Sichere Telearbeit

TIPPS UND HINWEISE FÜR UNTERNEHMEN

Legen Sie Unternehmensrichtlinien und -prozesse für Telearbeit fest und testen Sie diese nach Möglichkeit vorab

Legen Sie eine klare Richtlinie für Telearbeit fest, die den Zugriff auf Unternehmensressourcen und Ansprechpartner bei Problemen vorgibt. Legen Sie klare Prozesse für Sicherheitsvorfälle fest. Setzen Sie zusätzliche Maßnahmen hinsichtlich Dokumentation an das mittlere und obere Management um Unterschriften, Genehmigungen / Feedback und Informationen zu erhalten.

Sichern Sie Ihre Telearbeitsgeräte

Implementieren Sie Maßnahmen wie Festplattenverschlüsselung, Zeitlimits für Inaktivität, Blickschutz für Displays, starke Authentifizierung und Kontrolle sowie Verschlüsselung von Wechseldatenträgern (z. B. USB-Laufwerke). Implementieren Sie einen Prozess für die Remote-Deaktivierung von Zugriffen auf verloren gegangene oder gestohlene Geräte.

Sicherer Remote-Zugriff

Erlauben Sie Ihren Mitarbeitern nur über einen vom Unternehmen bereitgestellten/genehmigten VPN-Zugang mit Mehrfaktor Authentifizierung („multi-factor authentication“) eine Verbindung zum Unternehmensnetzwerk herzustellen. Stellen Sie sicher, dass Remote-Verbindungen nach einer bestimmten Zeit der Inaktivität automatisch getrennt werden („time out“) und nach Ablauf eine erneute Authentifizierung erforderlich ist.

Halten Sie Betriebssysteme und Apps auf dem neuesten Stand

Dies wird das Risiko verringern, dass Cyberkriminelle vom Hersteller behobene Sicherheitslücken ausnutzen.

Sichern Sie Ihre Unternehmenskommunikation

Bestehen Sie auf die Verwendung von Multi Faktor Authentifizierung für den Zugriff auf Unternehmens-E-Mail-Konten. Stellen Sie Ihren Mitarbeitern sichere Kommunikationskanäle Verfügung, damit sich diese leicht erreichen und mit externen Partnern kommunizieren können.

Erhöhen Sie Ihr Sicherheitsmonitoring

Überprüfen Sie ungewöhnliche Remotebenutzeraktivitäten und erhöhen Sie Ihre Warnstufen für VPN-bezogene Angriffe.

Sensibilisieren Sie Mitarbeiter für die Risiken der Telearbeit

Informieren Sie die Mitarbeiter über die Telearbeitsrichtlinien des Unternehmens. Nehmen Sie sich die erforderliche Zeit, um auf Cyber-Bedrohungen aufmerksam zu machen und insbesondere auf Phishing und Social Engineering zu sensibilisieren.

Treten Sie mit Ihren Mitarbeitern regelmäßig in Verbindung

Setzen Sie realistische Ziele, und gestalten Sie Arbeitspläne und Follow-up-Mechanismen nach Möglichkeit flexibel, um die persönlichen Umstände der Mitarbeiter zu berücksichtigen.

Bundesministerium Inneres
Bundeskriminalamt
EUROPOL EC3 European Cybercrime Centre

Sichere Telearbeit

TIPPS UND HINWEISE FÜR MITARBEITER

Zugriff auf Unternehmensdaten mit Unternehmensausstattung

Verwenden Sie nur vom Unternehmen bereitgestellte Geräte und Software. Erstellen Sie sichere Kennwörter (verwenden Sie vertrauenswürdige / genehmigte Kennwortmanager, falls verfügbar). Schreiben Sie Ihre Kennwörter nicht auf und schützen Sie sich davor, bei der Eingabe beobachtet zu werden. Vermeiden Sie Workarounds, auch wenn diese scheinbar genau das bieten, was Sie benötigen.

Stop.Think.Connect

Machen Sie sich vor Beginn der Telearbeit mit den Geräten, Richtlinien und Abläufen des Unternehmens vertraut. Vergewissern Sie sich, dass Sie die Bedienung der Geräte, sowie die Verhaltensregeln für deren Verwendung verstanden haben und die Kontakte für Hilfe kennen.

Sicherer Fernzugriff

Stellen Sie nur über das vom Unternehmen bereitgestellte/genehmigte VPN eine Verbindung zum Unternehmensnetzwerk her und schützen Sie die für die VPN-Verbindung erforderlichen Token (z. B. Smartcard).

Schützen Sie Ihre Arbeitsgeräte und Ihre unmittelbare Arbeitsumbebung, die Sie für die Telearbeit benötigen

Erlauben Sie Familienmitgliedern keinen Zugriff auf Ihre Arbeitsgeräte. Sorgen Sie für eine geeignete Sperre Ihrer Geräte, wenn diese unbeaufsichtigt sind und bewahren Sie sie an einem sicheren Ort auf, um Verlust, Beschädigung oder Diebstahl zu vermeiden. Verhindern Sie das unberechtigte Ablesen Ihres Bildschirms durch Verwendung eines Display-Sichtschutzes und positionieren Sie Bildschirme niemals vor Fenstern oder Kameras.

Informieren Sie Ihren Arbeitgeber

Sollten Sie ungewöhnliche oder verdächtige Aktivitäten auf Ihrem Arbeitsgerät bemerken, wenden Sie sich sofort über die entsprechenden Kanäle an Ihren Arbeitgeber.

Bleiben Sie wachsam

Achten Sie auf verdächtige Aktivitäten und Anfragen, insbesondere im Zusammenhang mit finanziellen Forderungen. Es könnte sich um CEO-Fraud oder Tech-Support-Scam durch Betrüger handeln! Rufen Sie im Zweifelsfall den Anforderer zur Verifizierung an. Klicken Sie nicht auf Links oder Anhänge in E-Mails und Textnachrichten unbekannter Herkunft.

Geben Sie keine persönlichen Informationen weiter

Antworten Sie niemals mit persönlichen Informationen auf Nachrichten, auch wenn diese angeblich von legitimen Unternehmen stammen. Wenden Sie sich stattdessen direkt an das Unternehmen, um die Anfrage zu verifizieren.

Entwickeln Sie neue Routinen

Besprechen Sie Arbeitspläne, Aufgabenverteilung, Fristen und Kommunikationskanäle während der Telearbeitszeit mit Ihrem direkten Vorgesetzten und den Teammitgliedern.

Verwendung von privaten Geräten

Wenn die Verwendung Ihres persönlichen Geräts die einzige und von Ihrem Arbeitgeber zugelassene Option ist, stellen Sie die Aktualität des Betriebssystems und der Software - insbesondere des Antivirus Programms - sicher. Zusätzlich sollten Sie nur von Ihrem Unternehmen genehmigte VPN Lösungen zur Verbindung ins Unternehmen nutzen.

Privates und Berufliches trennen

Verwenden Sie das Telearbeitsgerät nicht für private Zwecke und installieren Sie keine vom Arbeitgeber ungenehmigten Applikationen.

Bundesministerium Inneres
Bundeskriminalamt
EUROPOL EC3 European Cybercrime Centre