HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE

STÄRKUNG DER SICHERHEIT IHRER LIEFERKETTE

In diesem Infopaper beleuchten wir die Schwachstellen innerhalb von Lieferketten und erläutern, wie der Aufbau einer robusten Sicherheitskultur – unterstützt durch regelmäßige Schulungen zum Sicherheitsbewusstsein – entscheidend zur Gewährleistung der Datensicherheit sowohl bei Dienstleistern als auch bei den Unternehmen, die ihre Dienste in Anspruch nehmen, beiträgt.

DIE RISIKEN IN DER LIEFERKETTE

Moderne Unternehmen verlassen sich auf eine Vielzahl von Hardwarekomponenten, Softwareanwendungen und Cloud-Diensten, die alle von verschiedenen Anbietern bezogen werden. Diese gegenseitige Abhängigkeit schafft mehrere Risikopunkte:

- **Komplexe Anbieternetzwerke:** Jeder Lieferant, ob für physische Teile oder Softwarekomponenten, ist ein potenzielles Einfallstor für einen Angriff.
- **Phishing und Social Engineering:** Angreifer verwenden oft ausgeklügelte Phishing-Methoden, um Anbieter zu kompromittieren und dann deren Kunden ins Visier zu nehmen.

REALE BEISPIELE:

Angriffe auf NHS und Change Healthcare

Störungen kritischer Dienste hatten weitreichende Auswirkungen. Jüngste Angriffe legten die Diagnostik des NHS durch Ransomware (Synnovis) lahm und beeinträchtigten den Betrieb von Change Healthcare erheblich.

SolarWinds-Vorfall

Ein viel beachteter Sicherheitsverstoß, der zeigte, wie kompromittierte Updates Angreifern Zugang zu ansonsten sicheren Netzwerken verschaffen können. Der russische Geheimdienst veränderte ein Update von SolarWinds Orion und infiltrierte über den bösartigen Patch zahlreiche Organisationen.

3CX in Nordkorea

Nordkoreanische Hacker führten 2023 einen mehrstufigen Angriff durch, bei dem sie 3CX über eine Drittanbietersoftware auf einem Mitarbeiter-PC kompromittierten. Dies ermöglichte die weltweite Verbreitung eines bösartigen 3CX-Updates.

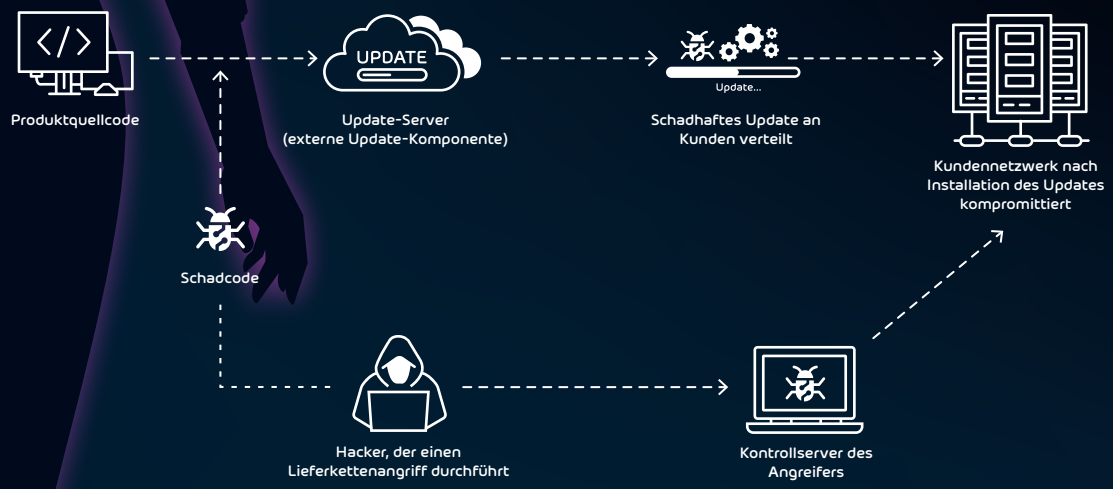
HORNETSECURITY

INFO
SHEET

ANATOMIE EINES ANGRIFFS AUF DIE LIEFERKETTE

Es ist wichtig zu verstehen, wie diese Angriffe funktionieren:

- **Kompromittierung des Anbieters:** Cyberkriminelle infiltrieren einen vertrauenswürdigen Anbieter über Abhängigkeiten von Drittanbietern oder Update-Mechanismen.
- **Einschleusen von bösartigem Code:** Sobald sie in das System des Anbieters eingedrungen sind, fügen die Angreifer schädlichen Code ein, der als Hintertür fungiert.
- **Verteilung an Kunden:** Das bösartige Update wird dann an die Endbenutzer verteilt und gefährdet deren Systeme.
- **Datendiebstahl und Unterbrechung:** Wenn Angreifer Zugang zum Zielunternehmen haben, können sie Daten stehlen und den Betrieb stören.



DIE NOTWENDIGKEIT VON SICHERHEITSBEWUSSTSEIN

In Lieferketten ist es wichtig, daran zu denken, dass nicht nur die Sicherheit der eigenen Daten eines Dienstleisters auf dem Spiel steht, sondern auch die aller Unternehmen, für die er tätig ist. Selbst die ausgefeiltesten technischen Sicherheitsvorkehrungen können durch menschliches Versagen untergraben werden. Bei der Cyber-Resilienz geht es nicht nur um den Einsatz fortschrittlicher Technologien, sondern auch um den Aufbau einer Sicherheitskultur.

- **Ermächtigen Sie Ihr Team:** Die Schulung der Mitarbeiter zur Erkennung von Phishing-Versuchen und anderen Social-Engineering-Taktiken ist Ihre erste Verteidigungslinie.
- **Kontinuierliche Verbesserung:** Regelmäßige, automatische Schulungen helfen den Mitarbeitern, wachsam zu bleiben und mit den sich entwickelnden Bedrohungen Schritt zu halten.

09-25

HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE: IHR SCHUTZSCHILD GEGEN SUPPLY-CHAIN-ATTACKEN

Der Security Awareness Service von Hornetsecurity wurde entwickelt, um die Lücke zwischen technischen Schutzmaßnahmen und menschlichen Schwachstellen zu schließen, durch:

- **Employee Security Index (ESI):** Bewertung der individuellen Risikoprofile und Anpassung der Schulung an die spezifischen Bedürfnisse.
- **Automatisierte, fortlaufende Schulungen:** Kontinuierliche simulierte Phishing-Übungen und Schulungsinhalte zur Verbesserung der Wachsamkeit im Laufe der Zeit.
- **Geringer Verwaltungsaufwand:** Nahtlose Integration in Ihre bestehende Sicherheitsinfrastruktur, wodurch Ressourcen freigesetzt werden und gleichzeitig ein robuster Schutz gewährleistet ist.
- **Nachgewiesene Ergebnisse:** Eine verbesserte Sicherheitskultur führt zu weniger Vorfällen von Phishing- und anderen Social-Engineering-Angriffen und schützt Ihre gesamte Lieferkette.

WICHTIGSTE VORTEILE

Risiken reduzieren:

Proaktive Risikominderung durch Aufklärung der Mitarbeiter über neue Bedrohungen.

Lieferanten-beziehungen stärken:

Zeigen Sie Ihr Engagement für Sicherheit, um Partner und Kunden zu beruhigen.

Resilienz in der Praxis:

Gewährleisten Sie die Geschäftskonti-nuität auch bei kom-plexen Angriffen auf die Lieferkette.

Wettbewerbsvorteil:

Nutzen Sie gut geschulte Mitarbeiter als Alleinstellungs-merkmal auf dem Markt.

Befähigen Sie Ihr Team zur Abwehr von Cyber-Bedrohungen!

MEHR LERNEN!

09/25