

Effiziente Konzepte für umfassende IT-Sicherheit

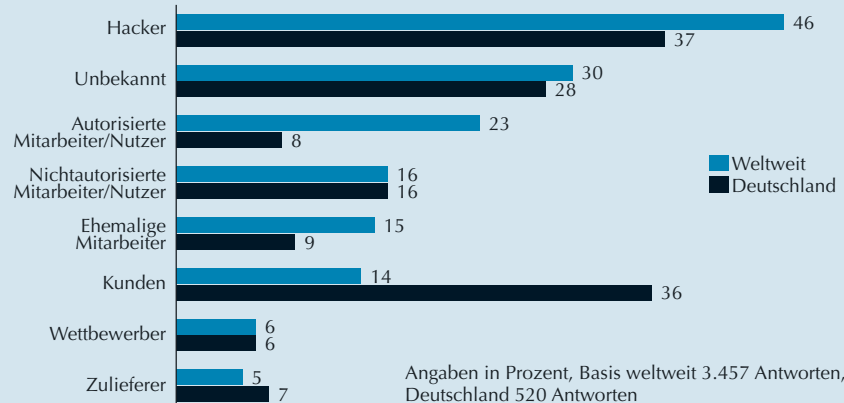
Dienstag
14. Mai 2002
9.00 – 18.00 Uhr
Wien

- ▶ Sicherheitspolicy
- ▶ Rechtliche Aspekte
- ▶ Grundlagen der Kryptographie
- ▶ Netz-Angriffe
- ▶ Netzwerkstrukturen/Netzangriffe
- ▶ Mit Live-Demo
Lösungen für Windows & Linux-Plattformen

Workshop

Sicherheitsverletzungen – Wer war's?

Wen vermuten Sie als Urheber von Sicherheitsverletzungen?



Quelle: PricewaterhouseCoopers/Information Week, Aug. 2001

Referenten:

Thomas Mandl (IT Consulting)

Josef Pichlmayr (Ikarus Software)

Christian Reiser (Internet Security AG)

Zielgruppe

- ▶ IT-Entscheidungs-träger
- ▶ Netzwerk- und Sicherheits-Verantwortliche
- ▶ Datenschutz-Beauftragte

Unsere Partner:

AUSTRIAN RESEARCH CENTERS

DER STANDARD

CON
CONSULTING
EVENTS
COMMUNICATIONS
TRAINING

Effiziente Konzepte für umfassende IT-Sicherheit

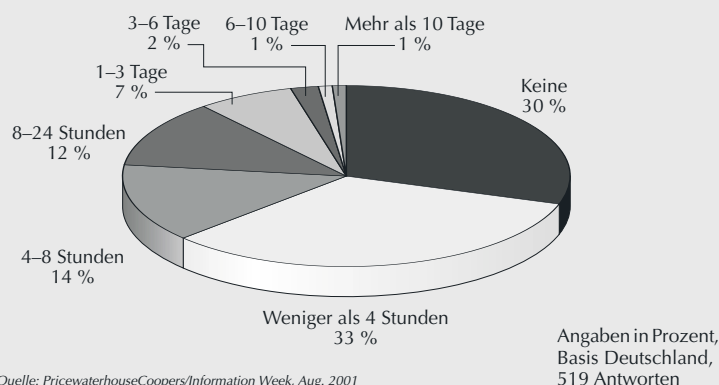
Ziel dieser Veranstaltung ist es, ausgehend von einer ganzheitlichen Sicherheitspolicy für ein Unternehmen, die entsprechenden möglichen Angriffsszenarien und Lösungsstrategien dafür vorzustellen sowie den Teilnehmern ein Problembewusstsein mitzugeben, wie wichtig ein umfassendes Sicherheitskonzept für die IT und ein verantwortungsvoller Umgang mit den Firmendaten für das gesamte Unternehmen ist. Im Rahmen des Workshop werden sowohl rechtliche Aspekte, Fragen der Standardisierung als auch technologische Konzepte in Verbindung mit Tipps aus der Praxis vorgestellt.

