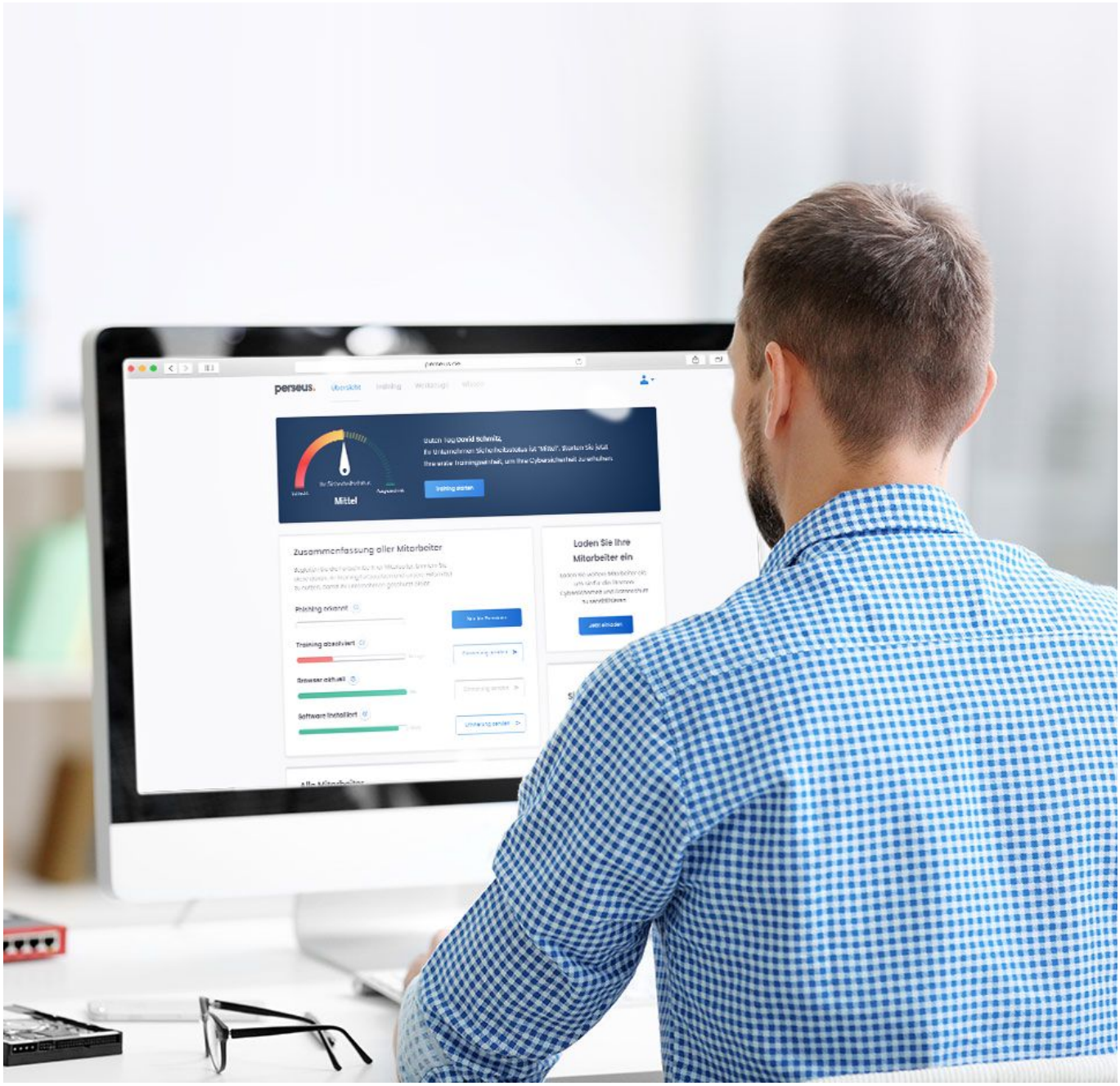

Leitfaden: Cybersicherheit im Homeoffice

Arbeiten im Homeoffice bietet viele Vorteile, aber auch Gefahren. So können Sie sich auch zuhause vor Cyberkriminellen schützen!

perseus.
Cybersicherheit auf den Punkt

1. Eine sichere Verbindung

Größere Unternehmen beschäftigen in der Regel IT-Spezialisten, in deren Verantwortung die Cybersicherheit des Unternehmens liegt. Das beinhaltet auch den Schutz Ihres Internetzugangs und der Unternehmens-Cloud gegen externe Angriffe. Sobald Sie aber das Büro verlassen, verlassen Sie diesbezüglich ein Stück weit sicheren Boden.

