IT-Sicherheit in der Lieferkette

Initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik

GRS - 638

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

IT-Sicherheit in der Lieferkette

Initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik

Alexander Schug
Oliver Rest
Claudia Quester

Mai 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Förderkennzeichen 4718R01611 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMU übereinstimmen.

GRS - 638
ISBN 978-3-949088-27-8

Deskriptoren

Advanced Persistent Threats, Cybersecurity, IT-Angriffe, IT-Sicherheit, IT-Sicherheitsvorfälle, Kerntechnische Anlagen, Lieferkette, Nuclear Facilities, Schadsoftware, Supply Chain

Inhaltsverzeichnis

1 Einleitung

Im Rahmen des Vorhabens mit dem Kennzeichen 4718R01611 „Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen“ wurde mit Genehmigung des Änderungsdienstes Revision 1 vom 18.03.2020 /BAS20l01/ durch das Bundesamt für die Sicherheit der nuklearen Entsorgung die Auswertung bisheriger Erkenntnisse zu IT-Angriffen unter Einsatz der unternehmerischen Lieferketten und die Vorstellung der Implikationen für die nukleare Sicherheit und Sicherung im Hinblick auf kerntechnische Anlagen und Einrichtungen in Deutschland durch die GRS in das Vorhaben aufgenommen.

Als Grundlage der Untersuchung wird der aktuelle Stand von Wissenschaft und Technik herangezogen. Die sicherheits- und sicherungstechnische Bedeutung der gewonnenen Erkenntnisse erfolgt dabei anhand der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ /BMU13n03/, der zugehörigen IT-Lastannahmen /BMU13n04/ und der Erläuterungen für Kernkraftwerke /BMU13n05/ sowie anhand der „Sicherheitsanforderungen an Kernkraftwerke“ /BMU15n01d/, der zugehörigen Interpretationen /BMU13n01/ und des nachgeordneten Regelwerks.

Im Rahmen dieses Berichts werden aktuelle Erkenntnisse zu ausgewählten IT-Angriffen mittels Lieferketten (Supply Chain) und IT-Sicherheitsvorfällen in Zusammenhang mit der Lieferkette vorgestellt. Dabei werden neben Lieferkettenangriffen mit Bezug zu kerntechnischen Anlagen auch solche Lieferkettenangriffe betrachtet, welche keinen direkten Bezug zu kerntechnischen Anlagen haben, jedoch Erkenntnisse für Lieferkettenangriffe auf kerntechnische Anlagen und Einrichtungen ermöglichen. Der Bericht gliedert sich in folgende Inhalte:

- Beschreibung bekannter IT-Angriffe und IT-Sicherheitsvorfälle über die Lieferkette mit kerntechnischen Bezügen
- Beschreibung bekannter herausragender IT-Angriffe über die Lieferkette ohne derzeit bekannte kerntechnische Bezüge
- Kurzbeschreibung weiterer IT-Angriffe über die Lieferkette ohne derzeit bekannte kerntechnische Bezüge
- Darlegung der Bedeutungsänderung von IT-Angriffen über die Lieferkette in der IT-Sicherheit

2 Übersicht über IT-Angriffe über die Lieferkette des letzten Jahrzehnts

IT-Angriffe über die Lieferketten haben mit der Digitalisierung und Internationalisierung der Lieferketten in den letzten 10 Jahren drastisch zugenommen und mit dem NotPetya Angriff im Jahr 2017 einen weltweit beachteten Höhepunkt erreicht, durch welchen ein finanzieller Schaden von ca. 10 Mrd. Dollar verursacht wurde und von dem auch eine kerntechnische Anlage betroffen war /WIR01r17, PRV01r17/. Der bisher bekannteste Lieferkettenangriff auf kerntechnische Anlagen bzw. mit Einfluss auf diese war dabei der Angriff mit der Schadsoftware Stuxnet auf eine Urananreicherungsanlage im Iran, der 2010 bekannt wurde. Dieser zuvor nie dagewesene, auf vier bis dahin unbekannten IT-Schwachstellen aufbauende Angriff verstärkte das Bewusstsein für die Gefahren von Angriffen auf IT-Systeme kerntechnischer Anlagen weltweit /FAR11r01/. Der Lieferkettenaspekt des Angriffs mit Stuxnet trat demgegenüber in den Hintergrund. Die Anzahl von Angriffen über die Lieferkette, darunter viele mit Bezug zu kritischen Infrastrukturen und auch mehrere mit Bezug zu kerntechnischen Anlagen, nahm in den letzten zehn Jahren beständig zu und beschäftigt daher Unternehmen und Aufsichtsbehörden im In- und Ausland /CPR01r19/.

IT-Angriffe über die Lieferkette werden beispielsweise aufgrund des in kerntechnischen Anlagen als Sicherungsmaßnahme zum Schutz besonders sensibler Systeme eingesetzten „Air Gaps“, welches letztlich auf die vollständige netzwerktechnische Trennung eines oder mehrerer IT-Systeme von den übrigen IT-Systemen und dem Internet abzielt, zu einem wirkungsvollen Szenario zur Überwindung dieser sowie verschiedener weiterer anlagenspezifischer Schutzmaßnahmen. Beispielsweise gelang die Überwindung der Air Gap im Angriffspfad sowohl beim Stuxnetangriff wie auch bei einem 2016 erkannten Virenfund in einem deutschen Kernkraftwerk /VER16r01/. Im Folgenden werden verschiedene, herausstehende IT-Angriffe über die Lieferkette, sowohl solche mit als auch ohne direkten bzw. bekannten Bezug zu kerntechnischen Anlagen, dargestellt und ihre Auswirkungen erläutert.

2.1 Supply-Chain-Angriffe mit Bezug zu kerntechnischen Anlagen

Nach bisherigen Kenntnissen der GRS sind insgesamt vier IT-Angriffe über Lieferketten mit direkter Betroffenheit von kerntechnischen Anlagen in den letzten zehn Jahren bekannt geworden. Zu den betreffenden Anlagen zählen ein deutsches Kernkraftwerk, mehrere Blöcke eines ukrainischen Kernkraftwerks, verschiedene französische kerntechnische Anlagen und ein japanisches Kernkraftwerk.

2.1.1 Virenfund in einem deutschen Kernkraftwerk

Übersicht

Am 23.04.2016 meldete ein Kernkraftwerk in Deutschland im Rahmen der Meldepflicht gemäß AtSMV, dass auf mehreren IT-Systemen der Anlagensicherung Schadsoftware gefunden wurde. Bei den betroffenen IT-Systemen handelt es sich um IT-Systeme, welche im äußeren und im inneren Sicherungsbereich eingesetzt wurden. Nach bisherigen Erkenntnissen wurde die Schadsoftware bereits bei der Installation eines IT-Systems in das Kraftwerk eingebracht und verteilte sich anschließend mittels Wechseldatenträgern und Netzwerkfreigaben. Zu einer bekannten, direkten Auswirkung auf die IT-Systeme kam es dabei nicht. Das Ereignis hatte somit eine geringe sicherheitstechnische Bedeutung, jedoch eine größere sicherungstechnische Bedeutung. /VER16r01/

Beschreibung

Am 23.04.2016 führte das betroffene Kernkraftwerk, ausgelöst durch eine Weiterleitungsnachricht aufgrund eines Schadsoftwarefundes in einem weiteren deutschen Kernkraftwerk, Scans auf Schadsoftware auf schutzbedürftigen IT-Systemen durch. Auf insgesamt 9 PCs (davon 3 Ersatzsysteme) und zwei Wechseldatenträgern wurden unterschiedliche Schadsoftwarekomponenten gefunden. Die betroffenen Systeme sind im äußeren und inneren Sicherungsbereich eingesetzt und über ein autarkes, nicht nach außen verbundenes IT-Netzwerk miteinander vernetzt. Die betroffenen Ersatzsysteme waren laut Aussage des Betreibers nie mit diesem IT-Netzwerk verbunden. Infolge der Entdeckung der Schadsoftwarekomponenten wurden diese entfernt und es wurde eine forensische Analyse durchgeführt. Im Verlauf dieser Analyse konnte anhand der Metadaten der Infektionsdaten erkannt werden, dass die Schadsoftware bereits im Jahre 2010 im Rahmen der Einrichtungsphase auf einem betroffenen IT-System installiert wurde.

Es ist zu vermuten, dass die Schadsoftware durch die Installation des betroffenen IT-Systems in die Anlage eingebracht wurde. Von diesem System verbreitete sich die Schadsoftware auf die anderen betroffenen IT-Systeme und Wechseldatenträger. Welche Person oder Unternehmen für die initiale Schadinfektion verantwortlich ist, ließ sich im Rahmen der forensischen Analyse nicht mehr feststellen. /VER16r01/

Eingesetzte Schadsoftware

Insgesamt drei unterschiedliche Schadsoftwarekomponenten wurden von dem eingesetzten Virenscanner auf den betroffenen IT-Systemen gefunden, alle aus dem Jahr 2010 oder vorher stammend und auf das Betriebssystem Windows ausgelegt: „W32.Pilleuz!gen2“, „Packed.Generic.291“ und „AngryIPScanner“. „W32.Pilleuz!gen2“ ist ein auf die Betriebssysteme Windows XP, Windows Server 2003 und ältere Windowsversionen ausgelegter Trojaner[1] mit wurmartigen[2] Verbreitungsmöglichkeiten. Die Schadsoftware verbreitet sich als EXE-Datei, häufig mittels Peer-to-Peer[3] Anwendungen, manipulierten Chatnachrichten und Emailanhängen. Infiziert die Schadsoftware ein System, versucht sie dort Informationen zu sammeln, diese an die C&C[4]-Server weiterzuleiten und sich über das Netzwerk weiter zu verbreiten. „Packed.Generic.291“ ist ein von Symantec gegebener Name für die Schadsoftware „W32.Pilleuz!gen2“, welcher darauf hindeutet, dass „W32.Pilleuz!gen2“ die eigenen Daten verschlüsselt, um sich vor Antivirensoftware zu verstecken. Die Software „AngryIPScanner“ ist im eigentlichen Sinne keine Schadsoftware, sondern ein seit 2001 entwickeltes, frei verfügbares IT-Werkzeug zur Erkennung von Netzwerkteilnehmern und Durchführung von Portscans. Sie wird z. B. von Unternehmen genutzt, um Schwachstellen und Sicherheitsprobleme in ihrem IT-Netzwerk aufzuspüren. Kombiniert mit einer Schadsoftware kann „AngryIPScanner“ aber auch dazu genutzt werden, angreifbare Systeme im Netzwerk aufzuspüren und die Schadsoftware weiter zu verbreiten.

---

[1] Unter Trojanern wird eine Sorte Schadsoftware verstanden, welche mit legitimer oder legitim erscheinender Software zusammen verbreitet werden und dabei unentdeckt bleiben.

[2] Computerwürmer sind Schadprogramme, welche sich unkontrolliert und vollautomatisch verbreiten können. Wurmartige Schadsoftware besitzt diese Eigenschaft der Computerwürmer.

[3] Anwendungen, bei welchen direkte Nutzer-zu-Nutzer-Verbindungen genutzt werden, z. B. im Bereich des Filesharing.

[4] C&C steht für Command and Control. C&C Server sind die Kontroll- und Steuerungsserver, über welche IT-Angreifer auf kompromittierte Systeme zugreifen, von denen sie Schadsoftwarekomponenten nachladen und an die sie ausgespähte Informationen senden.

Im Zusammenspiel können „W32.Pilleuz!gen2“ und „AngriyIPScanner“ sich unter Umständen innerhalb von IT-Netzwerken unkontrolliert verbreiten, wenn keine Schutzmaßnahmen bestehen. Auf den betroffenen IT-Systemen wirkt „W32.Pilleuz!gen2“ dann im schlimmsten Fall als Spionagesystem, welches Passwörter, Daten und anderen Informationen auslesen kann. /VER16r01/

Auswirkung auf kerntechnische Anlagen

Nach bisherigen Erkenntnissen hatte das Ereignis nur eine geringe Bedeutung für die Sicherheit der betroffenen Anlage. Die gefundene Schadsoftware war nicht darauf ausgelegt, Manipulationen an den betroffenen IT-Systemen zu verursachen und aufgrund der nichtbestehenden Verbindung zum Internet war auch keine Aufklärungsmöglichkeit gegeben. Weiterhin war die Schadsoftware für ältere Windows Betriebssysteme ausgelegt, welche nicht von den betroffenen IT-Systemen verwendet wurden. Es handelte sich um weit verbreitete Schadsoftware, die nicht spezifisch für die hier betroffenen IT-Systeme angepasst oder entwickelt wurde. Insgesamt ist zu vermuten, dass es sich um eine zufällige Infektion und nicht um einen gezielten IT-Angriff handelt. /VER16r01/

Sicherheitstechnisch kommt diesem Ereignis eine maßgebliche Bedeutung zu, da die als wichtige Schutzhürde angesehene Luftschnittstelle bzw. Netztrennung von der Schadsoftware überwunden wurde und sich Schadsoftware für insgesamt sechs Jahre unbemerkt auf schutzbedürftigen IT-Systemen innerhalb des Netzwerkes ausbreiten konnte. Weiterhin ist der Vorfall der erste gemeldete mögliche Lieferkettenvorfall in der IT-Sicherheit von Kernkraftwerken in Deutschland. /VER16r01/

Direkte getroffene Maßnahmen

Nach der Detektion wurden sämtliche schutzbedürftige IT-Systeme auf eine Infektion mit Schadsoftware überprüft. Von den betroffenen IT-Systemen wurde die Schadsoftware entfernt. Eine forensische Untersuchung zur Nachvollziehbarkeit der Infektionsumstände wurde eingesetzt und durchgeführt. /VER16r01/

Auswirkungen auf langfristige Maßnahmen

Das betroffene Kernkraftwerk führte ein neues Konzept zum Umgang mit mobilen Datenträgern ein sowie weitere Schutzmaßnahmen bei Datentransporten und Einbringung von Datenträgern und IT-Systemen. /VER16r01/

2.1.2 NotPetya/Wiper

Übersicht

Am 27. Juni 2017 waren weltweit Unternehmen und weitere Organisationen von einem massiven Ausfall ihrer IT-Infrastruktur betroffen. Die Schadsoftware NotPetya, auch unter dem Namen Wiper geführt, breitete sich in den betroffenen IT-Netzwerken aus, vernichtete sämtliche gespeicherte Daten der betroffenen Systeme und versuchte, weitere IT-Systeme zu infizieren. Innerhalb weniger Tage entstand ein geschätzter wirtschaftlicher Schaden von ca. 10 Mrd. Dollar für weltweit agierende Unternehmen /WIR17r01/. Betroffen war unter anderem auch das Kernkraftwerk Tschernobyl. Dort fiel die automatisierte Strahlungsmessung aus /PRV17r01/.

