proofpoint.

THREAT BRIEFING

Lieferkettenangriffe

Die Fakten

BESCHREIBUNG

Lieferkettenangriffe lassen sich in zwei Hauptkategorien einteilen: E-Mail-Betrug und Drittanbieter-Software. Bei diesen Angriffen kompromittieren Cyberkriminelle Lieferanten oder Service-Anbieter, um deren Kunden und Partner anzugreifen. Die ursprüngliche Kompromittierung von Lieferanten erfolgt häufig durch Phishing oder Malware. Sind die Angreifer in ein System eingedrungen, können sie E-Mail-Konten nachahmen und damit Phishing, Rechnungsbetrug und andere Arten von Angriffen gegen die Kunden starten. Nach der Kompromittierung der Kundensysteme haben sie die Möglichkeit, vertrauliche Daten zu stehlen, Ransomware zu installieren oder den Zugriff für eine weitere Welle an Phishing- oder E-Mail-Betrugsversuchen zu nutzen.

DER WERKZEUGKASTEN

Bei Lieferkettenangriffen werden in der Regel Phishing-Betrug zur Erbeutung von Anmeldedaten (Kontoübernahme), Malware (Stuxnet, NotPetya, Sunburst, Kwampirs) sowie Impostor-Bedrohungen wie Business Email Compromise (BEC) eingesetzt.

ANGRIFFSTYPEN

- **Business Email Compromise (BEC) oder E-Mail-Betrug:** Die Angreifer geben sich als jemand aus, dem der Empfänger vertraut – typischerweise ein Geschäftspartner, Lieferant oder Anbieter. Der Empfänger wird darum gebeten, eine Überweisung zu tätigen, eine gefälschte oder geänderte Rechnung zu bezahlen, Gehaltszahlungen umzuleiten oder Bankverbindungen für künftige Zahlungen zu ändern. Bei einigen E-Mail-Betrugsmaschen kompromittiert der Angreifer das tatsächliche E-Mail-Konto des Lieferanten, um sich als dieser Lieferant ausgeben und dabei sogar existierende E-Mail-Threads ausnutzen zu können.
- **Software-Lieferkettenangriffe:** Die Angreifer erlangen Zugang zu den Systemen eines Software-Anbieters oder Managed Service Providers und infizieren künftige Builds, die dann an die Kunden und Partner verteilt werden. Diese Angriffe sind im Vergleich zu den oben aufgeführten Formen recht selten, allerdings können dabei durch einen einzigen Zwischenfall mehrere Opfer kompromittiert werden.

RISIKOFAKTOREN

- Beauftragung von Anbietern für Professional Services und Beratung
- Mangel an angemessenen Cybersicherheitsmaßnahmen
- Gewähren von Zugriff für Mitarbeiter, die fahrlässig handeln oder keine Sicherheitsschulungen erhalten haben
- Komplexität der Lieferkette – Unternehmen setzen zunehmend auf eine Vielzahl an Cloud-Plattformen und SaaS-Diensten

Lieferkettenangriffe in den Schlagzeilen

Target muss 18,5 Mio. USD für Datenschutzverletzung von 2013 zahlen, bei der 41 Mio. Kunden betroffen waren

Von einem Target-Lieferanten gestohlene Kontoanmeldedaten ermöglichten Angreifern, die Systeme des Einzelhandelsriesen zu kompromittieren und vertrauliche Zahlungsinformationen von über 41 Millionen Kunden zu entwenden.

Hacker greifen Lieferkette von COVID-19-Impfstoffen an

Bei einem Phishing-Angriff wurden Führungskräfte aus weltweit 44 Unternehmen ins Visier genommen. Ziel war die Kompromittierung der globalen Lieferkette für COVID-19-Impfstoffe.

Gemeinnützige Wohnungsbaugesellschaft verliert 1,2 Mio. USD durch BEC-Betrug

Angreifer fälschten eine Anbieterdomäne und stahlen bei einer gemeinnützigen Wohnungsbaugesellschaft in der Nähe von London Mieteinnahmen in Höhe von beinahe einer Million britische Pfund.

Ablauf eines Lieferkettenangriffs

1. **Infiltration**

   Die Angreifer nutzen eine Vielzahl an Methoden für die erste Kompromittierung:

- Brute-Force-Angriffe mit automatisierten Tools, die Kombinationen von Benutzernamen und Kennwörtern ausprobieren, bis die richtige gefunden ist

- Nachahmung eines vertrauenswürdigen Kontakts, um Phishing-, Impostor-E-Mails oder Links bzw. Anhänge mit Malware (z. B. Keylogger oder Stealer) zu verschicken

- Übernahme des Kontos eines vertrauenswürdigen Lieferanten

2. **Aufklärung**

- Sobald die Angreifer gültige Anmeldedaten gestohlen haben, können sie damit das Netzwerk und den Ruf des Lieferanten missbrauchen. Anschließend überwachen sie die Kommunikation zwischen dem Lieferanten und seinen Kunden und suchen nach möglichen Opfern.

