**APPGUARD**

Die Malware-Defensive

# Abschwächen der Lieferkettenrisiken:

## Schützen Sie Ihr Unternehmen, auch wenn Ihre Software-Lieferkette kompromittiert wurde

WHITEPAPER

**ZUSAMMENFASSUNG:**

*Der jüngste SolarWinds-Lieferkettenangriff ist eine eindringliche Mahnung, dass wir alle Teil irgendeiner Lieferkette sind und das jede Kette ein schwaches Glied hat. Dieses Dokument verdeutlicht, wie sich Angriffe auf Lieferketten entwickeln und erläutert die Schritte, die Sie mit Hilfe einer Zero-Trust- Lösung ergreifen können, um nicht dem nächsten Lieferketten-Exploit zum Opfer zu fallen.*

## Die Lieferkettenbedrohung

Wenn Sie in der Sicherheitsbranche arbeiten und dafür verantwortlich sind, die Vermögenswerte Ihrer Organisation vor Einbrüchen zu schützen, haben Sie wahrscheinlich von dem jüngsten SolarWinds-Angriff gelesen. Dies ist nicht der erste hervorstechende Lieferkettenangriff und mit Sicherheit nicht der letzte. Hacker haben erkannt, dass erfolgreiche Angriffe auf Lieferketten einen Dominoeffekt zur Folge haben: indem sie nur einen einzigen Anbieter angreifen, können sich Angreifer Zugang zu allen Kunden dieses Anbieters verschaffen.

Lieferkettenangriffe sind besonders gefährlich. Bei einem Angriff auf eine Lieferkette infiltrieren Angreifer vertrauenswürdige Anwendungen von dritten Parteien, die auf Ihre Systeme und Daten zugreifen - ohne dass Sie oder der Anbieter davon wissen. Ohne Kontrolle über die Sicherheitslage und die Praktiken einer außenstehenden Organisation, jedoch abhängig von ihrem Angebot, sehen sich Unternehmen einem schwierigen Sicherheitsdilemma gegenüber - wie soll man sich vor derartigen Angriffen schützen?

