## AUFSTEIGER UND UMSTEIGER DES MONATS

**MANFRED TROGER** | MATURITY
Der langjährige Geschäftsführer von Gartner Österreich, Manfred Troger, ist zum IT-Benchmarking- und Beratungsunternehmen Maturity gewechselt. Von Wien aus betreut er das Management mittlerer und großer Unternehmen der CEE-Region in strategischen und persönlichen Fragen.

**CHRISTIAN TRESCHAN** | VIEWSONIC
Christian Treschan ist neuer Account Manager Reseller bei ViewSonic. Zuvor war er bei BenQ, Asus und MAXDATA tätig. Er hat in den letzten Jahren bei BenQ wesentlich den Aufbau des Friends-Partnerprogramms entwickelt sowie als Key Account Manager die Distribution mit verantwortet.

**SPOMENKA SKVORC** | TECHNOGOUP
Als neue Bereichsleiterin verantwortet Spomenka Skvorc den Personal- und Kommunikationsbereich in der Hochheimer Unternehmenszentrale des IT-Dienstleisters Technogroup. Mit ihrem Team ist die diplomierte Betriebswirtin zuständig für operative und strategische Themen ihres Fachbereiches.

**KURT BEICHL** | DOLPHIN TECHNOLOGIES
Kurt Beichl verstärkt das Team des Wiener Technologie-Unternehmens Dolphin Technologies. Dabei übernimmt er als Chief Commercial Officer die kommerzielle Gesamtverantwortung der Vertriebsaktivitäten. Beichl hat langjährige internationale Erfahrung im Software- und Technologievertrieb.

**PETER VOITH** | ATOS ÖSTERREICH
Peter Voith hat die Verantwortung als Leiter des Bereichs Consulting & System Integration (C&SI) bei Atos Österreich übernommen. In dieser Position berichtet er an Martin Endres, Head of C&SI CEE, und Johann Martin Schachner, Country Manager Atos Österreich.

**YOGESH GUPTA** | PROGRESS
Progress hat den Software-Veteranen Yogesh Gupta zum neuen CEO ernannt. Der bisherige CEO Phil Pead zieht sich von seinem Posten zurück, bleibt aber als Mitglied des Progress Board of Directors weiterhin für das Unternehmen tätig.

**ANNA GATTI** | UPC
Anna Gatti, bisher Managing Director Customer Experience beim Mutterkonzern Liberty Global, wird ab 1. Dezember Mitglied des UPC Managements und neue Chief Marketing, Products und Digital Officer. Gatti folgt auf Ivo Hoevel, der mit Ende des Jahres das Unternehmen verlassen wird.

**OLIVER KEIZERS** | FIDELIS
Oliver Keizers hat in Zukunft bei Fidelis Cybersecurity im deutschsprachigen Raum die Zügel in der Hand. Keizers verfügt über mehr als 20 Jahre IT-Erfahrung. Vor seiner Tätigkeit für Fidelis Cybersecurity war Oliver Keizers unter anderem für Blue Coat, SailPoint, NetiQ und Quest tätig.

**... MEHR AUF COMPUTERWELT.AT**

# CYBERVORFÄLLE RICHTIG KOMMUNIZIEREN

Kein Business ist immun gegen Datenlecks und Cyberattacken.

Alexander Kleedorfer ist Berater im Wiener Büro der Brunswick Group.

Drei einfache Fragen genügen, um das Potenzial für einen Hackerangriff auf ein Unternehmen zu bestimmen: Verwenden Sie Computer? Benützen Sie das Internet? Erzeugen oder verarbeiten Sie Daten?

### HACKER VISIEREN IMMER MEHR IT-FERNE SEKTOREN AN

So gesehen betrifft Cybersecurity alle. Jene Wirtschaftszweige, die bisher von Hackerangriffen verschont wurden, sind ob der vermeintlichen Sicherheit einem erhöhten Risiko ausgesetzt. Wer würde beispielsweise Immobilien für ein lohnendes Hackerziel halten? Im Falle eines Hacks könnten bei vernetzten Objekten die Sprinkler aktiviert und Heizungen ausgeschaltet werden, enorme Schäden an Gebäudeeinrichtung- oder Ausstattung wären die Folge. Daher investieren Immobilienfonds derzeit verstärkt in die Datensicherheit bzw. IT-Infrastruktur ihrer Objekte, um Hacks zu unterbinden.

### VORBEREITUNG VERRINGERT KRISENPOTENZIAL

Ein Datenleck ist im ersten Schritt eine technische Herausforderung. Aber als strategische Kommunikationsberater sehen wir für das betroffene Unternehmen noch ganz andere Risken, schließlich steht auch die Reputation der Führungsebene auf dem Spiel; auch Kundenbeziehungen werden durch Cybervorfälle nachhaltig gestört, wie eine unserer aktuellen Studien zeigt.

Ein Datenleck kommt der Suche nach der Nadel im Heuhaufen gleich. Recherchen, Schadensbewertung und mögliche Lösungsszenarien erfolgen unter höchstem Zeit- und Erfolgsdruck. In der Kommunikation stellen vor allem die Hektik und die anfangs unklare Sachlage eine große Herausforderung dar. Daher sind die Verantwortlichen gut beraten, für die latent vorhandene Gefahr eines Cyberangriffs gut vorbereitete Kommunikationspläne in der Schublade (sic!) zu haben. Zu den wichtigsten Adressaten zählen Mitarbeiter, betroffene Kunden bzw. Partner, diese sollten zuerst informiert werden. Wird das Leck nicht zeitnahe eingedämmt, ist der Schritt an die Öffentlichkeit vorprogrammiert. Bewusste Falschinformation oder Verschleierungsversuche sind keine Option, sonst wird aus einem Cybervorfall sehr schnell eine veritable Kommunikationskrise.

**ALEXANDER KLEEDORFER** | BRUNSWICK GROUP