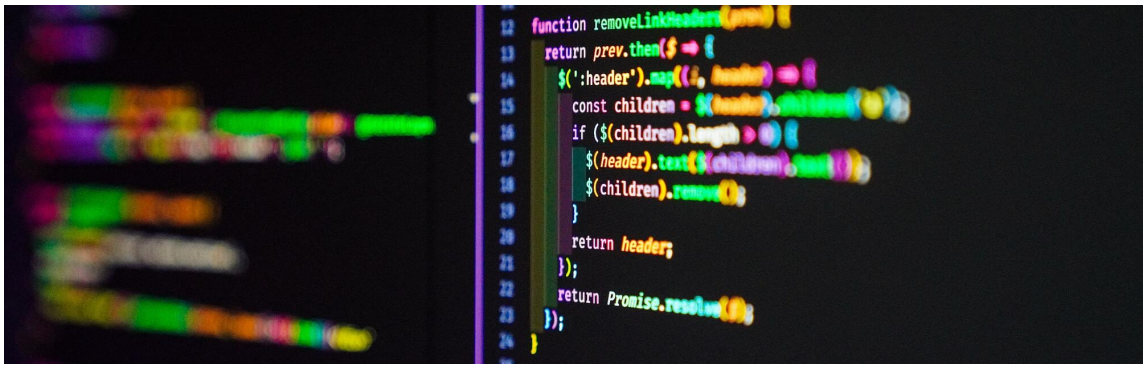
spektrum.de

SolarWinds-Hack: Ein Hackerangriff, der um die Welt geht

Eike Kühl

13-16 Minuten

Der Angriff auf das Unternehmen SolarWinds gilt als größter Hack seit Jahren. Zehntausende Firmen könnten betroffen sein. Um was geht es, wie gefährlich ist es und wie kann man sich schützen? Antworten auf die wichtigsten Fragen.



Es begann, als die Hacker selbst gehackt wurden. Am 9. Dezember 2020 bemerkten Experten der IT-Sicherheitsfirma FireEye, dass sie Opfer eines Cyberangriffs wurden. Jemand hatte sich Zugriff zu ihren Systemen verschafft und Software gestohlen, die FireEye eigentlich dazu verwendet, um die Abwehrsysteme seiner Kunden zu testen.

Wenige Tage später wurde bekannt, dass Abteilungen der US-Regierung ebenfalls gehackt wurden, darunter das Finanz- und Handelsministerium. Schnell war klar: Die Fälle hängen zusammen. Alle Opfer nutzten die Softwareplattform Orion des

Unternehmens SolarWinds. Über ein kompromittiertes Update konnten die Angreifer eine Hintertür, »Sunburst« getauft, in die Systeme und Netzwerke der Nutzerinnen und Nutzer einschleusen.

Langsam wird das Ausmaß des Cyberangriffs deutlich. Manche Experten sprechen von einem historischen Ereignis, vom Beginn einer neuen Cyberspionage-Ära und von einem der größten Hackerangriffe seit Jahrzehnten. Sind die Superlative gerechtfertigt? Wieso ist der SolarWinds-Hack so gefährlich? Um welche Schwachstelle handelt es sich und sind vielleicht auch deutsche Firmen und Forschungsinstitute betroffen? All diese Fragen beantworten wir in dieser FAQ.

Zurück zum Inhaltsverzeichnis

Was ist das Unternehmen SolarWinds?

SolarWinds ist ein börsennotiertes, US-amerikanisches Unternehmen mit Sitz in Austin, Texas. Es bietet als Dienstleister Softwarelösungen für das IT- und Netzwerkmanagement an. Kunden können etwa Datenflüsse verfolgen und optimieren, Datenbanken verwalten und Systeme verwalten. Weltweit zählt SolarWinds mehr als 300 000 Kunden und wie die »New York Times« berichtet, nutzen fast alle Fortune-500-Unternehmen in den USA Produkte von SolarWinds.

Zurück zum Inhaltsverzeichnis

Welche Netzwerke sind betroffen und seit wann ist das bekannt?