Wenn Sie außerhalb des Büros arbeiten ist vor allem bei fremden WLAN-Netzwerken und Computern Vorsicht geboten. Betrüger könnten sich mittels spezieller Software oder über unzureichend gesicherte Anwendungen zwischen Sie und dem entsprechenden Server platzieren, um Ihre Kommunikation mitzulesen oder zu manipulieren. Dadurch verschaffen sie sich Zugang zu der Unternehmens-IT und sensiblen Daten. Man spricht bei solchen Vorfällen von einem Man-in-the-middle Angriff.

Firewall aktivieren!

Aktivieren Sie Ihre Firewall in den Sicherheitseinstellungen Ihres Computers*
Vorsicht bei nicht gesicherten WLAN-Netzwerken! Stellen Sie die Funktion, sich automatisch mit offenen WLAN-Netzwerken zu verbinden ab. Nutzen Sie stattdessen mobile Daten und surfen Sie mit Ihrem Laptop per Handy-Hotspot oder über ein virtuelles privates Netzwerk (VPN), wenn Ihre Firma eines zur Verfügung stellt.

**Weitere Information in der angehängten Kurzanleitung "Firewall"*

2. Gefahren durch private Endgeräte oder "Schatten-IT"

Unter Schatten-IT versteht man Programme, Dienste oder private Geräte, die Mitarbeiter im Zusammenhang mit Firmendaten ohne vorherige Abstimmung nutzen.

In der aktuellen Situation, in der viele Beschäftigte ohne lange Vorausplanung ins Homeoffice entlassen wurden, ist die Gefahr groß, dass Mitarbeiter, die beispielsweise ihren Desktop-PC vom Arbeitsplatz nicht mit nach Hause nehmen können, von ihrem Privatrechner aus auf die Unternehmens-Cloud zugreifen, um ihre Arbeit fortführen zu können.

Jedes unbekannte Gerät oder Programm stellt ein mögliches Sicherheitsrisiko für Unternehmensdaten dar. Wenn die Verantwortlichen nicht von ihrer Existenz wissen, können sie nicht die notwendigen sicherheits- oder datenschutzrelevanten Vorkehrungen treffen.

Keine Informationen auf privaten Endgeräten

Verarbeiten Sie keine Firmendaten auf privaten Endgeräten. Wenn es sich angesichts der aktuellen Situation nicht vermeiden lässt, lassen Sie sich diese Nutzung im Vorfeld genehmigen oder statten Sie das Gerät mit der nötigen Software für ein sicheres Arbeiten aus.

DSGVO: Datenschutz gilt auch Zuhause!

Auch wenn Sie nicht in Ihrem Büro arbeiten, bleibt Datenschutz ein wichtiges Thema:

- Die Datenschutz-Grundverordnung (DSGVO) enthält zwar keine speziellen Regelungen zum Homeoffice, aber Ihre Pflichten bleiben bestehen. Entsprechend wichtig ist es, durch geeignete technische und organisatorische Maßnahmen (sogenannte TOMs) mögliche Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit der von zu Hause aus verarbeitenden personenbezogenen Daten zu vermeiden.
- Neben den bereits genannten Maßnahmen empfiehlt sich die Herausgabe einer sogenannten zusätzlichen Richtlinie für die Heimarbeit - die ist jedoch keine Pflicht. Bestehende (IT-)Betriebsvereinbarungen haben auch im Homeoffice ihre Gültigkeit!

