



Rohde & Schwarz Cybersecurity

HOME OFFICE SECURITY

Zur Sicherheit von Telearbeit:
Was Unternehmen jetzt wissen müssen

ROHDE & SCHWARZ

Make ideas real



INHALT

Sicheres mobiles Arbeiten	3
Sicherheitsbewusstsein im Home Office	3
Phishing-E-Mails, Malware & Ransomware: Welche Cyberbedrohungen Sie aktuell besonders abwehren sollten	5
Geschützter Remote-Zugriff auf das Firmennetzwerk	6
Telearbeits-Tipps für erhöhte IT-Sicherheit Ihrer Mitarbeiter	8
Sicherheit – niemals optional, immer anwendbar	11
Sichere Kommunikation über verschiedene Standorte hinweg	11
Hybrid, Public, Private Cloud oder doch SaaS?	11
Checkliste sichere Zugänge & Anwendungen im Home Office	12
Sicherheitslösungen von Rohde & Schwarz Cybersecurity zur Home Office Security	13
Lösungen für Netzwerksicherheit	13
Lösungen für Endpoint-Sicherheit zur Absicherung von Telearbeitsplätzen	15
Lösungsfamilie für datenzentrische Sicherheit in der Cloud	18

SICHERES MOBILES ARBEITEN

Sicherheitsbewusstsein im Home Office

Krisen bieten zugleich enorme Chance für Behörden und auch immer noch für Unternehmen ihre digitale Transformation schneller voranzutreiben. Die Digitalisierung der Arbeitswelt erfährt aktuell einen deutlichen Schub: Home Office (oder: Telearbeit) und mobiles Arbeiten etablieren sich als alternative Arbeitsformen und führen zu einer breiten Nutzung digitaler Arbeitsmittel. Etliche Papierprozesse müssen digitalisiert werden, wobei Home Office, Bring Your Own Device (BYOD) und Cloud-Anwendungen hilfreiche Vorantreiber sind. Derzeit etablieren sich neue Standards, die die räumliche und zeitliche Verteilung der Arbeit betreffen. Unternehmen wie Behörden sind gezwungen, mitunter neue Formen des Arbeitens auszuprobieren und Lösungen für einen reibungslosen Arbeitsalltag zu schaffen.

Der Branchenverband Bitkom hat hierzu in einer eigenen Studie ermittelt: „Neun von zehn Unternehmen empfehlen Arbeit von zu Hause aus, zwei Drittel haben das sogar angeordnet.“¹

Diese Chancen gehen für die IT-Sicherheit oft mit Herausforderungen einher, die IT-Infrastruktur der eigenen Organisation „von heute auf morgen“ auf den Remote-Zugriff umzustellen. Viele Behörden und Organisationen befinden sich dann in einer Art Schnelldurchlauf der Digitalisierung, da die Mitarbeitenden ausschließlich von zu Hause aus arbeiten – eine Situation, auf die nur die wenigsten ausreichend vorbereitet sind.

„Digitale Technologien ermöglichen es, unabhängig von Zeit und Ort zu arbeiten. Home Office wird für immer mehr Beschäftigte zum Alltag.“

Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder²

¹ <https://www.bitkom.org/Presse/Presseinformation/Digitale-Wirtschaft-schickt-ihre-Mitarbeiter-flaechendeckend-ins-Homeoffice>

² <https://www.bitkom.org/Presse/Presseinformation/Vier-von-zehn-Unternehmen-setzen-auf-Homeoffice>

Wenn neue digitale Prozesse, Technologien und deren Anwendungen noch nicht fest etabliert, kommt IT-Sicherheit mitunter zu kurz. In dieser Handreichung soll daher versucht werden, einen Überblick zu geben, wie Sie Telearbeit sicher gestalten und Zeit und Ressourcen bestmöglich einsetzen, um sich vor Cyberbedrohungen und schlechterem (breiten) Perimeterschutz zu wappnen. Informationssicherheit sollte auch im Home Office immer oberste Priorität haben.

Für jeden Remote-Mitarbeiter – ob Festangestellte, Externe (feste Freie), Partner oder Dienstleister – sollten Unternehmen Sicherheitsstrategien definieren und anwenden, damit sie ihre Geschäftsaufgaben erfüllen, produktiv bleiben können und gleichzeitig das Risiko von Cyberangriffen geringhalten.

IT-Sicherheit sollte niemals zu komplex sein, damit Ihre Mitarbeiter einzelne Maßnahmen auch anwenden können; Usability und Sicherheit sollten nicht im Widerspruch stehen. Es ist wichtig, das Bewusstsein für digitale Sicherheit gerade in der aktuellen Zeit zu stärken, da es bereits eine Zunahme von Phishing-Angriffen gab. Angreifer nutzen die derzeitige Situation ggf. aus, bleiben Sie also besonders wachsam bei Phishing-E-Mails und Betrügereien.

Machen Sie sich in Ihrem Haus dafür stark, sich strategisch und prozessual angemessen aufzustellen, um resilient zu sein gegenüber gesteigerten Angriffsszenarien durch dezentralisiertes Arbeiten.