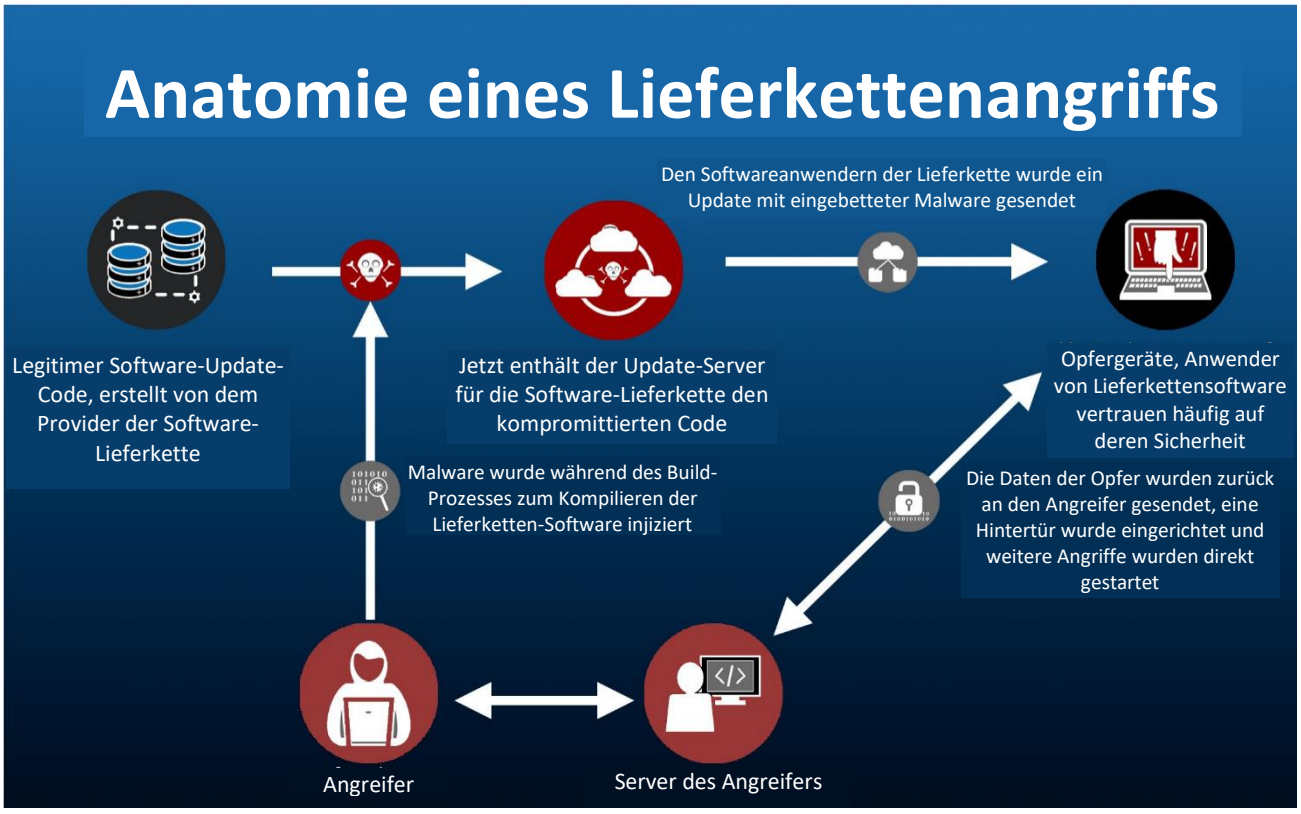
Im Falle der SolarWinds-Angriffe kann die Ernsthaftigkeit des Angriffs nicht genug hervorgehoben werden und unglücklicherweise ist die Wahrscheinlichkeit ähnlicher Angriffe in naher Zukunft ziemlich hoch. Der SolarWinds-Angriff war aufgrund seines beispiellosen Ausmaßes wahrscheinlich der bisher dramatischste. Obwohl das gesamte Ausmaß der Auswirkungen erst in einigen Monaten bekannt sein wird, wissen wir bereits, dass bis zum Ende 2020 mehr als 18.000 Organisationen und mehrere US-Regierungsbehörden betroffen waren, wie ein von SolarWinds im Dezember 2020 bei der SEC eingereichter Bericht mitteilt.

## Vertrauenswürdigen Apps kann man nicht immer trauen

Der SolarWinds-Angriff erinnert wieder einmal daran, dass man selbst vertrauenswürdigen Anwendungen nicht immer vollständig vertrauen kann. Hacker haben ihr Handwerk verfeinert und wissen, wie sie den Quellcode von Anwendungen erfolgreich infiltrieren können und so vollständigen Zugang zu den Daten von Softwareanbietern und Endkunden erlangen. Kompromittierte Anbieter übertragen die Malware unfreiwillig an ihre Kunden.

Lieferkettenangriffe erfolgen heimlich und verwenden häufig mehrere Angriffsvektoren, die vorhandene Schutzmechanismen umgehen. Im Fall von SolarWinds war der böswillige Code in digital signierte Binärdateien eingebettet, wodurch sichergestellt war, dass die kryptographischen Schutzmaßnahmen der Organisationen der Kunden versagten. Als SolarWinds sein Produkt aktualisierte, war der versteckte Code in dem Update-Paket enthalten - was den Zugang zu Servern und Daten dritter Parteien ermöglichte.

Während der SolarWinds-Angriff wohl einer der bedeutendsten vom Staat unterstützten Hacks der letzten Jahre ist, handelt es sich nicht um einen Einzelfall. Angesichts des heutigen digitalen Zeitalters und der Abhängigkeit der Welt von Software, um Unternehmen und Regierungen zu betreiben, müssen Organisationen ihre Sicherheitsinitiativen priorisieren, um zu gewährleisten, dass sie sich effektiv vor Lieferkettenangriffen schützen können.



