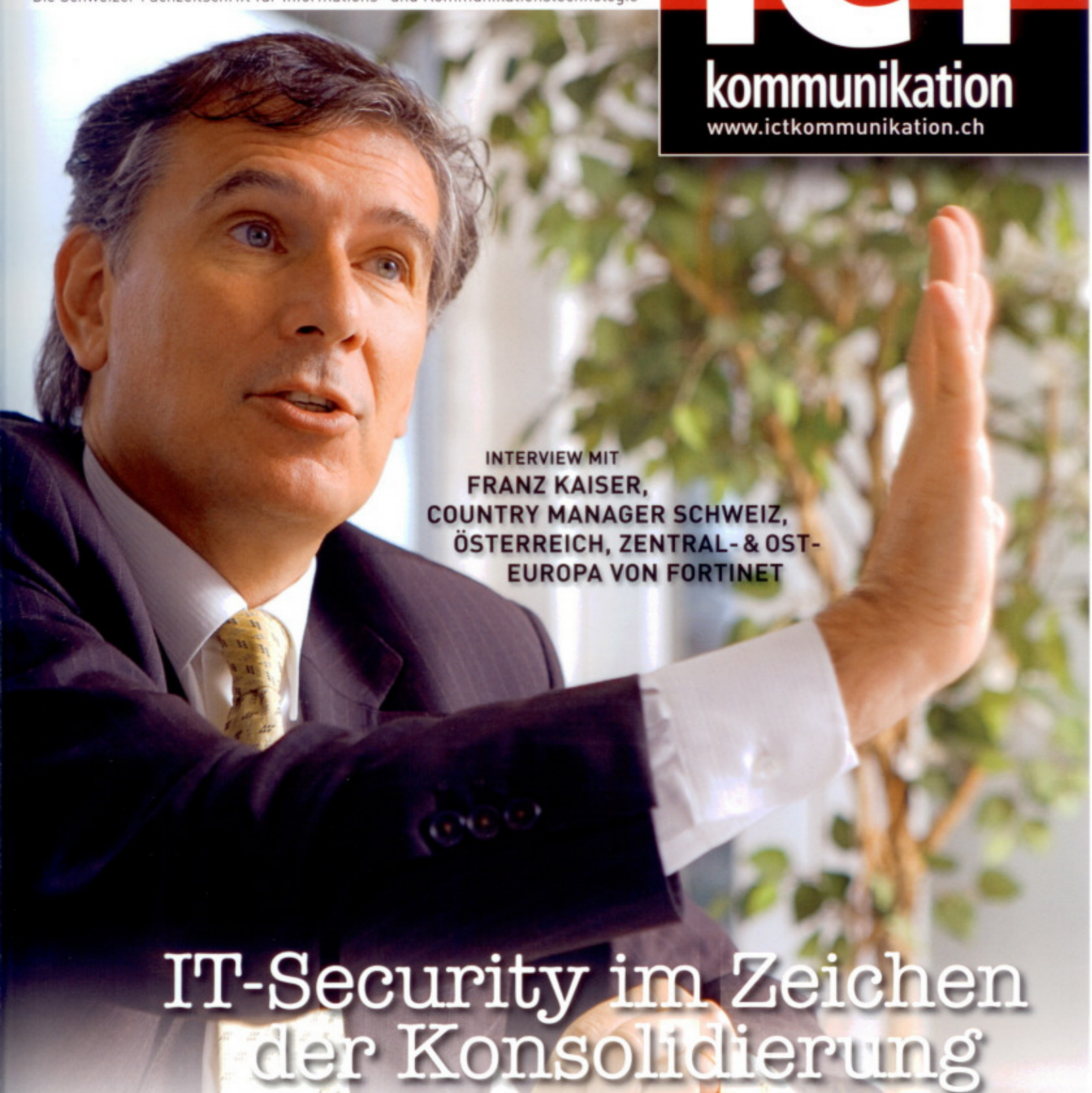
10 | 2008 CHF 6.–

ICT kommunikation

www.ictkommunikation.ch

Die Schweizer Fachzeitschrift für Informations- und Kommunikationstechnologie



INTERVIEW MIT
FRANZ KAISER,
COUNTRY MANAGER SCHWEIZ,
ÖSTERREICH, ZENTRAL- & OST-
EUROPA VON FORTINET

IT-Security im Zeichen der Konsolidierung

SPIEGELN STATT SUCHEN
TRENDS BEI DIGITALEN SPIEGELREFLEXKAMERAS

WENN DIE DATEN WEG SIND
AM SCHLUSS DER KETTE BLEIBT DIE DATENRETTUNG

DAS FINANCE FORUM 2008
KONZENTRATION AUF THEMENWELTEN UND QUALITÄT

IT-Security
im Zeichen der Konsolidierung

Die Security-Spezialistin Fortinet ist mit Lösungen bekannt geworden, die sämtliche Sicherheitsfunktionen in einer Appliance vereinen. Im Gespräch des Monats erläutert Fortinets Country Manager Franz Kaiser, wie sich KMU und Grossunternehmen heute wirksam schützen, wo sich die Security-Prophylaxe hinbewegt und wie sein Unternehmen auf den Konsolidierungs-Hype setzt.

von Karlheinz Pichler (Interview) und Tanya Hasler (Fotos)

Fortinet wurde im Jahr 2000 von Ken Xie, dem vormaligen Gründer und CEO von Netscreen, das dann später für 3,5 Milliarden Dollar an Juniper verkauft wurde, aus der Taufe gehoben. Es handelt sich also um ein noch sehr junges Unternehmen, das aber von Gartner schon seit Längerem neben Juniper und Check Point als Leader im «magischen Quadranten» für Netzwerk-Firewall-Anbieter geführt wird. Was war für den raschen Aufstieg von Fortinet ausschlaggebend?

Unser Erfolg ist auf die Kombination verschiedener Elemente zurückzuführen: Die Vision unserer Führungsebene, unsere technische Innovationskraft sowie externe Antriebskräfte. Ken Xie gründete Fortinet mit der Vision, dass hochperformante Multi Threat Security Appliances in Zukunft die einzige Antwort auf die Security-Bedürfnisse jedes Unternehmens werden würden, das starke Sicherheit bei hoher Kosteneffizienz, Skalierbarkeit und Benutzerfreundlichkeit sucht. Bis heute haben wir weltweit bereits mehr als 350 000 Appliances verkauft und unsere Sicherheitslösungen werden von mehr als 25 000 Kunden eingesetzt.