Das dezentrale Arbeiten bildet eine ideale Grundlage für verschiedene Angriffsszenarien, von veralteter technischer Infrastruktur, die nicht durch das Firmennetz abgesichert ist, über ungesicherte Router und WLAN-Verbindungen zu unverschlüsselten Datenträgern, bis zu CEO-Fraud, Ransomware und klassische Phishing-E-Mails. Mitarbeitende haben einen gesteigerten Informationsbedarf – gleichzeitig müssen Organisationen ihr Sicherheitsbewusstsein fördern.

PHISHING-E-MAILS, MALWARE & RANSOMWARE: WELCHE CYBERBEDROHUNGEN SIE AKTUELL BESONDERS ABWEHREN SOLLTEN

Es häufen sich die Meldungen über betrügerische Massen-E-Mails³, die angeblich im Namen von Kreditinstituten, Sparkassen, aber auch Online-Versandhändlern in Umlauf gebracht werden. Cyberkriminelle versuchen auch in Zeiten, in denen eine Vielzahl Arbeitender weltweit aus dem Home Office arbeitet, unbefugten Zugriff auf Konten, Daten und Informationen zu erhalten.

Vordergründig geht es um „Hilfestellungen“ und angepasste „Sicherheitsmaßnahmen“; dahinter verstecken sich jedoch „klassische Phishing-E-Mails“, die derzeit ebenso in Umlauf gebracht, wie Personen auf gefakten Seiten zur Eingabe von Daten wie E-Mail-Adressen, Kontoverbindungen und Passwörtern – und damit zur Installation von Malware aufgefordert werden.



Besondere Vorsicht bei E-Mails von angeblich offiziellen Stellen mit Dateianhängen wie PDF, docx oder mp4

Hierin enthalten sein sollen angeblich relevante Sicherheitsinformationen, die dann beim Herunterladen jedoch Malware installiert, die Daten und so den Zugang zum eigenen Endgerät wie dem Firmennetzwerk verschlüsselt. Diese Art Phishing per E-Mail zählt nach wie vor zu einem der erfolgreichsten Angriffswerkzeuge von Kriminellen; die aktuelle Zunahme dieser Angriffe stellt eine globale Bedrohung dar.

³ <https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html>

PRAXIS-BEISPIEL:

Im vergangenen Jahr wurde der Angriff auf die Uniklinik Brno in der Tschechischen Republik bekannt⁴. Dort wurde das Krankenhausnetzwerk so erfolgreich angegriffen, dass es Wochen dauerte, den ursprünglichen Betrieb wiederherzustellen. Als Folge mussten sämtliche Computer heruntergefahren, Operationen abgesagt und Patienten in andere Häuser verlegt werden. Krankenhäuser gehören, wie andere kritische Systeme auch, zu besonders „beliebten“ Angriffszielen, da die Aufrechterhaltung ihrer Betriebe von hoher gesellschaftlicher Relevanz ist.

Ransomware-Angriffe⁵ auf Unternehmen aus dem Gesundheitswesen haben 2019 allein in den Vereinigten Staaten 764 Healthcare-Provider⁶ betroffen, was Ausfälle der Notrufnummer 911 zur Folge hatte, weswegen auch hier Operationen nicht stattfinden konnten.



Abbildung 1:

Statista zufolge betrug der finanzielle Schaden durch Internetkriminalität 2017 in Milliarden US-Dollar⁷

Geschützter Remote-Zugriff auf das Firmennetzwerk

In einer zunehmend vernetzten Arbeitsumgebung, in der Unternehmen und Behörden über weltweit verteilte Büros arbeiten, sind Virtual Private Networks (VPN) unerlässlich. Nur mit einer verschlüsselten VPN-Verbindung können Mitarbeiter sicher auf Unternehmensnetzwerke und -ressourcen zugreifen. Geschützte und abhörsichere Zugänge ins Behörden- und Firmennetzwerk sind

⁴ <https://www.behoerden-spiegel.de/2020/03/17/tschechisches-krankenhaus-lahmgelegt/>

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/>

„Wir sind der Überzeugung, dass Sicherheit nur unabhängig vom Betriebssystem erfolgen kann. Mit R&S®Trusted VPN Client gewährleisten wir Sicherheit bei gleichzeitiger digitaler Souveränität der Nutzer.“

Dr. Falk Herrmann, CEO von Rohde & Schwarz Cybersecurity

wichtiger Bestandteil des mobilen Arbeitens und des Arbeitens aus dem Home Office. Technische Schutzmaßnahmen im Behördeneinsatz müssen so zum Beispiel mindestens die unterste Geheimhaltungsstufe „Verschlussachen – Nur für den Dienstgebrauch“ (VS-NfD) erfüllen. Dass derzeit vermehrt Personen mit mobilem Zugang auf Unternehmens- und Behördennetzwerken remote arbeiten, stellt eine besondere Herausforderung dar. Kapazitätsprobleme können zu einer gedrosselten Systemleistung führen – und dies letztlich zu einer geringeren IT-Sicherheit. Um nun Laptops und andere mobile Endgeräte, die mit der unternehmenseigenen IT verknüpft werden, vollumfassend zu schützen, eignet sich eine softwarebasierte Sicherheits-Suite, bestehend aus sicherem Browser, VPN Client und Festplattenverschlüsselung optimal, denn diese erfordert keine Neuanschaffung an Hardware oder spezielle Nachschulungen der Anwender.

