

Tecan Group Ltd.

Pionier beim Schutz von Endgeräten – Führender Schweizer Laborausrüster setzt auf Symantec™ Endpoint Protection 11.0

Der Laborausrüster Tecan Group Ltd. betreibt Produktions-, Forschungs-, und Entwicklungsstätten rund um den Globus. Klar, dass dort sämtliche Endgeräte gut geschützt sein wollen. Dafür verlässt sich das Unternehmen auf die Lösung Symantec™ Endpoint Protection 11.0. Sie schützt Notebooks, Desktop-PCs und Server gleichermassen vor Angriffen – und zwar mehrschichtig, mit Intrusion Prevention, Firewall und Abwehr von Spionageprogrammen. Die neue Software von Symantec ermöglicht zudem proaktiven Schutz, indem sie auffällige Vorkommnisse sorgfältig beobachtet und analysiert. Bei alledem ist die Lösung über eine zentrale Verwaltungskonsole steuerbar. Ein weiterer Vorteil von Endpoint Protection: Es bietet die Möglichkeit, den Administratoren rollenbasierte Zugriffe zu gewähren. Und zu guter Letzt freut man sich bei Tecan auch über die hohe Skalierbarkeit der Lösung.

Eine wachsende Zahl von Endgeräten schützen

Die Lage im Netz ist ernst – das gilt nach wie vor. So zeigt der aktuelle Symantec Threat Report, dass die Bedrohungen aus dem Internet neue Dimensionen annehmen. Hartnäckiger und raffinierter denn je wird nach fremden Daten gegriffen. Neue Angriffstools sind in der Lage, völlig unbemerkt Informationen zu entwenden. Zwar geht es alles in allem in der Schweiz verglichen mit den USA oder China noch beschaulich zu. Dennoch gibt es im Land der Banken, das beim Phishing auf der Liste der Top Ten steht, alarmierende Zahlen. Laut Symantec-Sicherheitsreport sind Kreditkarten-Informationen die meistgehandelte Warengruppe auf Underground-Servern. Keine Frage: Weit reichender Schutz vor Bedrohungen ist unerlässlich. Dabei will nicht nur das Netzwerk gut gesichert sein – in den meisten Unternehmen gilt es überdies, eine wachsende Zahl von Endgeräten im Auge zu behalten, vom Server über den Desktop-PC bis hin zum Notebook.

Sicher wie ein Geldinstitut

Zuverlässigen Schutz für eine stetig zunehmende Zahl an Endgeräten – danach suchte auch der weltweit erfolgreiche Laborausrüster Tecan. «Wir sind zwar keine Bank», meint Patrik Büchli, Head of Infrastructure Services bei Tecan, augenzwinkernd, «aber punkto Sicherheit haben wir fast so hohe Anforderungen wie ein Geldinstitut.» Schliesslich liefert das Unternehmen seine Präzisionsgeräte ausschliesslich an hochkarätige Kunden mit hohem Sicherheitsanspruch. «Unsere Produkte gehen beispielsweise an Pharma- und Biotechnologie-Unternehmen oder an diagnostische

Unternehmensprofil

Die Tecan Group Ltd. ist einer der weltweit führenden Anbieter von Lösungen im Bereich der Life-Science-Zuliefererindustrie. Die Firma mit Sitz in Männedorf am Zürichsee entwickelt, produziert und vertreibt Geräte und Anlagen zur Automatisierung von Laborarbeiten. Mit seinem Vertriebs- und Servicenetz, das sich über 52 Länder erstreckt, bedient das Unternehmen die Kunden, darunter führende Pharma- und Biotechnologie-Unternehmen. Internationalität, Innovationsfreude und nicht zuletzt eine breite Produktpalette sorgten im Jahr 2006 für einen Gesamtumsatz in Höhe von 405,9 Mio. CHF.

Branche

Life-Science-Zulieferer

Symantec Produkte

Symantec™ Endpoint Protection 11.0

«Wir sind zwar keine Bank, (...) aber punkto Sicherheit haben wir fast so hohe Anforderungen wie ein Geldinstitut.»

