Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Angriffs-Kampagnen gegen Energie-Firmen

Empfehlungen zur Detektion

CSW-Nr. 2017-200525-14k4, Version 1.4, 27.03.2018

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP-Amber: Organisationsinterne Verteilung

Informationen in dieser Stufe dürfen innerhalb der Organisation der Empfänger weitergegeben werden, jedoch nur auf Basis „Kenntnis nur wenn nötig“. Der Informationsersteller muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Derzeit verdichten sich Hinweise, dass eine oder mehrere Tätergruppen langfristige Anstrengungen unternehmen, um Energie-Infrastrukturen aufzuklären. Dafür sprechen sowohl aktuelle Meldungen über Spearphishing-Angriffe auf amerikanische und europäische Energie-Unternehmen und Kernkraftwerks-Betreiber, als auch eine Reihe von Kampagnen der letzten Jahre. Das BSI nimmt dies zum Anlass, einen kurzen Überblick über die aktuelle Sicherheitslage und Empfehlungen zur Detektion von Angriffen zu geben.

Update 4:
Diese Aktualisierung des allgemeinen Gefährdungshinweises erfolgt *nicht* aufgrund eines aktuellen kritischen Anlasses.

Mit dem Update soll der Bezug zu dem aktuellen Hinweis des US-CERT hergestellt werden [14] und Ihnen darüber hinaus zusätzliche neue, aber im Umfang beschränkte TLP-AMBER-Informationen übermittelt werden.

Sicherheitslage:

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Seit einigen Jahren zeichnet sich ab, dass eine oder mehrere Gruppen Schadsoftware entwickeln, die speziell für Angriffe auf Prozesssteuerungsanlagen (ICS) geeignet ist. Bereits im Jahr 2014 wurde die Schadsoftware Havex entdeckt, die weltweit zu Infektionen führte und in Netzwerken nach ICS-Systemen und Informationen über deren Konfiguration suchte [3]. Der genaue Zweck dieser Kampagne war damals nicht ersichtlich, da es keine Hinweise gab, dass wirtschaftlich oder politisch verwertbare Informationen gestohlen wurden. Berichte über destruktive Aktionen dieser Schadsoftware gab es ebenfalls nicht.

Seit 2015 gab es mehrere Angriffe auf Kritische Infrastrukturen in der Ukraine, die mittels modifizierten Varianten von Black-Energy durchgeführt wurden. Diese Schadsoftware hatte zwar keine ICS-spezifischen Funktionen. Sie wurde aber eingesetzt, um den Tätern Zugriff auf Steuerungssysteme von Stromnetzbetreibern zu ermöglichen. Die Täter hatten zudem ausreichend Kenntnisse über die Systeme und Prozesse der Betreiber, um durch manuelle Änderungen großflächige Stromausfälle zu bewirken [4].

Mitte Juni 2017 wurde erstmals über eine Schadsoftware namens Industroyer bzw. CrashOverride [6, 8] berichtet, die die Funktionalität aufweist, über ICS-spezifische Protokolle Steuerungsanlagen kontrollieren zu können. Die modulare, erweiterbare Architektur, sowie die detaillierten Implementationen von ICS-Protokollen legen den Schluss nah, dass diese Tätergruppe über aufwändige Test-Umgebungen verfügt und das langfristige Ziel verfolgt, in ICS-Netzwerke einzudringen.

Auch die aktuellen Berichte über Spearphishing- und Watering-Hole-Angriffe auf amerikanische und europäische Energie-Firmen und Kernkraftwerksbetreiber [1, 2] fügen sich in das Gesamtbild ein. Auch wenn Kompromittierungen bisher nur in Büro-Netzen gefunden wurden, sind die ausgewählten Watering-Holes für die ICS-Supply-Chain relevant. Es ist anzunehmen, dass in den Büro-Netzen zunächst Informationen für weitere Angriffe gesammelt werden sollen.

Das BSI geht davon aus, dass all diese Angriffe auf zwei Gruppen zurückzuführen sind, die unter Umständen dieselben strategischen Ziele verfolgen. In Medien und Analyseberichten werden diese Gruppen als EnergeticBear/Dragonfly und Sandworm/VodooBear bezeichnet.

Die Sicherheitslage wird dadurch verschärft, dass im Mai ein Mann verhaftet wurde, der offenbar vertrauliche Informationen über europäische Energietransportwege an einen russischen Agentenführer verkauft haben soll [5].

