2021/01 Ausland

https://shop.jungle.world/artikel/2021/01/durch-die-hintertuer

Mutmaßlich russischen Hackern gelang ein Angriff auf eine wichtige Softwarefirma

Durch die Hintertür

Von **Boris Mayer Elke Wittich**

Mangelnde Sicherheitsmaßnahmen einer Softwarefirma erleichterten einen Cyberangriff mutmaßlich russischer Geheimdiensthacker. Betroffen sind zahlreiche Behörden und Unternehmen.

Es wird Monate dauern, bis das ganze Ausmaß des Angriffs mutmaßlich russischer Geheimdiensthackergruppen, die als »Fancy Bear« und »Cozy Bear« bekannt sind, auf das Unternehmen Solarwinds analysiert ist. Betroffen ist eine noch unbekannte Anzahl von Regierungsstellen, die Software von Solarwinds nutzen. Nach eigenen Angaben hat das Unternehmen weltweit 33 000 Kunden für seine Plattform Orion, von denen 18 000 die betroffenen Versionen verwendeten. Unter den Kunden sind die Nato, diverse US-Behörden und fast alle der Unternehmen, die das US-Wirtschaftsmagazin *Fortune* zu den 500 umsatzstärksten der Welt rechnet. In Deutschland sind dem *Handelsblatt* zufolge die Telekom, Siemens und die Stadtsparkasse Hagen Kunden von Solarwinds.

Die in Sicherheitsumgebungen üblichen Verteidigungsmaßnahmen wurden bei dem Angriff geschickt umgangen. Bisherige Attacken hatten entweder ein bestimmtes Unternehmen, eine Behörde oder eine Regierung zum Ziel, um genau dort Daten zu stehlen, oder sie hatten es auf jedes einzelne Informationssystem eines bestimmten Typs abgesehen – dazu gehören neben Computern oder Handys auch Infrastrukturgeräte wie Router oder Modems. Breitgestreute Angriffe sind einfacher, weil es eine große Zahl von Geräten mit veralteter Software gibt. Bei den wirklich interessanten Zielen hingegen schließen Administratoren und Spezialisten für IT-Sicherheit eben solche Angriffswege regelmäßig. Selbst wenn bei einem Massenangriff ein wertvolleres Ziel infiltriert werden kann, ist es sehr aufwendig, unter den Millionen erfolgreich übernommenen Systemen einen Glückstreffer zu identifizieren, sofern er überhaupt vorhanden ist.

> Solarwinds forderte seine Kunden auf, die Software des Unternehmens von der Überwachung durch andere Sicherheitsprogramme auszuschließen, weil das die Funktionalität gefährden würde.

Doch »Operation Sunburst« war ein Massenangriff gegen Organisationen ab einer gewissen Größe. Den Hackern war es gelungen, ihren Programmcode in die Orion-Plattform einzuschleusen, die die Grundlage für die von Solarwinds angebotene Spezialsoftware ist, die Server, das sie verbindende Netzwerk und alles, was sonst noch dazu gehört, zu überwachen und konfigurieren hilft. Eine solche Software braucht weitreichende Zugriffsrechte auf die zu überwachenden Systeme und bekommt diese Rechte auch zugeteilt, schließlich ist sie mit dem elektronischem Zertifikat von Solarwinds ausgestattet und gilt daher als unbedenklich. Jährliche Lizenzen für einzelne Softwarepakete sind bei Solarwinds erst ab mehreren Tausend US-Dollar zu haben.

Wenn Firmen oder Behörden aus sicherheitskritischen Bereichen Software programmieren lassen, wird oft in einem aufwendigen Prozess jede einzelne Zeile Quellcode einem *security screening* unterzogen. Diese Überprüfung wird nie von dem implementierenden Software-Entwickler vorgenommen. Damit ist es für eine einzelne Person praktisch unmöglich, Schadcode direkt einzuschleusen.

Doch auch Firmen mit hohem Sicherheitsbedürfnis verwenden Software von Drittherstellern. Ob es sich dabei um in den eigenen Programmierprojekten verwendete Bibliotheken handelt oder um eine völlig eigenständige Software, die in den Rechenzentren läuft, ist egal, so sie denn die Möglichkeiten bietet, mit den eingeschmuggelten Programmzeilen den Hackern die nötigen Zugriffsrechte zu beschaffen. Eine solche indirekte Attacke wird in der Welt der IT-Sicherheit *supply chain attack* genannt – ein Angriff über die Lieferkette.

