Angriff auf die digitale Lebensader: Telekommunikation ist die Königsklasse für die Cyberkriminalität

Ein Kommentar von Michael Veit, Cybersicherheitsexperte bei Sophos

Cyberattacken auf Telekommunikationsinfrastrukturen treffen nicht nur einzelne Anbieter, sondern eine wichtige Lebensader für Wirtschaft, Gesellschaft und Politik. Die dramatischen Auswirkungen wurden kürzlich wieder deutlich, als Cyberkriminelle im Februar 2026 in die Systeme von Odido, dem größten Mobilfunkanbieter der Niederlande, eindrangen und Daten von 6,2 Millionen Kunden stahlen. Die Angreifer erbeuteten Namen, Adressen, Bankverbindungen sowie teilweise sogar Passinformationen, drohten mit der Veröffentlichung der Daten und forderten ein Lösegeld. Odido lehnte die Erpressung ab, informierte umgehend die niederländische Datenschutzbehörde (AP) und startete die Kommunikation mit ihren Kunden. Der Vorfall zeigt die Verwundbarkeit kritischer Infrastrukturen trotz Vorgaben wie NIS2, und welche systemischen Risiken von solchen Angriffen ausgehen. Die Experten des Sophos X-Ops Research-Teams warnen: Gestohlene Daten dieser Art sind eine Goldgrube für Kriminelle und können für Identitätsdiebstahl, Betrug, gezielte Spionage oder gesellschaftliche Einflussnahme genutzt werden. Der Odido-Fall zeigt deutlich, dass derartige Cyberangriffe nicht nur auf Daten und Erpressung abzielen, sondern auch auf die Destabilisierung kritischer Infrastrukturen und Gesellschaften.

Sprungbrett Telekommunikation
Telekommunikationsunternehmen sind für Cyberkriminelle und staatlich gesteuerte Angreifer besonders attraktiv, da diese nicht nur große Mengen an sensiblen Kundendaten speichern, sondern auch als Einfallstor für weiterführende Angriffe auf andere kritische Infrastrukturen und Organisationen dienen. Der Zugriff auf Kommunikationsdaten ermöglicht es Angreifern, persönliche Netzwerke zu analysieren, etwa von Politikern, Militärs oder Geschäftsleuten, und gezielt Spionage oder Erpressung zu betreiben. Ein kompromittierter Telekommunikationsanbieter ist zudem der Türöffner für Angriffe auf Banken, Krankenhäuser oder Regierungsnetzwerke, was sie zu einem „Single Point of Failure“ mit systemischen Risiken für alle Industriesektoren macht. Fällt ein solches Netzwerk aus, sind die Adern der Wirtschaft und Gesellschaft betroffen – von Finanztransaktionen bis zu Notfalldiensten.

In Krisenzeiten können Angreifer Telekommunikationsnetzwerke gezielt lahmlegen oder manipulieren, um Chaos zu stiften. Beispiele wie der Angriff auf Viasat KA-SAT (Februar 2022), der während der russischen Invasion die Satellitenkommunikation in der Ukraine und Europa unterbrach und sogar die Fernwartung von 5.800 deutschen Windkraftanlagen lahmlegte. Diese Vorfälle verdeutlichen die Kaskadeneffekte, die von Angriffen auf Telekommunikationsnetzwerke ausgehen können. Doch längst nicht alle Angriffe zielen auf sofortige Zerstörung oder Erpressung ab. Gruppen wie Bronze Tiger (China) infiltrieren Telekommunikationsinfrastrukturen, um langfristig Daten zu sammeln – etwa für politische oder wirtschaftliche Spionage. Solche Angriffe bleiben oft jahrelang unentdeckt, untergraben aber das Vertrauen in digitale Kommunikation und können strategische Vorteile für die Angreifer schaffen. Die Bedrohung ist dabei nicht nur technischer Natur, sondern betrifft auch die Glaubwürdigkeit ganzer Gesellschaftssysteme, etwa wenn Bankdaten oder Regierungsinformationen kompromittiert werden.

Überwachung, Erkennung und frühe Reaktion
Angesichts dieser Bedrohungen müssen Telekommunikationsunternehmen und andere Betreiber kritischer Infrastrukturen proaktiv handeln. Ein zentraler Schritt ist eine risikobasierte Sicherheitsstrategie, die mit einer vollständigen Bestandsaufnahme aller IT-Assets beginnt.

Nur wer weiß, welche Daten und Systeme geschützt werden müssen, kann gezielt handeln. Entscheidend aber ist eine umfassende Überwachung, um Angriffe mit Hilfe von KI und menschlichen Security-Experten frühzeitig zu erkennen. Wer mit kontinuierlicher Überwachung eine Bedrohung im Anfangsstadium erkennt, ist in der Lage, einen Angriff und gravierende Schäden für den Kritis-Anbieter und die gesamte Kommunikationskette abzuwenden.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de