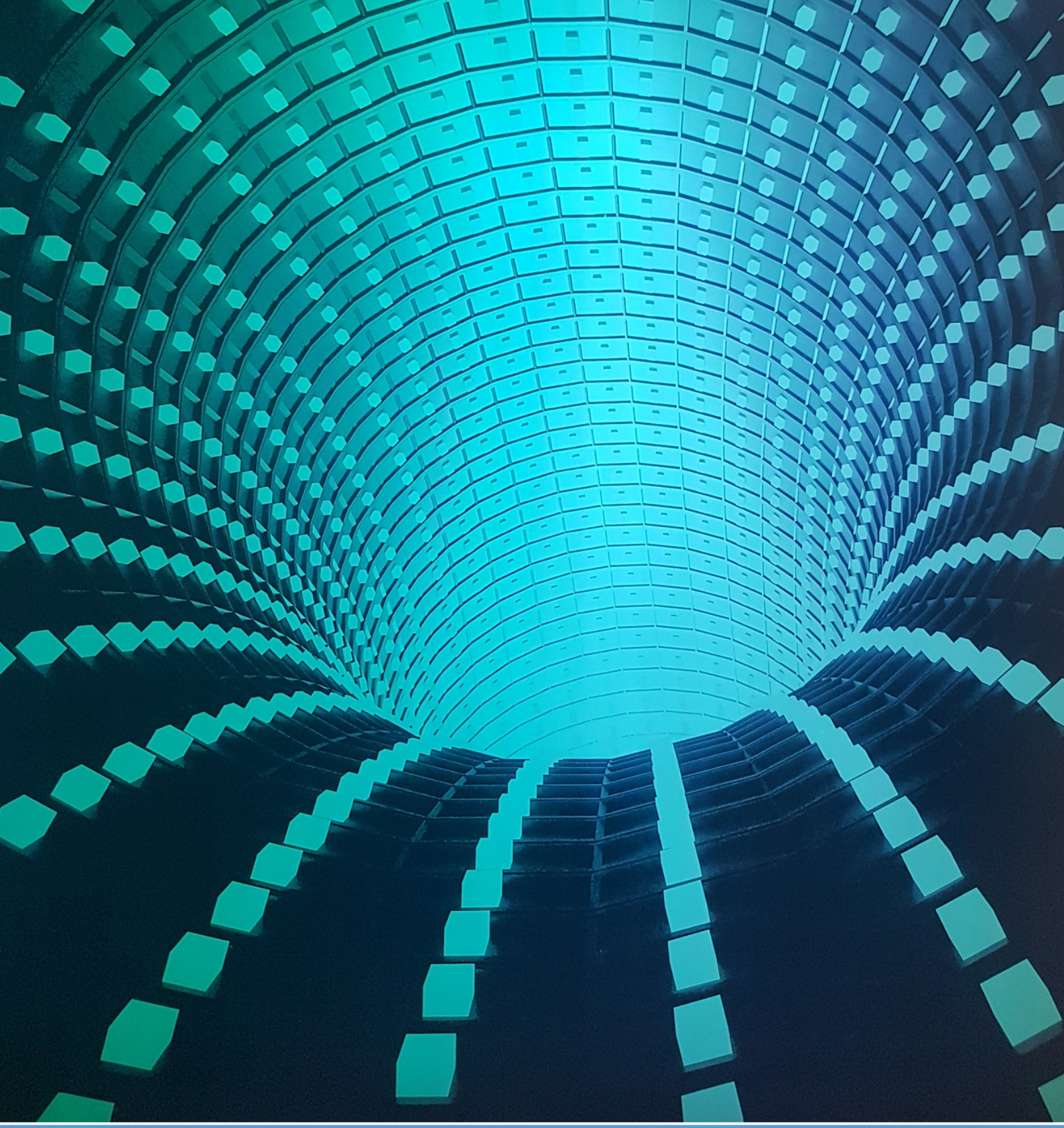
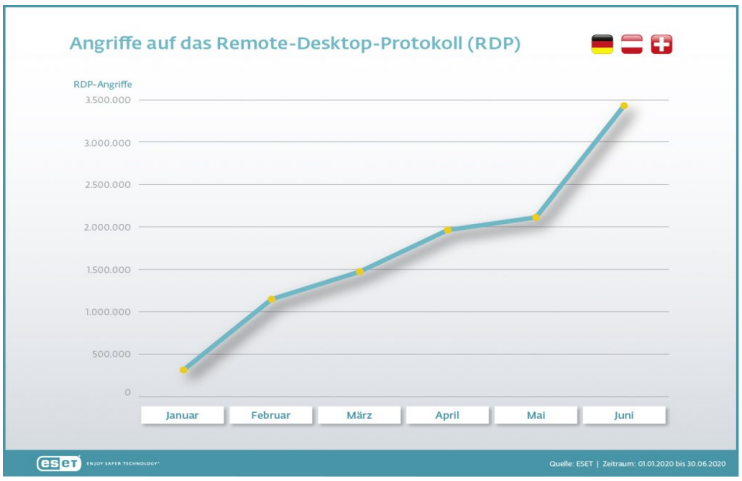


