Managed Network Security MSS-i

White paper

Markus Kaegi

Zurich, 20 December 2014

Play it safe:

Eliminate any worries about threats to your corporate network

Many companies face a dilemma: on the one hand they must effectively protect their IT and network infrastructure against cyber risks; on the other hand, they have increasingly fewer means at their disposal to do so. A growing number of companies are thus handing over the security of their IT systems and networks to specialised companies and in doing so get maximum security at a price they can plan into their budgets. Here a key motivating factor is that the security and stability of their networks, the available of central applications and communication between those involved are guaranteed 24/7. Only in this way is it possible to effectively protect central assets and data – from any company's perspective, a prerequisite for its long-term success. When working together with a security service provider it is thus important that its specialists monitor and manage the infrastructure on site around the clock. By doing so, these specialists can respond immediately to any incidents and more quickly avoid any possible damage.

The unhindered flow of information

The potential of threats to corporate IT infrastructures is growing larger and at a rapid pace. This is not something the security sector has simply made up. It is today's reality and is nothing terribly surprising. Trends such as the "Internet of Things" and "Machine to Machine", which not long ago were simply considered futuristic ideas, have already worked their way into our everyday lives. Social media, having meanwhile become a commodity, is our constant companion, and this not only in our private but also professional lives. Smartphones are being mass produced, and who can think of these devices without they many apps they now run? Further, given the high rate of technological development, we never get a chance to catch our breath. For instance, the "Internet of Things" is establishing itself into our everyday business world with great power and speed. The everyday objects we deal with are integrating ever more intelligence, and the resulting trend is an increase in the networking of all of them with each other. Today, there is hardly no limit to where information comes from and where it goes.

Quiet, efficient and unnoticed

Running parallel to this development has been a change in the situation as regards cybersecurity. Simple viruses, spread out extensively, will soon be a thing of the past. Attacks and threats are intelligent and have specific targets. A modern attack is aimed at a defined target and thus appears at just the right time at just the right place. It ends as fast as it came and thus is very difficult to detect. It uses multiple channels, whereby each channel by itself is absolutely clean – a threat arises only when both channels are put to use at roughly the same time.

Attacks are transforming themselves from unorganised and loud with effective impacts on media to quiet, efficient and unnoticed. Known methods of attack such as easily identifiable phishing attacks using spam e-mails have become passé. We now more frequently see attacks targeted as certain sectors such as banks and industry. E-mail spoofing is becoming ever more effective and tempts users, despite all efforts to warn them to the contrary, to click on a link in an e-mail or open an attachment.

Define what is worth protecting

Considering the multitude of threats and the wide prevalence of cybercriminal elements, we face a key question: in a world which is so dominated by digital technology, is it still possible to effectively protect our data, applications and systems? Even more important than the question of if there is adequate protection, though, is when and under which circumstances we must provide protection. The Swiss Air Force is fully capable of monitoring Switzerland's airspace around the clock; it has, however, defined that in practical terms this task must be performed only during office hours – primarily for budgetary reasons. Similarly, each organisation must ask when and where it wishes to have protection. How it achieves this protection can be reasonably determined only once these questions have been answered.

When the need for protection is established and the information to be protected is defined and classified, the next task is to determine where this should be performed within the overall system. Just a few years ago this was set at what is known as the perimeter – the interface between a corporate network (LAN) and the public network (WAN, Internet). A person or a computer was either located in the corporate network or was not. This situation of having a perimeter no longer exists in this pure form. Through innovations such as the cloud, the smartphone and other mobile devices, the perimeter no longer describes an interface but rather a zone or an area. There are two implications to this. First, there is less importance on security for a conventional perimeter. Second, there has been a basic change in the way corporations must improve their IT and Internet security. According to an online survey conducted by the University of Regensburg and the business association Bitcom, today every sixth company already gets its security services such as virus protection and user authentication from the cloud.

The result of all these clarifications is a security strategy which always reflects the individual situation. The requirements on information security can differ dramatically depending on the requirements of the company, security managers, the business sector, regulators and any other applicable stakeholder groups.