Laut SolarWinds gibt es etwa 33 000 Kunden der Plattform Orion. Von diesen hätten »weniger als 18 000« das besagte

Update im Zeitraum zwischen März und Juni 2020 installiert. Das bedeutet, die »Sunburst«-Hintertür war mindestens seit Frühjahr aktiv. Erste Anzeichen auf einen Angriff von außen konnte SolarWinds bereits im September 2019 identifizieren. In Hackerkreisen sei bereits 2017 über Schwachstellen im System von SolarWinds diskutiert worden, schreibt die Nachrichtenagentur Reuters. Die Hacker hatten also womöglich lange Zugriff auf die Systeme von SolarWinds, bevor sie ertappt wurden.

Die Liste der Betroffenen wächst täglich. Mittlerweile umfasst sie allein mehr als ein Dutzend US-Behörden. Das Heimatschutzministerium ist ebenso betroffen wie die amerikanische Telekommunikationsbehörde NTIA und die Nationale Verwaltung für Nukleare Sicherheit (NNSA). Softwareentwickler wie Microsoft und VMware gehören zu den Opfern, ebenso der Finanzdienstleister Equifax, die Wirtschaftsprüfer von Deloitte sowie die Tech-Firmen Nvidia, Belkin, Intel und Cisco. Vor allem in den USA, wo SolarWinds die meisten Kunden hat, wurden prominente Unternehmen angegriffen.

Zurück zum Inhaltsverzeichnis

Was genau ist die Schwachstelle?

Den Hackern gelang es, den Build-Prozess von SolarWinds zu infiltrieren. Das ist der Punkt in der Softwareentwicklung, an dem aus dem Quellcode ein ausführbares Programm wird. Hier wurde der »Sunburst«-Trojaner in ein Update für die Orion-Plattform eingeschleust. Damit alles echt wirkte und unerkannt blieb, haben die Angreifer die Dateien mit einem gültigen kryptografischen Schlüssel von SolarWinds unterzeichnet. Wer

anschließend das Update installierte, fing sich den Trojaner ein. Nach einer Ruhezeit von zwei Wochen, fing der Trojaner an, sich mit dem Command-and-control-Server der Angreifer im Internet zu verbinden. Diese konnten ihm dann befehlen, Daten auszulesen, das Netzwerk zu analysieren oder einen weiteren Schadcode zu laden.

> »Das waren sicherlich keine Anfänger, sondern professionelle Hacker«
> (Rüdiger Trost, Experte des IT-Sicherheitsunternehmens F-Secure)

»Das waren sicherlich keine Anfänger«, sagt Rüdiger Trost, Experte des IT-Sicherheitsunternehmens F-Secure, »sondern professionelle Hacker, die über Ressourcen und Wissen verfügen.« Und »Sunburst« könnte nicht die einzige Schwachstelle in Orion gewesen sein. So gibt es inzwischen Hinweise auf eine zweite Hintertür, deren Ursprung noch nicht geklärt ist.

Zurück zum Inhaltsverzeichnis

Wie ließe sich die Hintertür zuschließen?

SolarWinds hat die Sicherheitslücken in Orion nach Bekanntwerden schnell schlossen. Das schützt aber nur vor weiteren Zugriffen auf diesem Weg. Es sei denkbar, dass die Angreifer bereits weitere Schadsoftware eingeschleust haben und es somit noch andere Hintertüren gibt, sagt IT-Sicherheitsexperte Rüdiger Trost: »Es bringt nichts, die Tür abzuschließen, wenn schon fünf Fenster offen stehen.« Man könne jedem SolarWinds-Kunden deshalb nur raten, die Schutzmaßnahmen zu verstärken und genau zu überprüfen, was in dem Netzwerk überhaupt passiert. »Ich muss genau

schauen: Welche Prozesse laufen, welche Verbindungen bestehen, wer hat worauf Zugriff?«, sagt Trost.

Noch drastischer formuliert es Hartmut Pohl, IT-Experte und Geschäftsführer der Firma softScheck: »Eigentlich muss man sofort alle betroffenen Systeme abschalten. Das klingt überzogen, aber unter dem Aspekt, dass die Angreifer Ihnen die ganze IT stilllegen können, muss man das riskieren.« Entscheidend seien die unbekannten Sicherheitslücken, die es noch im System geben könne. »Sonst lebt Ihr Unternehmen mit einer Hintertür, über die Angreifer jederzeit reinkommen«, sagt Pohl.

