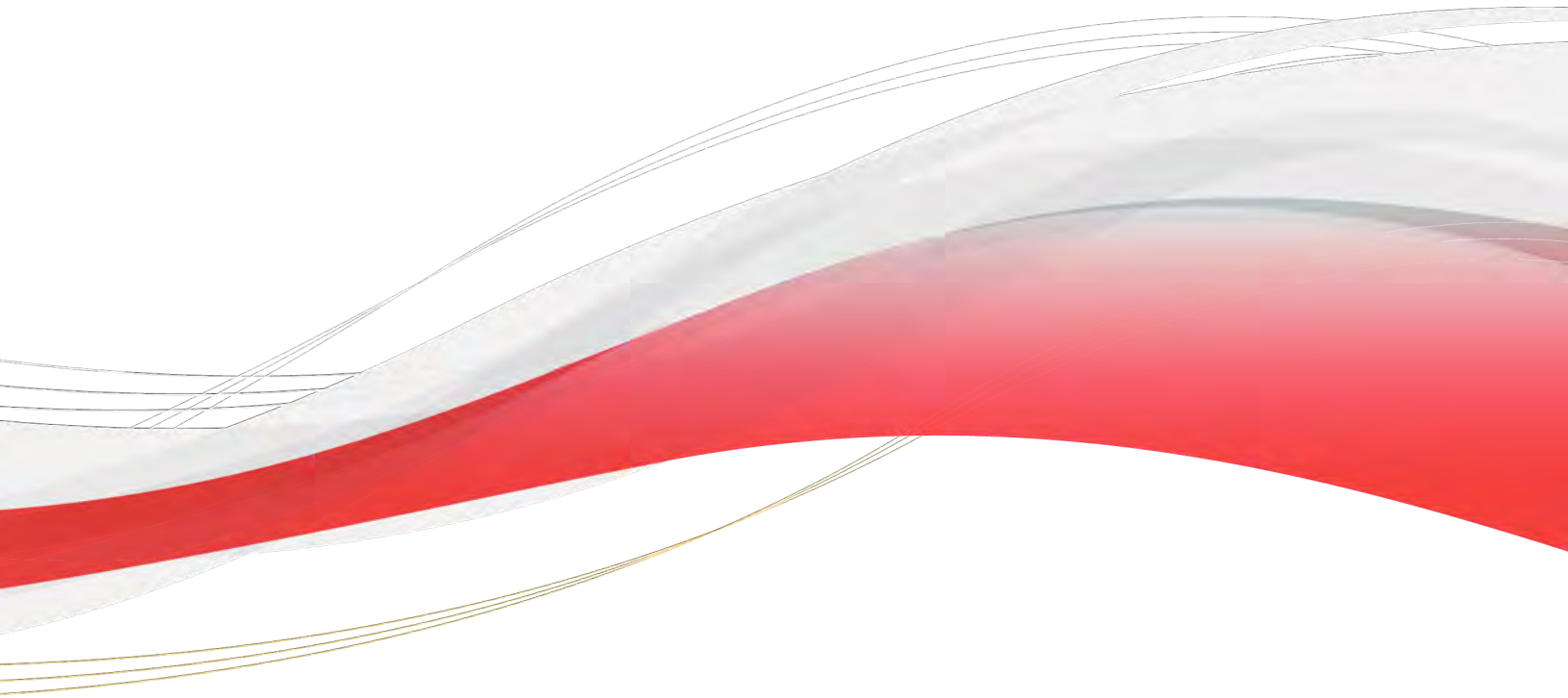
Forschungspapier
2013

SCADA in der Cloud

Diskussionsbeitrag zur Sicherheit



Autor: Kyle Wilhoit, Senior Threat Researcher bei Trend Micro

Inhalt

Einleitung

ICS-Systeme (Industrial Control Systems) sind Geräte, Systeme, Netzwerke und Kontrollmechanismen für den Betrieb und/oder die Automatisierung von Industrieprozessen. Diese werden in fast allen Branchen eingesetzt – von der Fahrzeugherstellung und dem Transportwesen bis hin zur Energie- und Wasserversorgung. SCADA-Netzwerke (SCADA = Supervisory Control and Data Acquisition) wiederum stellen Systeme und/oder Netzwerke dar, die mit ICS kommunizieren und den Betreibern Daten für die Überwachung und auch Kontrollmöglichkeiten für das Prozessmanagement liefern. Mit steigender Automatisierung nimmt auch der Einsatz von ICS-/SCADA-Systemen zu.