3. Phishing-Gefahren durch eingeschränkte persönliche Kommunikation

Kriminelle Hacker nutzen Sondersituationen geschickt aus, um ihre Opfer auszutricksen und an ihre Daten zu gelangen. Seien sie daher besonders aufmerksam, wenn sie von Unbekannten E-Mails zu aktuellen Ereignissen erhalten oder zu einer konkreten Handlung aufgefordert werden. Kriminelle geben sich oft auch als Kollegen und Vorgesetzte aus (CEO-Fraud). Achten Sie folglich auf Warnhinweise bei Schreibstil und Kommunikationsart. Kontaktieren Sie den Kollegen über einen zweiten Kommunikationskanal, um die Echtheit seiner Nachricht zu prüfen.

Updates installieren, suspekte Inhalte und Aufforderungen gegenprüfen!

Bei Phishing und insbesondere beim CEO-Fraud handelt es sich nicht zwingend um einen technischen Angriff.

Seien Sie bei E-Mails von Unbekannten misstrauisch, wenn Sie zu einer bestimmten Handlung aufgefordert werden, wie zum Beispiel zur Installation eines Programms, Herausgabe von Information oder Überweisung einer Geldsumme. Beachten Sie hier ihre internen Kommunikationsprozesse, die auch im Homeoffice gelten!

Wenn Vorgesetzte es eilig haben...

Für CEO-Fraud-Angriffe sollten Sie immer auf den Schreibstil und die Kommunikationsart ihrer vermeintlichen Vorgesetzten achten. Siezt Sie Ihr Chef plötzlich, obwohl sie sonst per Du sind? Verwendet er eine ungewöhnliche Grußformel? Schreibt er normalerweise ausschweifend, jetzt aber nur sehr knapp?

All das können Warnsignale sein. Und im Zweifel gilt: kontaktieren Sie den Kollegen über einen anderen Kommunikationskanal, um die Echtheit der Nachricht zu prüfen – lieber einmal zu viel, als zu wenig.

Arbeiten an der frischen Luft? Vorsicht vor neugierigen Nachbarn!

Wenn Sie nicht im Büro arbeiten, laufen Sie immer Gefahr, dass sensible Firmeninformationen “nach draußen” gelangen – einfach weil Sie selbst “draußen” sind.

Überlegen Sie sich genau, welche Telefonate oder Videokonferenzen Sie auf dem Balkon führen wollen, wenn potentiell die gesamte Nachbarschaft zuhört. Vielleicht doch lieber ein Gespräch im Online-Chat?

Ein Mitglied Ihres Haushalts arbeitet bei einem Mitbewerber? Nutzen Sie eine Sichtschutzfolie für Ihren Rechner - damit gehen Sie auf Nummer sicher!

Auch im Homeoffice gilt es Betriebsgeheimnisse zu schützen – von Kundendaten ganz zu schweigen!

Checkliste CEO-Fraud: Wie entlarve ich die Fake-Geschäftsführung?

1. Schreibstil

Jeder hat einen eigenen Schreibstil. Wenn es hier Abweichungen gibt, sollten Sie aufhorchen. Grüßt Sie Ihr Chef per Sie oder Du? Verwendet er immer gewisse Redewendungen oder Formulierungen? Hat er eine individuelle Signatur? Vielleicht steht unter den Nachrichten gewöhnlich “von meinem Mobiltelefon gesendet”, jetzt aber “von meinem iPhone gesendet” obwohl Ihr Chef ein großer Android-Fan ist?

2. Kommunikationswege

Wenn Ihr Chef immer per E-Mail kommuniziert, Ihnen jetzt aber plötzlich wichtige Anweisungen per Whatsapp schickt, könnte sein Handy durch SIM-Swapping gekapert worden sein. Gerade in Notsituationen sollte man sich auf verbindliche Kommunikationswege- und Prozesse einigen. Werden diese nicht eingehalten, sollten Sie nachfragen.