IHRE VORTEILE:

- **Verbesserte Effizienz:** Die einzelnen Komponenten der Suite sind perfekt aufeinander abgestimmt und ermöglichen optimale Workflows.
- **Gesteigerte Produktivität:** An der gewohnten Arbeitsweise ändert sich nichts, alle Sicherheitsmechanismen laufen im Hintergrund ab. Ihre IT muss weniger managen und hat Zeit für andere Prozesse.
- **Geringere Betriebskosten:** Im Gesamtpaket sparen Sie.

Der vom BSI zugelassene rein softwarebasierte VPN Client und die ebenfalls zugelassene Festplattenverschlüsselung ermöglichen Nutzern sicheres mobiles und verschlüsseltes Arbeiten unter Einhaltung der hohen Sicherheitsanforderungen deutscher Bundesbehörden. Mitarbeitende nutzen somit einen hochsicheren Zugang aus einer gesicherten Umgebung heraus mit einer Festplattenverschlüsselung zur Verhinderung von Datenverlusten, einem VPN-Fernzugriff für die verschlüsselte Datenübertragung und einem hochsicheren Browser mit Document Viewer.

TELEARBEITS-TIPPS FÜR ERHÖHTE IT-SICHERHEIT IHRER MITARBEITER



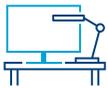
1. Informieren Sie Mitarbeitende über IT-Sicherheit & Datensicherheit

Verbindliche und eindeutige Regelungen die IT-Sicherheit und der Datensicherheit betreffend, sollten spätestens jetzt in Organisationen schriftlich an alle betreffenden Personen kommuniziert werden.



2. Benennen Sie eindeutige Kommunikationswege & Kontaktstellen

Klären Sie Zuständigkeiten und Ansprechpersonen bei etwaigem Verlust von Komponenten sowie Meldewege. Diese Kommunikationswege sollten allen Beschäftigten bekannt sein – und von ihnen auch verifiziert werden können.



3. Physische Home-Office-Sicherheitsmaßnahmen

Mitarbeitende sollten angehalten werden, auch während der Heimarbeit bestimmte Sicherheitsmaßnahmen selbst zu ergreifen. Dazu gehört, dass der Arbeitsplatz physisch vor Zugriff gesichert ist, also Türen verschlossen und Bildschirme gesperrt werden. Empfehlenswert ist zudem, die Webcam am Rechner oder Laptop abzudecken und Bildschirme vor etwaigen Einblicken von außen zu positionieren.



4. WLAN & Passwortsicherheit im Home Office

Sichern Sie Ihr WLAN Zuhause, indem Sie das Standard-Administrator-Passwort ändern, die WPA2-Verschlüsselung aktivieren und ein starkes Kennwort verwenden.



5. IT-Security: Achten Sie auf Phishing & CEO-Fraud

Sensibilisieren Sie vor Angriffen, die darauf abzielen, Informationen und Daten zu erhalten, die Hinweise auf Passwörter, Bankverbindungen oder Zugänge zu Systemen und Anwendungen enthalten. Weisen Sie besonders auf CEO-Fraud hin.



Social Engineering stellt eines der größten Risiken im Home Office dar

Angreifer täuschen und tricksen, um Mitarbeiter zu fehlerhaftem Verhalten zu animieren. E-Mail-Phishing ist ein Teilaspekt, wichtig ist aber auch besondere Vorsicht bei Telefonanrufen, SMS, Social-Media-Inhalten und gefälschten Nachrichten, die über Messenger in Firmenanwendungen, die zur Kollaboration verwendet werden, vertrieben werden.



6. VPN – Sichere Kommunikation im Home Office

Nutzen Sie sichere Kommunikationskanäle, um auf Unternehmensressourcen zuzugreifen. Verwenden Sie wo möglich sogenannte Virtual Private Networks (VPN), die als „Vermittler“ über einen „gesicherten Tunnel“ Verbindungen zwischen dem Endgerät und dem Unternehmensnetz aufbauen.



7. MFA & 2FA – Sichere Passwörter für gesicherte Anwendungen

Sichere Passwörter schützen Anwendungen zusätzlich vor unberechtigtem Zugriff. Etablieren Sie komplexe und eindeutige Passwörter und nutzen Sie zusätzlich eine Multi-Faktor-Authentifizierung (MFA oder 2FA). Passphrasen sind gute Passwörter, denn sie sind möglichst lang, komplex und verwenden zufällige Begriffe oder Sätze. „Wir verschlüsseln Datenträger!“ oder „keine-Zellen-in-Excel-verbinden“ sind Beispiele hierfür.

Beide sind stark, mit vielen Zeichen, leicht zu merken und zu tippen, aber schwierig zu knacken. Ergänzen Sie diese um Symbole, Zahlen oder Großbuchstaben. Wenn ein eindeutiges Passwort für jede Ihrer erforderlichen Anwendungen notwendig ist, empfiehlt sich ein Passwort-Manager, also ein Programm, das Passwörter in einer Art Tresor speichert und im Bedarfsfall automatisch abrufen – und eindeutige Passwörter sind grundsätzlich empfehlenswert. Andernfalls muss ein Angreifer lediglich eine von Ihnen benutzte Website erfolgreich kompromittieren, um an alle – auch Ihr – Passwort zu gelangen und sich dann einfach bei allen weiteren Konten erfolgreich anzumelden.