Infolge der Bedrohungen und Angriffe wie beispielsweise Stuxnet und Flame in den vergangenen zwei Jahren ist die Bedeutung der Sicherheit für ICS-/SCADA-Systeme viel diskutiert worden. Deren Sicherheitsmängel sind wohlbekannt und dokumentiert.[1]

Nicht nur SCADA steht im Mittelpunkt der Aufmerksamkeit, auch „Cloud Computing" wird in der heutigen IT-Welt diskutiert. Die Kombination der beiden Technologien aber löst weitere Debatten aus, einschließlich der damit verbundenen Kosteneinsparungen, Vorteile für die Systemredundanz und Verfügbarkeit. Und es stellt sich dabei immer die Frage: Wiegen die Einsparungen die Sicherheitsprobleme auf, die unter Umständen durch die Migration kompletter SCADA-Geräte in die Cloud entstehen?

Wozu SCADA-Geräte in die Cloud migrieren?

Die Cloud bietet der IT viele Einsatzmöglichkeiten. Und Unternehmen wie Apple und Google beweisen mit ihrem Angebot an integrierten, stabilen Cloud-Services, dass dies kein kurzlebiger Trend ist, der wieder verschwindet.[2] Zu den Vorteilen der Cloud-Nutzung gehören Kosteneinsparungen, Möglichkeiten der eingebetteten Sicherheit, die garantierte Verfügbarkeit sowie Systemredundanz.

SCADA-Geräte haben die gleichen Anforderungen wie andere kritische Systeme auch, nämlich Redundanz, Sicherheit, Kosteneinsparungen und hohe Verfügbarkeit. Mit der Migration dieser Geräte in die Cloud lassen sich verschiedene kritische Probleme lösen, so etwa das der Verfügbarkeit und Redundanz in ICS-Umgebungen (ICS = Industrial Control Systems).

1 http://www.trendmicro.de/media/wp/tm-wp-ics-scada-praxistestpumpstation-de.pdf
2 http://www.apple.com/icloud/; https://cloud.google.com/

ICS-Umgebungen sind berüchtigt für ihre hohen Anforderungen an die Verfügbarkeit. Hier kann die Cloud ihren Beitrag leisten. Zusätzlich zu den oben genannten Vorteilen ermöglicht es das Cloud Computing, von jedem beliebigen mit dem Internet verbundenen Standort aus einfach auf Daten in SCADA-Geräten zuzugreifen.

Aufgrund der Skalierbarkeitsmöglichkeiten lassen sich in nur wenigen Minuten neue Dienste auf den SCADA-Geräten aufsetzen. Die Migration von kritischen Geräten und/oder von Diensten in die Cloud kann zudem das Festlegen von Ausgangswerten für die Redundanz und Verfügbarkeit bei niedrigeren Kosten unterstützen

Vorteile bei Redundanz und Flexibilität

Mehr als 65 Prozent der Befragten in einer kürzlich von der InformationWeek durchgeführten Studie sind der Ansicht, dass die Fähigkeit, auf Geschäftsanforderungen schnell zu reagieren, sehr wichtig ist.[3]

Die Nutzung der Cloud kann hilfreich sein, wenn es um einen schnellen Zugriff auf Informationen auch in ICS- und SCADA-Geräten geht. Infolge der Möglichkeit, mithilfe der Cloud schnell eine Infrastruktur aufzubauen, lässt sich auch das Problem der Redundanz schnell lösen. Hinzu kommt, dass die Flexibilität dieser Methode ein schnelleres Geräte-Upgrade erlaubt, sollte mehr Speicherplatz oder CPU-Kapazität gebraucht werden.