3. Rückfragen nicht möglich

Wenn der Chef Ihnen eine wichtige Anweisung schickt und direkt darauf hinweist, für Rückfragen nicht zur Verfügung zu stehen, bringt Sie das in eine schwierige Situation. Durch die Arbeit im Homeoffice ist oft nicht klar, welche Termine und Verpflichtungen anstehen oder welche Entscheidungen getroffen wurden. Insbesondere in der aktuellen Situation sollte transparenz darüber herrschen, wer wann nicht verfügbar ist. Hier stehen auch Führungskräfte in der Pflicht: Sorgen Sie für transparenz, klare Prozesse und sichere Kommunikationskanäle, damit sich Mitarbeiter stets rückversichern können, insbesondere bei wichtigen, weitreichenden Entscheidungen.

Checkliste: Verwendung privater Endgeräte

1. Wenn möglich vermeiden

Ja, Sie haben einen Dienstrechner, aber der Monitor Ihres privaten Notebooks ist größer, der Prozessor ist schneller, und Sie haben da noch ein Grafikprogramm installiert, das Sie gerne verwenden, deshalb arbeiten Sie lieber auf dem eigenen Gerät? Stopp! Selbst wenn es verlockend ist: wenn Sie über entsprechende Firmengeräte oder Acces-Gates (z.B. Citrix, Microsoft Terminal Server) verfügen, verwenden Sie für geschäftliche Tätigkeiten immer diese, nicht Ihre privaten.

2. Genehmigung einholen

Nutzen Sie auf keinen Fall Ihre eigenen Endgeräte ohne Erlaubnis Ihres Vorgesetzten und der IT-Verantwortlichen Ihres Unternehmens. Sonst könnten Sie nicht nur gegen Ihren Arbeitsvertrag verstoßen, sondern haften eventuell sogar für entstandene Schäden.

3. Endgeräte prüfen und ausrüsten lassen

Selbst wenn Ihr Unternehmen Ihnen die Nutzung der eigenen Endgeräte erlaubt, sollten sie vorher geprüft und wenn nötig “nachgerüstet” werden. Zum einen sollte sichergestellt sein, dass sich auf Ihren Geräten keine Malware befindet, die Angreifern den Zugang zu Ihrem Unternehmensnetzwerk ermöglicht. Eine aktuelle Antivirensoftware, Firewall, Festplattenverschlüsselung und andere Maßnahmen zur Erhöhung der Cybersicherheit sollten zwingend vorhanden sein. Zum anderen benötigen Sie vielleicht gewisse Softwarelösungen, wie einen VPN-Client, um sicher auf Ihre E-Mails oder die Unternehmens-Cloud zugreifen zu können oder proprietäre Softwarelösungen, die Ihr Unternehmen verwendet. All das können Ihre IT-Spezialisten für Sie einrichten, damit Sie sicher und ohne Einschränkungen weiterarbeiten können, selbst wenn Ihr Computer im Büro bleiben muss.

Kurzanleitung: So aktivieren Sie Ihre Firewall

1. Was ist eine Firewall?

Eine Firewall überwacht den eingehenden und ausgehenden Netzwerkverkehr und lässt Datenpakete auf Basis von Sicherheitsregeln zu oder blockiert diese. Sie stellt eine Barriere zwischen Ihrem internen Netzwerk und eingehendem Datenverkehr von externen Quellen (z. B. dem Internet) dar. Auf diese Weise wird durch den integrierten Filtermechanismus der Netzwerkverkehr verwaltet und Angriffe von außen werden abgewehrt.

2. Konfiguration Windows 10

Öffnen Sie das Startmenü und geben Sie in die Suchleiste den Begriff "Windows Defender Security Center" ein. Klicken Sie auf den Tab/Reiter „Firewall-& Netzwerkschutz." Ihnen bietet sich die Auswahl zwischen „Domänennetzwerk", „Privates Netzwerk" und „Öffentlich Netzwerk". Wählen Sie alle nacheinander entsprechend aus und aktivieren Sie die Firewall, indem sie jeweils den Button umlegen.

3. Konfiguration Mac OS X 10.5 und neuer

Wählen Sie im Apple-Menü die Option "Systemeinstellungen" und klicken Sie auf den Tab/Reiter „Sicherheit". Klicken Sie auf den Tab „Firewall" und wählen Sie den Modus aus, der für die Firewall verwendet werden soll.

