

Sicherheitsmanagement mit Schwerpunkt Identity Management

- ▶ Sicherheitspolicy und IT-Governance
- ▶ Modelle und Standards (COBIT, ITIL, BS7799 u. a.)
- ▶ Auswirkungen von Sarbanes Oxley
- ▶ Informations- und Kommunikationssicherheit
- ▶ Identity- und Accessmanagement
- ▶ Kryptographie
- ▶ Best Practices: Verbund, Raiffeisen Informatik (Zertifizierung)

Referenten: Alfred Bach (Novell), Walter Fraißler (Verbund), Georg Hahn (Raiffeisen Informatik), Jörg Kaulhausen (APC), Christian Monyk (ARC Seibersdorf), Johannes Mariel (BRZ), Dirk Schadt (Computer Associates), Michael Schirnbrand (KPMG), Christian Tomanek (UTA), Wolfgang Ziegler (itversity)

Moderation: Edmund Lindau (Computerwelt), Bettina Hainschink (Future Network)

Mittwoch, 10. November 2004, 8.30 – 17.00 Uhr
Bundesrechenzentrum, Hintere Zollamtsstraße 4, 1030 Wien

Zielgruppe: Unternehmensleitung, IT-Spezialisten, IT-Vorstand, IT-Entscheider, Sicherheitsverantwortliche, Finanzen, Vertreter von Medien, Vertreter der Wissenschaft

Mit freundlicher Unterstützung von:



Agenda

8.30 Registration

9.00 Auswirkungen von IT-Governance auf Information Security Management

Michael Schirnbrand (KPMG)

9.45 Informationssicherheit bei Raiffeisen Informatik – Zertifizierung und Situationsbericht

Georg Hahn (Raiffeisen Informatik)

10.15 Quantenkryptographie

Christian Monyk (ARC Seibersdorf)

10.45 Pause

11.15 Social Engineering

Johannes Mariel (BRZ)

11.45 Physische Infrastruktur für hochverfügbare Netzwerke (NCPI)

Jörg Kaulhausen (APC)

12.15 eTrust Identity & Access Management

Dirk Schadt (Computer Associates)

12.45 Mittagsbuffet

14.00 Compliance und Novell Identity Management

Alfred Bach (Novell)

14.30 IT-Security für KMUs

Christian Tomanek (UTA)

15.10 Informationssicherheit – Eine Herausforderung für Organisation und Awareness

Walter Fraißler (Verbund)

15.40 Was darf Security kosten?

Wolfgang Ziegler (itversity)

Schlussdiskussion

17.00 Ende der Veranstaltung

Informationssicherheit reduziert Risiken

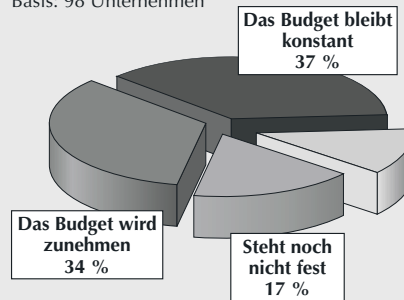
Unternehmen müssen heute durch ihr Verhalten, ihre Organisation, Prozesse und Infrastruktur sicherstellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gewährleistet sind.

Informationen sind Werte, die genauso wie die übrigen Geschäftswerte wertvoll für eine Organisation sind und infolgedessen in geeigneter Weise geschützt werden müssen. Informationssicherheit schützt Informationen vor einer Vielzahl von Bedrohungen. Sie soll die Aufrechterhaltung des Geschäftsbetriebs sicherstellen, geschäftsschädigende Einflüsse niedrig halten sowie die Investitionsrentabilität und die Geschäftsgelegenheiten maximieren.

Viele Produktions-, Logistik- und Geschäftsprozesse sind heutzutage ohne zuverlässig funktionierende IT-Systeme kaum noch vorstellbar. Störungen führen schnell zu Produktionsausfällen und verzögerter Bearbeitung. Dies bedingt verlässliche Sicherheitslösungen für IT-Systeme, Netze, Datenbanken und Anwendungen. Auch rechtliche Anforderungen und betriebswirtschaftliche Überlegungen zwingen heute alle Unternehmen und Institutionen, sich mit der Thematik der Informationssicherheit auseinander zu setzen.

