Rohde & Schwarz Cybersecurity

HOME OFFICE SECURITY

Work from home cybersecurity:
what enterprises need to know now

ROHDE&SCHWARZ

Make ideas real

CONTENTS

WORKING SECURELY AT HOME

Security awareness in the home office

Crises offer enormous opportunities for public authorities, and especially for enterprises, to accelerate their digital transformation. Numerous paper processes must be digitized, with home office, bring your own device (BYOD) and cloud applications acting as helpful drivers. A study carried out by the industry association Bitkom concluded that "nine out of ten enterprises recommend working at home, and two-thirds of them have even made this mandatory."[1]

These opportunities for IT security are often accompanied by the challenge of converting the corporate IT infrastructure to remote access virtually overnight. As a result, many public authorities and enterprises find themselves in a sort of accelerated digitalization process because their employees are all working at home – a situation that very few of them are sufficiently prepared for.

Security can suffer when new digital processes, technologies and applications are not yet well established. This guide is intended to provide an overview of how to securely fashion work from home and optimally deploy time and resources to defend against cyber threats and weaker (broad) perimeter protection. In home offices as well, information security should always have the highest priority.

"Digital technologies allow us to work independent of place and time. Home offices will become common practice for more and more employees."
Bitkom CEO Dr. Bernhard Rohleder[2]

[1] https://www.bitkom.org/Presse/Presseinformation/Digitale-Wirtschaft-schickt-ihre-Mitarbeiter-flaechendeckend-ins-Homeoffice (German only)
[2] https://www.bitkom.org/Presse/Presseinformation/Vier-von-zehn-Unternehmen-setzen-auf-Homeoffice (German only)

Enterprises should define and apply security strategies for every remote employee – whether permanent, external (fixed freelance), partner or service provider – in order to fulfill their business objectives, remain productive, and minimize the risk of cyberattacks.

IT security should never be so complex that your employees are not able to apply individual measures. Especially now, it is important to strengthen awareness of digital security because phishing attacks are on the rise. Attackers may take advantage of the current situation, so you must be especially alert to phishing emails and fraud.

Encourage your organization to take suitable strategic and process measures to remain resilient against heightened attack scenarios due to localized work arrangements.

Localized work forms an ideal basis for a variety of attack scenarios, from outdated technical infrastructure that is not secured by the corporate network, insecure router and WLAN connections to unencrypted data storage media, to CEO fraud, ransomware and classical phishing emails. Employees have a greater need for information, and at the same time organizations must raise their security awareness.

Create awareness of attacks: point out CEO fraud in particular.

PHISHING EMAILS, MALWARE AND RANSOMWARE: WHICH CYBER THREATS SHOULD YOU ESPECIALLY DEFEND AGAINST NOW?

There are more and more reports of fraudulent bulk emails[3] supposedly originating from banks, credit unions, or online mail-order merchants. Even in times when many employees worldwide are working at home, cybercriminals are trying to obtain unauthorized access to bank accounts, data and information.

Masquerading as offers of assistance or notifications of modified security measures; their messages conceal classical phishing emails, which are also being sent now with requests to enter data such as email addresses, account details or passwords on fake web pages, leading to the installation of malware.

Special caution with email from supposedly official bodies with file attachments such as PDF, docx or mp4.

These attachments are claimed to contain relevant security information, but when they are downloaded they install malware that encrypts data to block access to the user's endpoint and the corporate network. This sort of email phishing is still one of the most successful attack tools of criminals, and the current rise in these attacks poses a global threat.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html (German only)

CASE EXAMPLE:

An attack on the University Hospital of Brno in the Czech Republic became known a few months ago[4]. The attack on the hospital network was unfortunately so successful that it would probably take weeks to restore normal operation. As a result, all computers had to be shut down, operations canceled and patients transferred to other hospitals. Hospitals, like other critical systems, are especially attractive attack targets because maintaining their operation has high social relevance.

Ransomware attacks[5] on enterprises in the healthcare sector in the USA alone affected 764 healthcare providers[6] in 2019, resulting in unavailability of the emergency number 911 and cancellation of surgical procedures.

