Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 102 (2011)
Heft: (10)

Artikel: Im Visier von Viren, Würmern und Trojanern
Autor: Zwienenberg, Righard
DOI: https://doi.org/10.5169/seals-856863

Im Visier von Viren, Würmern und Trojanern

Cyberkriminalität und IT-Sicherheit in der Industrie

Der Supervirus Stuxnet hat gezeigt, wie anfällig industrielle Infrastrukturen sind, und dass sie Cyberangriffen gegenüber oft schutzlos sind. Auch wenn derzeit noch keine Schwemme von Industrieviren zu erwarten ist, sollten Unternehmen das Problem nicht unterschätzen: Stuxnet könnte der Anfang gezielter Sabotage- und Spionageattacken sein.

Righard Zwienenberg

Cyberattacken auf Industrieanlagen sowie staatliche Institutionen haben deutlich gemacht, dass dem Schutz der Infrastrukturen für Strom, Wasser, Kommunikation und Produktion höchste Priorität eingeräumt werden muss. So zielte der im Juli 2010 aufgetauchte Stuxnet-Wurm auf eine spezifische Konfiguration in Scada-Systemen von Siemens ab und umfasste einen Trojaner, mit dem PLCs (speicherprogrammierbare Steuerungen in sicherheitskritischen Systemen im industriellen Umfeld) umprogrammiert werden können.

Stuxnet ist ein hochentwickelter Virus, der ausgesprochen gezielt vorgeht und dessen Gefährlichkeit unter anderem auf seinem Verbreitungsweg beruht: Er nutzt alles, was an einen PC als Laufwerk angeschlossen werden kann. Jedes Gerät mit einer Drahtlosverbindung ist ein potenzieller Virus-Träger: ob USB-Stick, Mobiltelefon, Digitalkamera etc. Einmal angeschlossen, findet Stuxnet den Weg durch das Netz zu den Steuerungssystemen von alleine. Seit bekannt wurde, dass der Supervirus auf dem Schwarzmarkt gehandelt wird, könnte die Gefahr, dass praktisch jeder Malware-Autor diesen nutzen kann, rasant mutieren.

Es ist deshalb nur eine Frage der Zeit, bis Stuxnet oder ein Nachfolgevirus weit genug entwickelt ist, um Schäden an Kontroll- und sonstigen Systemen anzurichten, in denen infizierte Endgeräte genutzt werden (Bild 1).

Lösungen und Standards mit Hindernissen

Stuxnet hat Spuren hinterlassen und gezeigt, dass sich Malware-Angriffe nicht mehr nur auf die Office-Welt beschrän-

