MEINUNGEN

ANGRIFFE AUF CYBERSICHERHEIT SANBIETER UND DEREN LÖSUNGEN – EIN TREND, DER SICH BESTÄTIGT?

Stéphane Prevost
Product Marketing Manager, Stormshield

Die IT-Sicherheit von Cyberanbietern ist einem großen Druck ausgesetzt, denn die Anzahl der Angriffe auf die Cybersicherheit nimmt zu.

Die Destabilisierung von IT-Sicherheitsunternehmen und die Beeinträchtigung ihrer Sicherheitslösungen ist seit einiger Zeit ein Hauptaugenmerk des Malware-Ökosystems. Dieser Trend wird sich auch im Jahr 2021 fortsetzen. Kann man folglich sagen, dass die Anbieter von Cybersicherheitslösungen dabei sind, zu den Hauptzielen für Cyberattacken werden? Da diese Lösungsanbieter ein wichtiger Teil der Verteidigung eines Unternehmens gegen Cybersicherheitsangriffe sind, **haben Cyberkriminelle ein großes Interesse daran, sie zu schwächen und zu beeinträchtigen**. Es liegt somit in der Verantwortung der Lösungsanbieter, Cybersicherheit noch besser zu unterstützen.

DER GRUND FÜR EINEN ANGRIFF SEITENS CYBERKRIMINELLEN AUF CYBERAKTEURE...

Im April 2021 stellt das auf Code-Auditing spezialisierte Unternehmen Codecov fest, dass Hacker Zugriffe auf sein Bash-Uploader-Skript erzwungen haben und dass dieses Skript wiederholt modifiziert wurde, um Malware einzuschleusen. Ein Problem, dem rund 29.000 Unternehmen, Kunden und möglicherweise alle parallel geschädigten Personen

des Angriffsangriffs gegenüberstehen wie z. B. Rapid7 ein Cybersicherheitsanbieter, dessen Quellcode für bösartige Zwecke ausgenutzt wurde. Für viele Experten ist dieser Angriff auf Codecov ein „SolarWinds-Szenario", das sich wiederholt und auch in Zukunft noch einmal auftreten kann. Cyberkriminelle haben es nämlich verstanden: **Ein Angriff auf einen Cybersicherheitsanbieter ist mit vielen Vorteilen verbunden**.

Im Grunde genommen wird ein Cybersicherheitsanbieter unabhängig von seinem Tätigkeitsbereich von Unternehmen als eine Referenz wahrgenommen, da sie ihn als unerreichbar, unangreifbar betrachten können. Dies ist ein wahrer Glücksfall für Cyberkriminelle, die ein wachsendes Interesse daran sehen, Anbieter von Cybersicherheit anzugreifen, sich in deren Lösungen einzuschleusen und gleichzeitig mehrere Kundenunternehmen zu infizieren.

Natürlich *„sind die Folgen eines Angriffs auf einen Cybersicherheitsanbieter je nach dessen Geschäft nicht gleich"*, präzisiert **Adrien Brochot**, Product Manager Endpoint Security bei Stormshield. Diese Angriffe auf die Lieferkette können viele Formen und Szenarien annehmen. In einem ersten einfachen Cyberangriffsszenario versuchen Hacker, direkten Zugriff auf die Upgrade- oder Lieferkette neuer Software zu erlangen und sich dann Zugang zu Kundeninfrastrukturen zu verschaffen. Das zweite Szenario betrifft einen Anbieter von Cloud-Cyberlösungen, der Opfer eines DDoS-Angriffs wird. Anwenderunternehmen hätten danach keinen Zugriff mehr auf ihre verschiedenen, vom Anbieter gehosteten Dienste gehabt und daher nicht mehr ordnungsgemäß funktionieren können. Im dritten Szenario könnte der Angriff auf den Anbieter einer Antivirus-Software zu einer Übernahme der Arbeitsplätze des anvisierten Unternehmens führen, wobei die Administratorrechte von Antivirus-Software genutzt werden... Ein Angriff, der somit die Infrastrukturen der Kundenunternehmen verletzlich machen würde. Der Hypothese einer Veränderung des Software-Updates hat sich am Beispiel der Firma Click Studios, die Tausende von Unternehmen mit dem Kennwortmanager Passwordstate beliefert, im vergangenen April bewahrheitet, als die Firma bei einem Update durch eine Malware infiziert wurde.