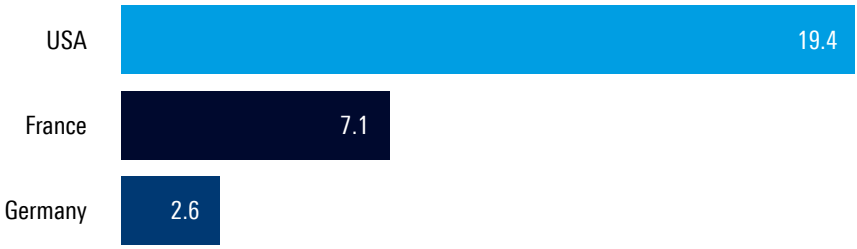


Fig. 1:

According to statista, the financial damage of cybercrime in 2017 was billions of US dollars[7]

[4] https://www.behoerden-spiegel.de/2020/03/17/tschechisches-krankenhaus-lahmgelegt/ (German only)
[5] https://www.kuppingercole.com/blog/balaganski/ransomware-during-the-pandemic-crisis
[6] https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
[7] https://de.statista.com/themen/1834/internetkriminalitaet/ (German only)

Remote access to the corporate network

The increasing number of people working remotely with mobile access to corporate and government networks poses a special challenge. Capacity problems can throttle system performance, and ultimately reduce IT security.

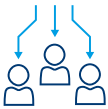
A software-based security suite is the ideal way to fully protect laptops and mobile endpoints linked to corporate IT systems, since it does not require the procurement of new hardware or specific retraining of users.

IT security for every employee:
a software-based security suite is the ideal solution.

WORK FROM HOME TIPS TO INCREASE THE IT SECURITY OF YOUR EMPLOYEES

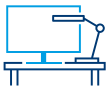
1. Inform employees about IT security and data security

Clear and binding regulations regarding IT security and data security should be communicated immediately in writing to all persons concerned.



2. Designate unambiguous communications channels and contacts

Clarify responsibilities and contact persons in the event of loss of components and reporting paths. These communications channels should be known to all employees and be verifiable by the employees.



3. Physical home office security measures

Employees should be urged to personally take specific security measures when working at home as well as in the office. This includes physically safeguarding the workplace against attack, which means locking doors and blocking screens. It is also advisable to cover the webcam on the desktop computer or laptop and position screens so they cannot be seen from outside.

4. WLAN and password security in home offices

Secure your home WLAN by changing the default administrator password, activating WPA2 encryption and using a strong password.

5. IT security: watch out for phishing and CEO fraud

Create awareness of attacks aimed at obtaining information and data that contain references to passwords, bank relationships, or access to systems or applications. Draw particular attention to CEO fraud.

Social engineering poses the biggest risk in the home office environment.

Attackers misrepresent themselves and use tricks to induce incorrect employee behavior. Email phishing is part of this, but special caution is also important with phone calls, text messages, social media content and fake messages via messaging services used for collaboration in company applications.

6. VPN – secure communications in the home office

Use secure communications channels to access corporate resources. Where possible, use virtual private networks (VPNs), which act as agents to establish connections from the user's endpoint to the corporate network though a secure tunnel.

7. MFA and 2FA – secure passwords for secure applications

Secure passwords provide additional protection against unauthorized access to applications. Establish complex and unique passwords, and additionally use a multi-factor authentication mechanism (MFA or 2FA). Passphrases are good passwords because they are as long as possible, complex, and use unpredictable terms or sentences. “We encrypt data storage media!” or “do not link cells in Excel” are examples of passphrases.

Both are strong, contain many characters and are easy to remember and type, but they are difficult to hack. Augment them with symbols, numbers or uppercase letters. If you need a unique password for each of your required applications, it is advisable to us a password manager, which is a program that saves passwords in a sort of safe and automatically retrieves them when needed. And unique passwords are fundamentally advisable. Otherwise an attacker only has to succeed in compromising one of the websites you visit to access all of the passwords – including yours – and then simply log in to all further accounts.

At haveibeenpwned.com you can quickly check whether email addresses have been compromised.