Patrik Büchli

Head of Infrastructure Services,
Tecan Group Ltd.

Laboratorien. Da ist höchste Qualität eine Selbstverständlichkeit – auch in der IT.»

Zentral gesteuert: Mehrschichtiger Endgeräteschutz

Bei Tecan wünschte man nicht nur absolut zuverlässigen Endgeräteschutz. Patrik Büchli wollte für sein Unternehmen darüber hinaus eine Sicherheitslösung, die er weltweit in den 15 Niederlassungen der Tecan einsetzen und zugleich zentral steuern kann. Genau diese Option bietet die Enterprise-Version der neuen Lösung Symantec™ Endpoint Protection 11.0. Das vereinfacht nicht nur die Administration, sondern bietet zudem erhöhte Sicherheit. «Ich muss nicht länger dafür sorgen, dass einzelne Tools ständig auf dem aktuellen Stand sind, ich muss nur eine Lösung überwachen», freut sich Patrik Büchli.

In Kürze wird die Zeit der Inselfösungen beim Endgeräteschutz in seinem Unternehmen vorbei sein. Nämlich dann, wenn Büchli Endpoint Protection für die rund 1.000 User seines Unternehmens ausgerollt hat. Zurzeit setzt er Symantec Endpoint Protection 11.0 bei etwa 100 Anwendern ein. Die übrigen Endgeräte und Server werden teilweise noch mit der Symantec-Lösung AntiVirus und Produkten anderer Anbieter geschützt.

Die klassische AntiVirus-Lösung von Symantec ist ein bewährtes und ausgezeichnetes Produkt. Im Gartner Report «Magic Quadrant 2006» wurde sie in den Führungsquadranten eingestuft. Symantec hat nun AntiVirus um eine innovative Bedrohungsabwehr erweitert sowie neue Steuerungsfunktionen integriert und präsentiert damit eine neue mehrschichtige Lösung: Symantec™ Endpoint Protection. Geschützt werden Notebooks, Desktop-PCs und Server gleichermaßen, auch vor sehr komplexen Angriffen wie Rootkits, Zero-Day-Angriffen und veränderlichen Spionageprogrammen. Dank zentraler Steuerbarkeit können Sicherheitsrichtlinien im gesamten Unternehmen von einem Punkt aus eingerichtet und durchgesetzt werden. «Mit Endpoint Protection haben wir ein Produkt, das für sämtliche

Niederlassungen zuverlässig mehrschichtigen Endgeräteschutz bietet, und zwar zentral steuerbar», erklärt Büchli zufrieden.

Weltweiter Bedrohungsschutz

Das ist wichtig für Tecan, denn das Unternehmen ist auch in den USA und China vertreten. Dort ist die allgemeine Bedrohungslage im Netz deutlich kritischer als in der Schweiz. So waren die USA laut Symantec Threat Report im ersten Halbjahr 2007 Hauptangriffsziel von Denial-of-Service-Attacken, und China kämpft mit der weltweit grössten Anzahl von Bot-infizierten Rechnern. Geräte, bei denen ohne Wissen des Anwenders ein Bot (Robot), ein Computerprogramm installiert wird, das dann Angreifern den Zugriff ermöglicht.

Stets das Ganze im Blick

Aber nicht nur die langjährige Erfahrung von Symantec in Sachen Bedrohungsabwehr und die zentrale Steuerbarkeit der Lösung haben Büchli überzeugt. Ausschlaggebend war letztlich die Möglichkeit, den Administratoren rollenbasierte Zugriffe zu gewähren. Jetzt erlaubt Büchli den regionalen Administratoren den Zugriff für deren jeweiligen Verantwortungsbereich und kann zugleich von der Zentrale aus – «als Big Brother» – einen Blick auf das Ganze werfen.

Insgesamt 99 Clients – darunter 5 Server, 30 mobile Geräte und Desktop-PCs – sind nun bei Tecan mithilfe der integrierten Lösung von Symantec vor internen und externen Gefahren geschützt. Die Lösung bietet nicht nur Intrusion Prevention, Firewall und Abwehr von Spionageprogrammen, sondern ausserdem Geräte- und Virenschutz an. Dabei lassen sich die einzelnen Komponenten bedarfsorientiert aktivieren. Patrik Büchli nutzt auch das Application Blocking: So hat er z. B. sowohl Desktop Search als auch Google Earth geblockt. «Diese Programme sind nicht geschäftsrelevant.»

Reibungslose Installation

Bei der Installation wurde Tecan von den Firmen Dinotronic und Ontrex

«Mit Endpoint Protection haben wir ein Produkt, das für sämtliche Niederlassungen zuverlässig mehrschichtigen Endgeräteschutz bietet, und zwar zentral steuerbar.»

Patrik Büchli

Head of Infrastructure Services,
Tecan Group Ltd.

unterstützt. Die Berater des 1996 in Horgen gegründeten Unternehmens Dinotronic widmen sich «mit Leidenschaft» der IT ihrer Kunden. IT-Consulting, Netzwerke, Mobilitätslösungen und vor allem Lösungen für die IT-Sicherheit sind ihre Spezialität. Hand in Hand mit den Fachleuten des Schweizer IT-Unternehmens Ontrex, das unter anderem Symantec-Platinum-Partner ist, führte Dinotronic bei Tecan die neue Sicherheitslösung ein. Insgesamt zehn Tage war ein Experte des Symantec-Partners vor Ort, um Konfiguration, Tests und Rollout für die Pilotgruppe von 99 Clients zu begleiten. «Unter den Testanwendern sind auch einige besonders kritische User, die wir bewusst ausgewählt haben, um auch Feedback zu möglichen Schwächen der Lösung zu bekommen – wenn es Anlass dafür gibt», erklärt Patrik Büchli. Den allerdings gab es nicht: Administration und Anwender sind mit der neuen Lösung zufrieden.

Zeit und Ressourcen sparen

Die zentrale Admin-Konsole ermöglicht es, Zeit zu sparen, und die Software selbst schont die Ressourcen. Mit nur einem Agenten wird die Nutzung der Systemressourcen reduziert. Insgesamt fallen weniger System- und Netzwerkklast an. So entsteht im Leerlauf beispielsweise nur ein Arbeitsspeicherbedarf von 25 MB, und auch in der Scan-Phase sollte Platz genug verbleiben, um mit anderen Programmen zu arbeiten. Damit befindet sich Endpoint Protection im Vergleich mit anderen Lösungen am unteren Ende der Skala, was die Belastung des Arbeitsspeichers betrifft, obgleich der Leistungsumfang der Lösung besonders gross ist.

Das kann Büchli bestätigen: «Auch während eines Virencans können wir die normalen Office-Programme weiterhin nutzen, ohne eine Beeinträchtigung zu spüren», erklärt er. «Bei Aufgaben wie Kompilieren und Gerätetests kann es aber sein, dass wir bei älteren Geräten die Belastungsgrenze erreichen.»

Einfach skalierbar

Gut und problemlos liess sich die neue Lösung implementieren. «Natürlich

DIE LÖSUNG AUF EINEN BLICK

Die Herausforderung

Die Endgeräte in allen Niederlassungen des Unternehmens mehrschichtig schützen – und zwar mit einer Lösung, die zentral steuerbar ist und rollenbasierte Zugriffe erlaubt.

Die Lösung

Die neue Lösung Symantec™ Endpoint Protection 11.0 bietet mehrschichtigen Schutz vor Angriffen aus dem Netz. Dabei lässt sie sich zentral steuern. Zudem ermöglicht sie es, rollenbasierte Zugriffe zu vergeben.

Eingesetzte Software

Symantec™ Endpoint Protection 11.0

IT-Umgebung

- Server: 1 Application-Server, 1 SQL-Server sowie pro Standort 1 Update-Server
- PCs: ca. 600 PCs, 400 Laptops

Beratendes Systemhaus

Ontrex AG, Winterthur, zusammen mit der Dinotronic AG, Horgen

Kaufmännische Ziele

- Einen weit reichenden Datenschutz implementieren
- Das Unternehmen vor Identitätsdiebstahl und Phishing schützen
- Eine integrierte Lösung mit zentralem Management statt Insellösung
- Hohes Sicherheitsniveau
- Zentrale Gerätekontrolle

Technische Herausforderungen

- Weit reichender Schutz vor Bedrohungen dank einer Technologie, die eine Vielzahl von Bedrohungen vorab erkennt
- Eine integrierte Lösung mit einem konsistenten System
- Eine Technologie, die auch in der Lage ist, neue Bedrohungen zu erkennen und abzuwehren
- Geringe Falscherkennungsrate
- Nur ein Agent auf jedem Client
- Rollenbasierte Administration, mit der sich die Befugnisse bei administrativen Zugriffen an den jeweiligen Verantwortungsbereich des Administrators anpassen lassen

braucht man Fachleute dafür», so Büchli. «Aber wer vom Fach ist, findet sich schnell in Endpoint Protection zurecht.» Einen Vorteil der Enterprise Edition von Symantec™ Endpoint Protection will Büchli nutzen: die hohe Skalierbarkeit. «Weiteres Wachstum können wir jetzt auch im Hinblick auf den Schutz von Endgeräten problemlos bewältigen.» Jüngstes Beispiel für Tecans generellen Wachstumstrend: Die Übernahme der Schweizer Firma REMP im Jahr 2006. Mit der Akquisition dieses Herstellers und Entwicklers von automatisierten Laborlager- und Logistiksystemen wurde Tecan zum Marktführer auch in diesem Bereich.

«Ich muss nicht länger dafür sorgen, dass einzelne Tools ständig auf dem aktuellen Stand sind, ich muss nur eine Lösung überwachen.»

Patrik Büchli

Head of Infrastructure Services,
Tecan Group Ltd.

Besseres Reporting

Da ist es umso besser, dass Endpoint Protection auch für das Reporting weit reichende Möglichkeiten bietet. So gehören das lästige Zusammensuchen und manuelle Erstellen von Reports in Form von Excel-Sheets bei Tecan jetzt der Vergangenheit an. Die Logfiles lassen sich in fast jeder Hinsicht auswerten. Das Programm bietet etwa 60 vordefinierte Reports an. Und natürlich ist zusätzliches Customizing möglich.

Und noch etwas freut Patrik Büchli: Die Rate der Fehlerkennungen, d. h. der fehlerhaft als Angriff identifizierte Vorkommnisse, ist bei Symantec™ Endpoint Protection 11.0 besonders gering. Das vermeidet nicht nur Verdruss bei den Benutzern, es entlastet auch die Administration.

Aktualisierung «per Mausklick»

Insgesamt 1.000 Lizenzen der Endpoint Protection hat Büchli erworben. Und bis Ende des Jahres will er sie aufgespielt haben. Ein Vorgang, der dort, wo bereits Symantec AntiVirus implementiert ist, gewissermassen «mit einem Mausklick» zu erledigen ist. Hier kann Symantec Endpoint Protection 11.0 automatisch aufgespielt werden.

Bestmögliche Sicherheit

Auch für die mobilen Benutzer bietet die Lösung bestmögliche Sicherheit: Bei jedem Login ins Unternehmensnetz wie auch ins Internet erfolgt ein automatisches Update der Bedrohungsabwehr. Der Benutzer muss sich um nichts kümmern – und die Administration kann die Patch-Updates zentral überwachen.

Patrik Büchli ist einer der Ersten, der Symantec™ Endpoint Protection 11.0 im Einsatz hat. Schon gut zwei Wochen vor der Markteinführung des Produktes lief bei seiner Testgruppe die Beta-Version. So konnte er bei der Launch-Party in Zürich bereits über die neue Bedrohungsabwehr für seine Systeme berichten. Fehlt ihm nur noch ein besserer Virenschutz, was die eigene Gesundheit anbetrifft – pünktlich zum Produkt-Kickoff fing er sich leider einen Magenvirus ein. ■