09.17

In Kooperation mit:

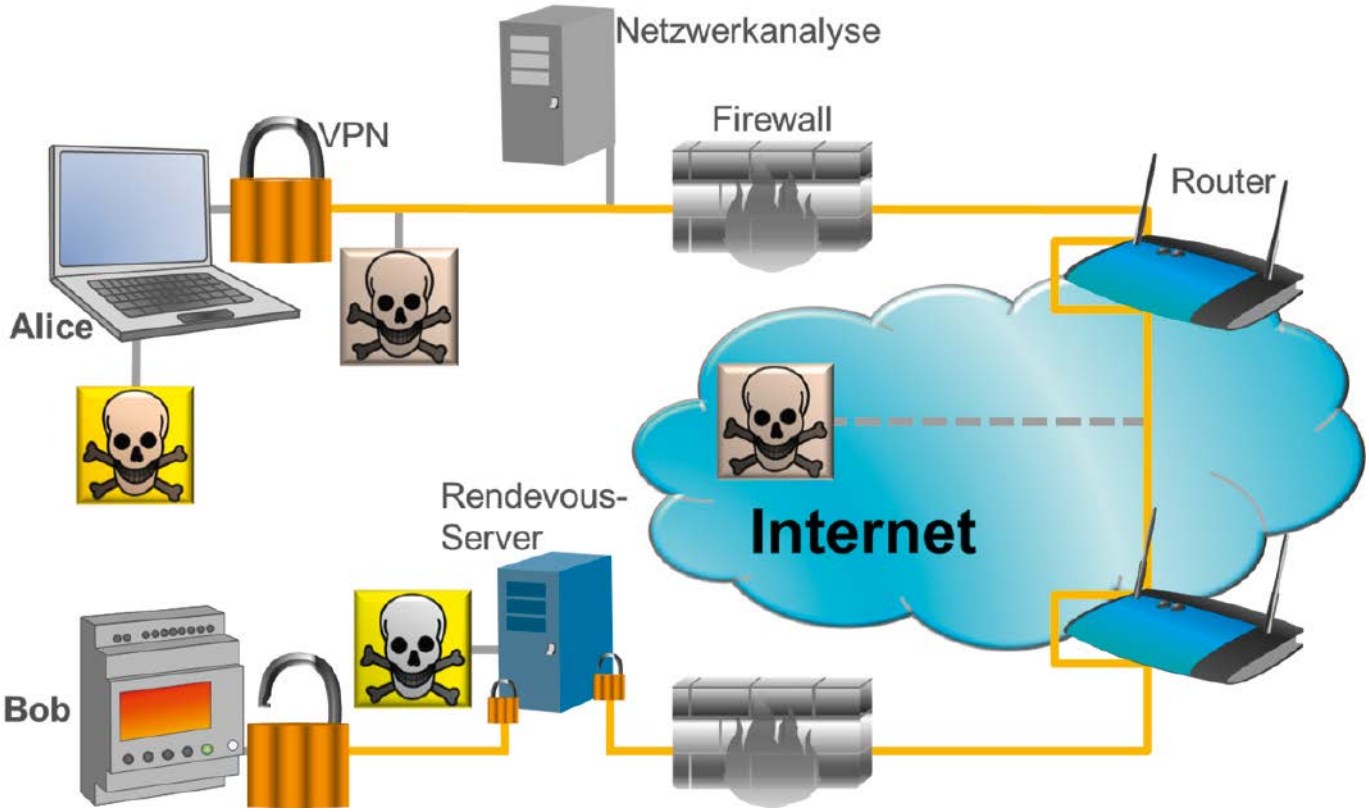
baua: DGUV
LASI Basi LIA.nrw

68. Jahrgang
September 2017
ISSN 2199-7330
1424

www.SISdigital.de

sicher ist sicher

ESV ERICH SCHMIDT VERLAG



BJÖRN OSTERMANN · CHRISTIAN WERNER

Sichere Fernwartung

Die Fernwartung von Maschinen oder Anlagen wird von vielen Betreibern genutzt. Über einen Remote-Zugriff ist der Servicetechniker in der Lage den Fehler aus der Ferne zu lokalisieren und – unter Umständen – zu beheben, sodass die Stillstandszeit der Maschine reduziert werden kann.
Eine sichere Fernwartung von Maschinen und Anlagen wird gerade im Hinblick auf „Industrie 4.0“ an Wichtigkeit gewinnen. Dabei muss nicht nur die IT-Security, sondern auch die funktionale Sicherheit mit betrachtet werden.