Wichtiger Hinweis: Die Aktivierung der Firewall muss bei Apple-Geräten manuell vorgenommen werden, sie gehört nicht zu den Default-Einstellungen.

Wir machen **Cybersicherheit** einfach.

Perseus 360°-Cybersicherheitspaket abschließen und Bußgelder, Betriebsunterbrechungen und Reputationsschäden vermeiden!

Unsere Angebote

Start

Individuell vorsorgen

Perfekt für die Einzelperson, die kostenlos und schnell die Grundlagen der Cybersicherheit und des Datenschutzes erlernen möchte. Online, jederzeit und an jedem Ort.

Pro

Jetzt kostenlos testen

Ganzheitlich schützen

Cybersicherheit als Komplettservice: Perfekt für kleine und mittlere Unternehmen, die eine einfache, günstige und umfassende Cybersicherheits- und Datenschutzlösung suchen.

Premium

Zusätzlich abgesichert

Perfekt für Unternehmen, die mit einer zusätzlichen Kostenabsicherung Ihr Cyberrisiko minimieren wollen. Cybersicherheit Komplettservice mit Kosten-Airbag.

Alle Funktionen	Start	Pro	Premium
Online-Sicherheitstraining	✓	✓	✓
24/7 telefonische Notfallhilfe	✗	✓	✓
Simulierte Phishing-E-Mails	✗	✓	✓
Cybersicherheits-Führerschein	✗	✓	✓
Datenschutz-Führerschein	✗	✓	✓
IT-Sicherheitsprüfung	✗	✓	✓
Intelligente Sicherheitssoftware (EDR)	✗	✓	✓
Cybersicherheitsübersicht für Ihr Unternehmen	✓	✓	✓
Kundenservice Hotline	✗	✓	✓
Malware-Scanner	✓	✓	✓
Browser-Check	✓	✓	✓
Passwort-Generator	✗	✓	✓
Datensicherheits-Check	✗	✓	✓
Angriffsalarm	✗	✓	✓
Cyber-Schutzbrief			
IT-Forensik-Experten vor Ort	✗	✗	✓
Datenwiederherstellung und Entfernung der Schadsoftware	✗	✗	✓
Systemverbesserung nach Angriff (bis zu 10.000 €)	✗	✗	✓
Prüfung datenschutzrechtlicher Informationspflichten (bis zu 2.000 €)	✗	✗	✓

Über **Perseus**

Die Perseus Technologies GmbH wurde im September 2017 mit der Vision gegründet, dauerhaft IT-Sicherheit und Datenschutz zu ermöglichen. Ziel des mitarbeiterzentrierten Angebots von Perseus ist die Etablierung einer langfristigen Cybersicherheitskultur entlang aller Phasen einer Cyberattacke. Das Perseus 360 Grad-Konzept umfasst browserbasierte Mitarbeitertrainings, eine 24/7-Cyber-Notfallhilfe, eine intelligente Antivirensoftware sowie einen Cyber-Schutzbrief.

Der Unternehmensname Perseus lehnt sich an die Legende des Perseus an. Dieser Held der griechischen Mythologie steht für Schutz und Sicherheit. Für sein Engagement wurde Perseus im Dezember 2018 mit dem Digitalen Leuchtturm Award für innovative Versicherungsprodukte, von Google und der Süddeutschen Zeitung, ausgezeichnet.

Perseus ist eine 100 Prozent-Gesellschaft der HDI Gruppe.
Die 30 Mitarbeiterinnen und Mitarbeiter kommen aus sieben Nationen und arbeiten gemeinsam im Fintech Hub H:32 in Berlin.

Kostenfreie Produkt-Demo: https://vimeo.com/393424143/2ba4c77d0f

Noch weitere Fragen?

Vereinbaren Sie einen unverbindlichen Beratungstermin mit unserem Kundenservice:

Hardenbergstr. 32, 10623 Berlin
Telefon: 030/95 999 80 80 (Mo - Fr 09:00-18:00 Uhr)
E-Mail: info@perseus.de

www.perseus.de

Erscheinungsdatum: März 2020

perseus.
Cybersicherheit auf den Punkt