SolarWinds-Hack Erkennung, backdoors identifizieren und Angriffe abwehren

Veröffentlicht am: 18.01.2021, 8:40
Pressemitteilung von: **softScheck GmbH // Hartmut Pohl**

Der größte Hack seit je in der digitalisierten Welt: Mindestens zwei (!) Hacker-Unternehmen haben (unabhängig voneinander) seit Mitte 2019 backdoors in Updates der SolarWinds-Netzwerksoftware eingebaut. Die Hacker-Unternehmen haben die backdoors ausgenutzt, um auch in Zukunft noch in die Information Technology (IT) und Operation Technology (OT) der 300.000 Kunden von SolarWinds einzudringen.

Offensichtlich sind die weltweit größten Unternehmen aller Branchen (Verteidigungsunternehmen, Technologieunternehmen, Banken, Consultants, Pharma/Chemie, Versorger, Telekommunikations- und Rohstoffunternehmen) in Nordamerika, Europa, Asien, im Nahen Osten und auch in Deutschland betroffen - insbesondere deren Cloud-Nutzung. Mit weiteren Angreifern und Angriffen, backdoors und covert channels wird gerechnet.

Die SolarWinds-Hacks werden von US-Behörden wie FBI u.a. als die schwerwiegendsten überhaupt gesehen und bezeichnen sie (etwas doppeldeutig?) als "Pearl Harbour des Informationszeitalters?.
Die Angriffe wurden von nicht-bekannten Hacking-Unternehmen durchgeführt, wie sie in den über 30 F&E-stärksten Nationen (ggf. verdeckt) weltweit beheimatet sein können. Technik und Aufwand gehen weit über den Hack des Deutschen Bundestags 2014 hinaus mit einem geschätzten Aufwand für Angriffsvorbereitung und Durchführung von bis zu 7 Millionen Dollar. Die Motive der Angreifer sind nicht bekannt, Terrorismus wird in den Berichten nicht erwähnt - wird aber nicht ausgeschlossen.

Empfehlung:
Die US-Behörden empfehlen, IT- und OT-Systeme inkl. der Netze schleunigst vom Internet zu trennen, stillzulegen und vor einem Wiederanlauf auf Sicherheitslücken und insbesondere backdoors zu prüfen. Die backdoors können in Daten und Programmen verborgen sein. Je nach Wert der verarbeiteten Daten und den gesteuerten Prozessen sollte auch auf covert channels geprüft werden.

Eine ausführliche Analyse des SolarWinds-Hacks finden Sie hier:
https://www.it-daily.net/it-sicherheit/cybercrime/26735-der-patch-ist-der-angriff (deutsch)
https://thekasaantimes.news/index.php/world2/europe/itemlist/user/872-profdrhartmutpohl (englisch)

Webinar:
https://www.softscheck.com/de/workshops-de/solarwinds-webinar/

Prof. Dr. Hartmut Pohl
softScheck GmbH
https://www.softscheck.com/de/
hartmut.Pohl@softScheck.com

Pressekontakt

Herr Hartmut Pohl
Geschäftsf. Gesellschafter

softScheck GmbH
Bonner Str. 108
53757 Sankt Augustin, Deutschland

Telefon: +49 2241 255 43 0
E-Mail: info@softscheck.com
Website: https://www.softscheck.com

Firmenportrait

softScheck ist seit über 10 Jahren in Europa als erfolgreicher Dienstleister im Bereich der Digital Security (Informationssicherheit) tätig. Unsere Kernkompetenzen reichen von klassischen Penetration Testing, Compliance Testing bis hin zu Security Audits von Software und IT-Infrastruktur sowie Begleitung der systematischen Entwicklung sicherer Software nach ISO-27034. Kern unseres Dienstleistungsangebotes ist ein toolgestützter, ganzheitlicher Security Testing Prozess für Soft- und Hardware, der von Anfang an den gesamten Entwicklungsprozess begleitet und bei Design, Implementierung sowie Deployment Sicherheitsaspekte prüft und analysiert. In der Designphase wird mit Hilfe von Threat Modeling die Sicherheitsarchitektur aus Angreifer-Sicht betrachtet und Bedrohungen identifiziert. Mittels Dynamic Analysis identifizieren wir halb-automatisiert und kostensparend bis dato nicht erkannte Fehler und Sicherheitslücken im Binärcode.