Die rasch fortschreitende Vernetzung der Wirtschaft und die damit verbundene Steigerung des Datenverkehrs zwischen Unternehmen rücken das Thema IT-Sicherheit schlagartig in den Mittelpunkt strategischen Denkens und Handelns. Das Grundproblem der IT-Security

besteht darin, die richtige Balance zwischen ungehinderten Funktionalitäten auf der einen Seite und Sicherheit auf der anderen Seite zu finden. Schon die Bezeichnung „offene Systeme“ wirkt in diesem Zusammenhang verräterisch. Die Sicherheitslücken sind zahlreich und reichen etwa von Passwörter auf der Unterseite der Tastaturen („Das Kleingeld jedes Hackers“) über „out of the box“-Installationen von Firewalls bis hin zu nicht durchgeführten Security-Checks und dem Fehlen von Verschlüsselungen. Selbst die beste Technik allein ist nicht genug für Security-Projekte,

Ausfallszeiten – Nichts geht mehr

Wie hoch war Ihre durch Sicherheitsverletzungen verursachte Ausfallszeit im vergangenen Jahr?



besteht darin, die richtige Balance zwischen ungehinderten Funktionalitäten auf der einen Seite und Sicherheit auf der anderen Seite zu finden. Schon die Bezeichnung „offene Systeme“ wirkt in diesem Zusammenhang verräterisch.

Einer Studie der US-Computersicherheitsfirma Riptech zufolge ha-

ben Cyber-Attacken pro Unternehmen im Zeitraum von Juni bis Dezember 2001 um 79 Prozent zugenommen. Aus einer anderen Untersuchung geht hervor, dass Virenschäden allein in Österreich jährlich einen Gesamtschaden von 51 Mio. Euro verursachen.

wenn das organisatorische Umfeld nicht passt.

Diese Mängelliste zeigt, dass IT-Security zwingend als Querschnittsmaterie zu betrachten ist, um bei neuen Bedrohungsszenarien die Sicherheit von Daten, Anwendungen und der Infrastruktur zu gewährleisten.

Einführung zum Thema Security

Vorgehensweise von Hackern, mögliche Angriffsarten auch anhand von Beispielen, und welche Tools zur Verfügung stehen.

Sicherheits-Policy

Die Sicherheitspolicy muss Bestandteil der gelebten Unternehmenskultur sein. Was sie beinhaltet und worauf zu achten ist, wird in diesem Referat gezeigt.

Stichworte zum Inhalt:

- ▶ Unternehmenssicherheit
- ▶ Management der Sicherheitsinfrastruktur
- ▶ Sicherheit der Daten

Rechtliche Aspekte

Erläutert werden die in Österreich geltenden Gesetze zum Thema Security anhand vom Telekommunikationsgesetz, Datenschutzgesetz, Signaturgesetz, Urheberrecht, Medienrecht sowie die rechtlichen Anforderungen an die IT-Sicherheit.

Grundlagen Kryptographie

Diese sind so alt wie die menschliche Sprache. Die Funktionsweise und wie sie in Virtual Private Networks (VPN) oder E-Mail Verschlüsselung verwendet wird, wird in diesem Vortrag erklärt.

Viren

- ▶ Welche Virenproblematiken kommen in Zukunft auf Sie und Ihre Kunden zu?
- ▶ Welche Gegenmaßnahmen sind notwendig und möglich?
- ▶ Sind Sie immer „Up-to-date“ und was können Sie konkret für Ihre Kunden tun?

- ▶ Welche Trends zeichnen sich bezüglich AV-Schutz (Anti-Viren-Schutz) ab?
- ▶ Was bedeutet Security Policy in Bezug auf AV-Schutz?

Netzwerkstrukturen, VPN, Firewalls

Hier wird auf Security-Fragen eingegangen, die z. B. bei der Einbindung von Teleworkern in das firmeninterne Netz auftreten können.
Firewalls: Typen – Möglichkeiten und Grenzen – Grundkenntnisse der Konfiguration einer Firewall

Ing. Thomas Mandl

Seit 1996 Senior System- und Netzwerkadministrator eines High-Tech-Microchip-Konzerns in Wien. Tätigkeitsschwerpunkte: Administrierung der heterogenen Netzwerkkumgebung mit Spezialisierung auf UNIX/Linux, Hochleistungs-Serversysteme und System-/Netzwerksicherheit.

