Praxistipps

- **Beziehen Sie die persönliche wie auch berufliche Identität ins Training mit ein:** Fokussieren Sie Ihr Training auf die Bedeutung persönlicher und beruflicher Identitäten der Mitarbeitenden. Klären Sie über Angriffsmethoden und ihre Konsequenzen auf und verdeutlichen Sie, wie wertvoll Ihre Mitarbeitenden für die Angreifenden sind.
- **Erweitern Sie das Training auf den Familienkreis:** Beziehen Sie Familienmitglieder in Trainings mit ein, um ihre Sicherheit im digitalen Raum zu verbessern, da Cyberkriminelle auch die Familie ausnutzen, um über sie in Netzwerke einzudringen oder Ihre Mitarbeitenden zu erpressen.
- **Decken Sie mit technischen Schutzmaßnahmen auch private Geräte und firmenfremde Hardware ab:** Nicht selten nutzen Mitarbeitende private Geräte für die Arbeit. Manche Software-Anbieter bieten Rabatte auf Tools und Maßnahmen, die die Sicherheit privater Geräte erhöhen, ohne Ihr Sicherheitsteam zusätzlich mit der Verwaltung neuer Hardware zu belasten.
- **Sichern Sie Remote-Verbindungen:** Stärken Sie den Schutz remoter Verbindungen durch MFA, VPNs, Endpunktprüfung und DLP, um die Freilegung sensibler Daten außerhalb der unternehmenseigenen Schutzmaßnahmen zu verhindern.
- **Stärken Sie Zugriffskontrollen:** Führen Sie unter der Annahme, dass es zu Datenschutzverstößen kommen wird, Audits aller Systeme durch, die den Schutz sensibler Daten und Prozesse gewährleisten. Bewahren Sie die Log- und Überwachungsdaten mindestens der letzten 12 Monate auf, um die Aktivitäten von Mitarbeitenden im Notfall zurückzuverfolgen. Reduzieren Sie Schwachstellen, indem Sie Passwortmanager überprüfen und aufräumen, geteilte Konten löschen und Zugriffsprotokolle stärken.

Organisation, die über persönliche Geräte oder Konten Ihrer Mitarbeitenden angegriffen wurde