Beschreibung

Im Frühling 2017 erlangten unbekannte Angreifer Zugriff auf die Server des Unternehmens Linkos Group und übernahmen unbemerkt die Kontrolle über die Updateserver des Unternehmens. Von hier aus verteilten die Angreifer auf IT-Systeme, welche das Programm M.E.Doc der Linkos Group installiert hatten, über die Updateroutinen des Programms eine Backdoor. M.E.Doc ist eine in der Ukraine weit verbreitete Software zur Unterstützung der Erstellung von Steuerabrechnungen und -erklärungen, welche auch von vielen in der Ukraine tätigen ausländischen Unternehmen und Konzerntöchtern verwendet wird. Die Angreifer luden auf allen betroffenen Systemen die Schadsoftware NotPetya mittels der installierten Backdoors hoch und aktivierten diese zeitgleich am 27.06.2017. Von diesen Initialsystemen aus verbreitete sich NotPetya weltweit. Zu Beginn berichteten ukrainische Unternehmen wie die Oschadbank von Angriffen auf ihre Computer, dann wurde weltweit von Computerabstürzen, Systemausfällen und vollständigen Netzwerkausfällen berichtet. /WIR17r01/

Dadurch, dass sich die Schadsoftware in den betroffenen Netzwerken verbreiten konnte, wurden teilweise Firmennetzwerke vollständig zerstört bzw. mussten, um die Verbreitung zu stoppen, vollständig abgeschaltet werden. Da NotPetya ebenfalls dauerhaft verbundene Datenbackups angriff, waren teilweise die Datenbackups betroffen und unbrauchbar. Gleichzeitig wurden auch sogenannte Always-On Systeme, welche sich durch ihre Redundanz vor Ausfall schützten und dauerhaft aktiviert und verbunden sind, zerstört.

Ein umfassendes Beispiel der Schadwirkung von NotPetya ist die Zerstörung des Firmennetzwerkes bei dem Logistikunternehmen Maersk. Eine einzelne Niederlassung von Maersk in der Ukraine nutzte die Software M.E.Doc für ihre Abrechnungen. Von hier aus verbreitete sich NotPetya im gesamten aus über 80.000 IT-Systemen bestehenden Netzwerk des Unternehmens. Jedes IT-System wurde infiziert und dessen gespeicherte Dateien unwiderruflich zerstört. Das Computernetzwerk von Maersk bestand zu dieser Zeit aus über 100 das Netzwerk steuernden Hauptsystemen. Diese Systeme wurden permanent betrieben und ihre Daten waren zueinander redundant, sodass der Ausfall eines oder mehrerer dieser Hauptsysteme keinen Einfluss auf das Gesamtnetzwerk haben sollte. Es gab keine weiteren Backups der Hauptsysteme. Durch NotPetya wurden bis auf ein einziges Hauptsystem, welches sich zum Zeitpunkt des Vorfalls in einem Flugzeug ohne Netzwerkverbindung befand, die Daten sämtlicher Hauptsysteme des Netzwerks zerstört. Ausgehend von diesem einen System konnte Maersk sein Netzwerk innerhalb einiger Wochen wieder in Betrieb nehmen. Ohne diesen Zufall wäre das Netzwerk unrettbar zerstört gewesen und ein vollständiger Neuaufbau hätte mehrere Monate oder gar Jahre gedauert. /WIR17r01/

Schlussendlich erlitt Maersk einen Schaden von über 300 Millionen Dollar, wobei der Betrieb des Unternehmens mit 50-80 % der Frachtkapazität durch Ersatzmaßnahmen aufrechterhalten wurde. Weltweit betrug der Schaden durch den Lieferkettenangriff mit NotPetya ca. 10 Milliarden Dollar. /WIR17r01/

Eingesetzte Schadsoftware

Die Schadsoftware NotPetya wird zum Teil der Schadsoftware Petya zugerechnet, unterscheidet sich aber fundamental von dieser. Zur Unterscheidung der Schadsoftware, die bei den IT-Sicherheitsvorfällen vom Juni 2017 eingesetzt wurde von der bereits früher bekannt gewordenen Schadsoftware Petya, wurde daher der Name NotPetya bzw. Wiper gewählt.

Bei der ursprünglichen Schadsoftware Petya handelt es sich um einen klassischen Verschlüsselungstrojaner[5], welcher mittels Emails verteilt wurde. Dabei wurde Petya in ein als PDF-Datei getarntes, ausführbares Programm integriert und verschlüsselte nach Ausführung des Programms verschiedene Dateien und somit auch Programme des betroffenen IT-Systems. Zu den verschlüsselten Dateien gehörte der „Master Boot Record", die zentrale Datei eines Windowssystems, welche die Startroutinen des IT-Systems dokumentiert. In der Folge einer Verschlüsselung des „Master Boot Record" stürzt der betroffene PC ab, beginnt einen Neustart und dabei verschlüsselt Petya die Datei „Master File Table", die Hauptdatei des Inhaltsverzeichnisses von in IT-Systemen eingesetzten Massenspeichern. Somit sind sämtliche Daten/Dateien des betroffenen PCs nicht mehr aufrufbar und es wird ein Sperrbildschirm angezeigt, der eine Lösegeldforderung für die Entschlüsselung enthält. Petya erschien in vier bekannten verschiedenen Versionen, wovon die ersten beiden mittels freier Programme entschlüsselbar und damit entfernbar waren und die letzten beiden aufgrund eines Programmfehlers überhaupt nicht mehr zu entschlüsseln waren. /KAS16r01/

NotPetya unterscheidet sich in seiner Verbreitung und Zielabsicht weitgehend von Petya. Zur Verbreitung wurde NotPetya nicht über Emails verteilt, sondern über die Lieferkette. Hierfür wurde die Schadsoftware von unbekannten Angreifern in offizielle Updates der Software M.E.Doc des Herstellers Linkos Group injiziert. Initial nutzten die Angreifer M.E.Doc zur Verbreitung von Backdoors in den betroffenen Systemen. Nach einem Befehl der Angreifer wurde auf allen betroffenen Systemen die Schadsoftware NotPetya installiert. /WIR17r01/

Einmal installiert nutzte NotPetya die Kombination von mehreren schweren Sicherheitslücken in Microsoft Windows aus, um sich weiter zu verbreiten. Dabei setzt NotPetya die von der NSA entwickelten Exploits EternalBlue und EternalRomance (nutzen die Schwachstellen CVE-2017-0144 bzw. CVE-2017-0145 in der Server Message Block (SMB)-Implementierung von Windows und allen Systemen, welche das Microsoft SMBv1-Serverprotokoll verwenden, aus) sowie das IT-Werkzeug Mimikatz (ein nicht von sich aus maliziöses, frei verfügbares Werkzeug zur Extraktion von Passwörtern und für Credential Harvesting).

[5] Besondere Form des Trojaners, bei welchem Daten des betroffenen IT-Systems von der Schadsoftware verschlüsselt werden, um gegebenenfalls Lösegeld für die Entschlüsselung zu erpressen.

Die von EternalBlue und EternalRomance ausgenutzten Schwachstellen von Microsoft Windows wurden nach Entwendung von NSA-Geheimpapieren Anfang 2017 öffentlich und betreffen alle Windowssysteme, welche das Sicherheitsupdate vom März 2017 noch nicht installiert haben. Mittels Ausnutzung dieser Schwachstellen erlangt eine Schadsoftware die Fähigkeit, beliebigen Code jederzeit auf dem betroffenen IT-System auszuführen. Bekannt wurden die Schwachstellen und die Exploits EternalBlue bzw. EternalRomance in Folge der IT-Sicherheitsvorfälle in Zusammenhang mit der Schadsoftware WannaCry und der Schadsoftware BadRabbit. Das IT-Werkzeug Mimikatz ermöglicht es Schadsoftware, die innerhalb des Arbeitsspeichers gespeicherten Passwörter auszulesen. Wenn es sich um Administratorpasswörter handelt, erhält die Schadsoftware damit die Möglichkeit, beliebigen Code auszuführen. Wenn diese Passwörter Universalpasswörter, z. B. für administrative Zugriffe auf alle Netzwerksysteme, sind, kann die Schadsoftware sich auf allen im Netzwerk verbundenen Windows Systemen mit diesen Passwörtern ausbreiten. Durch den Einsatz von Mimikatz konnte NotPetya auch Systeme infizieren, welche bereits das Windows Sicherheitsupdate vom März 2017 installiert hatten und damit den Einsatz der Exploits EternalBlue und EternalRomance verhinderten. Der kombinierte Einsatz von EternalBlue bzw. EternalRomance und Mimikatz führte dazu, dass sich NotPetya innerhalb kurzer Zeit in großen IT-Netzwerken verbreiten konnte und damit sämtliche verbundenen Windowssysteme infizieren konnte. NotPetya nutzte umfangreiche Systeme zur Verschleierung seiner Existenz und Handlungen auf den betroffenen Systemen. Am Tag des Angriffs erkannten nur 2 von über 50 Virenscannern NotPetya als Schadsoftware. /WIR17r01/

Wenn die Schadsoftware NotPetya Zugriff auf ein System erhielt, verschlüsselte sie die Datei „Master Boot Record“ umgehend, untersuchte den Arbeitsspeicher auf neue Passwörter, griff sämtliche verfügbaren IT-Systeme im Netzwerk an und erzwang dann einen Systemneustart. Im Rahmen des Systemneustarts wurde die Datei „Master File Table“ aller verbundener Massenspeicher verschlüsselt und der von der Schadsoftware Petya bekannte Sperrbildschirm angezeigt. NotPetya war aber nicht auf Entschlüsselung der betroffenen Datensysteme ausgelegt, es wurden keine Schlüssel zur Entschlüsselung generiert. Die betroffenen Datenspeicher waren unwiderruflich verloren, die IT-Systeme nicht mehr einsetzbar oder ohne Backups wiederherstellbar. /WIR17r01/

Auswirkung auf kerntechnische Anlagen

Nach bisherigen Informationen war auch eine kerntechnische Anlage betroffen, das ukrainische Kernkraftwerk Tschernobyl /PRV17r01/. Hier wurden Teile des Computernetzwerks des abgeschalteten bzw. havarierten Kernkraftwerks von NotPetya infiziert. Dadurch ist der Einsatz von elektronischen Dokumenten wie auch das Schreiben und Speichern von Berichten, das Archivieren und Dokumentieren von Zahlen und das Senden und Empfangen von elektronischen Nachrichten zeitweise gestoppt worden. Das auf Windowssystemen basierende automatische System zur Strahlungsüberwachung wurde ebenfalls von NotPetya beeinflusst, sodass manuelle Messungen der Strahlenbelastung als Ersatzmaßnahme notwendig wurden. Nach bisherigen Informationen kam es zu keinen weiteren Einflüssen auf die Systeme der Anlage und mittels Backups wurde die Verfügbarkeit der betroffenen Computersysteme wiederhergestellt. /PRV17r01/

Direkte getroffene Maßnahmen

Reaktive Maßnahmen, um die Ausbreitung zu reduzieren bzw. zu verhindern, waren beim NotPetya-Angriff nur eingeschränkt möglich. Die Schadsoftware verbreitete sich innerhalb von Netzwerken mit so hoher Geschwindigkeit, dass es in vielen Fällen nach Bemerken des Angriffes nicht mehr möglich war, die betroffenen IT-Systeme vom IT-Netzwerk zu trennen. Nur dauerhaft bestehende bzw. proaktive Netztrennungen stoppten in verschiedenen Unternehmen die Verbreitung der Schadsoftware. Die operativen Kapazitäten wurden von den betroffenen Unternehmen sowie dem Kernkraftwerk Tschernobyl durch entsprechende Ersatzmaßnahmen aufrechterhalten. /WIR17r01/

Auswirkungen auf langfristige Maßnahmen

Die Erkenntnisse und sich daraus ergebenden, langfristigen Maßnahmen wurden von den betroffenen Unternehmen im Einzelnen unterschiedlich ausgearbeitet. Im Wesentlichen umfassen die Maßnahmen die Sicherung der Softwarelieferkette, das betriebliche Softwaremanagement, das betriebliche Netzwerkmanagement sowie die Notfall- und Wiederherstellungspläne:

- **Sicherung der Softwarelieferkette**
  Die Sicherung der Softwarelieferkette ist ein zentrales Element zur Prävention weiterer Schadsoftwareeintragung über die Lieferkette. Die Kooperation mit Herstellern, die Bewertung des IT-Sicherheitsmanagements und die Risikoeinschätzung der Lieferanten und das Management der von den Lieferanten bezogenen Software ermöglicht dabei eine Risikoabsenkung. /FAY18r01/

- **Betriebliches Softwaremanagement**
  Im Falle von Lieferkettenangriffen zeigte sich die Notwendigkeit der Anpassung des Softwaremanagements an potenzielle Risiken. Während nicht aktualisierte Versionen von Microsoft Windows die Verbreitung von NotPetya ermöglichten, führte ein Update der lokalen Steuersoftware M.E.Doc zum Eintrittspunkt von NotPetya. Abhängig vom Einsatzgebiet, Notwendigkeit des Updates und Vertrauensbeziehung zum Lieferanten sind Softwareupdates unterschiedlich zu behandeln und durchzuführen. /WIR17r01/

- **Betriebliches Netzwerkmanagement**
  Die Verbreitung von NotPetya wurde durch die Struktur der betroffenen Firmennetzwerke erheblich vereinfacht, sodass ausgehend von einem einzelnen betroffenen System tausende Systeme infiziert wurden. Netzwerkbarrieren innerhalb von Firmennetzwerken, sich unterscheidende Accountnamen und Passwörter für administrative Lösungen und der Weggang von Einheitslösungen reduzieren langfristig die Möglichkeiten einer solch schwerwiegenden Betroffenheit durch Lieferkettenangriffe, welche vorhergehende Sicherungsmaßnahmen überwunden haben. /FAY18r01/

- **Notfall- und Wiederherstellung**
  Die Notfall- und Wiederherstellungsmaßnahmen im Rahmen der NotPetya Angriffe zeigten die Notwendigkeit schneller Backups und Wiederherstellungen der verwendeten Systeme auf sowie die Notwendigkeit zum Einsatz von IT-systemunabhängigen Ersatzmaßnahmen /LAN19r01/.