Die Hälfte unserer Mitarbeiter arbeitet in der Forschung und Entwicklung. Fortinet ist seit dem ersten Tag darauf bedacht, die Technologien ausschliesslich intern weiterzuentwickeln, um die bestmögliche Performance zu erzielen und sich von den sogenannten Point-Security-Anbietern abzuheben. Ausserdem haben wir in vielen anderen Bereichen Innovationen vorangetrieben. So ist Fortinet der einzige Anbieter, der Virtualisierung für die wichtigsten Sicherheitsfunktionen mit zusätzlichem Routing und Switching anbietet.

Es gibt zudem einige äussere Bedingungen, die den Einsatz konsolidierter Netzwerk-Security-Lösungen vorantreiben. Zum einen sehen sich Unternehmen mit einer ständig steigenden Anzahl von komplexen Internet-Bedrohungen konfrontiert und müssen immer mehr Compliance-Anforderungen erfüllen.

Zweitens sind IT-Abteilungen immer mehr vom wirtschaftlichen Abschwung betroffen und müssen daher nach Security-Lösungen suchen, die effektiv, aber auch kostengünstig und leicht zu managen und zu updaten sind. Drittens wird der Druck auf die Unternehmen, ökologisch und umweltgerecht zu agieren, immer grösser. Unsere integrierten Multi-Threat-Security-Lösungen helfen Unternehmen dabei, all diese Herausforderungen zu meistern.

> «Durch die Konsolidierung der Network Security entfällt der Kosten- und Managementaufwand für viele Einzellösungen.»

Fortinet wird vielfach als «Erfinderin» von Unified Threat Management (UTM) bezeichnet. Stimmt das, und was steckt genau hinter diesem Konzept, das seit einiger Zeit ja auch von etablierten Herstellern wie etwa Check Point promotet wird?

«Pro Tag werden von unseren Appliances weltweit zwischen 1 000 und 3 000 einzigartige Malware-Angriffe geblockt.»

Fortinet setzt seit seiner Gründung auf Unified Threat Management und ist in diesem Marktsegment Pionier und Leader im Gartner «Magic Quadrant». Unter UTM versteht man die Zusammenführung und Integration sämtlicher Sicherheitsfunktionen in einer einzigen Appliance.

