Sicheres Coworking in Zeiten von Corona

Ein Leitfaden von **PwC Cyber Security & Privacy**
20. März 2020

pwc

Herausforderungen

Pandemie

Viele Unternehmen stehen auf Grund der aktuellen Bedrohungslage von Covid-19 vor der Herausforderung, ihre Mitarbeiter remote anzubinden.

Sicherheit

Ad-hoc aufgebaute Strukturen sind anders als die etablierten Strukturen nicht auf Sicherheitslücken getestet und bergen damit nicht zu unterschätzende Risiken in Bezug auf Datenschutz und Datensicherheit.

Infrastruktur

Üblicherweise sind die Infrastrukturen von Firmen nicht auf die Anbindung aller Mitarbeiter an das Firmennetz ausgelegt.

Eine Möglichkeit zur Fortführung der Tätigkeiten der Mitarbeiter muss schnellstmöglich zur Verfügung gestellt werden.

Lösung

Dieser Leitfaden soll Sie unterstützen, die richtige Coworking Lösung für Ihr Unternehmen zu finden.

1

Risiken, Prioritäten und Compliance

Risiken bei der Bereitstellung von Ad-hoc Lösungen

Auslastung

Evtl. sehr hohe Auslastung von IT-Services, IT-Infrastruktur, Bandbreiten durch vermehrte Remote-Zugriffe auf das Unternehmensnetzwerk.

Monitoring

Verlagerung der Prioritäten innerhalb der IT-Organisation und dadurch fehlendes oder unzureichendes Monitoring von Sicherheitsvorfällen.

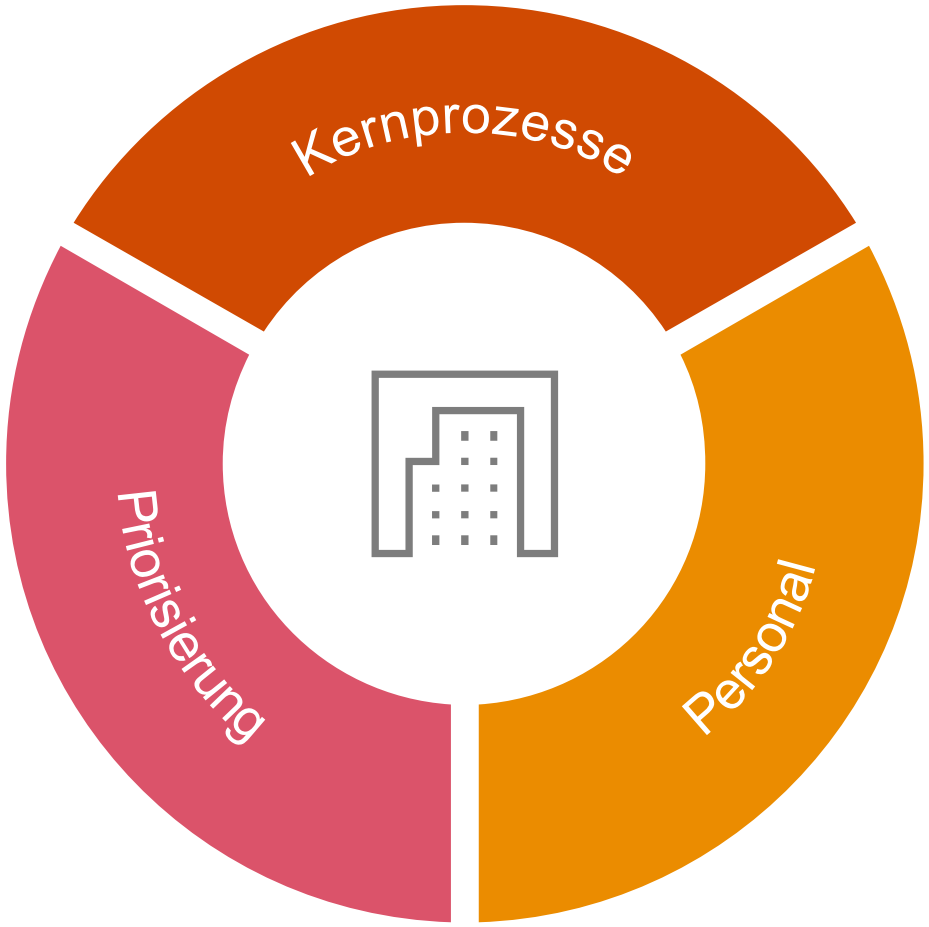
Nachvollziehbarkeit

Fehlende Koordination und mangelhafte Kommunikationswege.