If you use a password manager, you should protect it with a strong password and two-level verification.

8. Updated operating systems, web applications and apps

Ensure that all used technologies are up to date and that updates are implemented regularly. Employees should always work with the latest system version.

9. IT security with localized working at home

Regard laptops, company mobile phones and other resources, such as files and internal resources, regardless of their location, as what they are: simply resources. Sensitive company data remains sensitive no matter where it is, and controlled access to endpoints must always be maintained. Ensure that your screen is not visible to other persons. Always lock the screen when you take a break, to foster acting with data awareness and in the interest of corporate security at home as well as in the office.

Or in the words of the German Federal Office for Information Security (BSI): “Make sure unauthorized persons cannot view or access your data,” which also applies to posting information on social media. Remember that your social media postings from your home office often contain small clues that help people recognize where you live.

Postings with information such as location identifiers or position data give both strangers and acquaintances, and possibly also dubious persons, an opportunity to learn where you and other family members are. The BSI also offers information for citizens, such as a service phone number where private individuals can ask specific questions about IT security. The current focuses[8] include “Secure digital learning” and “Getting started with video calling”.

[8] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/digital-vernetzt-in-corona-zeiten.html (German only)

SECURITY: NEVER OPTIONAL, ALWAYS APPLICABLE

Secure communications over various sites

When employees access applications or systems from remote locations, communications between the devices must be secure, either by means of protocols such as HTTPS or through a corporate VPN.

Secure access to corporate applications from the home office is a decisive factor for remote employees. An optimal solution for identity and access management that automatically provides (authorized) remote employees with suitable access methods and technologies is helpful in this regard.

The principle of least possible privileges applied here means that only the minimum authorizations needed by an end user, an application, a service, a task or a system to perform the assigned task are granted. This prevents "overprivileged" access by users, applications or services, without impairing productivity or involving the IT department.

Hybrid, public or private cloud – or should you choose SaaS?

If you and your employees must all be able to access business critical systems, applications, infrastructure and data from home offices, in some cases a hybrid scenario may be suitable, in which some of the business applications are hosted directly on site or in a corporate data center and others in a private or public cloud, or the applications are based on software as a service (SaaS). Depending on the appropriate model, it is always critically important that persons working remotely can always access the necessary business applications independent of their personal location.

Checklist for secure access and applications in the home office

1. Set up VPN solutions that can also maintain a large number of simultaneous connections
2. Provide options for secure video conferences with stable audio and video functions
3. Ensure that business applications can only be accessed through encrypted communications channels (SSL VPN, IPsec VPN)
4. Use multi-factor authentication mechanisms on corporate application portals

In the current situation you should be especially alert with emails that ask you to check or update your access details. Even if they appear to come from a trustworthy source, try to verify the authenticity of the sender.

Do not click on suspicious links, and do not open suspicious attachments.

Be especially alert with emails from people you do not know that ask you to follow links or open files. In case of doubt, report these requests to your security officer.

5. Use only secure connections to send sensitive corporate data (e.g. by email)
6. Be especially careful with emails related to the Coronavirus or Covid, since they may be phishing attempts or frauds
7. If in doubt about the legitimacy of an email, always contact your security officer
8. Data at rest (e.g. on local drives) should be encrypted to protect it against theft and potential loss of the device
9. Do not distribute the URLs of calls or conferences via social media or other public channels, to ensure that only authorized persons can access your corporate meetings

SECURITY SOLUTIONS BY ROHDE&SCHWARZ CYBERSECURITY FOR HOME OFFICE SECURITY

Thanks to a broad portfolio of IT security solutions from a single source, Rohde&Schwarz Cybersecurity is your reliable partner for secure remote workstations of your employees.

Solutions for network security

R&S®SITLine ETH – Ethernet encryption for secure data transmission

The Ethernet encryptors of the R&S®SITLine ETH family protect enterprises against espionage and manipulation of data transmitted via Ethernet over fixed network, wireless or satellite links. The encrypted throughput can be increased up to 40 Gbit/s per device by means of a software upgrade with no need to exchange hardware. The devices combine easy administration (including separated network and security management) with a compact form factor and low system costs. They are BSI approved for classified communications at German and NATO RESTRICTED security levels.