No matter what the security strategy looks like in each individual case, a factor of central importance is making a distinction between a security policy and actual security operations. Those who wish to implement a sustainable security policy which meets the needs of their respective companies must unify operations and maintenance, in other words: standardise. Once an infrastructure is set up based on the security policy, its operation must be defined and followed by unified processes. Only by doing so can the security level defined in the policy be maintained. More to the point, security is not a standard, but in contrast its practical operation certainly is.

In a standardised operation, all infrastructure components are maintained according to the same methodology, in other words following unified processes. This means, for example, that release and patch management must be clearly organised. Furthermore, keeping in mind the fast pace of changes, it must also be determined who defines, releases and then also implements and verifies changes. After all, the following is true for all complex systems: once an error has managed to sneak in, going back a step to fix it generally involves massive effort.

Compliance places demands on every aspect of IT

There is great pressure to attain conformity in financial reporting and corporate management. In fact, companies must observe a wide range of regulatory requirements: from tax law to antitrust and commercial law, from the basics of data access to the testability of digital documents, and through to Basel III. In all these cases, data security must always be observed. This wide range of regulations has an impact on the overall corporate IT infrastructure: virus and firewall scanners, e-mail and storage architecture, ERP and BI systems, solutions for disaster recovery and business continuity. Thus, compliance cannot be reduced to mere regulatory conformance. Much more, it extends from storage and conventional security through to business assessment and reporting systems, from e-mail filters through to physical access security. In this respect, compliance is a task which cuts across all parts of a company and is a central element of security.

Considering these challenges, those who wish to play it safe are well advised to work with a partner who adheres to national and international norms and is also certified to meet standards such as ISO 27001 and ISAE 3402. It is just as important to observe recommendations issued by the Swiss Financial Market Supervisory Authority FINMA and the Swiss Federal Act on Data Protection. And because compliance never ends, such a security partner should be audited every year by an outside organisation.

People and machines continually in organised harmony

Once the basics for a standardised operation are established, the next task is to determine what is specifically needed in actual practice. Here the focus is on the division of tasks among machines (the technical platform) and people. There is no doubt that a machine – as long as it is properly configured – can perform important tasks in the implementation of a security policy. It can recognise and handle all standard cases based on known patterns. The more powerful it is, the higher the level of quality as well. However, as soon as a machine has reached its performance limits, there is the need for people who take action with analyses, assessments and responses.

As difficult as it might seem to exactly define the interplay between machines and people in specific cases, doing so is of central importance. Fundamentally, such a division of tasks presumes that machines will handle virtually all standard cases. People then get involved only in those cases where a machine is not able to proceed further. The result is that people must always be available who are able to respond quickly and address specific needs. The model of on-call service which many people rely on is no longer adequate. Instead, we much more need solutions which manage the interaction of people and machines around the clock. Just as indispensable are well-running processes and tools which keep everything operating together. There can be no high degree of maturity in security without people, whether this means an operator or an analyst. This, however, also ensures that people always get interesting assignments because machines handle routine tasks, anything that can be automated.

Service providers for security

Only one solution approach can deal with the wide-ranging catalogue of requirements and challenges. The security policy stipulated by management must be provided by a specialty department as a managed service. Here companies have two options: They run an in-house department staffed with a sufficient number of well-trained personnel who can handle service tasks in a professional manner, around the clock and according to plan. Or they decide to hire an external partner, a service provider for managed security. By outsourcing to external experts, companies profit from additional expertise in this area, and thanks to the benefits of scale they also gain from the experiences of other companies. Outsourcing does not in fact lead to an outflow of knowledge and expertise but rather to the acquisition of additional know-how into the company.

High quality through threat intelligence

In each case, a professional security advisor requires a corresponding management platform. There is a wide range of such platforms on offer. They are available in every price category and with a baffling variety of functions and features. Because the extent of the services provided is constantly changing and developing, you must keep several things in mind when selecting a platform which can intelligently detect attacks.

