

## **MEDIENINFORMATION**

Zürich, 23. November 2000

at rete ag führt Informationsveranstaltung durch über „Identität und e-Business: Warum findet PKI nicht statt“ im Widder Hotel in Zürich:

### **Public Key Infrastructures: Der E-Business-Handschlag**

**Verbindlichkeit ist die Voraussetzung zur Ausschöpfung des Potenzials im E-Business. Die Sicherstellung von Identität, Integrität, Authentizität und Vertraulichkeit der Daten resp. der Datenverfasser ist für alle Teilnehmer von Interesse. Public Key Infrastructures (PKI) schaffen diese Verbindlichkeit. Trotzdem harzt es bei ihrer Implementation. Schliesslich bestehen bereits bewährte Alternativen. Anlässlich der siebten at rete-Veranstaltung zu Entwicklungen der E-Economy verfolgen und diskutieren über 100 Netzwerk- und Telecom-Verantwortliche aus allen Branchen Fragestellungen rund um das Thema PKI.**

Dem E-Business gehört die Zukunft. Darüber herrscht Einigkeit. Die dank Internet sichergestellte weltweite Verfügbarkeit und die geringen Transaktionskosten ändern das Geschäftsverhalten im privaten sowie im geschäftlichen Umgang. Die eröffneten Chancen stehen im Widerspruch zu vielen Ängsten, welche das E-Business ebenfalls mit sich bringt. Die Hauptbefürchtungen liegen nach wie vor bei der scheinbar fehlenden Sicherheit und somit am mangelnden Vertrauen. PKI, Public Key Infrastructures, bieten eine Möglichkeit, bestehende Vorbehalte zu entschärfen. „Auch im virtuellen Raum werden Geschäfte zwischen Menschen abgeschlossen. In der realen Welt sehe ich meinen Geschäftspartner, ich kann ihn hören und riechen. Ich interpretiere unbewusst seine Körpersprache und bilde mir anhand des Gesamtbildes eine Meinung über seine Vertrauenswürdigkeit. Instanzen helfen mir dabei, ihn auf seine geschäftliche Integrität zu überprüfen. Wenn trotz allem etwas aus den Fugen gerät, kann ich den rechtlichen Weg beschreiten. Im E-Business fällt vieles weg. Also brauche ich eine Möglichkeit, welche mir Sicherheit und Vertrauen vermittelt. PKI ist eine davon.“ Mit dieser Aussage begrüsst Markus Schaad, Chief Executive Officer der at rete ag, rund 100 Gäste im Widder Saal in Zürich.

### **PKI ist die komplexeste Form von Verbindlichkeit**

Public Key Infrastructures sind eine Kombination von Software, Verschlüsselungstechnologien und Services, welche die sichere Geschäftskommunikation und Datentransaktion ermöglichen. Sie helfen bei der Bereitstellung und Verwaltung von Zertifikaten und kryptographischen Schlüsseln. PKI haben den Vorteil, dass sie sämtliche Verbindlichkeitskriterien in einem Aufwisch erfüllen. Daten werden verschlüsselt, jede Veränderung ist nachvollziehbar, Sender und Empfänger sind eindeutig nachweisbar und schliesslich bietet die digitale Signatur Rechtssicherheit im virtuellen Raum. Die Schwierigkeit besteht darin, dass PKI nicht einfach implementiert werden kann. Zuvor

muss sich ein Unternehmen vielen Fragen stellen, welche oftmals zu einer aufwändigen und teuren Untersuchung führen. Wenn der Aufwand nicht mehr im Verhältnis zum Wert der zu schützenden Information steht, werden oft Insellösungen einer Gesamtlösung vorgezogen. Shared Secret oder Diffie-Hellman-Algorithmus für die Vertraulichkeit, Hash Codes und Fingerprints für die Integrität, Passwörter und Tokens für die Authentizität sowie Logging für die Verbindlichkeit. Der Nutzen von PKI scheint auf den ersten Blick den Aufwand oft nicht zu rechtfertigen.

### **Welchen Nutzen hat PKI und wem nützt es wirklich**

PKI bringen dann einen Nutzen, wenn möglichst viele Anwendungen wie E-Mail, Virtual Private Networks, Single Sign On usw. im Konzept integriert werden. Es steht fest, PKI kann nicht alle technischen Sicherheitsprobleme lösen. PKI muss im Einklang zu allen weiteren Sicherheitsvorkehrungen stehen. Diese sind die physische Sicherheit, die Netzwerkabschottung durch Firewalls, der Virenschutz und beinhalten auch das Erkennen von Sicherheitsverletzungen. Das schwächste Glied in der PKI-Kette dürfte wie immer bei Security-Fragen der Mensch sein. Die Public Key Infrastructure basiert letztlich auf der Eigenverantwortung der Benutzer. Schulung und Support gehören deshalb zu den gewichtigsten Budgetposten bei der Implementation einer PKI-Lösung. Für Unternehmen, deren Marktwert direkt von Sicherheit und Vertrauen abhängt, typischerweise Finanzdienstleister, führt kein Weg an Public Key Infrastructures vorbei. Und schliesslich können PKI massgeblich dazu beitragen, dass die emotionalen Vorbehalte gegenüber dem E-Business überwunden werden. Dann wird aus dem E-Business endlich, was es schon lange verspricht: ein rentables Geschäft.

at rete ag, Zürich, erbringt professionelle Dienstleistungen an der Infrastruktur für erfolgreiche E-Business-Tätigkeiten. Die Professional Services umfassen die Bereiche Engineering mit Fokus auf Design und Redesign der Netzwerke, unter Berücksichtigung von Sicherheit, Skalierbarkeit, Verfügbarkeit und Stabilität. Zudem begleitet und berät das Unternehmen seine Kunden bei der Evaluation für Technologien und Lieferanten oder übernimmt die entsprechende Verhandlungsführung. Konfiguration, Implementation und Betrieb der gewählten Lösungen, Markt- und Kostenanalysen, Prozess- und Organisationsberatung sowie Projektmanagement- und -leitungsaufgaben runden das Serviceangebot ab. Mit rund 45 Mitarbeiterinnen und Mitarbeitern gehört das Zürcher Unternehmen in der Schweiz zu den führenden Anbietern auf diesem Gebiet.

\*\*\*\*\*

### **Weitere Informationen:**

Johnny Strebel, Head of Security Services, Tel. 01 266 55 55 // Fax: 01 266 55 88  
info@atrete.ch