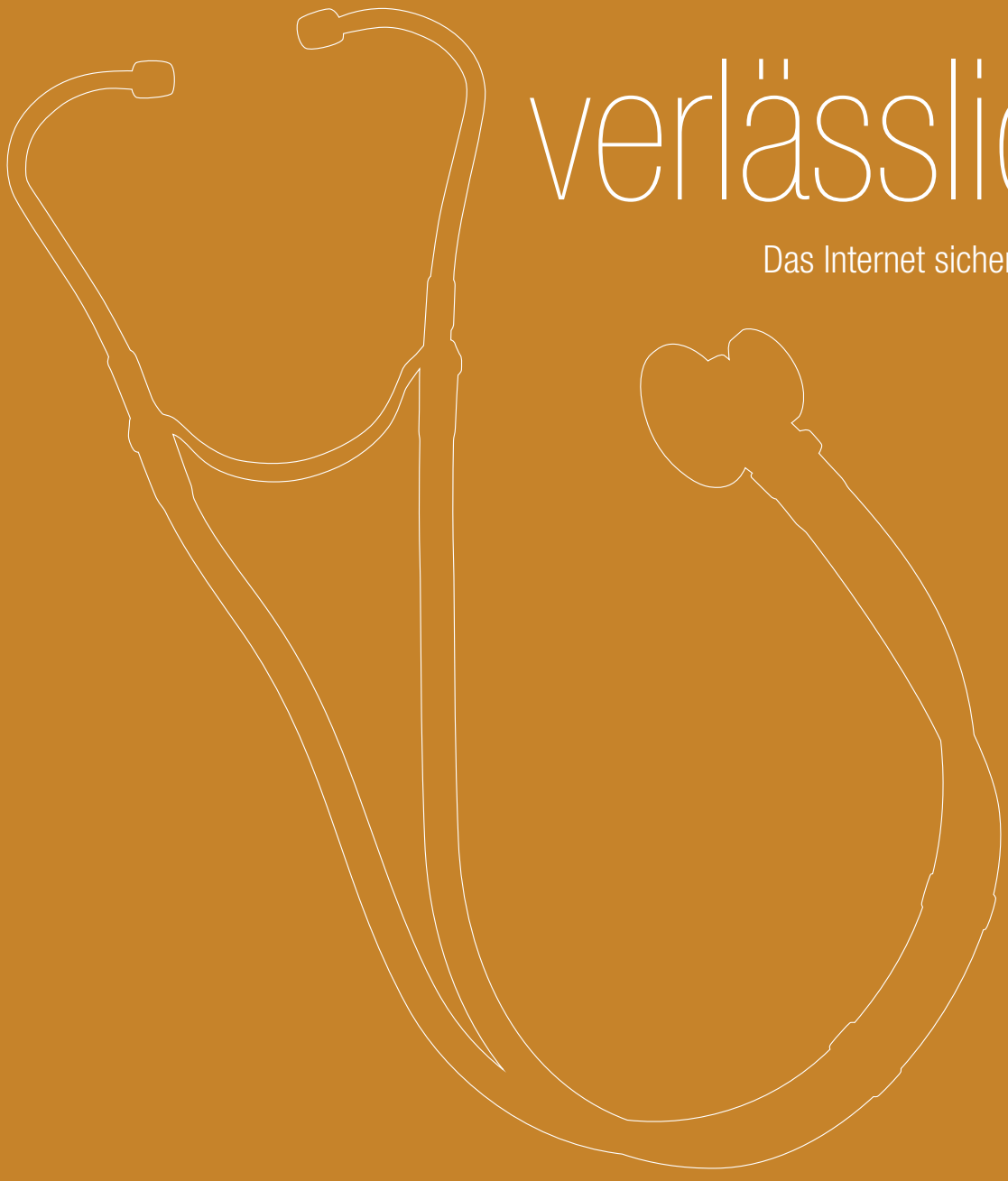
2|11

ispa
Internet Service Providers Austria

News



verlässlich

Das Internet sicher machen

verlässlich

Das Internet sicher machen

Impressum: ISPA – Internet Service Providers Austria, 1090 Wien, Währingerstraße 3/18 | Redaktion: Edith Michaeler | Druck: Gutenberg Druck GmbH, 2700 Wr. Neustadt | Grafik: www.allesgrafik.at
Blattlinie: Informationsmedium des Vereins Internet Service Providers Austria (ISPA) und dient zur Unterstützung des Ziels der Vereinstätigkeit: Förderung des Internets in Österreich. Namentlich gekennzeichnete Beiträge stellen selbstverständlich nicht automatisch die Position der ISPA dar. Die ISPA haftet nicht für Schäden, die aus inkorrekten oder verspäteten Inhalten oder aus Handlungen resultieren, die im Vertrauen auf die Richtigkeit des Inhaltes getätigt wurden. Die in dieser Publikation enthaltenen Informationen stellen keine Rechts- oder Anlageberatung sondern lediglich eine Information dar.

Editorial

Von Andreas Wildberger

Wer beschützt das Internet? Wer macht es verlässlich sicher? Diese Fragen drücken Sorgen von Gesellschaft, Politik aber auch Wirtschaft um jene Infrastruktur aus, die über die letzten zwei Jahrzehnte unser Kommunikationsverhalten stark geprägt hat, politische Geschicke beeinflusst hat und ohne die viele Geschäftsprozesse nicht mehr laufen würden: das Internet.

Zur Sicherheit beitragen!
Internetarchitektur ist über die Jahre wesentlich komplexer geworden als sie zu ihren Anfängen war. Die Verwobenheit des Internets mit unserem täglichen Leben wurde dadurch intensiver. Wie können wir also sicher sein, dass das Internet da ist, wenn wir es brauchen?
Wir können das Internet zwar nicht 100 Prozent absichern – aber jeder kann ein Scherflein dazu beitragen – beispielsweise durch laufende Updates von Systemsoftware und Antivirenprogrammen.
Und: Wie stellen wir sicher, dass all jene, die das Internet verwenden, dies auch sicher tun können? Auch hier werden wir keine 100-prozentige Sicherheit erreichen. Denn alle Medienerziehung für InternetnutzerInnen jeden Alters der Welt wird jenes Grundproblem der Gefahr für den Menschen niemals in den Griff bekommen: den Menschen selbst.

Wer beschützt das Internet?
Der Schutz des Internets geht uns alle an. Der Frage „Wer beschützt das Internet?“ sind wir in unserem ISPA Forum am 18. Mai nachgegangen: Mehr Informationen zu unserer Veranstaltung finden Sie ab Seite 4.

internet sicher nutzen!
Unter dem Motto „internet sicher nutzen“ steht auch die neu aufgelegte ISPA-Broschüre, die dazu anhält, die Nutzung des Internets zu einer positiven und sicheren Erfahrung zu machen: Die Neuauflage erhalten Sie druckfrisch mit dieser Ausgabe der ISPA News serviert. Genaueres über die Neuerungen der 3. Auflage finden Sie auf Seite 18.

Abgesicherte Entscheidungen?
Dass politische Beschlüsse nur eine Scheinsicherheit erzeugen, haben wir anhand des Beschlusses des österreichischen Parlaments zur Umsetzung der Vorratsdatenspeicherung erlebt. Diese wird ab April 2012 auf für alle BürgerInnen „aufgedreht“. Freilich: Auf EU-Ebene setzen sich die obersten DatenschützerInnen schon intensiv für die Abänderung dieser umstrittenen Richtlinie ein. Wir informieren Sie über die Neuerungen ab Seite 12.

Sichere Information!
Auch einer der letzten beiden Workshops der ISPA Academy stand unter dem Motto Sicherheit: Bei der Academy zu Telefonie Fraud wurden ISPA Mitglieder intensiv über die verschiedenen Arten von Telefonie Fraud und mögliche Gegenstrategien informiert. Eine Zusammenfassung finden Sie ab Seite 14.

Lassen auch Sie sich durch diese ISPA News Ausgabe zu einem sicheren Internet verführen?

Sicher!

ISPA Forum 2011

Wer beschützt das Internet?

Der Schutz des Internets geht uns alle an. Beim ISPA Forum 2011 erörterten Expertinnen und Experten die Sicherung kritischer Informationsinfrastruktur.

Im Rahmen des ISPA Forums 2011 „Wer beschützt das Internet? Kritische Informationsinfrastruktur auf dem Prüfstand" diskutierten nationale und internationale ExpertInnen die Gefahren für das Internet ebenso wie mögliche Schutzmechanismen.

Schutz des Internets im Krisenfall ist für Provider wichtig

In seiner Begrüßung hob ISPA Präsident Andreas Koman hervor, dass eine robuste Informationsinfrastruktur heute wichtiger denn je sei: „Nahezu jeder Bereich der Wirtschaft, der Verwaltung sowie des Privatlebens ist heute vernetzt. Menschen verlassen sich auf das Internet. Sowohl die Provider als auch alle involvierten Stellen arbeiten gemeinsam daran, das Internet auch im Krisenfall zu schützen."

Europäischer Kooperation und Koordination sind wesentlich

In seinem Impulsreferat betonte Steve Purser, technischer Leiter der ENISA, der Europäischen Agentur für Netzwerk- und Informationssicherheit, die Bedeutung der europäischen und internationalen Vernetzung. „Genauso wie das Internet global ist, kann auch ein Schutz der Infrastruktur nur gemeinsam geschehen." Paneuropäische Cybersecurity-Übungen wie jene vom November letzten Jahres seien erste wichtige Schritte, um Wissen zu bündeln und für alle verfügbar zu machen.



Eindrücke vom ISPA forum 2011

Intensive Vernetzung birgt Chancen und Risiken

In der anschließenden Podiumsdiskussion erläuterten ExpertInnen grundlegende Gefahrenpunkte und Angriffsflächen sowie notwendige Gegenmaßnahmen: So verwies Sabine Fleischmann, Beraterin und ehemalige Geschäftsführerin von Sun Microsystems, auf die Bedrohung durch die zunehmende Vernetzung der Systeme: „Der Wirkungskreis eines möglichen Ausfallszenarios ist heute viel größer und tiefergehender." Darum sei der Schutz der Infrastruktur daher gerade für die Wirtschaft essentiell.

ISPA Forum 2011

Vernetzung muss vielschichtig sein

Roland Ledinger, Leiter der IKT-Strategie des Bundes, betonte, dass sich nicht nur die Technologie des Internets selbst, sondern auch die ExpertInnen, die sich mit der Sicherheit des Internets beschäftigen, stärker international vernetzen müssen. Er verwies auf erfolgreiche gemeinsame Projekte in Österreich und im europäischen Kontext. „Das Bundeskanzleramt ist in der Lage, in einem Anlassfall schnell auf ein breites Netzwerk von Kontakten und gebündeltem Know How zurückzugreifen."

ISPA Podium (v.l.n.r.): Andreas Wildberger, Andreas Komann, Amir Hassan, Steve Purser, Sabine Fleischmann, Robert Schischka, Roland Ledinger

Bedrohungsszenarien abseits der Technik sollen nicht vergessen werden

Auf ein anderes als das technologische Bedrohungsszenario wies Amir Hassan, Software-Entwickler und Technologieforscher bei Metalab hin: „Es sind weniger technische Probleme, die das Netz bedrohen als vielmehr wirtschaftlich-politische Entscheidungen im Zusammenhang mit Netzneutralität. Das darf in dieser Diskussion um Internetsicherheit nicht vergessen werden."

Alle sind für Netzwerksicherheit verantwortlich

Roland Schischka, Leiter des CERT, des österreichischen Computer Emergency Response Teams erläuterte, dass vor allem die gegenseitige Abhängigkeit von der Informationstechnologie und die zunehmende Vernetzung von Systemen eine Herausforderung darstelle. Er verwies darauf, dass Schutzmaßnahmen aber nicht nur große Rechenzentren betreffen, sondern auch HeimandwenderInnen für die Sicherheit des Netzes verantwortlich seien.

Beim anschließenden Buffet sorgten Schutzmaßnahmen für das Internet auch nach dem offiziellen Ende der Diskussion bei den Teilnehmerinnen und Teilnehmern des ISPA Forums für ausreichenden Gesprächsstoff. ■

Steve Purser, ENISA

Andreas Koman, ISPA Präsident

Info:

Statements der PodiumsteilnehmerInnen sowie ein Interview mit Impulsreferent Steve Purser finden Sie auf den nächsten Seiten.
Weitere Informationen zum ISPA Forum finden Sie unter: www.ispa.at/forum

ISPA Forum 2011

Wer beschützt das Internet?

Kritische Informationsinfrastruktur auf dem Prüfstand

Sabine Fleischmann
Beraterin

Während infrastrukturelle Ausfälle wie unterbrochene Leitungen noch vor 15 Jahren nur kleine Teile der Wirtschaft in ihrem Tagesgeschäft behindert haben (und dort auch nur Teile der Prozesse und Aufgaben), ist der Wirkungskreis eines möglichen Ausfallsszenarios heute größer und tiefergehender.

Das Internet ist eines der wichtigsten technologischen Betriebsmittel

Die letzte Wirtschaftskrise hat uns auch gezeigt, wie verknüpft die einzelnen Wirtschaftszweige sind, sowohl geografisch als auch branchenübergreifend. Die "zweite industrielle Revolution", zu einer Informations- oder Dienstleistungsgesellschaft hat sich längst vollzogen. Das Internet kann man heute durchaus als eines der wichtigsten technologischen Betriebsmittel bezeichnen. Durch die starke Verschränkung von Informationsaustausch und Prozessen zwischen Unternehmen und ihren Kunden und/oder Lieferanten kann die Auswirkung leicht einen Stillstand großer Teile des wirtschaftlichen Handelns umfassen. Daher ist die Frage nach dem Schutz des Internets für die Wirtschaft essentiell.