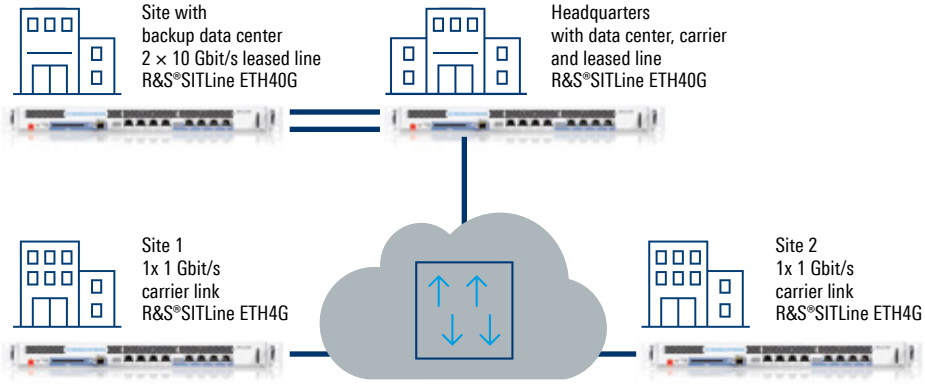


Fig. 2:

Preconfigured encryption for leased lines that automatically establishes encrypted Layer 2 connections over fast Ethernet

R&S®Trusted VPN – your IPsec encryption gateway

The solution consists of a VPN gateway that can be provided to individual sites in different variants, along with a central management station. Highly secure remote access to corporate resources is possible at all times with this solution, which is approved by the German Federal Office for Information Security (BSI).

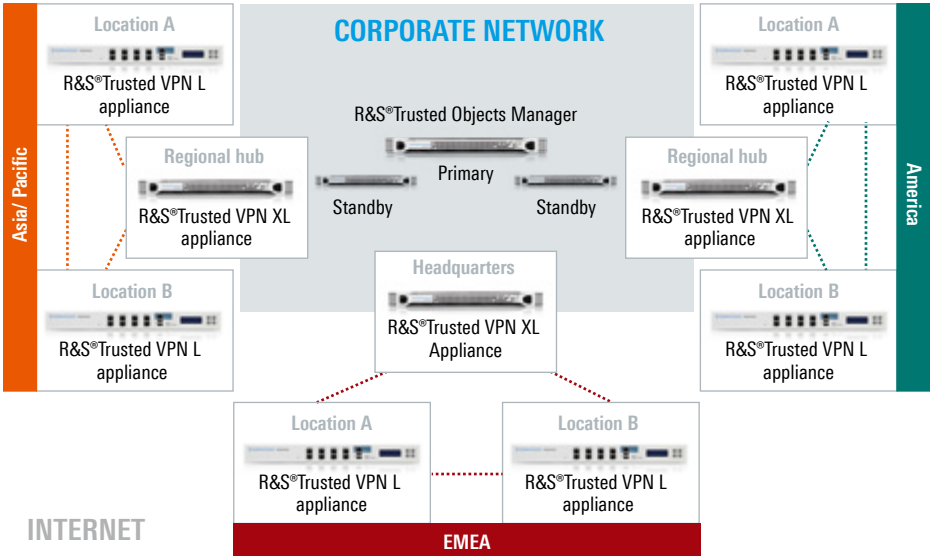


Fig. 3:

R&S®Trusted VPN implemented with three regional, fully meshed VPN clouds for EMEA, Asia/Pacific and the United States of America

Solutions for endpoint security

The **R&S®Trusted Endpoint Suite** – a remote software suite designed according to RESTRICTED security requirements – has a modular structure and has been developed specifically for Microsoft® Windows 10™ endpoints. It combines:

- A solution for highly secure VPN remote access to networks of government organizations and enterprises (R&S®Trusted VPN Client)
- Full disk encryption to prevent the loss of data (R&S®Trusted Disk)
- A solution for highly secure browsing in public authorities and enterprises (R&S®Browser in the Box).