3 http://www.informationweek.com/cloud-computing/software/time-to-think-about-cloud-computing/211300562

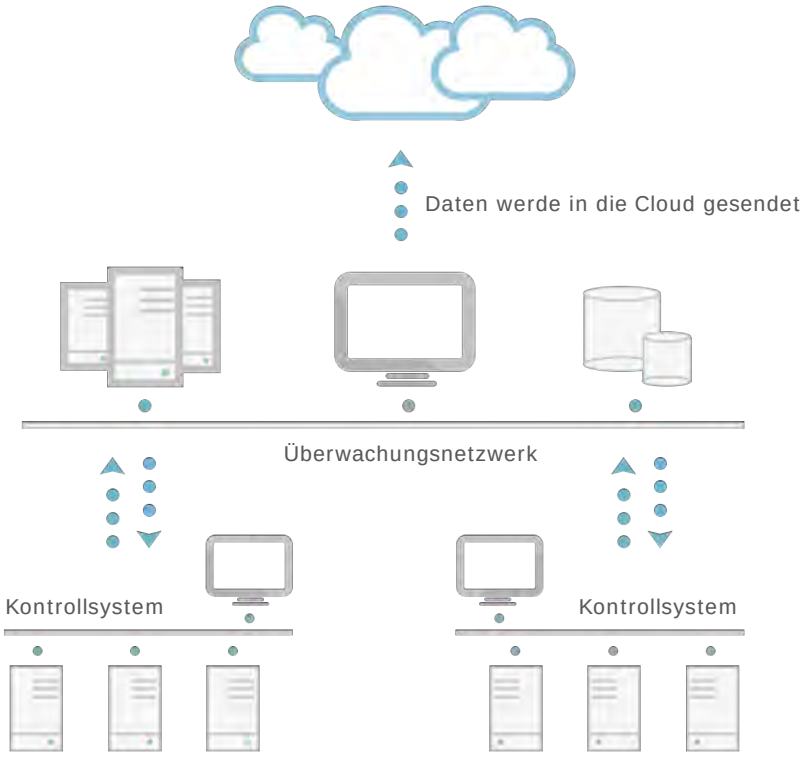


Abbildung 1:
Beispiel einer intern vorgehaltenen SCADA-Anwendung, in dem die Daten nach außen geschickt werden

Disaster Recovery und automatisierte Updates

Einer Studie der Aberdeen Group zufolge haben Cloud-Service-Provider viele der Probleme rund um Disaster Recovery im Griff. Unternehmen, die die Cloud nutzen, konnten beispielsweise die Probleme in durchschnittlich 2,1 Stunden lösen. Diejenigen aber, die keine Cloud nutzen, benötigten für dieselben Probleme acht Stunden.[4] Der Grund dafür liegt wahrscheinlich im Troubleshooting von möglichen Problemen hinsichtlich der Hardware.

Außerdem lassen sich auch automatisierte Updates direkt mit der Nutzung der Cloud in Verbindung bringen, denn die meisten Cloud-Service-Provider sind für die Server-Wartung verantwortlich, einschließlich dem Aufbringen von Sicherheits-Updates. Somit verschafft die Nutzung der Cloud IT-Administratoren mehr Zeit und Ressourcen für andere Projekte.

4 http://research.aberdeen.com/1/ebooks/Proven-Benefits-of-Backing-Up-Data-to-the-Cloud.pdf

Was bedeutet die Nutzung der Cloud für SCADA-Geräte?

Die Cloud lässt sich auf unterschiedliche Arten für SCADA-Geräte einsetzen. Hier werden lediglich zwei davon behandelt.