1. Safety vs. Security

Der Einfachheit halber wird im weiteren Verlauf des Artikels der Begriff „Safety“ für die funktionale Sicherheit und der Begriff „Security“ für die IT- oder Industrial-Security verwendet.

Die Themenbereiche Safety und Security lassen sich zunächst gut voneinander abgrenzen, da bei Safety die Gefahren betrachtet werden, die von einer Maschine auf den Menschen oder auf die Umwelt einwirken und bei Security die Gefahren betrachtet werden, die von einem (meist intelligenten) Angreifer auf eine Maschine bzw. die vorhandenen Daten ausgehen. Beide Bereiche weisen aber auch gemeinsame Schnittstellen auf, die mit betrachtet werden müssen. Wenn zum Beispiel die Daten einer Maschine durch ein Security-Problem korrumpiert werden, kann dies zu einem unerwarteten Verhalten der Maschine und somit zu Safety-Problemen führen.

2. Allgemeine Probleme bei der Umsetzung von Security

Kleine und mittelständige Betriebe, die Komponenten, Maschinen oder Anlagen bauen, haben häufig keine Mitarbeiter mit einer Ausbildung im Bereich Security. Die ausgelieferten Produkte

werden deshalb meist nur rudimentär auf etwaige Security-Probleme hin untersucht. Für die Fernwartung bedeutet das unter anderem, dass die Betriebe eine einfach einzurichtende, ausfallsichere Kommunikation herstellen wollen. Hierbei wird möglicherweise nicht daran gedacht, dass auch nicht-autorisierte Personen mit der Maschine kommunizieren könnten.

Ein weiteres Problem ist die Langlebigkeit von Industrieanlagen und deren Komponenten, wie zum Beispiel der eingesetzten Speicherprogrammierbaren Steuerung (SPS). Eine Industrieanlage ist in der Regel für 20 Jahre ausgelegt und wird meist auch darüber hinaus betrieben. Während dieser Zeit erfolgt häufig kein Firmwareupdate der SPS, da Inkompatibilitäten und Produktionsausfälle befürchtet werden. Somit werden auch bekannte Sicherheitslücken auf ausgelieferten Geräten meist nicht oder nur mit einer sehr großen Verzögerung geschlossen. Wird eine Sicherheitslücke in einer SPS öffentlich bekannt, stellt eine mit dem Netz verbundene SPS ohne Update der Firmware ab diesem Zeitpunkt ein Sicherheitsproblem dar. Für Komponenten, die in einer Industrie 4.0 Umgebung eingesetzt werden sollen, muss dieses Security-Problem gelöst werden.

Wird eine Sicherheitslücke in einer SPS öffentlich bekannt, stellt eine mit dem Netz verbundene SPS ohne Update der Firmware ab diesem Zeitpunkt ein Sicherheitsproblem dar.

Häufig hört man von Betreibern Sätze wie: „Ich habe nichts zu verbergen“, „Wer will mich denn angreifen“ und „Mich findet im Netz doch keiner“. Viele aufgedeckte Angriffe auf die unterschiedlichsten Schwachstellen verschiedenster Produkte haben gezeigt, dass dies ein Trugschluss ist. Im Internet existieren bereits Suchmaschinen [1], die speziell nach bestimmten Steuerungen oder Servern Ausschau halten, auf denen bestimmte Programme laufen.

Die Interessen der Angreifer sind vielfältig. Einigen geht es nur um die Herausforderung in ein fremdes System einzudringen. Vermehrt finden aber auch gezielte Angriffe statt, die zum Ziel haben, Firmendaten auszuspionieren oder den Produktionsablauf zu stören.

Problematisch ist ebenfalls die sich ständig ändernde Gefährdungslage für eine Maschine im Hinblick auf die Security. Aufgrund der technischen Weiterentwicklung stehen potentiellen Angreifern immer bessere und schnellere Systeme zur Verfügung, um z. B. Zugangsschlüssel zu berechnen. Im Vergleich zu einem Safety-System, welches nach Zertifizierung häufig unverändert über mehrere Jahre betrieben werden darf und als sicher gilt, ist diese Vorgehensweise für Security-Systeme nicht denkbar.