Wie wird sich Ihr IT-Security-Budget im Jahr 2004 gegenüber 2003 entwickeln?

Basis: 98 Unternehmen



Quelle: META Group Österreich

Informationssicherheit wird im Wesentlichen verstanden als Sicherung der

- Vertraulichkeit: Sicherstellung des Zugangs zu Informationen nur für Zugangsberechtigte;
- Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden;
- Verfügbarkeit: Sicherstellung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer.

Informationssicherheit wird durch die Implementierung von geeigneten Maßnahmen erzielt, die Politik, Praktiken, Verfahren,

Organisationsstrukturen und Softwarefunktionen sein können. Diese Maßnahmen sind zur Erfüllung der spezifischen Sicherheitsziele der Organisation festzulegen.

Motivation Informationssicherheit

Gerade die so Erfolg versprechende offene Vernetzung als Geschäftsmodell erhöht die Risiken des unbefugten Zugriffs auf geschäftskritische Hardware, Anwendungen und Daten immens. Vor allem im E-Business ist Sicherheit deshalb ein Top-Thema. Denn Kunden und Unternehmen nehmen nur dann am elektronischen Geschäftsverkehr teil, wenn sie darauf vertrauen, dass die in Firmen- und öffentlichen Netzen übertragenen Daten vor Missbrauch geschützt sind. Die Verbindung von öffentlichen und privaten Netzwerken und die gemeinsame Nutzung von Informationsressourcen erhöhen die Schwierigkeit, eine effektive Zugangskontrolle sicherzustellen.

Organisationen und ihre Informationssysteme und -netzwerke sehen sich Sicherheitsbedrohungen unterschiedlichster Herkunft, einschließlich Computerbetrugs, Spionage, Sabotage, Vandalismus, Feuers oder Überschwemmung, gegenüber. Gefahrenquellen wie Computerviren, Hacker und „Denial of Service“-Attacken werden immer verbreiteter, anspruchsvoller und raffinierter.

Der Trend hin zur verteilten Verarbeitung hat die Effektivität einer zentralen, fachlichen Kontrolle geschwächt. „Zugang“ meint hier und im Folgenden sowohl den physischen wie auch den logischen Zugang.

Viele Informationssysteme sind nicht auf Sicherheit hin ausgelegt. Die technisch erzielbare Sicherheit ist begrenzt und sollte durch entsprechendes Management und entsprechende Verfahren unterstützt werden. Die Identifizierung der benötigten Maßnahmen erfordert sorgfältige Planung und Detailgenauigkeit. Beim Informationssicherheitsmanagement ist die Mitwirkung aller Beschäftigten in der Organisation eine Mindestvoraussetzung. Außerdem kann auch die Mitwirkung von Zulieferern, Kunden oder Anteilseignern erforderlich sein. Das Gleiche gilt auch für eine Fachberatung durch externe Organisationen. Maßnahmen für die Informationssicherheit sind wesentlich kostengünstiger und effektiver, wenn sie in den Stadien der Anforderungsspezifikation und der Entwicklung integriert werden.

Identity Management: Ist die Fähigkeit, Benutzerkonten (über heterogene Zielsysteme), Benutzerprofile oder ähnliche Identity Stores, mit denen Personen identifiziert werden können, zu verwalten. Identitätsmanagement inkludiert auch die Fähigkeit zu abstrahieren und automatisch Daten von HR/HCM

Systemen (und anderen Identity Stores) in Beziehung zu setzen. Zusätzlich umfasst es Funktionen wie Anlegen, Ändern oder Löschen von Benutzerkonten/-profiles für einzelne Benutzer, im Falle von Self-Service Interfaces (wie eine Selbstregistrierung) die individuelle Veränderung oder automatisierte Zugriffe auf diese Daten (z.B. einen Wechsel im HR/HCM System).

Access Management: Ist die Fähigkeit, Methoden zur Zugangskontrolle bereitzustellen, zu verwalten und die Zugangskontrolle auch durchzuführen. In Folge der Entwicklung von Intranets, Extranets und unternehmensweiten Internetzugängen wird die Sicherheit des Zugriffs auf Daten oder Informationen ein immer wichtigeres Anliegen. Zugang durch unterschiedliche Benutzer von mehreren Orten, unter Verwendung unterschiedlichster Devices wird die Norm werden und muß technisch realisiert werden.