R&S®Trusted VPN Client – protected network communications with mobil Microsoft® Windows 10™ endpoints

R&S®Trusted VPN Client protects the communications of a client platform (laptop or tablet) with a government or corporate network over non-trustworthy networks such as the internet. This allows employees to work mobile without restrictions in airports, home offices or other public spaces.

R&S®Trusted Disk – full disk encryption for data protection

The most comprehensive and most secure way to protect your data in endpoints is encryption of the entire disk. Secure and effective encryption by R&S®Trusted Disk prevents access to sensitive data in the event of theft or loss.

R&S®Browser in the Box – secure and convenient browsing in a virtual environment

R&S®Browser in the Box offers proactive protection against cyberattacks. Thanks to the secure separation of the browser from other areas of the PC, your corporate network is protected against Trojan horses, ransomware, ATPs and zero day exploits. It also eliminates threats from active content, such as Java, JavaScript or Flash, or opening hazardous links. The management tool lets you easily configure security policies from one central interface. User rights are assigned in the browser with just a few clicks, e.g. for printing, uploads/downloads and copy/paste. R&S®Browser in the Box fulfills compliance guidelines according to applicable data protection law. Your system is also protected against data leaks through telemetry data in Microsoft® Office™ and Windows 10™ because the internet-intranet separation prevents the corresponding Microsoft services from reaching their counterpoints in the internet. This is transparent to users, who continue to enjoy unrestricted and secure internet access for their daily work.

The optional Docs in the Box product feature provides a viewer function that allows all attachments of standard Office applications and applications with internet access, such as Skype, to be tested in a protected virtual environment, providing additional protection against harmful attachments.

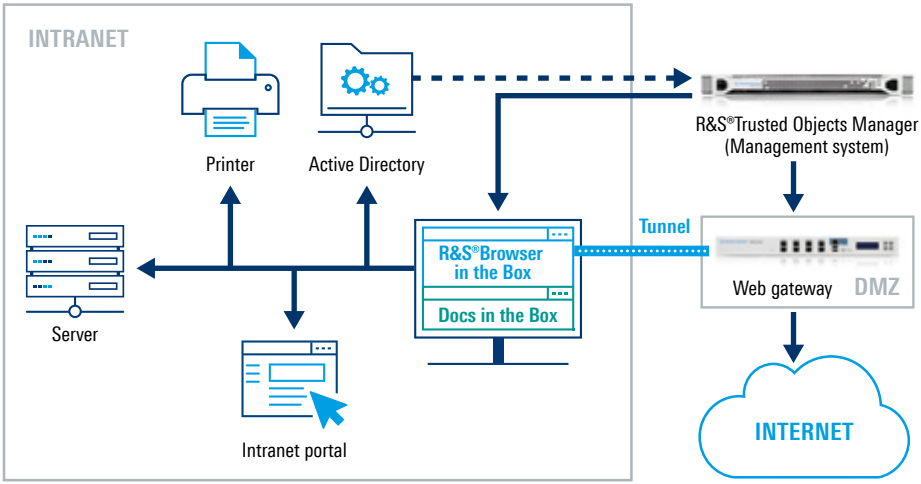


Fig. 4:

Network separation offers a protected space within which malware cannot reach local computers in the corporate network

Solution for application security

R&S®Web Application Firewall – protection for you web-based business processes

R&S®Web Application Firewall is an integrated security suite for web-based applications, web services and databases. It protects your data in business applications such as SAP or Oracle, on internet and intranet sites, in extranet apps (e.g. Microsoft® Outlook Web Access™ or SharePoint™), in web services for machine-to-machine-communications, and in backends for mobile apps.