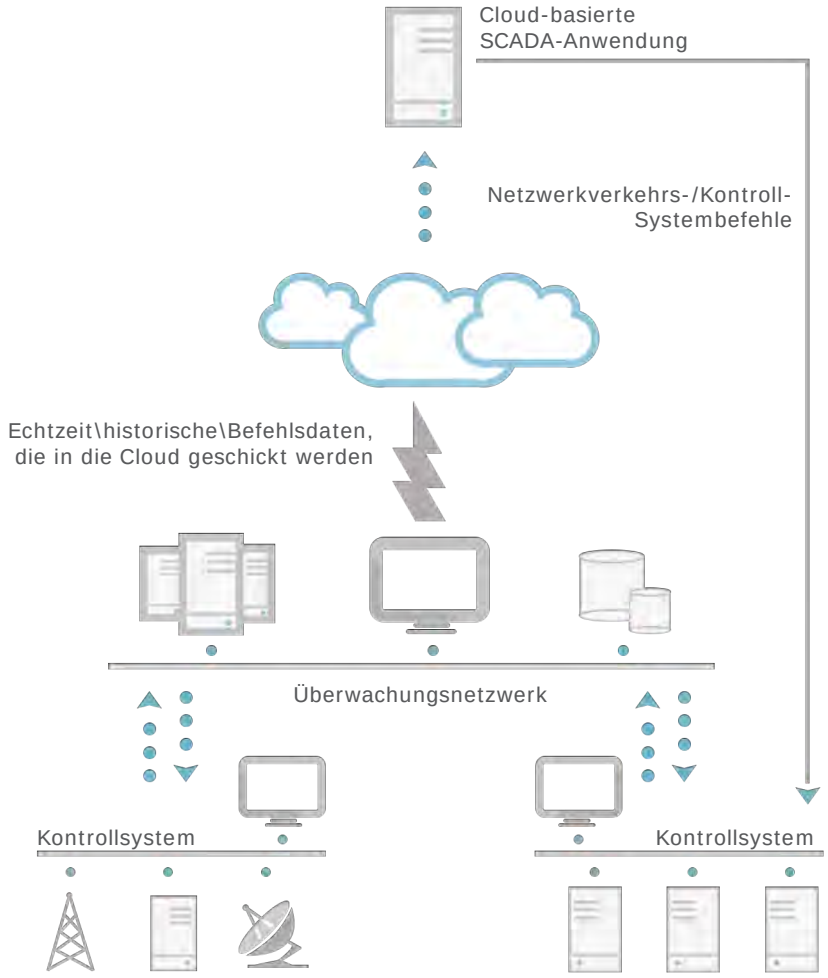


Abbildung 2:
Beispiel einer SCADA-Anwendung,
die komplett in der Cloud vorgehalten wird

Die erste Möglichkeit besteht darin, SCADA-Anwendungen direkt an ein Kontrollnetzwerk anzuschließen. Die Verarbeitung passiert dabei in der Cloud. Die zweite Möglichkeit ist, SCADA-Anwendungen komplett in der Cloud vorzuhalten, und Anweisungen zurück ans Kontrollgerät innerhalb des Unternehmensnetzwerks zu senden.

Anwendungen teilweise in der Cloud vorhalten

Cloud-basierte SCADA-Anwendungen werden meistens On-Premise installiert. Auf diese Weise sind die Anwendungen direkt mit dem Kontrollnetzwerk verbunden, und die Daten werden zu Analyse- und Zugangszwecken in die Cloud weiter geleitet. Dieses Setup ermöglicht es, das „Hochhieven" der für die Analyse über das Modell „Infrastructure-as-a-Service" (IaaS) zu handhaben.[5]

Komplett Cloud-basierte SCADA-Anwendungen

SCADA-Anwendungsarchitekturen können auch komplett in der Cloud betrieben und über eine Remote-Verbindung an das Kontrollnetzwerk angebunden werden. In einer solchen Architektur liegen die Daten entweder On-Premise oder in der Cloud, abhängig von den Anforderungen an die Anmeldung. Nachrichten bei der Kommunikation mit Command-and-Control-Servern werden für die Controller heruntergeladen und dann verarbeitet.

Unterschiede zwischen den beiden SCADA-Architekturtypen

Es bestehen signifikante Unterschiede zwischen den beiden beschriebenen Cloud-Architekturtypen. Im ersten Szenario liegt die SCADA-Anwendung auf der Hardware des Clients, üblicherweise im Kontrollnetzwerk. Zur Speicherung und Verarbeitung werden die Daten in die Cloud hochgeladen. Somit lässt sich die Datenverarbeitung und -abfrage in der Cloud durchführen. Die Kehrseite: Es ist ziemlich riskant, die vertraulichen ICS- und/oder SCADA-Daten in der Cloud zu lagern.

Das zweite Szenario umfasst eine Anwendung, die vollständig in der Cloud liegt. Die Anwendung generiert internen C&C-Verkehr und leitet diesen an die Controller auf der Client-Site. Diese Architektur birgt zwei hohe Sicherheitsrisiken:

- Ein Angreifer kann, je nach Wissen, die Echtzeitdaten und/oder Befehle, die von den ICS- oder SCADA-Geräten in die Cloud gehen, auf verschiedene Weise ausspionieren, fälschen, aufhalten oder modifizieren.
- Schickt wiederum eine Cloud-basierte Anwendung Befehle an die interne ICS- oder SCADA-Umgebung, so entsteht eine interne Verbindung, welche die Sicherheitsgeräte wie Firewalls umgeht. Damit aber wird ein Tor zu einem sicheren internen Netzwerk geöffnet, das typerweise geschlossen sein sollte, um Angreifer den Eintritt ins Netzwerk zu verwehren.

