



Bellevue Group protects its IT with Cisco Security Architecture

A network as secure as a bank vault

BB Bellevue
Group

BB Bellevue
Asset Management

BB Bank am Bellevue



Holger Schultes, Head of Information Technology (IT) at Bellevue Group: "The more important IT is for business operations, the more urgently you need to put effective safeguards in place to protect critical infrastructure."

At Bellevue Group in Switzerland, a heterogeneous mix of IT security solutions from various vendors was steadily driving up system management costs – so much so that, in 2010, the high-profile financial services group decided to unify its IT administration in a single-vendor solution from Cisco. The new security architecture, which also covers all kinds of mobile devices, protects crucial IT systems reliably against threats from cyberspace. The solution also means that Bellevue is now more than adequately equipped to meet the banking industry's increasingly stringent compliance requirements.

Headquartered in Küsnacht on Lake Zurich, Bellevue Group is an independent financial group comprising two autonomous divisions: Bank am Bellevue AG and Bellevue Asset Management AG. Bank am Bellevue AG is well-known within the Swiss financial services sector as a brokerage and provider of tailored corporate finance services. National and international institutional investors in particular rely on the bank's high-quality research services. Last year, the bank also stepped into the U.S. marketplace with its acquisition of a 10 percent stake in the New York stock-broking firm Auerbach Grayson & Co. The bank's corporate finance arm is very successful as well, both in its home market and abroad. The main activities in this segment are money-market transactions and capital structure optimization services.

In contrast, Bellevue Asset Management focuses on managing equity portfolios and institutional assets. They specialize in attractive and often unconventional risk-return profiles of a kind not often found in conventional portfolios. Bellevue Asset Management works with niche strategies that include investment options in emerging countries and, to a large extent, the healthcare market. The group's performance has been strong with its asset management arm reporting revenue growth of 34 percent between 2008 and 2010.

The hallmark of both divisions is their emphasis on complete customer focus and maximum efficiency. "We've built our international success on an open, methodical and proven approach to customer service that centers on making our customers' goals our own," says Holger Schultes, Head of Information Technology (IT) at Bellevue Group. His view is that high process efficiency, which for example is essential to support the bank's complex research services, requires one key factor: highly efficient IT. Not one of Bellevue's business processes would be viable today if it were not backed by reliable IT. To be better equipped to respond more flexibly to market and customer requirements, the bank embarked on a major reorganization of its IT landscape in 2007. One key

Background

Formed in 1998, Bellevue Group offers a select range of brokerage, corporate finance and asset management services. Bellevue's research products are genuine outperformers; since their launch in 2004, they have bettered Switzerland's SMI share index in 24 out of 28 quarters, in some cases several times over. Close to half of Bellevue's shares are held by its roughly 120 employees.

Challenge

Managing its previous security landscape with solutions from a variety of vendors had become increasingly complex for Bellevue. The group therefore began looking for a unified management platform that could reliably secure mobile access to critical systems and sensitive information.

Solution

Four Cisco ASA units have been deployed to firewall Bellevue's two mirrored data centres. Two Cisco IronPort Email Security Appliances and two IronPort Web Security Appliances are also in service, keeping Bellevue's systems free from spam and viruses. The Cisco AnyConnect Secure Mobility Solution is used to secure access by mobile devices like notebooks, smart phones and tablets.

Benefits

- Secure use of mobile devices with location-based security policies
- Freedom to procure mobile devices of choice
- Cost-efficient way to achieve compliance

focus of this initiative was on modernizing the group's security architecture. "The more important IT is for business operations, the more urgently you need to put effective safeguards in place to protect critical infrastructure," Schultes adds. And whilst mounting a reliable defense against viruses, spam and hacker attacks is crucial when it comes to ensuring the stability of the group's business processes, it's also vital to maintain confidentiality and the protection of highly sensitive information. These are both exceptionally important, given the Swiss financial services industry's reputation for discretion.

Standalone solutions versus an overarching security architecture from a single source

The components that made up the old the security platform had been put together in piecemeal fashion: the various solutions – for everything from firewalling and spam filtering to encryption, authentication and more – all came from different vendors. Bellevue had hoped, by combining these solutions, to put in place the best possible safeguards to meet the unique security requirements specific to each of these fields.

