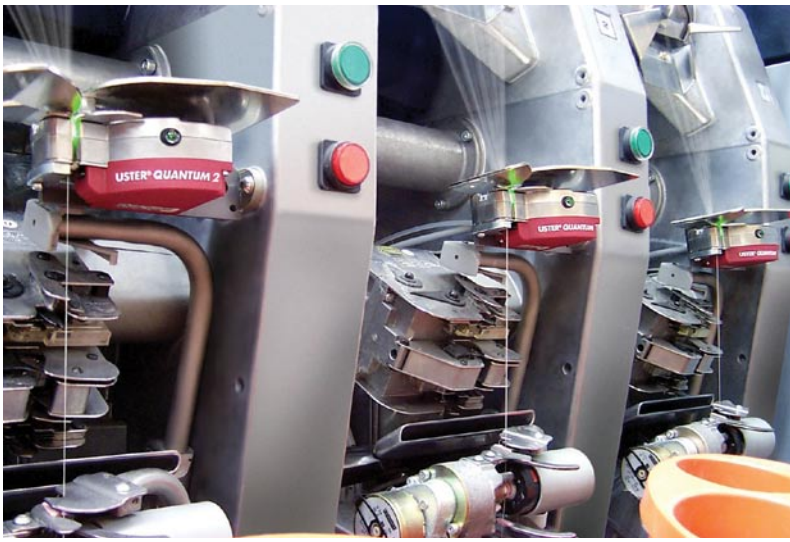
SUCCESS CASE STORY

Sicherheit bis in die letzte Faser

International der Markt, dezentral die Struktur: Die im Bereich Textil-Elektronik tätige Uster Technologies setzt auf Innovation und Qualität – auch im IT-Security-Umfeld.

Herstellern edler Garne und Gewebe ist die im zürcherischen Uster beheimatete Uster Technologies ohne Frage ein Begriff. Die weltweite Nummer eins für Systeme und Verfahren zur Qualitätskontrolle in der Textilindustrie ist überall dort anzutreffen, wo hoch stehende Anforderungen an die Prüfung von Fasern und Garnen gestellt werden – weltweit. Die modernen, mit hoch präzisen Sensoren sowie intelligenter Software ausgestatteten Systeme kommen einerseits in Prüflabors zum Einsatz. Andererseits sind sie Teil hoch leistungsfähiger Produktionssysteme für Spinnereien und Webereien. Diese so genannten Online-Prüfgeräte sorgen beispielsweise dafür, dass sich mehrere hundert Meter Garn pro Minute auf unterschiedlichste Qualitätsmerkmale wie z. B. Dicke und Verunreinigungen prüfen und entsprechend dokumentieren lassen. Auftretende Fehler werden sofort erkannt und behoben; daraus resultiert eine hundertprozentige Qualitätsgarantie für die Endprodukte. Dass die Lösungen von Uster Technologies einen weltweiten Standard setzen, wird durch die so genannte «Uster-Norm» eindrücklich untermauert. Sie hat sich als gültige Norm zur Qualitätssicherung im Textilbereich weltweit etabliert.



«Es ist unsere Aufgabe, die umfassenden Kommunikations-Bedürfnisse mit hohen Sicherheits-Anforderungen unter einen Hut zu bringen.»

Beat Grütter, Leiter IT, Uster Technologies

International verankert

Obwohl sich der Hauptsitz von Uster Technologies in der Schweiz befindet, spielt die «Musik der Textilindustrie» in anderen Regionen der Welt. So beispielsweise in Asien, in den USA und in Südamerika. Vor diesem Hintergrund erstaunt es nicht, dass Uster Technologies in zahlreichen Ländern mit eigenen Niederlassungen präsent ist. So z. B. in den USA (zwei Standorte), in Mexiko und Brasilien, in Deutschland, Indien, Thailand, Shanghai und Japan sowie in der Türkei. Ein besonders grosses Potenzial wird dem chinesischen Markt attestiert, was durch die Gründung von einer Niederlassung in Suzhou zum Ausdruck kommt. Beachtenswert ist dabei, dass im Land der aufgehenden Sonne auch Kompetenzbereiche wie Forschung und Entwicklung sowie Produktion angesiedelt sein werden.

«In unserem eigenen Rechenzentrum betreuen wir die gruppenweiten Applikationen und zeichnen für die gesamte Security- und Netzwerktechnologie verantwortlich»
Beat Grütter, Leiter IT, Uster Technologies