3. **Angriff**

- Nach der Aufklärung können die Angreifer über die kompromittierten Lieferantensysteme Phishing-Versuche starten, um an Anmeldedaten zu gelangen, gefälschte Rechnungen versenden oder Malware an Kunden verschicken.

Forschungserkenntnisse

Im Februar 2021 analysierte Proofpoint über einen Zeitraum von einer Woche Daten von 3.000 Unternehmen in verschiedenen Branchen in den USA, Großbritannien und Australien. Der überwiegende Teil der Unternehmen war in dieser Zeit von Lieferkettenangriffen betroffen.

98 % erhielten eine Bedrohung über einen Lieferanten, der entweder nachgeahmt oder kompromittiert wurde.

Die Wahrscheinlichkeit von Angriffen war über alle Länder und Branchen in der Probe gleich verteilt.

Von diesen Bedrohungen gingen etwa drei Viertel auf Phishing-Betrug oder Nachahmung zurück.

< 30 % der von Lieferantendomänen verschickten E-Mails enthielten Malware.

SO BEGÜNSTIGT CYBERCRIME-AS-A-SERVICE LIEFERKETTENANGRIFFE

Das Dark Web ist ein berüchtigter Marktplatz für Exploit-Kits und maßgeschneiderte Malware, auf dem auch Dienstleistungen wie Botnet-Vermietungen und Ransomware-Software angeboten werden. Ähnlich wie die meisten SaaS-Anbieter stellen Cyberkriminelle Tools und Plattformen für diejenigen bereit, die Lieferketten- und Ransomware-Angriffe sowie andere Arten von Cyberverbrechen ausführen möchten. Bedrohungsakteure ohne umfangreiches technisches Wissen haben es dadurch leicht, Angriffe auszuführen.

So schützen Sie Ihr Unternehmen

Im Folgenden erläutern wir einige wichtige Sicherheitskontrollen, die Unternehmen implementieren sollten, um Lieferkettenbetrug und Software-Lieferkettenangriffen zu verhindern.

Lieferkettenbetrug

Für Lieferantenrechnungsbetrug sollten Unternehmen einen ganzheitlichen, mehrstufigen Ansatz wählen, da die Angreifer häufig sowohl Lieferanten nachahmen als auch Lieferantenkonten kompromittieren.

BEC-Betrug beginnt häufig mit einer E-Mail, deren Absender sich als vertrauenswürdige Person ausgibt. Dazu ahmt der Angreifer entweder diese Person nach oder übernimmt deren Konto. Da bei BEC-Angriffen keine Schaddaten verwendet werden, sind sie für herkömmliche Gateways, die ausschließlich auf Reputation und Malware-Sandbox-Analysen setzen, nur schwer zu erkennen.

Im Folgenden erfahren Sie, wie Sie die häufigsten und kostspieligsten Lieferkettenangriffe stoppen können.

Verschaffen Sie sich einen Überblick über Ihre Risiken
Um die Risiken besser zu verstehen, zu kommunizieren und zu minimieren, sollten Sie folgende Fragen beantworten:

- Welche BEC-Risiken bestehen in unserem Unternehmen?
- Welche Anwender sind am stärksten gefährdet?
- Welche Lieferanten stellen ein Risiko für unser Unternehmen dar?
- Was können wir tun, um die Risiken zu minimieren?

Sie sollten wissen, welche Anwender am häufigsten von Impostor-Bedrohungen angegriffen werden und wer am ehesten auf solche Bedrohungen hereinfällt.

Gleichzeitig kann Ihnen ein detaillierter Überblick über BEC-Bedrohungen und die Identifizierung gängiger BEC-Maschen (z. B. Betrug mit Lieferantenrechnungen und Umleitung von Gehaltszahlungen) helfen, BEC-Risiken besser zu verstehen und zu kommunizieren.

Erkennen und blockieren Sie Impostor-Bedrohungen, noch bevor sie Ihr Unternehmen erreichen
Um Betrugsversuche über Lieferanten-E-Mails zu stoppen, müssen alle E-Mail-Betrugstaktiken wie Display Name-Spoofing, Doppelgänger-Domänen und raffinierter Lieferantenbetrug aufgedeckt werden. Wählen Sie eine Lösung, die Nachrichten auf zahlreiche Taktiken, die zum Lieferantenbetrug gehören, dynamisch analysiert, z. B.:

- Änderungen der Reply-to-Adresse
- Verwendung schädlicher IP-Adressen
- Verwendung nachgeahmter Lieferantendomänen
- Wörter und Formulierungen, die für Lieferantenbetrug typisch sind

Die meisten E-Mail-Sicherheitsprodukte setzen lediglich auf statische Regelabgleiche oder begrenzte Kontextdaten, wodurch manuelle Optimierungen erforderlich sind.

