SolarWinds-Hack: Eine neue Angriffs-Dimension

Unternehmen: indevis.de

Bis Ende letzten Jahres war SolarWinds wenigen Menschen ein Begriff. Doch mittlerweile ist der Name der US-amerikanischen Firma auch in der breiten Masse angekommen – anders allerdings, als sich dies Unternehmen vorgestellt haben dürften. Denn der Name SolarWinds wird seit Dezember 2020 mit dem bisher größten Cyberangriff der US-Geschichte in Verbindung gebracht. Die Firma ist auf Netzmanagement-Software spezialisiert und bedient Unternehmen und Behörden auch mit Programmen, die beim Überwachen der IT-Infrastruktur unterstützen. Für indevis-Kunden kann Entwarnung gegeben werden: indevis nutzt keine Software des Herstellers Solarwinds.

Endpoint Management Software als Einfallstor für Hacker

Ende letzten Jahres wurde bekannt, dass SolarWinds Opfer von Hackern geworden ist und die Software, die Kunden eigentlich vor Angriffen schützen sollte, das Einfallstor für Datenspionage im großen Stil war. Die Hacker haben ihre Schadsoftware zwischen März und Juni 2020 in ein Update der Orion Plattform von SolarWinds eingeschleust, eine Endpoint Management Software, mit der das gesamte IT-Stack von Unternehmen überwacht, analysiert und verwaltet werden kann.

Haben SolarWinds-Kunden das Update heruntergeladen, wurde den Hackern die Tür geöffnet. Die Malerware mit Namen Sunburst konnte sich so durch die Überwachungs- und Verwaltungsplattform von SolarWinds lange unbemerkt verbreiten, dauerhaft in Unternehmensnetzwerken einnisten und über eine Backdoor mit den Angreifern kommunizieren. So hat Sunburst auch unbemerkt Einzug in zahlreiche Regierungsorganisationen, Behörden und Großunternehmen gehalten.

Nahezu unsichtbar war der Schadcode für die infiltrierten Unternehmen, weshalb er lange unentdeckt blieb. Mittlerweile haben Forscher mit „Supernova" eine zweite Backdoor entdeckt. Dabei scheint es sich um zwei voneinander unabhängige Trojaner unterschiedlicher Angreifergruppen zu handeln.

Cyber-Angriffe haben eine neue Ebene erreicht

„Wir haben eine neue Qualität der Angriffe erreicht", sagt Wolfgang Kurz, CEO von indevis. „Der Angriff übersteigt das Ausmaß dessen, was man sich noch vor Kurzem vorstellen konnte um einiges. Hacker führen einen zweistufigen Angriff über eine Third Party aus, um das eigentliche Ziel anzugreifen."

Im Falle von SolarWinds handelt es sich bei der Third Party sogar um eine Firma im IT-Bereich, die auch Sicherheitsprodukte anbietet. Durch die Verteilung des Schadcodes über die Software von SolarWinds konnten auf einen Schlag mehrere tausend Unternehmen infiltriert werden.

Besorgniserreichend ist nicht nur die Größenordnung des Angriffs, sondern auch, dass sich der Schadcode aufgrund der Kundenstruktur von SolarWinds in stark gemanagten Umgebungen und kritischen Infrastrukturen ausbreiten konnte.

Neben Behörden und Ministerien hat der Angriff auch vor Tech-Giganten wie Microsoft nicht Halt gemacht, dessen Produktionssysteme betroffen waren, wodurch die Hacker den Source-Code einsehen konnten. Laut Microsoft sei dieser Umstand zwar nicht mit einem erhöhten Risiko verbunden. Es zeigt sich dennoch, dass Angreifer ambitionierte Ziele verfolgen und sehr tief in interne Netzwerke eindringen können. Auch Wolfgang Kurz zeigt sich alarmiert über den SolarWinds-Hack, der „die Vorstufe zum ersten großen Cloud-Hack sein könnte".