Amir Hassan
Software Developer

Der pluralistische und offene Charakter des Internets fördert die gleichberechtigte Kommunikation und den freien Informationsaustausch in zuvor unvorstellbarem Ausmaß. Damit wirkt es als wichtiger Träger sowohl technischer als auch sozialer Innovation und fungiert als Stütze einer freien Zivilgesellschaft.
Daraus erklärt sich auch das vermehrte Bestreben durch Unternehmen und Nationalstaaten, den Netzzugang politisch motivierten oder profitorientierten Manipulationen zu unterwerfen und somit die Kontrolle der breiten Öffentlichkeit zu entreißen. Ein solche Korruption halte ich für das bedrohlichste Ausfallszenario.

Angriffe auf die Netzneutralität sind die größte Bedrohung

Ein technischer Komplettausfall hätte mehr oder minder kurzfristig die vollständige Unverfügbarkeit des Internets zur Folge. Eine Verletzung der Netzneutralität hingegen zieht langfristige und tiefgreifende strukturelle Schäden nach sich und erscheint angesichts weltweiter Entwicklungen erheblich wahrscheinlicher. Ein Ansatz zum effektiven Schutz der neutralen Datenübertragung liegt in erster Linie in Internationalen Schutz- und Kontrollbestrebungen, könnte jedoch letztendlich in der Loslösung vom derzeitigen Zugangsmodell liegen.

Roland Ledinger
Bundeskanzleramt

Die Verfügbarkeit von IKT und dem Internet ist heute ein wesentlicher Faktor für eine funktionierende Verwaltung. Kein Ministerium kann heute einfach auf den Papierakt oder auf Karteien zurück steigen. Informationen liegen in vielen Bereichen nur noch in digitaler Form vor und stellen auch rechtlich das Original dar. So erstellen die Bediensteten in den Bundesministerien pro Jahr ca. eine Million Akten in elektronischer Form, dazu gibt es keine Kopien in Papierform. Eine Menge, die ohne Einsatz von IKT und dem Internet nicht mehr bewältigt werden kann.

Sicherheit der Services ist für die Verwaltung essentiell

Daher brauchen wir Sicherheit und Vertrauen für unsere Services und das wiederum bedingt entsprechende Strukturen. GovCERT mit der technischen Expertise von CERT.at bildet dazu das Netzwerk für die öffentliche Verwaltung. Der Austrian Trust Circle ist die Grundlage für den privaten Sektor. So ist das Bundeskanzleramt in der Lage in einem Anlassfall schnell auf ein breites Netzwerk an Kontakten und ein gebündeltes Know how der Experten zurückzugreifen. Zum Schutz der kritischen Informationsinfrastruktur sind also nicht nur die technischen Parameter zu betrachten, sondern auch die notwendigen Koordinations- und Eskalationsmechanismen zu etablieren.

Robert Schischka
cert.at

Ein „Ausfall des Internets“ ist als Bedrohungsszenario zu kurz gegriffen – es geht vielmehr um die Abhängigkeit von der Informationstechnologie und die zunehmende Vernetzung von Systemen in allen Bereichen des täglichen Lebens. Die konkreten Bedrohungen liegen derzeit vor allem auf den Gebieten der Internetkriminalität und Wirtschaftsspionage, aber auch Bedrohungen von „innen“ wie Unachtsamkeit oder gezielte Sabotage können zu existenzbedrohenden Ausfällen führen.

Sicherheit im Netz hängt von jedem Einzelnen ab

Sicherheit kann letztendlich nicht nach außen delegiert werden – es sei denn man gibt auch die damit verbunden Einrichtungen komplett aus der Hand. Insofern sind alle Beteiligten ein Stück mitverantwortlich. Dies trifft nicht nur die Betreiber großer Rechenzentren oder Kommunikationsdienstleister, sondern in letzter Konsequenz auch alle HeimanwenderInnen.
Der Schutz der strategischen Infrastruktur kann nur in Zusammenarbeit von öffentlicher Hand und der Privatindustrie wirksam erfolgen. Der Staat kann hier Rahmenbedingungen schaffen und koordinierend und unterstützend tätig werden. Die eigentlichen Maßnahmen in der Vorbeugung, Gefahrenabwehr und Vorfallsbehandlung werden aber stets beim betroffenen Unternehmen selbst liegen müssen.

ISPA Forum 2011

Wer beschützt das Internet?

Interview

»Internationale Kooperation ist unerlässlich«

Wie die Europa hinsichtlich der Netzwerksicherheit zusammenarbeitet und warum das so wichtig ist, erklärt Steve Purser, Leiter des Technical Competence Department der ENISA, im Interview.

Von Andreas Wildberger

ISPA: Sie leiten das Technical Competence Department der Europäischen Agentur für Netz-und Informationssicherheit ENISA. In aller Kürze: Was ist das Mandat der ENISA?

Steve Purser: Kurz gesagt, das Mandat der ENISA ist, gemeinsam mit der Kommission und den Mitgliedsstaaten die Informationssicherheit der EU zu sichern. Unser übergeordnetes Ziel ist es, sicherzustellen, dass der europäische Ansatz über geografische Grenzen kohärent ist und konsequent verfolgt wird. Als europäische Agentur hat die ENISA eine grenzüberschreitende Sicht auf die Informationssicherheit. Gemeinsam mit den Mitgliedstaaten arbeiten wir daran, dass der europäische Ansatz so weit wie möglich mit nationalen Ansätzen abgeglichen ist.

Was ist dabei besonders wichtig?

Es ist wichtig, dass über Grenzen hinweg kohärent gearbeitet wird, denn das hilft, „weak links" zu vermeiden. Weiters ermöglicht dieser Ansatz, die Vorteile des Grundsatzes des „Defense in Depth" einzusetzen. Das ist eines der ältesten Prinzipien in der Informationssicherheit. Es bedeutet, mehrere Steuerelemente gegen bestimmte Risiken umzusetzen.

Kohärenz ist eine große Herausforderung und es ist sehr leicht, dabei Fehler zu machen. Wie viele Organisationen haben ein Vermögen ausgegeben, um Daten „on the wire" zu sichern, damit die Empfänger in einem Internet-Café die gleichen Daten sehen?

Zeitliche Konsistenz ist ebenso wichtig, denn ohne sie wäre es nicht möglich, auf früheren Fundamente aufzubauen.

In Ihrem Impulsreferat beim ISPA Forum erwähnten Sie, dass der Dialog, politische Zusammenarbeit und ein internationaler Aktionsplan der Schlüssel für die globale Netzwerksicherheit sei. Können Sie das erläutern?

Nur wenige Menschen würden bestreiten, dass wir in einer global vernetzten Welt leben. Die europäischen Bürgerinnen und Bürger nehmen Dienstleistungen, die überall auf der Welt betrieben werden, in Anspruch und sie brauchen ein Sicherheitsmodell, das diese Tatsache berücksichtigt.

Wenn Sie in Großbritannien leben und ein Element von einer asiatischen Webseite einkaufen, können sich die rechtlichen Rahmenbedingungen, die eine solche Transaktion erfordern, als kompliziert erweisen. Das ist einfach zu erkennen.

Subtiler sind jedoch Bedenken in Bezug auf Privatsphäre und

Datenschutz, in denen Gesetze und Erwartungen dazu neigen, international stark zu variieren. Die Sache wird noch komplizierter, wenn wir neue Geschäftsmodelle, wie Cloud Computing, auf denen Daten „in der Wolke“ gespeichert werden, betrachten. Die Information, nur zu wissen, wo die Daten gespeichert sind, kann eine Herausforderung darstellen. Die Tatsache, dass Systeme und Daten weltweit verbunden sind, erfordert auch einen globalen Ansatz zur Sicherung der Systeme.

Welche Bereiche kann das noch betreffen?
Die internationale Zusammenarbeit ist ein sehr wichtiger Faktor für die Wiederherstellung des Systems nach jeglicher Art von Cybervorfall. Eine solche Zusammenarbeit kann ganz unterschiedlich sein: von politischen Vereinbarungen über die Handhabe eines kriminellen Vorfalls bis zur Umleitung des Datenverkehrs nach einem Netzausfall. Der Punkt ist, dass solche Probleme im Allgemeinen nicht von einzelnen Mitgliedstaaten alleine gelöst werden können, sondern dass alle europäischen Initiativen mit der unserer internationalen Kollegen ausgerichtet werden müssen.

Aus Ihrer Sicht: Welche Rolle sollten ISPs in Bezug auf den Schutz der Informationsinfrastruktur spielen?
Generell sollten jene Gruppen die Sicherheitsmaßnahmen umsetzen, für die sie zuständig sind - das sagt der Hausverstand. Da ISPs auf der Netzwerkebene arbeiten, eignen sie sich vor allem dafür, bestimmte Netzwerk-Kontrollen einzuführen. ISPs sind aber nicht geeignet, Steuerelemente oder Zugriffe auf Daten von Back-End-Servern oder Arbeitsstationen der Endbenutzer zu implementieren.

Sie erwähnten auch eine europaweite Information Security-Übung. Können Sie diese kurz beschreiben?
In der Übung wurde geprobt, wie sich die Mitgliedsländer im Fall eines Sicherheitsvorfalls verhalten. An der Übung beteiligten sich alle EU-Mitgliedsländer und die EWR-Länder. Die Übung selbst wurde als „Distributed Tabletop“-Ansatz durchgeführt. Die Mitgliedstaaten nahmen an einer zentralen Stelle teil, hatten aber per Telefon Zugang zu ihren nationalen Kontakten.
Ziel der Übung war, drei Aspekte der Kommunikation zu testen und zu sehen, wie Sie im Fall eines grenzüberschreitenden Vorfall reagieren würden: An wen würden Sie sich wenden? Wie gut ist Ihr Verständnis für das Mandat und Entscheidungsbefugnisse von diesem Kontakt? Welche Kanäle würden Sie für welche Information verwenden?
Auch wenn das trivial aussieht: Wir haben dadurch einiges gelernt und die ENISA arbeitet nun mit dieser Gemeinschaft daran, nächste Schritte zu identifizieren. ▶

Steve PURSER
Ist Leiter der technischen Abteilung der ENISA (Europäische Agentur für Netzwerk- und Informationssicherheit).

Er wurde in Großbritannien geboren und studierte an den Universitäten von Bristol und East Anglia, wo er hat einen Bsc. in Chemie machte und in Chemischer Physik promovierte. 1985 begann er im Bereich Software Entwicklung zu arbeiten und übernahm nach und nach Aufgaben in Projekt Management und Beratung. Von 1993 bis 2008 war er als Information Security Manager für eine Reihe von Unternehmen im Finanzsektor tätig.
Im Dezember 2008 kam er als Leiter der technischen Abteilung zur ENISA (European Network and Information Security Agency), wo er derzeit für alle operativen Aktivitäten zuständig ist.
Steve Purser ist Mitbegründer des ‚Club de Securité des systèmes Informatiques au Luxembourg‘ (CLUSSIL) und derzeit ENISA Vertreter in der ISO SC 27 Arbeitsgruppe. Er veröffentlicht häufig Artikel in der Fachpresse und ist der Autor von ‚A Practical Guide to Managing Information Security‘ (Artech House, 2004).

Sind Sie zufrieden mit dem Ergebnis?
Sehr. Die Übung ist ein perfektes Beispiel, wie die Mitgliedstaaten zusammenarbeiten, um grenzüberschreitende Sicherheit zu etablieren. Nicht nur, dass die Mitgliedstaaten die Ziele, die sie sich setzten, rechtzeitig und innerhalb des Budgets erreicht haben, sie schufen auch eine Gemeinschaft. Diese tauscht Informationen und „Good-practice"-Beispiele aus.
Einfach gesagt: Die Gemscheinschaft kann so von sich selbst auf einer kontinuierlichen Basis lernen. Und damit hat die Übung genau ihr Ziel erreicht.

Wird es künftig mehr Übungen geben?
Es wird weitere Übungen geben. Voraussichtlich wird die Zusammenarbeit mit Gruppen, die ähnliche Aufgaben in anderen Ländern durchführen, geübt werden. Voraussichtlich werden wir künftig auch mit anderen Gruppierungen zusammenarbeiten. Wir überlegen da vor allem, wie wir den privaten Sektor in diese Übungen einbinden können, da ein erheblicher Teil der Critical Information Infrastructure von privaten Unternehmen betrieben wird.

Ich weiß aus Ihrer Biographie – Sie haben lange in der Wirtschaft gearbeitet – dass Ihre Sicht auf strategische Aufgaben stark von einem praktischen Ansatz getrieben wird. Wie tarieren Sie die Vielfalt an Meinungen in Bezug auf Netz- und Informationssicherheit in der EU aus?
Es ist meine Aufgabe, das Team zu führen. Es ist das Team, das die Analyse macht und Empfehlungen ausspricht. Präziser: Das ENISA-Team arbeitet eng mit Arbeitsgruppen, die von Experten aus den Mitgliedstaaten bestehen, zusammen. Daher spiegelt die Arbeit, die wir produzieren, die Erfahrungen der EU-Gemeinschaft als Ganzes wider. Ich persönlich bin fest davon überzeugt, dass der Rat, den wir der Gemeinschaft geben, auf fundierten Erfahrungen aus der Praxis fussen muss. Zu dieser Sicht ermutige ich auch mein Team. Am Ende des Tages, es ist eine Teamleistung - das Team besonders vielfältig in diesem Fall!