3. Beispiele für safety-relevante Security-Probleme

Die Presse berichtet regelmäßig über größere Security-Probleme von Maschinen und Anlagen. Nach einer im Jahr 2015 durchgeführten Studie waren mehr als 28.000 SPSen über das Internet frei für jeden erreichbar [2]. Ein weit verbreitetes SPS-Modell hatte zu diesem Zeitpunkt eine Sicherheitslücke, über welche Schadsoftware aufgespielt werden konnte. Die Schadsoftware konnte dann für weitere Angriffe in das Firmennetz genutzt werden. Durch die dabei eingeschleusten Zusatzroutinen wurde unter anderem die Zykluszeit der Steuerungen erhöht, sodass errechnete Antwortzeiten nicht mehr stimmten. Dies kann an einer Anlage z. B. beim Einsatz von Laserscannern zu einem Safety-Problem führen, wenn Abstände zwischen einem Mitarbeiter und einer Gefahrenstelle aufgrund der verlängerten Reaktionszeit nicht mehr ausreichen.

Ebenfalls im Jahr 2015 waren laut einer Untersuchung mehrere Steuerungen von Wasserwerken online frei erreichbar [3][4] und bei mindestens einem der Wasserwerke konnten die Pumpen ferngesteuert werden. Im Zuge dieser Untersuchung wurden über 100 Betreiber von Industrieanlagen darüber informiert, dass ihre Steuerungen frei über das Internet erreichbar waren. Die Reaktionen der Betreiber auf die Meldung fielen sehr unterschiedlich aus. Einige reagierten umgehend und schlossen die Sicherheitslücke, andere wiederum zeigten keinerlei Reaktionen. Auch in den zuletzt genannten Fällen sah der Hersteller der Software keinen Handlungsbedarf und seine Kunden in der Handlungspflicht.

Diese Beispiele belegen, dass es immer noch Hersteller von Industriekomponenten gibt, die sich der Security Problematik nicht bewusst sind. Sie zeigen aber auch, dass die Aufgabenverteilung zwischen Komponentenhersteller, Maschinen- oder Anlagenbauer und Betreiber hinsichtlich der Security besser koordiniert werden muss.

In diesem Jahr haben Wannacry und NotPetya die Schlagzeilen beherrscht. Bei Wannacry wurde eine mehrere Monate alte Sicherheitslücke genutzt um vornehmlich in Windows XP PCs einzubrechen. Dieser Angriff war ungezielt, hat aber auf Produktionsanlagen, die noch mit älteren Windowsversionen ausgestattet waren, zu erheblichem Schaden geführt.

NotPetya war eine gezielte Attacke, bei der zuerst die ukrainische Software MeDoc kompromitiert wurde. MeDoc wird weltweit genutzt, um in

der Ukraine Rechnungen zu stellen und Steuern zu zahlen. Über mehrere Monate wurden über die Updates der Software auch Hintertüren verteilt, über die die Angreifer in die Systeme großer Firmen eindringen konnten. Dort konnten sie Daten der Firmen abgreifen und schließlich, durch das Verschlüsseln vieler Computer, erheblichen Schaden – auch in der Produktion – anrichten. Grund dafür war bei vielen Firmen, dass die Produktionsnetze nicht sauber von den Büronetzen getrennt sind.

4. Vor-Ort-Wartung vs. Fernwartung

Nicht alle Safety- oder Security-Probleme und die daraus resultierenden Anforderungen an die Fernwartung sind neu. Viele Punkte (Authentifizierung der Teilnehmer, Erkennung von Übertragungsfehlern etc.) werden bereits durch die Betrachtung im Rahmen der Wartung vor Ort aufgegriffen. Gänzlich neu ist die Einbeziehung eines meist intelligenten Angriffes von Dritten entweder auf die Maschine, den Wartungs-PC oder auf die Datenverbindung zwischen den beiden Parteien.

4.1 Gemeinsamkeiten der Wartungsarten

Vor-Ort und Fernwartung dürfen nur von qualifizierten Mitarbeitern ausgeführt werden und die durchzuführenden Arbeiten müssen vorher mit dem Anlagenpersonal abgestimmt sein. Weiterhin müssen die vorgenommenen Änderungen protokolliert werden, um Änderungen im Nachhinein zuordnen zu können. Die vorgenommenen Änderungen müssen auf Rückwirkungsfreiheit in Bezug zu Safety-Komponenten getestet worden sein.

Um die Wartung zu starten, muss sich der Servicetechniker authentifizieren (Name, Passwort, etc.) und es muss sichergestellt werden, dass auf die richtige Maschine bzw. Komponente zugegriffen wird. Während der Wartung übernimmt das Wartungspersonal die Kontrolle über die Anlage bzw. die Komponente. Es müssen geeignete Maßnahmen getroffen werden, um einen Arbeitsunfall zu vermeiden.