Für Lieferantenrechnungsbetrug sollten Unternehmen einen ganzheitlichen, mehrstufigen Ansatz wählen, da die Angreifer häufig sowohl Lieferanten nachahmen als auch Lieferantenkonten kompromittieren.

Stärken Sie die Resilienz Ihrer Anwender gegenüber BEC-Lieferkettenangriffen
BEC richtet sich gegen Menschen und versucht, diese zum Ausführen von Angriffen zu bringen, ohne dass diese es merken. Da diese Impostor-Angriffe auf Social Engineering und Identitätstäuschung setzen, bilden Ihre Anwender häufig die letzte Verteidigungslinie. Daher sind zur Minimierung von BEC-Risiken sowohl Technologie als auch Schulungen erforderlich.

Schulen Sie Ihre Anwender darin, verdächtige Impostor-E-Mails zu identifizieren und zu melden. Dadurch vermitteln Sie Ihren Endnutzern die Kenntnisse und Fähigkeiten, mit denen sie Ihr Unternehmen vor diesen personenzentrierten Bedrohungen schützen können.

Warnhinweise in E-Mails können das Risiko jeder E-Mail sichtbar machen, zum Beispiel indem Sie die Anwender warnen, wenn eine Nachricht von einem externen Absender oder einer neu registrierten Domäne stammt. Dies ermöglicht ihnen, im Zweifelsfall eine informierte Entscheidung zu treffen.

Schützen Sie Ihre eigene Marke vor Missbrauch in E-Mail-Betrugsangriffen
Während Sie sich über die Risiken durch Ihre Lieferanten sorgen, könnten Ihre Kunden ähnliche Bedenken Ihrem Unternehmen gegenüber haben.

Angreifer richten sich direkt gegen Ihre Kunden und Geschäftspartner und versuchen, über Ihren Firmennamen und Ihre Marke an Geld zu gelangen. Auch wenn Marken-Spoofing keine direkten finanziellen Schäden für Ihr Unternehmen bedeutet, kann es die Reputation und das Vertrauen Ihrer Kunden schädigen und das Geschäft beeinträchtigen.

Verhindern Sie den Versand betrügerischer E-Mails, die von Ihnen oder Dritten verschickt werden, durch den Einsatz von DMARC-E-Mail-Authentifizierung.

Software-Lieferkettenangriffe

Neben den oben erläuterten verbreiteten Lieferketten-angriffen wird durch die Nutzung von Software, die von Drittanbietern oder Managed Service Providern stammt, ein weiteres Risiko in der Lieferkette geschaffen.

Wenn ein kompromittierter Anbieter Software oder Cloud-Dienste bereitstellt, können Angreifer den Quellcode verändern und Malware in das Build oder den Update-Prozess injizieren. Die infizierten Programme oder Dienste werden dann – einschließlich der von den Angreifern eingeschleusten Schaddaten – an Kunden und Partner weitergegeben.

Häufig fehlen den Anwendern die Kenntnisse, um die von ihnen verwendeten Drittanbieterprogramme überprüfen zu können. Sie müssen sich also darauf verlassen, dass ihre Software-Anbieter und Lieferanten zuverlässige Schutzmaßnahmen getroffen haben. Wenn eine kompromittierte Software an ein Unternehmen geliefert wird, kann es einer ganzen Palette an Angriffen ausgesetzt sein, die von Datendiebstahl bis hin zu einer Ransomware-Infektion reichen.

Diese Art von Angriff lässt sich besonders schwer verhindern. Nicht gepatchte Software-Schwachstellen sind einer der am häufigsten genutzten Vektoren für Cyberangriffe. Die Aktualisierung der Software auf die neueste Version wird daher immer als eine empfohlene Vorgehensweise angesehen – nun jedoch ist auch dies zu einem Angriffsvektor geworden.

Weitere Informationen

Angesichts der vielen in den Schlagzeilen stehenden Lieferkettenangriffe wird deutlich, dass Drittanbieter-Dienste, Lieferanten und Auftragnehmer eine ernste Gefahr für die Sicherheit von Unternehmen darstellen. Eine personenzentrierte Lösung, die neue Tools, Ziele und Taktiken der Angreifer erkennt, kann dieses Risiko minimieren.

Weitere Informationen zur effektiven Abwehr von Lieferkettenangriffen finden Sie unter **www.proofpoint.com/de**.