Auf haveibeenpwned.com kann schnell überprüft werden, ob E-Mails kompromittiert wurden.

Wenn Sie einen Passwort-Manager verwenden, schützen Sie diesen am besten mit einer starken Passphrase sowie einer zweistufigen Verifizierung.



8. Aktualisierte Betriebssysteme, Webanwendungen und Apps

Stellen Sie sicher, dass verwendete Technologien auf dem aktuellsten Stand sind und Updates regelmäßig ausgeführt werden. Mitarbeiter sollten stets mit der neuesten Systemversion arbeiten.



9. IT-Security beim dezentralen Arbeiten im Home Office

Betrachten Sie Laptops, Firmenhandys und andere Arbeitsmittel wie Dateien und interne Ressourcen unabhängig von Ihrem eigenen Standort als das, was sie sind: reine Arbeitsmittel. Sensible Unternehmensdaten bleiben sensibel – unabhängig von Ihrem individuellen Aufenthaltsort, und ein kontrollierter Zugang zu Endgeräten ist immer einzuhalten. Achten Sie darauf, dass der Bildschirm nicht einsehbar ist. Wenn Sie Ihre Arbeit unterbrechen, aktivieren Sie immer die Bildschirm Sperre. So helfen Sie, auch zuhause datenbewusst und im Sinne der Unternehmenssicherheit zu handeln.

Oder, wie es das Bundesamt für Sicherheit in der Informationstechnik (BSI) formuliert: „Stellen Sie sicher, dass Unbefugte keinen Einblick in Ihre Daten haben“, was auch das Posten von Informationen auf Social Media betrifft. Denn: Bedenken Sie, dass Ihre Social-Media-Beiträge aus dem Home Office oft nur kleine Indikatoren liefern können, die den Menschen helfen können, zu erkennen, wo Sie leben.

Postings mit Informationen wie Standortkennzeichnungen und Orientierungspunkten geben sowohl Fremden als auch bekannten, aber möglicherweise zweifelhaften Personengruppen die Möglichkeit, Sie, Ihre Kinder und andere Familienmitglieder zu lokalisieren. Das BSI bietet übrigens auch „Informationen für Bürger“ sowie eine Service-Telefonnummer, unter der Privatpersonen konkrete Fragen rund um das Thema IT-Sicherheit stellen können. Themenschwerpunkte sind derzeit⁸ „Sicher digital lernen“ oder „Videotelefonie leichtgemacht“.

⁸ <https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/digital-vernetzt-in-corona-zeiten.html>

SICHERHEIT – NIEMALS OPTIONAL, IMMER ANWENDBAR

Sichere Kommunikation über verschiedene Standorte hinweg

Wenn Mitarbeitende von entfernten Standorten aus auf Anwendungen oder Systeme zugreifen, muss die Kommunikation zwischen den Geräten sicher sein – entweder über Protokolle wie HTTPS oder über ein Firmen-VPN.

Für Remote-Mitarbeitende ist der gesicherte Zugriff auf Unternehmensanwendungen entscheidend aus dem Home Office. Eine optimale Lösung für das Identitäts- und Zugriffsmanagement hilft dabei, die geeigneten Zugriffsmethoden und -technologien automatisiert für (berechtigte) Remote-Mitarbeitende bereitzustellen.

Das hierbei angewandte Prinzip der geringsten Privilegien bedeutet, dass nur die Mindestberechtigungen gewährt werden, die von einem Endbenutzer, einer Anwendung, einem Dienst, einer Aufgabe oder einem System benötigt werden, um zugewiesenen Aufgaben auszuführen. So kann „überprivilegiertes Zugriff“ durch Benutzer, Anwendungen oder Dienste verhindert werden, ohne die Produktivität zu beeinträchtigen oder die IT zu involvieren.

Hybrid, Public, Private Cloud oder doch SaaS?

Wenn Sie und Ihre Angestellten sämtlich aus dem Home Office auf geschäftskritische Systeme, Anwendungen, Infrastruktur und Daten zugreifen müssen, eignet sich unter Umständen ein hybrides Szenario, in dem einige Geschäftsanwendungen direkt am Standort oder im unternehmenseigenen Rechenzentrum, andere in einer privaten oder öffentlichen Cloud oder die Anwendungen auf Software as a Service (SaaS) basieren. Je nach geeignetem Modell ist immer von entscheidender Bedeutung, dass Remote-Arbeitende unabhängig vom persönlichen Standort immer sicher auf die notwendigen Geschäftsanwendungen zugreifen können.

Checkliste sichere Zugänge & Anwendungen im Home Office

1. Richten Sie VPN-Lösungen ein, die auch eine große Anzahl gleichzeitig stattfindender Verbindungen aufrechterhalten können
2. Stellen Sie Möglichkeiten sicherer Videokonferenzen bereit, die über stabile Audio- und Videofunktionen verfügen
3. Sorgen Sie dafür, dass Geschäftsanwendungen des Unternehmens nur über verschlüsselte Kommunikationskanäle (SSL VPN, IPSec VPN) zugänglich sind
4. Setzen Sie auf Multi-Faktor-Authentifizierungsmechanismen auf unternehmenseigenen Anwendungsportalen

In der gegenwärtigen Situation sollten Sie besonders wachsam sein bei E-Mails, in denen Sie aufgefordert werden, Zugangsdaten zu überprüfen oder zu erneuern. Selbst, wenn diese von einer vertrauenswürdigen Quelle zu stammen scheinen, versuchen Sie bitte, die Authentizität der Anfrage zu überprüfen.