Zurück zum Inhaltsverzeichnis

Warum sind die Angriffe bedenklich?

Zum einen handelt es sich um einen Angriff auf die Lieferkette (»Supply Chain«). Statt direkt die Server eines einzelnen Ziels anzugreifen, suchen die Angreifer eine Hintertür in der Software von Dritten. Gelingt das, können in kurzer Zeit eine Vielzahl von Zielen infiltrieren. »Die Analogie wäre, bei einem Hersteller von Türschlössern einzubrechen und nicht nur einen Schlüssel zu kopieren, sondern sich gleich den Generalschlüssel zu besorgen«, sagt Trost. Das Perfide: Solche Angriffe seien nur schwer zu erkennen, weil sich der Schadcode in Software versteckt, der man als Unternehmen eigentlich vertraut. »Mit einer gewöhnlichen Firewall oder Antiviren-Software kann man als Systemadministrator wenig ausrichten, solange die Lücke unentdeckt ist.«

Zum anderen ist Orion eine Software, die von Haus aus über weit reichende Rechte verfügt. »Orion ist dazu da, um die Systeme der Kunden zu verwalten und zu analysieren«, sagt

Sven Herpig, Leiter für Internationale Cybersicherheitspolitik bei der Stiftung »Neue Verantwortung«: »Wenn Angreifer dort Zugriff haben, kommen sie schnell in das ganze Netzwerk hinein und müssen sich nicht erst noch sehr viel lateral bewegen.« Soll heißen: Die Hacker könnten vergleichsweise schnell viel Schaden anrichten und sich tief einnisten.

Zurück zum Inhaltsverzeichnis

Was bedeutet das für die Nutzerinnen und Nutzer?

Schlimmstenfalls, dass alle Daten ihres Systems in den vergangenen Monaten bereits kopiert wurden. Das können E-Mails und Adressbücher sein, aber auch Passwörter und vertrauliche Dokumente, Datenbanken, Forschungsergebnisse, Baupläne und Firmengeheimnisse. In der Industrie und Forschung könnten Maschinen, Computer und Laborinstrumente manipuliert und sabotiert werden, kritische Infrastruktur stillgelegt werden. Vieles ist denkbar, wenig bekannt.

»Wenn die manipulierte Software erst einmal mit erweiterten Administratorrechten läuft, können Angreifer nahezu alles machen«, sagt Rüdiger Trost. Sie könnten sich einen genauen Plan des Netzwerks machen und über Monate hinweg Informationen sammeln, um schließlich gezielt zuzuschlagen. »Ich fürchte, dass wir noch am Anfang stehen und erst in den kommenden Monaten sehen werden, wer denn wirklich zu den Opfern zählt«, so der Experte.

Zurück zum Inhaltsverzeichnis

Welche Daten wurden gestohlen oder verändert?

Bei fast allen Opfern laufen noch Untersuchungen. Während bei

FireEye spezielle Hacking-Software gestohlen wurde, berichtet Microsoft, dass sich unbekannte Angreifer Einblicke in den Quellcode von Produkten verschafft hatten; was aber wohl nicht allzu schlimm sei. Anders als bei anderen Hacks, gab es bislang keine bekannten Lösegeldforderungen von Seiten der Angreifer. Offenbar geht es den Tätern nicht darum, das schnelle Geld zu machen.

> »Wer auf einmal viele Daten stiehlt oder Sabotage betreibt, wird schneller entdeckt«
> (Sven Herpig, Experte für Cybersicherheitspolitik)

Das sei nicht ungewöhnlich, sagt Herpig: »Bei bis zu 18 000 Zielen ist es letztlich eine Frage der Kapazität: Die Angreifer müssen sich selbst erst einmal einen Überblick verschaffen, in welchen Systemen sie drin sind und was es da zu holen gibt.« Zudem haben sie ein Interesse daran, möglichst lange unentdeckt zu bleiben. »Wer auf einmal viele Daten stiehlt oder Sabotage betreibt, wird schneller entdeckt. Und dann fliegt die ganze Operation auf.«

Zurück zum Inhaltsverzeichnis

Sind auch deutsche Firmen und Behörden betroffen?