___ In letzter Zeit ist im Security-Bereich der Begriff «Konsolidierung» zu einem ständig wiederkehrenden Schlagwort geworden. Ist dieser Begriff im direkten Zusammenhang mit UTM zu sehen? Dürfen die Anwender im Rahmen des Konsolidierungstrends mit deutlichen Kosten- und Komplexitätsreduktionen rechnen?

Die Konsolidierung und Integration von Security-Funktionen im Rahmen einer UTM-Strategie bietet in Bezug auf Kosten und Effizienz eine wirksame und wirtschaftliche Lösung für Unternehmens-Netzwerke aller Grössenordnung. Durch die Konsolidierung entfällt der Kosten- und Managementaufwand für viele Einzellösungen. Unternehmen müssen nicht mehr entscheiden, welche Security-Elemente sie brauchen und auf welche sie verzichten können. Network-Security-Konsolidierung integriert das komplette Spektrum der Netzwerk-Sicherheit in einer Appliance und macht so das Netzwerk robust und gegenüber den meisten Attacken unempfindlich. Eine einzige Appliance ersetzt alle Security-Lösungen zum Filtern und Schützen – hinsichtlich Budget- und Personaleinschränkungen ein sehr grosser Vorteil.

___ Ihr Flaggschiff im Netzwerksicherheitsbereich ist Fortigate. Es verfügt über Asic-beschleunigtes UTM. Wie wichtig sind solche Prozessor-orientierte Beschleuniger? Was können sie leisten?

Sowohl Unified Threat Management (UTM) als auch vollständige Content Protection erfordern einen erheblichen Prozessorenaufwand. Daher haben Unternehmen bisher oft gezögert, UTM-Plattformen einzusetzen, da sie sich vor den Auswirkungen auf die Netzwerk-Performance scheuten. Dank spezialisierter, Asic-basierter Hardware sind diese Bedenken mittlerweile hinfällig. Asic-Prozessoren ermöglichen Content-Analysen in Echtzeit, Scanning und die Beschleunigung von Security-Funktionen wie Firewall und Verschlüsselung oder Entschlüsselung. Plattformen auf Basis spezialisierter Hardware haben die Performance-Barriere durchbrochen und bringen Unternehmen jeder Grösse die Vorteile konsolidierter Netzwerk-Security-Lösungen.

___ Fortinet hatte seine Lösungen ursprünglich für KMU entwickelt, ist aber mittlerweile längst im Enterprise-Bereich angelangt. Warum diese «bottom-up»-Entwicklung? Lassen sich die KMU-Lösungen hinaufskalieren? Welches Segment ist für Sie heute wichtiger?

ZUR PERSON

Franz Kaiser ist Country Manager Austria, Switzerland and Central Eastern Europe bei Fortinet. In dieser Position leitet er das Vertriebsgeschäft über die indirekten Kanäle und ist zudem mit dem Ausbau des bestehenden Partner-Netzwerks in seiner Vertriebsregion betraut. Vor seinem Eintritt bei Fortinet 2004 war er Sales & Marketing Director beim Zürcher Distributor und Integrator Gutenberg Communication Systems. Zwischen 1993 und 2000 war er bei Swissphone Telecom unter Vertrag, wo er die Position des Vertriebs- und Profitcenterleiters für Mobile Communications innehatte. Bei Zellweger Uster, einem Hersteller von Prüf- und Messsystemen, war Kaiser Leiter Produktmanagement für Unix-Datensysteme. Kaiser begann seine IT-Karriere in Südafrika bei Micromation, einem Telefonie-Unternehmen, und war dort zuletzt General Manager. Franz Kaiser ist Diplom-Elektroingenieur der Technischen Universität Graz. Ein MBA in General Management der University of London rundet seine Ausbildung ab.

Franz Kaiser privat:
Seine Hobbies sind Gourmet-Essen, Science Fiction, Raumflug, Musik, Skifahren, Wandern und Lesen, vor allem Belletristik.

Kaiser hat sich vor Kurzem ein Ticket für die 2009 beginnenden Weltallflüge von Virgin Galactic gesichert. Für Kaiser ist diese Reise die Erfüllung eines Kindheitstraumes. Mit 9 Jahren hat er den Flug zum Mond mitverfolgt und diese tagelange Live-Sendung hat sein ganzes Leben geprägt.