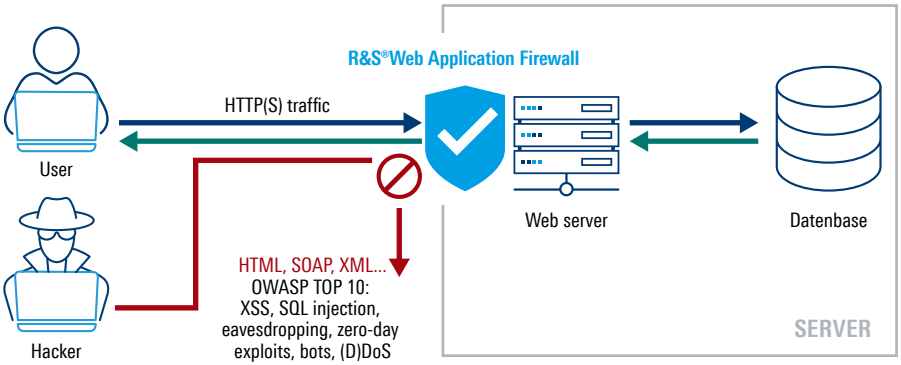


Fig. 5:
Effective security against a multitude of attacks

Solution family for data-centric security in the cloud

R&S®Trusted Gate – secure, data-protection compliant working in the cloud and with collaboration tools

The R&S®Trusted Gate product family applies innovative encryption technologies and fragmentation of sensitive documents to enable secure and data-protection compliant working in clouds (e.g. Google Drive) and collaboration tools (e.g. Microsoft® SharePoint™ or Microsoft® 365™). With R&S®Trusted Gate you can control where your data is stored and ensure that it does not leave a particular region. Document-centric encryption and role-based access control keep your business-critical information protected against cyberattacks and espionage, from any location.

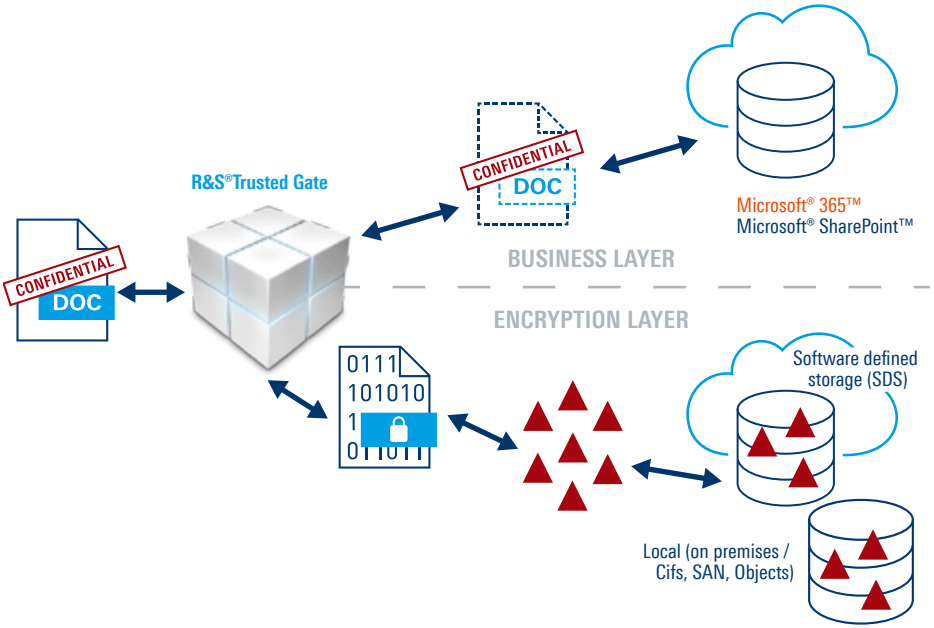


Fig. 6:

Secure collaboration in the cloud – original data is encrypted and fragmented before landing in a configurable storage system

FURTHER INFORMATION

For more information about our products, such as white papers, webinars and product flyers, visit our webpage at:

www.rohde-schwarz.com/cybersecurity/home-office-security

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity is a leading IT security company that protects digital assets of companies and public institutions around the world against cyberattacks. The IT security expert provides innovative data protection solutions for cloud environments, advanced security for websites, web applications and web services as well as network encryption, desktop and mobile security. To prevent cyberattacks proactively, the trusted security solutions are developed according to the security-by-design approach.

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 3608.6083.61 | Version 01.00 | August 2020 (sch)
Home Office Security
Cover image: ©www.istock.com - MV

3608608362
3608.6083.62 01.00 PDP 1 en