Top security at the price of a business lunch

Dieter Steiner is the managing director and founder of SSP Europe and an European pioneer in the managed security segment. In addition, the company has developed a highly secure file exchange platform out of the cloud, which has "more paying customers than Dropbox and Box.com" in the DACH area, as Steiner in the interview with monitor.at proudly betrays.

SSP Europe GmbH, headquartered in Munich, is developing cloud and IT security services, which are suitable for use at small companies and large international corporations. The SSP in the corporate name stands for "Secure Service Providing". The core products include among other things the "Secure Data Space", which offers a high-security data exchange platform from the cloud to both, private and business customers. The product portfolio also includes IT security services and solutions for firewall and intrusion prevention systems, spam and virus protection, remote access, IT services and solutions such as Hosted Exchange, Online Backup, Secure Data Space, to the point of performance providing, housing and hosting.

In the interview with monitor.at, Managing Director Dr. Dieter Steiner talks about his first touch points with the managed security concept, which advantages it offers and why small businesses should not feel too secure against cyberattacks.

Mr. Steiner, how did you get into contact with the subject of managed security?
Dieter Steiner: For this I have to go far back. I founded my first company in Regensburg in 1993. In the mid-nineties, we specialized in IT networking solutions. At that time the Internet and e-mail came up and we moved quickly towards IT security consulting. The companies wanted to access the Internet and we supported the companies locally with our know-how. The Managed Security Services came at the end of the nineties. At that time the companies have probably already purchased the hardware and software themselves, but specialized companies such as the SSP have taken over the management of the systems as external partners. Next came up this question: Why should companies spend a lot of money on hard- and software? Software needs updates, and hardware has to be renewed every two years. Why not going straight into a completely managed model? Our approach was to go into the colocation area of data center infrastructure vendors, where we set up professional security components, then connect the company sites to it, and then make a secured Internet breakout. This brings a huge range of advantages. We have implemented this in 2003. As a result, we have received the WAN and Security operation from more than 700 locations from the Bavarian Red Cross. This was the signal for us to build the infrastructure in parallel, thereby the service can be offered to many customers. It is completely irrelevant in such a company model, whether a company has three computers, or 3,000.

What problems, fears, or security concerns do customers have most frequently come to you?
This is the whole range of topics, that you can hear about the media: from data pioneering and industrial pioneering to hackers who want to make quick money. Above all, current fraud scenarios, for example, where someone as a boss issues and transfers in millions of dollars. As well as the excessive demand of users with the modern app world is a topic for us. To upload a photo of a business deal with a partner on Facebook to the private account is

one thing. But if I can then as a user no longer distinguish whether I can send sensitive company data over such channels - perhaps not Facebook but WhatsApp, Dropbox or as they all are called - then I come in a completely different dimension. Awareness for this difference among companies has been one of our tasks for many years. Many entrepreneurs have not yet understood that their greatest treasure is in form of data. Whether as a carpenter with a computer-controlled machine or in research and development. Getting to these data is extremely interesting for dubious characters.

How do the requirements of small, medium and large enterprises differ when it comes to IT security?
The damage is the same for every company and goes up to the threat of existence, whether I am a two-man company or one with 100,000 employees. The scenario of threat and interests are the same. Most small businesses think they aren´t interesting for attackers, without recognizing that over 90 percent of the scan and attack variants are automated and target public IP addresses. Every company, every device that moves on the Internet, has such an address.

What are the advantages of Managed Security - or, as you call it, Secure Service Providing?
There are several areas. Economically I do not have an extremely high investment cost, I can change into a subscription model, I have SLAs, I can book a replacement service, have a hotline and on request up to 24/7 service - and I can do it worldwide. If you figure out how many IT stuff you must hire, if you wanted to do something like this yourself, maybe even at several locations, you quickly see the cost savings potential. Technically speaking, a reputable managed security provider is always up-to-date. It can also react proactively to new attack waves. The next, and under the most underestimated topic is the legal. Topics such as compliance, data protection and data security up to the insurance protection play a decisive role. If I build a security solution today together with my own IT department and I am attacked - even if it is a new malware variant, see Ransomware & Co. - no insurance in this world pays a cent. But if I have sourced out that to an external partner, there is insurance protection up to liability damage level. Just this point leads back to the economic factor. That´s why I´m sure, that nobody will do anything about it. So I get top security at the price of no more than one business lunch per month, I am legally secured and I can face my partners with good conscience. As a supplier in the industry or in any industry, you need to adhere to certain safety standards. Finally I can manage this with a few Euros per month.

If I as a small company, either newly established or so far in security matters rather carefree, decide to tackle the issue properly, where should I start?
I must somehow plug into the Internet. That starts with the firewall. But you should not operate only with pure packet filters, but choose a firewall with appropriate intelligence. If I choose a security-as-a-service model, then the firewall can be quiet stupid because it only provides an encrypted connection to the data center. Then all traffic is protected by the data center and I can build the following security after the modular system: Enterprise Security for computer protection, a mail security solution for the gateway to filter viruses and spam, proxy, so that the employees do not accidentally rely on Dodge or God-knows-what land up to remote access or file exchange. A solid state-of-the-art security then starts at € 8 per user and month and goes up to € 12 or € 15. For this I can build a high-level security solution, which is high-performance and stable.

How long does it take, as a company with 20 users, to put a project on track?
If there is support, the organization is done, e.g. the access data from the internet provider, then it is done in a week.

Apart from "classic" security topics such as hackers, malware or espionage, you also deal with the handling of sensitive data in the company environment?
That's exactly why we developed the Secure Data Space. Since we combine for the user simple functionality with manageability and highest protection, which can be integrated into such a file exchange solution, for the company. Secured, but applicable. As a "hidden champion", we are not so familiar in the market. However, if we then become aware of the fact that we are strongly represented by OEM partners such as Hutchison Drei in Austria, Deutsche Telekom, Bechtle AG and many more, who are therewith selling their own product on the market under their own corporate identity, the picture changes.

Do these OEM partners operate the product in their own data center?
This is mixed. For example, Deutsche Telekom is making it for itself. For Hutchison Drei in Austria, we are doing business with the local provider Anexia. We are not only suggesting security here, but we are also looking closely at the fact that the data do not leave the national boundaries. The user can also decide for himself whether the client-side is encrypted again. If I use client-side encryption, we could also install the Secure Data Space solution on the servers of the NSA, because even at the current encryption level, they would need over a year to crack data fragments.

Is on your product Secure Data Space currently the focus of SSP Europe- apart from managed security? Is there the greatest demand?
Yes. We have developed a clear, customer-oriented enterprise file sync and share solution, with the experience that we have accumulated over many years. This is a solid foundation for our success. With our partner, we now have over a quarter million active, paying users with our partners together. With test accounts, there are more than 400,000 customers. The user numbers exponentially go up, the more the solution learns. In the DACH region, we have more users than Dropbox and Box.com.

To the person:
Dr. Dieter Steiner is the Managing Director of SSP Europe GmbH, headquartered in Munich. The engineer and promoted business economist designed SSP Europe's Security Service Providing concept and, with a team of technicians and engineers, became the managing partner of A.P.E. GmbH IT-Security. The development of the model began in 2004. At the beginning of 2008, Dr. Dieter Steiner founded the strategic business unit in SSP Europe GmbH. In his career, which began in the IT industry in 1993, Dieter Steiner has, among other things, introduced two IT system houses to the market and implemented numerous large-scale projects.

The original article can be found at
http://www.monitor.at/index.cfm/storyid/17013_Interview_-_Dieter_Steiner_SSP_Europe-Top-Security_zum_Preis_eines_Geschaeftsessens