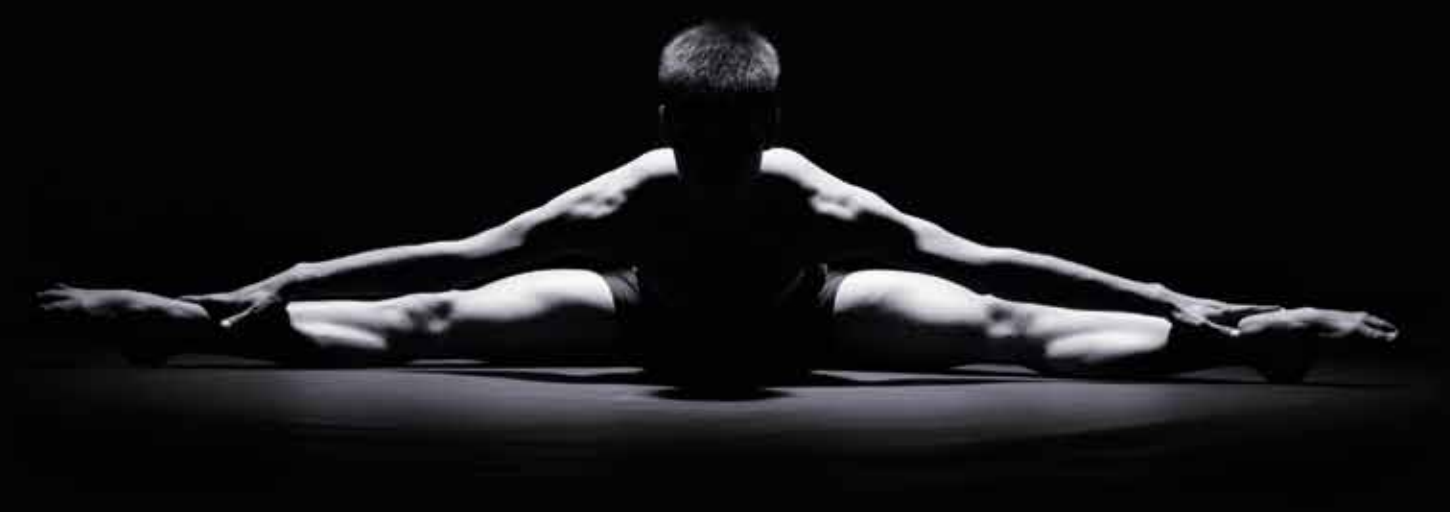
Wenn Sie drei Wünsche zum Verschieben von Europas Netz-und Informationssicherheit einen Quantensprung nach vorn hätten, welche wären das?
Mein erster Wunsch wäre ein erfolgreicher Abschluss des ENISA-Mandats. Dies scheint im Moment ganz glatt zu gehen, also bin ich verhalten optimistisch.

Die wahrscheinlich größte Veränderung ist das Verhalten der Menschen in der elektronischen Welt. Als die ersten Autos in Betrieb genommen wurden, wurden Leute angestellt, die vor dem Auto hergingen und eine rote Fahne für Fußgänger schwangen um sie vor der Gefahr zu warnen. Seitdem ist viel passiert, wir haben unser Verhalten an das Risiko angepasst.
Ein ähnlicher Prozess muss in der elektronischen Welt passieren. Bürgerinnen und Bürger müssen lernen, Risiken durch intuitive Risikomodelle, zu beherrschen. Ich nenne das oft „elektronischer Hausverstand". Das wird mit der Zeit geschehen und es ist unsere Aufgabe, solche Entwicklungen zu fördern.
Außerdem glaube ich, dass es wichtig ist, der Sicherheits-Community selbst ein wenig von der „algorithmischen" Sicht ihrer Sicherheitsbedenken zu nehmen, sie dazu zu führen, dass sie mehr in Prinzipien denken sollten. Sicherheit ist oft kontextbezogen: Eine ideale Lösung in einer Umgebung würde in einem anderen Kontext überhaupt keinen Sinn machen.
Aber ich glaube, dass es eine gute Sache ist, um den Austausch bewährter Verfahren zu fördern. Dazu ist es unerlässlich, dass „good praxis" korrekt interpretiert wird und nicht gedankenlos angewandt wird.

Vielen Dank für das Gespräch! ■

waveline-mar.com

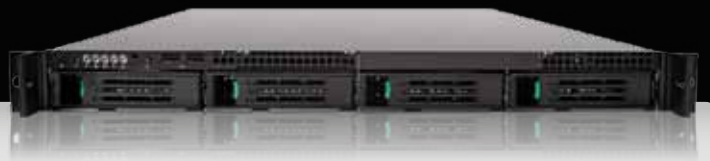
Der Spagat zu mehr Effizienz und Performance



Energieeffizienter und performanter als vergleichbare Systeme namhafter Hersteller!

Vier Server in einem: Intel® Server-System SR1640TH High-Density-1U-System

- Performance-optimiertes System zur Einsparung von Platz- und Stromverbrauch
- Ideal für kleine Business-Umgebungen als Hosting-Server und Web-Server
- Geringe Anschaffungs- und Betriebskosten für Intel® Xeon® 3400 Prozessoren
- 1U Gehäuse mit vier unabhängigen Single-Socket Servern der Intel® Xeon® 3400 Serie mit 4 DIMMs pro Serverknoten
- Zwei einzelne, von vorne zugreifbare Recheneinschübe für reduzierte Stillstandszeiten
- Intel® Intelligent Power Node Manager und IPMI 2.0 Schnittstelle bereits integriert
- Optimierte Kühlung und zwei redundante, hocheffiziente 450W (80-Plus Silver) Netzteilen



Gebaut für geringsten TCO: Intel® Server-System SR1695WB

- Unterstützung von bis zu zwei Intel® Xeon® Prozessoren der 5500 oder 5600 Serie
- Neuesten Technologien zur Kühlung und Stromersparnis, für hohe Rechendichte und energieeffizienten Betrieb der Intel® Xeon® 3400 Serie
- Intel® Intelligent Power Node Manager mit integrierter IPMI 2.0 Schnittstelle
- Hoch skalierbarer DDR3 Speicher (8 DIMM Sockel)
- Ein PCI Express 2.0 (x8) Erweiterungsslot auf Riser-Karte
- Intel® Remote Management Module 3 für KVM- und Medien-Umleitung
- Variable Speicherkontroller Optionen

Ihre möglichen Konfigurationen für SR1640TH und SR1695WB erhalten Sie auch als Leihstellung!

System-Kit SR1640TH
Intel® Xeon® Processor L3406 (4M Cache, 2.26 GHz)
8x 2GB DDR3/1333 Samsung ECC Registered
4x Western Digital 500GB SATA

System-Kit SR1695WB
Intel® Xeon® Processor L3426 (8M Cache, 1.86 GHz)
8x 4GB DDR3/1333 Samsung ECC Registered
4x Western Digital 500GB SATA

intel Technology Provider Platinum 2011

Ihre Leihstellung zwei Wochen kostenlos!
Sie werden feststellen, dass unsere Systeme auch das halten was wir versprechen! **Try before you buy** und fordern Sie gleich Ihre kostenlose Teststellung per Email an oder kontaktieren Sie Ihren persönlicher Ansprechpartner: **Mario Marek Tel.: 06 64-24 55 605, Email: MMarek@microtronica.com**

MICROTRONICA
www.microtronica.com/isp-a

http://technologyprovider.intel.com

Das bringt die Vorratsdatenspeicherung

Ende April wurden die Gesetze zur Umsetzung in Österreich im Parlament beschlossen. Hinter den Gesetzen verbergen sich einige interessante Neuerungen.

Von Maximilian Schubert

Die Richtlinie zur Vorratsdatenspeicherung wurde in Folge der Terroranschläge von London und im Rat der EU-Justiz- und Innenminister beschlossen. Sie soll die Ermittlungsbehörden dabei unterstützen, organisierte Kriminalität und Terrornetzwerke zu bekämpfen beziehungsweise der Ermittlung, Feststellung und Verfolgung schwere Strafdaten dienen.

Zu diesem Zweck müssen sogenannte Verkehrsdaten von den Betreibern gespeichert werden. Diese geben Aufschluss darüber, welche Personen zu welchem Zeitpunkt an welchem Standpunkt kommuniziert haben. Was die Dauer der Speicherung dieser Daten angeht, so stellt es die Richtlinie den Mitgliedstaaten frei, die gespeicherten Verkehrsdaten als so genannte Vorratsdaten für einen Zeitrahmens von sechs bis 24 Monaten zu speichern.

Keine Vorratsspeicherung von Kommunikationsinhalten

Der Inhalt der Kommunikation (sog. Inhaltsdaten, z.B. Inhalte eines Telefonats, Text in einem E-Mail) ist von der Richtlinie nicht erfasst und muss bzw. darf auch in Hinkunft nicht gespeichert werden. So müssen Betreiber zwar speichern, welche eindeutige Kennung (IP-Adresse einer Teilnehmerin oder eines Teilnehmers) der Nutzung im Internet zugewiesen war, nicht jedoch welche Webseiten aufgerufen wurden.

Gesetzesentwurf durch eine Grundrechts-Forschungsinstitut

Was die Umsetzung in Österreich bemerkenswert macht, ist, dass das Bundesministerium für Verkehr Innovation und Technologie das in Wien ansässige Ludwig Bolzmann Institut für Menschenrechte (BIM) mit der Erstellung eines Umsetzungsentwurfes beauftragt hat. Dieser Gegebenheit ist es somit wohl auch zu verdanken, dass sich die Umsetzung der Richtlinie beinahe ausschließlich entlang der Minimalerfordernisse bewegt und somit z.B. eine Speicherdauer von sechs Monaten anstatt von zwei Jahren vorsieht. Jedoch wurde im Rahmen der Entwurfserstellung nicht nur strikt die Richtlinie umgesetzt. Dem BIM war auch daran gelegen, die großteils unübersichtliche Regelung, wann ein Betreiber Daten seiner Kundschaft beauskunften muss, zu vereinfachen und schlüssiger zu gestalten.

Lückenlose Protokollierung aller Beauskunftungs-Anfragen

Um sowohl die Übermittlung von Beauskunftungs-Anfragen als auch deren Beantwortung sicher, nachvollziehbar und auf das unbedingt Notwendige zu beschränken, wird nicht nur das Format der Antworten bis ins Detail festgelegt, es wird auch eine Durchlaufstelle (DLS) geschaffen. Diese DLS ist zwar gänzlich blind gegenüber den von Ihr transportierten (verschlüsselten) Daten, dafür protokolliert sie aber jede Anfrage der Strafverfolgungsbehörden (nicht nur auf Vorratsdaten, sondern auch auf Verkehrsdaten) sowie die Antworten der Betreiber mit.

Zugriff auf Vorratsdaten nur nach vorhergehender Autorisierung

Während die Richtlinie in anderen Ländern derart umgesetzt wurde, dass den Strafverfolgungsbehörden direkter Zugang zu den gespeicherten Verkehrsdaten der Betreiber gewährt werden muss, sieht die österreichische Umsetzung der Vorratsdatenspeicherungs-Richtlinie vor, den Zugriff der Behörden an eine Autorisierung durch Staatsandwaltschaft oder RichterInnen zu binden. Auf diese Weise sollen unrechtmäßige Zugriffe auf Verkehrsdaten und damit auch behördliches ›Data Mining‹ vermieden werden. Auch von Seiten des Providers müssen strenge Vorlagen (4-Augen-Prinzip, revisionssichere Protokollierung) eingehalten werden, um den Zugriff von Unbefugten auf Vorratsdaten auszuschließen.

Das Schicksal des Entwurfs im Ministerrat

Doch der ursprüngliche Entwurf des BIM wurde im Ministerrat abgeändert: So wurde etwa der Grundsatz des Richtervorbehalts für einen Großteil der Anfragen auf Vorratsdaten gestrichen beziehungsweise durch eine Anordnung des Staatsanwaltes ersetzt. Der Grundsatz der Mindeststrafe wurde durch einen Verweis in der Strafprozessordnung ebenfalls gestrichen, was gleichzeitig dazu führt, dass es möglicherweise für die Betreiberfirmen für einen Großteil der Beauskunftungen von Vorratsdaten keinen Kostenersatz geben wird.

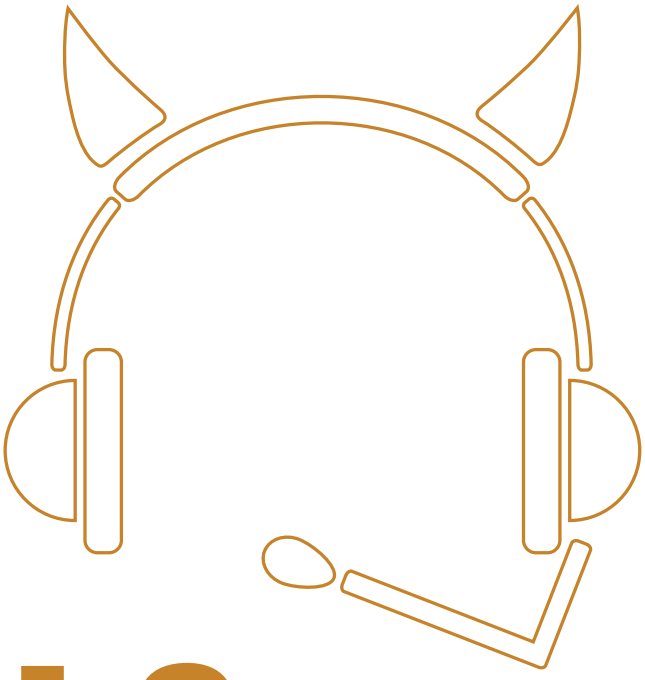
Doch hilft die Vorratsdatenspeicherung wirklich?