sicheres Homeoffice durch sicheren Tunnel

Homeoffice als Herausforderung

Einleitung

Für viele Unternehmer ist eine der größten Herausforderungen 2020, den wachsenden Bedarf an Telearbeitsplätzen umzusetzen. Unweigerlich folgen Fragen nach der Umsetzung, den Kosten aber auch nach der Sicherheit.



Zahlreiche Unternehmen haben in den vergangenen Jahren bereits viel in Ihre hauseigene IT-Sicherheit investiert, doch für die meisten ist das Thema Homeoffice gänzlich Neuland.
Die Gefahren sind nicht zu unterschätzen, die Zahl der Hacker-Angriffe auf RDP-Verbindungen sind laut den ESET-Forschern, allein im ersten Halbjahr 2020 von 310.000 Angriffen pro Tag auf bis zu knapp 3,4 Millionen Angriffen pro Tag (!) erhöht und die Tendenz ist weiterhin steigend.

Die Ursachen sind einfach erklärt. Zu Beginn des ersten Lockdowns im März blieb vielen Betrieben nicht viel Zeit den kompletten Betrieb oder zumindest die wichtigsten Abteilungen von den privaten Schreibtischen der Mitarbeiter aus zu organisieren. IT-Firmen waren zum Teil überlastet und bei neuer Hardware kam es zu Lieferengpässen. Also musste improvisiert werden. Doch das Thema Homeoffice

verliert nicht an Dringlichkeit und wird zum stetigen Begleiter für viele Arbeitgeber und Arbeitnehmer. Hilfe und Aufklärung bleiben also ein wichtiges Thema.

Inhaltsangabe

1. **VPN-Tunnel und unsere Lösungen**
2. **Einfach. Sicher. Mobil.**
3. **Die besten Argumente**
4. **Sec-Stick und GoDital**

VPN- Tunnel und unsere Lösung für Sie

Die wahrscheinlich häufigste Lösung fürs mobile Arbeiten ist eine sogenannte VPN-Verbindung. Bei einem VPN handelt es sich um ein geschlossenes Netzwerk, bei dem die Clients räumlich voneinander getrennt über einen IP-Tunnel eine Verbindung haben.

Dazu benötigen Sie eine spezielle VPN-Software, die von dem mobilen Endgerät aus mit dem Zielnetzwerk kommuniziert. Dadurch sind die Teilnehmer einer solchen Verbindung in der Lage, auf die firmeneigenen Dienste und Daten zuzugreifen. Somit ist der Unternehmensalltag nahezu 1:1 auch mobil umzusetzen. Doch diese Variante ist nicht ohne IT-spezifisches Vorwissen umzusetzen, da die Gefahr, Angreifern von außen unbewusst Türen und Tore zu den firmeneigenen sensiblen Daten zu ermöglichen, groß ist. Und selbst bei einer fachmännischen Einrichtung eines IT-Systemhauses schützen VPN-Verbindungen nur vor Angriffen von außen. Wird das private Endgerät des Mitarbeiters über andere Wege von einer Schadsoftware befallen, befindet sich die Schadsoftware, sobald die VPN-Verbindung aufgenommen wird, im inneren Kreis des Netzwerkes und kann sich unbemerkt auch im Firmennetzwerk ausbreiten.