5 http://en.wikipedia.org/wiki/Cloud_computing

Sicherheitsrisiken

Das Konzept, kritische Geschäftsfunktionen in die Cloud zu migrieren, ist äußerst sinnvoll und auch sehr sicher. Dennoch müssen Anwender solcher Dienste sich einige Gedanken zu Sicherheitsbelangen im Zusammenhang mit der Art dieser Daten, Angriffen auf Webanwendungen, Kontrolle, Authentifizierung, Verschlüsselung und Protokollierung machen.

Art der Daten

Zwar behauptet jeder Cloud-Service-Provider, die Daten auf seinen Servern seien öffentlich nicht zugänglich. Doch ist zu bedenken, dass die Daten dennoch auf einem gemeinsam mit hunderten oder tausenden anderen Kunden genutzten Server liegen. Somit aber können andere sie absichtlich oder zufällig sehen. Einbrüche, wie der bei der Citigroup 2011, wo in der Cloud gespeicherte Daten kompromittiert wurden, sind ein Beispiel dafür.[6]

Die zu stellende Frage beim Speichern von Daten in der Cloud lautet: Ist es in Ordnung, wenn Dritte die gespeicherten Informationen einsehen können?

Angriffe auf Webanwendungen

Angriffe auf Webanwendungen stehen immer noch an erster Stelle bei den Bedrohungen für Cloud-Infrastrukturen.[7] Auch SCADA-Geräte sind gegen diese Angriffe nicht gefeit.

Diese Gefahr besteht natürlich auch, wenn die Geräte im lokalen Rechenzentrum stehen, doch ist sie höher, wenn ein Unternehmen die Dienste eines bekannten Cloud-Service-Providers nutzt. Es kann nämlich zum Opfer zufälliger Angriffe werden, das heißt, ein Angreifer scannt den IP-Bereich eines bekannten Cloud-Service-Providers und stößt dabei auf die SCADA-Anwendung, die er dann attackiert. Der Hacker mag über SCADA-Protokolle und -Geräte nicht allzu viel Spezialwissen besitzen, doch die Angriffsfläche des Unternehmens vergrößert sich automatisch, wenn es einen bekannten Provider wählt.

Die Frage, die sich ein Unternehmen hier stellen muss, lautet: Macht es mir etwas aus, wenn meine Anwendungen Zufallsangriffe auf sich ziehen? Was kann ich tun, um das Risiko zu verringern?

6 http://www.infoworld.com/d/security/citigroup-breach-exposed-data-210000-customers-664
7 http://www.alertlogic.com/resources/cloud-security-report/

Kontrollverlust

Durch die Datenmigration in die Cloud verliert das Unternehmen zum Teil die Kontrolle über die Informationen, zu deren Inhaber dann der Cloud-Service-Provider wird. Entscheidet dieser zum Beispiel, neue Verbindungen ins Backend seiner Infrastruktur zu integrieren, die mit dem SCADA-Anwendungsserver verbunden ist, so könnte es Verbindungen geben, von denen der Dateneigentümer nichts weiß. Auch die dadurch neu entstandenen Risiken bekommt der Kunde nicht mit. Ein kürzlich veröffentlichter Bloomberg-Artikel zeigt, wie private Daten in die Öffentlichkeit geraten können.[8]

Hier sollte sich ein Unternehmen folgende Frage stellen: Kann ich dem Cloud-Service-Provider vertrauen, der Updates an der Backend-Infrastruktur und den Verbindungen von Dritten an die Server, auf denen alle meine Daten liegen, durchführen kann?

Mängel bei der Authentifizierung

Die beiden bekanntesten SCADA-Protokolle – Modbus und DNP3 – weisen grundlegende Mängel auf bezüglich der Möglichkeiten der Authentifizierung. Viele SCADA-Protokolle unterstützen keine Authentifizierung oder führen sie nicht durch.[9] Damit aber findet auch kein „Vertrauens-Check" zwischen zwei Parteien statt, die über DNP3 oder Modbus interagieren. Es gibt aber eine DNP3-Version („Secure DNP3") die Authentifizierung unterstützt, wenn auch nicht auf älteren Kontrollsystemen.