Auswirkungen von IT-Governance auf Information Security Management

- ▶ Aktuelle Entwicklungen
- ▶ Überblick IT-Governance
- ▶ Internationale Standards und Modelle (Primär Cobit, etwas ITIL, hier auch BS 7799, div andere)
- ▶ Auswirkungen von Sarbanes Oxley (primär section 404)
- ▶ Nationale Anforderungen, besonders im Hinblick auf Risikomanagement und Compliance
- ▶ Integration von Cobit, ITIL, BS 7799 ua
- ▶ Implementierung von IT-Governance unter Berücksichtigung der neuen Anforderungen
- ▶ Ausblick

Besondere Schwerpunkte werden auf neueste Anforderungen im Bereich des Internen Kontrollsystems/des Risikomanagements, die

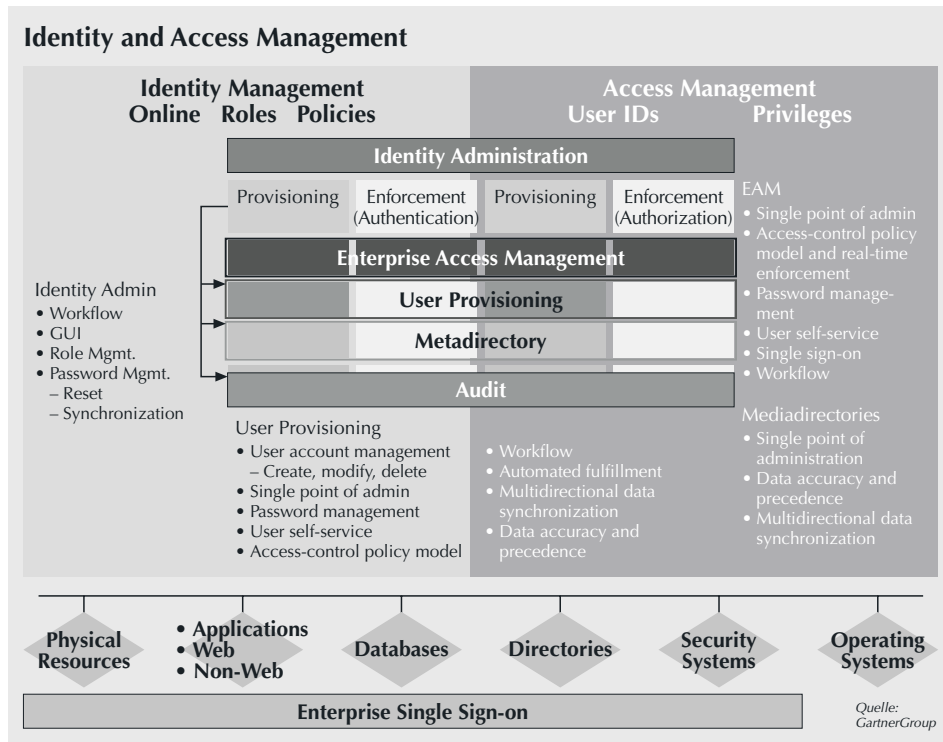
zu kennen, die wesentlichen Elemente der diesbezüglichen Standards und deren mögliche Interaktion darzustellen sowie über ausreichende Kenntnisse verfügen, um selbständig unter Verwendung der dargestellten Ressourcen diesbezügliche Lösungen zu erarbeiten.

Informationssicherheit bei Raiffeisen Informatik-Zertifizierung und Situationsbericht

Motivation des Raiffeisen Informatik Managements sich einer periodischen Auditierung zu unterziehen. Ein kurzer Erfahrungsbericht aus dem Zertifizierungsprozess und ein Auszug der wesentlichsten Erkenntnisse.