Bei der Plattform von Solarwinds waren auf jeden Fall mehr als genug für Hacker zu nutzende Zugriffsrechte vorhanden. Zudem wurde bei Solarwinds die Sicherheit vernachlässigt, der New York Times zufolge gab es nicht einmal einen Informationssicherheitsbeauftragten. Erst jetzt wurde bekannt, dass bereits 2017 Zugriff auf die Computer von Solarwinds im Darknet angeboten wurde. 2019 machte der indische Sicherheitsexperte Vinoth Kumar Solarwinds darauf aufmerksam, dass das FTP-Password ihres Servers für die Auslieferung von Updates an die Kunden »solarwinds123« lautet – und dies im Klartext in einem Projektarchiv (*repository*) nachzulesen ist. Solarwinds forderte seine Kunden sogar auf, die Software des Unternehmens von der Überwachung durch andere Sicherheitsprogramme auszuschließen, weil das die Funktionalität gefährden würde.

Im Darknet angebotene Zugänge und ein so schwaches Passwort machen es extrem einfach, die Computer einer Firma zu übernehmen. In Unternehmen ohne Sicherheitsbeauftragten und dessen Schulungen ist es zudem nicht schwer, einen eigenen Quellcode einzuschleusen. Man muss nur einen patriotischen Programmierer finden, bei diesem als Geheimdienstler auftreten und darauf verweisen, dass man gerne eine Hintertür eingebaut hätte, weil auch der »Islamische Staat« die Software verwende. Glaubwürdig ist das in jedem Fall, da die Innenminister vieler demokratischer Länder nicht müde werden, Hintertüren für Strafverfolgungsbehörden in Kryptosoftware zu fordern – wieso nicht auch in einer Netzwerküberwachungssoftware?

Welche Lücke bei Solarwinds ausgenutzt wurde, ist eigentlich nicht wichtig. Es hätte jede sein können, das Ergebnis wäre dasselbe gewesen. Der Grund dafür, dass erst einmal keinerlei Sicherheitsmaßnahmen anschlugen, als der Schadcode aktiv wurde, ist die ausgefeilte Programmierung des Angriffscodes. Selbst das Frühwarnsystem »Einstein« der US-Sicherheitsbehörden erkannte den Angriff nicht.

Auch auf andere gängige Sicherheitsmaßnahmen war Sunburst abgestimmt. Wenn Administratoren das mit der Schadsoftware versehene Update zunächst einmal ein paar Tage oder eine Woche – was durchaus so üblich ist – in einer isolierten Testumgebung betrieben und überwachten, passierte nichts. Die Software war so geschrieben, dass sie bis zu 14 Tage lang nur passiv Informationen aufnahm, bevor sie begann, nach außen zu senden. Dann aber konnten sich die Autoren der Schadsoftware aussuchen, welche Firmen oder Behörden für einen dedizierten Angriff interessant sind. Dazu konnte Sunburst über die Rechte von Solarwinds beliebige Software laden und den überwachten Systemen im Netzwerk versichern, dass die neuen Programme bekannt seien, ihnen vertraut werden könne und ihnen Zugriff gewährt werden müsse. Sobald Sunburst aktiv war, musste das gesamte Netzwerk entsprechend als infiziert gelten. Und weil man nie sicher sein kann, wirklich alles Eingeschmuggelte gefunden zu haben, bedeutet dies, dass die Infrastruktur komplett und von Grund auf neu aufgebaut werden muss.

Die digitalen Spuren verweisen nach Angaben mit dem Fall vertrauter US-amerikanischer Software-Experten auf russische Staatshacker. Doch als Sicherheitsexperten von Microsoft das Solarwinds-Paket gründlich auseinandernahmen, stießen sie auf eine weitere Überraschung: Sie fanden Beweise für einen in die Plattform eingeschleusten weiteren Schadcode. Diesem noch unbekannten Angreifer war es allerdings noch nicht gelungen, den Code auch signieren und damit als vertrauenswürdig einstufen zu lassen.