Nutzt nun ein Teil einer Cloud-basierten SCADA-Architektur, vor allem in einer öffentlichen Cloud, eines dieser Protokolle, so kann ein Angreifer nicht nur IP-Adressen einfach nachahmen, sondern auch Nutzernamen und Netzwerkverkehr, und sich so einen Zugang zu Daten verschaffen, den er ansonsten nicht erlangt.

Bezüglich der Sicherheitsprobleme ist die wichtigste Frage daher: Welchen Risiken bin ich ausgesetzt, falls ein Angreifer Zugang zu meinen nicht authentifizierten Daten erhält?

Keine Verschlüsselung

Nicht nur bezüglich der Authentifizierung weisen SCADA-Protokolle Mängel auf, sondern sie ermöglichen auch keine Form der Verschlüsselung, um die Daten zu schützen. Vor allem Modbus und DNP3 unterstützen von Haus aus keine Art der Verschlüsselung und öffnen somit „Man-in-the-Middle-Angriffen und dem Ausspionieren des Verkehrs Tür und Tor.[10] Diese Methoden ermöglichen es Angreifern, nicht nur die Daten unterwegs zu sehen, sondern auch den Verkehr mit allen gewünschten Änderungen an jedes Gerät umzuleiten.

Gerade wenn Cloud-basierte Services für SCADA-Umgebungen mit den genannten Protokollen im Einsatz sind, stellt dieser Mangel eine erhebliche Sicherheitslücke dar. Diese Tatsache müssen Sicherheitsverantwortliche bei der Migration von SCADA-Geräten in die Cloud unbedingt berücksichtigen.

Hier ist die folgende Frage von Bedeutung: Macht es etwas aus, wenn Angreifer meine kritischen Kontrollsystemdaten sehen?

8 http://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html
9 http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf
10 http://de.wikipedia.org/wiki/Man-in-the-middle-Angriff

Die Logging-Zwickmühle

Wie bei jeder Service-Lösung stellt auch hier die Protokollierung die Verantwortlichen vor eine Herausforderung. Während die lokale Protokollierung von Daten relativ einfach zu bewerkstelligen ist, so ist das Rückführen von Logs über eine WAN-Verbindung (WAN = Wide Area Network) schon schwieriger und häufig unzuverlässig für ein zentrales SIEM-System (SIEM = Security Information and Event Management).[11] Außerdem erfordert diese Rückführung von Logs in die Unternehmensinfrastruktur das Vorhandensein von Firewall-Regeln, um die Verbindung zu erlauben. Diese öffnet die Kommunikation von außen zu einem sicheren, vertrauenswürdigen Netzwerk – ein erhöhtes Sicherheitsrisiko.

Di e Log-Übertragung an eine interne Logging-Infrastruktur wird häufig im Klartext durchgeführt – unter Umständen ein gefundenes Fressen für MiTM-Techniken.

Die diesbezüglich wichtigste Frage lautet: Welche Sicherheitsrisiken würden entstehen, wenn ich den Zugang zu meinen ICS- und/oder SCADA-System-Logs verliere?

Was kann ein Unternehmen für die Sicherheit tun?

Will ein Unternehmen SCADA in der Cloud nutzen, kann es einiges tun, um die Cloud zu sichern und die Daten zu schützen. Die folgende Liste umfasst jedoch nicht alle Lösungen:

- „Internet Protocol Security“ verwenden: Wenn möglich, sollten Anwender die Vorteile von IPSec nutzen. IPsec unterstützt sowohl Authentifizierung als auch Verschlüsselung und erschwert es Angreifern, in Cloud-basierten SCADA-Systemen zu schnüffeln sowie Netzwerkverkehr zu ändern oder nachzuahmen.
- Sichere Protokolle einsetzen: Verwenden Organisationen, soweit vorhanden, sichere Protokolle (etwa „Secure DNP3“), so sparen sich Verantwortliche einige Probleme bezüglich der Authentifizierung und Verschlüsselung. [12]
- Gespeicherte Daten („Data at Rest“) verschlüsseln: Die Verschlüsselung von gespeicherten Daten in einer ICS- oder SCADA-Umgebung ist nicht immer von Vorteil, doch in einer Cloud-Umgebung hat das Verfahren einen erheblichen Nutzen. Sollten Angreifer beispielsweise Daten kompromittieren, die auf dem Server eines Cloud-Service-Providers liegen, so wird es für sie schwer, diese zu entschlüsseln und die Informationen zu lesen. Deshalb ist es immer empfehlenswert, Verschlüsselung für Daten, die außerhalb des eigenen Unternehmens liegen, zu verwenden.

