HOB Cyber Security

HOB Solutions at Work

My Home Is My Castle!

A Forsa survey carried out in Germany on behalf of the BITKOM group shows that two-thirds of the respondents would prefer to work at home. Thanks to the ubiquitous nature of the Internet and technologically mature remote access solutions, also for communal and other governmental networks, this desire is easy to fulfill, bringing with it many benefits for all involved.

Klaus Brandstätter, CEO of HOB GmbH & Co. KG, discusses the technical and economical advantages and drawbacks of the most important types of remote access solutions that provide employees with convenient access to their communal data and applications – without compromising on data security and privacy laws.

A large majority of Germans, according to the survey, want more flexible working conditions, to which the possibility of working in a home office belongs. Two-thirds prefer to work regularly at home and about 50% would like to like to work at home several days a week. And 17 percent prefer working in a home office to working at the corporate offices. This desire is especially strong with 80 of those between the ages of 30 and 39.

IT-workers also place great value on freedom and flexibility: A CIO online survey showed that the respondents want a clause in their employment contracts providing them with a home office, more so than a company car. This is a result that is also backed by a study from the personnel consultancy firm Watson Wyatt, which found that 51 percent of the IT employees say that a home office is very important to them.

There is a wide range of reasons for this: Different biorhythms of „owls“ who like to work at night and early-rising „larks,“ or better coordination of professional and family life to optimize the work-life-balance.

In the Interest of Employers

When their special interests are provided for, the employee‘s satisfaction, and with it motivation, are increased. This is especially true in the public service sector, which cannot be so generous with financial incentives. In view of Germany‘s aging demographics, this is also important: The earlier employees can align their desire to have children with the need to retain their job, the earlier they will then have children. Progressive employers therefore offer women and men the possibility of working at home during their parental leave, thereby retaining their valuable capabilities and, in many instances, years of experience. High workforce fluctuation, delayed projects and other drawbacks can be prevented and the cost of recruitment and training of new personnel minimized. Besides facilitating smooth workflows, this also has positive effects for the entire economy.

In addition to the desires of individual employees, the actual necessity of comprehensive service from support workers, e.g., in municipal computer centers, is another reason for flexible working hours and locations.

Implementation

The solution for these requirements and scenarios are remote workplaces, such as the association Kommunale Datenverarbeitung Region Stuttgart (KDRS - Municipal Data Processing for the Stuttgart Region) provides for its staff and associate members since 2002. The municipal data processor for Reutlingen-Ulm, in Bavaria, also offers over 800 members and customers from the public and private sectors flexible, secure Internet access to their data and applications for their home-users, administrators and service employees.

Thanks to modern technology, this is not a problem – quite the opposite: In many cases the use of home offices or the outsourcing to freelancers who are completely integrated into the corporate infrastructure results in considerable cost savings.

Which Type of Access is Best?

These days, the technical requirements for secure remote access are no longer a problem: Almost everyone has one or more PCs or mobile devices that are connected to the internet. When on the road, most employees have their laptops or a smartphone with them. In an emergency, there are always Internet cafés or the computer in the hotel lobby which can be used, e.g., to check e-mail.

The two methods of access, over your own PC or or one in the hotel lobby, do not work in the same way: Whereas on your own hardware you can install client software, on a third-party‘s machine this is often not possible. Therefore, when selecting the type of remote access to use, you have to proceed strategically and carefully weigh the pros and cons.

When dealing with public agencies where much of the data being processed is personal data, privacy protection and data security should be in the center of these deliberations. Practicality, ease of administration and cost are, of course, also to be taken into consideration. Security is a primary concern because the Internet brings with it not only the advantages of rapid communication, but also the risks of security breaches, e.g., in establishing the authenticity of the communicating parties and the integrity and confidentiality of the data. To ensure this security, the user has to take suitable measures.

The two most widely accepted and deployed methods for secure remote access over the Internet are IPsec- and SSL-based solutions, which differ mainly in the encryption standard used. The question is, which of these solutions is best for your enterprise?

Complete Network Access Over IPsec VPN

A widely accepted solution is the IPsec VPN, standardized in 1998 and using the protocols IPsec for encryption and IKE/ISAKMP for authentication. The name VPN (Virtual Private Network) itself implies that this solution provides the user with their own secure network even through the Internet. IPsec works on the network layer (Layer 3). It thus provides an infrastructure for all IP protocols and is transparent for all transport protocols based on them, as well as applications, e.g., Voice over IP.

Contrary to the popular opinion that IPsec VPNs and the administration thereof are complicated, there are solutions, such as HOBLink VPN Gateway and HOBLink VPN Anywhere Client, that are simple to implement with central installation and administration. A „Silent Client Installation“ is used for this: During a company-wide rollout, the central administrator creates a client CD that, after being booted, automatically installs all the desired features, rules and add-ons. Alternatively, the client can just be downloaded from a web server. The user just needs to run the client software without any need for administration- or installation rights. After the client started, the user just needs to type in his username and password and can then log on to the corporate network and, depending on the rights given him, directly access his data and applications.

However, with IPsec data packages are sent that, in certain network infrastructures, cannot reach their destinations. This is due to the fact that some, usually inexpensive, components do not support the IPsec protocol.

Multifunctional End-to-End Connection via SSL

Another generally accepted and, according to IT experts, quickly spreading method used for secure remote access is that of SSL VPNs, using the TLS (Transport Layer Security) protocol. This method establishes a connection on the application layer, which works in any environment and is only blocked in very few instances.

HOB‘s solution, HOB RD VPN, combines an SSL VPN with a performant Java client for remote computing, providing users with secure remote access from one package. With HOB RD VPN users have easy and secure remote access to the data and system for which they are authorized – including their desktop PCs in the corporate infrastructure. The major advantage here is that the client machine requires no client software installation, no special drivers nor does the user need to have administrator rights. All that is required is a Java-capable browser. The first time a user accesses the target site, the browser downloads a Java applet and starts the application. The applet remains in the cache and is checked to see if it is the latest version at each subsequent connection. Complete network access over HOB‘s SSL VPN solution is also possible; to achieve this, the HOB PPP Tunnel is used.

Authentication System for Additional Security

To meet the high security requirements of, e.g., the public sector, SSL VPN's also need an authentication system. With such a system, all connection attempts to the corresponding networks or network components are checked for authorization and identity with user name, password, alphanumeric tokens and RADIUS . Rights administration can be saved in almost any type of database.

Conclusion

For many governmental agencies whose employees work from home offices or small branch offices, or who want to interconnect a number of municipal offices spread out over a state or region, providing their staff with secure remote access to all data and applications they may need, an SSL VPN is often the most secure and economical solution.

07/2016 TE