Verbindliche Security-Standards

«Unsere dezentrale Struktur verschafft uns die notwendige Nähe zu Märkten und Kunden», sagt Beat Grütter, Leiter IT, Uster Technologies, und er ergänzt: «Gleichzeitig stellt uns die weltweite Präsenz beziehungsweise die Integration unterschiedlicher Niederlassungen, Produktionsstätten und Dienstleistungsbereiche vor grosse Herausforderungen im Bereich der Informations- und Kommunikationstechnologie.» Vor diesem Hintergrund setzt Uster Technologies sowohl auf zentrale als auch auf dezentrale integrierte Dienste. Das in Uster domizilierte IT-Team bildet den eigentlichen Dreh- und Angelpunkt für sämtliche ICT- und Security-Aufgaben. «In unserem eigenen Rechenzentrum betreuen wir die gruppenweiten Applikationen wie SAP, betreiben die gesamte Mail-Server-Infrastruktur und zeichnen für die gesamte Security- und Netzwerktechnologie verantwortlich», erklärt Grütter. «Ebenfalls von uns betreut werden die in den einzelnen Niederlassungen installierten Server, nicht jedoch die rund 500 eingesetzten Desktop-PCs und Notebooks. Diese sind – mit Ausnahme der installierten Sicherheitskomponenten – in der Obhut der jeweiligen IT-Verantwortlichen vor Ort. Um trotz dieser Verteilung der Verantwortung auf eine firmenweit konsistente IT-Infrastruktur zählen zu können, haben wir betreffend Konfiguration und Wartung verbindliche Standards definiert.»

Den Gefahren wirkungsvoll begegnen

Als besondere Herausforderung bezeichnet Grütter die firmenweite IT-Security; gilt es doch, die umfassenden Kommunikations-Bedürfnisse mit hohen Sicherheits-Anforderungen unter einen Hut zu bringen. Dementsprechend hat Uster Technologies in den vergangenen Jahren sämtliche Standorte mit Cisco PIX Firewalls ausgestattet. Diese ermöglichten den Aufbau von VPN-Verbindungen via Internet und unterstützten die damals gewählte Strategie, den gesamten Internetverkehr über den zentralen Server in Uster zu schlaufen. «Von dieser damaligen Entscheidung haben wir Abschied genommen», sagt Grütter und erwähnt als einen der Gründe die ungenügende Performance beziehungsweise die störenden Verzögerungen bei der erzwungenen (Daten-)kommunikation über die Schweiz. Als noch wichtiger aber deklariert er Aspekte wie Flexibilität und Sicherheit. «Die bisher eingesetzte VPN-Lösung bedingt auf den dedizierten Endgeräten eine so genannte Client-VPN-Software, was die Anzahl nutzbarer Endgeräte einschränkt. Demgegenüber ermöglichen Clientless-VPN-Lösungen eine geschützte Datenkommunikation via Tunnel, ohne dass spezifische Software auf dem Endgerät installiert werden muss. Ein Standard-Webbrowser, User-Name und Passwort sowie eine dritte Sicherheitsstufe wie etwa ein

«Wir setzen auf eine firmenweit konsistente IT- und Security-Infrastruktur»

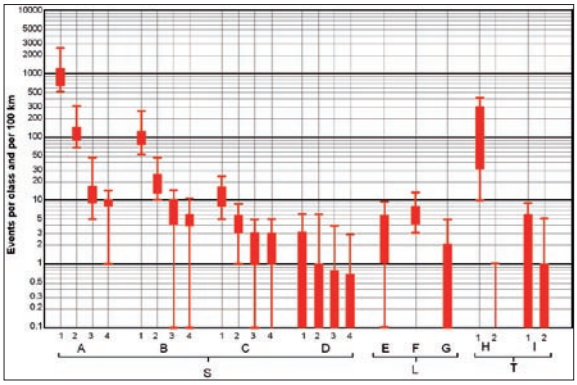
Uster Techologies

Die Uster Technologies AG wurde im Anschluss an den Erwerb der Zellweger Uster im Jahre 2003 durch das Management sowie die beiden Finanzinvestoren Quadriga Capital und Capvis gegründet.

Das Unternehmen deckt das gesamte Spektrum von der Garnerzeugung bis zum fertigen Gewebe ab und ist seit über sechzig Jahren in diesem Marktsegment aktiv. Es verfügt innerhalb der Textilindustrie über einen weltweit bekannten, für höchste Qualitätsansprüche stehenden, Markennamen.

Uster Technologies betreibt neben dem schweizerischen Hauptsitz in Uster weltweit noch zwei weitere Technologiezentren, in Knoxville USA, sowie Suzhou China. Darüber hinaus ist Uster mit neun regionalen Verkaufs- und Servicezentren weltweit vertreten.

USTER®
Think quality



Bildlegende: Statistics for Classimat Quantum

Zertifikat genügen bereits.» Ferner macht Grütter auf den Umstand aufmerksam, dass bei der bisherigen Lösung kein Virenscanning im VPN-Tunnel möglich war. «Was aber, wenn ein infizierter Computer via VPN-Tunnel mit den Systemen einer anderen Niederlassung kommuniziert?», fragt er und gibt die Antwort gleich selbst: «Der Virus kann sich unbemerkt verbreiten und sein Unwesen treiben. Dies gilt es mit allen Mitteln zu verhindern.»

Aufs richtige Pferd gesetzt

Dies und weitere Faktoren haben Grütter und sein Team veranlasst, nach einer innovative(re)n Security-Lösung Umschau zu halten. Diese sollte möglichst zahlreiche Sicherheits-Funktionen in einem System beinhalten und eine effektive Abwehr in Echtzeit gegen Malware jeglicher Art ermöglichen.