Eine Schädigung muss nicht zwangsläufig durch einen unbeabsichtigten Fehler des Wartungspersonals erfolgen. Auch ein mit Schadsoftware verseuchter Wartungs-PC kann dazu führen, dass Anlagen mit Schadsoftware infiziert werden und in Folge dessen auch Personen geschädigt werden können. Der Stuxnet-Virus [5], der es durch die Manipulierung eines Überwachungs- und Steuerungssystems von Uranzentrifugen eines iranischen Atomkraftwerkes zu Berühmtheit gebracht hat, wurde lokal installiert und ist damit kein spezielles Fernwartungs-Problem.

4.2 Zusätzliche Anforderungen an eine sichere Fernwartung

Bei der Fernwartung befindet sich das Wartungspersonal nicht vor Ort, und die Kommunikation mit der Maschine erfolgt meist über das Intra- oder Internet. Hieraus ergeben sich verschiedene neue oder erweiterte Anforderungen an eine sichere Fernwartung. Eine nicht erschöpfende Liste der Anforderungen ist im Folgenden dargestellt:

- Etablierung einer sicheren Kommunikation
- Verwendung von sicheren und geprüften Kommunikationspartnern
- Beschränkung des Zugriffs nur auf die einzelne Maschine/Komponente
- Bestätigung der richtigen Auswahl der zu wartenden Maschine vor Ort
- Freigabe der Wartung durch einen Mitarbeiter vor Ort (Produktion gestoppt, keine Person im Gefahrenbereich, etc.)
- Ggf. Betreuung bei Neuinitialisierung durch Mitarbeiter vor Ort nötig
- Testung der neuen Software nur durch Mitarbeiter vor Ort möglich

5. Bestehende Lösungsansätze für eine sichere Fernwartung

Es existieren bereits verschiedene Lösungen, um eine sichere Fernwartung durchzuführen, die aber alle ihre Vor- und Nachteile aufweisen. In der Praxis hat es sich bewährt, mehrere Ansätze zu kombinieren.

5.1 VPN-Tunnel für Industrieanlagen

Ein erster Ansatz ist es, Wartungs-PC und Maschine über ein virtuelles privates Netzwerk (VPN) zu verbinden. Dabei findet die Kommunikation zwischen beiden Teilnehmern verschlüsselt und meist über das Internet statt, sodass Dritte diese nicht mitlesen oder unbemerkt verändern können.

Eine mögliche Variante ist hierbei den Wartungs-PC mit dem Netz des Maschinenbetreibers zu verbinden. Da bei dieser Verbindung das Wartungspersonal Zugriff auf mehrere Maschinen oder Netzbereiche hat, sollte diese Variante nur verwendet werden, wenn es unvermeidbar ist.

Eine bessere Variante ist es, den Wartungs-PC direkt mit der Maschine zu verbinden und dem Wartungspersonal nur den Zugriff auf die zu wartende Maschine oder Komponente zu gewähren. Alle anderen Maschinen oder Netze können dann gegen einen Zugriff gesperrt werden.

Ein großer Nachteil bei der VPN-Option besteht darin, dass sich die Betreiber und Hersteller komplett auf die Sicherheit des VPN-Zugangs verlassen und die übertragenen Daten durch die bestehenden Firewalls verschlüsselt getunnelt werden. Dadurch kann eine Schadsoftware vom

DIE AUTOREN

Dr.-Ing. Björn Ostermann
Wissenschaftlicher Mitarbeiter – Referat 5.2 „Maschinen und Anlagen" – im Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), St. Augustin,
bjoern.ostermann@dguv.de

M.Sc. Christian Werner
Leiter des Referats 5.2 „Maschinen und Anlagen" im Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), St. Augustin,
christian.werner@dguv.de

Wartungs-PC direkt auf die Maschine übertragen werden. Dieses kann verhindert werden, wenn ein zusätzlicher Schutz in die Verbindung implementiert wird. Es kann zum Beispiel ein VPN-Zugang vom Wartungs-PC zur Firewall (beim Betreiber) und ein weiterer VPN-Zugang von der Firewall zur Maschinensteuerung aufgebaut werden (Stichwort: Rendezvous-Server [6] – siehe Artikelbild).