Ob die Vorratsdatenspeicherung ein effektives Mittel im Kampf gegen den Terrorismus ist, erscheint auch im Licht des von der Kommission kürzlich veröffentlichen Evaluierung als sehr fraglich. Bereits vor dem Beschluss wurde der Entwurf der Richtlinie heftig kritisiert, da die Vorratsdatenspeicherung in eine Reihe von Grundrechten eingreift. Kritiker sehen ein großes Problem darin, dass den Ermittlungsbehörden durch die anlasslose Speicherung von Verkehrsdaten ein Datenpool zur Verfügung gestellt wird, der es ermöglicht, Daten systematisch auf Auffälligkeiten zu untersuchen. Das kann Betroffene dazu bringen, sich unbegründet rechtfertigen zu müssen.

Noch neun Monate bis zur Umsetzung

Die nunmehr bestehenden gesetzlichen Regelungen werden, auch bedingt durch den Druck der Europäischen Kommission, wohl nicht mehr zu ändern sein. Als kleiner Trost verbleibt neben all den grundrechtlichen Einschränkungen, dass Betreiber ab 1. April 2011 nur dann zur Speicherung der Vorratsdaten verpflichtet sind, sofern Ihre hierfür notwendigen Investitionskosten zuvor vom Bund zu 80 Prozent beglichen wurden. Somit gilt auch im Zusammenhang mit der Vorratsdatenspeicherung: »Ohne Geld, ka Musi«. ■

Info: ISPA Positionen zur Voratsdatenspeicherung finden Sie auf unserer Website www.ispa.at → Service → Positionspapiere.



Ist Voice over IP gefährlich?

Um Telefonie Fraud ging es bei einem der letzten Workshops der ISPA Academy. Die wichtigsten Punkte finden Sie hier zusammengefasst.

Von Klaus Darillion

Betrug und Missbrauch im Telefoniesektor sind vermutlich so alt wie die Telefonie selbst. So gibt es Betrug zwischen Betreibern, wie z. B. Interconnect-Fraud, Terminierungs-Fraud und False-Answer-Services, zwischen Endkunden und Betreibern, wie z. B. den Subscription-Fraud (Anmeldung unter falschem Namen mit gefälschten Papieren) oder zwischen Endkunden wie z.B. beim PBX Hacking, bei der ein Angreifer in eine PBX eindringt oder einfach nur unsichere PBX Konfigurationen ausnutzt (z.B. 2stage-dialing ohne Autorisierung).

Durch den Siegeszug des IP-Protokolls und des Internets änderten sich auch Telefoniedienste. Telefone und Telefonanlagen verwenden IP-Protokolle als flexiblen kostengünstigen Ersatz zu den alten Protokollen und Betreiber bieten Ihren Kunden Webportale an, mit denen sie die Telefondienste selbst verwalten können. Wenn nun Telefondienste über das Internet verwendet werden, ergeben sich für Angreifer zusätzliche Angriffsmöglichkeiten um die Systeme zu manipulieren. Das heißt, zusätzlich zu den bereits bestehenden Betrugsszenarien kommen neue Möglichkeiten hinzu, die folgend aufgezeigt werden und deren Lösungen diskutiert werden.

Voice over IP (VoIP)

Bei Voice over IP (VoIP) werden die Telefoniedaten nicht wie bisher über ein eigenes Netz geführt, sondern die Telefonie wird zu einem der möglichen Dienste in IP-Netzen. Es gibt eine Vielzahl von VoIP Protokollen – öffentlich standardisierte sowie proprietäre von diversen Herstellern. Das bekannteste und am meisten verwendete Protokoll ist das Session Initiation Protokoll (SIP) für die Signalisierungsdaten (Gesprächsaufbau, Terminierung, ...) bzw. das Real-Time Transport Protokoll (RTP) zur Übertragung der Sprachdaten.

Zur Authentifizierung wird bei SIP, wie bei vielen anderen Internetdiensten, üblicherweise die Kombination Benutzername und Passwort verwendet. Dadurch ergibt sich schon ein riesiger Unterschied zu traditionellen Telefoniesystemen, welche ein physikalisches ›Token‹ zur Authentifizierung verwenden. Bei der Festnetztelefonie ist das die Zweidrahtleitung, bei der Mobiltelefonie die SIM Karte. Diese sind schwer stehlbar, so ist z. B. die physische Präsenz des Angreifers erforderlich und ein Diebstahl fällt schnell auf. Wenn ein Angreifer jedoch Benutzername und Passwort stiehlt, dann fällt das nicht sofort auf, da die Zugangsdaten eigentlich nicht gestohlen sondern kopiert wurden und dadurch der Dienst vom Benutzer und Angreifer gleichzeitig verwendet werden kann.

Die konkrete Art des Angriffes bzw. der Schutz vor diesem hängt stark vom jeweiligen Angriffsszenario ab. Im Folgenden werden drei oft verwendete Anwendungsszenarien dargestellt:

Private Branch Exchange (IP-PBX)

Bei einer IP-PBX (Private Branch Exchange, Nebenstellenanlage) werden die Nebenstellenapparate über ein IP-Netz an die Telefonanlage ›angeschlossen‹. Für dieses Szenario ist es nicht notwendig, dass die Telefonanlage eine Verbindung in das Internet hat – reisenden Mitarbeitern wird der Telefoniedienst z.B. nur über das Firmen-VPN gewährt. Dadurch können Angreifer, die üblicherweise über das Internet angreifen, nicht mehr auf die PBX zugreifen bzw. diese hacken. Administratoren machen jedoch oft den Fehler sich dadurch in Sicherheit zu wiegen und verwenden auf der PBX eine unsichere Konfiguration (z.B. unsichere Passwörter oder gar keine Autorisierung). Später wird dann z. B. einmal der PBX für andere Dienste ein Zugriff ins Internet erlaubt und schon haben Angreifer ein einfaches Spiel die unsicheren Passwörter herauszufinden und die Telefonanlage für Telefonate zu Mehrwertdiensten oder teuren Auslandsdestinationen zu missbrauchen.

Hosted VoIP

Unter ›hosted‹ versteht man, dass der Endkunde nicht selbst eine SIP Infrastruktur betreibt, sondern der Dienst von einem VoIP Anbieter betrieben wird und beim Kunden nur ein SIP Telefon oder SIP Softphone verwendet wird. Der angebotene Dienst kann vom einfachen ›POTS-Replacement‹ (Festnetzersatz) bis zu einer virtuellen Nebenstellenanlage reichen. Hier wird die Verbindung sehr oft über das Internet hergestellt und Benutzer wie auch der VoIP Anbieter sind den Angriffen von Hackern ausgesetzt.

Für den Benutzer lässt sich hier sehr einfach Abhilfe schaffen: Firewalls sollen so konfiguriert werden, dass die SIP Telefone nur Verbindung zu den IP-Adressen des VoIP-Anbieters haben und somit gegen Angreifer aus dem Internet geschützt sind. Für die VoIP-Anbieter ist das Absichern schon um einiges komplizierter, da ein beliebtes Feature ja die Verwendung des Dienstes von überall auf der Welt ist und dadurch der VoIP-Anbieter den Zugriff nicht im Vorhinein einschränken kann. Hier ist es besonders wichtig sichere Passwörter zu verwenden. Lange zufällige Passwörter (mehr als zwölf Zeichen) stellen kein Problem dar, da der Benutzer sich das Passwort ja nicht merken muss, sondern das Passwort nur einmalig in seinem ▶

Gerät konfiguriert. Gerade für ›Brute-Force‹ Attacken gibt es frei verfügbare Programme welche einfach zu bedienen sind und sehr oft angewendet werden. Nahezu täglich sind solche Angriffe auf den Servern der VoIP-Anbieter erkennbar. Andere Methoden diese Hacker abzuwehren sind das Ausweichen auf einen anderen Port als den Standardport 5060 sowie das Erkennen von solchen Angriffen und das dynamische Sperren der IP-Adresse des Angreifers.

SIP-Trunking

Hier wird mittels SIP ein sogenannter ›Trunk‹ zu einem VoIP-Anbieter hergestellt. Trunks unterscheiden sich zu normalen VoIP-Verbindungen darin, dass der Kunde eine größere Anzahl von gleichzeitigen Telefonaten führen kann und mit einem einzigen Benutzernamen/Passwort unterschiedliche Absendernummern verwenden kann. SIP-Trunks werden üblicherweise von Telefonanlagen verwendet oder von VoIP-Gateways, die eine traditionelle Telefonanlage VoIP-fähig machen. Die Angriffszenarien und Präventionen sind ähnlich zu ›hosted‹-Diensten. Der Endkunde sollte seine Geräte durch Firewalls so schützen, dass die Kommunikation nur mit den Servern des VoIP-Anbieters erlaubt wird, bzw. der VoIP Anbieter sollte seinen Kunden sichere Passwörter vorschreiben.

Erkennen von Angriffen

Das Hauptproblem für einen VoIP-Anbieter ist, dass er einen ›guten‹ nicht von einem ›bösen‹ Benutzer unterscheiden kann. Falls der Angreifer in Besitz der Zugangsdaten eines legitimes Benutzers kommt, z. B. durch Phishing oder Brute-Force Attacken, so kann er diese verwenden um sich gegenüber dem VoIP-Anbieter auszuweisen und für den VoIP-Anbieter ist der Unterschied nicht erkennbar. Ident ist die Situation wenn ein Angreifer Kontrolle über das Kundenequipment hat (PBX-Hacking). Der VoIP-Anbieter sieht in diesem Fall ein Telefonat von der PBX des Kunden, kann aber nicht erkennen, ob dahinter ein Angreifer oder legitimer Nutzer steht.

Die einzige Möglichkeit solche Angriffe zu erkennen bieten ›Fraud-Detection‹ Systeme, die das Telefonieverhalten der Benutzer überwachen und z. B. bei vielen Telefonaten zu ›speziellen‹ Destinationen oder bei Erreichen eines Gebührenlimits Alarm schlagen und ev. den Account automatisch sperren. Diese Systeme können einen Angriff nicht verhindern, jedoch den Schaden gering halten – gehackte Telefonanlagen können übers Wochenende schnell einen Schaden von mehreren zigtausend Euro verursachen. Speziell kostengünstige Ansätze wie »die Telefonanlage konfiguriert mir der HTL Schüler meines Nachbarn« können so schnell zu Eigentoren werden. Das liegt wohl daran, dass im Internet viele Anleitungen kursieren, die hauptsächlich auf Funktionalität aber nicht auf Sicherheit ausgelegt sind und Administratoren oft nicht alle potentiellen Schwachstellen der Protokolle und jene der verwendeten Software kennen. Darum empfiehlt sich bei Telefonanlagen im Eigenbau eine Kontrolle der Konfiguration durch einen VoIP-Sicherheitsexperten.

Für Privatkunden, die VoIP nur selten verwenden (z.B. während Auslandsaufenthalten), empfiehlt sich auch die Verwendung von Pre-Paid Diensten, da hier der mögliche Schaden begrenzt ist.

Fazit

Je mehr Protokolle ein System unterstützt, umso mehr Angriffsmöglichkeiten gibt es. Diese potentiell höheren Angriffsmöglichkeiten können jedoch schon durch ein paar einfache Grundregeln abgewehrt werden. Man kommt sich als VoIP-Security Experte schon etwas lächerlich vor, wenn man Anwendern immer wieder predigen muss, dass sie sichere Passwörter verwenden sollen. Trotzdem sind unsichere Passwörter immer noch der Hauptgrund für erfolgreiche Angriffe auf VoIP-Systeme.

Wer sich also an die Grundregeln hält und die Konfiguration von Experten überprüfen lässt, der kann die Vorteile und Flexibilität von VoIP-Systemen mit gutem Gewissen verwenden. ■

Info: Bei Fragen wenden Sie sich bitte direkt an klaus.darilion@ipcom.at.

DI Dr. Klaus Darilion
ist Experte für VoIP/SIP Security. Er ist seit sechs Jahren bei nic.at bzw. deren Tochter IPCom GmbH angestellt und beschäftigte sich dort mit dem Aufbau von ENUM. Aktuelle Aufgabengebiete sind SIP Beratung und Security Audits von SIP Service Providern. Darilion ist außerdem sehr aktiv in den Communities der Open Source Projekte Asterisk (IP-PBX) und Kamailio (SIP-Proxy).

In der ISPA Academy »Medienarbeit für IT-Unternehmen« wurden die Grundlagen guter Pressearbeit erläutert.

»IT-Themen sind in der Presse sehr gefragt«

Von Edith Michaeler

Wie kann ich mein Unternehmen richtig in den Medien präsentieren? Was muss ich beachten, wenn ich mein Unternehmen bewerben will? Welche Medien sind für IT-Themen relevant? Diese Fragen wurden im Rahmen des ISPA Academy Seminars „Medienarbeit für IT-Unternehmen" gestellt. Denn Medien- und Öffentlichkeitsarbeit für IT-Unternehmen stand im Mittelpunkt des Seminars, das diesmal in Zusammenarbeit mit der APA (Austria Presse Agentur) veranstaltet wurde.