SolarWinds-Hack: Auf der Suche nach dem Schuldigen

Angreifer gehen mittlerweile die Extrameile und hacken sich in das Code Repository eines Herstellers. Deshalb sind Softwarehersteller angehalten, noch aufmerksamer zu sein. Ein besserer Schutz und ausgeklügeltere Sicherheitsvorkehrungen hätten vermutlich auch im Fall von SolarWinds verhindern können, dass der eigene Code verändert wird und dies so lange unbemerkt bleibt: durch den Einsatz einer strukturierten Deployment Chain mit Unit-Tests, automatischer Codeanalyse sowie einer strengeren Prüfung der Updateversionen.

Doch SolarWinds muss sich aktuell noch andere Anschuldigungen gefallen lassen. Denn Berichten zufolge wurde das Unternehmen bereits 2019 auf das Datenleck hingewiesen. Außerdem stand nicht nur das Passwort für die Übernahme des manipulierten Update-Servers bei SolarWinds in öffentlich zugänglichen Dokumentationen. Es lautete „solarwinds123" und war damit zudem alles andere als sicher.

Während auch Wolfgang Kurz der Meinung ist, dass SolarWinds hier nicht aus der Pflicht genommen werden kann, könne man den Kunden von SolarWinds wiederum kaum einen Vorwurf machen. Denn diese haben die Software wohl nach bestem Wissen und Gewissen eingesetzt und sich für einen börsennotierten amerikanischen Softwarehersteller entschieden, der durchaus ein gewisses Standing hat.

Von Hack betroffen – was tun?

Vom SolarWinds-Hack sind rund 18.000 Unternehmen betroffen, die das schadhafte Update erhalten haben. Dies allein bedeutet allerdings noch nicht, dass ein Unternehmen tatsächlich kompromittiert wurde. Die verantwortlichen Angreifer hatten nicht die Möglichkeit, zu beeinflussen oder zu kontrollieren, welche Unternehmen das Update erhalten. Es ist davon auszugehen, dass nicht bei allen Unternehmen, die den Schadcode erhalten haben, auch tatsächlich Schaden angerichtet wurde. Zumal sich die Hacker angesichts der hohen Anzahl der betroffenen Unternehmen wohl auf die für sie besonders interessanten Ziele konzentrieren mussten. Dennoch ist Vorsicht geboten.

Unternehmen, die vom SolarWinds-Hack betroffen sind, sollten ihre Systeme isoliert untersuchen. Bei einem konsequenten Vorgehen müsste die Software neu installiert und nicht nur gepatched und geupdatet werden. Der Aufwand hierfür ist allerdings sehr groß. SolarWinds hat mittlerweile Hotfixes veröffentlicht, mit denen die kompromittierten Elemente entfernt werden sollen. Diese lösen allerdings nur die Schwachstellen, können aber den Schaden, der bereits angerichtet wurde, nicht wiedergutmachen.

Unternehmen, die mit einem externen Sicherheitsdienstleister zusammenarbeiten, sollten sich mit diesem in Verbindung setzen, um das für sie beste Vorgehen zu besprechen.

Quellen & Ressourcen:
https://indevis.de/herstellerloesungen/vectra-network-detection-response
https://indevis.de/herstellerloesungen/palo-alto-networks-cortex
https://www.solarwinds.com/securityadvisory
https://www.computerbild.de/artikel/cb-News-Sicherheit-solarwinds-fireeye-29415771.html
https://www.heise.de/news/Cyberangriffe-via-SolarWinds-Software-neue-Entwicklungen-im-Ueberblick-4991255.html
https://www.heise.de/news/SolarWinds-Zweite-unabhaengige-Backdoor-Malware-fuer-Orion-Plattform-entdeckt-4996505.html
https://www.solarwinds.com/securityadvisory
https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/
https://t3n.de/news/solarwinds-hack-microsoft-source-code-1347660/
Bildquelle: Thaut Images - stock.adobe.com