11 http://en.wikipedia.org/wiki/Security_information_and_event_management
12 http://www.digitalbond.com/scadapedia/protocols/secure-dnp3/

- Gründliche Protokollierung durchsetzen: Wenn möglich, sollten alle Logs an eine zentrale Logging-Lösung geschickt werden. Verantwortliche müssen auch für Redundanz in der Logging-Lösung sorgen und dafür, dass so viele Logs wie möglich an ein SIEM weiter geleitet werden. Einen guten Anfang machen System-, Sicherheits-, Netzwerk- und Anwendungs-Logs von Windows-Workstations.
- Wasserdichte Verträge aufsetzen: Solide Vereinbarungen mit dem Cloud-Dienstleister sind wichtig, um sicherzustellen, dass nicht gewollte Verbindungen Dritter auf dem eigenen Server nicht erlaubt sind. Damit wird der Vertrag vielleicht etwas teurer, doch die Sicherheit erhöht sich signifikant.
- „Virtual Private Networks“ (VPNs) oder „Secure Sockets Layer“ (SSL) nutzen: Der Einsatz von Site-to-Site-VPNs, SSL-VPNs oder SSL-Verkehr bringt viele Sicherheitsvorteile. Damit ist sichergestellt, dass die Kommunikation von der Quelle bis ans Ziel immer geschützt ist und kein Schnüffeln und/oder „Spoofing“ möglich ist.
- Vorhandene Sicherheitslösungen einsetzen. Falls mehrere Sicherheitslösungen verfügbar sind, sollten Anwender eine wählen, die folgende Fähigkeiten besitzt:
  - Sie kann die Ausführung von Programmen, die nicht auf einer bewilligten Anwendungsliste stehen, verhindern.
  - Sie ist leicht zu installieren und kann aktualisiert werden, ohne die Komponenten zu stoppen.
  - Sie hat einen kleinen „Footprint“ im Vergleich zu anderen Endpoint-Sicherheitslösungen, die auf großen Pattern-Dateien basieren, die ein stetiges Aktualisieren erfordern.
  - Sie nutzt eine rollenbasierte Administration, die die Kontrolle während der Installation und des Setups sicherstellt, sowie einfaches Monitoring und die Wartung während des Betriebs liefert.
  - Sie verfügt über grafische sowie Befehlszeilen-Schnittstellen, um ein einfaches, bequemes Arbeiten damit zu gewährleisten:
  - Sie arbeitet mit anderen Sicherheitslösungen zusammen, die dazu dienen, Bedrohungen von Geräten direkt und einfach zu entfernen.

Schlussfolgerungen

Wie auch die meisten IT-Unternehmen können ICS- und/oder SCADA-Controller die Vorteile der Cloud nutzen. SCADA-Geräte unterscheiden sich nicht von anderen kritischen Systemen, denn sie benötigen wie alle anderen Redundanz, Sicherheit, möglichst niedrige Kosten und eine hohe Verfügbarkeit. Werden SCADA-Geräte in der Cloud betrieben, so dient das beispielsweise der höheren Verfügbarkeit von ICS-Umgebungen.

Leider haben diese Vorteile für SCADA-Umgebungen in der Cloud auch ihre Schattenseiten, denn sie bieten auch Angreifern Chancen, einen Fuß in die Tür zu zuverlässigen Umgebungen zu setzen. Die Anwender von Cloud-Diensten müssen sich um verschiedene Sicherheitsaspekte in Bezug auf die Art der Daten, Angriffe auf Webanwendungen, Kontrolle, Authentifizierung, Verschlüsselung und Protokollierung kümmern.

Die Besitzer von SCADA- und/oder ICS-Geräten sollten die Cloud mit Vorsicht nutzen, solange die Sicherheit für SCADA und ICS nicht vollständig gewährleistet werden kann.

