CLIENT STORY

opensystems | Swiss Re

When it comes to company global networking, the Switzerland-based reinsurer Swiss Re relies on security and availability. That's why Risto Wieland, Director IT, and his Infrastructure Team only implement solutions that make sense from both the operational and security points of view.

«It has to make sense from both the operational and security points of view.»

Risto Wieland, Director IT, Swiss Re

Mr. Wieland, IT security is no doubt right at the top of the priority list for a global reinsurer.

Risto Wieland That's certainly the case. Swiss Re has very high expectations in this regard. Our company stands for stability and quality throughout the world. So we need to prioritize security and availability.

Which helps explain why IT security is anchored not only in our processes but also in our corporate culture. Swiss Re creates an awareness of IT security among new employees, followed up with special training, and the topic is also firmly established in our continuing professional development program.

«So the challenge is to bring the internet closer to the users again **without having to compromise** on security or monitoring.»

Risto Wieland, Director IT, Swiss Re

How do you believe this topic changed over the years?

The internet has completely changed everything – both in terms of the way we work and the nature of the threats to the company.

These days, no company can afford not to be permanently connected to the internet. Companies need to be globally connected over the internet like we, people, need air to breathe. Not only as a means of communication, but increasingly also because business-critical applications and data are used on the internet.

You mentioned the change in the nature of the threats. Can you go into more detail?

Security remains a really big issue. In general, it is reasonable to assume that at least one third of the attacks on an organization or company are carried out through the browser.

But a threat can also arise if the existing network infrastructure is not designed to cope with heavy internet usage. This results in the fast-expanding data traffic clogging up the proxy infrastructure and, in the worst case, the performance of the business-critical applications is then massively reduced. A further critical point is the user experience when accessing data on the internet, be it on a website or an application used from the browser. If full performance is not provided here, productivity declines while employee dissatisfaction increases.

So the challenge is to bring the internet closer to the users again without having to compromise on security or monitoring. →

You and your colleagues from Operations have spent the last few months addressing these challenges together with the Information Security Team, and optimized the Swiss Re network for internet usage. What can you tell us about the project?

Data traffic in our network increased massively, of course, due to the use of social media and multimedia channels like YouTube. Our users employ these tools at the workplace for both private and work reasons – it's hard to draw a clear line between the two these days. But usage became so intense and traffic so heavy that the performance of business-critical applications was affected.

With the rollout of video-conferencing and document sharing, coupled with the shift of applications to the cloud, the user dissatisfaction was further intensified due to the slow internet access. The users became impatient when they had to access applications or tried to surf the web. They compared the performance at the workplace with their private connection at home. Someone in Sydney wanting to view a local weather page and having to wait 10 seconds before it appeared was quite rightly annoyed.

So the pressure came straight from the business?

Yes, and the criticism was completely justified, because our network was quite simply no longer fit for its purpose, given the heavy internet usage. Out of security and cost considerations over the years, we had reduced access points to the internet for our 60 or so worldwide locations, first to seven, and then to just two: Zurich for Europe and Asia, and Armonk (NY/USA) for North and South America. We wanted to fundamentally rethink this concept but could not afford to compromise security in any way.

In the meantime, our proxy infrastructure was becoming increasingly troublesome. The old platform had definitely reached the end of its life cycle. There were interruptions and we had to keep rebooting the system overnight in order to release storage capacity. It became ever clearer that we were heading towards an operational risk. Nonetheless, it was difficult for us to find a solution that made sense from both the operational and security points of view.

That sounds like a lively debate between operations and security. Who is responsible for implementing these things in the company?

In organizational terms, the setup at Swiss Re is so that the Infrastructure Team is responsible for designing and ensuring the smooth running of the networks, telephony and video platforms. The task of ensuring and overseeing security is, of course, also integrated in this operational responsibility. A central function in this regard is performed by our internal Product Delivery Team, which coordinates and oversees the cooperation with external partners.