2.1.3 Dragonfly

Übersicht

Unter Dragonfly werden mehrere Cyberangriffskampagnen zusammengefasst, welche der APT[6] Gruppe Dragonfly zugeordnet werden. Die Gruppe Dragonfly, die auch unter verschiedenen weiteren Namen wie Energetic Bear oder Berserk Bear bekannt ist, wurde für IT-Angriffe auf kritische Infrastruktur bekannt, wobei sie eine hohe Anzahl verschiedener Werkzeuge und Angriffspfade wie z. B. auch Lieferketten einsetzt, um Zugriff auf IT-Systeme, darunter auch Leittechniksysteme, zu erhalten und Informationen über diese Systeme auszuspähen. Es sind mehrere Angriffswellen durch Dragonfly auszumachen: Eine erste Angriffswelle, welche 2011 anfing und 2014 vom IT-Sicherheitsunternehmen Symantec aufgedeckt wurde, sowie eine seit 2015 laufende und im Jahr 2017 intensivierte Kampagne. Die Ziele der Gruppe Dragonfly sind hauptsächlich im Energiesektor beheimatet, darunter Netzbetreiber, Kraftwerkshersteller, Zulieferer und Betreiber. Ein Großteil der bekannt gewordenen angegriffenen Unternehmen und Institutionen liegt in westlichen Industrieländern, dies änderte sich aber im Rahmen geopolitischer Entwicklung wiederholt. /SYM14r01, SYM17r01/

Beschreibung

Beginnend im Jahr 2011 wurde eine IT-Angriffsserie auf Unternehmen und Institutionen im westlichen Energiesektor festgestellt. Diese Angriffe liefen weitgehend nach dem gleichen Schema ab und basierten auf initialen Zugriffspfaden über Phishing, Watering Hole-Angriffen, d. h. die Kompromittierung von Webseiten, welche häufig von Personen aus dem Energiesektor besucht werden, und kompromittierten Updates auf Hersteller-Webseiten. Über die ersten beiden Pfade konnten Kontaktinformationen, Zugriffsinformationen und Login-Informationen von Firmen bzw. deren Lieferanten und Dienstleister ausgespäht werden. Nach bisherigen Erkenntnissen wurden weiterhin mindestens drei Hersteller von industriellen Steuerungssystemen (der belgische Hersteller Ewon, der schweizerische Hersteller MESA und der deutsche Hersteller MB Connect Line GmbH /SAN16r01/) von den Angreifern der Gruppe Dragonfly kompromittiert und verteilten zeitweise Schadcodes mittels Updates an deren Kunden.

---

[6] APT steht für Advanced Persistend Threat. Ein Term für Angriffe und Gruppen, welche sich durch ihre langanhaltende Bedrohung und umfangreichen Ressourcen auszeichnen. APT Gruppen werden häufig mit staatlichen Institutionen und Mitteln in Verbindung gebracht.

Ausgehend vom Erstzugriff auf das Anlagennetzwerk der eigentlich anvisierten Ziele wurden verschiedene Schadsoftwarekomponenten der Angreifer eingesetzt, um Informationen zu sammeln und IT-Aufklärung durchzuführen. /SYM14r01/

Nach bisherigen Erkenntnissen wurden die IT-Angriffe nicht durchgeführt, um direkte Schäden zu verursachen. Es wird vermutet, dass sie als Vorbereitung weiterer Angriffe dienten. Mit der Entdeckung durch ein IT-Sicherheitsunternehmen im Jahr 2014 wurde die heute als Dragonfly benannte Angriffsserie beendet. Die entdeckten Angriffswerkzeuge wurden weltweit bekannt und die IT-Angriffe durch die Gruppe Dragonfly dadurch massiv erschwert. /SYM14r01, SYM17r01/

Mitte bis Ende des Jahres 2015 wurden neue IT-Angriffe auf Unternehmen und Institutionen in der Energiebranche beobachtet, welche nach dem bisherigen Schema der Gruppe Dragonfly ausgeführt wurden. Auch diese zweite Angriffswelle war vornehmlich auf Unternehmen mit Verbindung zum Energiesektor ausgerichtet, einschließlich der Nuklearindustrie und des Öl- und Gassektors. 2017 war beispielsweise auch das US-Kernkraftwerk Wolf Creek betroffen /NYT17w01/. Ein Sprecher des US-Department of Homeland Security wird in diesem Zusammenhang mit der Aussage zitiert, es hätte den Anschein, als wären die möglichen Auswirkungen der Kompromittierung des Anlagennetzwerks von Wolf Creek auf administrative und geschäftliche Teile des Netzwerks beschränkt.

Anstatt ihre bekannten Schadsoftwarewerkzeuge zu verwenden, nutzte die Gruppe im Rahmen der zweiten Angriffswelle häufiger frei verfügbare Schadsoftware wie Phishery, vermutlich um die Attribuierung zu erschweren. Die neuere Kampagne fokussiert sich neben der Aufklärung nach bisherigen Erkenntnissen auch auf das Ausspähen von Informationen zum Betrieb und zur Bedienung von industriellen Steuerungssystemen, beispielsweise über das systematische Erfassen von Screenshots. Eine Manipulation der industriellen Steuerungssysteme wurde nach bisherigen Erkenntnissen bislang unterlassen, obwohl die Angreifergruppierung Dragonfly nach übereinstimmender Einschätzung von verschiedenen Analysten dazu durchaus in der Lage wäre. /SYM17r01/

Eingesetzte Schadsoftware

Die Gruppe Dragonfly nutzt eine Vielzahl von IT-Angriffswerkzeugen zum Eindringen in das Anlagennetzwerk des anvisierten Ziels. Zu den eingesetzten Angriffswerkzeugen dienen insbesondere Phishing-Angriffe mit Hilfe der seit 2016 öffentlich zugänglichen Software Phishery, Watering-Hole-Angriffe, sowie die Kompromittierung von legitimen, auf Herstellerseiten zum Download bereitstehenden Updates. Bei den ersten beiden Angriffstechniken geht es den Angreifern hauptsächlich um das Ausspähen von legitimen Nutzernamen-Passwort-Kombinationen für Zugriffe auf die eigentlich anvisierten Ziele. Im letzten Fall wurde zunächst ein Zwischenziel kompromittiert, um über die Lieferkette zum eigentlich anvisierten Ziel zu gelangen. Dies ist aus mehreren Gründen eine vielversprechende Taktik für Angreifer. Zum einen werden die bei Zulieferern und anderen Elementen der Lieferkette realisierten IT-Sicherheitsmaßnahmen häufig als geringer eingeschätzt als die IT-Sicherheitsmaßnahmen des eigentlich anvisierten Ziels. Zum anderen führt die Kompromittierung eines Updates dazu, dass die Schadsoftware im Rahmen eines von der Anlage vorgesehenen Vorgangs in die Anlage gelangt und die Installation unwissentlich durch autorisierte Personen erfolgt. Hiermit werden die IT-Sicherheitsmaßnahmen der Anlage umgangen. Nach gelungenem Erstzugriff auf die IT-Systeme setzt Dragonfly sogenannte Remote Access Trojaner[7] ein, mit welchen die IT-Systeme aus der Ferne ausgespäht und gesteuert werden können, insbesondere die Trojaner Karagany.B und Heriplor, welche in den aufgefundenen Versionen und Modifikationen nur von Dragonfly eingesetzt wurden. /SYM14r01/

Ein weiteres zentrales Element der ersten Angriffswelle war die Schadsoftware Havex, welche neben Stuxnet, BlackEnergy, Industroyer und Triton eine der fünf bisher bekannten Vertreter ICS-angepasster Schadsoftware ist, welche in den letzten zehn Jahren im Rahmen von Angriffen auf industrielle Steuerungssysteme eingesetzt wurden. Bei Havex handelt es sich um einen von Dragonfly eingesetzten Remote Access Trojaner, welcher entwickelt wurde, um zentrale Informationen der betroffenen Leittechniksysteme auszuspionieren und als Backdoor die Möglichkeit zur Installation weiterer Schadsoftware zu bieten. Zusätzlich ist Havex in der Lage, über die OPC Kommunikation auf Leittechniksysteme zuzugreifen.

[7] Remote Access Trojaner, auch RAT abgekürzt, sind Formen der Trojaner, welche den Angreifern langfristige Fernzugriffsmöglichkeiten auf infizierte Systeme geben.

OPC (Open Platform Communications) ist ein Kommunikationsprotokoll, welches von industriellen Steuerungssystemen zur Steuerung von und Kommunikation mit anderen Systemen eingesetzt wird. Da das OPC Protokoll auf offene Kommunikation und Komptabilität ausgelegt ist, ermöglicht dies Havex die Kommunikation einer Vielzahl von industriellen Steuerungssystemen abzufangen. Havex sammelt dabei Daten, unter anderem die Servernamen, Programm-IDs, OPC Versionen, Verkaufsversion, Betriebszustand, Anzahl und verfügbare Bandbreite und schickt diese an die C&C Server der Angreifer. Nach bisherigen Kenntnissen dient Havex ausschließlich als Aufklärungsschadsoftware. /SEC14r01/

Auswirkung auf kerntechnische Anlagen

2017 wurde bekannt, dass auch mindestens ein Kernkraftwerk in den USA von den Dragonfly Angriffen betroffen war. Die amerikanische Bundespolizei und das amerikanische Heimatschutzministerium gaben im Juli 2017 bekannt, dass ein Betreiber eines Kernkraftwerks angegriffen wurde. Dabei gaben die Behörden keine Informationen, ob der IT-Angriff dem Ausspähen von Informationen oder der Sabotage diente. Es gibt nach Informationen der New York Times keine weiteren Informationen, ob die Angreifer von den betroffenen Computern von Angestellten des Betreibers auf die IT-Systeme der Anlage zugreifen konnten oder ob IT-Systeme der Anlage selbst betroffen waren. Weitere Kommentare wurden von den Bundesbehörden abgelehnt, es wurde jedoch noch ausgesagt, dass keine Systeme des Anlagenbetriebs betroffen waren und dass es keine Hinweise für eine Bedrohung der öffentlichen Sicherheit gab, sondern nur administrative und geschäftliche Netzwerke betroffen waren. /NYT17w01/

Direkt getroffene Maßnahmen

Nach Bekanntwerden der ersten Angriffswelle wurden die eingesetzten Schadsoftwarekomponenten in alle bekannten Virensignaturen aufgenommen, wodurch betroffene Unternehmen grundsätzlich die Möglichkeit bekamen, die bestehenden Infektionen aufzuspüren und zu entfernen /SYM14r01/. Aktuelle Warnmeldungen des BSI /BSI20i02/ zeigen jedoch, dass die zweite Angriffswelle nach wie vor andauert.

Auswirkungen auf langfristige Maßnahmen

Die APT-Gruppierung Dragonfly hatte und hat mit den beiden IT-Angriffskampagnen Auswirkungen auf die IT-Sicherheit von Unternehmen und Staaten, insbesondere im Bereich der kritischen Infrastruktur. Mit verschiedenen Angriffstechniken über Emails, Watering Holes und Herstellerwebseiten, dem Ausnutzen der Lieferkette, mehreren maßgeschneiderten Schadsoftwarekomponenten und weltweiten Angriffszielen, sind die Dragonfly-Kampagnen eines der prominentesten Beispiele für die Gefahr durch APTs geworden. Die Weiterentwicklungen nationaler und unternehmerischer IT-Abwehrmaßnahmen sind unter anderem mit Hinblick auf die Dragonfly Kampagnen erarbeitet worden. /INS18r01/

2.1.4 Ingérop Datenverlust

Übersicht

Am ersten November 2018 wurde bekannt, dass Daten des französischen Baudienstleisters Ingérop zuerst teilweise im Internet aufzufinden waren und anschließend ein aus 11.000 Dateien bestehendes Archiv im Darknet[8] angeboten wurde. Ingérop arbeitet als Baudienstleister für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo /HEI18r01/ mit und bewirbt sich immer wieder für Bauprojekte aus dem Bereich der kritischen Infrastrukturen. Die Daten wurden nach bisherigen Erkenntnissen infolge eines Phishing-Angriffes[9] auf Mitarbeiter Ingérops entwendet. /HEI18r01/

[8] Als Darknet werden Bereiche des Internets genannt, welche nicht im freien Netz öffentlich sind und somit nicht direkt gesucht werden können.

[9] Bei einem Phishing-Angriff wird versucht Daten einer Person „abzufischen“. Dabei werden den Zielpersonen fingierte Aufforderungen zur Eingabe bzw. Preisgabe ihrer Daten und Passwörter z. B. per Email zugeschickt, wodurch die Angreifer an diese Daten gelangen.

Beschreibung

Im November 2018 veröffentlichten deutsche und französische Medien Berichte über den Datenverlust des französischen Baudienstleisters Ingérop. Nach bisherigen Erkenntnissen wurde dieser im ersten Halbjahr 2018 Opfer einer Phishing-Attacke, bei welcher ein oder mehrere Mitarbeiter des Konzerns mittels fingierter Emails zur Installation der bisher nicht bekannten Schadsoftware verleitet wurden. In Folge der Schadsoftwareinfektion wurden insgesamt 11.000 Dateien mit einer Gesamtgröße von 65 Gigabyte von den Angreifern entwendet. Im Juli 2018 wurde von der Polizei NRW ein IT-Servicedienstleister in Dortmund durchsucht, in dessen Räumlichkeiten Server betrieben wurden, welche Teile der entwendeten Daten im Internet zur Verfügung stellten. Einen Monat später wurde das gesamte Archiv der Ingérop Daten im Darknet zum Verkauf angeboten. Zu den Daten gehören Informationen zu verschiedenen Bauprojekten im Bereich der kritischen Infrastruktur, an welchen Ingérop beteiligt ist, sowie Mitarbeiterinformationen und Emailkorrespondenzen. /HEI18r01/

Eingesetzte Schadsoftware

Nach bisherigen Informationen ist die im Rahmen des Phishing-Angriffes auf Ingérop eingesetzte Schadsoftware nicht bekannt. Die bisher veröffentlichten Informationen zum Angriff zeigen, dass die eingesetzte Schadsoftware in der Lage war, mehrere Systeme innerhalb des Ingérop-Netzwerkes anzugreifen und Daten von den betroffenen Systemen zu entwenden. /ZFK18r01/

Auswirkung auf kerntechnische Anlagen

Nach bisherigen Kenntnissen sind auch Daten aus zwei nuklearen Anlagen in den veröffentlichten Dateien enthalten. Zum einen sind umfassende Daten Ingérops zum geplanten Endlager für hochradioaktive Abfälle Cigéo im Department Meuse /HEI18r01/ veröffentlicht worden. Das geplante Endlager befindet sich in einer Planungs- und Forschungsphase und soll nach bisherigen Kenntnissen ab 2025 für umfangreiche Erprobungen genutzt werden. Nach Medienberichten wurden geheime Dokumente mit den Daten veröffentlicht, jedoch wird nicht weiter ausgeführt, in welcher Form diese Dokumente geheim sind oder welche Inhalte in diesen Dokumenten beschrieben werden, außer dem Konflikt zwischen Ingérop und den örtlichen gegen das Endlager protestierenden Landwirten.

