



## Stuxnet – Alarmsignal für Industrieunternehmen

### Vernetzte Produktionsanlagen sind anfällig – Sicherheitszonen und die Kontrolle externer Zugriffe bieten Schutz



Die nahezu vollständige Vernetzung aller Lebens- und Arbeitsbereiche bietet uns immer neue Möglichkeiten: Wir können ständig und ganz unkompliziert mit anderen

Personen kommunizieren, Freunde gewinnen, die wir gar nicht kennen, gepriesene Urlaubsziele und Hotels vorab aus allen Perspektiven begutachten, zu jeder denkbaren Frage eine Vielzahl von Informationen finden, effizient mit Kollegen weltweit zusammenarbeiten oder komplexe Maschinen steuern und schon in Kürze sicher noch vieles mehr. Dieses flächendeckende Netz ist oftmals sehr nützlich – aber auch gefährlich: Denn nicht alle Informationen und Dateien sollen überall hin. Es muss gesteuert werden, wer wann worauf zugreifen darf und wer nicht. Dies gilt sowohl für den privaten wie auch den Industriebereich. Hier hat Stuxnet eine Schwachstelle aufgezeigt, für die wir eine sichere Lösung bieten.

Aber nicht alles geht online besser. Komplexe Fragestellungen können mit Kunden häufig bei einem klassischen Vor-Ort-Termin viel besser geklärt werden. Um die Wege kurz zu halten, hat GeNUA in Köln eine Service-Niederlassung eröffnet – wir freuen uns auf Sie!

Dr. Michaela Harlander  
Geschäftsführerin GeNUA mbH

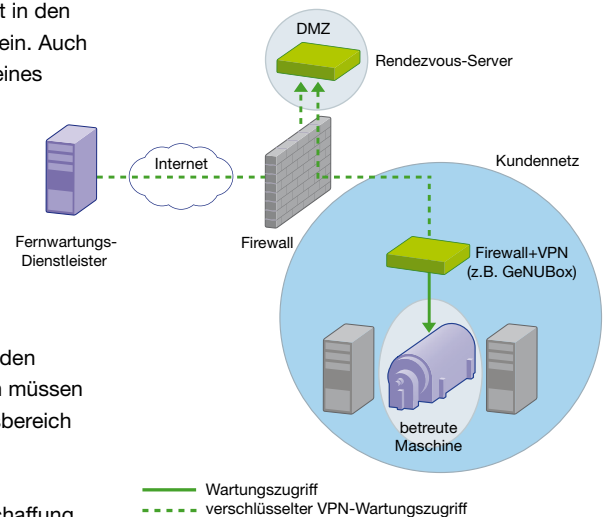
Stuxnet hat weltweit die Aufmerksamkeit auf eine Schwachstelle gelenkt, die bisher kaum beachtet wurde: Viele Industrieunternehmen haben ihre Anlagen vollständig automatisiert und vernetzt, um effizient produzieren zu können – häufig ohne für ausreichende IT-Sicherheit bei den verbundenen Systemen zu sorgen. Jetzt kommt der Schadcode Stuxnet und nistet sich massenhaft in den Steuerungssystemen für die Simatic S7 ein. Auch wenn Stuxnet offensichtlich das Werk eines Spezialisten-Teams ist, zeigt gerade die wohl ungewollte, schnelle Verbreitung dieses Codes, wie anfällig Industrieanlagen gegen Hacker-Angriffe sind. Die Experten sind sich einig: Es wird schnell Nachahmer geben – von Kriminellen über Terroristen bis hin zu Freizeit-Hackern – die über diesen Weg erheblichen Schaden anrichten können. Industrieunternehmen müssen deshalb die IT-Sicherheit im Produktionsbereich verbessern.

Eine grundlegende Maßnahme ist die Schaffung einer eigenen Sicherheitszone für die Systeme der Produktionsabteilung. Diese Zone wird mit internen Firewalls von anderen Bereichen des lokalen Firmennetzes abgetrennt, so dass nur die Steuerungs-Software WinCC auf die S7-Anlagen zugreifen kann. Denn weder die Buchhaltung, der Vertrieb oder die Personalabteilung müssen auf die Systeme der Produktionsabteilung zugreifen – sie sind aber mit ihren zahlreichen PC-Anwendern und Außenkontakten gut erreichbare Angriffsziele für Hacker. Sollte z. B. über einen unterwegs infizierten Laptop Schadcode in das Vertriebsnetz eindringen, kann er von hier nicht auf die Produktions- und Steuerungssysteme weiter wandern, da die internen Firewalls keine Verbindung zulassen.

Nicht alle Verbindungen in die Sicherheitszone der Produktions-Server können gekappt werden. Denn viele Industrieunternehmen lassen ihre zahlreichen Maschinenanlagen von den Herstellerfirmen via Fernzugriff betreuen, um den störungsfreien Betrieb sicherzustellen. Für die Fernwartung müssen die Hersteller via Internet auf die Steuerungssysteme der Anlagen zugreifen

können. Diese externen Zugänge in das Netz der Produktionsabteilung müssen zuverlässig abgesichert werden, da hier sonst durch Unachtsamkeit oder Missbrauch Schadcode eindringen kann.