Der dreistündige Workshop war in zwei Teile gegliedert: Karin Thiller, Geschäftsführerin der APA-OTS, gab eine Einführung in die Grundlagen der Medienarbeit. Werner Müllner, stellvertretender Chefredakteur der APA, stellte anschließend die Besonderheiten des Agenturjournalismus vor.

Pressearbeit ist nicht Marketing

Da viele Teilnehmerinnen und Teilnehmer in den Mitgliedsunternehmen auch für Marketing-Agenden zuständig sind, ging Karin Thiller auf die Unterschiede zwischen Pressearbeit und Marketing ein: Während Marketing vor allem der Absatzförderung dient und somit eine klare ›werbliche‹ Aussage haben soll, ist es die Aufgabe der Pressearbeit, das Image eines Unternehmen darzustellen und gegebenenfalls zu verbessern. Während beim Marketing die KundInnen zur Zielgruppe zählen, spricht PR Multiplikatoren wie JournalistInnen an.

Nach dieser grundlegenden Einführung standen einige Instrumente der Medienarbeit im Mittelpunkt: die Presseaussendung, die Pressekonferenz, das Interview, der Hintergrundbericht und der Exklusivbericht.

Starkes Interesse an IT-Themen

Generell sei ein steigendes Interesse der Öffentlichkeit an IT-Themen zu bemerken, erläuterte die Geschäftsführerin des IT-Portals. Die Trennung zwischen Fachpublikum und KonsumentInnen sei vielfach nicht mehr möglich. Die Themen in der IT-Berichterstattung würden häufig von deutschen und US-amerikanischen Leitmedien vorgegeben. Spezifische Berichterstattung aus Österreich beschränke sich häufig auf IT-Politik, da Zahlen und Daten aus Österreich schwer zu bekommen seien.

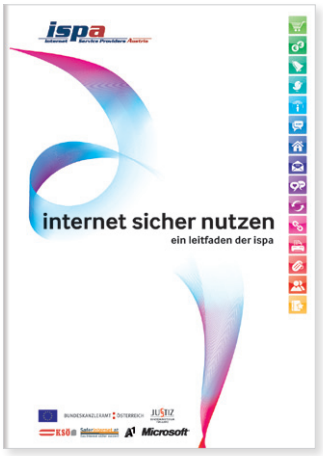
In diesem Zusammenhang forderte Karin Thiller die SeminarteilnehmerInnen auf, mehr Presseinformationen zu heimischen Entwicklungen und Zahlen einzubringen. Allerdings machte sie auch darauf aufmerksam, dass das bereitgestellte Material Mehrinformationen wie etwa aktuelle Vergleichszahlen bieten müsse. Information, die in der Presse angenommen werde, müsse mehr bieten als reine Produktwerbung, denn diese werde sofort erkannt und aussortiert, betonte die APA-OTS Geschäftsführerin.

IT-Fakten aus Österreich gesucht

Abschließend appellierten die Workshopleiter an IT-Unternehmen, ihre Themen und Berichte aktiv an die Presse heranzutragen. Sie berichteten von einer Podiumsdiskussion zu IT-Journalismus in Österreich, in der führende IT-Journalisten bekundeten, dass sie stark an Informationen und Hintergründen zu IT-Themen in Österreich interessiert seien. ■

Info: ISPA-Mitglieder finden die Unterlagen zur ISPA Academy »Medienarbeit für IT-Unternehmen« auf unserer Website www.ispa.at im Mitgliederbereich unter Termine → Rückblick.

Neuauflage der »internet sicher nutzen«-Broschüre



Bereits zum drittem Mal legte die ISPA die Broschüre »internet sicher nutzen« auf.

Von Romana Cravos

Bereits zum dritten Mal wurde die Saferinternet Broschüre neu aufgelegt und das aus gutem Grund: Der ISPA als Interessensvertretung der Internetwirtschaft war es immer schon ein großes Anliegen jene zu schulen, die als Bezugspersonen die aufwachsende Generation bei der Internetnutzung aktiv begleiten. Justizministerin Beatrix Karl und Josef Ostermayer, Staatssekretär für Medien und Koordination haben sich ebenfalls in den Dienst der guten Sache gestellt und für die erweiterte und aktualisierte Ausgabe der Broschüre »Internet sicher nutzen« ein Vorwort geschrieben.

Internetkompetenz Erwachsener wird unterstützt

Informationsmaterial wie der Ratgeber »internet sicher nutzen« sorgen dafür, das Wissensgefälle zwischen den Altersgruppen zu verringern. Ziel ist es, die Generation der über Dreißigjährigen internetfit zu machen und genau das gelingt mit der Themenauswahl der Neuauflage.

Gerade Erwachsene und Eltern, die der Altersgruppe 30+ angehören, haben hier Nachholbedarf. In der Altersgruppe der 35- bis 44-jährigen nutzen laut Statisik Austria nur 27 Prozent soziale Netzwerke, Instant Messaging, Blogs, Newsgroups oder Online-Diskussionsforen. Außerdem verdeutlichte die EU Kids Online Studie (Jänner 2011), dass österreichische Eltern die Online-Risiken ihrer Kinder unterschätzen.

Das Ziel der ISPA ist, dieser Entwicklung entgegen zu wirken und Erwachsenen das Wissen rund um eine sichere Nutzung des Internets näher zu bringen. Denn nur wenn Erwachsene selbst informiert sind, können sie Kinder und Jugendliche bei der Nutzung des Internet authentisch unterstützen.

Erweiterung des Themenkatalogs

Neben einer rechtlichen und inhaltlichen Aktualisierung des Kompendiums wurde das Kapitel Soziale Netzwerke um einen Facebook-Check und den Bereich Location Based Services erweitert. Auch die Frage »Wie sorge ich dafür, dass meine Passwörter sicher sind?« wird umfangreich beantwortet. Fragen rund um das Thema Sexualität und Internet werden im Zusammenhang mit Erziehung ebenfalls beantwortet.

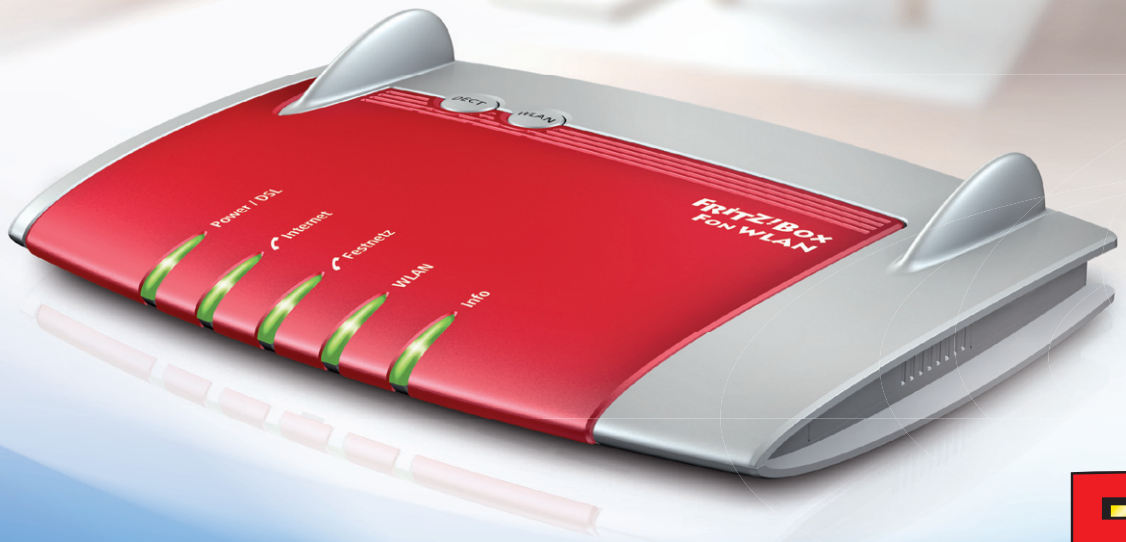
Gelungene Zusammenarbeit

Aber was wäre ein derartiger Ratgeber ohne Support durch Partner? An dieser Stelle ein Dankeschön für die Unterstützung durch das Bundeskanzleramt, das Bundesministerium für Justiz, das Kuratorium Sicheres Österreich, die Europäische Union, unsere Projektpartner von Saferinternet sowie der Bank Austria und der Erste Bank und Sparkassen. ■

Info: Ein Exemplar der neuen Broschüre finden Sie beigelegt.
Die Broschüre können Sie auch auf unserer Website www.ispa.at → Service → Broschüren herunterladen.

Daheim-Agent 7390

Im Dienste Ihrer Heimvernetzung



Spezialgebiete

- Rasantes VDSL & ADSL
- Schnelles Dual-WLAN N
- Speicher & Mediaserver

ADSL VDSL | WLAN | Telefon | DECT | Media

FRITZ!

FRITZ!Box Fon WLAN 7390 – der Auftrag: Internet, Telefon, digitale Medien

Willkommen in der Breitband-Zentrale – Ihrem Zuhause! Die FRITZ!Box Fon WLAN 7390 ist ein eindrucksvolles Multitalent, denn sie läuft an jedem Anschluss, verbindet alle Ihre Endgeräte und bringt Sie mit phänomenalen Geschwindigkeiten ins Internet.

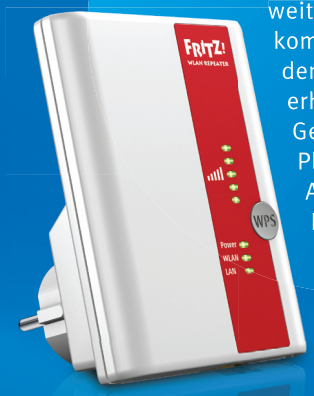
- NEU ADSL und VDSL für Top-Performance bis zu 100 MBit/s
- NEU Dual-WLAN N für gleichzeitigen 2,4-GHz- und 5-GHz-Einsatz
- Integrierte TK-Anlage und DECT-Basisstation
- NEU Interner Netzwerkspeicher mit NAS-Funktionalität
- Mediaserver für Musik, Bilder und Filme im Netzwerk
- NEU Gigabit-Ethernet und zwei USB 2.0-Anschlüsse

Was die FRITZ!Box Fon WLAN 7390 noch alles kann, erfahren Sie im guten Fachhandel, überall, wo es Computer gibt und unter www.fritzbox.eu

Mrz 2010 CHIP ONLINE Testsieger | PC Magazin TESTSIEGER 8/2010 | PCgo 5/10 sehr gut | connect SEHR GUT Heft 6/2010 | Computer Bild 03/2011 „Der derzeit beste WLAN-Router"

FRITZ!WLAN Repeater 300E

Der FRITZ!WLAN Repeater 300E erweitert sicher und schnell Ihr Heimnetz: Auf Knopfdruck lässt sich die Reichweite des WLAN-Netzes komfortabel erhöhen. Über den Gigabit-LAN-Anschluss erhalten netzwerkfähige Geräte wie Drucker und Player eine WLAN-Anbindung an das Heimnetz.



NEU!

11/006

www.fritzbox.eu

HIGH-PERFORMANCE COMMUNICATION BY ... AVM

members Juni 2011

A

a.gunsch.at ACHS
Technologiezentrum Tirol,
Eduard-Bodem-Gasse 5-7/210
6020 Innsbruck
Tel.: +43-699 167 80 000
E-Mail: alfred@gunsch.at
Web: www.gunsch.at

abaton EDV-Dienstleistungs GmbH CHS
Hans-Resel-Gasse 17
8020 Graz
Tel.: +43-316-817 896 0
E-Mail: office@abaton.at
Web: www.abaton.at

ACOnet Vienna University Computer Center BR
Universitätsstraße 7
1010 Wien
Tel.: +43-1-4277-14010
E-Mail: helpdesk@aco.net
Web: www.aco.net

ACW Netzwerk Produkte & Dienste GmbH ABCHS
Erdbergstrasse 52-60/7/3
1030 Wien
Tel.: +43-1-743 45 48
E-Mail: acw@acw.at
Web: www.acw.at

adRom Media Marketing GmbH HS
Lustenauerstraße 66
6850 Dornbirn
Tel.: +43-(0)5522/748 13 0
E-Mail: office@adrom.net
Web: www.adrom.net

AGNITAS AG HS
Werner-Eckert-Straße 6
D-81829 München
Tel.: +49-89/55 29 08 0
E-Mail: info@agnitas.de
Web: www.agnitas.de

Alcatel-Lucent Austria AG BCS
Scheydgasse 41
1210 Wien
Tel.: +43-1-27722 6507
E-Mail: margret.resch@alcatel-lucent.com
Web: www.alcatel-lucent.at

ANEXIA Internetdienstleistungs GmbH HS
Feldkirchnerstraße 140
9020 Klagenfurt
Tel.: +43-463-208501
E-Mail: info@anexia.at
Web: www.anexia.at

APA-IT Informations Technologie GmbH ABCHS
Laimgrubengasse 10
1060 Wien
Tel.: +43-1-360 60-6060
E-Mail: it-vertrieb@apa.at
Web: www.apa-it.at

ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H. ACHS
Grasbergergasse 13, 1030 Wien
Tel.: +43-(0)50 4009 5702
E-Mail: philipp.reschl@arz.at
Web: www.arz.at

ASCUS Telekom GmbH AHS
Viktringer Platz 5, 9073 Viktring
Tel.: +43-1-298 99 600
E-Mail: office@ascus-telecom.com
Web: www.ascus-telecom.com