UTM-Lösungen stehen für Kosteneffizienz, Bedienerfreundlichkeit, einfaches Management und leichte Wartung.

Franz Kaiser

Fortinet hat sich nicht direkt für eine «bottom-up»-Entwicklung entschieden. Die KMU waren einfach die ersten Anwender von UTM-Lösungen aufgrund der Vorteile dieses Konzeptes: Kosteneffizienz, Bedienerfreundlichkeit, einfaches Management und leichte Wartung. Grosse Unternehmen, Carrier und Service Provider hingegen suchten eher nach den besten Einzellösungen mit der höchsten Performance und waren für lange Zeit davon überzeugt, diese nur bei Point-Security-Anbietern zu finden. Ich würde nun nicht sagen, dass unser Erfolg auf dem KMU-Markt uns die Eroberung des Enterprise-Marktes ermöglichte. Aber die Erfahrungen bei der Entwicklung von Midrange Appliances haben geholfen, unsere Produktlinie so zu erweitern, um auch leistungsstarke Enterprise-Lösungen anbieten zu können.

___ Kann man die Sicherheitsbedürfnisse von KMU mit denjenigen von grösseren Betrieben grundsätzlich vergleichen?

Die aktuelle Marktlage zwingt mittlerweile alle Unternehmen dazu, dieselben Anforderungen an ihre Unternehmenssicherheit zu stellen. Sie benötigen Lösungen, die effektiv vor jeder Art von Bedrohung schützen und dabei vereinfachtes Management sowie eine einfache Wartung bei bestem Preis-Leistungs-Verhältnis bieten. Beim Kauf einer Security-Lösung sind einfaches Management und die Preisfrage die Top-Kriterien für kleine Unternehmen mit begrenzten IT-Ressourcen. Für grössere Unternehmen hingegen, die die Komplexität der Netzwerk-Infrastruktur und des täglichen betrieblichen Aufwands reduzieren wollen, spielen Performance und das vereinfachte Management die wichtigste Rolle.

___ Wie unterscheiden sich die Fortinet-Lösungen konzeptionell und anwendungsspezifisch von denjenigen der Konkurrenz?

Fortinet ist der einzige Security-Hersteller, der einen Schutz gewährleistet, der sich durch das gesamte Unternehmen hindurch zieht, vom Gateway bis zum Endpunkt. Unsere Multi Threat Appliances bieten Netzwerksicherheit, unsere E-Mail-Plattform Fortimail vollständige Content Security und unsere Forticlient Security Software für Desktops, Laptops und mobile Geräte Endpoint Security. Diese Produkte stammen zu 100 Prozent aus unserer eigenen Entwicklung, sind Asic-beschleunigt und richten sich an alle Marktsegmente, vom kleinen Büro bis hin zu den grossen Unternehmen. Zudem haben wir gerade erst Lösungen für die Applikationssicherheit auf den Markt gebracht. Wir decken allerdings nicht nur ein grosses Spektrum an Sicherheitsfunktionen ab, sondern bieten zudem auch unsere eigenen Security Intelligence Services über das Fortinet Threat Response Team an, um Updates automatisch und in Echtzeit rund um die Uhr zur Verfügung zu stellen.

___ Viren, Spam, Schadcode etc. scheinen in diesem Jahr wieder beträchtlich zugenommen zu haben. Wie viele diesbezügliche Signaturen registriert man derzeit pro Tag?

Die Anzahl derartiger Angriffe variiert von Tag zu Tag, aber man kann sagen, dass pro Tag ungefähr zwischen 1000 und 3000 einzigartige Malware-Angriffe von unseren Appliances weltweit geblockt werden. Dies zeigt, dass, obwohl die Anzahl der Attacken und Viren weiterhin steigt, die Vielfalt bei den Angriffen gar nicht so gross ist.

___ Worin sehen Sie momentan und in absehbarer Zukunft die grössten Bedrohungen für die Unternehmen? Welche Rezepte empfehlen Sie den Unternehmen, um bestehende Risiken möglichst vermeiden zu können?

