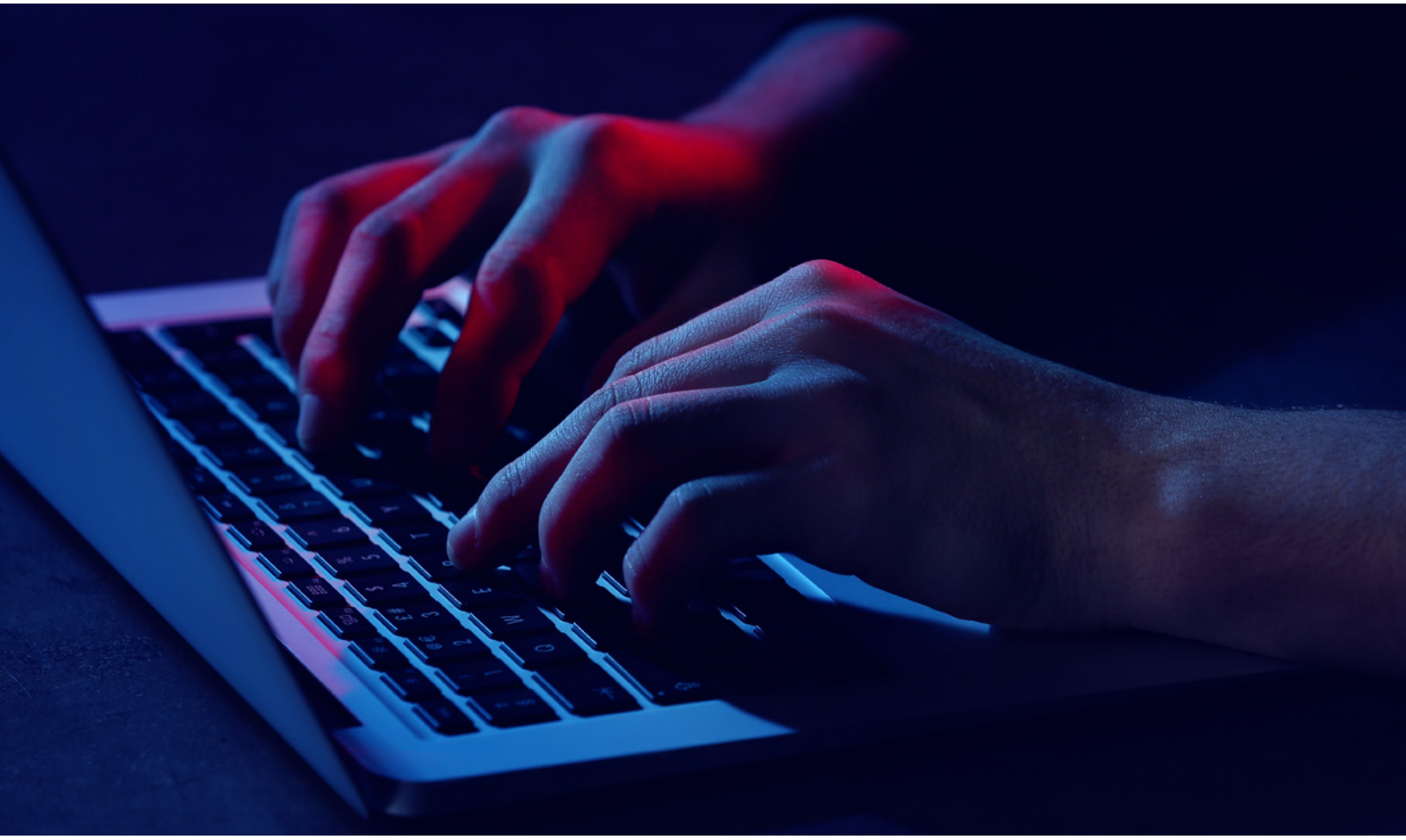
sosafe

Sicheres Arbeiten im Homeoffice

Die Gefahren beim mobilen Arbeiten
und wie Sie sich vor ihnen schützen



Angriffsziel Homeoffice

→ Schäden in Milliarden-Höhe

Allein in Deutschland entsteht jährlich ein Schaden von mehr als 50 Milliarden Euro durch Homeoffice-bedingte Cybervorfälle.

→ Erhöhtes Schadensrisiko

Datenschutzvorfälle kosten Organisationen durchschnittlich 4,42 Millionen US-Dollar, im Kontext von Remote Work noch einmal 1,07 Millionen US-Dollar mehr.

→ Unzureichende Kontrolle

Nur 38% der Organisationen sichern Arbeitsgeräte über eine Verbindung zum Unternehmensnetzwerk ab.

Welche Gefahren bestehen beim Arbeiten im Homeoffice?

Phishing

Cyberkriminelle nutzen aktuelle Themen gnadenlos für manipulative Cyberangriffe, zum Beispiel per E-Mail oder Telefon aus.

Nutzung von Cloud-Tools

Zur Kollaboration im Homeoffice werden oftmals Cloud-Tools eingesetzt, zuweilen auch nicht offiziell autorisierte. Angreifende nutzen die Tools als mögliches Einstiegstor in Unternehmenssysteme.

Verunsicherung

Neue Arbeitsbedingungen erhöhen das Risikopotenzial: Die Hälfte aller Mitarbeitenden klickt auf Phishing-Mails, die im Kontext der Einführung von Kollaborationstools versendet werden.

Fehlender Flurfunk

Phishing-Mails werden bei mobilem Arbeiten bis zu dreimal häufiger geklickt als bei Büroarbeit – vermutlich nicht zuletzt, weil der Austausch mit den Kolleginnen und Kollegen fehlt.

Bring-your-own-device

Viele Mitarbeitende nutzen aus Mangel an vom Unternehmen bereitgestellten Geräten private Endgeräte wie Laptops oder Smartphones für geschäftliche Zwecke. Diese sind oftmals aber schlechter abgesichert. Außerdem kann die Unternehmens-IT die Geräte nicht auf Unregelmäßigkeiten prüfen.

Unzureichend abgeschirmte Arbeitsplätze

Sind Arbeitsplätze nicht ausreichend für den Zugriff von Dritten abgeschirmt, ermöglicht das Kriminellen auf Unternehmensdaten zuzugreifen.

5 Tipps, um sicher im Homeoffice zu arbeiten

- Bewahren Sie Dokumente und Unterlagen sowie portable Datenträger unzugänglich auf – auch für Ihre Familie oder Besuch in Ihrer Wohnung.
- Sperren Sie immer Ihren Bildschirm oder Rechner, sollten Sie gerade nicht davorsitzen. Sorgen Sie außerdem dafür, dass Ihr Bildschirm nicht einsehbar ist – zum Beispiel durch Ihr Fenster.
- Nutzen Sie nur passwortgeschütztes WLAN und wählen sich zum Beispiel über eine VPN-Verbindung in das Netzwerk Ihres Unternehmens ein. Verwenden Sie nur von Ihrer IT-Abteilung freigegebene (Cloud-)Tools.
- Schließen Sie niemals ungeprüfte, externe Datenträger (zum Beispiel USB-Sticks) an Ihr Arbeitsgerät an.
- Machen Sie vertrauliche Dokumente unkenntlich, bevor Sie diese im Hausmüll entsorgen.

Auf unserem Awareness-Blog mehr über Informationssicherheit im Homeoffice erfahren