Täuschend echte Kundenrechnung führt zu Ransomware-Angriff auf einen Elektriker

Das betroffene Unternehmen

Branche: Herstellung elektronischer Erzeugnisse
Mitarbeiter: 50
Umsatz: 7.500.000 €

Infobox “Active Directory (AD)”

Active Directory ist ein Verwaltungssystem von Microsoft, das die zentrale Organisation und Verwaltung von Computern und Benutzern in einem Unternehmensnetzwerk ermöglicht.

Der Ablauf des Cyberangriffs

Ein Mitarbeiter erhält eine täuschend echte Phishing-E-Mail, die vorgibt, von einem bekannten Geschäftspartner zu stammen. In der E-Mail befindet sich ein Anhang, der als Rechnung getarnt ist.

Beim Öffnen des Anhangs wird Schadsoftware unbemerkt auf den Computer des Mitarbeiters installiert. Die Hacker nutzen die Schadsoftware, um Zugriff auf das Active Directory zu erhalten.

Sie erlangen Administratorrechte aufgrund schwacher Account-Passwörter, sperren die Benutzer-konten, verschlüsseln kritische AD-Daten und fordern für die Freigabe ein Lösegeld von 30.000€.

Die Auswirkung auf den Betrieb

● Schaden: 92.000 €

Kundendaten & Termin-pläne sind unzugänglich → Aktuelle Projekte verzögern sich, neue nicht möglich → Die Systemwieder-herstellung dauert mehrere Tage → Lösegeld + Bußgelder durch den Verlust von Kundendaten

Wie hätte der Cyberangriff durch Baobab...

...abgedeckt werden können?

- ✓ **24/7 erreichbare Notfall-Hotline** mit erfahrenen Ansprechpartnern sowie Kostenübernahme für die forensische Untersuchung, inkl. der IT-Spezialisten
- ✓ Übernahme der Kosten zur **Prüfung der Ansprüche** Dritter sowie Befriedigung berechtigter Ansprüche
- ✓ **Entschädigung für Einnahmeverluste** durch Betriebsunterbrechungen

...verhindert werden können?

- ✓ Regelmäßiger Angriffsoberflächen-Scan
- ✓ Umgehende Meldung bei Sicherheitslücken
- ✓ Vorlage zur Erstellung komplexer Passwörter
- ✓ Active Directory Gruppenrichtlinien
- ✓ Automatische Erkennung und Abwehr des Angriffs durch Baobab MDR