

Background Article

IT security as a success factor: Key to the successful integration of East European branches

Many Austrian companies are finding new opportunities in the markets of Eastern Europe. Since the collapse of communism, the majority of countries in Eastern Europe have developed at an impressive rate. Macro-economic stabilisation, robust growth and rising living standards are the result of a successful, radical transformation process. In spite of the marked tendency of the global economy to treat Central and Eastern Europe as an export market and investment target, Austria's business community continues to be at the forefront in this region.

Austrian companies and firms which decide to access the Eastern European market are often faced with the task of securely integrating their geographically remote branches into their existing network infrastructure. After all, critical data, applications and processes are exposed to countless security risks during everyday business. Innsbruck-based phion AG, which is one of the leading specialists in Europe in the protection of company infrastructures and branch networks, describes here, based on its long years of experience, the key challenges in this area. This issue is not only about offering protection against hackers and malware. Being part of a secure branch network also means maintaining the various sites' productivity in adverse circumstances.

Limitless danger: hackers, malware and web-based threats

The image of the ingenious hacker or virus programmer at work in their bedroom is long gone. The threat nowadays comes from the most highly organised criminal networks which are looking to steal and use sensitive data. The geographical location of the target is of little importance in this case. Branches in Eastern Europe are facing the same dangers as the branches in Austria. This means by implication that these locations must be integrated into the company-wide IT security infrastructure with the same care and functionality provision.

The main priority in this case is the integration of a firewall/VPN gateway, which monitors incoming and outgoing connections and encrypts any company communication sent via the Internet. This can also help prevent hackers gaining access to the company network via the branches, along with solutions for intrusion detection/prevention. The ever-growing torrent of viruses, worms etc. also means that Internet and email traffic on the gateway must be scanned in real time in order to block malware and spam before these threats reach the user's mailbox.

Specialised products are available for all these tasks – and this is where there is a problem. The lack of integration between the various security solutions means that gaps occur between them, which are currently being deliberately targeted by attackers using a variety of methods. In particular, the new generation of flexible web-based attacks are presenting challenges for traditional standalone solutions. For instance, a simple link in a spam email can lead to a manipulated website, which in turn facilitates the automatic and unnoticed download of spyware, key loggers, backdoors etc. All the links in this infection chain can be modified, updated or replaced at any time by the attacker, making it extremely difficult to recognise them.

Malware developers have also had to come up with ideas for the follow-up communication with their malicious codes. This is where protocols such as HTTPS or XML-based web services are being used as they cannot be scanned by many security solutions.

Another form of effective protection also used therefore is to filter known websites as being potentially dangerous, ideally using a database which is as extensive as possible and constantly being updated. It must also be guaranteed that all the data traffic, including HTTPS- and XML-based traffic on the gateway, can be scanned for dangerous content. Ideally, an automatic check should also be carried out here on the digital certificates which websites use to prove their reliability. Other positive contributions to safety and productivity can be achieved

if the gateway also regulates applications just as popular as bandwidth hungry applications for instant messaging, peer-to-peer file transfer and Internet telephony.

Access control protects against attacks via the backdoor

In addition to the gateway, there is another component worthy of a particularly close look: endpoints, such as laptops or desktops. It is typically at endpoints where the actual work is produced, which means that they contain a horde of sensitive data, making them a much sought-after target. Precisely because of the growing mobile workforce, a particular security risk is posed at the endpoints as it is often difficult to ensure total implementation of company-wide security guidelines. Staff often disable, for instance, the installed security solutions in order to use low-cost WLAN hotspots in hotels or at airports or establish a direct connection to private devices using Bluetooth. If an infection occurs during all this, it may possibly be snuck into the network the next time company resources are accessed.

The only method to help counter this is to control the endpoint before and ideally also while the connection is being established with the company. This access control can be achieved using a number of different technical methods. For instance, it is possible to establish integration at network component level, including for instance routers. However, this may require considerable investment and implementation effort not only with existing networks.

Providers like phion are following another route. In this case, access control is carried out via an appliance along with client software installed on the devices. Only if devices comply with the company's security guidelines (i.e. the latest version of firewall and antivirus software is installed) will access be permitted to the network. The security specifications for this can be defined centrally and distributed to all endpoints, which offers considerable benefit, particularly in infrastructures distributed across the whole of Europe.

Unified Threat Management = total solution in a box?

Companies which embark on an assessment of the market based on the requirements specification described above will inevitably come across the concept of Unified Threat Management (UTM). UTM is a security concept which is aimed not at isolated standalone products but at the widest possible integration and interoperability among all security components. The obvious benefits from this lie in better harmonisation of the individual security aspects and the significant improvement in the overview of the infrastructure, which only allow complex, far-reaching processes to be carried out in many cases.

However, numerous providers wrongly use UTM as a synonym for appliances, i.e. "all-in-one-box" network security products. Using these appliances can provide a sensible solution when establishing a branch network in particular. In many situations, however, UTM should be understood as a concept whose aim is to implement a unified security strategy for the entire IT infrastructure, which is administered centrally. Specific implementation is then determined by the individual situation of the company.