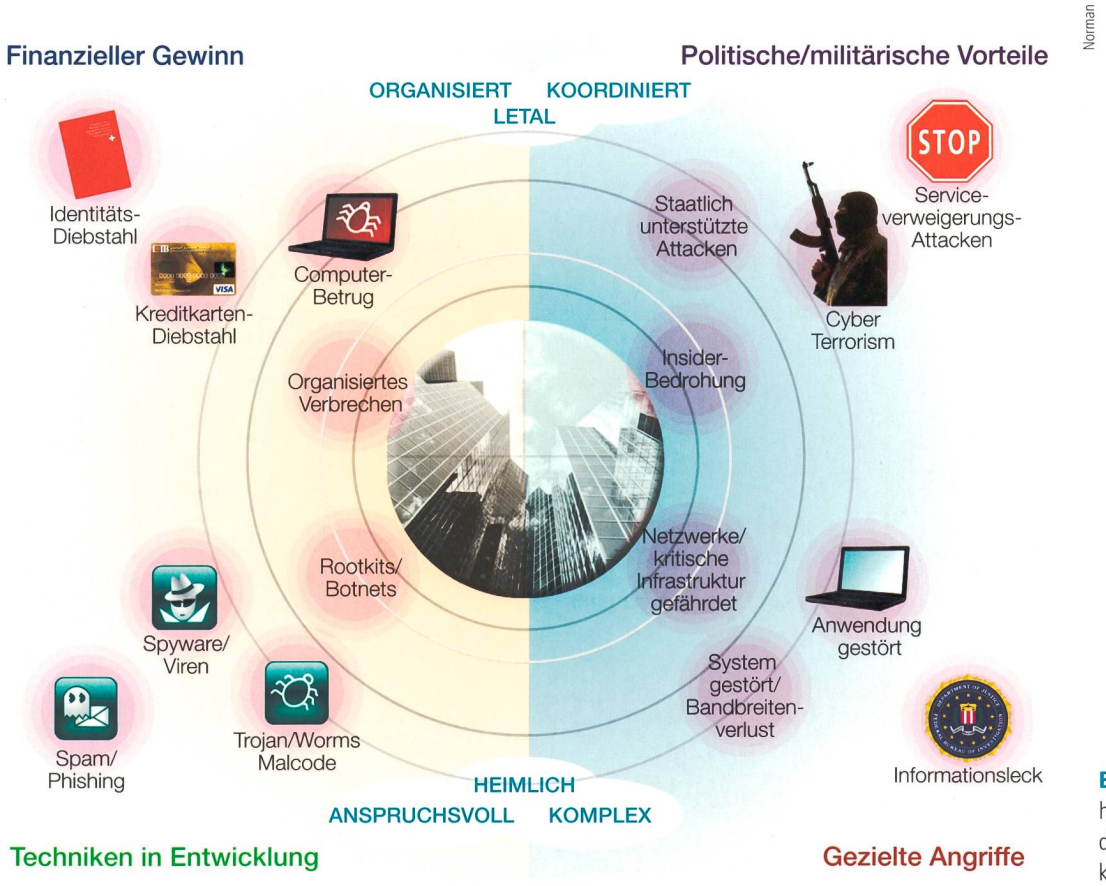
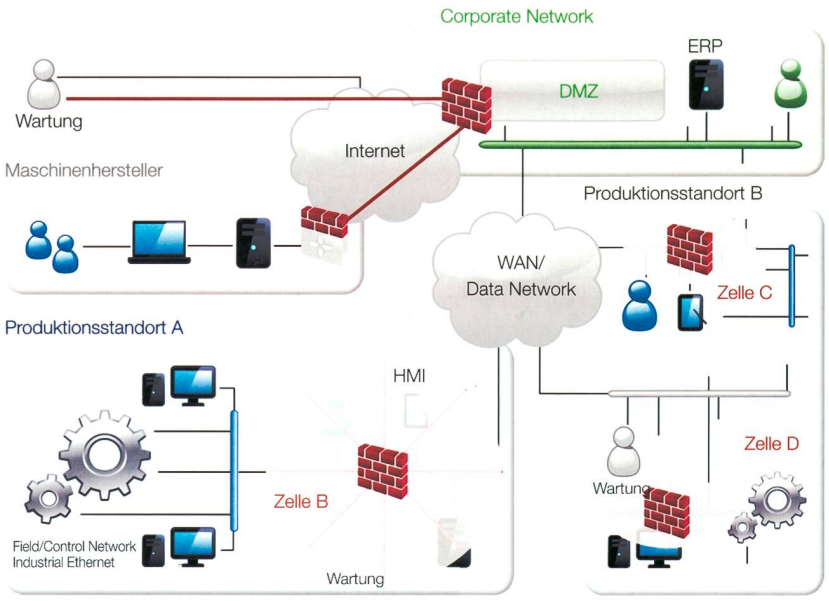


Bild 1 Die Bedrohungsszenarien aus dem Cyberspace sind komplex, zielgerichtet und vielfältig motiviert.

ken, sondern auch, dass das industrielle Umfeld nicht ausreichend vor Angriffen geschützt ist. Dies aufgrund des Zusammenwachsens von IT und Produktion sowie der Vereinheitlichung von Kommunikationsinfrastrukturen. Denn um effizient produzieren zu können, haben immer mehr Unternehmen ihre Anlagen automatisiert, sich die Vorteile einer durchgängigen Vernetzung zunutze gemacht und setzen vermehrt Lösungen und Standards aus dem Office-Umfeld ein: Von PC-Techniken in Maschinen, über das Internetprotokoll TCP/IP bis hin zu Industrial Ethernet, das die Office- und die Produktionswelt verbindet und die zentrale Steuerung aller Prozesse direkt aus den PPS- (Produktionsplanungs- und Steuerungs-) sowie ERP-Systemen ermöglicht.