Quantenkryptographie

Quantenkryptographie (exakt: Quantum Key Distribution) ist ein Verfahren, das es ermöglicht, an zwei voneinander getrennten Orten eine identische Bitfolge zu erzeugen, die in der Folge zur Verschlüsselung von Nachrichten herangezogen werden kann. Aufgrund von quantenphysikalischen Naturgesetzen ist das unbemerkte Abhören des Schlüssels nicht möglich. Die prinzipielle Einsetzbarkeit von Quantenkryptographie wurde in der Vergangenheit von mehreren Forschergruppen an Universitäten bewiesen. ARC Seibersdorf research verfolgt gemeinsam mit dem Institut für Experimentalphysik der Universität Wien unter der Leitung von Prof. Anton Zeilinger das Ziel, die Ergebnisse der universitären Grundlagenforschung in ein marktfähiges System zur sicheren Kommunikation überzuführen. Neben der Verbesserung des quanten-optischen Aufbaus sind dabei auch umfangreiche Entwicklungsarbeiten in den Bereichen Kryptographie, Elektronik, Signalverarbeitung und Software-Entwicklung erforderlich. Eine weitere Anforderung ist die Integration der Verschlüsselungstechnologie in bestehende IT-Infrastruktur, eine Aufgabe, die gemeinsam mit Siemens Österreich durchgeführt wird. Quantenkryptographie ist eine Punkt-zu-Punkt-Verbindung, für ein funktionsfähiges Kommunikationssystem ist jedoch der Aufbau einer Netzwerkstruktur erforderlich. Im Rahmen eines von ARC Seibersdorf research geleiteten EU-Projektes wird seit April 2004 an der Entwicklung einer marktfähigen Komplettlösung für die globale sichere Kommunikation mit Hilfe von Quantenkryptographie gearbeitet.



Die heutigen Sicherheitsmodelle widerspiegeln sehr „weitmaschige“ Strukturen, während in Zukunft die Sicherheitsnetze engmaschiger werden müssen. Wir glauben, dass Verzeichnisdienste und -services die zentralen Komponenten dieser engmaschigen Sicherheitstechnologien sein werden. Verzeichnisdienste sind optimal für die Verwaltung, also Aufnahme und Speicherung von zugangsrelevanten Daten geeignet. Hierarchische Strukturen wie LDAP eignen sich hervorragend um Beziehungen, seinen es internen oder externe, entsprechend dem „real world“ Modell abzubilden. Unternehmensweite Verzeichnisdienste werden der Standard für Autorisierung, Authentifizierung und Provisioning werden.

aus den USA auch zu uns gelangen – namentlich jene des Sarbanes Oxley Acts – und deren Auswirkungen auf die IT dargestellt.

Standard-Prozessmodelle zur Steuerung der IT werden dargestellt, besonders wird auf Cobit als anerkanntestes Modell zur Umsetzung von IT-Governance, dessen Bestandteile sowie diesbezügliche neue Entwicklungen eingegangen.

Die Schnittstellen zwischen derartigen Standards und deren sinnvolle und praxisorientierte Integration unter besonderer Berücksichtigung der Informationssicherheit werden erläutert.

Nach Besuch dieses Vortrages sollten sämtliche Teilnehmer in der Lage sein, aktuelle Entwicklungen auf dem Gebiet der IT-Governance

Social Engineering

Ist die Methodik, berechnete User eines EDV-Systems durch Täuschung über die Identität des Angreifers oder andere Tatsachen dazu zu

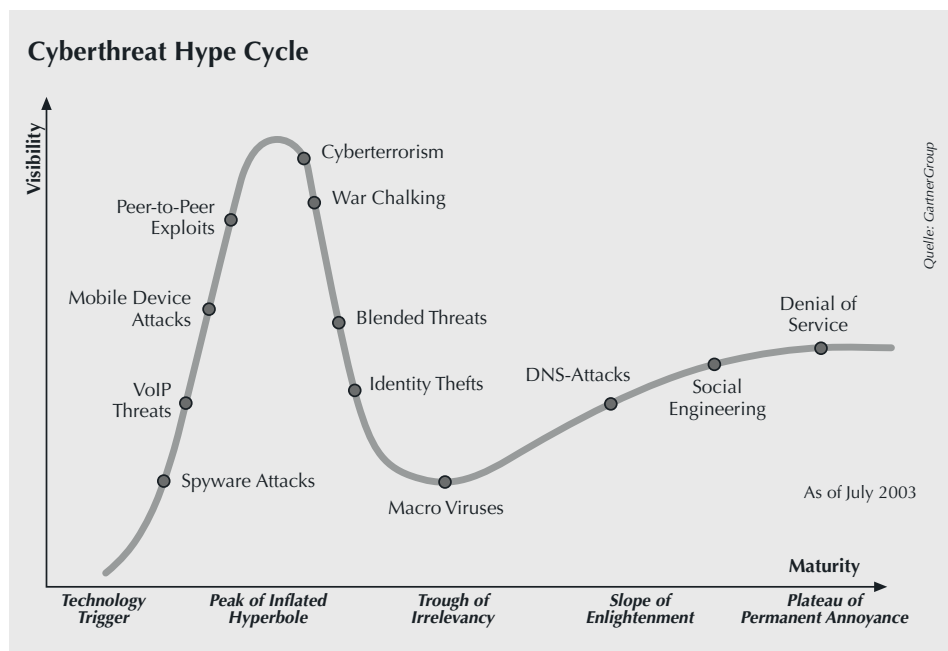
verleiten, dass sie zweckdienliche Angaben für einen Einbruch in das EDV-System bekannt werden lassen oder direkt Daten daraus unberechtigt weitergeben.