Wenn wir von den grössten Risiken und Bedrohungen für Unternehmen sprechen, so müssen diese zu-

ZUR FIRMA

Fortinet wurde 2000 gegründet und ist auf Asic-beschleunigte Multi-Threat-Sicherheitssysteme fokussiert. Die Lösungen des Unternehmens kombinieren mehrere Security Level Firewall, Antivirus, Intrusion Prevention, VPN – und schützen vor Spyware und Spam. Sie wehren Bedrohungen auf Netzwerk- und Content-Ebene unternehmensweit ab. Fortinet ist in privater Hand und hat seinen Hauptsitz in Sunnyvale, Kalifornien.

nächst begreifen, dass es heute viele Übertragungsmöglichkeiten für Viren gibt. Bislang wurden Viren, Trojaner und Spyware hauptsächlich über «Click-me»-E-Mails mit schädlichen Attachements verteilt und heruntergeladen. Das ist mittlerweile nicht mehr der Fall. Vielmehr machen nun sogenannte Drive-by-Installationen den Grossteil, nämlich 60 Prozent an Bot-Infizierungen aus. Hierbei werden Nutzer einfach durch das Besuchen einer Website mit schädlichem Inhalt infiziert oder durch das Besuchen einer legitimen Website mit schädlichen Verweisen. Auch mobile Geräte wie infizierte USB-Sticks, CD und Laptops können leicht ins Unternehmensnetz eindringen. Um ihre Netzwerke zu schützen, müssen Unternehmen daher in effektive und durchgängige Security-Lösungen investieren, um Bedrohungen auf allen Ebenen abzuwehren und sich gegen die Vielzahl der Angriffsmöglichkeiten zu stellen. Wir empfehlen den Aufbau solider, durchdachter Firewall-Strategien, eine ständige Sensibilisierung der Nutzer, schnell greifende Patching-Richtlinien und den Einsatz von Best-of-Breed-Multi-Threat-Security-Lösungen an den Netzwerkrändern sowie Antivirus- und IPS-Anwendungen innerhalb des Firmen-Netzwerkes.

___ Fortinet hat zu Sommerbeginn die Technik und das Produktportfolio von IPlock gekauft. IPlock ist, respektive war, auf Datenbanksicherheit und Auditing spezialisiert. Wie passt der Kauf der IPlock-Technik strategisch ins Fortinent-Portfolio?

Wir haben mit dieser Übernahme unser Netzwerk-Security-Portfolio um Datenbankschutz und -Compliance erweitert. Die Lösungen sind ideal für Unternehmen mit sehr hohem Anspruch an die Datensicherheit. Publik gewordene Sicherheitslükken und Datenverluste haben die negativen finanziellen, betrieblichen und rufschädigenden Folgen eines unzureichenden Datenschutzes gezeigt. Speziell Datenbanken werden immer mehr zum Ziel interner und externer Attacken durch Cyberkriminelle. Die Übernahme der IPlocks-Technologien eröffnet uns neue Märkte und neues Umsatzpotenzial. Laut Forrester Research beträgt der Markt für Datenbank-Auditing und -Sicherheit in Echtzeit zirka 450 Millionen US-Dollar. Forrester erwartet eine Verdoppelung bis 2010, da immer mehr Unternehmen ihre Datenbanken automatisieren und absichern wollen.

___ Fortinet operiert global vor allem über den Channel. Welche Channel-Strategie verfolgen Sie in der Schweiz? Wie erreichen Sie Ihre Kunden? Unterscheidet sich der Schweizer IT-Security-Markt von demjenigen anderer Länderer?

Es ist wichtig, dass unsere Partner über ein gutes Know-how unserer Produkte verfügen. Alle Projekte mit unseren Endkunden werden von unseren Partnern konzipiert und realisiert. Wir haben unsere Anwesenheit an Veranstaltungen drastisch erhöht, um im Markt präsenter zu sein und wir vertrauen sehr stark auf direkten Endkundenkontakt zur Unterstützung unserer Partner mittels eigenen Major Account Managern. Die Schweizer Firmenanwender sind bereits sehr gut informiert und haben dementsprechend hohe Anforderungen an ihre Lieferanten.

___ Fortinet hat in der Schweiz gerade erst eine neue Niederlassung eröffnet. Welche Funktion hat diese, zumal sie ja über den Channel agieren? Werden Grosskunden von hier aus nun direkt betreut?

Der Partner ist für Fortinet ein sehr wichtiger Kunde und unser Multiplikator in den Markt. Umso wichtiger ist es, lokal präsent zu sein und mit unseren Partnern eng zusammen zu arbeiten. Auch die Präsenz beim Endkunden wollen wir erhöhen. Somit werden Grosskunden von uns auch direkt betreut. Abgewikkelt werden die Projekte aber von den Partnern. □