Ein Angriff auf einen Cybersicherheitsanbieter kann auch bedeuten, dass man dessen Quellcode untersucht, um sensible Kundendaten zu stehlen oder eine Zero-Day-Schwachstelle zu identifizieren, die ausgenutzt werden könnte, oder um Informationen für kommerzielle oder industrielle Spionagezwecke zu erfassen. Dies ist die gleiche Logik, die in Bezug auf Zero-Days für jeden Lösungsanbieter gilt, aber sie ist sogar noch kritischer, wenn es sich um einen Cybersicherheitsanbieter handelt. Vor allem, wenn dessen Quellcode für Cyberkriminelle einfach zu „knacken" zu sein scheint, wie das Eindringen in die Netzwerke von Microsoft, SonicWall oder auch Stormshield Ende 2020. Was Stormshield betrifft, so waren die Auswirkungen des Angriffs begrenzt, und bei den mit dem ANSSI durchgeführten Untersuchungen wurde keine Codeänderung beobachtet. Der Quellcode von Lösungsanbietern übt eine besondere Anziehungskraft aus, auch wenn die verwendeten Bibliotheken und die vorgeschlagenen Funktionalitäten oft auf Open Source basieren. Doch der böswillige Schritt hört für Cyberkriminelle, die es schaffen, Cybersicherheitsanbieter zu beeinträchtigen, noch lange nicht bei dem Quellcode auf. Wenn sie auch deren Lösungen beispielsweise durch die Einschleusung

durch eine Hintertür beeinträchtigen, können sie andere Organisationen, die Kunden des Lösungsanbieters sind, ins Visier nehmen und ihren Angriff auch weiter ausbreiten. Und dies kann dramatischen Folgen haben...

... UND AUF DEREN SICHERHEITSLÖSUNGEN

Damit eine Cybersicherheitslösung effektiv ist, muss sie genau auf die Infrastruktur des Kunden abgerichtet werden, um ein Maximum an Informationen zu erfassen. Cybersicherheitslösungen werden daher so konzipiert, dass sie möglichst nahe bei sehr empfindlichen Vermögenswerten eines Unternehmens eingesetzt werden. Ein **Angriff auf eine Cybersicherheitslösung ist daher eine Möglichkeit, direkten Zugriff auf eine große Menge an Informationen auf den mit diesen Lösungen geschützten Computern** und auf ein hohes Maß an Berechtigungen zu haben und somit die Kontrolle darüber zu übernehmen, sie zu deaktivieren und die Sicherheitsbarrieren zu knacken und anschließend unbemerkt bösartige Aktionen auf einem Informationssystem durchzuführen. Cyberkriminelle können auch Lösungen „knacken", indem sie eine bekannte Schwachstelle in der Lösung ausnutzen, die von den Unternehmen, die die Lösung einsetzen, nicht gepatcht wurde. Dies zeigt auf, wie wichtig es für Administratoren ist, ihre Sicherheitslösungen regelmäßig zu aktualisieren, und für Lösungsanbieter, Schwachstellen aufzuspüren und zu beheben. Eine bekannte Sicherheitslücke in der VPN-Lösung Pulse Connect Secure von Pulse Secure wurde kürzlich für bösartige Zwecke ausgenutzt.

Kurz gesagt, wenn es um Angriffe auf Cybersicherheitslösungen geht, ist für Cyberkriminelle alles möglich, denn sie können jede Tür nutzen, um ihre Angriffe zu verbreiten. Türen, die manchmal von den Sicherheitslösungsanbietern selbst schlecht verschlossen werden...

EINE TÜR KANN WIEDER EINE ANDERE VERBERGEN: DIE BESAGTEN HINTERTÜREN

Es handelt sich also um Hintertüren, die sich aus verschiedenen Gründen in einem Sicherheitsprodukt befinden können, wie uns **Sébastien Viou**, Cyberverkünder und Consultant bei Stormshield, in Erinnerung ruft: *„Es kann sich dabei um unbeabsichtigte Hintertüren, die bei der Produktentwicklung durch den Hersteller verwendet und zum Zeitpunkt der Veröffentlichung vergessen wurden, und um absichtliche Hintertüren handeln, die von einem Hersteller wissentlich hinterlassen werden, um in das System eines Kunden eingreifen zu können."* Eine solche Hintertür wird beispielsweise während der Entwicklung der Lösung als Debugging-Zugang verwendet und dann versehentlich in die Produktion gebracht. Umgekehrt kann sich ein Lösungsanbieter die Möglichkeit vorbehalten, im Falle eines Problems bei einem Kunden einzugreifen, indem er eine Hintertür vorhält, diese aber nicht dokumentiert. Hinzu kommen staatlich geförderte Hintertüren, die den Softwareanbietern staatlich auferlegt wurden und insbesondere durch die Edward-Snowden-Affäre und die Abhör- und Ausspähpraktiken der NSA im Jahr 2013 entdeckt wurden – Praktiken, die im Zuge der Aufdeckungen in Zusammenhang

mit der Operation Dunhammer heute erneut auf der Tagesordnung stehen. Zum Zeitpunkt der Snowden-Affäre war der prominenteste Fall zum Hintertür-Thema der Anbieter Juniper Netzwerke, dessen Lösungen teilweise von der NSA installierte Hintertüren enthielten, die den Zugriff auf die Daten der Anbieterkunden ermöglichten.

