BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Social Engineering

Social Engineering ist eine Methode, bei der Manipulation und menschliche Interaktion genutzt werden, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen.

ZIEL / SCHADEN

Social-Engineering-Angriffe können zu Datenverlusten, finanziellen Verlusten und Identitätsdiebstahl führen.

INFEKTIONSWEG

Meist über Kommunikationswege wie E-Mail, Telefon oder soziale Medien, wo der Angreifer sich als vertrauenswürdige Quelle ausgibt.

ABWEHR

Seien Sie vorsichtig bei der Preisgabe persönlicher Informationen und prüfen Sie die Authentizität von Anfragen. Bilden Sie Mitarbeiter in Sicherheitsbestimmungen und -protokollen aus.

BEFREIUNG MÖGLICH?

Ja, durch sofortige Änderung von Passwörtern und Überwachung von Konten auf ungewöhnliche Aktivitäten.

ANGRIFF - WAS NUN?

Wenn Sie glauben, dass Sie Opfer eines Social-Engineering-Angriffs geworden sind, ändern Sie sofort alle Passwörter und überwachen Sie Ihre Konten auf ungewöhnliche Aktivitäten. Informieren Sie das betroffene Unternehmen oder die Organisation.