Fehlender Fokus auf die Dokumentation der Implementierung von Ad-hoc Lösungen.

Fokus auf der Bereitstellung von Services, nicht auf Funktions- und Sicherheitstests vor Inbetriebnahme.

Welche Prozesse sind essentiell für den Fortbestand des Unternehmens?



Kernprozesse

Welche Unternehmensbereiche bzw. Prozesse sind auf Ad-hoc Lösungen angewiesen (und geeignet)?

Welche Prozesse erbringen für das Unternehmen bzw. dessen Kunden essentielle Leistungen?

Personal

Welche MitarbeiterInnen bzw. Benutzerzugänge sind für die Aufrechterhaltung dieser Prozesse zwingend erforderlich?

Priorisierung

Welche Bereiche und Prozesse werden priorisiert für Coworking freigeschaltet?

Priorisierung dafür notwendiger IT-Services und ggf. Entlastung dieser, durch Sperrung nicht benötigter Services und Benutzerzugänge?

Compliance

Abgleich der Lösungsansätze mit **Sicherheitsrichtlinien** innerhalb der Organisation.

Einhaltung geltender Gesetze **(z.B. Datenschutz)** und vertraglicher Regelungen zur Cyber Security (z.B. Kundenverträge).

Berücksichtigung von **Sicherheitsstandards** bei der Beschaffung von Lösungen für den Notfallbetrieb.

2

Leitfaden

Sind Coworking Möglichkeiten vorhanden?

JA

Ausbau und Verwendung

Dinge, auf die Sie nun achten müssen:

- Systemressourcen
- Beschränkungen
- Lizenzen
- Information der Mitarbeiter
- Einhaltung der Richtlinien
- Sicherheitsrisiken durch Last

NEIN

Auswahl und Implementierung

Dinge, auf die Sie nun achten müssen:

- Auswahl der richtigen Produkte/Lösungen
- Geeignete Skalierung
- Lizenzen und Vertragslaufzeiten
- Implementierungsaufwand
- Information der Mitarbeiter
- Sicherheitsaspekte und Risiken
- Eventueller Rückbau der Lösung

Eine Coworking Möglichkeit EXISTIERT.

Dinge, auf die Sie nun achten müssen:

- Systemressourcen
- Beschränkungen
- Lizenzen
- Information der Mitarbeiter
- Einhaltung der Richtlinien
- Sicherheitsrisiken durch Last

Upscaling

von vorhandenen Möglichkeiten des Remote-Arbeitens.

Implementierung

Sind genügend Systemressourcen (WAN, LAN, CPU, RAM) für alle nötigen Mitarbeiter vorhanden?

Wo sind die Bottlenecks der Lösung?

Last als Sicherheitsrisiko?

Lizenzen

Wo werden Lizenzen benötigt?

Sind genügend Lizenzen vorhanden?

Wer benötigt Lizenzen?

Werden neue Lizenzen benötigt?

Wer beschafft die Lizenzen?

Monitoring

Wie werden die Anforderungen der Nutzer bedient?

Wie werden die Lösungen überwacht?

Richtlinien

Werden die vorhandenen Richtlinien (Umgang mit Firmeninformationen, etc.) eingehalten?

Müssen Richtlinien angepasst werden?

Risiken

Welche Risiken entstehen?

Wie können Risiken vermieden werden?

Mitarbeiter

Wie werden die Mitarbeiter über die Möglichkeiten informiert?

Welche Informationen benötigen die Mitarbeiter (Handout, Anleitung)?

Planung

Welche Anforderungen existieren? Welche Produkte kommen in Frage?

Systemressourcen

On Premise vs. Cloud
Wie schnell lässt sich die Lösung bereitstellen?
Kann die Lösung remote ausgerollt werden?

