we run your business

Cyberangriff bei Colt Technology Services

Ein Alarmruf für mittelständische Unternehmen

Wenn Sie zu den glücklichen gehörten, die für den 13.08.2025 eine Portierungsbestätigung von Microsoft für die Nutzung von Teams als Telefonie Plattform erhalten haben, fanden Sie die Nachricht von Microsoft vermutlich nicht witzig.

"Due to a technical issue on our partner's side, port-in, new number acquisition and other number related operations in most of our European markets are currently unable to proceed."

Kurz gesagt: Bei unserem Partner (Colt Technology Services) können aufgrund eines technischen Vorfalls momentan keinen keine Portierungen und ähnliche Vorgänge ausgeführt werden.

Seitens Colt erfuhr man bis zum 14.08.2025 erstmal nichts!

Bis heute ist die Statusseite von Colt eher eine Sammlung warmer Worte für die Kundschaft!

Was wissen wir heute?

1. Hintergrund & Ablauf

- **Angriffsdaten**: Am 12. August 2025 begann ein Vorfall bei Colt mit Störungen in internen Systemen. Zwei Tage später wurde Ransomware eindeutig bestätigt.

- **Täter und Daten**: Die Gruppe *WarLock* übernahm Verantwortung und bot eine Datenbank mit über 1 Million Dokumenten (Mitarbeiter-/Kundendaten, Finanzunterlagen, Netzwerk- und Softwaredetails) für 200.000 USD zum Verkauf an.

- **Taktik der Täter**: Anders als typische Ransomware-Angriffe wurde keine Dateikopie veröffentlicht; stattdessen erfolgt der Verkauf über eine Dark-Web-Auktion.

2. Technische Ursache & Reaktion

- **Angriffspunkt**: Wahrscheinlicher Eintritt war eine kritische SharePoint-Schwachstelle (CVE-2025-53770), die Remote-Code-Ausführung erlaubte.

- : Betroffene Systeme, darunter das Kundenportal und die Voice-API, wurden vorsorglich offline genommen. Externe Fachleute und Strafverfolgung wurden eingeschaltet.

- **Transparenz als Schutz**: Colt informiert Kunden aktiv, bietet Einblick in betroffene Dateinamen via Callcenter und isolierte Infrastruktur zur Risikominimierung.

3. Bedeutung für mittelständische Unternehmen

- **Strukturelle Verwundbarkeit**: Auch kleinere Unternehmen mit sensiblen Services (z. B. Data-Centern, CRM-Systemen) können Ziel solcher Angriffe sein – und oft fehlt die Ressourcenbreite für schnellen Schutz.

- **Patch-Management ist entscheidend:** SharePoint & Co. gehören zu den kritischen Einfallstoren – regelmäßige Updates sollten Priorität haben.

- **Segmentierung schafft Resilienz:** Trennung interner und kundenrelevanter Systeme kann im Ernstfall drastische Ausfallzeiten verhindern. Colt konnte hier den Schaden begrenzen.

- **Notfallpläne sind keine Option, sondern Pflicht:** Angriffe wie dieser zeigen: Reaktion muss agiler sein als klassische IT-Notfallpläne. Es geht um das Management einer aktiven Krise.

4. Handlungsempfehlungen für den Mittelstand

- **Frühwarnsysteme implementieren**: Etwa regelmäßige Überwachung öffentlicher Angriffsflächen (Attack Surface Management).
  IDS/IMS Intrusion Detection & Management System
  SIEM Security Information and Event Management

- **Patch-Automation einführen**: Kritische Systeme, insbesondere externe Plattformen, sollten automatisiert gepatcht werden.

Systeme segmentieren & isolieren: Verhindert, dass ein Vorfall unkontrollierte Auswirkungen hat.

- **Transparenz & Kommunikation**: Offene Informationspolitik gegenüber Kunden und Partnern mindert Schaden und stärkt Vertrauen – auch gegenüber Angreifern.

- **Externe Expertise nutzen**: Zusammenarbeit mit Incident-Response-Teams und Forensikern verkürzt die Reaktionszeit.

IT-Sicherheit zur Chefsache machen: Struktur die von oben nach unten wächst.

- **Sicherheitsleitlinie:** Klare Verpflichtung zur IT-Sicherheit im Unternehmen
- **Notfallstrukturen:** planen, aufbauen, testen.

- **Sicherheit braucht Struktur:** Managementsysteme etablieren. ISMS, BSI-**Grundschutz.**

- **Externe Berater:** „Sicherheitsbeauftragte“ im Unternehmen integrieren. Ggf. durch externe Berater realisieren.
-

Fazit

Der Angriff auf Colt ist nicht nur ein weiterer Cybervorfall – er ist ein Weckruf für den Mittelstand. Jede Firma mit digitalem Fundament ist potenziell gefährdet. Nur durch gezielte Investitionen in Sicherheit, Planung und Reaktion lässt sich Resilienz erreichen – und das eigene Geschäft nachhaltig schützen.

Sichern Sie sich gleich Ihr kostenloses Beratungsgespräch mit uns!

Quellen:

https://www.techradar.com/pro/security/colt-confirms-customer-data-stolen-as-warlock-ransomware-crew-auctions-off-details?utm_source=chatgpt.com

https://www.itpro.com/security/cyber-attacks/uk-telecoms-firm-takes-systems-offline-after-cyber-attack?utm_source=chatgpt.com

https://www.it-daily.net/en/shortnews-en/ransomware-attack-hits-british-telecom-provider-colt?utm_source=chatgpt.com

https://www.techradar.com/pro/security/colt-forced-to-take-services-offline-following-apparent-cyberattack?utm_source=chatgpt.com

https://www.computing.co.uk/news/2025/security/colt-confirms-data-theft?utm_source=chatgpt.com

https://doublepulsar.com/colt-technical-services-gets-ransomwared-via-sharepoint-initial-access-some-learning-points-617da7e27ebc?source=rss----8343faddf0ec---4&utm_source=chatgpt.com

https://www.theregister.com/2025/08/15/london_telco_colts_services_disrupted/?utm_source=chatgpt.com