Die Lieferkette als primäres Ziel für Cyberangreifer

Die Lieferkette ist aufgrund ihrer vernetzten Struktur aus unterschiedlichen Akteuren anfällig für Störungen und für Cyberkriminelle nach wie vor ein beliebtes Angriffsziel. Technische und gesellschaftliche Entwicklungen verschärfen diese Gefahr. Aber: Unternehmen können sich wehren. Michael Veit, Cybersecurity-Experte bei Sophos, gibt einen kompakten Überblick.

Mit dem stetigen Voranschreiten der digitalen Transformation in den letzten Jahren wurden Unternehmen zunehmend abhängig von zahlreichen Partnern und Lieferanten. Diese Verschiebung hat zu einer komplexeren IT-Infrastruktur geführt und signifikant die Angriffsfläche vergrößert, die Cyberkriminelle ausnutzen können. Sie haben es auf das schwächste Glied in der Lieferkette abgesehen, um Zugang zum Gesamtsystem zu bekommen.

Ein Beispiel: Im November 2024 wurde der US-amerikanische Software-Provider Blue Yonder Opfer einer Ransomware-Attacke, die sich auf den Betrieb von 3.000 Firmen in 76 Ländern auswirkte. Das führt zu der Frage: Wie können wir die gesamte Lieferkette vor immer häufigeren und anspruchsvolleren Cybergefahren schützen?

Chancen und Risiken bei Open Source und KI

Angesichts des vernetzten Charakters von Unternehmens-, Lieferanten- und Partnersystemen suchen sich Cyberkriminelle immer stärker Drittparteien als Ziel aus, um ihre Attacken auszuführen und Unternehmensdaten und -systeme zu kompromittieren. KMUs und Subunternehmer sind aufgrund ihrer limitierten Ressourcen im Bereich Cybersicherheit besonders verwundbar.

Gerade Open-Source-Softwarekomponenten bieten eine Angriffsfläche. Da der Codiercode öffentlich ist, können Angreifende diesen nach Mängeln erforschen und zeitgleich möglicherweise viele Software-Anwendungen ausnutzen, indem sie kritische Fehler entdecken. Der offene Ansatz bietet aber auch Vorteile. Beliebte Open-Source-Bibliotheken werden kontinuierlich geprüft und verbessert, und zwar durch Hunderte Mitwirkende, was zu einem schnelleren Aufdecken von Problemen und rascheren Updates führt.

Remote-Arbeit, KI, Arbeits-E-Mails auf dem Privathandy: alles Angriffsflächen

Cyberkriminelle nutzen zudem vermehrt Social Engineering, um Arbeitnehmende mit strategischem Zugang oder hochprivilegiertem Status innerhalb der IT-Infrastruktur ins Visier zu nehmen. Das erlaubt ihnen, die technische Abwehr mithilfe von menschlichen Manipulationstaktiken zu umgehen. Die rasante Entwicklung Künstlicher Intelligenz hat diese Techniken weiter verfeinert, indem es ultra-zielgerichtete Phishing-Kampagnen, Deepfakes und überzeugende mobile Angriffe ermöglicht. Schlussendlich haben der Anstieg an Fernarbeit und der Gebrauch von persönlichen Geräten wie Mobiltelefone für den professionellen Nutzen die Angriffsfläche für Cyberkriminelle vergrößert.

Verteidigungsstrategien vertrauen auf Zero Trust und MFA

Um diese Risiken zu verringern, müssen Unternehmen umfassende Verteidigungsstrategien implementieren. Es gilt, durch die Anwendung der richtigen Konzepte, Werkzeuge und Partner, mögliche Attacken zu bekämpfen. Der Zero-Trust-Ansatz ist ein Eckpfeiler einer starken Cybersicherheits-Strategie. Er basiert auf dem Prinzip „niemals vertrauen, immer überprüfen“.

Das beinhaltet auch, starke Authentifizierungsmethoden wie zum Beispiel Multifaktortechnologien zu realisieren, kombiniert mit strengen Kontrollen und segmentierter

Zugangsverwaltung. Es ist essenziell, sicherzustellen, dass nur die richtigen Mitarbeitenden den angemessenen privilegierten Stand haben. Zudem sind Zugänge regelmäßig zu überprüfen und gegebenenfalls anzupassen, besonders für externe Lieferanten oder Partner.

Regulierungen helfen, Lieferkettenangriffe zu bremsen
Es ist gleichermaßen wichtig, zu gewährleisten, dass alle Mitglieder des Ökosystems über adäquaten Sicherheitsschutz verfügen, sowohl aus Cybersicherheitsgründen als auch zur Einhaltung von gesetzlichen Auflagen. Seitdem die DORA Regulierung (Digital Operational Resilience Act) im Januar 2025 in Kraft trat, müssen zum Beispiel Finanzdienstleister zusichern, dass all ihre Lieferanten und Partner die etablierten Sicherheitsstandards erfüllen.

Cyberkriminelle greifen mit wachsender Vorliebe Lieferketten an, um sichere Systeme zu infiltrieren – indem sie kleinere, weniger gut ausgestattete Lieferanten und Partner ausnutzen. Um die Geschäftskontinuität zu gewährleisten und zunehmend komplexe und vernetzte IT-Infrastrukturen zu schützen, müssen Unternehmen effektive Cybersicherheitsstrategien und bewährte Verfahren entwickeln und umsetzen. Das beinhaltet Zusammenarbeit nicht nur mit Dritten, sondern auch mit Cybersicherheitsexperten, die zugeschnittene Lösungen bereitstellen, beraten und unterstützen, um den technischen Rahmen zu schaffen, der nötig ist, um das gesamte Ökosystem unter Einhaltung gesetzlicher Regelungen zu schützen.

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