Wie Sie Remote-Teams vor den größten Cyberbedrohungen schützen können

Remote-Arbeitsmodelle haben die Geschäftswelt verändert, aber auch besondere Herausforderungen für die Cyber Security mit sich gebracht. Wir haben eine umfassende Liste der größten Cyberbedrohungen für Remote-Mitarbeiter:innen und diejenigen, die dezentrale Teams managen, sowie praktische Tipps zur Risikobewältigung zusammengestellt.

BEDROHUNG
Phishing-Angriffe

Cyberkriminelle verwenden betrügerische E-Mails oder Textnachrichten, um Mitarbeiter:innen dazu zu bringen, vertrauliche Informationen preiszugeben oder auf schädliche Links zu klicken.

SCHUTZMASSNAHMEN

- Sensibilisieren Sie Ihr Personal regelmäßig mit Schulungen zum Thema Phishing.
- Verwenden Sie E-Mail-Sicherheitsfilter, um verdächtige E-Mails zu blockieren.
- Implementieren Sie die Mehrfaktor-Authentifizierung (MFA) für zusätzliche Sicherheit.

BEDROHUNG
Unsichere Kennwörter

Mitarbeiter:innen, die einfache Kennwörter verwenden oder Kennwörter wiederverwenden, machen es Cyberkriminellen leicht, auf Konten zuzugreifen.

SCHUTZMASSNAHMEN

- Setzen Sie strenge Kennwortrichtlinien durch und sorgen Sie dafür, dass Kennwörter regelmäßig geändert werden.
- Ermöglichen Sie die Nutzung einer offiziell genehmigten Kennwortmanagement-Software.
- Implementieren Sie die MFA für alle kritischen Konten.

BEDROHUNG
Unverschlüsselte WLAN-Netzwerke

Öffentliche oder ungesicherte Netzwerke bergen die Gefahr, dass sensible Unternehmensdaten von Hacker:innen abgefangen werden.

SCHUTZMASSNAHMEN

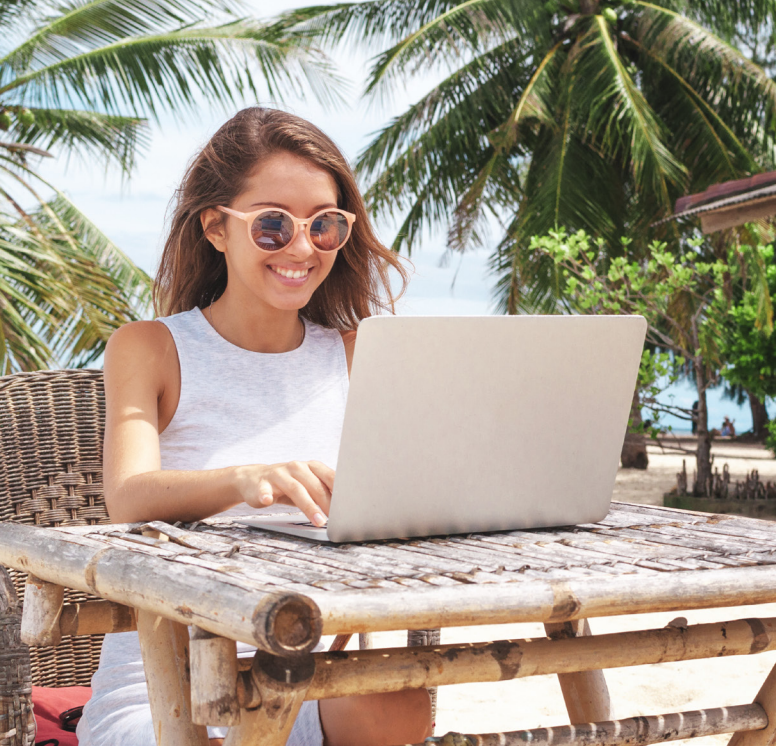
- Verlangen Sie von Ihren Mitarbeiter:innen, dass sie ein sicheres VPN verwenden, wenn sie sich in Unternehmenssysteme einloggen.
- Weisen Sie Ihr Team auf die Risiken öffentlicher WLANs hin und empfehlen Sie die Nutzung privater Hotspots.
- Deaktivieren Sie die Dateifreigabe und Wi-Fi Direct auf den Geräten, um unbefugten Zugriff auf Dateien zu verhindern.

BEDROHUNG
Nicht gepatchte Software und Systeme

Veraltete Software kann Schwachstellen enthalten, die von Cyberkriminellen ausgenutzt werden können.

SCHUTZMASSNAHMEN

- Richten Sie automatische Updates für Betriebssysteme und Anwendungen ein.
- Überprüfen Sie regelmäßig, ob die Geräte im Unternehmen auf dem aktuellen Stand sind.
- Überwachen Sie die Geräte mithilfe von EDR-Tools (Endpoint Detection and Response).



BEDROHUNG
Keine sicheren Tools für die Zusammenarbeit

Die Verwendung nicht genehmigter oder unsicherer Kommunikations- und Filesharing-Tools kann zu Datenschutzverletzungen führen.

SCHUTZMASSNAHMEN

- Stellen Sie sichere Tools für die Zusammenarbeit bereit (z. B. Microsoft Teams, Slack oder Google Workspace).
- Überprüfen Sie regelmäßig die von den Mitarbeiter:innen genutzten Tools und verbieten Sie nicht autorisierte Apps.
- Verschlüsseln Sie Dateien, bevor Sie sie freigeben.

