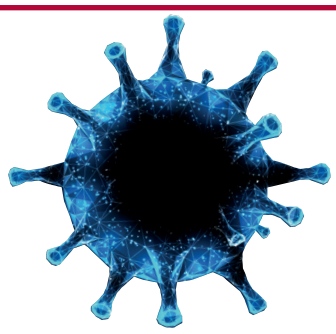
CORONA
SARS-COV-2 (COVID-19)



COVID-19-Krise - Erhöhte Gefahr im Homeoffice

Absicherungsmöglichkeiten durch Vertrauensschaden- und Cyberversicherung

Aufgrund der COVID-19-Krise befinden sich die meisten Arbeitnehmer derzeit im Homeoffice und arbeiten webbasiert für ihr Unternehmen. Einer der entscheidenden Nachteile dieser Arbeitsform: Die Betroffenen bewegen sich oft in einer nicht ausreichend gesicherten IT-Umgebung.

Zudem besteht derzeit ein erhöhtes Informationsbedürfnis zum aktuellen Stand der Epidemie, zu möglichen Schutzmaßnahmen oder auch zu finanzieller Unterstützung. Das bedeutet zweierlei: Zum einen bewegen sich die Arbeitnehmer immer wieder in mehr oder weniger geschützten Cyber-Räumen und Foren, um sich auf dem Laufenden zu halten. Zum anderen wecken die besonderen Umstände der Krise auch das Interesse von Internet-Kriminellen. Diese haben sich, so zeigen die Warnungen des BKA und Europol, sehr schnell auf die neuen Gegebenheiten eingestellt und setzen ihre kriminelle Energie zur Nutzung der vermehrten Schwachstellen ein.

Ob Malware, die sich hinter einer angeblichen „Echtzeit"-Karte von Corona-Infektionen verbirgt, Phishing-Mails, die mit Videoanweisungen zum Schutz vor Viren locken oder betrügerischen Internetseiten zum Abruf von Fördergeldern: Nahezu jede Angriffsfläche wird von Cyber-Kriminellen ausgenutzt.

Aus diesem Grund ist es für Arbeitgeber jetzt besonders wichtig, ihre Mitarbeiter entsprechend zu sensibilisieren, sowie die internen Prozesse und Schutzmaßnahmen zu prüfen. Nicht zuletzt muss es dabei auch um eine wirksame Absicherung von Vermögensschäden gehen, falls sich die Angreifer trotz aller Gegenmaßnahmen nicht abwehren lassen.

Viele Versicherer die Produkte in den Sparten Cyber und Vertrauensschäden anbieten (Euler Hermes, MARKEL, HISCOX, AGCS etc.) liefern derzeit hilfreiche Hinweise. Wir haben diese für Sie zusammengefasst und ergänzt.

Welche Maßnahmen muss ich als Unternehmer setzen?

Informieren und schulen Sie Ihre Mitarbeiter aktiv über die aktuellen Gefahren und die Besonderheiten im Homeoffice. Verfassen Sie eine „Homeoffice-Datenschutz-Richtlinien" bzw spezielle Dienstanweisungen und führen Sie Awareness-Schulungen für die gesamte Belegschaft, insbesondere zum Thema Phishing -Attacken, durch.

Weisen Sie Ihre Mitarbeiter darauf hin, dass Web-Adressen immer selbständig eingegeben werden sollen und Links bzw. Anhänge nicht unüberlegt angeklickt werden dürfen. Fordern Sie Ihre Mitarbeiter dazu auf Dateierweiterungen von heruntergeladenen Dateien zu überprüfen, Dokumente und Videodateien sollten weder im EXE- noch im LNK-Format erstellt worden sein. Ihre Mitarbeiter sollen beim vermeintlichen Auftraggeber oder Absender einer E-Mail nachfragen, wenn ihnen eine durchzuführende Aktion seltsam vorkommt. Dafür sollte aber unbedingt ein anderer Kommunikationsweg wie etwa die bereits bekannte Telefonnummer gewählt werden.

Auf unerwünschte Nachrichten sollten Ihre Mitarbeiter nicht antworten, jedoch unverzüglich die IT-Abteilung über deren Eingang informieren.