Lizenzen

Kommerziell vs. Open Source
Wo werden Lizenzen benötigt?
Sind genügend Lizenzen vorhanden?
Wer benötigt Lizenzen?
Werden neue Lizenzen benötigt?
Wer beschafft die Lizenzen?

Monitoring

Wie werden die Anforderungen der Nutzer bedient?
Wie werden die Lösungen überwacht?

Richtlinien

Werden die vorhandenen Richtlinien (Umgang mit Firmeninformationen, etc.) eingehalten?
Müssen Richtlinien angepasst werden?

Risiken

Welche Risiken entstehen?
Wie können Risiken vermieden werden?

Mitarbeiter

Wie werden die Mitarbeiter über die Möglichkeiten informiert?
Welche Informationen benötigen die Mitarbeiter (Handout, Anleitung)?

Eine Coworking Möglichkeit EXISTIERT NICHT.

Dinge, auf die Sie nun achten müssen:

- Auswahl des richtigen Produkts
- Geeignete Skalierung
- Lizenzen und Vertragslaufzeiten
- Implementierungsaufwand
- Information der Mitarbeiter
- Sicherheitsaspekte und Risiken
- Eventueller Rückbau der Lösung

3

Mögliche Lösungen

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen.

Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden, ob im Anwendungsfall personenbezogene Daten verarbeitet werden.

Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Collaboration – Voice and Video

Lösung	Sicherheit	Risiko			Implementierung			
	Sicherheitsaspekte / Best Practice	Niedrig	Mittel	Hoch	Lizenzierung	Deployment	Standards	Website
(GSM-)Telefonie	Kommunikation erfolgt unverschlüsselt			×	Nicht notwendig	Bereits vorhanden	Offen	-
Microsoft Skype (for Business)	P2P-Kommunikation, verschlüsselt, MFA	×			2 $/Nutzer/Monat, kostenlos enthalten in Office 365	Installation/ schnell	Proprietär	.skype.com
Google Hangouts (Meet)/Chats	Nur Transport-Verschlüsselung, MFA		×		Ab 4,68 €/Monat, Lizenzierung über GSuite	Browser/ schnell	WebRTC	hangouts.google.com
Cisco Webex	Ende-zu-Ende Verschlüsselung, MFA	×			Ab 12,85 €/Monat/Gastgeber	Browser/ Installation	WebRTC/proprietär	webex.com
Zoom	Transport-Verschlüsselung, Ende-zu-Ende Verschlüsselung(optional)			×	Für kurze Meetings mit wenig Teilnehmern kostenlos	Installation	Proprietär	zoom.us
Slack	Nur Transport-Verschlüsselung, MFA		×		Ab 6,25 € für Teams bis 15 Mitglieder	Installation	WebRTC	slack.com
Microsoft Teams	Nur Transport-Verschlüsselung, MFA		×		Ab 4,20 €/Monat/Nutzer für Office 365	Browser/ Installation	Proprietär	products.office.com/de-DE/microsoft-teams
Jitsi	Ende zu Ende Verschlüsselung, selbst gehostet	×			Open Source	Server-installation	Offen	www.jitsi.org

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Collaboration – Voice and Video – Aktuelle Empfehlungen

Wegen der aktuellen Situation bieten zahlreiche Hersteller ihre Software für einen begrenzten Zeitraum kostenlos an.

So darf beispielsweise **Team**Viewer aktuell auch ohne Lizenz unbegrenzt kommerziell genutzt werden, **CISCO** bietet eine vollwertige Testversion kostenlos für 90 Tage an.

Mit der Open Source Lösung **jitsi.org** bietet sich die Möglichkeit, Videokonferenzen selbst zu hosten.