BEDROHUNG
Unsichere private Geräte

Mitarbeiter:innen, die ohne angemessene Sicherheitsmaßnahmen auf ihren privaten Geräten arbeiten, können Unternehmensdaten gefährden.

SCHUTZMASSNAHMEN

- Stellen Sie vom Unternehmen verwaltete Geräte mit vorinstallierten Sicherheitstools zur Verfügung.
- Verlangen Sie die Installation von EDR-Software auf privaten Geräten, die für die Arbeit genutzt werden.
- Implementieren Sie Richtlinien zur Trennung von privaten und geschäftlichen Aktivitäten.

BEDROHUNG
Insider-Bedrohungen

Mitarbeiter:innen können sensible Daten versehentlich offen legen oder ihre Zugangsberechtigung in böswilliger Absicht ausnutzen oder fahrlässig damit umgehen.

SCHUTZMASSNAHMEN

- Beschränken Sie den Zugang zu vertraulichen Informationen auf Basis der Rolle im Unternehmen.
- Nutzen Sie Verhaltensanalyse-Tools, um ungewöhnliche Aktivitäten zu erkennen.
- Veranstalten Sie regelmäßige Schulungen, um das Bewusstsein für Insider-Bedrohungen zu schärfen.

BEDROHUNG
Ransomware-Angriffe

Cyberkriminelle verwenden Ransomware, um Unternehmensdaten zu verschlüsseln. Für die Entschlüsselung wird ein Lösegeld verlangt.

SCHUTZMASSNAHMEN

- Sichern Sie kritische Daten regelmäßig und verschlüsseln Sie die Backups.
- Sensibilisieren Sie Ihr Personal für verdächtige Links oder Downloads.
- Setzen Sie moderne Anti-Malware-Software ein, um Ransomware zu erkennen.

BEDROHUNG
Schatten-IT

Mitarbeiter:innen, die nicht autorisierte Apps oder Services verwenden, können IT-Sicherheitskontrollen umgehen und so Schwachstellen schaffen.

SCHUTZMASSNAHMEN

- Erstellen Sie eine Liste genehmigter Software und Tools für die geschäftliche Nutzung.
- Bieten Sie Ihren Mitarbeiter:innen Alternativen zu häufig verwendeten Tools an. So geraten sie weniger in Versuchung, nicht genehmigte Tools zu verwenden.
- Überwachen Sie den Netzwerkverkehr, um Schatten-IT-Bedrohungen zu identifizieren.

BEDROHUNG
Social Engineering-Angriffe

Cyberkriminelle bringen Mitarbeiter:innen über persönliche Interaktionen dazu, vertrauliche Informationen preiszugeben.

SCHUTZMASSNAHMEN

- Führen Sie rollenspezifische Schulungen durch, damit Ihr Personal Social Engineering-Taktiken erkennt.
- Ermutigen Sie Ihre Mitarbeiter:innen dazu, Anfragen zu sensiblen Informationen über vertrauenswürdige Kanäle zu prüfen.
- Fördern Sie eine Kultur der Meldung verdächtiger Aktivitäten.

BEDROHUNG
Schwache Sicherheit des Heimnetzwerks

Schlecht gesicherte Heimnetzwerke können ein Einfallstor für Cyberkriminelle sein.

SCHUTZMASSNAHMEN

- Schulen Sie Ihre Mitarbeiter:innen darin, ihre privaten Router zu sichern (z. B. Standardpasswörter ändern und WPA3-Verschlüsselung aktivieren).
- Stellen Sie eine Checkliste für die Sicherung von IoT-Geräten in Heimnetzwerken zur Verfügung.
- Wenn möglich, bieten Sie IT-Support für die Überprüfung und Sicherung von Heimnetzwerken an.

BEDROHUNG
Datenlecks durch Remote-Arbeitsumgebungen

Wenn Mitarbeiter:innen in gemeinsam genutzten oder öffentlichen Räumen arbeiten, können sensible Daten offengelegt werden.

SCHUTZMASSNAHMEN

- Empfehlen Sie die Verwendung von Sichtschutz für Laptop-Bildschirme.
- Fordern Sie Ihr Personal auf, vertrauliche Informationen nicht in öffentlichen Bereichen zu besprechen.
- Schränken Sie den Offline-Zugriff auf vertrauliche Dateien ein.

BEDROHUNG
Kein remote-fähiger Incident Response Plan

Eine verspätete Reaktion auf Zwischenfälle kann den Schaden eines Cyberangriffs vergrößern.

SCHUTZMASSNAHMEN

- Entwickeln Sie einen Incident Response Plan, der remote-fähig ist.
- Schulen Sie Ihr Personal darin, wie es Zwischenfälle schnell melden und darauf reagieren kann.
- Testen Sie Ihren Incident Response Plan regelmäßig in simulierten Übungen.

Cyber Security für Remote- und Hybrid-Arbeitsumgebungen erfordert einen mehrschichtigen Ansatz, der Technologie, Richtlinien und Schulungen kombiniert. Durch einen proaktiven Umgang mit diesen Bedrohungen können Unternehmen Risiken mindern und sich vor kostspieligen Datenschutzverletzungen schützen.

Benötigen Sie Hilfe bei der Erstellung eines zuverlässigen Sicherheitsplans für Ihre Remote-Mitarbeiter:innen?
Kontaktieren Sie uns noch heute, um Ihr Unternehmen zu schützen und Ihre remote arbeitenden Teams zu unterstützen.

Kreuziger Hybrid IT Services
info@kreuziger-it.de +4966317551050 https://www.kreuziger-it.de