An dieser Stelle bietet der Sec-Stick von team2work Ihnen eine sichere und unkomplizierte Verbindung für mobiles Arbeiten und ist somit ein idealer Partner fürs Homeoffice. Die Technik ist einfach. Der SEC-Stick baut jederzeit und von überall eine sichere Verbindung zu Ihrem mobilen Büro auf. Auf dem USB-Stick sind bereits viele Standardanwendungen für Ihr lokales Netzwerk installiert. Der Stick fungiert als mobiler SSH-VPN Client. Nach einer einmaligen Installation im LAN wird der SEC-Stick zum persönlichen digitalen Schlüssel, der den Remote-Zugang durch ein Passwort sicher macht. Durch diese 2-Faktor-Authentifizierung wird die Sicherheit der Verbindung um ein vielfaches erhöht. Selbst wenn ein Angreifer an das Passwort gelangt, kann er ohne den SEC-Stick keine Verbindung aufbauen. Durch Sicherheitsmaßnahmen in der Software ist ein Kopieren der Software auf einen anderen USB-Stick nicht möglich.

EINFACH. SICHER. MOBIL.

Einfach. Sicher. Mobil.

Seien Sie immer und überall verbunden. Das Produkt bietet Ihnen jederzeit eine sichere und mobile Remote Office Anbindung zu den Daten in ihrem Unternehmen. Sie oder Ihr IT-Dienstleister haben jederzeit Einblick in den Status ihrer VPN-Verbindungen über eine eigene Benutzerverwaltung inkl. Logging aller Aktionen und Zugriffe. Mit dem USB-Sec-Stick haben Sie die Möglichkeit auf der ganzen Welt sich Zugriff auf Ihren Rechner bzw. Ihr Netzwerk zu verschaffen.

Er baut eine sichere Leitung auf, womit Ihre Daten von Dritten geschützt sind. Die Verbindung wird durch gängige Verschlüsselungsverfahren, die nach heutigem Stand nicht hackbar sind, aufgebaut.

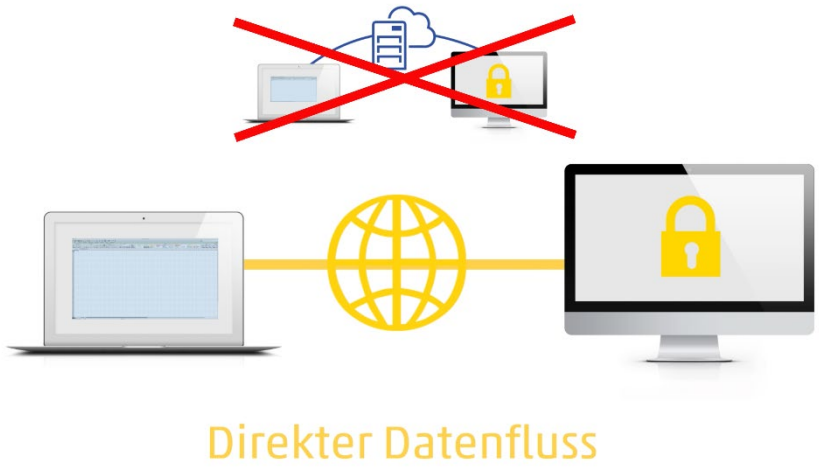
Nach Eingabe Ihres Benutzernamens & Passwortes baut der Stick eine sichere Verbindung zu Ihrem Rechner im Büro auf. Sie sehen die Desktop Oberfläche Ihres Rechners und können wie gewohnt daran arbeiten.