Weitere Lösungen sind **Google Hangouts** und

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Collaboration – Data Exchange

Lösung	Sicherheit	Risiko			Implementierung			
	Sicherheitsaspekte / Best Practice	Niedrig	Mittel	Hoch	Lizenzierung	Deployment	Risiken	Partner
Email (On Premise) (Enduser / Technical Staff)	• Webzugang zum Emailpostfach ist von extern erreichbar • Verschlüsselter Dateiversand (Ende-zu-Ende möglich) • Mehrfaktor Authentifizierung	✕			Es sind normalerweise keine zusätzlichen Lizenzen nötig.	Schnell	• Angriffe von Außen • Unzureichende Ressourcen	OWA
Email (Cloud) (Enduser / Technical Staff)	• Cloud Anwendungen ist mit zentralem Verzeichnisdienst verknüpft • Cloudanbieter befindet sich in Deutschland • Mehrfaktor Authentifizierung		✕		Lizenzen müssen beschafft werden.	Sehr schnell	• Verlust der Datenhoheit • Datenschutz evtl. nicht gegeben	Office 365
Anwendungen / Dateiablage (On Premise) (Enduser / Technical Staff)	• Webzugang zur Dateiablage ist von extern erreichbar • Mehrfaktor Authentifizierung		✕		Es können weitere Lizenzen nötig sein.	Mittel	• Angriffe von Außen • Unzureichende Ressourcen • Unsichere Übertragung/Ablage von sensiblen Daten	Sharepoint, Nextcloud, Owncloud, Jira, Confluence
Anwendungen / Dateiablage (Cloud) (Enduser / Technical Staff)	• Cloud Anwendungen ist mit zentralem Verzeichnisdienst verknüpft • Cloudanbieter befindet sich in Deutschland • Mehrfaktor Authentifizierung		✕		Lizenzen müssen beschafft werden.	Sehr schnell	• Verlust der Datenhoheit • Datenschutz evtl. nicht gegeben • Unsichere Übertragung/Ablage von sensiblen Daten	Office 365, Google Suite, Mega, Jira, Confluence, Libre Office Online
Instant Messenger (Enduser)	• Daten werden Passwort gesichert verpackt und anschließend verschickt • Trennen von Beruflichen und Privaten Daten			✕	Es sind normalerweise keine zusätzlichen Lizenzen nötig.	Sehr schnell	• Eventuell unverschlüsselte Datenübertragung und Speicherung beim Betreiber	Threema, Whatsapp, Slack
Analogen Datenaustausch (Enduser)	• Speicherung auf verschlüsselten und sicheren USB Sticks • Sicherer Transport		✕		nicht notwendig	Schnell	• Abfluss von Firmendaten • Verlust von Datenträgern	Bitlocker, Veracrypt

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Collaboration – Data Exchange – Aktuelle Empfehlungen

Kurzfristiges Ausweichen auf Dateiablagesysteme

OneDrive
Businesskunden von Office365 können den Dienst OneDrive mit 1TB zur Dateiablage nutzen.

OwnCloud
Das Open Source Dateiablagesystem lässt sich kostengünstig on Premise ausrollen.

Mega
Die Business-Variante von Mega bietet unbegrenzten und verschlüsselten Speicherplatz in europäischen Rechenzentren. Darüber hinaus kann dort auch verschlüsselt per Sprach/Video/Text kommuniziert werden. Dienstleister können zudem Dateien hochladen ohne sich am Dienst anzumelden.

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Connectivity – Anbindung der Remote-Arbeitsplätze

Lösung	Sicherheit	Risiko			Implementierung			
	Sicherheitsaspekte / Best Practice	Niedrig	Mittel	Hoch	Lizenzierung	Deployment	Risiken	Partner / Lösungen
VPN (Enduser / Technical Staff)	Nutzung sicherer Schlüssel und aktueller kryptographischer Algorithmen, Multi-Faktor Authentifizierung, No Split-Tunneling, Load Balancing.	×			Je nach Lösung, teilweise aufwändig	Mittel	Hohe Last auf VPN Gateway / WAN	Always On VPN, IPSEC (Nahezu jede Firewall)
VDI On-Premises (Enduser / Technical Staff)	Absicherung der Infrastruktur, angemessenes Load Balancing, Dimensionierung, Multi-Faktor-Authentifizierung.	×			Zeitaufwändig	Langsam	Fehler bei der Konfiguration, Komplex, Scaling	Citrix, VMWare Horizon, Nutanix, Nvidia VDI
VDI Cloud (Enduser / Technical Staff)	Absicherung der Cloud Umgebung, Multi-Faktor-Authentifizierung, Berücksichtigung Datenschutz.		×		Flexibel, schnell	Schnell	Datenschutz nicht gewährleistet, Datenhoheit	Amazon WorkSpaces, Itopia, Azure VDI
Terminalserver (Enduser / Technical Staff)	Absicherung der Verbindung (VPN).		×		Flexibel, schnell	Mittel	Scaling	Microsoft Terminalserver
Remote Desktop (Technical Staff)	Beschränkung des Zugriffs auf Benutzer und Maschinenebene, Datenschutz.			×	Flexibel, je nach Lösung mittel - schnell	Sehr schnell	Evtl. unsichere Verbindung, skaliert schlecht	Teamviewer, Microsoft RDP, Splashtop
SSH (Technical Staff)	Verwendung sicherer Schlüssel / SSH over VPN, Absicherung technischer User, sichere Konfiguration des SSH Servers.	×			Nicht notwendig	Sehr schnell	Unsichere User	Putty, Bitvise, OpenSSH
Lokales Arbeiten (Enduser)	Absicherung der Endpoints (Verschlüsselung), regelmäßiges Backup der Daten, sicherer Datenaustausch.	×			Nicht notwendig	Schnell	Datenverlust, Inkonsistente Datensätze	Nutzung der Workstation im HomeOffice

