

Austrian Security Forum stellt die TechConsult Multiclient-Studie »IT-Security in Österreich 2008« vor

Das Austrian Security Forum (ASF), eine Vereinigung der führenden IT-Sicherheitsdienstleister in Österreich hat die, vom Beratungsunternehmen TechConsult durchgeführte Studie initiiert, da zum Thema IT-Security und Informationssicherheit in den letzten Jahren keine relevanten Datenerhebungen in Österreich erfolgt sind, erklärt Peter Latzenhofer, Präsident des ASF im Rahmen eines Events in am 3. April in der Vereinigung Österreichischer Industrieller.

Die Studie informiert über den Status quo im IT-Security-Markt für Österreich. Im Rahmen der Erhebung wurden neue Erkenntnisse zu Technologie-Trends und IT-Strategien gewonnen. Weiters beantwortet die Studie, welches die zukünftigen Anforderungen an Hersteller und Dienstleister im Feld von IT-Sicherheit sind.

Methodik der Untersuchung waren telefonische Interviews mit CIOs und IT-Entscheidern in österreichischen Anwenderunternehmen. 100 Unternehmen ab 250 Mitarbeitern wurden branchenübergreifend befragt. Für TechConsult sprach Peter Lohner, der Österreichrepräsentant.

Die Kernaussagen der Studie kurz zusammengefasst:

- Datenschutz und die Datensicherheit gehören in Österreich zu einem der wichtigsten Aufgabengebiete der internen IT-Abteilungen.
- Wenn kein dediziertes Security-Team im Unternehmen besteht, ist die IT-Abteilung mit den Security-Aufgaben betraut. Jährlich bringt diese etwa 30% ihrer Arbeitszeit (bei einer Referenz von 200 Manntagen im Jahr) für Aufgaben der IT-Sicherheit auf.

- Verstärkt ist es immer mehr die Geschäftsführung die als Initiator für neue Security-Projekte gilt.
- Waren es etwa in einer älteren Untersuchung der TechConsult in 2004 gerade ein Drittel der Betriebe, die bereits schriftlich fixierte Richtlinien für die IT-Sicherheit formuliert und eingeführt hatten, haben österreichische Unternehmen heute bereits zu fast drei Vierteln IT-Security-Richtlinien schriftlich fixiert und 16% planen die Einführung in naher Zukunft.
- Der Einsatzgrad dezidiert mobiler IT-Sicherheitsrichtlinien liegt weit niedriger als der der allgemeinen IT-Security Policies – in der Gesamtbetrachtung sind es 49% gegenüber 72%. Dennoch ist Österreich hier eine Vorbildrolle zuzusprechen, da das Thema Mobile Security im europäischen Vergleich schon expliziter adressiert wird.
- Noch immer wird Malicious Code wie Viren, Trojaner, Würmer etc. als die größte Bedrohung für Anwender angesehen. Wichtige neue Sicherheitsfragen ergeben sich speziell für die Mittelständler ab 500 Mitarbeiter durch die Nutzung mobiler Endgeräte.
- Die häufigste wirklich eingetretene Schadensart ist jedoch der Verlust von Daten. Fast die Hälfte der Befragten hat diesbezüglich Erfahrungen machen müssen. Neben dem Datenschutz bleibt somit die Datensicherheit, also die Verfügbarkeit bzw. die Wiederherstellung von Daten oberste Priorität.
- Die drei wichtigsten Themen der Zukunft sind Mobile Security – ein zunehmender Teil des Datenverlustes steht im Zusammenhang mit dem Verlust mobiler

Endgeräte -, E-Mail-Security zur Absicherung gegen Schadcode und Phishing sowie Identity Management, um einen zielgerichteten und bewussten Umgang mit Identitäten innerhalb des Unternehmens sowie angebundener Einheiten und mit Zugriffsrechten Dazu Peter Rogy, schoeller network control: »Die 3 identifizierten Hauptthemen der IT-Sicherheit Mobile-Security, E-Mail-Security sowie Identity Management decken sich mit den Trends und Erfahrungen die schoeller network control auf dem Markt beobachten kann. In allen drei Teilbereichen kann das Unternehmen schoeller network control Erfahrungen in die Diskussion mit dem Kunden einbringen und Lösungen für den Kunden anbieten.«

- Die Spanne des Anteils am IT-Budget, der für IT-Security ausgegeben wird, erstreckt sich von unter 1 % bis über 15 %. Der Mittelwert liegt bei 12 %. Die Ausgabe umfassen sowohl Ausgaben für Datenschutz wie für Datensicherheit. 60 % der Unternehmen wendet über 10 % des IT-Budgets für IT-Security auf. 31 % sogar über 15 %.
- Insgesamt werden Österreichische Unternehmen mit mehr als 250 Mitarbeitern in 2008 ca. 475 Mio. € für IT-Security ausgeben.
- Da die Unternehmen mit den größer wachsenden absoluten Budgets den Markt überproportional beeinflussen, lässt sich ein Wachstum von 16 % errechnen, so dass 2009 ein Marktvolumen von 551 Mio. € zu erwarten ist.