> *Was also kann eine Organisation tun, wenn sie keine andere Wahl hat, als der Sicherheit von Lieferkettenanbietern zu vertrauen, jedoch keine Kontrolle über das Sicherheitsmanagement dieser Anbieter hat?*
>
> *Verwenden Sie Sicherheitssoftware, die Regeln implementiert, die Lieferkettenaktivitäten wie alle anderen behandelt. Selbst den vertrauenswürdigsten Anwendungen kann man nicht vollständig trauen.*

## Lieferkettenangriffe überlisten herkömmliche Tools zur Endpunkt-Absicherung

Unglücklicherweise haben Lieferkettenangriffe ihre Fähigkeiten bewiesen, die von den meisten Endpunkt-Absicherungstools verwendeten Methodologien zu unterminieren. Angesichts der Tatsache, dass herkömmliche Antivirus-Programme und Antivirus-Tools der nächsten Generation Einbrüche feststellen, indem sie bekannten böswilligen Code identifizieren oder Code, der sich nicht auf ihrer Liste vertrauenswürdiger Codes befindet, wird böswilliger Code, der in verbreitete Unternehmenssoftware eingebettet ist, nicht von diesen Tools erkannt.

Im Falle der SolarWinds-Angriffe deaktivierten die Widersacher das Tool für die Erkennung und Reaktion am Endpunkt (Endpoint Detection and Response (EDR)) auf dem ursprünglich kompromittierten Host und konnten so einige „geräuschvolle“ Aktionen ausführen - einschließlich des Einpflanzens von Malware, die geräuschlos arbeitete und legitime Vorgänge imitierte, um der Erkennung zu entgehen. Nach Abschluss der „geräuschvollen“ Aktivitäten wurden der Host und die EDR-Tools neu gestartet. Da die Lieferketten-Malware keine auffindbaren Dateien hinterlässt, die von den EDR-Tools erkannt werden könnten, dachten sich die SOC-Mitarbeiter nichts, als ein einzelner Endpunkt im Bericht der EDR-Plattform für kurze Zeit aufgrund von Deaktivierung abwesend war. Die Malware lief monatelang, ohne von den EDR-Tools erkannt zu werden.

## Verstärken Sie Ihre Lieferkettensicherheit mit AppGuard

Was also kann eine Organisation tun, wenn sie keine andere Wahl hat, als der Sicherheit von Lieferkettenanbietern zu vertrauen, jedoch keine Kontrolle über das Sicherheitsmanagement dieser Anbieter hat? Verwenden Sie Sicherheitssoftware, die Regeln implementiert, die Lieferkettenaktivitäten wie alle anderen behandelt. Selbst den vertrauenswürdigsten Anwendungen kann man nicht vollständig trauen.

AppGuard ist auf einzigartige Weise als Abwehr von Lieferkettenangriffen geeignet, denn es ist so konzipiert, dass es Kontrollen anwendet, die in der Annahme, dass alles an irgendeiner Stelle wahrscheinlich kompromittiert werden wird, missbrauchte Anwendungen unschädlich machen, selbst wenn sie unerkannt bleiben. Da sich AppGuard auf das Kontrollieren der hochriskanten Aktionen konzentriert, die ausgeführt werden müssen, damit ein Angriff einen messbaren Effekt hat, ist sein Schutz immer gleich stark, egal, woher der Angriff kommt - eingeschlossen vertrauenswürdige dritte Parteien.

