanwälte

6

Workshop 6: Neues über VoIP-Sicherheit

- VoIP-Verschlüsselung: Erfahrungen und neueste Entwicklungen
- Probleme und Tücken beim Einsatz von IEEE 802.1X im Zusammenhang mit IP-Telefonen
- Für und Wider von logischer Netztrennung für VoIP im LAN
- Welche Kombinationen von VoIP-Sicherheitsmechanismen sind sinnvoll? Für wen?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung

Änderungen im Programm behält sich der Veranstalter vor!