Seit 2000 auch selbständiger Konsulent im IT und Securitybereich. Analyse von Hackerangriffen, Hackertools, Penetration Tests, Angriffsmethoden von Hackern, Forensische Analyse, Firewalls, OS Hardening, Installation von Linux/UNIX Servern, Vorträge und Beratung im IT Securitybereich sind einige Themen seiner Tätigkeit als selbständiger Konsulent.



Josef Pichlmayr

Geschäftsführer und Inhaber des 1986 gegründeten österreichischen Virenschutzunternehmens Ikarus Software GesmbH und beschäftigt sich seit 1992 mit Computerviren. Verfügt über fundierte Kenntnisse der Viren- und Virenschreiberszene. Mitglied der ICSA (International Computer Security Agency) seit 1995, seit 1999 Reporter der internationalen Wild-List-Organisation, Mitglied zahlreicher nationaler und internationaler Fachverbände. Laufende Vortragstätigkeit und Publikationen im Bereich Virenschutzmaßnahmen und Computerviren.



Dipl.-Ing. Christian Reiser

Ist Sicherheits-Experte und Vorstand (CTO) der Internet Security, einem Distributor und Dienstleistungsunternehmen im Bereich Internet-Sicherheit. Zu seinen Spezialgebieten zählen Firewalls, Verschlüsselungen, elektronischer Zahlungsverkehr, Rechtsfragen des Internets und Beratung in organisatorischen Sicherheitsbelangen.



AGENDA

8.30 Begrüßung und Registration

8.45 Einführung zum Thema Security
Christian Reiser (Internet Security AG)

9.30 Sicherheits-Policy
Christian Reiser (Internet Security AG)

10.00 Kaffeepause

10.15 Rechtliche Aspekte
Christian Reiser (Internet Security AG)

11.00 Grundlagen Kryptographie
Christian Reiser (Internet Security AG)

12.00 Mittagspause

13.00 Viren
Josef Pichlmayr (Ikarus Software)

13.45 Netzwerkstrukturen, VPN, Firewalls
Christian Reiser (Internet Security AG)

14.15 Kaffeepause

14.30 Live-Demonstration mit einer Analyse möglicher Angriffszenarien und wie man sich davor schützen kann für Plattformen wie Windows & Linux
Thomas Mandl (Mandl IT Consulting)

18.00 Ende der Veranstaltung

TERMIN & ORT

Dienstag, 14. Mai 2002, 9.00–18.00 Uhr
Future Network, Kaiserstraße 14/2 1070 Wien

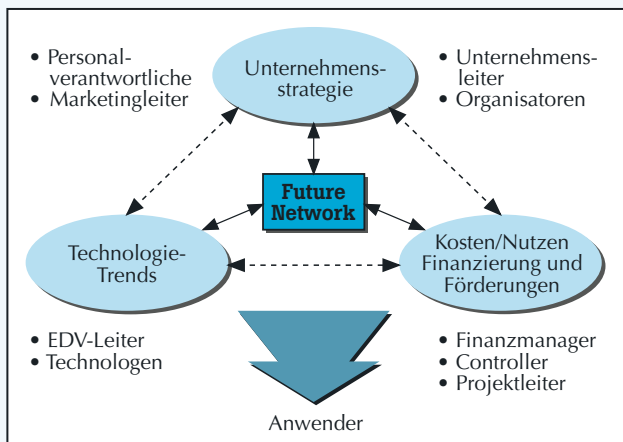
GEBÜHREN

Für Mitglieder des Future Network:
€ 650,00 zuzüglich 20 % MWSt.

Für Nichtmitglieder:
€ 750,00 zuzüglich 20 % MWSt.