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Connectivity – Aktuelle Empfehlungen

Kurzfristiges Ausweichen auf virtuelle Desktop Infrastruktur (geräteunabhängig)

itopia

Itopia & Google
Nutzung vergünstigter Desktop as a Service Modelle
https://www.itopia.com/desktop-as-a-service/

Microsoft Virtual Desktop
https://azure.microsoft.com/en-us/services/virtual-desktop/#product-overview

Microsoft Azure

Amazon WorkSpaces
https://aws.amazon.com/workspaces/

Sofern eine Anbindung an das Unternehmensnetzwerk benötigt wird, muss die bestehende Infrastruktur an die Cloud Lösung angebunden werden.

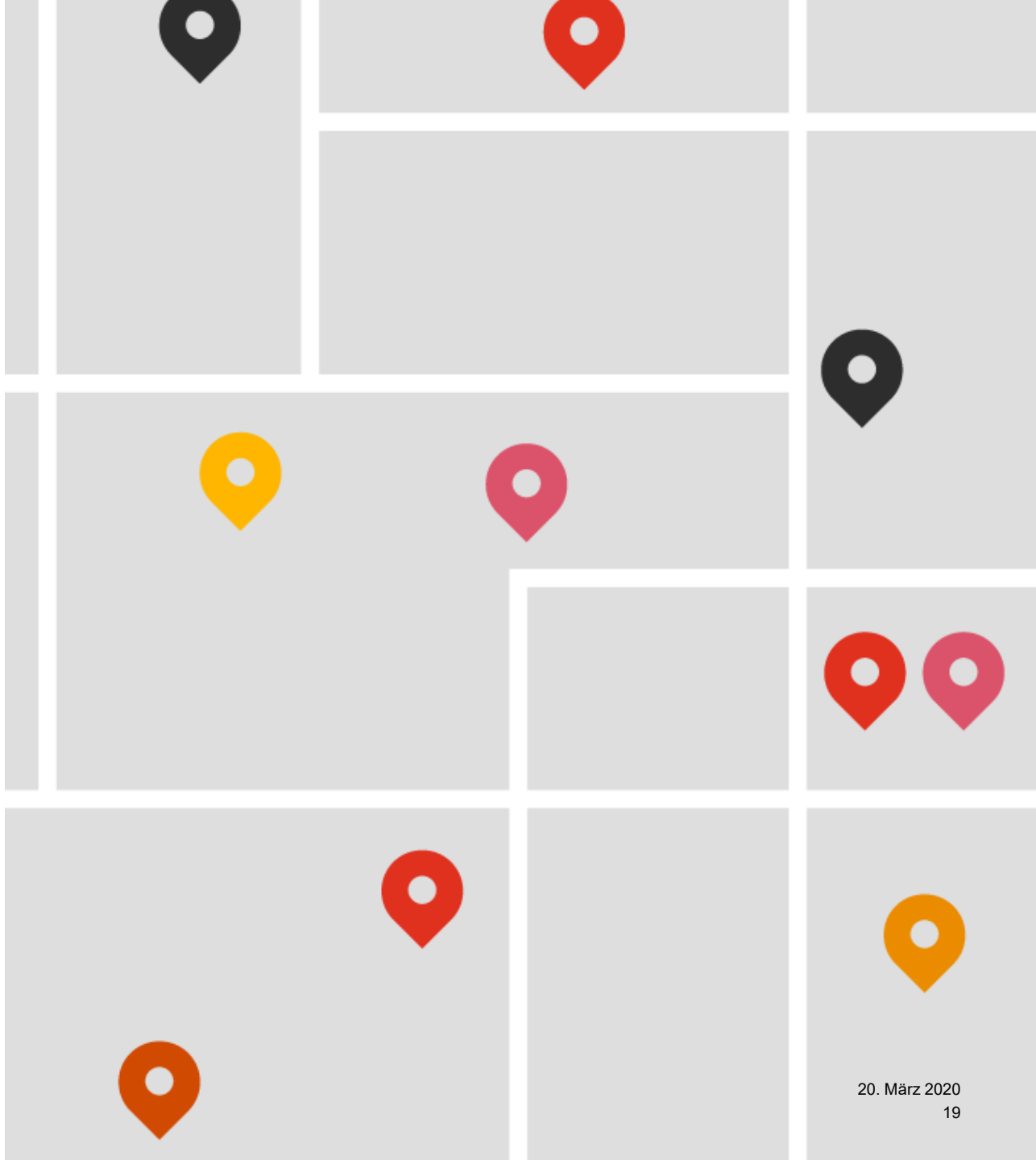
In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Endpoints – Bereitstellung von Hardware im Homeoffice