Sicherheitsaspekte des SEC-Sticks:

Reduzierung der Komplexität sorgt für besseren Schutz

- Authentifizierung – Public Key
- RSA Schlüssel Länge: 2048 bit (konfigurierbar)
- Starke Verschlüsselung – AES 256 bit
- Datenkompression
- SSH Protokoll Version: SSHv2
- Applikationsbasierter Zugriff auf zentral freigegebene Anwendungen
- Client- und Serverauthentifizierung
- keine öffentlichen Verbindungsserver im Internet benötigt
- keine IP-Verbindung in das lokale Netzwerk, lediglich ein TCP-Port muss für eingehende Verbindungen geöffnet sein
- Sichere, frei konfigurierbare Verschlüsselungsalgorithmen (AES-CTR, AES-GCM, ChaCha20, etc.), Hash-Algorithmen (SHA256, SHA512, Poly1305, etc.), Public Key Algorithmen (RSA, ECDSA, Ed25519, Ed448, etc.)
- Perfect Forward Secrecy durch modernste, konfigurierbare Schlüsselaustauschverfahren (DH Key Exchange, X25519, X448, etc.)
- Optionale Unterstützung für 2-Faktor-Authentifizierung mit vielen gängigen Techniken – als Referenzimplementierung TOTP mit Smartphone-APP jetzt verfügbar

Über den Team2Work Stick laufen Ihre Daten nicht wie bei anderen Anbietern über eine Cloud oder externe Server. Es wird eine direkte Verbindung zu Ihrem Rechner aufgebaut und Ihre Daten bleiben weiterhin auf dem Server in Ihrem Büro.



Der SEC-Stick funktioniert unter **Windows, Mac OS** und **Linux**. Eine Version für **Android** ist über den Google Play Store erhältlich.

Die besten Argumente

1. Der RDP Server ist für Dritte unsichtbar
   Damit ein Server über das Internet erreicht werden kann, muss auch der Serverdienst erreichbar sein. Dadurch können aber auch Angreifer sehen, welche Dienste bereitstehen und auf diese zugreifen.
   Der SEC-Stick Server verhindert einen direkten Zugriff auf den Terminalserver zuverlässig zu 100%. Der SEC-Stick Server steht vor dem Terminalserver und macht diesen für Angreifer „unsichtbar“.
2. Zusätzliche sichere Autorisierung
   Damit der vorgelagerte SEC-Stick Server die Benutzer autorisieren kann, benötigen Sie Ihren privaten digitalen Schlüssel auf dem SEC-Stick.
3. Der Benutzer sieht nur seine persönliche Umgebung
   Nach der Anmeldung sehen die Benutzer nur die für sie persönlich freigegebenen Ressourcen. Die Benutzerverwaltung wird vom Administrator zentralverwaltet.
4. Kinderleichte Bedienung
   Die Benutzung ist kinderleicht und seit vielen Jahren erprobt.
5. Keine Installation von Clientsoftware notwendig
   Den SEC-Stick verbinden sie mit ihren Windows, Mac oder Linux PC per USB und können direkt eine Verbindung bereitstellen. *Es ist keine Installation notwendig!*
6. Denial-of-Service und Bruteforce Schutz inklusive
   Der SEC-Stick Server schützt das Netzwerk effizient gegen „Denial-of-Service“ Attacken und gegen „Bruteforce“ Angriffen auf die Benutzerkonten.

Vergleich IPsec VPN und SSH VPN

Der team2work SEC-Stick benutzt die sichere Art der
SSH VPN Anwendungsverbindung für den Entfernten Zugriff.