ATVIRTUAL.NET KG HRS
Albert Heypeter-Gasse 25
2301 Gross-Enzersdorf
Tel.: +43-2249 28807
E-Mail: contact@atvirtual.net
Web: www.atvirtual.net

Austria COM Online Media Computerdienstleistung GmbH & Co.KG ABC
Rooseveltplatz 12, 1090 Wien
Tel.: +43-1-409 31 22
E-Mail: webmaster@austria.com
Web: www.austria.com

AUSTROGATE- Internet- und Telekomdienstleistungen Brunner & Partner OG HRS
Berggasse 36, 2463 Gallbrunn
Tel.: +43-720-007 700
E-Mail: office@austrogate.net
Web: www.austrogate.net

Avalaris CHS
Josefstaedterstrasse 72/2/2
1080 Wien
Tel.: +43-1-4022858 0
E-Mail: ispa@avalaris.com
Web: www.avalaris.com

AVM GmbH for International Communication Technology S
Alt-Moabit 95
D-10559 Berlin
Tel.: +49-30 39976 232
E-Mail: ict-info@avm.de
Web: www.avm.de

B

barga.com technische Dienstleistungen GmbH HS
Leusbuendtweg 49a
6800 Feldkirch
Tel.: +43-676/435 50 10
E-Mail: reg@barga.com
Web: www.barga.com

BAWAG P.S.K. Bank für Arbeit und Wirtschaft u. Österr. Postsparkasse AG S
Seitzergasse 2 - 4
1010 Wien
Tel.: +43-1-534 53 31 272
E-Mail: it-sicherheit@bawagpsk.com
Web: www.bawagpsk.com

BK-DAT Electronics e.U. AS
Hieflauer Straße 18
8790 Eisenerz
Tel.: +43-3848 60048
E-Mail: info@bkdat.net
Web: www.bkdat.net

Brennercom Tirol GmbH ABS
Eduard-Bodem-Gasse 8
6020 Innsbruck
Tel.: +43-512/279 279
E-Mail: christian.braito@brennercom-tirol.at
Web: www.brennercom-tirol.at

Bundesrechenzentrum GmbH AHRS
Hintere Zollamtsstrasse 4
1030 Wien
Tel.: +43-1-711 23 0
E-Mail: office@brz.gv.at
Web: www.brz.gv.at

C

CC I Communications (CCC.at) - Fa. Andrea Seregelyes ACHS
Kaiserbrunnstraße 34
3021 Pressbaum
Tel.: +43-1-50164 0
E-Mail: office@ccc.at
Web: www.ccc.at

Christoph Schmoigl / 3+1 it systems® CH
Erlafstraße 1/5-6
1020 Wien
Tel.: +43-1-710 85 02
E-Mail: christoph.schmoigl@3plus1.at
Web: www.3plus1.at

Cisco Systems Austria GmbH S
Handelskai 94-96
1200 Wien
Tel.: +43-1-24 030 6024
E-Mail: hgreiner@cisco.com
Web: www.cisco.at

Citycom Telekommunikation GmbH ABCHS
Andreas Hofer Platz 15
8010 Graz
Tel.: +43-316 887 0
E-Mail: office@citycom.co.at
Web: www.citycom.co.at

COLT Technologies Services GmbH RS
Kärnter Ring 12
1010 Wien
Tel.: +43-1-20 500-0
E-Mail: klaus.strobl@colt.net
Web: www.colt.net

ComneX - Computer und Netzwerk GmbH ACHS
Sossenstraße 11
2380 Perchtoldsdorf
Tel.: +43-1-86 919 81 0
E-Mail: office@comnex.net
Web: www.comnex.net

Compass-Verlag GmbH CS
Matznergasse 17
1141 Wien
Tel.: +43-1-981 16 0
E-Mail: nikolaus.futter@compass.at
Web: www.compass.at

comteam ACHSW
Mitterfeldstr. 1
3300 Amstetten
Tel.: +43-7472 222 8100
E-Mail: internet@comteam.at
Web: www.comteam.at

CoreTEC IT Security Solutions GmbH CS
Wiedner Hauptstraße 15
1040 Wien
Tel.: +43-1-503 72 73 0
E-Mail: m.kirisits@coretec.at
Web: www.coretec.at

creativ wirtschaft austria S
Wiedner Hauptstraße 63
1045 Wien
Tel.: +43-(0)5 90 900 0
E-Mail: gertraud.leimueller@wko.at
Web: www.creativwirtschaft.at

CSO.Net Internet Services GmbH ACHS
Franzosengraben 10
1030 Wien
Tel.: +43-1-206 30 0
E-Mail: office@cso.net
Web: www.cso.net

CUBiT IT Solutions GmbH. ACH
Zieglergasse 67/3/1 Hoftrakt
1070 Wien
Tel.: +43-1-718 98 80 0
E-Mail: paul.witta@cubit.at
Web: www.cubit.at

CYAN Networks Software GmbH S
Hainburgerstrasse 34
1030 Wien
Tel.: +43-720 555 444 0
E-Mail: klaus.thurnhofer@cyan-networks.com
Web: www.cyan-networks.com

D

dark-green Information Technology GmbH. HS
Brühler Straße 9
2340 Mödling
Tel.: +43-2236/86 01 30 0
E-Mail: markus@dark-green.com
Web: www.dark-green.com

Datenhafen GmbH S
Schwindgasse 4/7
1040 Wien
Tel.: +43-1-503 58 70 42
E-Mail: office@datenhafen.at
Web: www.datenhafen.at

datenwerk innovationsagentur GmbH CH
Hofmühlgasse 3-5
1060 Wien
Tel.: +43-1-585 60 71
E-Mail: office@datenwerk.at
Web: www.datenwerk.at

DIALOG telekom GmbH & Co KG ACS
Goethestrasse 93
4020 Linz
Tel.: +43-732-662 774 0
E-Mail: rpassecker@dialog-telekom.at
Web: www.dialog-telekom.at

DIC-Online & Co. KG ACHRS
Dr.-Stumpf-Strasse 70
6020 Innsbruck
Tel.: +43-512-341033
E-Mail: office@dic.at
Web: www.dic.at

DiTech GmbH CHS
Dresdner Strasse 43
1200 Wien
Tel.: +43-059 555
E-Mail: office@ditech.at
Web: www.ditech.at

domainfactory Telek. GmbH AHS
Parkring 10
1010 Wien
Tel.: +43-0800 311 821
E-Mail: tm@domainfactory.de
Web: www.domainfactory.at

domainname.at - webagentur.at Internet Service GmbH CBHRS
Neustiftg. 2
2500 Baden
Tel.: +43-2252 259 892
E-Mail: office@webagentur.at
Web: www.domainname.at

DREI-BANKEN-EDV Gesellschaft mbH S
Untere Donaulände 28
4020 Linz
Tel.: +43-732 780 22 625
E-Mail: lothar.handl@3beg.at
Web: www.3beg.at

E

echonet communication GmbH C
Schottenfeldgasse 24
1070 Wien
Tel.: +43-1-526 26 76 16
E-Mail: office@echonet.at
Web: www.echonet.at

eCircle GmbH S
Nymphenburger Höfe NY
II, Dachauer Str. 86
D-80335 München
Tel.: +49-89-12 009 600
E-Mail: a.goermer@ecircle.com
Web: www.ecircle.com

EDV-Dienstleistungen Rappaport GmbH & Co. KG S
Geblergasse 95/8
1170 Wien
Tel.: +43-1-906 80 20 10
E-Mail: dominik.rappaport@rappaport.at
Web: www.rappaport.at

EDV-Himmelbauer ACHSW
Kremserstr. 8
2070 Retz
Tel.: +43-2942 20670
E-Mail: jhimmelbauer@edv-himmelbauer.at
Web: www.edv-himmelbauer.at/

EDV-Service Strolz CHWS
Sonnenwiese 10
6580 St. Anton am Arlberg
Tel.: +43-5446 302 49
E-Mail: office@arlberg.com
Web: www.arlberg.com

Elektronische Datenverarbeitung GmbH ACHR
Hofmühlgasse 3-5
1060 Wien
Tel.: +43-1-599 07-0
E-Mail: gernot.nusshall@edvg.at
Web: www.edvg.at

emerion WebHosting GmbH HR
Vienna Twin Tower,
Wienerbergstraße 11/16a
1100 Wien
Tel.: +43-1-29 888 00
E-Mail: office@emerion.com
Web: www.emerion.com

eM-I.T. Michael Gamsjäger ACHWS
Wiesingerstrasse 3/12
4820 Bad Ischl
Tel.: +43-664/851 55 74
E-Mail: office@em-it.at
Web: www.em-it.at

Empirion Telekommunikations Services GmbH ABCHS
Horneckgasse 8, 1170 Wien
Tel.: +43-1-480 5000
E-Mail: office@empirion.at
Web: www.empirion.at

Energie AG Oberösterreich Data GmbH ABS
Böhmerwaldstrasse 3, 4021 Linz
Tel.: +43-059000 3900
E-Mail: manfred.litzl-bauer@energieag.at
Web: www.energieag.at

ERESNET GmbH ACHRS
Mariahilfer Straße 33, 1060 Wien
Tel.: +43-1-58 65 828
E-Mail: info@immobilien.net
Web: www.eres.net

fairytel communications gmbh ACHWS
Trappelgasse 4, 1040 Wien
Tel.: +43-(0)720 345 111
E-Mail: office@fairytel.at
Web: www.fairytel.at

Faxonline GmbH S
Mariahilferstraße 136, 1150 Wien
Tel.: +43-0800 802 102
E-Mail: info@faxonline.at
Web: www.faxonline.at

F-Secure GmbH S
Zielstattstrasse 44
D-81379 München
Tel.: +49-89 787467 0
E-Mail: juergen.schopper@f-secure.com
Web: www.f-secure.com

Futureweb OG HS
Innsbrucker Strasse 4
6380 St. Johann in Tirol
Tel.: +43-5352 65335 0
E-Mail: info@futureweb.at
Web: www.futureweb.at

G

G.Grasl Ges.m.b.H. Druck & Neue Medien CH
Druckhausstrasse 1
2540 Bad Vöslau
Tel.: +43-2252 402 0
E-Mail: w.grasl@grasl.eu
Web: www.grasl.co.at

GEOCOMP Handelsges.m.b.H. A
Salzburgerstraße 1
4840 Vöcklabruck
Tel.: +43-7672-277 770
E-Mail: office@geocomp.at
Web: www.geocomp.at

Gernot Bauer IT Dienstleistungs-GmbH AW
Perbersdorf 14
3364 Neuhofen/Ybbs
Tel.: +43-7475/56 497
E-Mail: office@gernot-bauer.at
Web: www.gernot-bauer.at

GiGaNet.at, Bernhard Kröll A
Rauchenwald 651
6290 Mayrhofen
Tel.: +43-5285 630 850
E-Mail: office@giganet.at
Web: www.giganet.at

GRZ IT Center Linz GmbH AH
Goethestrasse 80, 4020 Linz
Tel.: +43-70 6929 1507
E-Mail: bachleitner@grz.at
Web: www.grz.at

H

HAPPY-FOTO GmbH & Co KG CR
Marcusstraße 8-10
4240 Freistadt
Tel.: +43-7942/76200
E-Mail: sekretariat@happyfoto.at
Web: www.happyfoto.at

HEROLD Business Data GmbH CS
Guntramsdorfer Strasse 105
2340 Mödling
Tel.: +43-2236-401-651
E-Mail: frank.bieser@herold.at
Web: www.herold.at

HostProfis ISP Telekom GmbH AHS
Tirolerstraße 17, 3. Stock
9500 Villach
Tel.: +43-(0)59900 202
E-Mail: oberdorfer@hostprofis.com
Web: www.hostprofis.com

hotze.com GmbH ABH
Eduard-Bodem-Gasse 6
6020 Innsbruck
Tel.: +43-512-353 640
E-Mail: office@hotze.com
Web: www.hotze.com

Hutchison 3G Austria GmbH ACS
Gasometer C Guglgasse 12/10/3
1110 Wien
Tel.: +43-05 0660 0
E-Mail: gerhard.horvath@drei.com
Web: www.drei.at

I

I.M.H. gtld.at registry HS
Seekirchnerstraße 11
5162 Obertrum am See
Tel.: +43-6219-7462
E-Mail: office@gtld.at
Web: www.gTLD.at

i3b Internetbreitbandbetriebs GmbH AB
Viktringer Platz 5, 9073 Viktring
Tel.: +43-676/843 435 301
E-Mail: marco.brands-taetter@i3b.at
Web: www.i3b.at

IBCL Informatik-Büro e.U. HS
Sebastian-Kneipp-Weg 17
6020 Innsbruck
Tel.: +43-680/205 68 23
E-Mail: office@ibcl.at
Web: www.ibcl.at

ICE-Vienna, Verein zur Förderung von Medienaktivitäten im schulischen und außerschulischen Bereich CS
Alserbachstraße 23/2. Stock
1090 Wien
Tel.: +43-664/540 46 81
E-Mail: barbara.novak@spw.at
Web: www.ice-vienna.at

IFO.net Internet Service GmbH ACHS
Impulszentrum Haus KB5
8082 Kirchbach
Tel.: +43-(0)311-621 000
E-Mail: ispa@ifo.net
Web: www.ifo.net

IKARUS Security Software GmbH CS
Blechturmgasse 11, 1050 Wien
Tel.: +43-1-58995
E-Mail: pichlmayr.j@ikarus.at
Web: www.ikarus.at