Gegenmaßnahmen sind Security-Policies, die realistisch, konsistent sind, keine unerfüllbaren Forderungen enthalten, einfach zugänglich (Intranet) sind, laufend aktuell gehalten werden, durch Awareness-Maßnahmen unterstützt.

die Basisdaten von Benutzern bis hin zu Produktinformationen in einer Vielzahl von Verzeichnissen obendrein oftmals redundant abgelegt sind.

Novell Identity Manager 2 ist eine außergewöhnliche Lösung, um verschiedenste Datenquellen und Verzeichnisdienste miteinander zu synchronisieren. Damit revolutioniert Novell die Möglichkeiten im E-Business, indem klassische Barrieren verschiedenster

unterstützende Infrastruktur für die Netzwerk-kritische IT auf dem Stand der 80er und 90er Jahre verharret, sorgen heutige Serversysteme, Switches oder IP-Telefonie für nie geahnte, höchste Strom- und Wärmelasten. Stromzuführung, IT-Management, Ventilation, Klimatechnik und Racktechnologie müssen mit dieser Entwicklung Schritt halten, besser noch, müssen sie vorausschauend begleiten. Erfahren Sie die neuesten Trends in Netzwerk-kritischer physikalischer Infrastruktur (NCPI)..



Security-Investitionen
 Von einem EURO Security-Invest sollten:
 15 Cent in Technik
 20 Cent in Security-Betrieb
 25 Cent in Sicherheits-Organisation
 40 Cent in Sensibilisierungsmaßnahmen
 investiert werden, um die Bedrohung durch SOCIAL ENGINEERING zu verhindern.

eTrust Identity & Access Management – Alter Wein in neuen Schläuchen?

Moderne Benutzerverwaltungen ermöglichen es, heterogene Geschäftsprozesse effizient und effektiv zu unterstützen, sowie Anforderungen aus Regularien besser zu erfüllen ohne den Überblick zu verlieren. Konsequente Integration von Kernprozessen durch standardisierte Methoden und Werkzeuge geben Unternehmen heute die Chance, dynamisch auf ihre Märkte zu reagieren und dabei neben durchgängiger Nachvollziehbarkeit auch noch Kosten zu reduzieren

Compliance und Novell Identity Management

Eines der größten Hemmnisse bei der Verknüpfung verschiedener EDV-Systeme zu E-Business Infrastrukturen, ist die Tatsache, dass

Datenformate und Verwaltungsstrukturen überwunden werden.

Neben den traditionellen IT-Risiken sind in jüngster Zeit ganz neue Risikoszenarien für die Wirtschaft entstanden, ausgelöst durch die zunehmende Integration von Unternehmensprozessen sowie die Anbindung externer Partner und Kunden an bislang geschlossene interne IT-Systeme.

Compliance, also das nachweisbare Einhalten der einschlägigen nationalen und internationalen Bestimmungen, wird zu einem der wichtigsten Treiber für Identity Management mit den zentralen Bereichen der Authentifizierung, Autorisierung und Überwachung.

Diese Anforderungen lassen sich aber angesichts einer immer komplexeren Anwendungs- und Systemlandschaft nur dann sicher und flexibel realisieren, wenn alle Komponenten auf gemeinsame Identitäten zugreifen können. Die Integration von Identitäten ist also Voraussetzung, wenn die IT den Business-Anforderungen des Unternehmens gerecht werden soll.