Our colleagues from the Information Security Team define the security guidelines. The team is attached organizationally to the risk management function, which ensures its independence from IT in terms of reporting lines. The Information Security Team is also responsible for sampling compliance – meaning that they monitor our checks on compliance with the security guidelines. →

That sounds like a clean separation of execution and supervision.

Yes, in our case it's even twofold supervision. I think that this has to be practiced in the global setting of today, even though certain conflicts of interest between operations and security do sometimes hinder the internal discussion somewhat and delay solutions.

But we deliberately have this discussion because it ensures that we do not make decisions solely from the operational point of view. Although that would partly be easier, it would not always be safe. So we're pretty happy that we have tough but competent partners in the Information Security Team for whom security has top priority.

«The design for the Zurich location was then completed in two days. After a further eight days, everything was installed, commissioned and tested. I have never experienced anything like it in my 20 years in the industry. This gave me **great confidence** that we would get to grips with our proxy problem quickly and efficiently.»

Risto Wieland, Director IT, Swiss Re

What happened then?

From the operational point of view, we wanted to set about the life-cycle management of the proxy infrastructure as quickly as possible. Together with the existing network provider, we took a look at various options – including in the cloud – but these options were out of the question as far as the Information Security Team was concerned. In addition, we were certain that we did not want to set up a separate new proxy infrastructure for either operational or security reasons, either at the head office or at the individual locations.

The Information Security Team wanted to be certain that all their requirements were met. They would have preferred to test all the options before a decision was taken, but there wasn't enough time to do so from the operational perspective. →

Stability and innovation combined

No other firm has shaped the global reinsurance business as comprehensively as Swiss Re. Established in 1863, the company is today one of the world's biggest and most successful institutions in this discreet industry, which is always on hand when major loss events need to be handled.

www.swissre.com

And how did you decide on Mission Control Security Services?

We already had a cooperation arrangement in place with Open Systems and used the Mission Control Security Services to protect our central applications. When chatting with a member of the management team at Open Systems, I mentioned our problems and our expectations in terms of operations and security. After that, things started happening very quickly…

And was everyone happy with the solution?

Yes, partly because the pressure from the business kept on growing. Shortly before Christmas 2012, we had a workshop at Open Systems with the whole project team. The solution they presented featuring the proxy service managed by Mission Control impressed all of us. It already became evident during the meeting that we could stand firmly behind this solution.

The design for the Zurich location was then completed in two days. After a further eight days, everything was installed, commissioned and tested. I have never experienced anything like it in my 20 years in the industry. This gave me great confidence that we would get to grips with our proxy problem quickly and efficiently.

How did you set about migration?

The first step involved migrating the locations in and around Zurich. Out of business contingency considerations, we opted for a flexible migration path instead of a big bang. So we carried out migration to the new Mission Control security solution building by building, step by step. This had the big advantage that we could reverse changes at any time and without any major impact on operations. Unfortunately, this made migration somewhat more long-winded, mainly due to the countless special applications we deploy. Most of these applications and services are located on the internet and are protected by static IP filters. So we first had to deactivate these before updating them with the IP addresses of the new Mission Control security solution.

In a second step, we migrated the location at Armonk, USA. Thanks to the lessons learned from our Zurich location, this naturally went much faster. And we started work on the regional internet breakouts at the same time.

How are these spread geographically?

We now have regional internet breakouts in Australia, China, India, Switzerland, Brazil and South Africa, as well as on the east and west coasts of the United States. The users can surf the web through these locations. In terms of access to applications, we will end up with traffic engineering in the medium to long term, because access is more efficient or more reliable for certain applications via a different breakout. Even though we have no intention of allowing dozens of exceptions, it is worth taking a close look at the critical applications to see from where and to where access occurs. →

How satisfied are you with the Mission Control Services?

From the operational point of view, the Mission Control Security Services are very good. The Information Security Team was also fully won over by the operating organization, the technology employed and the Mission Control Portal with the clear division of roles and competencies, and the complete transparency and auditability.