Klicken Sie nicht auf verdächtige Links und öffnen Sie keine verdächtigen Anhänge

Seien Sie zudem besonders aufmerksam gegenüber E-Mails von Personen, die Sie nicht kennen und in denen Sie gebeten werden, sich mit über Links zu verbinden oder Dateien zu öffnen. Im Zweifelsfall melden Sie diese Anfrage an die jeweiligen Sicherheitsbeauftragten.

5. Verschicken Sie sensible Unternehmensinformationen (z. B. per E-Mail) ausschließlich über sichere Verbindungen
6. Seien Sie besonders vorsichtig mit E-Mails, die sich auf den Coronavirus oder Covid beziehen, da es sich dabei um Phishing-Versuche oder Betrügereien handeln kann
7. Wenden Sie sich bei Zweifeln an der Legitimität einer E-Mail immer an die jeweiligen Sicherheitsbeauftragten
8. Daten at rest (im Ruhezustand, z. B. lokale Laufwerke), sollten verschlüsselt werden, um sie vor Diebstahl und bei etwaigem Verlust des Gerätes zu schützen
9. Geben Sie die URLs von Calls und Konferenzen nicht in sozialen Medien oder auf anderen öffentlichen Kanälen weiter, so dass nur Befugte auf Ihre Unternehmensmeetings zugreifen können

SICHERHEITSLÖSUNGEN VON ROHDE & SCHWARZ CYBERSECURITY ZUR HOME OFFICE SECURITY

Dank eines breiten Portfolios von IT-Sicherheitslösungen aus einer Hand und umfassender IT-Security-Expertise ist Rohde & Schwarz Cybersecurity Ihr verlässlicher europäischer Partner für gesicherte Remote-Arbeitsplätze Ihrer Mitarbeitenden und damit auch für die Infrastruktur im Unternehmen. Digitale Souveränität bietet ihnen die Möglichkeit zur unabhängigen, digitalen Selbstbestimmung, die insbesondere im internationalen Kontext eigene Gestaltungs- und Innovationspielräume erlaubt und einseitige Abhängigkeiten vermeidet.

Lösungen für Netzwerksicherheit

R&S®SITLine ETH – Sichere Datenübertragung durch Ethernet-Verschlüsselung

Ethernet-Verschlüsseler der R&S®SITLine ETH-Gerätefamilie schützen Unternehmen vor Spionage und Manipulation von Daten, die über Festnetz, Funk oder Satellit per Ethernet übertragen werden. Der Krypto-Durchsatz kann ohne Gerätetausch per Software-Upgrade auf bis zu 40 Gbit/s pro Gerät angepasst werden. Die Geräte überzeugen durch einfache Administration, getrenntes Netzwerk- und Sicherheitsmanagement, kompakte Bauweise und niedrige Systemkosten. Sie sind vom BSI für VS-NfD sowie NATO RESTRICTED zugelassen.

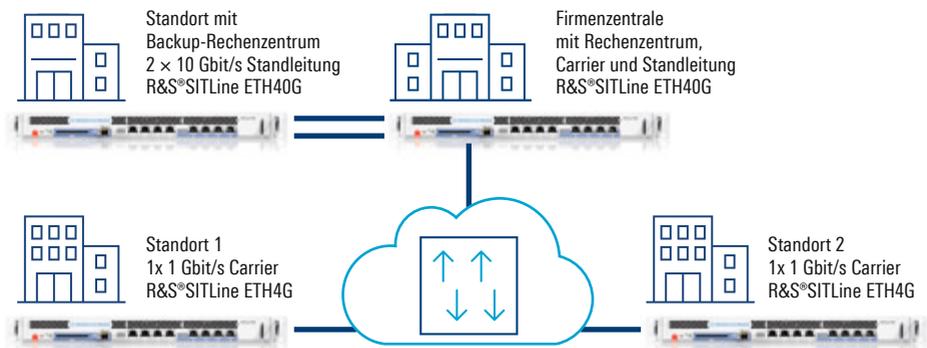


Abbildung 2:

Vorkonfigurierte Verschlüsselung für Standleitungen, die beim Start automatisch verschlüsselte L2-Verbindungen über Fast Ethernet herstellt

R&S®Trusted VPN – Ihr IPsec-Verschlüsselungs-Gateway

Die Lösung besteht aus einem VPN-Gateway, das in verschiedenen Varianten an einzelnen Standorten bereitgestellt werden kann, sowie einer zentralen Management-Station. Durch die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Lösung ist der hochsichere Fernzugriff auf Unternehmensressourcen jederzeit möglich.