Weiterhin wurden Daten des Kernkraftwerks Fessenheim /HEI18r01/ veröffentlicht, welches aus zwei Druckwasserreaktoren besteht, wovon der erste seit Februar 2020 und der zweite seit Juni 2020 abgeschaltet ist. Es ist bisher unbekannt, welche Daten genau zum Kernkraftwerk Fessenheim veröffentlicht wurde. /HEI18r01/

Direkt getroffene Maßnahmen

Ingérop meldete den Vorfall bei der Staatsanwaltschaft Paris, sodass die in Teilen veröffentlichten Daten infolge einer Durchsuchung der Polizei NRW in Dortmund vom Netz genommen worden sind. Weitere Maßnahmen sind bisher nicht veröffentlicht worden. /HEI18r01/

Auswirkungen auf langfristige Maßnahmen

Langfristige Maßnahmen Ingérops oder seiner Kunden aus dem nuklearen Sektor Frankreichs sind bisher nicht veröffentlicht worden.

2.1.5 Schadsoftwarefund im japanischen Kernkraftwerk Monju

Übersicht

Am 2. Januar 2014 wurde Schadsoftware auf einem Computer in der Warte des japanischen Kernkraftwerks Monju /JAT14r01/ entdeckt. Der inzwischen stillgelegte Brutreaktor der japanischen Atomenergiebehörde „Japan Atomic Energy Agency“ befand sich zu dieser Zeit bereits im Langzeitstillstand. Die Schadsoftware gelangte wahrscheinlich über den Update-Mechanismus eines Video-Wiedergabeprogramms auf einen Computer, der von den Mitarbeitern hauptsächlich für Büroarbeiten und zu Dokumentationszwecken genutzt wurde. Obwohl keine Verbindung zu leittechnischen oder anderweitigen Steuersystemen des Kernkraftwerks vorlag, bestand die Gefahr des Diebstahls sensibler Dokumente wie E-Mails, Schulungsunterlagen und Mitarbeiterdaten. /JAT14r01/

Beschreibung

Am 6. Januar 2014 veröffentlichte die japanische Atomenergiebehörde die Meldung, dass auf einem für Büroarbeiten genutzten Computer im Kernkraftwerk Monju Schadsoftware gefunden wurde. /JAE14r01/ Verdächtige Aktivitäten wurden erstmals am 2. Januar 2014 in Form einer externen Kommunikation mit einem südkoreanischen Server festgestellt. Nachdem der betroffene Computer vom Netzwerk getrennt und untersucht wurde, stellte man am 3. Januar 2014 fest, dass eine externe Verbindung über 30 Mal innerhalb von fünf Tagen hergestellt wurde. Nach ersten Untersuchungen wurde festgestellt, dass die gefundene Schadsoftware vermutlich von einem in der Anlage angestellten Mitarbeiter heruntergeladen wurde, der mutmaßlich, obwohl er kein Administrator für das System war, ein Softwareupdate eines Video-Wiedergabeprogramms durchgeführt hatte. /SOP14r01/

Die eingesetzte Schadsoftware gelangte wahrscheinlich über den Update-Mechanismus des Video-Wiedergabeprogramms „GOM Player“ des südkoreanischen Unternehmens Gretech Corporation auf den Computer. Dieses Programm ist insbesondere in Südkorea und Japan beliebt und weit verbreitet.

Eingesetzte Schadsoftware

Laut Kaspersky handelte es sich bei der eingesetzten Schadsoftware um den Remote Access Trojaner „Backdoor.Win32.Miancha“, durch den Angreifer Zugriff und die Kontrolle über ein System erlangen können. Dabei ist es bei einem IT-Angriff über eine Backdoor denkbar, dass Angreifer Informationen sammeln, weitere Schadsoftware installieren oder das infizierte System über Fernzugriff steuern. /ENS20w01/

Auswirkung auf kerntechnische Anlagen

Nach Angaben der japanischen Atomenergiebehörde handelt es sich bei den auf dem betroffenen Computer gespeicherten Daten um Ausbildungsberichte und Schulungsunterlagen für das Dienstpersonal und ähnliche administrative Dokumente, sowie um etwa 42000 gespeicherte E-Mails. Eine Verbindung zur Steuerung oder Überwachung des Anlagenbetriebs bestand laut der vorliegenden Informationen nicht. /JAE14r01/

Nach Ansicht von Experten war die kerntechnische Anlage nicht gezielt für einen Angriff ausgewählt worden, sondern wurde wahrscheinlich Opfer eines zufälligen Angriffs, der durch das unbedachte Vorgehen eines Mitarbeiters erst ermöglicht wurde, wobei angesichts des Verlaufs des IT-Sicherheitsvorfalls auf die Wichtigkeit der IT-Sicherheit für Kernkraftwerke hingewiesen wurde um solche Vorfälle in Zukunft zu verhindern. Dazu wurde angemerkt, dass nur von Experten bzw. Administratoren zugelassene und entsprechend gewartete Software verwendet werden sollte. /CSI14r01, SOP14r01/

Direkte getroffene Maßnahmen

Laut Angaben der japanischen Atomenergiebehörde wurde nach Entdeckung der Schadsoftware die Kommunikation mit dem südkoreanischen Server sofort unterbrochen und der Computer vom Netzwerk getrennt. Anschließend wurde eine umfangreiche Untersuchung des betroffenen Systems und des gesamten Vorfalls angeordnet und durchgeführt.

Auswirkungen auf langfristige Maßnahmen

Langfristige Maßnahmen durch die japanische Atomenergiebehörde sind nicht bekannt.

2.2 Supply-Chain-Angriffe ohne bekannt gewordenen Bezug zu kerntechnischen Anlagen

Eine Vielzahl unterschiedlicher Lieferkettenangriffe ohne bislang ersichtlichen Bezug zu kerntechnischen Anlagen wurde in den letzten zehn Jahren bekannt. Dabei handelt es sich um Angriffe mit unterschiedlicher Zielsetzung, wahrscheinlich mit politischen oder ökonomischen Interessen.

2.2.1 ShadowHammer

Übersicht

Im März 2019 veröffentlichte Kaspersky Labs einen bis dahin unbekannten Lieferkettenangriff über den Hersteller für PCs ASUSTeK Computer Inc. (ASUS), welcher ShadowHammer genannt wurde. In Rahmen dieses Lieferkettenangriffes wurde eine schadhafte Version einer ursprünglich offiziellen Software auf der Webseite des Herstellers zur Nutzung für Kunden bereitgestellt, womit Schadsoftware auf die PCs der Anwender verteilt wurde. /KAS19r01/

Beschreibung

Nach bisherigen Erkenntnissen wurden die Arbeiten an der ersten Version des Lieferkettenangriffes im ersten Halbjahr 2018 abgeschlossen. Wahrscheinlich wurde ab Mitte bis Ende Juni 2018 die mit dem Schadcode versehende Software auf der Webseite des Herstellers verbreitet. Die erste Version der manipulierten Software wurde am 29. Juni 2018 auf der Prüfwebseite VirusTotal hochgeladen. Der Lieferkettenangriff wurde nach bisherigen Kenntnissen im November 2018 beendet oder unterbrochen, die letzte Prüfung manipulierter Software fand auf VirusTotal am 17. November 2018 statt. Nach bisherigen Erkenntnissen waren insgesamt ca. 600 MAC Adressen vom vollständigen Umfang der Schadsoftware betroffen, wovon 270 zu von ASUS ausgelieferten Systemen gehören und sich ansonsten auf andere Unternehmen verteilen. Am 29. Januar 2019 entdeckte Kaspersky Lab den Lieferkettenangriff und unterrichtete ASUS am 30. Januar 2019 hiervon. Einen Tag später konnte bestätigt werden, dass die aktuelle Version der Software nicht manipuliert war. Ende März 2019 wurden die Erkenntnisse veröffentlicht. /SEN19r01/

Eingesetzte Schadsoftware

Die eingesetzte Schadsoftware beinhaltet zwei nacheinander ausgeführte Payloads, wobei die erste Payload alleinig dazu dient, Zugriff auf den betroffenen PC zu erhalten, und die zweite Payload dann weitere Funktionen bereithält.

Die erste Payload wird über die Lieferkette verteilt. Hierzu wurde auf der Webseite des Herstellers ASUS eine von den Angreifern modifizierte Version einer Software für Kunden des Unternehmens angeboten. Die manipulierte Software wurde in Form eines ZIP-Archivs verteilt, in welchem sich eine EXE-Datei befand.

Für die Nutzer war eine Manipulation nicht erkennbar, da die manipulierte Datei ein offizielles Zertifikat des Herstellers besaß. Zertifikate verfallen im Normalfall bei Änderungen an der Software, in diesem Fall waren die Angreifer jedoch in der Lage, Schadcode über genutzte Bibliotheken in die Software einzuarbeiten, so dass weder das Zertifikat verfiel noch Virenscanner auf die Manipulation reagierten. Wenn Nutzer die manipulierte Software ausführten, wurden sämtliche legitime Funktionen der Software ausgeführt und zusätzlich unerkannt die Schadfunktionen. Im Rahmen der Schadfunktionen werden dabei die MAC-Adressen der betroffenen Geräte ausgelesen, mit einer im Schadcode festgeschriebenen Liste von MAC-Adressen verglichen und bei einer Übereinstimmung wird die zweite Payload heruntergeladen und ausgeführt. Bei fehlender Übereinstimmung wird die Schadsoftware nach bisherigen Erkenntnissen inaktiv und verbleibt auf dem betroffenen System. /KAS19r01/

Die zweite Payload wurde von einer fest vorgegebenen URL, welche eine Verbindung zu ASUS vorgibt, heruntergeladen. Da bei Entdeckung des Lieferkettenangriffes die zweite Stufe des Schadcodes unter der URL nicht mehr verfügbar war, existieren bisher keine bekannten Analysen der zweiten Stufe. /KAs19r01/

Direkt getroffene Maßnahmen

Nach bisherigen Erkenntnissen wurden nur Maßnahmen zur Aufklärung und Analyse der Schadsoftware getroffen, da mit Bekanntwerden des Lieferkettenangriffes dieser bereits eingestellt worden war. Weiterhin wurden notwendige Informationen zur Erkennung der Schadsoftware an die Hersteller von Antivirensoftware weitergeleitet. /KAS19r01/, /SEN19r01/

Auswirkungen auf langfristige Maßnahmen

Das betroffene Unternehmen wie auch weitere Unternehmen haben keine langfristigen Maßnahmen infolge des Lieferkettenangriffes veröffentlicht.

2.2.2 Target Datendiebstahl

Übersicht

Zwischen dem 27. November 2013 und dem 15. Dezember 2013 wurde das amerikanische Einzelhandelsunternehmen Target Ziel eines IT-Angriffes, welcher über die Lieferkette ausgeführt wurde. Im Rahmen des Angriffes, welcher über das Netzwerk eines kleinen Dienstleisters begann, wurden insgesamt die persönlichen und finanziellen Informationen von ca. 110 Millionen Kunden, welche mit Kredit- bzw. Debitkarte zahlten, entwendet.

Beschreibung

Zu einem unbekannten Zeitpunkt vor dem IT-Angriff führten die Angreifer eine Aufklärungskampagne zur Entdeckung möglicher Eintrittspunkte in das IT-Netzwerk von Target durch. Dabei oder darauf folgend führten die Angreifer eine auf Zulieferer und Vertragspartner von Target abzielende Phishing-Kampagne durch, mit welcher sie Zugriff auf die IT-Systeme eines lokalen Kühlsystempartners erreichen. Dort konnten sie Login-Details entwenden, welche die Angreifer für die darauffolgenden IT-Angriffe auf das IT-Netzwerk von Target nutzen konnten. Zu einem Zeitpunkt vor dem 27. November 2013 erlangten die Angreifer Zugriff auf das IT-Netzwerk von Target und konnten dort die auf Kassensysteme spezialisierte Schadsoftware installieren. Am 27. November 2013, der Hochphase des amerikanischen Weihnachtsgeschäfts, aktivierten die Angreifer ihre Schadsoftware und begannen die Kredit- und Debitkarteninformationen der Kunden von Target auszulesen. Am 13. Dezember 2013 informierte Target die Justizbehörden der USA über den IT-Angriff, einen Tag später wurde ein IT-Dienstleister zur Untersuchung des Datendiebstahls engagiert und am 15. Dezember 2013 wurde der Datendiebstahl nach Angaben von Target vollständig unterbunden. Bis dahin wurden 110 Millionen Informationssätze gestohlen. Mit einem Bericht vom 18. Dezember 2013 wurde der IT-Angriff über die Lieferkette auf den Einzelhandelskonzern Target öffentlich. Der Gesamtschaden des Angriffes wird von Target auf 184 Millionen Dollar geschätzt. /ZDN15r01/

Eingesetzte Schadsoftware

Die Angreifer nutzten im Rahmen des IT-Angriffes auf Target über die Lieferkette mehrere, zum Teil unbekannte IT-Angriffswerkzeuge und Schadsoftwarekomponenten um Stück für Stück ihr Ziel, die Kredit- und Debitkartendaten der Kunden, zu erreichen.