Angriffsmethoden:

Die Angriffsmethoden der beiden Gruppen sind vielfältig. Angesichts der verschiedenen Kampagnen, die erst nach und nach entdeckt werden, können die folgenden Erläuterungen keinen Anspruch auf Vollständigkeit erheben. Es ist anzunehmen, dass weitere Methoden und Angriffsinfrastrukturen noch unentdeckt genutzt werden, bzw. die Täter nach den aktuellen Veröffentlichungen ihre Angriffsmittel ändern.

Die aktuelle Kampagne gegen Energieunternehmen und Kernkraftwerke verwendet Spearphishing. Die an die gezielten E-Mails angehängten Dokumente enthalten keinen Schadcode, sondern versuchen, über SMB ein Office-Template nachzuladen. Bei diesem Vorgang werden Authentifizierungs-Daten übermittelt, die die Täter abgreifen können. Solche Daten können ggf. genutzt werden, um sich per VPN in ein Unternehmensnetz oder per Webmail-Portal in Email-Postfächer einzuloggen.

Zeitgleich nutzen die Täter für die Zielbranche relevante Webseiten, um dort Schadcode zu platzieren ("Watering-Holes").

Die Angriffsvektoren für Industroyer/CrashOverride sind nicht bekannt. Die Täter konnten sich aber offenbar in den kompromittierten Netzwerken ausbreiten und Rechner infizieren, die Netzwerkverbindungen zu ICS-Systemen besaßen.

Update 2:
Zwischenzeitlich hat Symantec einen umfassenden Bericht über Dragonfly veröffentlicht [12]. Die dazugehörigen Indikatoren sind in dem öffentlichen Bericht nicht enthalten und werden in diesem Warnungs-Update zur Verfügung gestellt. Das Format für Indikatoren wird mittelfristig überarbeitet werden, um eine einfachere Verwendung durch die Empfänger zu ermöglichen.

Das BSI wird auch weiterhin den Themenkomplex beobachten und bei einer Änderung der Bedrohungslage informieren.

Update 3:
Das US-CERT hat vergangene Woche als TLP-White [13] wie auch heute (24.10.2017) neue Indikatoren als TLP-Amber zur Verfügung gestellt. Anhängend finden Sie Listen aller Indikatoren mit der Bitte um Beachtung.

Update 4:
Das US-CERT hat am 15.03.2018 als TLP-White [14] die Informationen unter [13] aktualisiert.

Die nun unter [14] TLP-White verfügbaren Information hatte Ihnen das BSI in den Vorversionen zu dieser Warnung bereits *im vergangenen Jahr* unter TLP-Amber zur Verfügung gestellt.

Im Anhang finden Sie nun auch je eine um einzelne TLP-Amber Informationen ergänzte Fassung der Dateien TA18-074A_TLP_WHITE.csv und TA18-074A_TLP_WHITE.stix.xml von [14]. Bitte beachten Sie, dass TLP-Amber-Informationen allgemein und damit dieses Dokument bzw. Informationen daraus sowie die Anlagen ausschließlich im Rahmen der Vorgaben zum TLP verwendet werden dürfen. Insbesondere dürfen die Informationen nicht auf Internetplattformen hochgeladen werden, *auch nicht* auf Virenerkennungsplattformen wie beispielsweise VirusTotal.

Bewertung

Die geschilderten Kampagnen belegen, dass Akteure langfristig und mit großem Aufwand Kompetenzen aufbauen und spezifische Angriffsmethoden und -werkzeuge entwickeln, um wirksam Angriffe gegen Prozesssteuerungsanlagen durchführen zu können – vor allem im Energiesektor. Als besonders kritisch ist zu bewerten, dass die beobachteten Aktivitäten nicht nur auf reine Informationsbeschaffung abzielen, sondern auch Sabotage-Fähigkeiten und -Absichten zeigen.

Das BSI geht stark davon aus, dass auch deutsche Unternehmen im Fokus der Angreifer stehen.

Update 4:
Es handelt sich bei der US-CERT-Warnung vor allem um die Veröffentlichung bisher als TLP Amber verfügbaren Indikatoren, die das BSI im letzten Jahr bereits verteilt hatte.