Interestingly, we had quite different expectations with regard to the internal workload. We continue to rely upon internal specialists who carry out a pre-qualification of the incident tickets and change requests before passing them on to Mission Control Operations. We would actually have liked this to be taken over completely by the Mission Control engineers.

Do you think that you are now ready for further development?

I'm certain we are, because we now have a platform that is highly resilient as well as flexible and scalable. This means that in the future we'll also be able to meet growing demands in areas like unified communication and collaboration. We are increasingly employing cloud solutions (SaaS, PaaS, IaaS), video-conferencing and tools like MS Lync. This will likewise mean an increase in the necessary bandwidth.

I am personally convinced that the managed services model will become even more important for companies like Swiss Re: where the internal specialists can concentrate on the core processes and interaction with the business side. We need to identify the business requirements at an early stage in order to draw up and implement solutions promptly. We should simply not waste any time bothering ourselves with hardware or software. O

Swiss Re was formed by Helvetia General Insurance Company, Schweizerische Kreditanstalt (Credit Suisse) and Basler Handelsbank in 1863 following a terrible fire in Glarus. The company's sphere of influence has been global from the outset, with the major San Francisco earthquake of 1906 representing a big early test. Be it hurricanes, earthquakes or winter storms – Swiss Re has dealt with many natural catastrophes over the course of its history. But the company has also lived up to its responsibilities following disasters caused by people and dreadful events, like the terrorist attacks of September 11, 2001.

Over 14,000 employees at more than 60 locations

Listed on the Swiss stock exchange, SIX Swiss Exchange, the Swiss Re Group is today one of the leading wholesale providers of reinsurance, insurance and other insurance-based forms of risk transfer. The Zurich-based institution has a workforce of over 14,000 working at more than 60 locations through a network of Group companies and representative offices. The international clients served directly by Swiss Re or through brokers include insurers, medium-sized to large corporations and public-sector organizations.

Key contribution to social progress

Building on its expertise and ability to innovate, Swiss Re devises solutions that range from standard products all the way through to sophisticated client-specific insurance cover for all business segments. Thus, Swiss Re makes it possible for companies to assume costed risks, which is of vital significance to their success, and provides a key contribution to social progress. The traditional strengths of the company include disciplined underwriting and a circumspect investment policy. Furthermore, Swiss Re is in great shape for the future thanks to its outstanding capital base and the strength of the long-term customer relationships.

Holding structure with three separate business units

The Swiss Re Group adopted a holding structure in 2011. Three separate business units operate under a common roof: Reinsurance, Corporate Solutions and Life Capital. In terms of earnings, the Reinsurance business unit, which is responsible for conventional reinsurance business, is the largest segment at Swiss Re. It serves property and casualty, and life and health insurers. The Reinsurance business unit is divided into the two business segments of Property & Casualty and Life & Health, and generates around 80 % of the net premiums and fees realized by the Swiss Re Group.

Corporate Solutions, the second independent business unit of the Swiss Re Group, offers innovative, first-class insurance capacity for medium-sized and large international corporations throughout the world. Its offerings range from standard cover for risk transfer and multi-line programs through to highly individual solutions.

The third business unit, Life Capital, offers risk and capital management solutions under which Swiss Re acquires closed books of in-force life and health insurance business, whole lines of business or the entire capital stock of life insurance companies. Thus, Life Capital makes it possible for its clients to sell business units that are not part of their core business and hence to reduce their administration costs and to release capital.

For security, health and prosperity

Set up by Swiss Re in 2012, the not-for-profit Swiss Re Foundation has been tasked with strengthening the ability of society to deal with risks and challenges such as natural threats, climate change, population growth, drought and pandemics, and the promotion of security, health and prosperity. Additionally, the Swiss Re Foundation supports local, non-commercial projects at the company's various locations and voluntary work performed by company employees.