In einem ersten Schritt nutzten die Angreifer Phishing-Emails, um Zugriff auf die Systeme möglicher Dienstleister und Lieferanten von Target zu erhalten. Mit einer solchen Email waren die Angreifer erfolgreich, sodass die Systeme eines lokalen Kühlsystemlieferanten mit dem Trojaner Citadel infiziert wurden. Der Trojaner Citadel ist eine Variante des Banktrojaners Zeus, welcher auf die Entwendung von Accountdetails und Passwörtern spezialisiert ist, um so Zugriff auf das Onlinebanking seiner Opfer zu erhalten. Mit dem Trojaner Citadel waren die Angreifer in der Lage, die Login-Details für verschiedene Portale und Netzwerke mit Verbindung zu Target zu erlangen. Obwohl der Trojaner zum Tatzeitpunkt von sämtlichen großen Antivirenprogrammen erkannt wurde, blieb er bei dem Vertragspartner unerkannt, da kein Antivirenprogramm mit Echtzeiterkennung eingesetzt wurde. /ZDN15r01/

Die Angreifer nutzten mit den ausgespähten Informationen einen bisher nicht veröffentlichten Pfad über die Portale und Netzwerke von Target und waren dabei in der Lage, sich Zugriff auf die Server von Target zu verschaffen. In dieser Zeit wurde von einem Angriffserkennungssystem ein Alarm ausgelöst, welchem jedoch von Target nicht nachgegangen wurde. Nach erfolgreichem Eindringen in die Server von Target nutzten die Angreifer den Trojaner POSRAM um die Kassensysteme (point of sale, POS) von Target anzugreifen. Die Schadsoftware las die im RAM[10] der Kassensysteme gespeicherten Kredit- und Debitkarteninformationen der Kunden aus und sammelte diese an einem bestimmten unbeachteten Punkt im Netzwerk, sodass die Angreifer die Daten anschließend abrufen und entwenden konnten. /ZDN15r01/

Direkte getroffene Maßnahmen

Neben der Entfernung der Schadsoftware von den IT-Systemen von Target sind keine weiteren Maßnahmen veröffentlicht worden.

Auswirkungen auf langfristige Maßnahmen

Target gab bekannt, dass es mit einem 100 Millionen Dollar Investitionsprogramm die IT-Sicherheit seines Unternehmens stärken will. Dazu gehören folgende Maßnahmen /ZDN15r01/:

[10] Random Access Memory, der Zufallszugriffsspeicher von IT-Systemen, auf welchem laufend Daten für schnelle Aufrufe vom Betriebssystem abgelegt werden.

- Bessere Beobachtung und Dokumentation von Systemaktivitäten
- Whitelisting für die IT-Systeme der Kassensysteme
- Managementsysteme für die Kassensysteme
- Neue Firewall-Regeln
- Limitierung oder Beendigung des Zugriffs von Zulieferern und Vertragspartnern auf das IT-Netzwerk von Target
- Die Privilegien von 445.000 Mitarbeiter- und Vertragspartneraccounts zurücksetzen, abschaffen oder reduzieren
- Verbreitung der Zwei-Faktor-Authentifizierung
- Training des Personals zum Passwortwechsel

Weiterhin wurden die Urheber des Angriffes strafrechtlich verfolgt und im Jahr 2018 wurde der identifizierte Haupturheber des Angriffes zu einer Freiheitsstrafe von 14 Jahren verurteilt /WAP18r01/.

2.2.3 Magecart

Übersicht

Der Begriff Magecart steht für einen spezifischen IT-Angriff über die Lieferkette, der dazu diente, von Webseiten Kundendaten, insbesondere Kreditkartendaten, zu entwenden. Hierbei werden Javascripte der Anbieter sowie von Drittanbietern auf Webseiten soweit manipuliert, dass der Datendiebstahl vollautomatisiert ohne Bemerkung des Kunden durchgeführt werden kann. Magecart Angriffe finden seit 2015 statt und wurden durch einen IT-Angriff auf die Fluggesellschaft British Airways bekannt, bei welchem im August und September 2018 Angreifer mittels Magecart die Namen, Rechnungsadressen, Emailadressen und Kreditkarteninformationen sowie teilweise CVV[11] Nummern von mindestens 380.000 Kunden über die Webseite und die App der Fluggesellschaft ausspähten. /STR18r01/

[11] CVV Nummern sind 3-stellige Zahlenfolgen auf der Rückseite von Kreditkarten und dienen als Sicherheitsidentifikationsmerkmal beim Onlinekauf mit Kreditkarten.

Beschreibung

Seit 2015 werden die Diebstähle von Kreditkartendaten beim Onlinehandel auf Magecart zurückgeführt. Zu den Opfern gehören unter anderem der Ticketverkäufer Ticketmaster und das Onlinegeschäft von Cancer Research UK. Größere Aufmerksamkeit erhielt der Angriff auf die Webseite und App der britischen Fluggesellschaft British Airways. Beginnend um 22:58 Uhr britischer Zeit am 21. August 2018 schalteten die Angreifer ein manipuliertes Javascript eines Drittanbieters auf der Webseite der Fluggesellschaft scharf. Um 21:45 Uhr britischer Zeit am 5. September 2018 wurde das manipulierte Javascript schließlich entfernt. Die Fluggesellschaft veröffentlichte eine Woche später, dass die Daten von ungefähr 380.000 Kunden gestohlen wurden. Am 29. Oktober 2018 berichtete die Fluggesellschaft, dass die Daten von 185.000 zusätzlichen Kunden, welche Kredit- und Debitkarten verwendeten, gestohlen wurden und dass bei 77.000 Kunden die Sicherheitszahl CVV entwendet wurde. Magecart wird darauffolgend immer wieder bei verschiedenen Onlinegeschäften entdeckt und konstant von Angreifern weiterentwickelt. Da Webseiten zur vollen Funktionalität eine zum Teil hohe Anzahl von Javascripten, insbesondere auch solche von Drittanbietern, benötigen, sind die Angriffsmöglichkeiten für Magecart Angriffe weiterhin umfangreich. Angriffe auf Unternehmen wie Ticketmaster oder Newegg verliefen nach ähnlichem Schema wie dem bei British Airways angewandten. /STR18r01/

Eingesetzte Schadsoftware

Bei IT-Angriffen mit Magecart werden von den Angreifern programmierte Javaskripte bzw. Teilskripte eingesetzt, welche häufig von den Angreifern in die Webseiten- bzw. Drittanbieterskripte integriert werden und infolge dessen bestimmte, von den Nutzern eingegebene Details wie Adressen oder Kreditkarteninformationen auslesen. Beim Angriff auf British Airways waren die Angreifer in der Lage, eine legitime Javaskript-Bibliothek zu modifizieren und ihren Schadcode zu dieser hinzuzufügen. Dadurch wurden sämtliche Daten bei der Zahlung auf der Webseite und in der App von den Angreifern ausgelesen. Die ausgelesenen Informationen wurden anschließend an eine Webadresse mit offiziell klingendem Namen weitergeleitet. Zur Verschleierung nutzten die Angreifer für die Webadresse ein legitimes SSL[12]-Zertifikat eines anerkannten Bezahlzertifizierer. /STR18r01/

[12] Secure Sockets Layer, ein Verschlüsselungsprotoll für den Datenverkehr

Direkte getroffene Maßnahmen

British Airways reagierte auf den Angriff nach Entdeckung mit der Beendigung der Nutzung des manipulierten Skripts. Weiterhin benachrichtigte die Fluggesellschaft die betroffenen Kunden sowie deren Kreditinstitute der kompromittierten Kredit- und Debitkarten. Weitere direkt getroffene Maßnahmen sind nicht bekannt. /STR18r01/

Auswirkungen auf langfristige Maßnahmen

Bisher wurden keine langfristigen Maßnahmen der betroffenen Unternehmen bekannt. Magecart Angriffe finden Stand Juni 2020 weiterhin statt, Sicherheitsunternehmen, Scriptanbieter und Magecart nutzende Angreifer befinden sich in einem konstanten Entwicklungswettbewerb. /RAP20r01/

2.2.4 Ccleaner Hack

Übersicht

Am 13. September 2017 veröffentlichten Analysten des IT-Sicherheitsunternehmens Cisco Talos die Warnung, dass die populäre Software Ccleaner, ein kostenloses Programm zur Optimierung von Betriebssystemen, mit Schadsoftware versehen und seit mehr als einem Monat in dieser Form auf der offiziellen Webseite des Herstellers herunterladbar ist. Insgesamt 2,27 Millionen Nutzer haben die manipulierte Version von Ccleaner heruntergeladen, ungefähr 1,65 Millionen IT-Systeme waren insoweit betroffen, dass dort die Schadsoftware an die C&C Server der Angreifer Daten sendete. Lediglich bei insgesamt 40 Systemen von elf verschiedenen Unternehmen wurden zusätzlich die in der Schadsoftware enthaltenen Funktionalitäten genutzt, um eine weitere Payload, die zweite Stufe der Schadsoftware, zu installieren. Dies führte anschließend zum Download und zur Installation der dritten Payload, der Schadsoftware Shadowpad. Insgesamt handelte es sich daher um einen sehr zielgerichteten IT-Angriff mit präzise definierter Zielgruppe. /WIR18r01/

Beschreibung

Der IT-Angriff über die Lieferkette mittels der Software Ccleaner begann am 11. März 2017. An diesem Tag erlangten die Angreifer erstmalig Zugriff auf die IT-Systeme des Herstellers von Ccleaner, Piriform.

Hierfür nutzten die Angreifer einen ihnen vorliegenden administrativen Zugriff über die bei Piriform eingesetzte Software TeamViewer, eine Software zur Steuerung und (Fern)Wartung externer PCs. Die Entwickler von Ccleaner vermuten, dass diese Daten bei einem früheren Angriff auf Piriform in Erfahrung gebracht wurden. In den nachfolgenden Tagen erweiterten die Angreifer ihren Zugriff auf verschiedene IT-Systeme im Netzwerk von Piriform und installierten ihre Schadsoftware Shadowpad auf diesen IT-Systemen, zu denen auch ein Build Server für die Software Ccleaner gehörte. Zwischen April und Juli 2017 arbeiteten die Angreifer anschließend an einer eigenen Version des Ccleaners, welche mit Schadsoftware manipuliert wurde. Am 18. Juli 2017 wurde Piriform von dem IT-Sicherheitsunternehmen Avast gekauft, insbesondere aufgrund von Ccleaner, welcher in seiner Geschichte über 2 Milliarden Mal heruntergeladen wurde. Am 2. August 2017 ersetzten die Angreifer dann die auf den Servern von Avast vorliegende Ccleaner-Version mit der mit Schadsoftware manipulierten Version des Ccleaners. Am 13. September 2017 entdeckten die Analysten von Cisco Talos die manipulierte Version und informierten Avast, welche die Version sofort aus dem Netz nahmen. Bis dahin hatten 2,27 Millionen Nutzer die manipulierte Version heruntergeladen. In Zusammenarbeit mit der amerikanischen Bundespolizei FBI konnte Avast am 16. September 2017 die Command and Controlserver (C&C Server) der Schadsoftware abschalten und die 40 IT-Systeme identifizieren, welche von der zweiten Stufe der Schadsoftware und damit wahrscheinlich auch von Shadowpad betroffen waren. /WIR18r01/

Eingesetzte Schadsoftware

Im Falle der manipulierten Ccleaner Versionen wurde eine eigens entwickelte Schadsoftware eingesetzt, welche dazu diente, die betroffenen IT-Systeme und ihre Besitzer zu identifizieren und im gewünschten Fall die umfassende Schadsoftware Shadowpad nachträglich zu installieren. Die erste Payload wurde mittels einer legitimen DLL des CCleaner an die Nutzer ausgeliefert. Wird diese Payload ausgeführt, wird die erste Stufe der Schadsoftware installiert, wobei die zweite Stufe der Schadsoftware verschlüsselt in der DLL verbleibt. Die erste Stufe der Schadsoftware sammelt eine Reihe von Daten über das betroffene IT-System und sendet diese in regelmäßigen Abständen an einen C&C Server, welcher als Aktivierungsserver genutzt wird. Der Aktivierungsserver sendet unter bestimmten, bisher nicht genau bekannten Umständen, einen Entschlüsselungsschlüssel als Antwort an das betroffene IT-System zurück. Infolgedessen entschlüsselt die Schadsoftware die in der DLL enthaltende zweite Payload und installiert diese. Die zweite Stufe der Schadsoftware ermöglich die Kommunikation mit einem weiteren C&C Server der Angreifer.

Von dort soll anschließend die Shadowpad Schadsoftware als dritte Stufe heruntergeladen werden. Shadowpad selbst ist ein umfassendes Kontroll- und Überwachungssystem mit Funktionen zum Protokollieren sämtlicher Eingaben in verschiedenen Programmen wie Mozilla Firefox, Google Chrome oder Microsoft Word, das Auslesen von Passwörtern und die Übernahme des betroffenen IT-Systems. Neuere Versionen von Shadowpad sind modular aufgebaut und ermöglichen das zielgerichtete Laden von Modulen der Schadsoftware. Nach bisherigen Erkenntnissen verschickte der Aktivierungsserver insgesamt 40 Aktivierungsbefehle für die zweite Stufe der Schadsoftware. Die betroffenen IT-Systeme gehören zu 11 verschiedenen Unternehmen, unter anderem Google, Cisco, Intel, Samsung oder Gauselmann. /INS18r01/

Direkt getroffene Maßnahmen

Die mit Schadsoftware versehene Version des CCleaner wurde von den bereitstellenden Servern entfernt. Die C&C Server der Schadsoftware wurden mit Hilfe des FBI abgeschaltet. Bekanntgewordene Virensignaturen der Schadsoftware wurden mit den Berichten von Analysten eines IT-Sicherheitsunternehmens öffentlich und anschließend in Antivirenprogramme aufgenommen. Weitere Maßnahmen sind nicht bekannt. /WIR18r01/

Auswirkungen auf langfristige Maßnahmen

Avast selbst gibt bekannt, dass die größte Erkenntnis für sie der Umgang mit der IT-Sicherheit bei Unternehmensübernahmen war. Weiterhin führen sie aus, dass wo früher hauptsächlich auf legale, patentrechtliche und finanzielle Fragen im Fokus standen, in Zukunft auch die IT-Sicherheit zu einem wichtigen Thema werden solle. Weitere langfristige Maßnahmen wurden bisher nicht veröffentlicht. /WIR18r01/

2.2.5 Kingslayer

Übersicht

Am 30. Juni 2016 wurde ein Schadsoftwarefund in der Software Evlog des kanadischen Unternehmens Altair Technologies Ltd. bekannt. Bei Evlog handelt es sich um eine Software, welche Systemadministratoren dabei unterstützt, die auflaufenden Meldungen von Microsoft Windows auszulesen und zu bearbeiten. Anfang 2015 waren die Angreifer in der Lage, einen Zertifizierungsschlüssel für Evlog zu erlangen und somit die Echtheit einer mit Schadsoftware versehenden Version von Evlog vorzutäuschen.