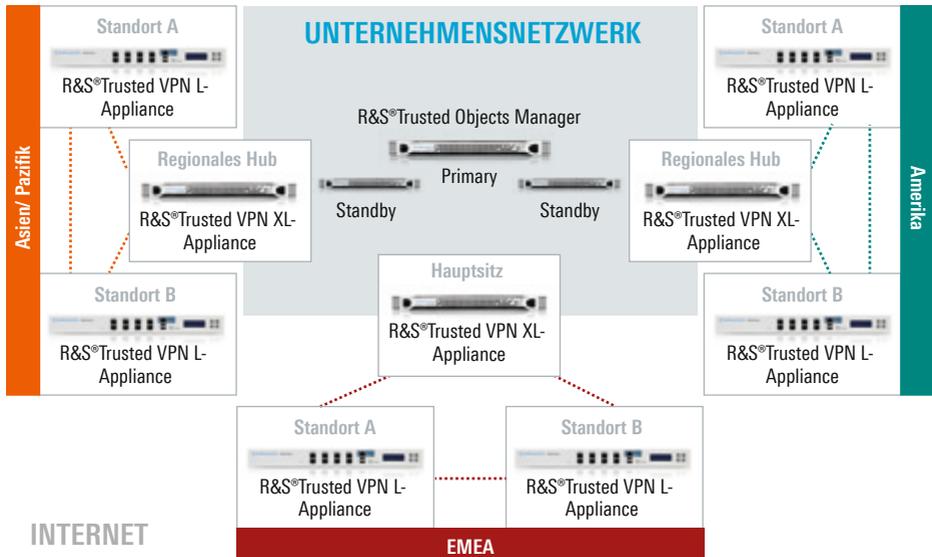


Abbildung 3:

R&S®Trusted VPN implementiert mit drei regionalen, vollständig vermaschten VPN-Clouds für EMEA, Asien / Pazifik und Amerika

Lösungen für Endpoint-Sicherheit zur Absicherung von Telearbeitsplätzen

Die Remote-Software-Suite **R&S®Trusted Endpoint Suite** – konzipiert gemäß VS-NfD-Anforderungen – ist modular aufgebaut und eigens für Microsoft® Windows 10-Endgeräte entwickelt. Sie vereint

- ▶ eine Festplattenverschlüsselung zur Verhinderung von Datenverlusten sowie (R&S®Trusted Disk)
- ▶ eine Lösung für hochsicheren VPN-Fernzugriff auf Netzwerke von Regierungsorganisationen und Firmen (R&S®Trusted VPN Client)
- ▶ eine Lösung für hochsicheres Browsen in Behörden und Unternehmen (R&S®Browser in the Box).

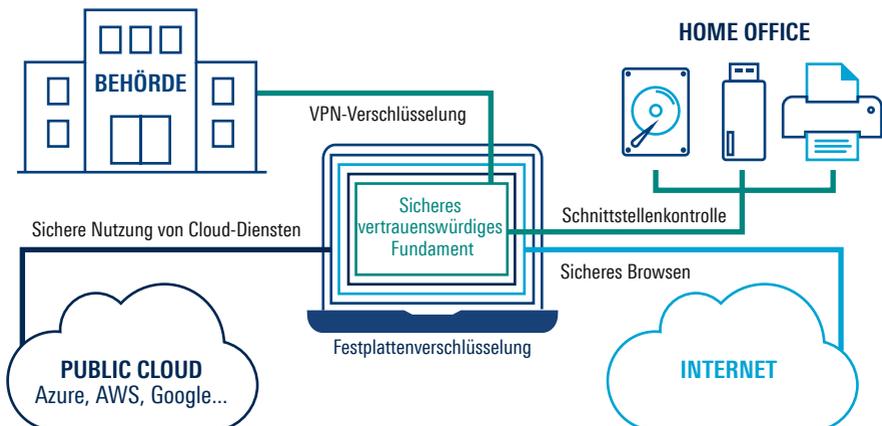


Abbildung 4:

Herausforderungen an eine sichere mobile Behörde

R&S®Trusted Disk – Datenschutz durch Festplattenverschlüsselung

Die umfassendste, sicherste Methode zum Schutz Ihrer Daten in Devices ist die Verschlüsselung der gesamten Festplatte. R&S®Trusted Disk verhindert im Fall eines Diebstahls oder Verlusts durch eine sichere und effektive Verschlüsselung der Festplatten den Zugriff auf sensible Daten. Die Festplattenverschlüsselung ist vom BSI für VS-NfD zugelassen.

R&S®Trusted VPN Client – Geschützte Netzwerkkommunikation mit mobilen Microsoft® Windows 10-Endgeräten

R&S®Trusted VPN Client schützt die Netzwerkkommunikation einer Client-Plattform (Laptop, Tablet) mit einem Behörden- oder Unternehmensnetzwerk über ein nicht vertrauenswürdiges Netzwerk wie z. B. das Internet. Mitarbeitende können so auch am Flughafen, im Home Office oder anderen öffentlichen Räumen ohne Einschränkungen mobil arbeiten.