But one absolute must is to integrate all security products under central management. The reason for this is that in large environments with multiple sites, this can otherwise lead to configuration and operation costs rising not proportionally, but exponentially in relation to the number of systems. Consequently, administrators from head office must have the facility to monitor the status of branch gateways, administer configurations and software, define global rules and record data from one or more gateways.

Centralised configuration management should include as part of this not only VPN and firewall policies, but also parameters such as software licences, as well as support remote disaster recovery. Centralising management in this way has the additional effect of being able to restrict to a minimum the group of people in the branches with security-related knowledge.

Communications infrastructure still in the development phase

After security, connectivity is the second main priority in establishing a branch network. Just as there has been an upturn in the economy, this has had a positive impact too on the development of the communications infrastructure in many East European countries. But the standard achieved by the Western European countries has still not been reached yet in every region. The coming few years will bring even further harmonisation as the new Eastern European EU member states have to open up their telecommunications markets and the EU also subsidises the development of broadband infrastructures.

At the moment, while integrating their East European sites into their networks, Austrian companies are continually facing the problem that connection lines are significantly less reliable and connection types such as xDSL are not available at all outside the major cities or only with restricted data transmission rates. Added to this are unforeseeable events, including power cuts, wrong configurations from the provider, damage caused by building work and even natural disasters. These risks are actually not restricted to Eastern Europe, but are certainly the order of the day too in Western and Asian industrial areas.

The risks for business continuity are obvious. If central applications, such as ERP or CRM systems, are difficult to access, if accessible at all, due to a line failure, this may mean that whole branches will be sitting idle. The damage caused gets worse if the locations affected are production sites which are integrated as part of a Just-In-Time production process. When it comes to integrating their East European locations into their networks, companies must therefore pay particular attention to the fact that the productivity of their branches is still maintained, even in adverse circumstances.

Intelligent response to unforeseeable problems

In order to minimise the impact of the problems described above, it is recommended using a technology for which phion has coined the name “traffic intelligence”. As a permanent fixture in state-of-the-art security solutions, the task of traffic intelligence is to ensure that, as soon as data traffic stops flowing, the

system automatically switches between different lines and ISPs.

Bearing in mind in particular the East European infrastructure, traffic intelligence offers the benefit in this situation that the entire range of connection types can be used, from frame relay and leased lines, xDSL and ISDN to dial-up, UMTS or even satellite uplink. Unlike other supposed failover solutions, traffic intelligence also takes care of automatically switching back to the primary connection if the fault has been repaired. Otherwise this aspect can turn out to be a major expense if ISDN, for instance, is used as a backup line. Outside Western Europe ISDN flat rates are not extensively available, which means that if the opportunity to switch back is missed, this can quickly run up costs amounting to several thousand euros.

The adjective “intelligent” can also only apply to security solutions which give priority to different types of data traffic. If this component is missing, this can easily lead to situations where the backup line is occupied by people surfing the net while business-critical processes grind to a halt. Traffic intelligence must therefore have bandwidth management integrated as part of it so that data can be distributed via the available line capacities in order of importance. But even all this is not enough. Further challenges are emerging as a result of the growth of applications being used and the growth of application data traffic resulting from this. Data traffic compression is also used to achieve optimum use of the available bandwidth in WANs in order to speed up response times and reduce the load.

BOB - the Branch Office Box

The specific challenges posed by integrating branches in a network have obviously not escaped the attention of manufacturers who have been involved for some time in promoting the concept of the Branch Office Box (BOB). By integrating the key functions in a single device, the requirements of the branches should be covered with this single solution, which also means minimal rollout effort. What exactly a BOB needs to do to meet the high expectations is explained by the manufacturers, depending on their own area of expertise and technology portfolio. According to the sales argument presented by phion, at

least the key requirements of application and connectivity optimisation, as well as security must be seamlessly integrated so that companies can fully leverage the technical and economic potential of the BOB.

In particular, there is a clear difference of opinion about integrating security functions into the BOB. But if this is not done, dedicated security solutions will have to be implemented in the branches, which in turn incurs costs and management time and goes against the spirit of what a BOB is meant to do.

Summary

Integrating branches in Eastern Europe does not require any more or less security than integrating branches in Austria. It is not acceptable to downgrade the security level in view of the growing threat situation, no matter how small the branch is. In particular, attention is also being focused on maintaining connectivity and maximising application performance as these factors determine the productivity of all the locations. Finally, centralised management promotes technically and financially efficient management of the infrastructure and makes it easy to expand the infrastructure with the business's continuing success.

About phion

phion is one of the leading European providers of solutions to protect company communications. With the netfence product portfolio phion offers solutions for the most demanding standards in terms of availability, security and management. netfence appliances consistently address all security-related aspects: From perimeter defence to the safe and highly available connections to branch offices, right up to blocking dangerous contents and protecting internal networks. airlock protects web applications like e-banking platforms and web services from any attacks or misuse.

All phion products have core management and are distinguished by their remarkable TCO.

phion is listed at the Vienna stock exchange (symbol: PHIO) and is based in Innsbruck, Austria and Zurich, Switzerland. phion's customers include well-known, internationally operating companies from all sectors of industry.