Homeoffice Security

Red-Flag-Analyse

Homeoffice wird mehr und mehr genutzt. Speziell durch COVID-19 erhöhte sich die Zahl der Homeoffice-Arbeitsplätze signifikant. Das Homeoffice bietet gerade für Organisationen große Chancen. Den Chancen gegenüber stehen Risiken. Haben Sie sich bereits mit dem erhöhten Cyberrisiko befasst? Kennen Sie die aus dem Homeoffice verstärkt resultierenden Bedrohungen? Haben Sie ausreichende Maßnahmen zum Schutz gesetzt? Gemeinsam stellen wir sicher, dass Sie trotz Homeoffice sicher und effizient agieren können.

Assessment

Identifikation von Cyberrisiken

PwC prüft mithilfe eines Kontrollkatalogs Ihre Schutzmaßnahmen hinsichtlich des Betriebs von **Homeoffice-Arbeitsplätzen** und der daraus resultierenden Verbindung zu zentralen Systemen und Informationen. Wir analysieren zudem Ihre bestehenden Prozesse und zeigen mögliche **Cyberrisiken** auf.
Die Analyse inkludiert die Betrachtung von neu geschaffenen Lösungen und Prozessen für die Arbeit aus der Ferne.

Bericht

Konkrete Handlungsfelder und Verbesserungsvorschläge

Unsere PwC-Cybersecurity-Experten führen eine **Red-Flag-Analyse** (remote oder vor Ort) durch und identifizieren Risiken, so genannte Red Flags, zu denen entsprechende **Handlungsempfehlungen** ausgearbeitet werden.

Sie erhalten damit einen Einblick in Homeoffice-bezogene Risiken und können risikoorientierte Maßnahmen zum Schutz Ihrer Organisation treffen.

Unser Angebot

Schnell zum sicheren Ergebnis

Wir stehen Ihnen in dieser herausfordernden Zeit mit einem schnellen und effizienten Werkzeug zur Seite, deshalb adressiert die Homeoffice-**Red-Flag-Analyse** bewusst das Arbeiten aus der Ferne und die damit verbundenen Cyberrisiken.

Der Aufwand für die Analyse beträgt **einen Tag (remote oder vor Ort)**.

Homeoffice-Red-Flag-Analyse

Georg Beham
Partner
Cybersecurity & Privacy Leader Austria
Tel.: +43 732 611 750 4019
georg.beham@pwc.com

Peter Kleebauer
Senior Manager
Informationssicherheit und Privacy
Tel.: +43 732 611 750 4054
peter.kleebauer@pwc.com

Erik Rusek
Senior Manager
Cybersecurity-Culture und Awareness
Tel.: +43 732 611 750 4075
erik.rusek@pwc.com

Sie haben Fragen, melden Sie sich gerne bei uns!

Cybersecurity & Privacy

Homeoffice Security

Wir alle stehen vor der enormen Herausforderung der globalen COVID-19-Pandemie, die viele von uns gezwungen hat, aus der Ferne zu arbeiten.

Stellen Sie sicher, dass Ihr Unternehmen und Ihre Mitarbeiter auch remote sicher und effizient agieren können.

Risiken und Konfliktfelder für Cybersecurity im Homeoffice

Unternehmen setzen verstärkt auf Homeoffice, um Ihren Aufgaben und Verpflichtungen in einer zunehmend digitalen Welt weiterhin nachkommen zu können. Bedingt durch COVID-19 wurde die Schaffung von Homeoffice-Arbeitsplätzen weitestgehend ohne Vorbereitung und ohne spezifische Sicherheitsmaßnahmen umgesetzt. Dadurch wurden kritische Cyberrisiken nicht oder unzureichend adressiert bzw. erst gar nicht erkannt. Dies resultiert in einem gestiegenen Risiko der Kompromittierung. In unserer Homeoffice-Red-Flag-Analyse behandeln wir daher unter anderem die folgenden Themenschwerpunkte:

Verdächtige E-Mails

Aufgrund der derzeit ungewohnten Lage sind Ihre Mitarbeiter ein noch beliebteres Ziel für Phishing-Attacken (z.B. CEO-Fraud).

Das Platzieren von Schadsoftware via Phishing-EMails kann in einer Beeinträchtigung der Infrastruktur resultieren, welche unter Umständen einen Unternehmensstillstand zur Folge haben kann.

Verwendung von VPN

Beim Arbeiten aus der Ferne müssen die Mitarbeiter laufend auf Informationen der Organisation zugreifen, um Ihrer Arbeit nachzugehen.

Wird keine sichere Verbindung ermöglicht, steigert dies das Risiko eines unbefugten Zugriffes auf Daten, was in einem Diebstahl von vertraulichen Kunden- und Projektinformationen resultieren kann.

Web-basiertes Arbeiten

Regelmäßige Abstimmungen und Termine werden im Homeoffice ausschließlich per Telefon oder über Videokonferenzlösungen durchgeführt.

Das ungeregelte Nutzen von ggf. nicht durch die Organisation freigegebenen Lösungen stellt ein erhebliches Risiko dar, da vertrauliche Gespräche in nicht ausreichend sicheren, digitalen Konferenzräumen abgehalten werden.

Austausch von Daten

Beispiel: Ihre Mitarbeiter arbeiten an einem Projekt und müssen dazu Projektdaten nutzen und austauschen. Zum Austausch dieser nutzen sie diverse öffentliche Cloud-Dienste.

Risiko: Die Nutzung unkontrollierter und öffentlicher Dienste für die gemeinsame Verwendung von Daten kann dazu führen, dass sensible Informationen an Dritte gelangen.

Administratorenrechte

Ihre Mitarbeiter haben möglicherweise Administratorenrechte auf den Geräten, die sie für das Unternehmen nutzen. Mögliche Schadsoftware könnte unkontrolliert und außerhalb der Monitoring-Systeme Ihrer Organisation installiert werden.

Die Kompromittierung lokaler Administratorenrechte kann in weitreichenden Zugriffsrechten für unbefugte Personen resultieren.

Gesund und glücklich sein

Ihr Team arbeitet möglicherweise lange Zeit von zu Hause aus und es fehlt an sozialer Interaktion.

Es ist wichtig, gesund und glücklich zu bleiben. Vereinbaren Sie tägliche Videoanrufe mit Ihren Kollegen und kommunizieren Sie mit Ihrem Team nicht nur über schriftliche Nachrichten. Das Sehen von Live-Bildern und das Hören einer echten Stimme sind wichtig, um entspannt zu bleiben und sich an das Team und die Firma zu erinnern.