Was soll ich bei Finanztransaktionen beachten?

Falls Sie im Homeoffice auf physische Unterschriften verzichten, macht es unter Umständen Sinn, ein 6-Augen-Prinzip einzuführen. Sprachsynthesizer und/oder Stimmensimulation bilden eine ganz neue Gefahrenquelle. Nehmen Sie deshalb weder interne noch externe Zahlungsanweisungen oder Änderungen von Bankdaten per Telefon entgegen. Hinterfragen Sie die (vorgebliche) Bitte Ihres CEO oder CFO bei finanziellen Transaktionen. Rufen Sie die Person unter einer Ihnen bereits bekannten Telefonnummer zurück. Bestehen Sie auf einer schriftlichen Anweisung und leiten Sie diese an Ihren Vorgesetzten weiter. Höhere Finanztransaktionen sollten aus diesem Grund ausschließlich im Call-Back-Verfahren mit dem Vorgesetzten freigegeben werden.

Prüfen Sie alle Änderungen von Kontoverbindungen, egal ob von Kunden oder von Lieferanten.

Wie kann ich die Kommunikation zu meinen Mitarbeitern absichern?

Tauschen Sie die wichtigsten Telefonnummern (dienstliche wie auch private Nummern) für Rücksprachen mit Kollegen und Vorgesetzten aus.

Insbesondere „WhatsApp“ wird derzeit gerne von Betrügern verwendet. Sollten WhatsApp-Nachrichten für die Kommunikation genutzt werden, klären Sie den Inhalt durch einen Telefonanruf – aber keinen WhatsApp-Anruf oder ein FaceTime-Video – mit den betroffenen Kollegen ab. Misstrauen Sie grundsätzlich jeder „WhatsApp“-Sprachnachricht.

Apps sollten lediglich aus vertrauenswürdigen Quellen – etwa Google Play, App Store oder unternehmenseigene Anwendungspools – heruntergeladen werden.

Grundsätzlich ist von der betrieblichen Nutzung von WhatsApp dringend abzuraten!

Welche Maßnahmen soll ich im Bereich der IT-Infrastruktur umsetzen?

Beschränken Sie die Zugriffsrechte von Personen, die eine Verbindung zum Unternehmensnetzwerk herstellen. Gewährleisten Sie, dass Ihre Mitarbeiter sichere Passwörter verwenden. Passwörter sollten lang, komplex und mit Sonderzeichen ausgestattet sein. Weisen Sie Ihre Mitarbeiter darauf hin, dass die Nutzung von Firmen-E-Mail-Adressen oder Passwörtern für die private Registrierung bei Online-Diensten nicht erlaubt ist!

Installieren Sie die neuesten Updates für Betriebssysteme und Apps, sobald verfügbar, um Schwachstellen soweit wie möglich zu schließen.

Nutzen Sie keine öffentlichen/privaten Computer für dienstliche Zwecke, denn diese können manipuliert sein. Es besteht die Gefahr, dass Daten gestohlen oder manipuliert werden. Sofern Ihre Mitarbeiter private Computer verwenden muss dies mit der IT-Abteilung abgestimmt und die IT-Sicherheit von dieser überprüft werden.

Worauf soll ich im digitalen Bereich besonders achten?

Seien Sie bei E-Mails von unbekannten Absendern mit Anhängen oder Links besonders achtsam.

Betrüger nutzen Informationen aus sozialen Netzwerken. Seien Sie also vorsichtig bei der Preisgabe von Informationen im Internet.

Kann ich die Restrisiken absichern?

Aufgrund der rasant ansteigenden Schadenzahlen in diesem Bereich raten wir trotz Umsetzung der oben angeführten Maßnahmen dringend zu einer Absicherung durch eine Vertrauensschaden- und Cyberversicherung!

Bei Fragen steht Ihnen Frau Mag. Kerstin Keltner gerne zur Verfügung.

KOBAN SÜDVERS GROUP GmbH
Kopfgasse 7, 1130 Wien, Österreich
Telefon: +43 50 871 2217
Mobil: +43 664 357 64 20
E-Mail: kerstin.keltner@kobangroup.at