Mit dem Office-LAN, dem Intranet und dem Internet verbunden, sind die Wege für Malware zu den Produktionssystemen automatisch geöffnet. Viren, die bisher in Office-Netzen für Datenverluste und Ausfallzeiten sorgten, nutzen neu Standardprotokolle, um in bisher isolierte Netzwerkbereiche zu gelangen. Malware, die Lücken wie ungepatchte Schwachstellen oder infizierte mobile Geräte entdeckt, kann jetzt ungehindert bis ins Produktionsnetz und in Automatisations-Umgebungen vordringen.

Während im Büro die IT-Sicherheit parallel mit der Internet- und Netzwerkentwicklung gewachsen ist, hinkt die Industrie dieser Entwicklung klar hinterher. Die möglichen Auswirkungen im industriellen Umfeld sind jedoch weit gravierender als im Office-Umfeld, da Störungen zu Produktionsstillständen mit enormen Verlusten führen können (Bild 2).



TÜV Rheinland i-sec

Bild 2 Typische IT-Landschaft in der Produktion mit eingebauter Sicherheitstechnologie.

Office und Industrie: zwei verschiedenen Welten

Im langjährigen Kampf hat die Office-Welt praktikable Strategien und Produkte gegen Malware entwickelt. Viele Unternehmen gehen deshalb davon aus, dass die dafür entwickelte Security-Lösungen wie Firewall, Virenschutz, Patch-Management und Intrusion Prevention Systeme (IPS) auch für vernetzte Produktionsanlagen und Automatisierungssysteme ausreichen und sich 1:1 auf die jeweilige Umgebung übertragen lassen. Jede Produktions- und Automatisierungslösung ist jedoch individuell und die Interaktion unter Umständen sehr komplex. So werden z.B. On-Access-Scanner auf den Produktionssystemen so gut wie nie genutzt, weil der Ressourcenbedarf des Scanprozesses den Verkehr der Produktionsdaten beeinträchtigen und den Produktionsprozess zum Erliegen bringen kann.

Virenscanner können Steuerungsprozesse stören, die als Echtzeitprozesse auch im ungünstigsten Fall definierte Antwortzeiten einhalten müssen, damit es nicht zu Personen- oder Sachschäden kommt. Lokaler Malwareschutz kommt nicht in Frage, da er ebenfalls Echtzeitprozesse beeinträchtigen kann oder weil Herstellergarantien erlöschen können.

Die Radikallösung, die Verbindung des Produktionsnetzes zum Intranet bzw. Internet zu kappen, dürfte in den meisten Unternehmen mit erheblichen Konsequenzen verbunden und deshalb nicht praktikabel sein. Weiter stellen IT-Systeme in der Industrie besondere Ansprüche an die Verfügbarkeit, Robustheit und an Parameter wie Echtzeitfähigkeit. Anders als in der Bürowelt, in der Computer unabhängig voneinander agieren, sind Produktions-PCs zur Steuerung komplexer Maschinen und Anlagen aufeinander abgestimmt und ununterbrochen in Betrieb. Jedes Reboot-Update an Produktions-PCs hat deshalb eine Unterbrechung des Gesamtablaufes zur Folge und verursacht hohe Kosten durch Produktionsausfall.