Infotech EDV-Systeme GmbH ACHSW
Schaerdinger Strasse 35
4910 Ried im Innkreis
Tel.: +43-7752-81711-0
E-Mail: office@infotech.at
Web: www.infotech.at

Innsbrucker Kommunalbetriebe AG ASW
Langer Weg 29
6020 Innsbruck
Tel.: +43-512/502 7290
E-Mail: g.wieser@ikb.at
Web: www.ikb.at

Institut für empirische Sozialforschung (IFES) GmbH C
Teinfaltstraße 8, 1010 Wien
Tel.: +43-1-546 70
E-Mail: wasserbacher@ifes.at
Web: www.ifes.at

Internet Viennaweb Service GmbH H
Pefektastrasse 19/2, 1230 Wien
Tel.: +43-1-956 46 06
E-Mail: office@viennaweb.at
Web: www.viennaweb.at

internic Datenkommunikations GmbH CHS
Schönngasse 15-17 / 8
1020 Wien
Tel.: +43-1-403 96 85
E-Mail: info@internic.at
Web: www.internic.at

Interxion Österreich GmbH ABCHS
Louis-Haefliger-Gasse 10
1210 Wien
Tel.: +43-1-290 36 36 0
E-Mail: vienna.info@interxion.com
Web: www.interxion.com

Invitel International AG BS
Ortsstrasse 24, 2331 Vösendorf
Tel.: +43-1-699 94 08 0
E-Mail: office@mtcag.com
Web: www.invitel-int.com

ipcom GmbH S
Karlsplatz 1
1010 Wien
Tel.: +43-664/144 56 86
E-Mail: office@ipcom.at
Web: www.ipcom.at

iPlace Internet & Network Services GmbH ACHS
Ringstraße 5, 1. Stock
6830 Rankweil
Tel.: +43/5552-20 500
E-Mail: office@iplace.at
Web: www.iplace.at

it & tel (Geschäftsbereich der Elektrizitätswerk Wels AG) A
Bahnhofplatz 4
4600 Wels
Tel.: +43-7242-9396 7100
E-Mail: office@itandtel.at
Web: www.itandtel.at

J

JM-DATA GmbH ABCHS
Am Winterhafen 13
4020 Linz
Tel.: +43-(0)50 / 30 50 80
E-Mail: office@jm-data.at
Web: www.jm-data.at

Josef Edtbauer e.U. - Pyhrn-Priel.TV AHWS
Egger-Weg 9
4582 Spital am Pyhrn
Tel.: +43-7563/21800
E-Mail: office@pptv.at
Web: www.pptv.at

K

KABEL TV AMSTETTEN GMBH AHS
Kruppstraße 3, 3300 Amstetten
Tel.: +43-7472/66667 0
E-Mail: office@ktvam.at
Web: www.ktvam.at

kabelsignal AG AHWRS
Südtstadtzentrum 4
2344 Maria Enzersdorf
Tel.: +43-2236-45564-0
E-Mail: ispa@kabelsignal.at
Web: www.kabelsignal.at

KAPPER NETWORK-COMMUNICATIONS GmbH - kapper.net ABCHRSW
Löblichgasse 6, Top 2G
1090 Wien
Tel.: +43-1-319 55 00 0
E-Mail: info@kapper.net
Web: www.kapper.net

Kapsch BusinessCom AG W
Wienerbergstraße 53, 1121 Wien
Tel.: +43-(0)50-811 0
E-Mail: WebAdmin@kapsch.net
Web: www.kapschbusiness.com

kitznet - Stadtwerke Kitzbühel ACHS
Jochberger Str. 36
6370 Kitzbühel
Tel.: +43-5356-65 651
E-Mail: internet@kitz.net
Web: www.kitz.net

Kriegsauer EDV - Consulting GmbH AHS
Wienerstraße 5/1, 8230 Hartberg
Tel.: +43-3332 62212 70
E-Mail: office@htb.at
Web: www.htb.at

KT-NET Communications GmbH AHWS
Ramingdorf 51
4441 Behamberg
Tel.: +43-7252/778 52
E-Mail: office@kt-net.at
Web: www.kt-net.at

L

LEOX Telekommunikations GmbH ACH
Hauptplatz 3
8700 Leoben
Tel.: +43-3842-477 86 0
E-Mail: office@leox.net
Web: www.leox.net

LexisNexis Verlag ARD Orac GmbH & Co KG CS
Marxergasse 25
1030 Wien
Tel.: +43-1-534 52 1010
E-Mail: ivo.sklenitz-ka@lexisnexis.at
Web: www.lexisnexis.at

Licht- und Kraftvertrieb der Gemeinde Hollenstein/Ybbs AS
Walcherbauer 2
3343 Hollenstein an der Ybbs
Tel.: +43-7445/218 16
E-Mail: lkv@hollenstein.at
Web: www.oganet.at

Linz Strom GmbH ABCHRS
Wiener Straße 151
4021 Linz
Tel.: +43-732 3400 3113
E-Mail: m.past@linzag.at
Web: www.linzag.at

LinzNet Internet Service Provider GmbH ACHSW
Hafenstr. 1-3
4020 Linz
Tel.: +43-732 2360
E-Mail: office@linznet.at
Web: www.linznet.at

LIWEST Kabelmedien GmbH. ARS
Lindengasse 18
4040 Linz
Tel.: +43-732 94 24 24
E-Mail: office@liwest.at
Web: www.liwest.at

M

makeit information systems GmbH HS
Mooslackengasse 17, 1190 Wien
Tel.: +43-1-5137356-0
E-Mail: office@makeit.at
Web: www.makeit.at

MakeNewMedia Communications GmbH ABCHWS
Louis-Häfliger-Gasse 10
1210 Wien
Tel.: +43-1-338 333 0
E-Mail: sales@make-newmedia.com
Web: www.makenewmedia.com

MediaClan - Gesellschaft für Online Medien G.m.b.H. CS
Nestroyplatz 1/1/14a, 1020 Wien
Tel.: +43-1-407 50 60-0
E-Mail: office@mediaclan.at
Web: www.mediaclan.at

Medienwirtschaft Verlags GmbH CS
Walfischgasse 11/ Top 8A
1010 Wien
Tel.: +43-676/848 920 290
E-Mail: martin.staudinger@medienwirtschaft.at
Web: www.medienwirtschaft.at

MELON Informationstechnologie GmbH C
Weyringergasse 13, 1040 Wien
Tel.: +43-1-505 66 10
E-Mail: office@melon.at
Web: www.melon.at

Microsoft Österreich GesmbH. C
Am Euro Platz 3, 1120 Wien
Tel.: +43-1-61064-0
E-Mail: austria@microsoft.com
Web: www.microsoft.com/austria

mieX.at – Mühlviertler Internet Exchange - Thaller - Wagner OG ABCHW
Veldner Str. 29
4120 Neufelden
Tel.: +43(0)5900 8008
E-Mail: office@miex.at
Web: www.miex.at

MMC Kommunikationstechnologie GesmbH ACHRS
Mühlgasse 14/E
2353 Guntramsdorf
Tel.: +43-2236-3903
E-Mail: office@mmc.at
Web: www.mmc.at

molco.at Handels GmbH ACWS
Mischekgasse 3 / Top A
2320 Schwechat
Tel.: +43-2236/378333 31
E-Mail: m.zelinka@molco.at
Web: www.molco.at

MP2 IT-Solutions GmbH HS
Effingergasse 23a, 1160 Wien
Tel.: +43-1-523 55 55
E-Mail: gerlinde.pascher@mp2.at
Web: www.mp2.at

mquadr.at software engineering und consulting GmbH S
Halbgasse 26/TOP 3, 1070 Wien
Tel.: +43-1-505 40 50 744
E-Mail: tkp@mquadr.at
Web: www.mquadr.at

Multikom Austria Telekom GmbH AHWS
Jakob-Haringer-Str. 1
5020 Salzburg
Tel.: +43-(0)59 333 5000
E-Mail: w.flatscher@multikom.at
Web: www.multikom.at

mur.at - Verein zur Förderung von Netzwerkkunst ABCR
Leitnergasse 7a, 8010 Graz
Tel.: +43-316-821451 26
E-Mail: verein@mur.at
Web: www.mur.at

myNET Internet Solutions ABHS
Bruggfeldstraße 5
6500 Landeck
Tel.: +43-676/841 810 300
E-Mail: hh@mynet.at
Web: www.mynet.at

MyServices EDV Dienstleistungen GmbH ACH
Maximilianstraße 8a, 4600 Wels
Tel.: +43-7242/467 81 0
E-Mail: office@myservices.at
Web: www.myservices.at

N

NA-NET Communications GmbH AHWS
Wiedenstrasse 3, 2130 Mistelbach
Tel.: +43-2572-20 233 0
E-Mail: office@nanet.at
Web: www.nanet.at

nemox.net ABCHRS
Eduard-Bodem-Gasse 9
6020 Innsbruck
Tel.: +43-5 0234-0
E-Mail: info@nemox.net
Web: www.nemox.net

NeoTel Telefonservice GmbH & Co KG S
Esterhazygasse 18a/15
1060 Wien
Tel.: +43-1-409 41 81 0
E-Mail: office@neotel.at
Web: www.neotel.at

NESSUS Internet Dienstleistungs GmbH CHS
Fernkorngasse 10/A/2/101
1010 Wien
Tel.: +43-720/002828
E-Mail: fs@nessus.at
Web: www.nessus.at

Net4You Internet GmbH ABCHS
Tiroler Straße 80, 9500 Villach
Tel.: +43-4242-50 0 5
E-Mail: office@net4you.net
Web: www.net4you.net

NetMan Network Management und IT-Services GmbH ACHS
Lindengasse 43/19, 1070 Wien
Tel.: +43-1-253 6000
E-Mail: michael.lichtenegger@net-man.at
Web: www.net-man.at

netservice dienstleistung gmbh HS
Erzherzog Johann Gasse 18
8741 Weißkirchen
Tel.: +43-3577-811 80 0
E-Mail: office@netservice.at
Web: www.netservice.at

Netvisual OG ACHS
Louis-Häfliger-Gasse 10, 1210 Wien
Tel.: +43-(0)50 955
E-Mail: office@netvisual.tv
Web: www.netvisual.tv

next layer Telekommunikationsdienstleistungs- und BeratungsGmbH ABHS
Mariahilfer Gürtel 37/7, 1150 Wien
Tel.: +43-(0)5 1764 0
E-Mail: office@nextlayer.at
Web: www.nextlayer.at

NextiraOne Austria GmbH AS
Kommunikationsplatz 1, 1210 Wien
Tel.: +43-0577 33 4658
E-Mail: wolfgang.leindecker@nextiraone.at
Web: www.nextiraone.at

nfon GmbH ACHS
Schillerplatz 1, 3100 St. Pölten
Tel.: +43-2742/75566
E-Mail: office.at@nfon.net
Web: www.nfon.at

nökom ABCHWFS
EVN Platz, 2344 Maria Enzersdorf
Tel.: +43-2236 200 50301
E-Mail: office@noekom.at
Web: www.noekom.at

O

ÖBB Telekom Service GmbH - Profinet Services ABCHRS
Brünnerstraße 20, 210 Wien
Tel.: +43-1-93000-39000
E-Mail: office@oebbtel.at
Web: www.oebbtel.at

Ocilion IPTV Technologies GmbH CS
Schaerdinger Strasse 35
4910 Ried im Innkreis
Tel.: +43-7752/2144 0
E-Mail: office@ocilion.com
Web: www.ocilion.com

OeKB - Oesterreichische Kontrollbank AG CH
Am Hof 4, Postfach 70, 1011 Wien
Tel.: +43-1-531 27-2175
E-Mail: ewald.jenisch@oekb.at
Web: www.oekb.co.at

ÖIAT - Österreichisches Institut für angewandte Telekommunikation CS
Margaretenstraße 70/2/4
1050 Wien
Tel.: +43-1-595 21 12 13
E-Mail: office@oiat.at
Web: www.oiat.at

OmanBros.com Internetdienstleistungen GmbH ACHS
Guglgasse 8/2/85
1110 Wien
Tel.: +43-1-969 03 04 0
E-Mail: office@omanbros.com
Web: www.omanbros.com

OÖ. Ferngas Service GmbH AB
Neubauzeile 99
4030 Linz
Tel.: +43-732-3883 367
E-Mail: christian.schmidt@ooefg.co.at
Web: www.ooeferngas-servicegmbh.at

OÖ. Tourismus Technologie GmbH CHS
Freistädter Straße 119
4041 Linz
Tel.: +43-732-7277 312
E-Mail: wolfgang.erlebach@ttg.at
Web: www.ttg.at

optivo GmbH S
Wallstrasse 16
D-10179 Berlin
Tel.: +49-(0)30/76 80 78 0
E-Mail: joeran.nemitz@optivo.de
Web: www.optivo.de

Orange Austria Telecommunication GmbH S
Brünnerstraße 52
1210 Wien
Tel.: +43-1-27728 0
E-Mail: robert.koenig@orange.co.at
Web: www.orange.at

ORF Online und Teletext GmbH & Co KG CS
Heiligenstädter Lände 27c
1190 Wien
Tel.: +43-1-87878 0
E-Mail: online@orf.at
Web: www.orf.at

P

Peter Ostry e.U. CHS
Linzerstraße 95/5
1140 Wien
Tel.: +43-1-877 74 54-0
E-Mail: service@ostry.com
Web: www.ostry.com

PGV Computer Handels GmbH & CoKG AHS
Kremser Landstrasse 34
3100 St. Pölten
Tel.: +43-2742-366301
E-Mail: online@pgv.at
Web: www.pgv.at