Die manipulierte Software wurde vom 9. April bis zum 25. April 2015 auf der Webseite von Altair angeboten. Nutzer der Software berichten im Nachhinein von der Kompromittierung ihrer IT-Netzwerke unter Verwendung der in Evlog beinhalteten Schadsoftware bis zum August 2015. Mitte 2016 wurde der Lieferkettenangriff schließlich entdeckt und forensisch untersucht. Zu den bisher bekannten Opfern des Lieferkettenangriffes gehören vier große Telekommunikationsanbieter, mehr als zehn westliche Militärorganisationen, fünf große Vertragsnehmer des amerikanischen Verteidigungsministeriums, 36 große IT-Produkt- oder Serviceanbieter, 24 westliche Regierungsorganisationen, mehr als 24 Banken und mindestens 45 Universitäten. /COM17r01/ /KOS17r01/

Beschreibung

Nach bisherigen Erkenntnissen gelang es den Angreifern im Frühjahr 2015, den Zertifizierungsschlüssel des Herstellers der Software Evlog zu stehlen. Am 17. März 2015 registrierten die Angreifer die erste, legitim erscheinende Webadresse. Am 31. März 2015 nutzten sie den gestohlenen Zertifizierungsschlüssel, um die manipulierte Version der Software Evlog zu zertifizieren. Am 9. April 2015 wurde die manipulierte Version auf einer Update Webseite von Altair bereitgestellt, welche u. a. dann am 22. April 2015 von einem Systemadministrator eines Vertragsunternehmens des amerikanischen Verteidigungsministeriums heruntergeladen wurde. Am 26. April 2015 wurde die manipulierte Version von Evlog vom Updateserver entfernt, es ist nicht bekannt warum und von wem diese Entfernung durchgeführt wurde. Das oben genannte Unternehmen aus dem Verteidigungssektor wurde am 15. Juli 2015 sowie am 17. August 2015 nachweislich von den IT-Angreifern über die Schadsoftware, die mit Evlog verteilt wurde, angegriffen. Am 17. April 2016 begannen Analysten mit der forensischen Analyse des Angriffs auf dieses Unternehmen, woraufhin am 30. Juni 2016 eine Sicherheitswarnung des Herstellers herausgegeben wurde. Aufgrund der gerichtlich angeordneten Übernahme der Webseite am 14. Juli 2016, welche die Schadsoftware zum Nachladen von Schadcode nutzte, konnten die weiteren betroffenen Unternehmen ermittelt) und kontaktiert werden. Das Vertragsunternehmen des U.S. Verteidigungsministeriums begann am 5. August 2016 mit Gegenmaßnahmen. Zu den weiteren betroffenen Unternehmen zählen unter anderem 3M, FedEx, Northrop Grumman, Symantec, Citigroup, Paypal, die BBC und der U.S. Marshals Service. /KOS17r01/ /COM17r01/

Eingesetzte Schadsoftware

Die in die Software Evlog integrierte Schadsoftware Kingslayer führte bei Ausführung dazu, dass von einer legitim erscheinenden Webseite weiterer Schadcode heruntergeladen wurde. Hierdurch konnte die Menge an Schadcode in der manipulierten Software stark verkürzt gehalten werden und wurde daher von gängigen Antivirenprogrammen initial nicht entdeckt. Da die Software Evlog als Unterstützung für Systemadministratoren verwendet wird, erlangten die IT-Angreifer mit Hilfe der Schadsoftware Kingslayer auf diesem Wege umfangreiche Administratorrechte im infizierten Netzwerk. In weiteren Schritten verbreitete sich die Schadsoftware im betroffenen Netzwerk und lud weiteren Schadcode nach, darunter die Etablierung eines vollständigen lokalen C&C-Servers sowie weitere Fähigkeiten zum Stehlen von Passwörtern und sensiblen Daten. /COM17r01/

Direkt getroffene Maßnahmen

Es ist bisher nicht bekannt, ob die Entfernung der mit der Schadsoftware Kingslayer manipulierten Version von Evlog vom 26. April 2015 absichtlich passierte oder ein Zufall war. Ebenfalls ist die Urheberschaft dieser Entfernung nicht bekannt. Die ersten direkten Maßnahmen wurden von beteiligten IT-Sicherheitsunternehmen durchgeführt, welche den IT-Angriff über die Softwarelieferkette forensisch analysierten und sich per Gerichtsbeschluss die von den Angreifern genutzte Webseite aneigneten. Daraufhin konnten die betroffenen Unternehmen ermittelt und gewarnt werden und der Hersteller von Evlog einen Sicherheitshinweis herausgeben. /KOS17r01/

Auswirkungen auf langfristige Maßnahmen

Bisher sind keine langfristigen Maßnahmen der betroffenen Unternehmen bekannt geworden.

2.2.6 Operation Red Signature

Übersicht

Im August 2018 veröffentlichte Trend Micro Incorporated, ein international agierender japanischer Softwareanbieter und Experte für Serversicherheit, in Zusammenarbeit mit der südkoreanischen Expertengruppe für Schadsoftwareanalysen und Cyber-Security, IssueMakersLab, einen Bericht über die sogenannte „Operation Red Signature“. Dabei handelt es sich um einen lieferkettenbasierten Angriff mit dem Ziel des Diebstahls von Informationen von Firmen und Organisationen in Südkorea. Durch den kompromittierten Update-Server eines Anbieters für Fernwartungssoftware gelangte die Schadsoftware über den Update-Mechanismus in das jeweilige System. /TRM18r01/

Beschreibung

Der in Operation Red Signature durchgeführte Angriff begann mit dem Diebstahl des Signierungszertifikats der Fernwartungssoftware. Nach Angaben von Trend Micro könnte dies bereits im April 2018 geschehen sein, da am 8. April 2018 eine andere Schadsoftware, signiert mit dem gestohlenen Zertifikat, entdeckt wurde. Das bereitgestellte, kompromittierte Update der Fernwartungssoftware wurde mit dem gestohlenen Zertifikat signiert und auf einen Server der Angreifer hochgeladen. Laut Trend Micro wurde die Schadsoftware am 17. Juli 2018 kompiliert.

Anschließend wurde der Update-Server des Unternehmens der Fernwartungssoftware gehackt und so konfiguriert, dass die Datei „update.zip“ vom Server der Angreifer abgerufen wird, wenn sich ein Client mit einer IP-Adresse aus dem IP-Adressbereich bestimmter Organisationen in Südkorea verbindet. Die genannte Datei wurde entsprechend an die Clients gesendet, sobald die Fernwartungssoftware ausgeführt wurde, welche das Update als normal erkannte und die darin enthaltene Schadsoftware ausführte. Diese wiederum lud weitere Schadsoftware vom Server der Angreifer nach und führte sie aus. Die Angreifer konfigurierten die Schadsoftware derart, dass der Angriff am 18. Juli 2018 startete und zeitlich begrenzt bis zum 31. Juli 2018 fortgeführt werden sollte. Ende Juli 2018 entdeckten Trend Micro und IssueMakersLab die Angriffe und veröffentlichten Informationen hierzu am 21. August 2018.

Eingesetzte Schadsoftware

Bei der Schadsoftware, die im Rahmen des kompromittierten Updates der Fernwartungssoftware heruntergeladen wurde, handelt es sich um einen Remote Access Trojaner namens RAT 9002. Die kompromittierte Datei „update.zip“ beinhaltete die Datei „update.ini“, welche die Konfiguration zum Herunterladen der zwei Dateien „file000.zip“ und „file001.zip“ enthielt. Diese wurden als „rcview40u.dll“ und „rcview.log“ in den Installationsordner der Fernwartungssoftware extrahiert, woraufhin die Schadsoftware ausgeführt wurde.

Mit Hilfe dieser Backdoor wurde weitere Schadsoftware vom Server der Angreifer heruntergeladen und ausgeführt. Dabei handelt es sich um eine Vielzahl von Dateien und Programmen, unter anderem „WebBrowserPassView“, einem Werkzeug um in Browsern gespeicherte Passwörter wiederherzustellen, „printdat.dll“, einem weiteren Remote Access Trojaner, „Sharphound“, einem Werkzeug, um Informationen über Verzeichnisse zu sammeln sowie weiterer schadhaft wirkender Programme.

Direkte getroffene Maßnahmen

Direkt betroffene Maßnahmen sind bisher nicht bekannt.

Auswirkungen auf langfristige Maßnahmen

Bisher sind keine langfristigen Maßnahmen bekannt geworden.

2.2.7 MediaGet

Übersicht

Im März 2018 berichtete Microsoft von einem Schadsoftwarebefall bei rund 400.000 Nutzern innerhalb weniger Stunden überwiegend in Russland, der Türkei und der Ukraine. Ein laut Microsoft hochentwickelter Trojaner gelangte mutmaßlich über den Filesharing-Client „MediaGet“ des BitTorrent Filesharing-Protokolls auf die Rechner der Nutzer und installierte einen Krypto-Miner. Beim illegalen Krypto-Mining installieren Angreifer unbemerkt eine spezielle Software auf dem Rechner des Opfers, die dann Krypto-Währung für sie generiert, indem sie die Rechenleistung des Rechners zur Transaktionsverarbeitung, Absicherung und Synchronisierung der Nutzer im Netzwerk ausnutzt.

Die Opfer merken oftmals nichts von dem Angriff und den auf ihren Rechnern ausgeführten Prozessen. Die Software MediaGet wird von Microsoft als potenziell unerwünschte Anwendung eingestuft. Obwohl File-Sharing-Programme häufig für die Verbreitung von Schadsoftware benutzt werden, war der Befall in diesem Fall jedoch nicht auf Downloads innerhalb des Torrent-Netzwerks mit MediaGet zurückzuführen. Vielmehr wurde die Schadsoftware über den kompromittierten Update-Server der russischen Entwickler von MediaGet verteilt. /MSS18r02/

Beschreibung

Nach Angaben von Microsoft begannen die Täter mit den Vorbereitungen des Angriffs bereits Mitte Februar 2018 durch die Kompromittierung des Update-Servers von MediaGet. Der Befehl zur Aktivierung der Schadsoftware wurde ab dem 1. März 2018 gegeben und am 6. März 2018 wurde die massenhafte Vermehrung und Aktivierung von Microsoft bemerkt, wobei nach Angaben von Microsoft die Windows Defender Antivirus-Software über 80.000 Instanzen des Trojaners an diesem Tag registrierte und blockierte. Innerhalb der nächsten 12 Stunden wurden bereits über 400.000 Instanzen registriert.

Innerhalb einiger Millisekunden wurde der Angriff von cloudbasierten Machine-Learning-Modulen des Windows Defenders geblockt und nach wenigen Minuten wurde das Microsoft Defender ATP Research Team alarmiert. Am 7. März 2018 wurde eine entsprechende Sicherheitswarnung veröffentlicht und am 13. März 2018 folgte eine ausführliche Meldung nach eingehender Analyse des IT-Sicherheitsvorfalls und der Schadsoftware durch Microsoft. /MSS18r02/

Eingesetzte Schadsoftware

Bei der eingesetzten Schadsoftware handelt es sich laut dem Microsoft Defender ATP Research Team um die Schadsoftware „Dofoil“ (auch bekannt als „Smoke Loader“), die sich mit einem externen Server verbindet und beliebige weitere Schadsoftware herunterladen und ausführen kann. Im betrachteten Fall wurde ein Krypto-Miner für die Electroneum-Währung installiert.

Microsoft bezeichnete den Angriff als sorgfältig geplant, da die unbekannten Täter die Schadsoftware bereits zwei Wochen vor dem Angriff auf dem Server des russischen Entwicklers von MediaGet platziert hatten.

Die signierte „mediaget.exe“-Datei des offiziellen Update-Servers lud dabei die ebenfalls signierte Datei „update.exe“ herunter, die wiederum die nicht signierte Datei „mediaget.exe“ installierte. Diese Datei funktioniert wie die Originaldatei, beinhaltet zusätzlich allerdings eine Backdoor.

Microsoft vermutet, dass die Datei „update.exe“ mit einem gestohlenen Zertifikat eines Dritt-Softwareherstellers signiert wurde, da die legitime Datei „mediaget.exe“ eine signierte Datei „update.exe“ voraussetze. Die mit dem Trojaner behaftete Datei „mediate.exe“ stimmte zu 98% mit der Originaldatei überein. /MSS17r01/

Direkt getroffene Maßnahmen

Die direkt getroffenen Maßnahmen erfolgten in diesem Fall zunächst durch automatisierte, cloudbasierte Anwendungen, die durch maschinelles Lernen von Microsoft speziell für diese Fälle sich schnell ausbreitender Schadsoftware entwickelt wurden. Dadurch wurden die ersten Gegenmaßnahmen bereits innerhalb der ersten Millisekunden getroffen. Nachdem Microsoft den Angriff erkannt hatte, wurden unmittelbar Untersuchungen eingeleitet und die betroffene Software MediaGet identifiziert. Microsoft trat mit den Entwicklern von MediaGet in Kontakt, um Ihnen bei der Analyse des Vorfalls zu helfen und gaben Einzelheiten über die unrechtmäßige Verwendung des in „update.exe“ verwendeten Zertifikats an den Zertifikatsinhaber weiter.

Auswirkungen auf langfristige Maßnahmen

Bisher sind keine langfristigen Maßnahmen der Entwickler von MediaGet bzw. des Zertifikatsinhabers bekannt geworden. Die Software MediaGet wird von Microsoft weiterhin als potenziell unerwünschte Anwendung eingestuft.

2.2.8 Weitere bekanntgewordene Attacken

Zahlreiche weitere IT-Angriffe über die Lieferkette mit geringen Auswirkungen, Relevanz oder verfügbaren Informationen sind in den letzten zehn Jahren bekannt geworden. Ausgewählte Angriffe werden nachfolgend kurz beschrieben.