Sind PC-Systeme Bestandteil von Maschinensteuerungen, kann das Aktualisieren und Patchen der Software eine Veränderung der Systeme darstellen, die zum Verlust der Herstellergarantie führen kann. Produktionsnahe PC-Systeme laufen deshalb meist mit älteren, seit Jahren nicht aktualisierten oder gepatchten Betriebssystemen und Anwendungen.

Smart Meter als Netzwerkkomponenten

Eine besondere Herausforderung hinsichtlich IT-Sicherheit kommt auf die Energieversorger zu: Mit dem Ausbau in Richtung intelligenter Stromnetze (Smart Grids), wird sich der Einsatz von Informationstechnologien in Energieversorgungsnetzen weiter verstärken. Denn mit Smart Grids werden nicht nur die Erzeugung, der Transport, die Speicherung, die Verteilung und der Verbrauch von Strom gesteuert und kontrolliert. Das Strom- und Datennetz wird miteinander verknüpft und alle Akteure, das heisst Stromerzeuger, -verbraucher und -speicher untereinander vernetzt. Je vernetzter, desto mehr Angriffspunkte entstehen und desto anfälliger ist ein Unternehmen für Angriffe von aussen. Mit intelligenten Stromzählern (Smart Meter), die in Privathaushalten zur Anwendung kommen sollen, wird der Stromverbrauch zwar kontrollier- und regelbar gemacht, indem Informationen über ein Datennetz ausgetauscht und Steuerbefehle empfangen werden. Smart Meter sind jedoch nicht nur Messgeräte mit einer Verbrauchsanzeige, sondern auch Netzwerkkomponenten, die Zählerdaten senden und empfangen. Diese zu manipulieren, um durch gezielte punktuelle Überlastung Stromausfälle hervorzurufen oder die

Stromverteilung bewusst umzulenken, ist ein reales Szenario.

Das Risiko Mitarbeiter

Eine kürzlich von Norman durchgeführte Umfrage ergab, dass mehr als die Hälfte der befragten Personen bei Sicherheitsaspekten am eigenen PC/Laptop mehr Vorsicht walten lässt als am Dienstgerät. Es verwundert deshalb nicht, dass die Gefährdung von Netzwerken und Netzwerkteilnehmern zum grössten Teil von innen – und nicht wie oft vermutet, von ausserhalb einer Anlage – kommt und die meisten Datenverluste von Mitarbeitern verursacht werden. Nicht aus böser Absicht, sondern aus Unachtsamkeit oder Fahrlässigkeit. Dabei sind oft mobile Datenträger involviert, die verloren gehen oder gestohlen werden. Dass deren Daten in falsche Hände geraten, kann nicht ausgeschlossen werden, da schätzungsweise mehr als 40 % der Datenträger nicht verschlüsselt sind. Die Überwachung der Schnittstellen und der Geräte, die an den Office-PC angeschlossen werden, spielt deshalb eine zentrale Rolle beim Schutz vor Datendiebstahl und -verlust. Zwar sind auf dem Markt eine ganze Reihe von Verschlüsselungstechniken und Lösungen erhältlich, mit denen sich der Zugriff nicht registrierter mobiler Geräte auf Unternehmensressourcen reglementieren lässt. Der grösste Schwachpunkt der mobilen Wegbegleiter besteht aber darin, dass IT-Abteilungen oft nicht den Überblick über alle Geräte haben, die im Einsatz stehen und diese nicht in eine vorhandene Sicherheitsstrategie mit einbeziehen können.