Dazu Hans Jörg Pollirer von Securdata:

»Die KMUs sind das Rückgrat – im IT-Jargon würde man sagen, das »Backbone« – der österreichischen Wirtschaft. Von den insgesamt rund 350.000 österreichischen Unternehmen fallen 99,6 % unter den europäischen KMU-Begriff. 261.000 österreichische Unternehmen beschäftigen weniger als 10 Mitarbeiter. Sie beschäftigen aber ca. 2 Mio. Mitarbeiter (ca 65 %) und erwirtschaften 56 % der gesamten Wertschöpfung.

Angesichts der Bedeutung der KMUs für die österreichische Wirtschaft erhebt sich die Frage, wie es um die IT-Security bei dieser Unternehmensgruppe bestellt ist. Die Antwort auf diese Frage lautet schlicht und einfach: »schlecht«! Bei den meisten KMUs herrscht Unklarheit

darüber, welches Risiko etwa Hackerangriffe, Virenschäden oder Serverausfälle für ihren Betrieb darstellen. Während es für die KMUs selbstverständlich ist, z. B ihr Lager abzusperren, vernachlässigen die meisten die Frage der IT-Security und setzen sich damit unnötig existentiellen Gefahren aus. Und dass es Gefahren gibt und diese im Steigen begriffen sind, zeigen die verschiedensten Sicherheitsstudien internationaler und nationaler Herkunft ganz deutlich auf.«

Über das ASF:

Das Austrian Security Forum wurde im Februar 2002 durch eine gemeinsame Initiative der Firma Beko und Computer Associates gegründet.

Als Partner konnten in der Folge Cisco Systems, Colt, Novell, RSA Security, Siemens, Schoeller Network Control, und der Fachverband Unternehmensberatung & Informationstechnologie der Wirtschaftskammer Österreich sowie die Computerwelt gewonnen werden.

Ziele des »Austria Security Forum« sind die Zusammenarbeit bei der Definition von Standards, Regeln und Normen, die Sammlung und Weitergabe von Wissen, ein gemeinsames Auftreten gegenüber dem Kundenmarkt und Organisationen sowie die bereichsübergreifende Bearbeitung von Projekten. Von allen Partnern werde IT-Security als ganzheitlicher Prozess definiert, um bei steigendem Kostendruck und neuen Bedrohungen die Sicherheit von Daten, Anwendungen und Infrastruktur zu gewährleisten.

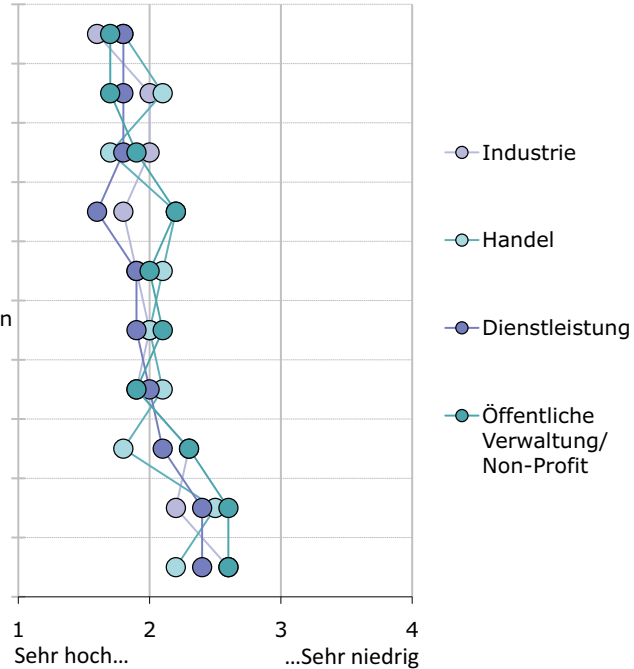
Kontakt:

Austrian Security Forum
p.A: CON•ECT Eventmanagement
Mag. Bettina Hainschink
1070 Wien, Kaiserstraße 14/2
Tel: (01) 522 36 36 - 11
office@conect.at
www.conect.at

Grafiken siehe Beilage

Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) ein?

- Virenbefall/"Malicious Code"
- Neue Sicherheitsfragen durch Nutzung drahtloser Technologien
- Neue Sicherheitsfragen durch Nutzung mobiler Endgeräte
- Missbrauch von Benutzerrechten durch eigene Mitarbeiter – „Innentäter“
- Unautorisiertes Eindringen durch Dritte (Hacker, Wettbewerber)
- Manipulation/Offenlegung von Transaktionen (Web/Email)
- Neue Sicherheitsfragen durch Nutzung von Web Services
- Distributed-Denial-of-Service-Attacken (DDoS)
- Physischer Einbruch/Diebstahl von HW
- Verbreitung illegaler oder „politisch unkorrekter“ Inhalte im Unternehmensnetzwerk



Welche Herausforderungen sehen Sie im Zusammenhang mit dem Thema IT-Security für die Unternehmen Ihrer Branche in den nächsten Jahren?