Ein Vorteil des VPN-Zugangs ist, dass die Security durch den VPN-Tunnel erzeugt wird und es nicht zusätzlicher Hard- oder Software auf der Maschine bedarf. Das Sicherheitsniveau des VPN-Zugangs sollte dabei deutlich höher sein als das einer SPS. Weiterhin können nötige Security-Updates für den VPN-Zugang eingespielt werden, ohne auf die Steuerung der Maschine zugreifen zu müssen.

Dass ein VPN-Zugang nicht in jedem Fall eine ausreichende Sicherheit garantieren kann, sieht man am Beispiel des Point-to-Point Tunneling Protokolls (PPTP). Dieses Protokoll, mit dem ein VPN geschaffen wird, ist erfolgreich entschlüsselt worden. Das verwendete Passwort kann hierbei nach dem Mitschneiden der Kommunikation in unter 24 Stunden errechnet werden [7]. Trotzdem ist PPTP noch in vielen Produkten als VPN-Lösung vorhanden.

Eine direkte Kommunikation mit der Maschine findet nicht mehr statt und in Folge dessen kann auch keine Schadsoftware auf die Maschine aufgespielt werden.

Neben den verwendeten Protokollen können auch einzelne VPN-Produkte Security-Probleme haben. Beispielsweise existierte in Geräten von Cisco eine Sicherheitslücke, die es Angreifern erlaubt das Passwort von außen einfach anzufordern. Diese Geräte werden seit 2008 nicht mehr produziert. Sie sind trotzdem noch weit verbreitet. Wenn sie noch mit veralteter Firmware betrieben werden, bieten sie unter Umständen ein Sicherheitsrisiko. [8][9]

Auf dem Markt existieren auch Cloud-Lösungen, bei denen sich die Wartungs-PCs und die einzelnen Maschinen über VPN mit der Cloud verbinden. Dies reduziert den Aufwand beim Einrichten erheblich und die zu wartenden Maschinen können vom Wartungspersonal später schneller und bequemer angesprochen werden. Gleichzeitig wird damit die Cloud zum wichtigsten Angriffspunkt von außen. Wird diese erfolgreich angegriffen, liegen alle Teilnehmer offen.

5.2 Beschränkung der Zugriffe auf IP-Ranges/IPs

Jeder Teilnehmer im Internet benötigt eine IP-Adresse, auf der er Datenpakete senden oder empfangen kann. Daraus ergibt sich zur Absicherung der Kommunikation die Möglichkeit, durch eine Firewall nur solche Pakete an die Maschinensteuerung weiterzuleiten, die von einer bestimmten IP-Adresse stammen. Die gleiche Vorgehensweise muss auch auf die Antworten der Maschinensteuerung angewendet werden.

Diese Adresse als Absender zu fälschen ist leicht, die Antwort zu erhalten wiederum schwierig. Die IP-Adresse wird von den Kommunikationsteilnehmern als Absender selbst an die Nachricht angefügt. Das bedeutet, dass sich jeder beliebige PC als Wartungs-PC ausgeben kann, wenn die gültige IP-Adresse bekannt ist. Die Antwort in der Kommunikation wird dann aber an die Adresse des Wartungs-PC geschickt. Der Angreifer muss sich also in einem Netzabschnitt befinden, an welchem er Zugriff auf die Antwort hat, oder die Antwort durch andere Methoden zu sich umlenken.

5.3 Daten-Diode zum regelmäßigen Auslesen von Maschinendaten

Eine physikalisch unidirektionale Kommunikation (Daten-Diode) ist so aufgebaut, dass ein Sender keine technische Möglichkeit hat, Signale zu empfangen. Dies kann z. B. über eine Schnittstelle von LEDs auf Fotodioden erfolgen. Diese Schnittstelle kann auch intern im Gerät liegen, um Signale aus dem Gerät z. B. in der Form von Strom oder Spannungspegeln auszugeben. Diese Methode kann verwendet werden, wenn kontinuierlich Betriebsdaten von der Maschine ausgelesen werden sollen. Im Hinblick auf das Aufspielen von Schadsoftware für Maschinen und Anlagen ist es eine der sichersten Methoden, wenn nur Daten gesendet werden können.

Eine Wartung im herkömmlichen Sinne ist auf diese Weise allerdings nicht möglich, da keine Updates aufgespielt werden können. Auch Fehler in der Software oder andere komplexe Fehler können so meist nicht diagnostiziert werden.