Web Developer und weitere Browserplugins

Im Jahr 2017 wurde bekannt, dass eine Reihe von Erweiterungen für den weit verbreiteten Browser Google Chrome mit Schadsoftware versehen waren. Insgesamt 4,8 Millionen Nutzer waren von diesem IT-Angriff betroffen, welcher die Softwarelieferkette nutzte. Die Angreifer nutzten Phishing-E-Mails, um Zugriff auf die Browsererweiterungen zu bekommen und luden dann mit Schadsoftware versehene Versionen dieser hoch. Durch automatische Updates wurde die Schadsoftware an die Nutzer der Erweiterungen verteilt. /WOF17r01/

Die Angreifer zielten darauf ab, Webseitenaufrufe und Werbeaufrufe umzuleiten um somit über eigene Werbeanzeigen und Affiliate-Links[13] Geld zu verdienen. Insbesondere die an Webseitenentwickler gerichtete Erweiterung Web Developer war für die Angreifer interessant, da die Schadsoftware darauf ausgerichtet war, die Passwörter der Nutzer bei einem spezifischen Webdienstleister auszulesen und nachfolgend die Webseiten der Nutzer ebenfalls zu übernehmen. /WOF17r01/

Weiterer Shadowpad Angriff

Ein weiterer IT-Angriff mit der Schadsoftware Shadowpad erfolgte unter der Nutzung eines Server Management Systems des Unternehmens NetSarang und wurde wie der Angriff mittels des CCleaners 2017 bekannt. Infolge von Updates wurde eine Schadsoftware innerhalb einer legitimen DLL an die Nutzer ausgeliefert, wodurch die betroffenen Systeme kompromittiert wurden und anschließend bei mindestens einem bestätigten Fall die Schadsoftware Shadowpad installiert wurde. /ZDN17r01/

PDF-Reader

Microsoft veröffentlichte im Jahr 2018 einen Bericht über einen bis dahin unbekannten IT-Angriff über eine mehrstufige Softwarelieferkette. Hierbei wurde eine nicht genannte Drittanbietersoftware innerhalb eines nicht genannten PDF-Readers mit Schadsoftware versehen. Die Installation des PDF-Readers funktioniert so, dass hierbei direkt vom Server des Drittanbieters für den Betrieb des Readers notwendige Software mitheruntergeladen wird.

[13] Affiliate Links sind spezielle Verlinkungen im Internet, über die Besitzer der Verlinkungen durch die Nutzung der Links Geld verdienen können.

Dadurch bemerkte der Anbieter des Readers nicht, dass in die Drittanbietersoftware eine Schadsoftware des Typs Cryptominer[14] integriert wurde, welcher bei den Anwendern des PDF-Readers die Rechnerressourcen des betroffenen Systems zur Generierung von Digitalwährungen nutzt. Nach der Informierung des Anbieters des PDF-Readers erkannte dieser die Problematik und konnte mit seinem Zulieferer die Schadsoftware aus den Installationsdateien entfernen. /MSS18r01/

Equifax Breach

Bei Equifax handelt es sich um eine amerikanische Wirtschaftsauskunftei ähnlich der deutschen Schufa. Im September 2017 gab diese bekannt, dass ihr annähernd 148 Millionen Datensätze zu Personen aus den USA, Kanada und Großbritannien von Angreifern zwischen Mai und Juli 2017 entwendet wurden. Um Zugriff auf die Daten von Equifax zu erhalten, nutzten Angreifer eine seit März 2017 bekannte kritische Sicherheitslücke in der von Equifax genutzten Software Apache Strux, für welche ein Sicherheitsupdate bereitstand, welches von Equifax jedoch nicht genutzt wurde. Infolge des IT-Angriffes erbeuteten die Angreifer umfassende Daten zu Sozialversicherungsnummern, Führerscheinnummer, Namen, Adressen und weiteren Informationen, die Equifax über Verbraucher in den USA, Kanada und dem Vereinigten Königreich sammelt. /CSO17r01/

Dominos Breach

Im Jahr 2017 wurden Kunden des Pizzafranchiseunternehmens Dominos in Australien Opfer verschiedener Spamangriffe. Kunden, die Dominos hiermit konfrontierten, machten das Unternehmen auf ein Datenleck aufmerksam, welches sich durch einen ehemaligen IT-Dienstleister ergeben hatte. Infolge dessen konnten IT-Angreifer über die Lieferkette die Adressdaten, Emailadressen, Namen, Telefonnummern und Bestellfavoriten der Kunden von Dominos ausspähen und damit handgefertigte, echt wirkende Spamnachrichten an die Kunden verteilen. /FOR17r01/

[14] Ein Cryptominer ist eine Software zur Errechnung von Digitalwährungen.

Magento

2018 wurde bekannt, dass eine große Anzahl an E-commerce Webseiten weltweit Schadsoftware an die Benutzer verteilten und die Kreditkartendaten der Nutzer an Angreifer weitergaben. Die Zahl der betroffenen Webseiten nahm im Verlauf des Jahres 2019 noch einmal deutlich zu. Es stellte sich heraus, dass Magento, eine populäre open source Software für E-commerce Anwendungen, eine Reihe bekannter Standardpasswörter nutzt, wenn die Anwender die Passwörter bei der Installation nicht ändern. Dadurch erlangten die Angreifer vollen Zugriff auf die spezifischen Magentoanwendungen der betroffenen Webseiten und konnten ihren Schadcode über die Webseiten an die Kunden verbreiten. /ZDN19r01/

Heartbleed Bug

Der Heartbleed genannte Softwarefehler der Software OpenSSL war einer der schwerwiegendsten Softwarefehler des Jahres 2014. Im Normalfall kommunizieren ein OpenSSL nutzender Server und ein von Nutzern bedienter Client periodisch miteinander, auch wenn der Anwender keine weiteren Daten anfragt. Dabei sendet der Client eine spezifische Menge Daten und gibt an, dass er als Antwort eine spezifische Menge Daten zurückbekommen soll. Durch den Heartbleed Fehler ist es für Clients möglich, vom Server eine so große Menge Daten zurückzuverlangen, dass dieser eigentlich unzugängliche Bereiche seines RAM Speichers ausliest und zurückschickt. Infolge dessen erlangt der anfragende Client Informationen wie z. B. Accountdetails und Passwörter anderer Accounts, welche im Speicher des Servers zwischengespeichert sind. 17 % aller weltweit eingesetzten SSL Server nutzten 2014 OpenSSL und waren damit durch diesen Fehler verwundbar; dazu gehörten z. B. große Anbieter wie Yahoo. /ENG18r01/

Verizon Breach

2017 wurde das amerikanische Telekommunikationsunternehmen Verizon Opfer eines IT-Angriffs über seine Lieferkette. Ein zur Kundenbetreuung von Verizon beauftragtes Dienstleistungsunternehmen speicherte seine Daten ungeschützt auf den Servern des Webcloudanbieters Amazon. Angreifer entwendeten die Daten von insgesamt 14 Millionen Kunden Verizons. /ZDN17r02/

Pypi

Pypi, kurz für Python Package Index, dient als offizielle Sammlung für Drittanbieterbibliotheken für die Programmiersprache Python. In den vergangenen Jahren wurde mehrfach Bibliotheken mit Schadsoftware auf Pypi gefunden. Da es keine initiale Untersuchung der Bibliotheken auf Pypi gibt, ist davon auszugehen, dass deutlich mehr Bibliotheken als die bisher entdeckten betroffen sind. Nutzen Anwender von Python diese Bibliotheken, kann Schadcode in die von den Anwendern programmierte Software einfließen und weiterverbreitet werden. /ZDN18r01/

Eurofins Ransomware Befall

Eurofins ist eines der größten Labordienstleistungsunternehmen in Europa. Im Jahr 2019 wurde Eurofins Opfer eines IT-Angriffs, wodurch dessen IT-Systeme von einem Verschlüsselungstrojaner befallen wurden. Dadurch konnte Eurofins seine Dienstleistungen nicht mehr unbeeinträchtigt durchführen, was z. B. dazu führte, dass die britische Polizei ihre forensischen Analysen von anderen Laboren durchführen lassen musste und sich dadurch Gerichtsprozesse verzögerten. Ca. drei Wochen nach Bekanntwerden des Falls zahlte Eurofins 1,1 Millionen Dollar an die Erpresser um die Entschlüsselung der eigenen Daten durch die Angreifer zu bewirken. /HEI19r01/

Avast Breach 2019

Der Hersteller für Antivirensoftware Avast gab im Jahr 2019 bekannt, dass er Opfer eines versuchten Lieferkettenangriffes wurde. Die Angreifer zielten wieder auf das Produkt CCleaner von Avast ab, welches weltweit mehrere Milliarden Mal heruntergeladen wurde. Die Angreifer erlangten Zugriff auf das interne Netz von Avast mittels eines VPN Zugangs, dessen Zugangsdaten die Angreifer auf bisher unbekanntem Wege in Erfahrung brachten. Im Netzwerk von Avast eskalierten sie erfolgreich ihre Privilegien und versuchten Zugriff auf die Installationsdaten des CCleaners zu erlangen. Avast stoppte die Angreifer, nachdem das Ziel der Angreifer offensichtlich wurde und beendete deren Zugriff. /HNS19r01/

Wipro Breach

2018 gab die indische Beratungsfirma Wipro bekannt, dass sie Opfer eines IT-Angriffes wurde. Infolge einer Phishingkampagne erlangten Angreifer Zugriff auf die Systeme von Wipro und entwendeten Kundendaten. Die Angreifer nutzten anschließend die entwendeten Daten, um weitere Phishingkampagnen zielgerichtet auf die Kunden von Wipro durchzuführen. /KOS18r01/

DigiNotar

Im Jahr 2011 wurde ein Angriff auf die niederländische Zertifizierungsstelle DigiNotar bekannt. Zertifizierungsstellen für digitale Zertifikate (*certification authority*, CA) sind Organisationen, die digitale Zertifikate herausgeben, die dazu dienen, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Die Zertifizierungsstelle beglaubigt die Zuordnung durch die eigene digitale Unterschrift und trägt die Verantwortung für die Bereitstellung, Zuweisung und Integritätssicherung der von ihr ausgegebenen Zertifikate. Die Einsatzmöglichkeiten von digitalen Zertifikaten sind vielfältig und erstrecken sich in der alltäglichen Nutzung des Internets beispielsweise auf verschlüsselte Verbindungen zwischen einem Webbrowser und einem Webserver oder die Verschlüsselung und Signierung von E-Mails.

Im August 2011 berichtete ein nach eigenen Angaben im Iran lebender Nutzer von Google Mail, dass sein Browser beim Aufruf der SSL-gesicherten Google Mail-Seite einen Zertifikatsfehler meldete. Entscheidend für die Entdeckung dieses Falls ist, dass der Nutzer den Google-eigenen Chrome-Browser verwendete, der durch erweiterte Sicherheitsfunktionen nicht nur prüft, ob das Webseiten-Zertifikat gültig ist, sondern auch, ob es von der richtigen Zertifizierungsstelle stammt. Das von DigiNotar ausgestellte Zertifikat für die Google-Domains wurde durch Angreifer manipuliert. Nach Angaben der Electronic Frontier Foundation wurde das kompromittierte Zertifikat wahrscheinlich von der iranischen Regierung verwendet, um Nutzer von Google Mail zu überwachen. /TRP12r01/

ESTsoft/ALZip

Ein großangelegter Angriff auf den südkoreanischen Softwarehersteller ESTsoft fand im August 2011 statt. Angreifer mit einer chinesischen IP-Adresse platzierten Schadsoftware auf einem Updateserver des hauptsächlich in Korea und Japan verbreiteten Datenkompressionsprogramms ALZip. Die Schadsoftware gelangte unter anderem auf 62 Computer des südkoreanischen Unternehmens SK Communications, das Internet- und Telefonanschlüsse für Privatnutzer und Firmen in Südkorea anbietet, sowie das Internetportal Nate betreibt, welches im Rahmen eines sozialen Netzwerks und als Instant-Messenger mehrere Millionen Nutzer aufweist. Die Angreifer hatten dadurch Zugriff auf persönliche Daten von 35 Millionen Nutzern in Südkorea, inklusive Name, Benutzer ID, gehashte Passwörter, Geburtsdaten, Geschlecht, Telefonnummern, Adressen und E-Mail-Adressen. /TRE11r01/

Operation WilySupply

Am 4. Mai 2017 veröffentlichte das Microsoft Defender ATP Research Team eine Meldung über einen als „Operation WilySupply“ bezeichneten Angriff. Die Angreifer nutzten dazu den Update-Mechanismus eines nicht benannten Bearbeitungstools und zielten überwiegend auf Organisationen im Finanzbereich und der Bezahlindustrie ab. Dabei wurden Teile des Trojaners „Win32/Rivit.A!dha“ auf den Zielsystemen platziert, welcher im Kombination mit der Meterpreter Reverse Shell PowerShell-Skripte ausführte, die den Angreifern unbemerkt die Kontrolle über das System ermöglichten. Laut Microsoft wurde der Angriff finanziell motiviert gezielt durchgeführt und beschränkte sich, obwohl eine größere Anzahl an Systemen betroffen war, auf bestimmte, nicht näher genannte Organisationen. /MSS17r01/

SimDisk

Im Juni 2013 berichtete Trend Micro, dass Südkorea aufgrund mehrerer Vorfälle, die verschiedene Regierungs- und Nachrichtenwebsites in Südkorea betrafen, den Cyber-Sicherheitsalarm des Landes von Stufe 1 auf Stufe 3 erhöht habe. Dabei betraf ein Angriff unter anderem den Auto-Update-Mechanismus der Software SimDisk, einem südkoreanischen File-Sharing-Programm und Speicherdienst. Die Software ist so konfiguriert, dass sie automatisch Updates von einem bestimmten Server herunterlädt.