Lösung	Sicherheit	Risiko			Implementierung			
	Sicherheitsaspekte / Best Practice	Niedrig	Mittel	Hoch	Lizenzierung	Deployment	Risiken	Partner / Lösungen
Corporate Mobile Device (Enduser / Technical Staff)	Absicherung der Endpoints (Verschlüsselung), Regelmäßiges Backup der Daten, Sicherer Datenaustausch, Regelmäßige Sicherheitsupdates, Endpoint Security.	×			flexibel, schnell	Mittel	Beschaffung und Deployment skalieren schlecht.	Dell, HP, Lenovo, Apple, Fujitsu
Corporate Workstation (Enduser / Technical Staff)	Absicherung der Endpoints (Verschlüsselung), Regelmäßiges Backup der Daten, Sicherer Datenaustausch, Regelmäßige Sicherheitsupdates, Endpoint Security.	×			flexibel, schnell	Mittel	Beschaffung und Deployment skalieren schlecht.	Dell, HP, Lenovo, Apple, Fujitsu
BYOD / UYOD (Enduser)	Wenn möglich nur über VDI*.		(×*)	×	flexibel, schnell	Sehr schnell	Datenschutz nicht gewährleistet, Datenhoheit, Fehlende Absicherung der Endpoints.	Chromebook, Samsung, Apple, Huawei etc.
Chromebook / iPad / Tablet / Smartphone (Enduser)	Absicherung des OS, Aktuelle Firmware, Mobile Device Management, Endpoint Security.			×	flexibel, schnell	Mittel	Absicherung komplex.	Microsoft Terminalserver

In der Regel fallen für die gewerbliche Nutzung der genannten Lösungen Lizenzkosten an. Bei der Auswahl der Lösung sollte stets geprüft werden, welche Versionen im gewerblichen Kontext eingesetzt werden dürfen. Da einige Lösungen bzw. Dienste nicht in Einklang mit den Anforderungen der DSGVO stehen, sollte darüber hinaus geprüft werden ob im Anwendungsfall personenbezogenen Daten verarbeitet werden. Die hier aufgeführten Angaben zum Datenschutz beziehen sich auf die Angaben der Hersteller und wurden nicht explizit durch PwC geprüft.

Endpoints – Aktuelle Empfehlungen



Die Verlagerung der Arbeitsplätze führt teilweise zu Problemen bei der Bereitstellung von notwendiger Hardware.

Falls nicht genügend mobile Arbeitsplätze (Laptops, ThinClients) zur Verfügung stehen, kann die Nutzung von Workstations im Home-Office eine Alternative darstellen.
Dies ist insbesondere dann relevant, wenn die Leistung der Workstation oder spezielle Software relevant sind.