Überwachung der Schnittstellen

Ein weiterer Knackpunkt für IT-Verantwortliche liegt darin, dass sich die Nutzer- und Sicherheitsprofile dieser Tools nicht immer fixieren lassen. Fehlt beispielsweise ein Policy-Enforcement-Modul auf den Handhelds der Mitarbeiter, kann jeder Anwender firmenspezifische Voreinstellungen wie Netzwerkverbindungen nach seinem Gusto ändern, Dateien löschen und Software installieren. Ohne es zu ahnen, werden dadurch Viren ins Netzwerk eingeschleust. Der Schaden ist vorprogrammiert, denn meist erfolgt die Prüfung solcher Endgeräte erst während des Logins. Zu diesem Zeitpunkt hat das Endgerät jedoch bereits uneingeschränkten Zugang ins Netzwerk. Das DHCP (Dynamic Host Configuration Protocol) ist erfolgreich durchlaufen, der volle IP-Zugang zum lokalen Netzwerk besteht und Malware kann sich verbreiten. Ein Regelwerk, das festhält, welche Mitarbeiter welche Rechte in Bezug auf welche Daten einhalten und wer Zugriff auf welche Daten erhält, ist deshalb empfehlenswert. Doch Regeln allein helfen nicht, solange deren Einhaltung nicht überwacht wird. Zur Strategie im Zusammenhang mit Datenschutz und -sicherheit sollte eine Lösung gehören, die die Nutzung der Geräte an den Schnittstellen überwacht. Sie erlaubt es, die Wege der Daten von und zu externen Medien zu protokollieren, den Abfluss von Daten zu beschränken und auch unberechtigte Übertragungsversuche zu stoppen (Bild 3).

Stichwort

Malware-Entwicklung

Seit Januar 2001 ist die Signaturdatenbank von Norman um 4 Mio. Signaturen auf zirka 14 Millionen (Stand Juni 2011) gewachsen. Bis zu 50 000 neue Schadcodes kommen täglich in Umlauf. Die Angriffe nutzen nach wie vor Programmfehler in Anwendungen, neben Microsoft sind Adobe und Apple besonders betroffen.

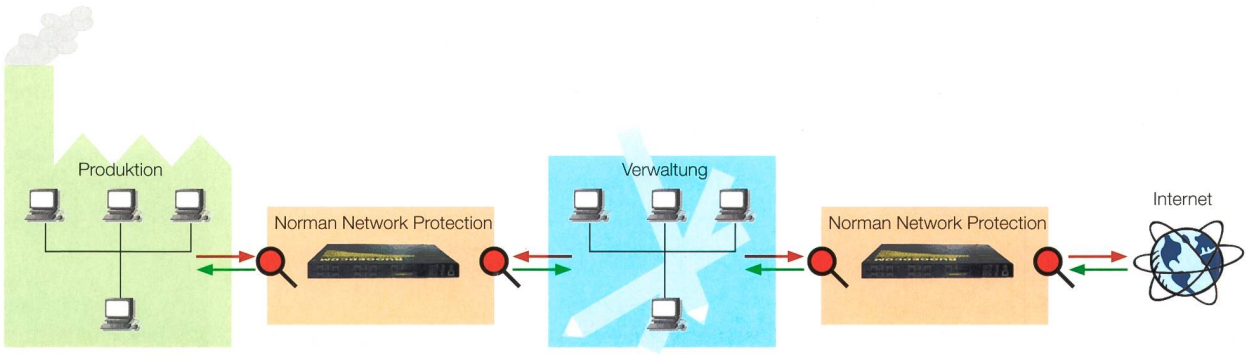
Die Entwicklung der letzten Zeit hat jedoch dazu geführt, dass die Software-Hersteller ihre Produkte sicherer machen, und dass die Nutzer ihren Virenschutz regelmässig aktualisieren und ihre Systeme patchen. Da sich den Cyberkriminellen dadurch Angriffsmöglichkeiten über technische Schwachstellen verschliessen, weichen diese vermehrt auf Social-Engineering-Techniken aus, die menschliche Eigenschaften und Verhaltensmuster ausnutzen. Das ist besonders erfolgversprechend auf Social-Media-Plattformen wie Facebook und Online-Spiele-Seiten.

Security-Strategie: von CIA zu ACI

Während in der «Büro-IT» die Sicherheitsfrage nach dem CIA-Prinzip (Confidentiality, Integrity, Availability; deutsch: Vertraulichkeit, Integrität, Verfügbarkeit) angegangen wird, müssen im industriellen Umfeld die Prioritäten anders, das heisst auf das ACI-Prinzip (Availability, Confidentity, Integrity) gelegt werden. Es gibt geeignete Best Practices für den Schutz von Produktionssystemen, die Penetrationstests und Sicherheitsbewertungen in der «allgemeinen IT» ähneln.