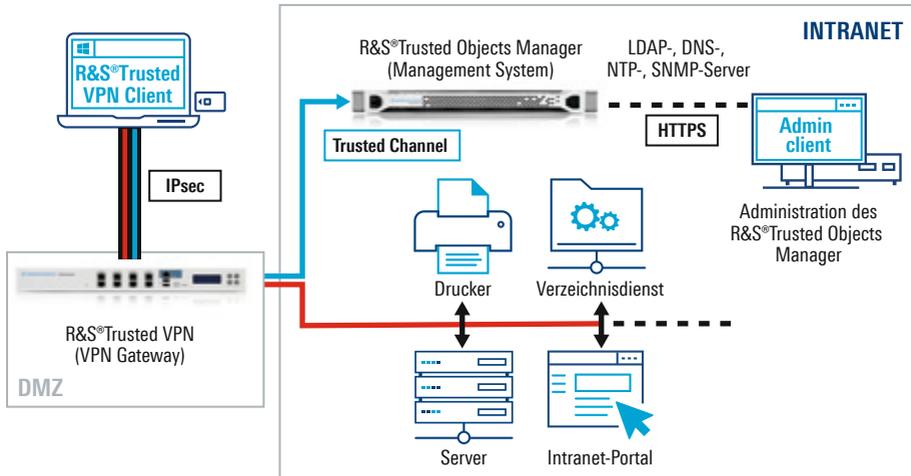


Abbildung 5:

Die R&S®Trusted VPN Client-Infrastruktur

R&S®Trusted VPN Client ist als reine Softwarelösung der erste, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene VPN Client für VS-NfD (Verschlusssachen – nur für den Dienstgebrauch). R&S®Trusted VPN Client setzt eine Zero-Trust VPN-Lösung um, bei der kein Vertrauen in potenziell unsichere Komponenten wie einem Betriebssystem bestehen muss. Die sogenannte Rot-Schwarz-Trennung (Netzwerk-trennung zwischen roten Verschlusssache-Daten und dem schwarzen Internetverkehr) findet außerhalb des Betriebssystems statt, sodass selbst bei Schwachstellen und Sicherheitslücken im Betriebssystem ein Abfluss von eingestufteten Daten verhindert werden kann.

R&S®Browser in the Box – Sicheres und komfortables Browsen in virtueller Umgebung

R&S®Browser in the Box bietet proaktiven Schutz gegen Cyberangriffe. Dank der sicheren Trennung des Browsers von den restlichen Bereichen des PCs ist Ihr Unternehmensnetzwerk gegen Trojaner, Ransomware, APTs und Zero-Day-Exploits geschützt. Aktive Inhalte, wie Java, JavaScript oder Flash und das Öffnen gefährlicher Links, stellen ebenfalls keine Bedrohung mehr dar. Mit dem Management-Tool konfigurieren Sie Sicherheitsrichtlinien komfortabel von einer zentralen Schnittstelle aus. Die Vergabe von Benutzerrechten im Browser (z. B. für Druckaufträge, Uploads/Downloads oder Copy/Paste) erfolgt mit wenigen Klicks. Compliance-Richtlinien werden gemäß des geltenden Datenschutzrechts erfüllt. Zudem wird Ihr System vor Datenabfluss durch Telemetriedaten in Microsoft® Office und Windows 10 abgesichert, da dank der Internet-Intranet-Trennung die entsprechenden Microsoft®-Dienste ihre Gegenstellen im Internet nicht mehr erreichen – für Nutzer unbemerkt, die weiter einen uneingeschränkten und sicheren Internetzugang für die tägliche Arbeit nutzen.

Das optionale Produkt-Feature Docs in the Box ermöglicht mittels Viewer-Funktion alle Anhänge gängiger Office-Anwendungen und Applikationen mit Internet-Zugriff wie Skype in einer geschützten virtualisierten Umgebung zu prüfen und bietet so zusätzlichen Schutz vor schädlichen Anhängen.

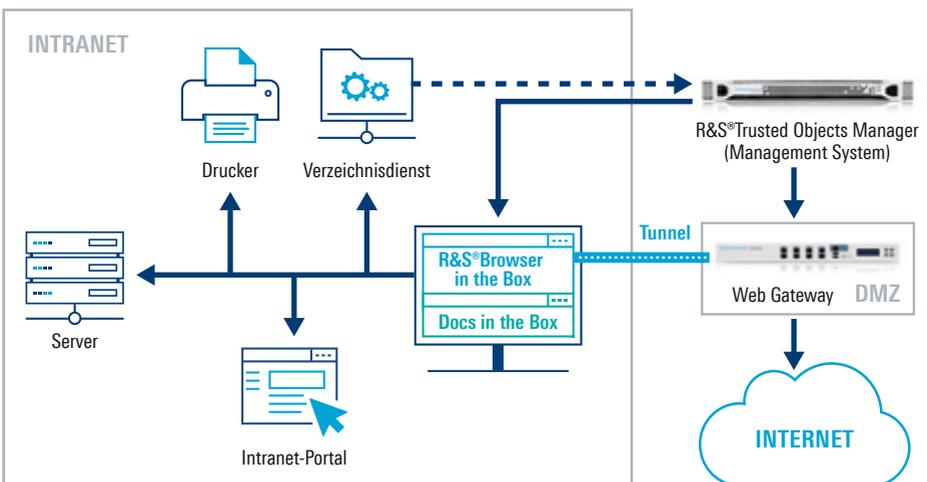


Abbildung 6:

Netzwerktrennung bietet „geschützten Raum“, in dem Schadsoftware nicht auf lokale Rechner/ in Unternehmensnetzwerke gelangt