GEFAHREN REGULÄRE IPSEC VPN	VORTEIL SSH VPN (SEC-STICK)
NETZTRENNUNG	
IPsec arbeitet direkt auf der Internetschicht (Internet layer) des Protokollstapels (Verbindung auf Netzwerkebene). Damit wird jeder IPsec VPN-Client automatisch auch Mitglied des gerouteten Firmen-LAN.	Das SSH Protokoll benutzt Secure Application Tunneling (Sicheres Tunneln) zum transparenten Schutz des LAN und TCP/IP-basierender Anwendungen als End-to-End-Security (E2EE). Somit wird der SSH Client niemals Mitglied im gerouteten Firmen LAN, sondern es wird lediglich der dedizierte Serverdienst entfernt zur Verfügung gestellt.
SERVER ZUGRIFFSREGELN	
IPsec Verbindungen können innerhalb des VPN Tunnel durch Firewallregeln beschränkt werden, ansonsten besteht eine volle Netzkopplung	SSH Tunnelverbindungen müssen pro Anwendung dediziert freigegeben werden und müssen dadurch granular autorisiert werden.
VERBINDUNGSAUFBAU / DATENFLUSS	
Der Datenverkehr kann in beide Richtungen stattfinden (VPN Client zu LAN und LAN zu VPN-Client).	Der Verbindungsaufbau findet immer nur vom Client zum Server statt. LAN Teilnehmer können standardmäßig nie auf den SSH-Client zugreifen.
FREIGABEZUGRIFFE / ÜBERTRAGUNG VON VIREN	
Der Zugriff auf Netzwerkfreigaben ist in beide Richtungen problemlos möglich.	Der Zugriff auf Netzwerkfreigaben ist nicht möglich. Dateiübertragung muss explizit konfiguriert werden.
KOMFORT	
Ein IPsec VPN benötigt immer einen virtuellen Netzwerkadapter, der auf dem Client-System installiert werden muss. Mehrere dieser Adapter unter Windows verursachen oft Probleme.	SSH Clients sind portabel und können auch ohne Adminrechte und Installation benutzt werden.

Der SEC-Stick und GoDigital

Das Corona-Virus stellt tausende von kleinen und mittleren Unternehmen vor die Frage: Wie kann ich meine Mitarbeiter UND mein Unternehmen schützen? Nicht jeder Mitarbeiter hat die benötigte Hardware oder Software, um vollumfänglich und vor allem kurzfristig von Zuhause weiter arbeiten zu können. Diese Tatsache stellt die Unternehmen neben der unsicheren, wirtschaftlichen Lage vor weitere finanzielle Engpässe.

Doch jetzt naht Hilfe – das „Go-Digital"-Förderprogramm

„Go-Digital" ist ein Förderprogramm des Bundesministeriums für Wirtschaft und Energie (kurz BMWi), das sich ganz gezielt an kleine und mittlere Unternehmen der gewerblichen Wirtschaft und dem Handwerk richtet.
Es werden verschiedene Module angeboten: Neben „Digitale Markterschließung" und „IT-Sicherheit" gibt es auch das Modul 3 „Digitalisierung von Geschäftsprozessen". Dieses Modul wird aufgrund der Corona-Krise erweitert und berücksichtigt die Einrichtung von Homeoffice-Arbeitsplätzen. Im Vordergrund stehen hierbei die Beschaffung und die Einrichtung der Hardware, aber auch die Installation der Software, die über das normale Maß hinausgehen. **Für unsere Kunden bedeutet das: Der SEC-Stick von team2work ist förderfähig!**

Unbürokratische Hilfe für ein sicheres Homeoffice

Sie müssen nicht auf Ihre Zuwendungsbescheide warten, sondern profitieren von einem sofortigen Maßnahmenbeginn! Das Förderprogramm „Go-Digital“ verspricht schnelle und unbürokratische Unterstützung.

Ihre nächsten Schritte?

Überzeugen Sie sich selbst von der KUMA IT-Solutions und fordern Sie ihr unverbindliches Angebot an.

KUMA IT kennenlernen:

Ihr persönliches Angebot:

Ausführliche Information:
https://kuma-its.de

info@kuma-its.de

Sprechen Sie uns an:
+49(0)2841 9814600