**AppGuard ist die einzige Software auf dem Markt, die innerhalb der Endpunkte Zero-Trust-Prinzipien anwendet.**

AppGuard versucht nicht, unter unendlichen Möglichkeiten gut und schlecht oder normal und abnormal zu unterscheiden. Es schränkt ganz einfach das Verhalten auf das ein, was erlaubt ist, und wendet dabei innerhalb der Endpunkte Zero-Trust-Prinzipien an. AppGuard konzentriert sich auf das normale Verhalten des Betriebssystems und wendet eine Kombination aus Kontrollen vor dem Start, Eingrenzung und Isolation an, um Malware-Techniken zu bekämpfen, ohne die Malware oder ihre Auswirkungen erkennen zu müssen. Anders als EDR-Tools, die Alarme generieren, die menschliches Eingreifen zwecks Untersuchung erfordern, hängt die Effektivität von AppGuard nicht von der Reaktion von Menschen auf Alarme ab. Stattdessen können sich jene, die AppGuard einsetzen, beruhigt zurücklehnen in dem Wissen, dass alle Aktivitäten außerhalb der vorgegebenen Bahn der Anwendung blockiert werden.

## AppGuard vs. Lieferkettenrisiko: Abschwächen der Bedrohung

AppGuard erzwingt mehrere Regelansätze, die in Kombination einen einzigartigen Schutz vor den am meisten verbreiteten Angriffsvektoren bieten. Es teilt das Dateisystem in vertrauenswürdige und nicht vertrauenswürdige Bereiche mit verschiedenen zulässigen Aktivitäten und Startfähigkeiten ein, isoliert riskante Aktionen und wendet eine patentierte Fähigkeit für einen Kind-Prozess an, der die auf seinen Eltern-Prozess angewandten Regeln „erbt“ (und dadurch das Anpassen der Regeln an den Kontext ermöglicht). So kann AppGuard einen leistungsstarken „Mittelweg“ anbieten - Zero-Trust-Prinzipien anwenden, ohne die betriebliche Integrität zu kompromittieren. Wie bereits zuvor bemerkt, ist es in einem Lieferkettenszenario besonders wirksam, da die Regeln weiter gleichmäßig angewendet werden, ohne in Betracht zu ziehen, dass eine Lieferkettenanwendung ein höheres Vertrauensniveau genießen sollte. Dadurch ist das Unternehmen ungeachtet der Quelle des Angriffs auf die gleiche Weise geschützt. Es folgen Beispiele, wie die Prinzipien der Regeln von AppGuard in einem Lieferketten-Angriffsszenario angewendet werden:

### *Kontrolle von verbotenen Starts*

Bei AppGuard werden die Startkontrollen auf den Dienstprogrammen des Betriebssystems platziert, die administrativen Zugang und die Funktionalität haben, hochriskante Aktivitäten durchzuführen, und die von Malware genutzt würden, um ihr Ziel zu erreichen, wie zum Beispiel Datendiebstahl, Systemkontrolle oder Einrichten eines Zugangs durch die Hintertür.

Solche Dienstprogramme können nur in bestimmten spezifischen Instanzen starten (generell durch Anwendungen, die im Management-System von AppGuard als PowerApps gekennzeichnet sind). Die Standardversion von AppGuard verfügt über grundlegende Restriktionen, die auf die meisten Living-off-the-Land-Binärdateien (LOLBAS) angewendet werden. Diese Restriktionen können bei Bedarf entsprechend den betrieblichen Bedürfnissen angepasst werden.

Wenn die gekaperte Anwendung bei einem Lieferkettenangriff versuchen würde, eines dieser Dienstprogramme laufen zu lassen, um ihr Werk zu vollenden, könnte sie das nur tun, wenn die Anwendung bereits gewollt die ausdrückliche Fähigkeit dazu erhalten hat. Es ist unwahrscheinlich, dass dies in den meisten realen Szenarien der Fall wäre, und selbst dann würden die zusätzlichen Regelwerke von AppGuard den Angriff in einer anderen Phase seines Lebenszyklus blockieren.

Im Beispiel von SolarWinds war wscript.exe ein verbotenes Hilfsprogramm, das an einer kritischen Stelle der Aktivität des Angriffs verwendet wurde. Die Kontrollen von AppGuard für verbotene Starts verhindern das Starten von wscript.exe in der Weise, wie es bei SolarWinds geschah, und hätten den Angriff vereitelt.