Referenzen

- http://blog.trendmicro.com/trendlabs-security-intelligence/no-excuses-when-it-comes-to-data-security/
- http://en.wikipedia.org/wiki/Cloud_computing
- http://en.wikipedia.org/wiki/Man-in-the-middle_attack
- http://en.wikipedia.org/wiki/Security_information_and_event_management
- http://research.aberdeen.com/1/ebooks/Proven-Benefits-of-Backing-Up-Data-to-the-Cloud.pdf
- http://www.alertlogic.com/resources/cloud-security-report/
- http://www.apple.com/icloud/
- http://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html
- http://www.digitalbond.com/scadapedia/protocols/secure-dnp3/
- http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf
- http://www.informationweek.com/cloud-computing/software/time-to-think-about-cloud-computing/211300562
- http://www.infoworld.com/d/security/citigroup-breach-exposed-data-210000-customers-664
- https://cloud.google.com/

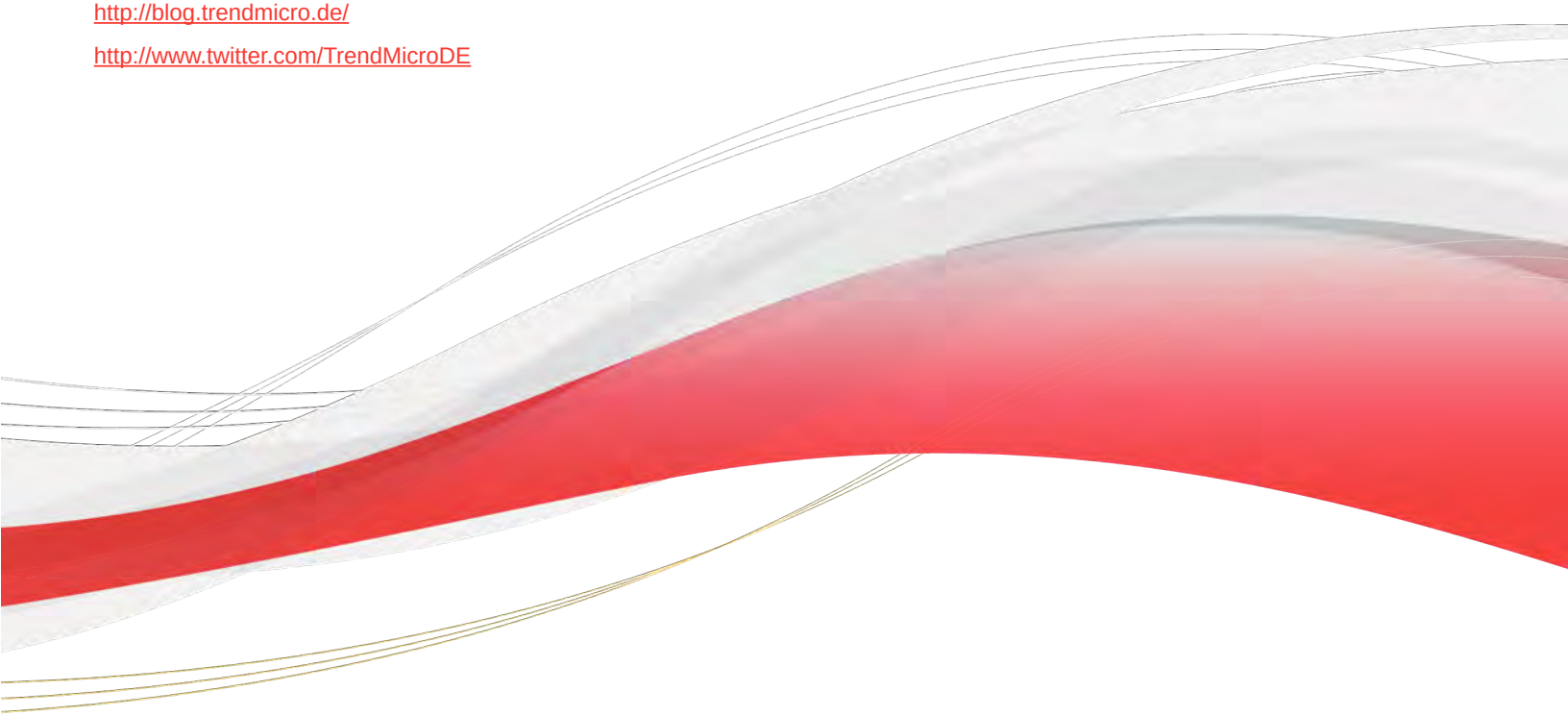
Über TREND MICRO

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/

http://blog.trendmicro.de/

http://www.twitter.com/TrendMicroDE



TREND MICRO™

Securing Your Journey to the Cloud

TREND MICRO DEUTSCHLAND GMBH
Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com