«Die Erkennung bösartigen Codes muss so früh wie möglich erfolgen»

«Die Erkennung bösartiger Codes muss so früh wie möglich erfolgen – bevor etwa Viren und Spam ins Netzwerk eindringen. Darauf legten wir grossen Wert. Darüber hinaus war für uns klar, dass eine neue Security-Plattform auch Funktionen wie SSL-VPN unterstützen muss, um den Datenverkehr via VPN-Tunnel ebenfalls kontinuierlich zu überwachen. Mit der Security-Appliance Fortigate von Fortinet sind wir fündig geworden.» Grütter betont, dass der Beschaffung kein weit reichendes Evaluationsverfahren vorausgegangen ist. «Einerseits sind auf dem Markt erst wenige Systeme erhältlich, die unsere Bedürfnisse abdecken – auch die bestehende Cisco-Infrastruktur konnte nicht um die gewünschten Features erweitert werden. Andererseits haben wir mit der in Effretikon do-

Bildlegende folgt

Die Security-Appliances von Fortigate sind in der Lage, Inhalte in Echtzeit zu prüfen.

mizilierten Sidarion einen langjährigen Netzwerk- und Security-Partner zur Hand, dessen Wissen und Erfahrung im Bereich der IT-Sicherheit von zentraler Bedeutung sind.

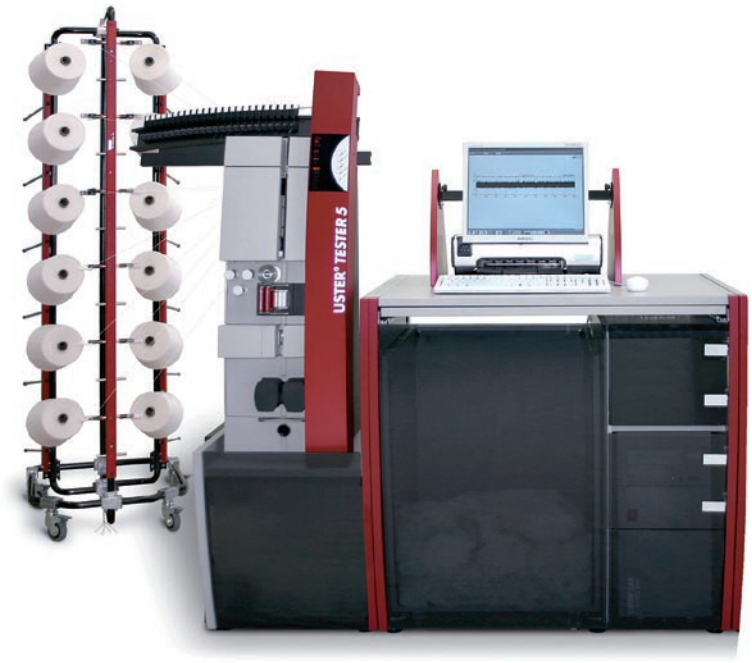
Komfortables Management

Die Migration der bisherigen Firewalls auf die neue Fortigate-Plattform erfolgt bei Uster Technologies schrittweise. Bereits mit den Systemen der Fortigate-Familie ausgestattet sind die Standorte Uster, Brasilien und China. Folgen werden die USA und im Laufe des kommenden Jahres weitere Standorte. Die in der Transitionsphase entstehende Heterogenität bereitet den IT-Verantwortlichen bei Uster Technologies kein Kopfzerbrechen. «Die Länder, die bereits mit einer Fortigate-Appliance ausgestattet sind, erhalten eine höhere Autonomie betreffend Kommunikation», lässt Grütter wissen, und er macht auf den Umstand aufmerksam, dass sich die beiden Plattformen von Cisco und Fortinet über eine zentrale Software steuern und überwachen lassen. «Sidarion ist mit der Entwicklung ihrer Firewall-Monitoring-Software „SIDmon" weit fortgeschritten. Diese ermöglicht ein komfortables Management heterogener Umgebung und informiert transparent über Netzwerk-Auslastungen, Netzprobleme und Verbindungswege.» Demnach dürfte es nur noch eine Frage der Zeit sein, bis es bei Uster Technologies heisst: «Sicherheit bis in die letzte Faser.»

«Sicherheit bis in die letzte Faser»

Beteiligte Unternehmen:

Kunde / Anwender	Uster Technologies AG, 8610 Uster Tel. 043 366 36 36 usterized@uster.com www.uster.com
Integrationspartner	Sidarion AG, 8307 Effretikon Tel. 043 544 10 66 info@sidarion.ch www.sidarion.ch
Systemlieferant	Fortinet, 8008 Zürich Tel. 043 488 37 56 www.fortinet.ch
Distributor	BOLL Engineering AG, 5430 Wettingen Tel. 056 437 60 60 info@boll.ch www.boll.ch



BOLL Engineering AG
Mythenstrasse 4, CH-5430 Wettingen
Tel. +41 56 437 60 60, Fax +41 56 427 29 29
www.boll.ch, info@boll.ch

IT Security Distribution
BOLL Engineering AG