ZIELGRUPPE

- ▶ T-Entscheidungsträger
- ▶ Netzwerk- und Sicherheits-Verantwortliche
- ▶ Datenschutz-Beauftragte



Vorstandsmitglieder des Future Network:

- Dr. Rupert Nagler** (Information Design Institute)
- Dipl.-Ing. Wolfgang Apfelbaum** (Apfelbaum Business Consulting)
- Dipl.-Ing. Dr. Franz Barachini** (Donauuniversität Krems)
- Dipl.-Ing. Erwin Gillich** (MA 14/ADV)
- Vstd.-Dir. Ing. Bernhard Graf** (Basler Versicherung)
- Ing. Johann Ehm** (OMV)
- Ing. Mag. Heinz Janecska** (IT Powergroup)
- Rudolf Mrstik** (AUA)
- Prof. Helmut Schauer** (Universität Zürich)
- Michael Vesely** (Consultant)
- Johannes Werner** (Kapsch)
- Sonja Haberl** – Finanzreferentin
- Mag. Bettina Hainschink** – Generalsekretärin

Unsere Partner:



Institut für Informatik der Universität Zürich

AUSTRIAN RESEARCH CENTERS
DER STANDARD

Web powered by:



Weitere Future Network Events finden Sie unter <http://www.future-network.at>

TEILNAHMEGEBÜHR: In der Teilnahmegebühr eingeschlossen sind die Arbeitsunterlagen zur Veranstaltung (die Zusammenfassung der Vorträge und Anschauungsmaterial der Referenten), Mittagessen (bei ganztägigen Veranstaltungen) und Pausenerfrischungen. Die Arbeitsunterlagen können Sie unabhängig von einer Veranstaltungsteilnahme auch käuflich bei uns erwerben. Wenden Sie sich diesbezüglich bitte an unser Büro.

ÜBERWEISUNG: Nach Erhalt Ihrer Anmeldung senden wir Ihnen Anmeldebestätigung und Rechnung zu. Bitte überweisen Sie Ihre Teilnahmegebühr rechtzeitig

vor der Veranstaltung oder legen Sie einen Verrechnungsscheck bei. Notieren Sie bitte Rechnungsnummer und Namen des Teilnehmers auf dem Überweisungsfeld. Bei Überweisung der Teilnahmegebühr später als 8 Tage vor der Veranstaltung bitten wir Sie, eine Kopie des Überweisungsauftrags am Veranstaltungstag vorzulegen.

SONDERKONDITIONEN: Bei Teilnahme mehrerer Mitarbeiter Ihres Unternehmens an einer Veranstaltung gewähren wir ab der zweiten Person einen Preisnachlass von 20% auf die Teilnahmegebühr. Ermäßigungen für Studenten auf Anfrage.

STORNIERUNG: Bei Stornierung der Anmeldung bis zum Anmeldeschluss fällt eine Stornogebühr in der Höhe von 10% der Teilnahmegebühr an. Bei Abmeldung nach diesem Termin wird die gesamte Gebühr fällig. Wenn Sie einen Ersatzteilnehmer melden, entfällt natürlich die Stornogebühr.

ADRESSÄNDERUNGEN: Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

- ▶ Ich melde mich zum Workshop „Effiziente Konzepte für umfassende IT-Sicherheit“ am 14.5.2002 an
- Als Mitglied des Future Network zum Preis von € 650,- (öS 8.944,20) exkl. MWSt.
- als Nichtmitglied zum Preis von € 750,- (öS 10.320,23) exkl. MWSt..

▶ **Anmeldeschluss: 10.5.2002**

Angebot für Nicht-Mitglieder:

- ▶ Bei Abschluss einer neuen Firmenmitgliedschaft (z. B. für eine Anwenderfirma mit bis zu 50 Mitarbeitern um € 726,73) ist der kostenfreie Veranstaltungsbesuch von zwei Events dieses Schwerpunkts inbegriffen!
- ▶ Bitte fordern Sie den Aufnahmeantrag in unserem Büro an!

▶ Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.
▶ Ich bin mit der Zusendung von Veranstaltungsinformationen per E-Mail einverstanden.
(Nichtzutreffendes bitte streichen)

An
Future Network
Kaiserstraße 14/2
1070 Wien

Tel.: +43/1/522 36 36-37
Fax: +43/1/522 36 36-10
E-Mail: office@future-network.at
<http://www.future-network.at>

Firma:	
Titel:	Vorname:
Nachname:	
Funktion:	
Straße, Hausnummer:	
PLZ:	Ort:
Telefon:	Telefax:
E-Mail:	
Ort, Datum:	Unterschrift, Firmenstempel: