



Bellevue Group schützt IT mit Cisco Security-Architektur Ein Netzwerk so sicher wie ein Banksafe

BB Bellevue
Group

BB Bellevue
Asset Management

BB Bank am Bellevue



Holger Schultes, IT-Leiter der Bellevue Group:
"Je bedeutsamer die IT für die Geschäftstätigkeit,
desto dringlicher der effektive Schutz."

Bei der schweizerischen Bellevue Group trieben heterogene IT-Sicherheitssysteme verschiedener Anbieter den Managementaufwand immer weiter in die Höhe. Der renommierte Finanzdienstleister stieg deshalb 2010 auf eine einheitlich administrierbare One-Vendor-Lösung von Cisco um. Die Security-Architektur, die sich auch auf mobile Endgeräte aller Art erstreckt, schützt kritische IT-Systeme zuverlässig vor Gefahren aus dem Cyberspace. Bellevue ist damit bestens gewappnet für die permanent steigenden Compliance-Anforderungen für Banken.

Die Bellevue Group mit Sitz in Küsnacht am Zürichsee ist eine unabhängige Finanzgruppe mit zwei eigenständigen Divisionen: die Bank am Bellevue AG und die Bellevue Asset Management AG. Die Bank am Bellevue AG ist im Schweizer Finanzmarkt als Broker-Haus und Anbieter massgeschneiderter Corporate Finance-Dienstleistungen renommiert. Von den hochkarätigen Research-Diensten der Bank profitieren vorrangig institutionelle Anleger – nicht nur in der Schweiz, sondern auch im Ausland. Seit vorigem Jahr ist die Bank über eine zehnpromtige Beteiligung an der New Yorker Brokerplattform Auerbach Grayson & Co. im amerikanischen Markt präsent. Die Corporate Finance-Sparte der Bank ist gleichfalls sowohl in der Heimat wie auch im internationalen Umfeld erfolgreich. In diesem Geschäftsbereich geht es hauptsächlich um Kapitalmarkt-Transaktionen und Dienstleistungen zur Optimierung der Kapitalstruktur.

Demgegenüber liegt der Schwerpunkt von Bellevue Asset Management auf der Verwaltung von Aktienportfolios, unter anderem für institutionelle Vermögen. Dabei werden attraktive Risiko-Rendite-Profile oft auf unkonventionelle Weise erschlossen – und zwar mit innovativen Anlagebausteinen, wie sie in einem orthodoxen Portfolio selten zu finden sind. Bellevue Asset Management arbeitet mit Nischenansätzen und nimmt Anlageoptionen in aufstrebenden Schwellenländern ebenso wahr wie insbesondere im Healthcare-Markt. Die Bilanz kann sich sehen lassen: Die Umsätze der Asset-Management-Sparte stiegen von 2008 bis 2010 um 34 Prozent.

Kennzeichnend für beide Unternehmenssäulen ist das Streben nach absoluter Kundenorientierung und maximaler Effizienz. „Basis unseres Erfolgs ist eine offene, methodisch vielfach erprobte Zusammenarbeit mit den Kunden, bei der wir die Kundenziele zu unseren eigenen machen“, sagt Holger Schultes, IT-Leiter der Bellevue Group. Seinen Worten zufolge erfordert hohe Prozesseffizienz, etwa im Hinblick auf die komplexen Research-Dienste der Bank, vor allem eines: eine hocheffiziente IT. Kein einziger der Bellevue-Geschäftsprozesse wäre heute ohne verlässliche IT-Unterstützung lebensfähig. Um flexibler auf Markt- und Kundenanforderungen reagieren zu

Hintergrund

Die 1998 gegründete Bellevue Group bietet ausgewählte Brokerage-, Corporate-Finance- und -Management-Services. Die Research-Produkte von Bellevue sind echte Outperformer: Seit ihrer Einführung 2004 lagen sie in 24 von 28 Quartalen zum Teil um ein Mehrfaches über dem Schweizer Aktienindex SMI. Fast die Hälfte der Bellevue-Aktien wird von der etwa 120-köpfigen Belegschaft gehalten.

Herausforderung

Das Management der bisherigen Sicherheitslandschaft mit Lösungen verschiedener Hersteller wurde immer aufwändiger. Bellevue suchte deshalb nach einer einheitlich administrierbaren Plattform, die überdies den mobilen Zugriff auf kritische Systeme und sensible Informationen zuverlässig schützen sollte.

Lösung

Vier Cisco ASA dienen als Firewall für die beiden gespiegelten Bellevue-Rechenzentren. Jeweils zwei Cisco IronPort E-Mail und Web Security Appliances halten Spam und Viren von allen Bellevue-Systemen fern. Für den sicheren Zugriff mobiler Notebooks, Smartphones oder Tablets sorgt die Cisco AnyConnect Secure Mobility Solution.

Nutzen

- sichere Nutzung mobiler Endgeräte mit standortbezogenen Security-Richtlinien
- freie Auswahl bei der Anschaffung mobiler Endgeräte
- Compliance auf kosteneffiziente Art

können, startete das Bankhaus bereits 2007 eine Grundsaniierung seiner IT-Landschaft, wozu insbesondere die Modernisierung der Sicherheitsarchitektur gehörte. „Je bedeutsamer die IT für Geschäftstätigkeit wird, desto dringlicher wird der effektive Schutz dieser kritischen Infrastruktur“, so der IT-Chef weiter. Unabdingbar ist eine verlässliche Abwehr von Viren, Spam und Hackerangriffen einerseits, um die Stabilität der Geschäftsprozesse zu garantieren. Zum anderen aber geht es um die Vertraulichkeit hochsensibler Informationen – immerhin gehört Diskretion zum Markenkern der Schweizer Finanzindustrie.

Einzellösungen versus übergreifender Sicherheitsarchitektur aus einer Hand

Die Elemente der Sicherheitsplattform wurden seinerzeit mosaikartig zusammengestellt: Lösungen für Firewaling, Verschlüsselung, Spamfilter, Authentifizierung und dergleichen mehr stammten von verschiedenen Anbietern. Durch eine Kombination dieser Lösungen wollte Bellevue die fachlich unterschiedlichen Security-Anforderungen auf jeweils bestmögliche Art und Weise erfüllen.

Soweit so gut. Doch die Praxis offenbarte auch eine andere Seite der Medaille: „Jede Lösung hatte eine individuelle Managementphilosophie und brachte ihre eigene Benutzeroberfläche mit. Jeder Bereich erforderte unterschiedliches technologisches Know-how mit entsprechendem Schulungsbedarf. Die Handhabung der heterogenen Lösungen erwies sich im Alltag als äusserst zeitraubend und kompliziert“, berichtet Holger Schultes. Aufwand verursachte zudem das Lizenzmanagement für das Konglomerat der heterogenen Einzellösungen. Kein Wunder also, dass die Nachricht von einer homogenen und übergreifenden Sicherheitsarchitektur den IT-Leiter im vorigen Jahr aufhorchen liess. Netcloud zeigte mit der Cisco Security-Architektur und dessen umfassenden Produktportfolio eine innovative Lösung zur Absicherung der gesamten IT des Unternehmens. Das Schweizer Systemhaus unterstützt seit Jahren die IT-Entwicklung der Bellevue Group. Alain Kistler, Account Manager bei Netcloud am Hauptsitz in Winterthur, kommentiert: „Die ganzheitliche End-to-End-Security-Architektur von Cisco adressiert umfassend und auf einheitliche Weise unterschiedliche IT-Sicherheits Herausforderungen. Dies steigert nicht nur die Effizienz beim Security-Management, sondern wird insbesondere der Tatsache gerecht, dass vormals feste Infrastrukturgrenzen in der modernen Arbeitswelt durchlässig werden – zum Beispiel, weil immer mehr mobile Mitarbeiter per Smartphone oder iPad auch unterwegs auf kritische Unternehmenssysteme zugreifen wollen. Vor diesem Hintergrund erweist sich die einheitliche Security-Architektur von Cisco als ein wesentlicher Treiber für uneingeschränkte Mobilität in der Geschäftstätigkeit und damit letztlich auch für mehr Agilität im Wettbewerb.“

Spam, Malware und Viren chancenlos

Die beiden Bellevue-Rechenzentren in Küsnacht sind durch eine Firewall aus insgesamt vier Cisco Adaptive Security Appliances der ASA 5500er Serie sicher von der digitalen Aussenwelt abgeschottet. Für die Web- und E-Mail-Sicherheit sorgen die Cisco IronPort S160 Web Security Appliance beziehungsweise die Cisco IronPort C160 E-Mail Security Appliance. Ebenso wie die gespiegelten Rechenzentren sind auch die IronPort-Lösungen jeweils doppelt installiert, um maximalen Ausfallschutz zu garantieren. Cisco IronPort C160 ist eine marktführende Lösung zum Erkennen und Blockieren von Spam und verseuchter Mailanhänge. „80 Prozent der rund 25.000 E-Mails, die täglich bei uns eingehen, sind Spam. Dank Cisco IronPort C160 landen davon null Prozent in den Postfächern unserer Mitarbeiter. Zudem hat es seit Inbetriebnahme der IronPort S160 noch kein einziger Virus geschafft, in unsere Systeme einzudringen“, bilanziert IT-Chef Schultes. Die Cisco IronPort S160 Web Security-Appliance durchleuchtet den kompletten Webverkehr. Verdächtige Seiten oder schadhafte Teile einer Page werden über den integrierten Reputation-Filter automatisch erkannt und blockiert. Ausserdem lassen sich Policies anlegen, um den Zugriff auf Websites, die keinen Bezug zur jeweiligen Arbeitsaufgabe haben, auf einfache Weise zu sperren.

Mobiles Arbeiten? Aber sicher!

Bis hierher könnte sich die Lösungsbeschreibung auch auf ein Anforderungsprofil beziehen, das fünf Jahre alt oder älter ist. In der Zwischenzeit aber hat sich unsere Arbeitswelt fundamental gewandelt: Der Siegeszug von Smartphones & Co. scheint unaufhaltsam. Über kurz oder lang kommt wohl kein Unternehmen am Megatrend Mobilität vorbei. In Kürze will man das auch gar nicht, denn das hiesse ja, auf wettbewerbsrelevante Flexibilitäts- und Produktivitätsvorteile zu verzichten. Doch wie lassen sich mobile Endgeräte unterschiedlichen Typs bruchlos in eine Sicherheitsplattform integrieren? „Mit der AnyConnect Secure Mobility Solution von Cisco“, antwortet Holger Schultes. Kernstück der Lösung ist eine extrem leichtgewichtige Clientsoftware, die sämtliche Online-Verbindungen vom Endgerät über eine verschlüsselte Tunnelverbindung zur zentralen Cisco ASA umlenkt – unabhängig vom momentanen Standort und dem jeweiligen Zugangsnetz. „Richtlinien und Verbindungsprofile können via ASA vorkonfiguriert und automatisch aktuell gehalten werden. Es entsteht also kein zusätzlicher dezentraler Managementaufwand für die mobilen Endgeräte“, fährt der IT-Chef fort.

Mitarbeiter aus seinem Team nutzen AnyConnect bereits, um ihre Wartungsaufgaben auch von zuhause aus erledigen zu können. In anderen Unternehmensbereichen hingegen steht die Einführung mobiler Clients noch bevor. Auch hat Bellevue noch nicht entschieden, welche Modelle angeschafft werden sollen. Doch dies ist auch völlig unerheblich, denn AnyConnect eignet sich für jedes Endgerät. Die erwähnte Clientsoftware läuft auf allen gängigen Betriebssystemen, auf Windows und Mac OS ebenso wie auf Android.