This aim was all well and good, but in practice there was a significant downside to this approach: "Each solution had its own distinct management philosophy and its own user interface. Each also represented a separate area of expertise and required specialized employee training. Working with a heterogeneous set of solutions proved to be extremely complicated and time-consuming in real life," Schultes explains. Managing the licenses for the range of individual standalone solutions was also costly. So it was hardly surprising that the news of a homogeneous, overarching security architecture last year quickly caught the IT executive's attention. Netcloud, a Swiss systems house which for years now has supported the development of Bellevue Group's information technology, offered to supply an innovative solution built around Cisco's Security Architecture and comprehensive product portfolio to secure the whole organization's information systems. Alain Kistler, an account manager at Netcloud's head office in Winterthur, says: "Cisco's complete, end-to-end security architecture covers a whole range of IT security challenges in a comprehensive and unified fashion. It not only makes security management altogether more efficient, it also addresses the fact that formerly tight infrastructure boundaries are becoming increasingly permeable in business today – not least because of the growing number of mobile workers using smart phones and iPads to access critical corporate systems while on the move. Against this backdrop, Cisco's unified security architecture is helping to support unconstrained mobility in business and to enable greater agility within the competitive arena."

No way in for spam, malware and viruses

Bellevue's two data centers in Küsnacht are cordoned off from the external digital world by a firewall consisting of four ASA 5500 Series Cisco Adaptive Security Appliances (ASAs). Cisco IronPort S160 and Cisco IronPort C160 Security Appliances are also in place to provide web and e-mail security respectively. Like the group's mirrored data centers, the IronPort solutions too have a duplicate failover system in place to provide maximum protection against outages. The Cisco IronPort C160 is a market-leading solution for identifying and blocking spam and infected e-mail attachments. "Eighty percent of the 25,000 e-mails we receive every day are spam. Thanks to the Cisco IronPort C160, zero percent of those e-mails land in our employees' inboxes. What's more, not a single virus has succeeded in penetrating our defenses to infect systems since we deployed the IronPort S160," reports Schultes. The Cisco IronPort S160 web security appliance analyzes all web traffic. Suspicious pages and malicious page content are detected and blocked automatically by a built-in reputation filter. In addition, the appliance allows policies to be created easily to block access to unproductive websites that have no relevance for employees' job tasks.

Making mobile working safe

Thus far, the solution described may not sound so different from requirements specification going back five or more years. However, the inexorable rise of smart phones and other handheld devices means that the business world has changed fundamentally since then. Sooner or later, the whole mobility megatrend will catch up with every business, and it's not something Bellevue Group is eager to avoid: after all, not embracing mobility would mean forgoing flexibility and productivity gains that are necessary to be able to compete effectively. The question is however, how do you seamlessly integrate different breeds of mobile devices within a single security platform? "With the AnyConnect Secure Mobility Solution from Cisco," says Holger Schultes. The solution centers on an extremely lightweight client software application which routes all online connections from the mobile device to the central Cisco ASA over an encrypted tunnel, regardless of the user's current location and access network. "Policies and connection profiles can be pre-configured in the ASA and kept up-to-date automatically. The mobile devices don't need additional decentralized management," Schultes continues.

People on his team are already using AnyConnect to carry out maintenance tasks from home. However other company units still have to roll out the mobile clients, and Bellevue hasn't decided yet which devices they want to deploy. At the end of the day though, the equipment they ultimately choose isn't particularly important because AnyConnect will work with any mobile device. The client software runs on all common operating systems, including Windows, Mac OS and Android. Holger Schultes sums up: "With our one-vendor platform, we're able to fulfill our security requirements with exceptional efficiency, and can continue to do so in the future. Going forward, this will be especially important given the rapidly changing compliance situation in Switzerland's banking industry."

Customer contact:

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

Phone: +41 (0)44 267 72 22
Fax: +41 (0)44 267 67 50

hsc@bellevue.ch
www.bellevue.ch

Solution partner:

Netcloud AG
Alain Kistler
Schlachthofstrasse 19
8406 Winterthur

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



The Cisco AnyConnect Mobility Client routes all online connections from the mobile device to the central Cisco Adaptive Security Appliance (ASA) – regardless of the user's current location and access network.



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 Söldnermoos 17
D-85399 Hallbergmoos

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

Cisco Systems Austria GmbH
Millenium 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