Physische Infrastruktur für hochverfügbare Netzwerke (NCPI)

Die heiße Phase in Ihrem Datacenter hat begonnen. Während die herkömmliche

IT-Security für KMUs

Sicherheit muß nicht teuer sein – professionelle und kostengünstige Sicherheitslösungen für KMUs.

Informationssicherheit – Eine Herausforderung für Organisation und Awareness – Ein Erfahrungsbericht des Verbund

Häufig wird Informationssicherheit auf IT-Sicherheit reduziert und damit der technologische Aspekt in den Vordergrund gerückt. Zahlreiche Untersuchungen zeigen einerseits die Bedeutung, andererseits aber auch die häufige Vernachlässigung der organisatorischen und personellen Aspekte. Der Erfahrungsbericht des Verbund zeigt, wie alle diese Bereiche in einem ausgewogenen Verhältnis abgedeckt werden können.

Was darf Security kosten?

Ausgehend von den derzeit verwendeten Verfahren zur Risikoanalyse wie ISO/IEC TR 13335 oder dem IT-Grundschutzhandbuch des deutschen BSI werden die Probleme und Schwachstellen von diesen Methoden analysiert. Dabei wird von der Bedrohungsanalyse systematisch der Weg von der Bedrohung zum Risiko dargestellt. Der betriebswirtschaftliche Aspekt zur Rechtfertigung von Kosten für IT-Sicherheitsmaßnahmen steht im Vordergrund. Beginnend mit der Frage: „Wieviel Sicherheit ist genug?“ wird untersucht, ob man mit den konventionellen Verfahren einen optimalen Maßnahmenmix gewinnen kann. Anschließend wird in einer kleinen Demonstration ein alternatives Konzept zur Risikobewertung vorgestellt. Mittels einer Beispielfirma wird ein Risikosimulationsmodell erzeugt und eine Antwort auf die Frage: „Wieviel Sicherheit ist genug?“ gegeben.



Wie viel Sicherheit ist genug

Kursnummer: SC210 Risikoanalyse und Sicherheitsmanagement

Zu wenig IT Security birgt zu viele Gefahren. Zu viel IT Security ist kaufmännisch unklug. Was aber ist nun das richtige Maß? In diesem Seminar wird die Antwort auf diese Frage gegeben.

Termin: 29. 11. 2004 – 30. 11. 2004

Ort: it-versity Wien

Voraussetzungen

Erfahrung mit der Erstellung von Information Security Policies

Zielgruppe

Personen, die mit der Erstellung von Unternehmensrichtlinien zu Information Security betraut sind.

Themen

- ▶ Die ISM Policy-Ansätze der ersten Generation
- ▶ Risk Assessment-Risk Management
- ▶ Common Frameworks
- ▶ Ansätze der zweiten Generation
- ▶ Integrated Business Risk-Management Models
- ▶ Valuation-Driven Methodologies
- ▶ Szenario Analysis Approaches
- ▶ Best Practicies
- ▶ Risk Modeling and Analysis
- ▶ Decision Modeling
- ▶ Computer Security Risk Model Analysis
- ▶ Datensuche
- ▶ Beispiele

Dauer: 2 Tage

Kosten: Pro TeilnehmerIn € 980,00 exkl. MwSt. Inkl. Unterlagen, Pausen- u. Mittagsbewirtung.

Vortragender: Wolfgang Ziegler
(Senior Security Consultant it-versity)

IT-Security und das Gesetz

Kursnummer SC310 – Rechtliche Grundlagen der IT-Sicherheit

IT-Sicherheit ist für jedes Unternehmen ein zentrales Thema. Neben dem technischen Fachwissen haben IT-Verantwortliche eine Vielzahl von Gesetzen zu beachten. Wer diese Regeln nicht kennt, ist nicht in der Lage eine sichere IT-Landschaft aufzubauen; darüber hinaus gilt es eine Vielzahl von Haftungsregeln zu beachten. Dieses Seminar gibt anhand von praktischen Beispielen einen Überblick über den rechtlichen Rahmen der IT-Sicherheit.