„Eine Backdoor ist eine Schwachstelle in einer Lösung, die natürlich versteckt ist, aber dennoch eine Schwachstelle bietet."

Simon Dansette, Product Manager Network Security Stormshield

Unabhängig von den **Gründen für das Vorhandensein einer Hintertür in einem Sicherheitsprodukt stellt diese auf jeden Fall ein Risiko dar, wenn sie in die Hände eines böswilligen Akteurs fällt**. *„Eine Backdoor stellt ein zusätzliches Risiko dar, da sie es ermöglicht, unsichtbar in eine Lösung einzubrechen*", sagt **Simon Dansette**, Product Manager Network Security bei Stormshield. *„Wenn ein Hacker erkennt, dass eine Hintertür in der Lösung vorhanden ist, kann er diese ausnutzen, um die Lösung für böswillige Zwecke zu knacken. Mit anderen Worten, eine Backdoor ist eine Schwachstelle in einer Lösung, die zwar versteckt ist, aber dennoch eine Schwachstelle bietet.*" Wie die ANSSI im Jahr 2016 in einer unterzeichnet von Guillaume Poupard unterzeichneten Notiz erinnerte, habe eine Hintertür in einem Verschlüsselungssystem *„den verhängnisvollen Effekt, den Entwicklern von Sicherheitsprodukten und -diensten eine Schwächung der kryptographischen Mechanismen aufzuerlegen.*" Ein Risiko folglich, dass sich vermeiden lässt.

BEWUSSTSEINSBILDUNG, SICHERHEIT, VERTRAUEN: DER NOTWENDIGE GEGENANGRIFF DER SICHERHEITSLÖSUNGSANBIETER

„Seit einigen Monaten zeigt sich ein deutlicher und erwiesener Trend, Anbieter von Cybersicherheitslösungen anzugreifen. Die Frage, die wir uns jetzt stellen müssen, lautet, wann diese Art von Angriffen stattfinden wird und wie sich die Lösungsanbieter dagegen schützen werden", warnt Sébastien Viou. Tatsächlich müssen sich Anbieter von Sicherheitslösungen mehr denn je darüber bewusst sein, dass sie ins Visier von Cyberkriminellen geraten können, und ihre Verteidigungshaltung entsprechend anpassen.

„Die Frage, die wir uns jetzt stellen müssen, lautet, wann diese Art von Angriffen stattfinden wird und wie sich die Lösungsanbieter dagegen schützen werden."

Sébastien Viou, Cyberverkünder und Consultant bei Stormshield

Die Sensibilisierung von Einzelpersonen – ob Mitarbeiter eines Lösungsanbieters oder die Lösung einsetzende Endkunden – scheint ein nicht zu unterschätzender Schritt zu sein. *„Einige Angriffe auf die Lieferkette erfolgen über den Faktor Anwender*", erinnert Adrien Brochot. Anbieter sollten ihren Kunden weiterhin empfehlen, die IT-Sicherheitsrichtlinien

nach den notwendigen Best Practices zu gestalten, insbesondere die systematische Aktualisierung ihrer Lösung nach der Veröffentlichung von Patches. Damit können sie ein Szenario wie das von Fortinet und seiner FortiOS-Lösung vermeiden. Ein Beispiel dafür, wie **wichtig die Sensibilisierung für die Cyberverwundbarkeit nach wie vor ist**.

„Auf der technischen Seite sollte man (vor allem) die intrinsische Sicherheit des Produkts nicht vergessen, und zwar mit einer Überwachung der Schwachstellen der integrierten Komponenten seitens des Anbieters, mit einer Härtung der Lösung oder auch einer Beachtung der Prinzipien der defensiven Programmierung… Einige allgemeine Produktsicherheitsprinzipien müssen befolgt werden wie z. B. der Einsatz sicherer Architekturen unter Anwendung des Prinzips der niedrigsten Berechtigung. Die goldene Regel dabei lautet: Entwickeln Sie Ihre Lösung richtig, um den Zugang für einen Angreifer zu begrenzen“, führt Adrien Brochot weiter aus.

Dieser Ansatz betrifft auch Kundenunternehmen, die auf ihrer Ebene handeln können, indem sie verlässliche Update-Prozesse für die von ihnen verwendeten Produkte strukturieren. Ein zusätzlicher Ansatz besteht in der Bevorzugung einer Pluralität bei der Auswahl von Sicherheitslösungen (und damit Vermeidung von Einheitlichkeit); diesen Ansatz sollte man verfolgen, um einerseits die Bedrohung besser abzudecken und andererseits die Folgen der Beeinträchtigung eines Sicherheitslösungsanbieters zu begrenzen. Kunden müssen außerdem die für sie „richtige“ Lösung, die sie in ihren Systemen anwenden wollen, auf kritische Weise wählen. Eine Wahl, die schwierig sein kann, weil sie zwischen zwei Optionen schwankt: der Robustheit einer Lösung einerseits oder ihrem Funktionskatalog andererseits.