Anbindung virtueller Arbeitsplätze

Die meisten Cloud Dienste bzw. virtuellen Arbeitsplätze (Siehe Connectivity) sind auf unterschiedlichen Endgeräten nutzbar. Daraus ergeben sich unterschiedliche Optionen:

- Nutzung über Tablets / Convertibles mit zusätzlicher Maus und Tastatur (z. B. über Bluetooth).
- Nutzung privater Geräte (BYOD / UYOD) unter Berücksichtigung der Sicherheitsaspekte (z.B. Vermeidung lokaler Datenhaltung durch Arbeiten über VDI).

Bereitstellung zusätzlicher Hardware

- Temporäre Bereitstellung älterer Hardware (sofern vorhanden) für Anwendungen ohne hohe Anforderungen an die Performance.
- Kurzfristige Beschaffung zusätzlicher Hardware über Mietmodelle (z.B. liverental.de oder grover.com, Dell PCaaS etc.).

4

IT-Sicherheitsaspekte im Home-Office

Bedrohungen im Home-Office

Endpoint Protection als Sicherheitsfokus bei der Remote Arbeit

Dateiaustausch über unsichere Kanäle

Anwender nutzen unsichere Dienste, um Firmendaten auszutauschen.

Unzureichender Malwareschutz

Es ist kein oder nur unzureichender Malwareschutz installiert. Anwender haben Administratorrechte.

Daten können durch Malware exfiltriert oder verschlüsselt werden.

Dateneinsicht durch Dritte

Durch unzureichenden Einsichts- oder Zugriffsschutz können Dritte Einblick auf Firmendaten über das physische Gerät erhalten.

Unverschlüsselte Datenträger

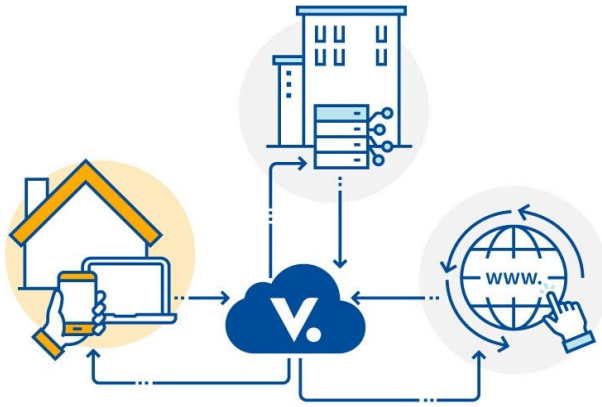
Bei Entwendung des Gerätes können lokal gespeicherte Daten ausgelesen, sofern einzelne Dateien oder das Dateisystem nicht verschlüsselt ist.

Integrierte cloudbasierte Sicherheitsdienste

Cloudbasierte Sicherheitslösungen haben den Vorteil, dass sie relativ schnell und kurzfristig auf Endgeräten eingesetzt werden können und flexibel lizenzierbar sind. Viele Cyber Security Service Provider (CSSP) ermöglichen eine Installation innerhalb weniger Minuten auf dem Client und die Integration in das bestehende Netzwerk.

Diese Lösungen sind einfach orchestrierbar und können je nach Bedarf erweitert oder reduziert werden. Oft werden mehrere Monitoring- und Visualisierungsmöglichkeiten angeboten, um Anomalien und damit mögliche Bedrohungen schnell erkennen zu können.