Holger Schultes fasst zusammen: „Mit unserer One-Vendor-Plattform werden wir heutigen und künftigen Sicherheitsanforderungen auf hocheffiziente Weise gerecht. Bedeutsam ist dies auch und gerade vor dem Hintergrund der äusserst dynamischen Compliance-Situation in der Schweizer Bankenbranche.“

Ansprechpartner beim Kunden:

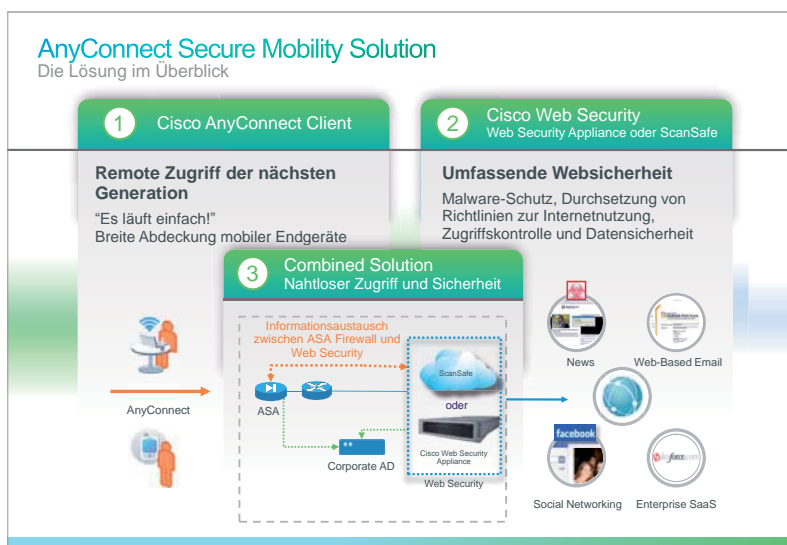
Bank am Bellevue AG
Holger Schultes
Seestrasse 16 / P.O. Box
CH-8700 Küsnacht

Telefon: +41 (0)44 267 72 22
Telefax: +41 (0)44 267 67 50
hsc@bellevue.ch
www.bellevue.ch

Lösungspartner:

Netcloud AG
Alain Kistler
Schlachthofstrasse 19
8406 Winterthur

Telefon: +41 (0)800 843 638
Telefax: +41 (0)800 843 329
kistler@netcloud.ch
www.netcloud.ch



Der Cisco AnyConnect Mobility Client lenkt den gesamten web-basierten Datenverkehr vom Endgerät über eine zentrale Cisco Adaptive Security Appliance (ASA) – unabhängig vom momentanen Standort und dem jeweiligen Zugangsnetz.



Cisco Systems GmbH
Kurfürstendamm 22
D-10719 Berlin

Cisco Systems GmbH
Neuer Wall 77
D-20354 Hamburg

Cisco Systems GmbH
Hansaallee 249
D-40549 Düsseldorf

Cisco Systems GmbH
Friedrich-Ebert-Allee 67-69
D-53113 Bonn

Cisco Systems GmbH
Ludwig-Erhard-Straße 3
D-65760 Eschborn

Cisco Systems GmbH
City Plaza
Rotenbühlplatz 21-25
D-70178 Stuttgart

Cisco Systems GmbH
Am Soldnermoos 17
D-85399 Hallbergmoos

Tel.: 0800-187 0318
www.cisco.de

Cisco Systems Austria GmbH
Millennium Tower, 30. & 31. Stock
Handelskai 94-96
A-1206 Wien
Tel: +43 (0)1 24030 6000
Fax: +43 (0)1 24030 6300

Büro Salzburg
Bürocenter am Arenberg
Eberhard Fugger Strasse 5
5020 Salzburg
Tel.0800 297 526,+43 (0)1 24030 6000
Fax: +43 (0)1 24030 6300

Tel.: 0800-297 782
www.cisco.at

Cisco Systems Switzerland GmbH
Richtstrasse 7
CH-8304 Wallisellen
Tel. +41 (0)44 878 92 00
Fax +41 (0)44 878 92 92

Cisco Systems Switzerland GmbH
Im Technopark - Morgenstr. 129
CH-3018 Bern
Tel. +41 31 998 50 50
Fax +41 31 998 44 69

Cisco Systems Switzerland GmbH
Avenue des Uttnis 5
CH-1180 Rolle
Tel. +41 21 822 16 00
Fax +41 21 822 16 10

Tel.: 0800-835 735
www.cisco.ch