Dieser wurde jedoch von Angreifern mit einer modifizierten Version kompromittiert, die eine Kopie des legitimen Programms enthielt, und außerdem einen Trojaner (TROJ_DIDKR.A) platzierte, der sich mit dem Tor-Netzwerk – einem Netzwerk zur Anonymisierung von Verbindungsdaten – verbindet. /TRM13r01/

3 Bedeutungszuwachs der IT-Sicherheit in der Lieferkette

IT-Angriffe über die Lieferkette haben für das Sicherheitsverständnis der Betroffen und die Angriffsmöglichkeiten der Angreifenden in den letzten 10 Jahren erheblich an Bedeutung gewonnen. Verschiedene Studien und Erhebungen der Betroffenen in den letzten Jahren zeigen einen konstanten Anstieg des Anteils der Lieferkettenangriffe an den wahrgenommenen Informationssicherheitsvorfällen. /POE17r01/

So veröffentlichte das Ponemon Institute LLC im September 2017 einen umfassenden Forschungsreport zu Informationssicherheitsvorfällen, für welchen mehr als eintausend Einzelpersonen[15] mit Aufgabenbereichen in der Informationssicherheit kontaktiert und befragt wurden. Aus diesem und den gegebenen Antworten des Jahres 2016 entwickelte Ponemon folgende zentrale Aussagen:

- 56 % der Organisationen[16] der befragten Personen sind 2017 von Datenverlusten durch Drittanbieter betroffen gewesen. Hierbei sind sowohl Datenverluste aufgrund von IT-Angriffen als auch Datenverluste aufgrund anderer Ursachen enthalten. 2016 waren es noch 49 %.
- 42 % der Organisationen der befragten Personen sind 2017 Opfer von Datenverlusten aufgrund von IT-Angriffen auf Drittanbieter geworden, 2016 waren dies 34%.
- 75 % der Befragten gaben an, dass die Anzahl der IT-Angriffe über die Lieferkette zunehme, 2016 sagten dies 73 %.
- 42 % der Befragten gaben an, dass ihre Organisationen effektiv in der Erkennung von Drittanbieterrisiken sind, jedoch nur 12 % in der Erkennung von Risiken von mehrgliedrigen Lieferketten.
- Während 2016 noch 22 % der Befragten angaben, dass ihre Organisationen effektiv in der Reduzierung von Drittanbieterrisiken durch IT-Angriffe sind, gaben dies 2017 nur noch 17 % der Befragten an.

---

[15] Die Aufteilung der Personen in Verantwortungsbereiche wird folgend angegeben: 5 % Senior Executive, 2 % Vizepräsidenten, 17 % Direktoren, 21 % Manager, 14 % Supervisor, 36 % Staff, 5 % Contractor

[16] Die Unternehmen teilen sich in folgende Bereiche auf: 18 % Finanzen, 12 % Service, 11 % Gesundheit, 10 % Öffentlicher Dienst, 9 % Industrie, 7 % Verkauf, 6 % Energie, 6 % Technologie und Software, 4 % Kommunikation, 4 % Gaststätten- und Hotelgewerbe, 4 % Transport, 3 % Konsumgüter, 2 % Bildung, 4 % Verschiedene

- 2016 gaben 21 % der Befragten an, dass in ihrem Unternehmen keine Person für Informationsrisiken über die Lieferkette verantwortlich ist, 2017 ging diese Zahl auf 16 % zurück.
- 2017 gaben 35 % der Befragten an, dass ihrem Unternehmen alle Drittanbieter mit Zugriff auf sensible Unternehmensdaten bekannt seien und 31 % gaben an, dass ihr Unternehmen informiert wird, wenn Drittanbieter sensible Daten des Unternehmens mit weiteren Teilgliedern der Lieferkette teilen.

In einer Befragung von VansonBourne im July 2018 von 1300 mit Informationssicherheit befassten Personen in Unternehmen und Sicherheitsdienstleistern gaben 66 % der befragten an, dass sie mindestens einen Lieferkettenangriff erlebt haben, davon 32 % innerhalb der letzten 12 Monate. 90 % der Befragten gaben an, dass aufgrund des erlebten Lieferkettenangriffs ein finanzieller Schaden davongetragen wurde. Trotz dieser Zahlen geben nur 33 % der befragten Personen an, dass ihre Organisation Lieferkettenangriffe als eines der drei wichtigsten Informationssicherheitsrisiken ansieht. /VAB18r01/

Eine im April 2019 von Carbon Black herausgegebene Studie ergab, dass von 40 Partnern des Sicherheitsunternehmens die Hälfte der Befragten angaben, dass behandelte und beobachtete Informationssicherheitsvorfälle mit der Lieferkette zusammenhängen. /CAB19r01/

Nach Angaben von Statista wurden Ende des Jahres 2019 über 5.000 Informationssicherheitsspezialisten befragt, ob und in welcher Form ihre Unternehmen im Jahr 2019 von mit der Lieferkette im Zusammenhang stehenden IT-Angriffen betroffen waren. Dabei gaben 66 % der 1000 in Deutschland arbeitenden Personen an, dass ihr Unternehmen 2019 von einem IT-Angriff mit Bezug zur Lieferkette betroffen war. Der Höchstanteil von IT-Angriffen mit Bezug zur Lieferkette wurde dabei von befragten Personen aus Belgien mit 73 % der Unternehmen angegeben und der geringste Anteil mit 60 % im Vereinigten Königreich. /STA20r01/

4 Fazit

In den vergangenen Jahren wurde eine Vielzahl von weltweit durchgeführten IT-Angriffen auf Unternehmen, Organisationen und auch sicherheitskritische Einrichtungen beobachtet, die mit der Lieferkette von IT-Systemen zusammenhängen. Auch kerntechnische Anlagen national und international sind in der Vergangenheit bereits betroffen gewesen. Diese Form der Angriffe über die IT-Lieferkette hat insbesondere aufgrund der Zunahme an IT-Sicherheitsvorfällen mit Bezug zur Lieferkette insgesamt, für das Sicherheitsverständnis der Betroffenen und für die Angriffsmöglichkeiten der Angreifer in den letzten Jahren erheblich an Bedeutung gewonnen. Obwohl die hohe Relevanz dieser Vorfälle für die IT-Sicherheit international zunehmend diskutiert wird, wird die Bedrohung über die Lieferkette von IT-Systemen in vielen Unternehmen und Organisationen bis heute unterschätzt. Häufig kommt es zu Datenverlusten bzw. Datendiebstählen bei Vertragspartnern, Auftragnehmern und Dienstleistern. Auch wenn es dabei nicht bzw. nicht immer zum Eindringen in die Netzwerke oder IT-Systeme der eigentlichen Besitzer der Daten kommt, werden über die Lieferkette zugängliche Informationen gestohlen. Solche gestohlenen Datensätze können in weiterführenden IT-basierten Angriffen genutzt werden, um Zugriff auf Netzwerke und IT-Systeme zu erlangen oder gezielte Angriffe per Spear-Phishing auf Mitarbeiter kritischer Unternehmen und Behörden durchzuführen.

Die in dieser Untersuchung beschriebenen durchgeführten IT-Angriffe über die Lieferkette zeigen, dass sowohl Datendiebstahl als auch Manipulationen innerhalb und außerhalb der angegriffenen Zielsysteme eine ernstzunehmende Bedrohung für kerntechnische Anlagen und Einrichtungen darstellen. Dies sollte aus Sicht der GRS weiter beobachtet werden und tiefergehende Untersuchungen zu notwendigen, möglichen Vorkehrungen im Rahmen der Vorbeugung und Abwehr von IT-Angriffen über die Lieferkette nach sich ziehen.

5 Literaturverzeichnis

/BAS20l01/ Bundesamt für die Sicherheit der nuklearen Entsorgung, Vorhaben 4718R01611, "Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen", Änderungsdienst Revision 1, 02.04.2020

/BMU13n01/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, November 2013

/BMU13n03/ BMU, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT), VS-NfD, Juli 2013

/BMU13n04/ BMU: Lastannahmen zur Auslegung kerntechnischer Anlagen und Einrichtungen gegen oder sonstiger Einwirkungen Dritter mittels IT-Angriffen (IT-Lastannahmen) VS-Vertraulich, Juli 2013

/BMU13n05/ BMU: Erläuterungen für die Zuordnung der IT-Systeme von Kernkraftwerken zu IT-Schutzbedarfsklassen, VS-Vertraulich, Juli 2013

/BMU15n01/ BMU: Sicherheitsanforderungen an Kernkraftwerke, November 2012, Neufassung vom März 2015

/CAB19r01/ Carbon Black, Global incident response threat report, April 2019

/COM17r01/ COMSEC Global: Kingslayer – A Supply Chain Attack, 2017

/CPR01r19/ Checkpoint Software Technologies LTD: The Evolution of Cyber Attacks in 2019

/CSI14r01/ Cyber Security Infotech(P) Ltd: Rogue GOM Player Update That Installed Malware at a Japanese Nuclear Plant Analyzed, 2014

/CSO17r01/ CSOnline, Equifax data breach FAQ: What happened, who was affected, what was the impact? 2017

/ENG18r01/ ENGINSIGHT, Berühmt-berüchtigte Sicherheitslücken: Der Heart-bleed-Bug 2018

/ENS20w01/ EnigmaSoft: Backdoor.Win32.Miancha, Informationen, 2020

/FAR11r01/ Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." Survival 53.1 (2011): 23-40.

/FAY18r01/ Fayi S.Y.A.: What Petya/NotPetya Ransomware Is and What Its Remidiations Are. In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738, 2018

/FOR17r01/ Forbes: Domino's Pizza Blames Supplier For Data Breach: Hackers Are Probing Third-Party Weaknesses, 2017

/HEI18r01/ Heise Online: Hacker stellen Daten zu französischen Atomanlagen ins Netz, 2018

/HEI19r01/ Heise Online: Erpressungstrojaner hat Laborgruppe Eurofins im Würgegriff 2019

/HNS19r01/ HelpNetSecurity, Avast breached by hackers who wanted to com-promise CCleaner again 2019

/INL18r01/ Idaho National Laboratory, Kevin E. Hemsley, Dr. Ronald E. Fischer: History of Industrial Control System Cyber Incidents, 2018

/INS18r01/ Inside IT: CCleaner-Hack: Raffinierte Malware mit Keylogger-Funktionalität entdeckt, 2018

/JAT14r01/ Japan Today: Monju power plant facility PC infected with virus, Japan, 2014

/JAE14r01/ Japan Atomic Energy Agency: Die Möglichkeit eines Informationsverlustes aufgrund einer Computervirusinfektion, 2014

/KAS16r01/ Kaspersky Sicherheitsbericht: Petya ransomware eats your hard drives, 2016

/KAS19r01/ Kaspersky Lab: Operation ShadowHammer: a high-profile supply chain attack, 2019

/KOS17r01/ Krebs on Security: How to Bury a Major Breach Notification, 2017

/KOS18r01/ Krebs on Security: Wipro Intruders Targeted Other Major IT Firms, 2018

/LAN19r01/ Paul Lanois: How to prepare for data breaches? Lessons learned from recent incidents, Journal of Data Protection & Privacy, Volume 2, Number 3, 2019

/MSS17r01/ Microsoft Security: Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack

/MSS18r01/ Microsoft Security: Attack inception: Compromised supply chain with-in a supply chain poses new risks, 2018

/MSS18r02/ Microsoft Security: Poisoned peer-topeer app kicked off Dofoil coin miner outbreak, 2018

/NYT17w01/ The New York Times: Hackers are targeting nuclear facilities, Homeland Security Dept. and F.B.I. say, 2017

/POE17r01/ Ponemon Institute LLC Research Report: Data Risk in the Thrid-Party Ecosystem, Second Annual Study, September 2017

/PRV17r01/ Pravda: Der Virusangriff betraf das Kernkraftwerk Tschernobyl, Kiev 2017

/RAP20r01/ Rapidspike: 2019 Magecart Timeline

/SAN16r01/ SANS Institute, Information Security Reading Room, The Impact of Dragonfly Malware on Industrial Control Computers, Nell Nelson, 18 January 2016

/SEC14r01/ Security Insider: Angriffsmuster der SCAD und ICS-Malware Havex, 2014

/SEN19r01/ Sentionel One™: ASUS ShadowHammer Episode – A Custom Made Supply Chain Attack, 2019

/SOP14r01/ Softpedia: Malware Stole Data from Computer at Japanese Nuclear Power Plant, 2014

/STA20r01/ Statista, Joseph Johnson, European firms experiencing a supply chain related cyber-attack 2019, by country, February 2020

/STR18r01/ Securonix Threat Research: British Airways Breach: Magecart Formgrabbing Supply Chain Attack Detection, Oleg Kolesnikov and Harshvardhan Parashar, 2018

/SYM14r01/ Symantic Enterprise, Dragonfly: Western Energy Companies Under Sabotage Threat, 2014

/SYM17r01/ Symantic Enterprise: Dragonfly: Western energy sector targeted by so-phisticated attack group, 2017

/TRE11r01/ The Register: Software maker fingered in Korean hackocalypse, 2011

/TRM13r01/ Trend Micro Security Intelligence Blog: Compromised Auto-Update Mechanism Affects South Korean Users, 2013

/TRM18r01/ Trend Micro Security Intelligence Blog: Supply Chain Attack Opera-tion Red Signature Targets South Korean Organizations, 2018

/TRP12r01/ Threadpost: Final Report on DigiNotar Hack Shows Total Compro-mise of CA Servers, 2012

/VAB18r01/ Vanson Bourne Vortrag: Securing the supply chain, July 2018

/VER16r01/ Meldung eines deutschen Kernkraftwerkes: Virenfund auf IT-Systemen, Deutschland 2016

/WAP18r01/ Washington Post: Hacker linked to Target data breach gets 14 years in prison, 2018

/WIR17r01/ Wired, Andy Greenberg: The untold Story of NotPetya, the Most Dev-astating Cyberattack in History, 2017

/WIR18r01/ Wored, Lily Hay Newman, Inside the Unnerving Supply Chain Attack That Corrupted CCleaner, 208

/WOF17r01/ Wordfence PSA: 4,8 Million Affected by Chrome Extension Attacks Targeting Site Owners, 2017

/ZDN15r01/ ZDNET: Anatomy of the Target data breach: Missed opportunities and lessons learned, 2015

/ZDN17r01/ ZDNET: ShadowPad: Kaspersky warnt vor Hintertür in Server-Management-Software, 2017

/ZDN17r02/ ZDNET: Millions of Verizon customer records exposed in security lapse, 2017

/ZDN18r01/ ZDNET: Twelve malicious Python libraries found and removed from PyPI, 2018

/ZDN19r01/ ZDNET: Two hacking groups responsible for huge spike in hacked Magento 2.x stores, 2019

/ZFK18r01/ Zeitung für kommunale Wirtschaft: Hacker klauen KRITIS-Daten, 2018

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Forschungszentrum
Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-949088-27-8