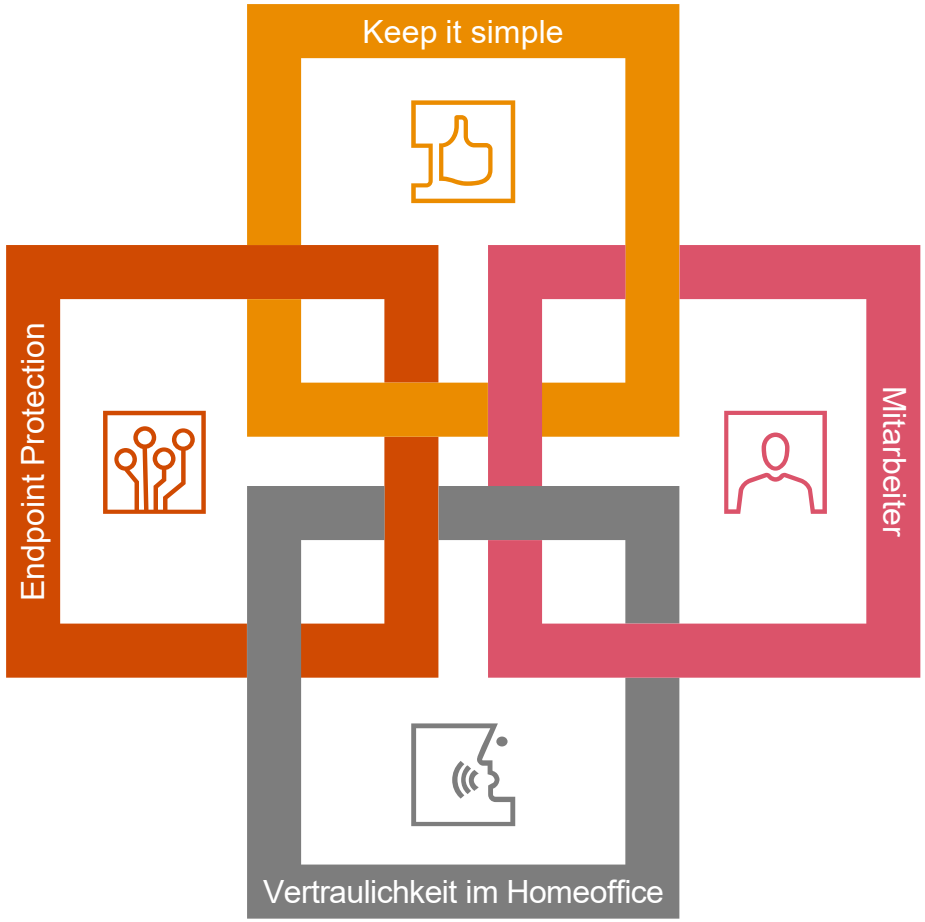
Veronym bietet einen solchen Service an und ist als einer der wenigen Anbieter DSGVO-konform. Damit kann diese Lösung gemäß der geltenden Datenschutzrichtlinien in Deutschland betrieben werden.



veronym.
security first

IT-Sicherheit im Home-Office

So stellen Sie Ihre IT-Sicherheit im Home-Office sicher.



Mitarbeiter

Den Mitarbeitern sollten verbindliche Richtlinien an die Hand gegeben werden, welche Sicherheitslösungen sie einsetzen sollen.

Keep it simple

Es sollte auf die bereits in Windows zur Verfügung gestellten Standardanwendungen, wie Windows Defender und Windows Firewall zurückgegriffen werden, um den Support-Aufwand gering zu halten.

Endpoint Protection

Die Absicherung der Endpoints (Datenhaltung, sichere Übertragung von Daten, Schutz vor Malware) bzw. des Heimarbeitsplatzes steht bei der Remote Arbeit im Fokus.

Vertraulichkeit im Homeoffice

Insbesondere im Homeoffice ist ein sorgsamer Umgang mit vertraulichen Informationen wichtig (z.B. Vertraulichkeit bei Telefongesprächen und Meetings). Informationen und Dokumente sind vor der Einsichtnahme Dritter zu schützen.

5

Kontakte

Unsere Ansprechpartner

Aleksei Resetko
Partner, CISA, CISSP
Cyber Security & Privacy

PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Friedrich-Ebert-Anlage 35-37
60327 Frankfurt am Main

Telefon + 49 69 9585 5059
Mobil + 49 151 14268214
aleksei.resetko@pwc.com

Jörg Asma
Partner
Cyber Security & Privacy

PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Konrad-Adenauer-Ufer 11
50668 Köln

Telefon + 49 211 982 6103
Mobil + 49 160 6142945
joerg.asma@pwc.com

Derk Fischer
Partner
Cyber Security & Privacy

PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Moskauer Str. 19
40227 Düsseldorf

Telefon + 49 211 981 2192
Mobil + 49 170 7946797
derk.fischer@pwc.com

Danke!

pwc.com

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.