Key importance is placed on actively making high-quality correlations. One tool for doing so is known as threat intelligence. This involves specific expertise and a digital library (threat library) in which various content is received from a wide range of sources: proprietary feeds as well as those from public and governmental sources. In addition, there are in-house feeds, which in the case of Swisscom play a key role – nobody is more familiar with the Swiss network than Swisscom. Information about threats which are recognised on the Swiss network are integrated immediately into the service intelligence.

On the other side, the security engine is fed with log information: logs from the security infrastructure in each company but also logs from customer systems. The more information which is available about the system environment, the more precisely you can draw conclusions. When they analyse logs, service providers such as Swisscom Security Devices – which manages systems both in Switzerland and abroad – learn about specific events around the world, which ultimately benefits all customers.

The Swisscom security platform continually compares customer logs to the various feeds. If an attack is detected, an alarm is issued. If there is a unambiguous match, defensive measures are taken immediately. Every recognised incident enhances the policy, which leads to an increasing number of safety threats being automatically recognised and handled. In the case of the Swisscom platform, updates take place hourly during running operation. In addition, a team of analysts keeps the threat library up to date.

When it comes to management platforms, it helps if the policy for every customer is identical to a large extent. In this way, customers who have not been subject to an attack can “proactively” profit from attacks on other customers. Even so, there must be the ability to design a policy so that an amount up to five per cent is tailored to a specific customer. This ensures that customer-specific requirements are covered without losing the economies of scale.

Security with a Swiss guarantee

Of course, security is only ensured if all the components in a system have the same level of quality and interact in union where they are all matched to each other. To clarify this situation, it is recommended to conduct an analysis of the current situation. This provides answers to questions such as “Which services can the company supply itself?” and “For which tasks does the company need a partner?” Only after such questions have been answered is it time to select a suitable partner.

Companies rely on having their systems, applications and data constantly being available in the desired state. Only experts can ensure this is the case. When transferring security to a company with the corresponding level of expertise, this also means that customers can profit from the economies of scale. Given this background, with MSS-i Swisscom has developed a flexibly scalable service which consists of a number of modules which can be combined to meet specific needs:

- **Managed VPN** so that your local branches don’t miss the connection
- **Managed Firewall** so that not just anybody can access and leave your sites at will
- **Managed IDS** making you the first to know when you have unwanted visitors
- **Managed Web Security/Proxy** allowing your employees to surf securely
- **Managed Mail Security** allowing you to receive and send e-mails securely
- **Managed Web Application Firewall,** preventing your applications from turning into self-service shops
- **Managed WAN Encryption** preventing your competitors from listening in

As one of the leading suppliers of managed security in Switzerland, Swisscom operates its own Security Operations Centre which is staffed around the clock. A disaster-proof site in Switzerland, georedundancy, a multi-level physical security concept and the redundant layout of power, network and system components – all these together guarantee the highest level of availability. At the same time, you can rest assured that regulatory and sector-specific compliance requirements are always met.

At Swisscom, security experts work on-site 24/7 to ensure that each customer's firewall, VPN, IDS, web and mail security plus WAN encryption always function flawlessly. These experts work according to clearly defined processes and assignment of tasks. In addition, guidelines, process plans and checklists mean they follow reliable procedures in case of emergencies. Companies thus have access to the expertise of security specialists at all times. Further, a Security Dashboard offers them a realtime overview of all security-related issues and events in their company.

The extent of a typical managed security service

A managed security service such as what Swisscom offers covers the following components and services:

- Binding, measurable and guaranteed services (KPIs – key performance indicators) which are set down in a Service Level Agreement
- Security Operation Centre which is staffed around the clock (24/7) by security analysts – in other words, not simply on-call services
- Security information and event management for the realtime analysis of security-related incidents
- Active scanning of networks, servers and databases as regards vulnerabilities
- Notification service in case of threats and vulnerabilities
- Log management and analysis
- Reporting in conjunction with monitored/managed systems or system components and security-related incidents

Your contact

Markus Kaegi

Security
Product Marketing and Management

e-mail: markus.kaegi@swisscom.com

The author has more than ten years of experience in the information security sector. He has been with Swisscom (Schweiz) AG since 2009 in the Enterprise Customer Division as a product manager responsible for Managed Security Services.