PLAY.FM GmbH C
Brunnengasse 51/15
1160 Wien
E-Mail: office@play.fm
Web: www.play.fm

Prager Consult EDV & Technologie Dienstleitungen HS
Schönbrunner Str. 5
1040 Wien
Tel.: +43-1-586 9031 20
E-Mail: prager@prager.at
Web: www.prager.at

Preisvergleich Internet Services AG CHS
Obere Donaustraße 63/2
1020 Wien
Tel.: +43-1-581 1609
E-Mail: mjy@geizhals.at
Web: www.geizhals.at

Q

quintessenz W
c/o Quartier 21, Museumsquartier,
Museumsplatz 1-4
1010 Wien
E-Mail: office@quintessenz.org
Web: www.quintessenz.org

R

Raiffeisen Datennetz GmbH. AS
Jacquingasse 47, 1030 Wien
Tel.: +43-(0)5 999 31888-12
E-Mail: peter.schmid@rdg.raiffeisen.at
Web: www.rdg.at

Raiffeisen Informatik GmbH ACH
Lilienbrunngasse 7 - 9, 1020 Wien
Tel.: +43-1-99 3 99 0
E-Mail: info@r-it.at
Web: www.r-it.at

RIS GmbH ACHS
Ing. Kaplangasse 1, 4400 Steyr
Tel.: +43-7252-86186-0
E-Mail: info@ris.at
Web: www.ris.at

S

s IT Solutions AT Spardat GmbH ACHRS
Geiselbergstraße 21 - 25
1110 Wien
Tel.: +43-(0)5100 39637
E-Mail: horst.ganster@s-itsolutions.at
Web: www.s-itsolutions.com

Salzburg AG für Energie, Verkehr und Telekommunikation ABCW
Bayerhamerstr. 16, 5020 Salzburg
Tel.: +43-662-8884-2781
E-Mail: herbert.stranzinger@salzburg-ag.at
Web: www.salzburg-ag.at

SC-Networks GmbH CS
Enzianstr. 2, D-82319 Starnberg
Tel.: +49-8151/555 160
E-Mail: info@sc-networks.com
Web: www.sc-networks.com

SILVER SERVER GmbH ABHRS
Lorenz Mandl Gasse 33/1
1160 Wien
Tel.: +43-(0)59944
E-Mail: office@sil.at
Web: www.sil.at

SIPit Kommunikationsmanagement GmbH ACS
Scherzergasse 12/1
1020 Wien
Tel.: +43-1-342 342
E-Mail: office@sipit.at
Web: www.sipit.at

sourceheads Information Technology GmbH C
Palmgasse 10
1150 Wien
Tel.: +43-1-917 417 0
E-Mail: info@sourceheads.com
Web: www.sourceheads.com

SPÖ Informationstechnologiezentrum (CRS)
Windmühlgasse 26
1060 Wien
Tel.: +43-1-534 27 283
E-Mail: office@itz.spoe.at
Web: www.spoe.at

d r f u n

Farmer Brown, Network Administrator

Sprint International Austria GmbH ABS
Schottenring 16
1010 Wien
Tel.: +43-1-537 12 4167
E-Mail: alexander.valenta@sprint.com
Web: www.sprintworldwide.com

Stadtwerke Feldkirch ABH
Leusbündtweg 49
6800 Feldkirch
Tel.: +43-5522 9000
E-Mail: kundencenter@stadtwerke-feldkirch.at
Web: www.stadtwerke-feldkirch.at

Stadtwerke Hall in Tirol GmbH AHS
Augasse 6
6060 Hall in Tirol
Tel.: +43-5223/5855 190
E-Mail: d.heiss@hall.ag
Web: www.hall.ag

Stadtwerke Kapfenberg GmbH AHS
Stadtwerkestraße 6
8605 Kapfenberg
Tel.: +43-3862-23 516 0
E-Mail: ispa@hiway.at
Web: www.hiway.at

Stadtwerke Klagenfurt Aktiengesellschaft AS
St. Veiter Straße 31
9020 Klagenfurt
Tel.: +43-463/521-600
E-Mail: reinhold.luschin@stw.at
Web: www.stw.at

Stadtwerke Kufstein GmbH ACHW
Fischergries 2, 6330 Kufstein
Tel.: +43-5372-693 03 23
E-Mail: schuster@stwk.at
Web: www.kufnet.at

Stadtwerke Wörgl Ges.m.b.H. AHW
Zauberwinklweg 2a
6300 Wörgl
Tel.: +43-5332-72566 303
E-Mail: steinwender@stadtwerke.woergl.at
Web: www.stadtwerke.woergl.at

Streams Telecommunications GesmbH ACHS
Universitätsstrasse 10/7
1090 Wien
Tel.: +43-1-401 59 128
E-Mail: office@streams.at
Web: www.streams.at

StuOnline Internet Service ACHS
Neuhofweg 8
9560 Feldkirchen
Tel.: +43-4276 5121 0
E-Mail: info@stuonline.at
Web: www.stuonline.at

Symantec GmbH S
Wipplingerstr. 34
1010 Wien
Tel.: +43-1-532 85 33 0
E-Mail: ernst_eisner@symantec.com
Web: www.symantec.at

SysUP OG CHS
Zanklstrasse 22
8051 Graz
Tel.: +43-316/22 8888 0
E-Mail: office@sysup.at
Web: www.sysup.at

Tele2 Telecommunication GmbH ABCHRS
Donau City Straße 11
1220 Wien
Tel.: +43-50500-8310
E-Mail: andreas.koman@tele2.com
Web: www.tele2.at

T

Telecom Europe SAT GmbH ABCHWS
Jüptnergasse 17
1190 Wien
Tel.: +43-664/225 25 14
E-Mail: office@eurosat.ag
Web: www.eurosat.ag

Telekurier Online Medien GmbH & CoKG CR
Lindengasse 52, 1070 Wien
Tel.: +43-1-52100 2208
E-Mail: ronald.schwaerzler@kurier.at
Web: www.kurier.at

TeleMax Internet Service ACHS
Sandgasse 26
6923 Lauterach
Tel.: +43-5574-79489
E-Mail: office@telemax.at
Web: www.telemax.at

Teleport Consulting und Systemmanagement Ges.m.b.H. ACHRSW
Gutenbergstaße 1
6858 Schwarzach
Tel.: +43-5572-501-735
E-Mail: webmaster@vol.at
Web: www.vol.at

TeliaSonera International Carrier Austria GmbH B
Schlosshoferstraße 4/4/22
1210 Wien
Tel.: +43-1-205 305 17
E-Mail: eva.haager@teliasonera.com
Web: www.teliasoneraic.com

Thomas Dorn, Xi-Development CHRS
Kerpengasse 69
1210 Wien
Tel.: +43-1-271 45 50
E-Mail: thomas@dorn.at
Web: www.dorn.at

Tinet GmbH AB
Hugenottenallee 167
D-63263 Neu-Isenburg
Tel.: +49-6102 823 5391
E-Mail: joerg.hartmann@tinet.net
Web: www.tiscali.net

TIWAG-Tiroler Wasserkraft AG, Bereich IT B
Eduard-Wallnöfer-Platz 2
6020 Innsbruck
Tel.: +43 (0)50607 0
E-Mail: bit-tk-abwicklung@tiwag.at
Web: www.tiroler-wasserkraft.at

T-Mobile Austria GmbH ACRSW
Rennweg 97-99
1030 Wien
Tel.: +43-1-79585 0
E-Mail: ispa@t-mobile.at
Web: www.t-mobile.at

TMS IT-Dienst CHRS
Hinterstadt 2
4840 Vöcklabruck
Tel.: +43-720 501 078
E-Mail: office@tms-itdienst.at
Web: www.tms-itdienst.at

Tripple Internet Content Services ACHRS
Florianigasse 54/2-5
1080 Wien
Tel.: +43-1-406 59 27 -0
E-Mail: office@tripple.at
Web: www.tripple.at

U

upstreamNet Communications GmbH BH
Lilienbrunngasse 7-9/3. OG
1020 Wien
Tel.: +43-1-212 86 44-0
E-Mail: office@upstreamnet.at
Web: www.upstreamnet.at

V

Verein servus.at - Kunst & Kultur im Netz AC
Kirchengasse 4
4040 Linz
Tel.: +43-732-731-300
E-Mail: office@servus.at
Web: www.servus.at

Verizon Austria GmbH ABH
Handelskai 340, 1023 Wien
Tel.: +43-1-727 14 0
E-Mail: alexander.fantl@at.verizonbusiness.com
Web: www.verizonbusiness.com/at/

VIM Internetdienstleistungen GmbH ACHS
Kärntnerstr. 17/13, 1010 Wien
Tel.: +43-1-7260 200
E-Mail: office@vim.at
Web: www.vim.at

virtual-business CHS
Hoelzelgasse 8, 1230 Wien
Tel.: +43-1-602 21 86 0
E-Mail: office@vibu.at
Web: www.vibu.at

vivomondo GmbH CHS
KR Martin Pichler-Str. 1
6300 Wörgl
Tel.: +43-6991/782 62 99
E-Mail: arno.abler@vivomondo.com
Web: www.vivomondo.com

web-crossing GmbH CHS
Eduard-Bodem-Gasse 8
6020 Innsbruck
Tel.: +43-512-20 65 67
E-Mail: info@web-crossing.com
Web: www.web-crossing.com

WEB-TECH COACHING CS
Siebeneichengasse 2
1150 Wien
Tel.: +43-1-492 51 63
E-Mail: info@web-tech.at
Web: www.web-tech.at

Wien Energie GmbH A
Thomas-Klestil-Platz 14
1030 Wien
Tel.: +43-1-4004 82000
E-Mail: christian.reim@wienenergie.at
Web: www.wienenegie.at

Wiener Zeitung GmbH C
Wiedner Gürtel 10, 1040 Wien
Tel.: +43-1-206 99 290
E-Mail: k.schiessl@wienerzeitung.at
Web: www.wienerzeitung.at

Wingsoft HS
Lanzendorfer Str. 45
2481 Achau
Tel.: +43-664/102 99 91
E-Mail: wilhelm.holzgruber@wingsoft.at
Web: www.wingsoft.at

WNT Telecommunication GmbH ABCHS
Haydngasse 17
1060 Wien
Tel.: +43-1-616 30 90
E-Mail: office@wnt-telecom.net
Web: www.wnt.at

World4You Internet Services GmbH HR
Hafenstrasse 47-51
4020 Linz
Tel.: +43-7227-20665 30
E-Mail: office@world4you.com
Web: www.world4you.com

WVNET Informations und Kommunikations GmbH ACHSW
Edelhof 3
3910 Zwettl
Tel.: +43-2822-53633 0
E-Mail: sales@wvnet.at
Web: www.wvnet.at

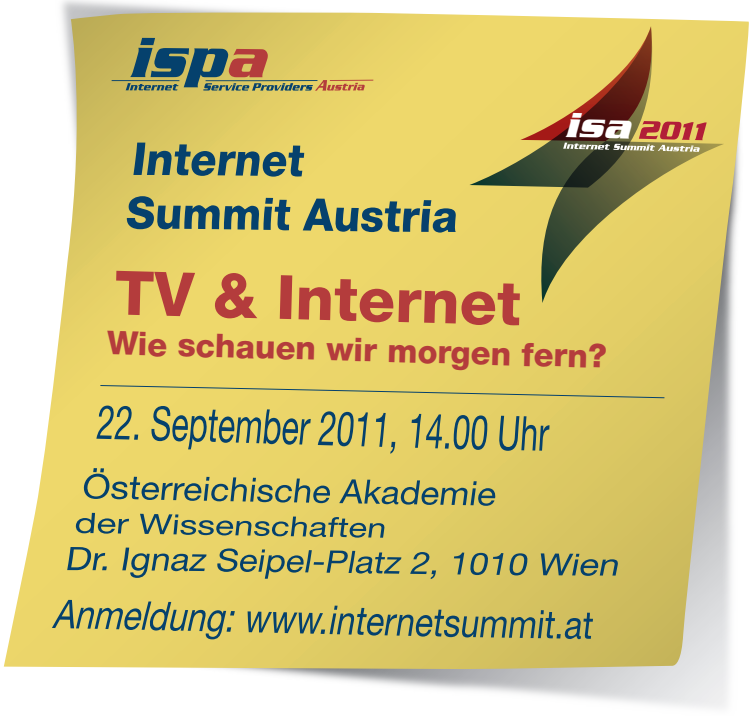
www.funknetz.at GmbH AHSW
Viktor Kaplan Straße 9b
2201 Gerasdorf
Tel.: +43-1-292 96 99 0
E-Mail: m.urbanek@funknetz.at
Web: www.funknetz.at

X

XQueue GmbH S
Christian-Pleß-Str. 11-13
D-63069 Offenbach am Main
Tel.: +49-69-83008980
E-Mail: frank.strzyzewski@xqueue.com
Web: www.xqueue.de

yasp.at HS
Fabrikstr. 8
4020 Linz
Tel.: +43-676/733 93 33
E-Mail: office@yasp.at
Web: www.yasp.at

ispa


ispa
Internet Service Providers Austria
isa 2011
Internet Summit Austria
Internet
Summit Austria
TV & Internet
Wie schauen wir morgen fern?
22. September 2011, 14.00 Uhr
Österreichische Akademie
der Wissenschaften
Dr. Ignaz Seipel-Platz 2, 1010 Wien
Anmeldung: www.internetsummit.at