ROBUSTHEIT VERSUS FUNKTIONEN: WOFÜR SOLLTE MAN SICH ENTSCHEIDEN?

„Die Digitalisierung treibt den Bedarf u. a. im Hinblick auf Funktionsvielfalt, Datenfluss und Leistung voran... Unternehmen neigen oft dazu, sich zuerst auf die Funktionsvielfalt zu konzentrieren, wobei man bedenken muss, dass die Robustheit ebenfalls zu den Vorzügen einer Lösung gehört“, bemerkt Simon Dansette. In der Tat sind sich viele Unternehmen des Themas Produktsicherheit wenig oder gar nicht bewusst und werden natürlich ein Gerät bevorzugen, das einen Katalog von Funktionen bietet, die man eigentlich gar nicht benötigt. **Ein Sicherheitsprodukt muss jedoch in erster Linie eine Sicherheitsfunktion bleiben**: Es muss korrekt das tun, wofür es konzipiert wurde. Außerdem führt die Funktionsvielfalt eine zusätzliche Komplexität ein, was automatisch mit mehr Risiken für Schwachstellen und infolgedessen mehr Angriffsfläche bedeutet. Für Adrien Brochot ist es notwendig, *„eine Lösung zu wählen, die den Herausforderungen, die sich das Unternehmen gestellt hat, gerecht wird und gleichzeitig robust ist*“. *„Es ist notwendig, das richtige Gleichgewicht zwischen Robustheit und der Funktionsvielfalt zu finden, doch Robustheit muss dabei immer an erster Stelle stehen.*“

Anbieter von Sicherheitslösungen müssen eine ganze Dynamik von Techniken und Prozessen vollständig integrieren, um die Integrität ihrer Produkte zu gewährleisten. Gleichzeitig muss bei den Anwendern dieser Produkte eine Kette des Vertrauens aufgebaut werden.

DIE BEDEUTUNG EINER VERTRAUENSKETTE

Wie können wir also einem Anbieter und seiner Sicherheitslösung vertrauen, wenn die Informatikangriffe, auf die es Hacker absehen, stark zunehmen? Eine berechtigte Frage, die sich Unternehmen stellen und auf die Sicherheitslösungsanbieter handfeste Antworten geben können. Obwohl es unmöglich ist, ein Sicherheitsprodukt ohne Fehler zu garantieren, gibt es mehrere Möglichkeiten, die Sicherheit von Lösungsanbietern und ihrer Produkte einer Prüfung zu unterwerfen.

Zunächst einmal gibt es den unparteiischen Dritten, der **in der Kette des Vertrauens eine wichtige Rolle spielt**. *„Der Einsatz einer vertrauenswürdigen dritten Partei ist für einen Sicherheitslösungsanbieter notwendig. Dadurch können wir einen Blick von außen auf das Produkt und seinen Code werfen. Die Tatsache, dass dieses von einem unparteiischen Dritten durchgeführt wird, ist eine zusätzliche Garantie für Seriosität"*, erklärt Simon Dansette. Anbieter von Cybersicherheitslösungen sollten wirklich ein Interesse daran haben, ihre Produkte von Drittanbietern prüfen zu lassen: Code-Reviews, Pentests und Bug-Bounties sind alles gute Möglichkeiten, um mögliche Fehler zu entdecken und eine Lösung zu testen.

Es ist auch wichtig, **Lösungen anzubieten, die von europäischen Referenzorganisationen qualifiziert sind**, wie z. B. der ANSSI für Frankreich, dem BSI für Deutschland oder dem CCN für Spanien. Diese Qualifikationen garantieren, dass die Sicherheitsvorgaben, die z. B. von der ANSSI validiert wurden, vorrangig den Bedürfnissen der Endkunden entsprechen: ein unbestreitbarer Vertrauensbeweis. Außerdem basieren diese Qualifizierungen oft auf einer Bewertung der Entwicklungsumgebung, was ein Plus bei der Prüfung der Robustheit der Produkte darstellt. Schließlich ist die Transparenz des Lösungsanbieters in Bezug auf die in seinen Produkten vorhandenen Sicherheitsmängel von entscheidender Bedeutung, ebenso wie die Tatsache, dass er die Feedbacks seiner Kunden berücksichtigt, was für die Optimierung einer Lösung unerlässlich ist, oder dass er regelmäßig korrigierende Versionen von Produkten bereitstellt.

Trotz eines anhaltenden Trends haben Lösungsanbieter mit pädagogisch, technisch und fachlich noch nicht das letzte Wort gesprochen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**

Version 1.1 - Copyright Stormshield 2022