Scripts, ausführbare Dateien und DLLs aus hochriskanten Speicherorten wie Ihrem Download-Ordner und anderen üblichen temporären Verzeichnissen, dürfen normalerweise nur ein Programm starten, das von einer Quelle signiert wurde, die sich auf einer Liste mit vertrauenswürdigen Herausgebern befindet. Obwohl eine Lieferkettenanwendung wahrscheinlich als vertrauenswürdiger Herausgeber gekennzeichnet ist, ist diese Regel in Kombination mit den anderen Richtlinien von AppGuard nach wie vor ein effektiver zusätzlicher Schutz. Durch ihr Vorhandensein muss ein Malware-Programmierer ganz genau festlegen, wie er seinen Angriff zustellt und ein einziger Fehler wird den Angriff unschädlich machen. Kombiniert mit den Anforderungen von den anderen von AppGuard generierten Richtlinien, wird das vollständige Ausführen der Malware bis zum Abschluss sehr schwierig.

Im Falle von SolarWinds wurden einige Binärdateien von SolarWinds gestartet und signiert - jedoch wurden einige auch aus dem noch gar nicht signierten Orion-Produkt von SolarWinds aus gestartet. Letzterer Vorgang wäre blockiert worden, hätte Teile des Angriffs unschädlich gemacht und so seine Fähigkeit zum Abschluss unterminiert.

## *Eingrenzung von hochriskanten Anwendungen*

Die Eingrenzungsregel von AppGuard verhindert, dass riskante Anwendungen und Dienstprogramme Änderungen vornehmen oder auf Speicher von Systemressourcen lesen/schreiben können, wobei für besondere Bedürfnisse Ausnahmen möglich sind. Dadurch können einige Anwendungen, die normalerweise am Starten gehindert würden, stattdessen mit restriktiven Kontrollen laufen, die verhindern, dass sie zum Erteilen von Befehlen und Kontrollieren des Systems verwendet werden. In der Voreinstellung würden die meisten

> *AppGuard ist mit seinem Zero-Trust-Ansatz ein entscheidendes Element in einer jeden effektiven Lieferkettenabwehr. Es ist „herkunftsagnostisch“ und blockiert die Ausführung von Malware von einer „vertrauenswürdigen“ Quelle in Ihrer Informationsarchitektur ähnlich dem, was während des SolarWinds-Angriffs passierte.*
>
> **Mark Kelton**
> **Ehemaliger Direktor Spionageabwehr, CIA**

Kind-Prozesse von Lieferkettenanwendungen in einer eingegrenzten Kategorie platziert, mit starken Restriktionen ihrer Fähigkeiten, solche Aktionen außerhalb ihrer normalen Aktivitäten auszuführen.

## *Vererbung von Hochrisiko-Regeln*

Sobald ein Prozess als „hochriskant“ markiert wurde, werden alle seine untergeordneten Prozesse ebenfalls als hochriskant gekennzeichnet. Dadurch kann sich die Regel schnell in Echtzeit anpassen, um neue und unbekannte Verhaltensweisen zu vereiteln, die letztendlich von einer neuen Art von Angriff stammen könnten.

Im Falle von SolarWinds könnte dies Versuche stoppen, Cobalt Strike auszuführen (ursprünglich ein Tool für Penetrationstests, wird heute aber auch von Angreifern verwendet, um ein „Leuchtfeuer“ auf einem System zu errichten) und sich zurück mit dem Netzwerk des Angreifers zu verbinden.

## *Isolationsregel über LSASS*

Die Isolationsregel blockiert den Zugang zu Speicher und Steuerung von wertvollen Systemressourcen, wobei nur wenige spezifische Ausnahmen als betriebliche Notwendigkeiten erlaubt sind, die durch einen Administrator konfiguriert werden. Local Authority Security Service (LSASS) ist ein Beispiel für einen zentralen Windows-Sicherheitsprozess, der administrative Zugangsdaten beherbergt und der Isolation unterliegt, weil er ein wertvolles Ziel für den Diebstahl von Zugangsdaten ist.