#### Sichere Fernwartung über Rendezvous-Server



#### Sichere Fernwartungs-Lösung: Rendezvous in der DMZ

Zur Fernwartung von Maschinenanlagen in sensiblen Produktionsbereichen hat GeNUA die Rendezvous-Lösung entwickelt. Das Konzept: Es werden keine einseitigen Wartungszugriffe von Herstellern in das Netz des Industrieunternehmens zugelassen. Stattdessen führen alle Fernwartungs-Zugriffe auf einen Rendezvous-Server, der in einem speziellen Bereich neben der Firewall, der so genannten demilitarisierten Zone (DMZ), installiert ist. Hierhin kommt das Industrieunternehmen dem Hersteller mit einer Verbindung von innen aus dem Produktionsbereich entgegen. Erst wenn es auf dieser zentralen Wartungsplattform zum Rendezvous kommt, kann der Hersteller die jetzt durchgängige Verbindung zum Zugriff auf die betreute Anlage nutzen. Die Verbindungen zu dem Rendezvous-Server werden mit dem VPN-Verfahren (Virtual Private Network) SSH aufgebaut, das starke Verschlüsselungs- und Authentifizierungs-Verfahren bietet. So kann die Datenkommunikation nicht abgehört werden, und nur berechtigte Teilnehmer erhalten

Zugang zur Wartungsplattform in der DMZ. Das Protokoll SSH unterscheidet sich zudem in einem wesentlichen Punkt vom dem VPN-Verfahren IPsec, das andere Herstellern häufig zum Aufbau von Fernwartungs-Verbindungen verwenden: IPsec erzeugt immer eine vollständige Koppelung zwischen den verbundenen Netzen. Sollte ein Rechner in einem Netz mit Schadcode infiziert sein, kann er in allen via IPsec angebotenen Netzwerken ungeschützte Systeme befallen und sich rasant ausbreiten. Mit SSH werden dagegen nur die tatsächlich notwendigen Verbindungen zwischen einzelnen Rechnern erzeugt, so dass Schadcode keine schnellen Verbreitungswege findet.

### Kein Weiterkommen: Firewall isoliert Wartungsbereich

Bei der Lösung von GeNUA sorgt im Produktionsbereich zusätzlich die Fernwartungs-Appliance GeNUBox für Sicherheit. Sie wird an der per Fernzugriff betreuten Anlage installiert und separiert mit einer Firewall-Funktion den Wartungsbereich vom den anderen Systemen in diesem Netzbereich. So führt die SSH-Verbindung ausschließlich zum Wartungsobjekt – Zugriffe auf andere Systeme im Netz der Produktionsabteilung sind nicht möglich. Selbst wenn Schadcode bis hierhin vordringen sollte, kann er von dieser isolierten Anlage aus keine weiteren Systeme infizieren.

## Firewalls sichern Ergebnis der Bundestagswahl

### Statistisches Bundesamt schützt Webserver mit Firewall-Cluster von GeNUA

Bei jeder Bundestags- und Europawahl kommt es bei Destatis (Statistisches Bundesamt) zu einem massiven Ansturm aus dem Internet. Sobald die ersten Stimmen gezählt sind, laufen die Ergebnisse aller Wahlkreise bei dem Amt in Wiesbaden zusammen und werden auf der Webseite des Bundeswahlleiters veröffentlicht. Hierauf wird innerhalb kurzer Zeit sehr häufig zugegriffen – bei der Bundestagswahl 2005 wurden in der Spitze fast 1,4 Millionen Hits pro Stunde gezählt. Auf diese besondere Situation musste die IT auch für die Bundestagswahl 2009 vorbereitet werden: Destatis installierte hierfür mehrere zusätzliche Server mit je drei Webserver-Instanzen und davor eine Phalanx zertifizierter Firewalls mit Load Balancing-Funktion, um alle Anfragen ohne Downtime möglichst schnell zu bedienen und die Webseiten vor Manipulationen zu schützen.

Weiter lesen: [www.genua.de/genuletter](http://www.genua.de/genuletter)



Statistisches Bundesamt in Wiesbaden

## GeNUA News

### GeNUBox 3.0: Zentrale Administration und neue Hardware

Mit der Sicherheits-Plattform GeNUBox werden geschützte Verbindungen via Internet aufgebaut, über die Maschinenhersteller komfortabel per Fernzugriff z. B. Fertigungsroboter oder Stromgeneratoren warten können, die weltweit bei ihren Kunden installiert sind. Die GeNUBox 3.0 kann jetzt über die Management Station GeNUCenter administriert werden, dem einheitlichen Verwaltungs-Tool für alle Sicherheitslösungen von GeNUA. So lassen sich zahlreiche Sicherheits-Plattformen und Fernwartungs-Verbindungen mit wenig Aufwand konfigurieren und betreiben. Zudem ist die GeNUBox 3.0 auf drei neuen Hardware-Plattformen für unterschiedliche Einsatzumgebungen erhältlich.



- GeNUBox 100C mit Display für Statusanzeigen und Smartcard Reader, über den der Key für das VPN eingesteckt wird, für Einbau in Server Racks
- GeNUBox 100IM mit Display zur Hutschienenmontage in Schaltschränken
- GeNUBox 100B für Einsatz in Bürumgebungen

Weitere Infos:  
[www.genua.de/genubox](http://www.genua.de/genubox)

### Service-Niederlassung in Köln eröffnet

Kunden von GeNUA bekommen zumeist schnellen Service via Internet – manchmal ist aber auch der Einsatz eines Spezialisten vor Ort erforderlich. Um auch in diesen Fällen umgehend reagieren zu können, hat GeNUA im Juli eine Service-Niederlassung in Köln eröffnet. Von hieraus erhalten die zahlreichen Kunden in Nordrhein-Westfalen über kurze Wege schnellen Vor-Ort-Support.

© Randy Glasbergen  
glasbergen.com



**“I knew it was time to simplify our organization  
when we started creating acronyms for our acronyms.”**