CYBERANGRIFFE – DIE UNTERSCHÄTZTE BEDROHUNG AUS DEM NETZ

Wie ein gezielter Cyberangriff ein komplettes Unternehmen lahmlegen kann, bekam im März 2024 auch ein langjähriger Kunde der TechniData IT-Service GmbH zu spüren. Das Maschinenbauunternehmen aus Süddeutschland wurde Opfer einer Hackergruppe, die bekannt ist für ihre ausgefeilten Umgehungstaktiken und Angriffe mit weitreichender Auswirkung: So zum Beispiel das Verschlüsseln von Dateien mit doppelten Erpressungstaktiken. Dabei werden die Dateien exfiltriert und die Angreifer drohen anschließend damit, diese zu veröffentlichen und nur gegen Lösegeldzahlungen wieder freizugeben.

KOMPLETT VERSCHLÜSSELT: KEIN ZUGRIFF AUF DATEN MÖGLICH

Der Kunde informierte die TechniData IT-Service GmbH, dass keine Anmeldungen im System mehr möglich sind. Schnell stellten die Experten des IT-Dienstleisters fest, dass das gesamte Unternehmen verschlüsselt wurde. Nach Alarmierung der Cyberversicherung organisierte diese ein Treffen mit den notwendigen Stabsstellen: Landeskriminalamt (LKA), Forensik, Versicherung, Kunde und die TechniData IT-Service GmbH.

Hierbei wurde folgendes Maßnahmenpaket verabschiedet:

- Keine Lösegeldforderungen erfüllen.
- Keine Kommunikation mit den Angreifern durchführen.
- Keine Systeme wieder ins Netz integrieren, die nicht zu 100% geprüft wurden.
- Keine Wiederherstellung von Systemen aus dem Backup. Lediglich Dateien und Dokumente, die gescannt wurden, dürfen in die neue Umgebung eingespielt werden.

WIEDERAUFBAU DER IT

Die Experten der TechniData IT-Service GmbH begannen umgehend mit dem Wiederaufbau der Kunden-IT. Bereits am Folgetag konnte eine entsprechende Leihhardware und Mitarbeitende zur Installation der Umgebung bereitgestellt werden. Die wichtigsten Leistungen in Bezug auf den Wiederaufbau waren:

FORENSIK

- Daten bereitstellen an externen Forensiker

ETABLIERUNG NOTBETRIEB

- Reinstallation aller Endgeräte
- Reset Netzwerkinfrastruktur und Wiederaufbau
- Isoliertes Produktionsnetz für Wiederaufbau
- Produktionssoftware etablieren und aufbauen

ACTIVE DIRECTORY (AD) UND DOMÄNE

- Export User und Daten (Scan) aus alter Domäne
- Härtung neue Umgebung mit aktuellen Empfehlungen (MFA, EDR etc.)
- Dokumentation

MAIL

- Ersatz-/ Übergangsumgebung bereitstellen
- Migration Exchange Online

TELEFONIE

- Unterstützung und Bereitstellung bei Inbetriebnahme Telekommunikation

TECHNI DATA it-service

VPN

- Bereitstellung VPN-Zugänge für externe Dienstleister zum Wiederaufbau des Maschinennetzwerks

INFRASTRUKTUR

- Wiederaufbau WLAN/ LAN
- Wiederaufbau Monitoring-Umgebung
- Segmentierung VLAN nach Produktionsnetzwerk, Servernetzwerk, Client etc.
- Wiederaufbau Backup
- Wiederaufbau und Härtung Clients

FREMD- UND DRITTANBIETER SOFTWARE
(ca. 40 Drittanbieter/ Dienstleister)

- Wiederherstellung des Maschinennetzwerks
- Reinstallation, Konfiguration und Koordination mit Drittanbietern

Aufgrund sehr guter Zusammenarbeit zwischen LKA und der TechniData IT-Service GmbH konnten wichtige Dokumente, die die Angreifer vom Kundennetzwerk erbeuteten, ausfindig und unkenntlich gemacht werden und eine Veröffentlichung verhindert werden.

BESSER GESCHÜTZT:
OPTIMIERUNG DER SICHERHEITSMASSNAHMEN

Durch den Angriff erkannte der Kunde die Notwendigkeit an, die Sicherheit höher zu setzen und ließ folgende technische Maßnahmen durch die Experten der TechniData IT-Service GmbH implementieren:

- Einführung MFA-Einrichtung/ Test und Dokumentation mit Security Key NFC
- Segmentierung des Netzwerks
- Aktuelle Umgebung; keine veralteten Systeme mehr im Netzwerk
- Exchange Online statt on-Prem
- Microsoft Defender
- Intune für Software Deployment

Darüber hinaus empfiehlt sich auch die Investition in den Einsatz von Awareness Schulungen, Penetrationstests und aktuellen technischen Maßnahmen wie MFA und Security Key.

Es existieren mittlerweile zahlreiche kriminelle Vereinigungen, die es sich zum Ziel gemacht haben, anhand von Datenerpressung Lösegelder einzufordern. Cyber-Bedrohungen nehmen kontinuierlich zu, daher müssen Unternehmen proaktiv Sicherheitsmaßnahmen ergreifen, um sich und ihre Daten langfristig zu schützen.