Möglicherweise. Der FDP-Bundestagsabgeordnete Manuel Höferlin hatte im Dezember eine schriftliche Anfrage an die Bundesregierung gestellt, ob SolarWinds-Produkte auch auf Bundesebene eingesetzt wurde. Die Antwort: Allein 16 Bundesbehörden und Ministerien gehören zu den Kunden, darunter das Bundeskriminalamt, das Kraftfahrt-Bundesamt, die Physikalisch-Technische Bundesanstalt, das Robert Koch-Institut und der zentrale IT-Dienstleister des Bundes, ITZ Bund. Allerdings haben nicht alle die unsichere Orion-Software

eingesetzt. Die Bundesregierung hat auf Höferlins Anfrage geantwortet, es habe keine unberechtigten Zugriffe auf Systeme der Bundesverwaltung gegeben. Der Direktor des ITZ Bund sagte gegenüber dem »Spiegel«, seine Stelle habe lediglich eine unkritische Version einer Server-Software von SolarWinds eingesetzt und sei somit nicht betroffen.

Für Sven Herpig ist das noch kein Grund zur Entwarnung. »Es gibt kein Zentralregister, wo alle Software und Hardware aufgelistet wird, die in der Bundesverwaltung eingesetzt wird.« Vor allem wenn ein Teil der IT an einen Dienstleister outgesourct wurde, sei es nicht immer sofort ersichtlich, welche Software dieser genau verwendet und mit dem System verbunden hat. Auch Hartmut Pohl bezweifelt, dass es für alle deutschen Kunden so glimpflich ausging. »Softwareaktualisierungen werden in der Regel automatisch aufgespielt, und es scheint mir unwahrscheinlich, dass das schädliche Update über Monate hinweg nicht heruntergeladen wurde.« Pohl vermutet, dass unter den insgesamt 33 000 Kunden von Orion und 300 000 Kunden von SolarWinds noch viel mehr deutsche und europäische Nutzer sind als bislang angenommen. Aus Angst vor einem Imageschaden könnten viele bislang schweigen.

> »Was den Umfang und das Vorgehen angeht, deutet vieles auf einen staatlichen Akteur hin«
> (Sven Herpig, Experte für Cybersicherheitspolitik)

Zurück zum Inhaltsverzeichnis

Wer steckt dahinter?

Glaubt man den amerikanischen Behörden, führen die Spuren nach Russland. Das stützen jüngste Untersuchungen des

Sicherheitsunternehmens Kaspersky. Deren Forscher fanden im »Sunburst«-Trojaner Spuren, die Ähnlichkeiten zu einer früheren Schadsoftware der russischen Hackergruppe Turla aufweist. Turla ist für raffinierte Spionageaktionen bekannt und wird mutmaßlich vom russischen Geheimdienst FSB unterstützt. »Man findet oftmals Codeschnipsel, die schon zuvor in anderen Hintertüren aufgetaucht sind«, sagt Rüdiger Trost von F-Secure. Das allein sei aber noch kein Beweis; Hacker kopieren häufig von anderen Gruppen oder legen bewusst falsche Fährten. Auch Kaspersky will keine abschließende Bewertung abgeben.

»Was den Umfang und das Vorgehen angeht, deutet vieles auf einen staatlichen Akteur hin. Und es ist nicht so, als würden alle russische Gruppen auf Zehenspitzen gehen«, sagt Sven Herpig. Denn während man von chinesischen oder US-amerikanischen Cyberangriffen zuletzt wenig gehört habe, seien vor allem russische Hacker immer wieder mit spektakulären Aktionen aufgefallen – man denke an den Angriff auf den deutschen Bundestag oder auf die Computer der US-Demokraten. Wer auch immer dahintersteckt, eines ist für alle Experten klar: Der SolarWinds-Hack ist vom Ausmaß her einer der größten Cyberangriffe der vergangenen Jahre. Und der genaue Schaden muss sich erst noch zeigen.