Im Falle von SolarWinds wurden Zugangsdaten vom LSASS gestohlen, um auf andere Ordner in der Infrastruktur des Unternehmens zuzugreifen. Für SolarWinds hätte keine spezifische LSASS-Zugriffsausnahme erstellt werden müssen, denn AppGuard hätte diesen Versuch in seinen Anfängen blockiert.

> *AppGuard ist die einzige Lösung auf dem Markt, die **innerhalb** der Endpunkte Zero-Trust-Prinzipien anwendet.*

Diese Beispiele verdeutlichen die Vorteile der wahren präventiven Techniken von AppGuard, die Redundanzen und Barrieren auf die gefährlichen Aktivitäten anwenden, die Malware versucht, im Verlauf eines Angriffs auszuführen.

Während die meisten Anbieter von Endpunkt-Absicherungen versuchen, böswilliges Verhalten zu erkennen und darauf zu reagieren, werden sie oft zum Narren gehalten, wenn eine solche Aktivität von einer vertrauenswürdigen Lieferkettenanwendung ausgeht. Der präventive Ansatz von AppGuard ist anders. Er begrenzt Aktivitäten innerhalb der Endpunkte, die es Malware erlauben, einen erfolgreichen Angriff durchzuführen und errichtet in den verschiedenen potenziellen Phasen eines Angriffs Barrieren. Dieser Ansatz gewährleistet, dass Schutzmaßnahmen den Erfolg des Angriffs bereits vereiteln, bevor er erkannt wurde. Lieferkettenangriffe sind schwierig zu erkennen, weil die böswillige Anwendung als vertrauenswürdig gilt. AppGuard bietet Schutz ohne Detektion - selbst gegen so ausgereifte Angriffe wie die SolarWinds-Attacke.

## Lieferkettenangriffe mit der richtigen Abwehr überlisten

Der jüngste SolarWinds-Lieferkettenangriff ist eine eindringliche Mahnung, dass wir alle Teil irgendeiner Lieferkette sind und dass jede Kette ein schwaches Glied hat. Selbst vertrauenswürdigen Anwendungen kann man nicht trauen. Der SolarWinds-Vorfall verdeutliche die erheblichen Auswirkungen, die Angriffe über Software-Lieferketten haben können und die Tatsache, dass die meisten Organisationen nicht auf das Verhindern und Erkennen solcher Angriffe vorbereitet sind. Organisationen müssen einen Zero-Trust-Ansatz verwenden, um sicherzustellen, dass die Endpunkte und Software von dritten Parteien frei von böswilligen Inhalten sind. Wer das nicht tut, ist stärker darauf angewiesen, die Nadeln in dem Detektions-Heuhaufen zu finden. Letzterer Ansatz hat die Unternehmen nicht vor den SolarWinds-Angriffen geschützt. Heute müssen Unternehmen mehr denn je Abwehrmechanismen einsetzen, die sie vor ihren eigenen vertrauenswürdigsten Anwendungen schützen, sollten diese kompromittiert sein.

## Über AppGuard

AppGuard ist ein Cybersecurity-Unternehmen, das es sich zur Aufgabe gemacht hat, einen neuen Standard zu setzen: echter Cyber-Schutz für alle. Die patentierte Technologie von AppGuard verhindert Kompromittierungen, bevor sie geschehen, indem sie Malware-Aktivitäten daran hindert, Schaden anzurichten, ohne sie wiederkennen zu müssen. Im Gegensatz zu erkennungsbasierten Lösungen überlistet AppGuard böswillige Akteure, damit Unternehmen ihren Aufgaben nachgehen können und die Schadsoftware nicht machen kann, was sie will.



**APPGUARD**

Die Malware-Defensive

www.appguard.us | software@ingrammicro.ch