Maßnahmen

Grundlegende Empfehlungen:

Das BSI empfiehlt die folgenden Dokumente zum Schutz von ICS-Systemen und -Netzen:

- BSI Grundschutz: IND - Industrielle IT (Bausteine und insbesondere Umsetzungshinweise) [9]
- BSI ICS-Kompendium [10]
- Fernwartung im industriellen Umfeld [11]

Kompromittierungen durch die aktuelle Energie-Kampagne im Ausland haben gezeigt, dass es in vielen Fällen ausreicht, Benutzername und Password zu stehlen, um in Unternehmensnetze einzudringen. Dies wird zum Anlass genommen, erneut auf die Empfehlung hinzuweisen, VPN- und Remote-Zugänge durch einen zweiten Faktor, IP-Listen oder Software-Zertifikate abzusichern.

SMBv1 sollte wenn möglich vollständig deaktiviert werden. Ausgehende SMB-Verbindungen sollten grundsätzlich blockiert oder nur für einzelne IP-Adressen freigegeben werden.

Update 1:
Um die in der Kampagne verwendete Technik zum Abfluss von Windows-Zugangsdaten zu verhindern, sollte sichergestellt sein, dass ausgehende WebDAV-Verbindungen blockiert werden.

Lateral Movement sollte durch das Unterbinden von RDP-Verbindungen zwischen Arbeitsplatzrechnern mittels GPOs erschwert werden.

Ebenso sollten Domain-Administrator-Accounts nur auf den Domain-Controller zugreifen dürfen, andernfalls besteht die Gefahr, dass die Zugangsdaten dieser sensiblen Accounts im Speicher anderer Systeme auffindbar sind.

Update 3:
Beachten Sie auch die "General Best Practices Applicable to this Campaign" in [13].

Update 4:
Die „General Best Practices Applicable to this Campaign“ in [14] sind unverändert zu [13] und sollten auch weiterhin beachtet werden.

Sicherheitsmonitoring:

In Netzwerken mit ICS-Systemen und an deren Netzübergängen sollte Sicherheitsmonitoring betrieben werden.

Um Angriffe mit Schadsoftware wie Industroyer/CrashOverride und auch zukünftig verwendete Techniken verlässlicher erkennen zu können, sollte der betriebliche Normalzustand erfasst werden. Aus der auch als *Baseline* bezeichneten Übersicht sollte hervorgehen, welche spezifischen Protokolle die einzelnen Systeme nutzen und welche einzelnen Komponenten miteinander kommunizieren dürfen. Auch die Quelle und Dauer zulässiger VPN-Verbindungen sollten darin erfasst werden. Mittels Monitoring detektierte Abweichungen sind gemäß ebenfalls zu definierender Sicherheitsprozesse zu behandeln.

Systemhärtung:

Viele in ICS eingesetzten Geräte werden nur selten aktualisiert oder gepatcht. Deshalb ist eine Systemhärtung (beispielsweise Application Whitelisting) empfohlen. Zusätzlich sollten detektierte Systemveränderungen an ein zentrales Managementsystem gemeldet und und untersucht werden.

Application Whitelisting sollte, sofern möglich, auch in Systemen eingesetzt werden, die Netzwerkverbindungen in Produktionsnetze haben.

DIE TLP-AMBER eingestuften Informationen / IoCs wurden aus diesem Dokument entfernt.

Links

[1] Talos, "Attack on Critical Infrastructure Leverages Template Injection", http://blog.talosintelligence.com/2017/07/template-injection.html

[2] CIPProject, "Document Indicates U.S. Energy/Critical Infrastructure Campaign May Have Hit Europe in March" , https://www.ci-project.org/blog/2017/7/10/document-indicates-campaign-may-have-targeted-european-energy-and-critical-infrastructure-in-march-2017

[3] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers", https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

[4] ICS-CERT, "Cyber-Attack Against Ukrainian Critical Infrastructure", https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[5] ARD Tagesschau, "Ein Maulwurf und der Schaden für die NATO", http://www.tagesschau.de/ausland/spionage-russland-101.html

[6] Dragos, "CrashOverride", https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[7] Dragos, CrashOverride IoCs, https://github.com/dragosinc/CRASHOVERRIDE

[8] ESET, "Industroyer", https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[9] BSI Grundschutz IND - Industrielle IT, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html

[10] BSI, ICS-Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf

[11] BSI, Fernwartung im industriellen Umfeld, https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_108.html

Update 2:
[12] Symantec, Dragonfly 2.0, https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Update 3:
[13] US-CERT, "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors", https://www.us-cert.gov/ncas/alerts/TA17-293A

Update 4:
[14] US-CERT, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", https://www.us-cert.gov/ncas/alerts/TA18-074A