Termin: 03. 12. 2004

Ort: it-versity Wien

Seminarziele

Nach Besuch des Seminars können Sie u. a. folgende Fragen beantworten:

- ▶ Muss jedes Unternehmen eine Sicherheitspolicy haben?
- ▶ Welche Gegenmaßnahmen sind im Fall eines Angriffs zu setzen?
- ▶ Dürfen Arbeitnehmer bei der Nutzung von Internet und E-Mail überwacht werden?
- ▶ Welche Rolle spielt der Betriebsrat?
- ▶ Wer haftet im Schadensfall?
- ▶ Ist Portscanning, Hacking, Phishing, War-driving erlaubt?
- ▶ Wie funktioniert Datenschutz in meinem Unternehmen, was habe ich zu beachten?
- ▶ Welche Datenanwendungen habe ich zu verfassen und welche Meldepflichten gibt es?

Inhalte

- ▶ Gesetzliche Grundlagen von IT-Security
- ▶ Haftungsfragen für IT-Security Management & GeschäftsführerInnen, Systemadministratoren
- ▶ Welche Security Policies gibt es; welche sind gesetzlich verpflichtend und Strafrechtliche Aspekte
- ▶ Rechte der Betroffenen
- ▶ Standard- & Musteranwendungen

Dauer: 1 Tag

Kosten: Für das eintägige Training pro TeilnehmerIn Euro 490,00 exkl. MwSt. inkl. Unterlagen, Pausen- und Mittagsbewirtung

Vortragender: Mag. Dr. Dominik Wallner
Jurist, Datenschutz- und Sicherheitsbeauftragter CCC AG

PKIs und das Drumherum

Kursnummer: SC450 Organisation und Verfahren bei der Verwendung von PKI

mit Zertifizierungsmöglichkeit
Alle organisatorischen und technischen Aspekte, welche zur Einführung einer Public Key Infrastructure benötigt werden und nicht von einem Betriebssystem abhängig sind.

Termin: 22. 11. 2004 – 26. 11. 2004

Ort: it-versity Wien

Zielgruppe

Alle Personen, welche planen, eine PKI einzuführen oder eine solche bereits betreiben

Inhalte

- ▶ Organisatorische Aspekte
- ▶ Grundlagen der Kryptografie
- ▶ Symetrische Verschlüsselungsverfahren
- ▶ Asymetrische Verschlüsselungsverfahren
- ▶ Arten von digitalen Zertifikaten
- ▶ Anwendungsgebiete
- ▶ VPNs
- ▶ Betriebssystemauthentifizierung
- ▶ E-Mail Signaturen
- ▶ Grundlagen der PKI
- ▶ Vertrauensstruktur in der PKI
- ▶ Varianten, Standards
- ▶ Komponenten
- ▶ Zertifikate Management
- ▶ Praktische Aspekte
- ▶ Rechtliche Aspekte
- ▶ Signaturgesetz

Dauer: 5 Tage

Kosten: Pro TeilnehmerIn Euro 2.250,00 exkl. USt, inkl. Unterlagen, Pausen- und Mittagsbewirtung

Vortragender: Wolfgang Ziegler
(Senior Security Consultant it-versity)

An
Future Network
Kaiserstraße 14/2
1070 Wien
Tel.: (01) 522 36 36-37
Fax: (01) 522 36 36-10
E-Mail: registration@future-network.at
<http://www.future-network.at>

ANMELDUNG

Ja, ich möchte am Management-Forum „Sicherheitsmanagement“ am 10. November 2004 bei freiem Eintritt teilnehmen.

Ich bestelle die Unterlagen zu einem Unkostenbeitrag von € 50,- + 20% MWSt

Firma:
Name:
Funktion:
Straße:
PLZ/Ort:
Tel./Fax:
E-Mail:

Oder legen Sie einfach Ihre Visitenkarte bei!
Anmeldeschluss: 8. November 2004

Beschränkte Teilnehmerzahl. Anmeldebestätigung erforderlich.
Das Future Network behält sich vor, Besucher ohne Teilnahmebestätigung abzuweisen.

Senden Sie mir bitte Informationen über das Future Network:

Ich ersuche um Zusendung von Detailprogrammen zu folgenden Workshops an meine E-Mail-Adresse:

- Wie viel Sicherheit ist genug** am 29.–31. 11. 2004
- IT-Security und das Gesetz** am 3. 12. 2004
- PKIs und das Drumherum** am 22. 11. 2004