Lösungsfamilie für datenzentrische Sicherheit in der Cloud

R&S®Trusted Gate – Sicheres, datenschutzkonformes Arbeiten in Clouds & Collaboration-Tools

Die R&S®Trusted Gate-Produktfamilie ermöglicht durch innovative Verschlüsselungstechnologie und Fragmentierung sensibler Dokumente sicheres und datenschutzkonformes Arbeiten in Clouds (z. B. Google Drive) und Collaboration-Tools (z. B. Microsoft® SharePoint, Microsoft® 365). Mit R&S®Trusted Gate kontrollieren Sie, wo Daten gespeichert werden und stellen sicher, dass sie eine bestimmte Region nicht verlassen. Durch dokumentenzentrierte Verschlüsselung und rollenbasierter Zugriffskontrolle bleiben ihre geschäftskritischen Informationen vor Cyberangriffen und Spionage geschützt – von jedem Standort aus.

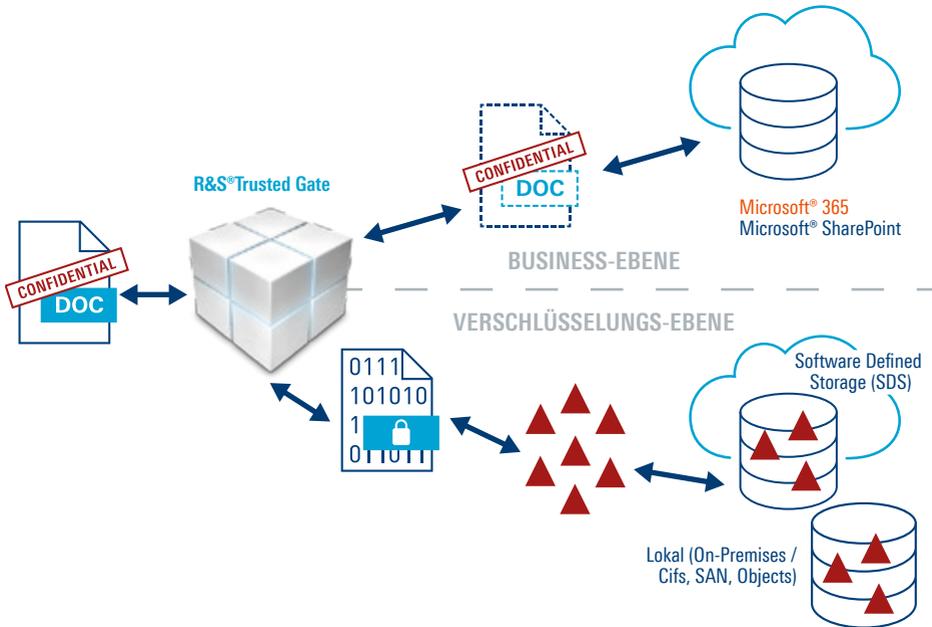


Abbildung 7:

Sichere Zusammenarbeit in der Cloud – Originaldaten landen verschlüsselt und fragmentiert im konfigurierbaren Speichersystem

WEITERE INFORMATIONEN

Weiteres Material wie Whitepaper, Webinare und Produkt-Flyer zu unseren Produkten finden Sie auf unserer Webseite:

[www.rohde-schwarz.com/cybersecurity/
home-office-security](http://www.rohde-schwarz.com/cybersecurity/home-office-security)

Rohde & Schwarz Cybersecurity

Rohde&Schwarz Cybersecurity ist ein führendes IT-Sicherheitsunternehmen, das digitale Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Institutionen weltweit vor Cyberangriffen schützt. Der IT-Sicherheitsexperte bietet innovative Datensicherheitslösungen für Cloud-Umgebungen, erweiterte Sicherheit für Websites, Webanwendungen und Webservices sowie Netzwerkverschlüsselung und Endpoint-Sicherheit. Die vertrauenswürdigen Sicherheitslösungen werden nach dem Security-by-Design-Ansatz entwickelt und verhindern Cyberangriffe proaktiv.

Rohde & Schwarz

Der Elektronikkonzern Rohde&Schwarz bietet innovative, Lösungen in folgenden Geschäftsfeldern: Messtechnik, Rundfunk- und Medientechnik, Sichere Kommunikation, Cybersicherheit sowie Monitoring and Network Testing. Vor mehr als 80 Jahren gegründet, ist das selbstständige Unternehmen mit seinem Firmensitz in München in über 70 Ländern mit einem engmaschigen Vertriebs- und Servicenetz vertreten.

Rohde & Schwarz Cybersecurity GmbH

Mühlendorfstraße 15 | 81671 München

Info: +49 30 65884-222

Email: cybersecurity@rohde-schwarz.com

www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG

www.rohde-schwarz.com

R&S® ist eingetragenes Warenzeichen der Rohde & Schwarz GmbH & Co. KG

Eigenennamen sind Warenzeichen der jeweiligen Eigentümer

PD 3608.6083.61 | Version 02.00 | Januar 2021 (sch)

Home Office Security

Titelbild: © www.istockphoto.com - MV

Daten ohne Genauigkeitsangabe sind unverbindlich | Änderungen vorbehalten

© 2020 - 2021 Rohde & Schwarz Cybersecurity GmbH | 81671 München