Eine besondere Version der Daten-Diode wird bereits durch einige Firmen für die Wartung genutzt. Diese Firmen sind dazu übergegangen die Kommunikation für eine Fernwartung von der Maschine weg hin zu einem externen Laptop, Tablet oder Wearable zu verlegen. Dabei werden von einem Mitarbeiter vor Ort nur noch Bilder an den Wartungs-PC übertragen. Diese Bilder von der Maschine oder deren Bedienschnittstelle reichen meist aus, um eine Fehlerdiagnose zu erstellen. Eine direkte Kommunikation mit der Maschine findet nicht mehr statt und in Folge dessen kann auch keine Schadsoftware auf die Maschine aufgespielt werden.

5.4 Protokollierung und Überprüfung von Datenvolumenströmen

Eine zusätzliche Möglichkeit das Einspielen von Schadsoftware zu erkennen besteht in der Überwachung und Protokollierung von ein- und ausgehenden Datenvolumenströmen. Diese werden auf Anomalien hin überwacht und geben bei Auffälligkeiten einen Alarm aus oder trennen die Kommunikation.

Diese Option kann die vorher aufgezeigten Sicherheitsmechanismen einer Fernwartung nicht ersetzen. Sie dient der übergeordneten Kontrolle, die den Angriff nicht verhindern, aber unter bestimmten Voraussetzungen den Angriff erkennen und zum Abbruch der Kommunikation führen kann.

Um eine Schadsoftware zu erkennen muss deren Größe bei Übertragung hinreichend groß sein, um als Anomalie gedeutet zu werden. Leider trifft dieses auf Schadsoftware oft nicht zu. Auch das Nachladen von weiteren Softwaremodulen kann zeitlich vom Angreifer so gestreckt werden, dass dies nicht erkannt wird.

Generell kann auch für bestimmte Geräte ein Alarm ausgelöst werden, wenn diese sich unerwartet verhalten und damit die Möglichkeit gegeben ist, dass sich eine Schadsoftware bereits auf der Maschine befindet. Maschinen, Drucker oder Scanner müssen in der Regel nicht mit dem Internet kommunizieren, wenn keine Wartung beantragt worden ist. Andere Geräte, wie zum Beispiel Entertainment-Systeme, müssen nur zu bestimmten Zeiten kommunizieren. Auch der interne Datenverkehr kann so überwacht werden. ■

LITERATUR

[1] *Shodan*
https://www.shodan.io/

[2] *Scada-Sicherheit: Siemens-PLC wird zum Einbruchswerkzeug, 07.08.2015, Uli Ries, heise Security*
http://www.heise.de/newsticker/meldung/Scada-Sicherheit-Siemens-PLC-wird-zum-Einbruchswerkzeug-2774812.html

[3] *Schwachstellen aufgedeckt: Der leichtfertige Umgang mit kritischen Infrastrukturen, 15.07.2016, Sebastian Neef und Tim Philipp Schäfers, golem.de*
http://www.golem.de/news/schwachstellen-aufgedeckt-der-leichtfertige-umgang-mit-kritischen-infrastrukturen-1607-122063.html

[4] *Nicht abgesichert: Steuerungen deutscher Wasserwerke über das Internet manipulierbar, 15.07.2016*
Dennis Schirrmacher, heise Security
http://www.heise.de/newsticker/meldung/Nicht-abgesichert-Steuerungen-deutscher-Wasserwerke-ueber-das-Internet-manipulierbar-3268693.html

[5] *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve, Ralph Langner – November 2013*
http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[6] *Verabredung in der DMZ – Sichere Fernwartung über zentralen Rendezvous-Server*
SPS Magazin, Sonderdruck aus Ausgabe 1+2/2011
http://www.we-conect.com/cms/media/uploads/events/wc1415/dokumente/SPS_-_Sichere_Fernwartung.pdf

[7] *Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2; DefCon 20; Moxie Marlinspike*
https://media.defcon.org/DEF%20CON%2020/DEF%20CON%2020%20video%20and%20slides/DEF%20CON%2020%20Hacking%20Conference%20Presentation%20By%20Marlinspike%20Hulton%20and%20Ray%20-%20Defeating%20PPTP%20VPNs%20and%20WPA2%20Enterprise%20with%20MS-CHAPv2%20-%20Video%20and%20Slides.m4v

[8] *NSA BENIGNCERTAIN tool can obtain VPN Passwords from CISCO PIX, 20.08.2016, Pierluigi Paganini*
http://securityaffairs.co/wordpress/50452/hacking/benigncertain-tool.html

[9] *The Shadow Brokers EPICBANANA and EXTRABACON Exploits, 17.08.2016, Omar Santos*
https://blogs.cisco.com/security/shadow-brokers