Bei der Anwendung dieser Verfahren, vor allem bei der Durchführung eines Penetrationstests auf einem realen System, kann es zu einem Systemabsturz kommen. Wichtig ist, dass Firmen entscheiden, was sie unternehmen möchten und das weitere Vorgehen festlegen.

Bei Unsicherheiten kann bereits ein Rundgang einen ersten Einblick in die Schwachstellen, und eine Bestimmung



Norman

Bild 3 Um sich vor Angriffen optimal zu schützen, sind Security-Komponenten auf mehreren Stufen sinnvoll. Inline-Detection-Lösung gleichen Schwachpunkte aus und erhöhen massiv den Schutz des Unternehmensnetzes.

der Zeit, die für die Behebung des Problems benötigt wird, ermöglichen.

Es ist nicht standardmässig festgelegt, wie die Verfahren genau durchzuführen sind. Es empfiehlt sich jedoch, einen systematischen Ansatz zu wählen und sich der Möglichkeit von Zugriffen auf höhere Ebenen zuzuwenden, wenn die Systeme offline sind. Die Alternative stellt eine Online-Bewertung oder sogar eine papierbasierte Checkliste für den Systemrundgang dar.

Résumé

La cible des virus, vers et autres chevaux de Troie

Cybercriminalité et sécurité IT dans l'industrie

Afin de pouvoir produire de manière efficace, de plus en plus d'entreprises ont automatisé leurs installations, exploité les avantages présentés par une interconnexion totale et utilisent davantage de solutions issues de l'environnement Office : de la technologie PC dans les machines à l'Ethernet industriel reliant le domaine Office et celui de la production en passant par le protocole internet TCP/IP. Cette contribution présente les dangers liés à la cybercriminalité favorisés par cette évolution et les solutions possibles pour les environnements industriels IT avec leurs potentiels et leurs limites. Elle montre ainsi en quoi les stratégies de sécurité de l'IT industrielle se différencient de celle de l'IT bureautique et de quelle manière les points faibles en matière de sécurité sont dépistés. No

IT-Risikoanalyse in Steuerungssystemen

Risiken innerhalb eines Steuerungssystems zu bewerten und diese durchzuführen, ist nicht schwieriger als bei anderen IT-Risikoanalysen. Sie zu beseitigen ist eine weit komplexere Aufgabe. Empfehlenswert ist, wenn Unternehmen zuerst ihre Anlagen, z.B. Scada, PLCs, drehzahlvariable Antriebe, CNC, Motion Control etc., bewerten und dann sämtliche vorhandenen Kommunikationsknotenpunkte wie Hubs und Switches sowie deren Basis (Echtzeit-Betriebssystem, altes System, aktuelles System, aktualisiert oder nicht aktualisiert etc.) prüfen. Anhand dieser Analyse kommen Sicherheitslücken im System ans Licht. Danach gilt es zu überprüfen, wie viele externe Verbindungen existieren und ob Prozesse eingerichtet sind, die eine Integration interner mobiler Geräte ins System verhindern. Weiter gilt es abzuklären, ob OEM-Geräte oder solche von Dritten über eine Dial-Out-Funktion verfügen. Anhand dieser Ergebnisse erhalten Unternehmen eine allgemeine Risikobewertung, um die gegebenen Sicherheitsrisiken weiter einschätzen zu können. Zur Bestimmung des realen Risikopotenzials müssen die Ergebnisse anschliessend in betriebswirtschaftlich greifbare Ergebnisse «übersetzt», werden. Dies umfasst:

- Welche Folgen hat ein Produktionsausfall?
- Welche Konsequenzen ergeben sich für Gesundheit und Sicherheit?
- Wie und wofür hafte ich?
- Kann dies zu einer Schädigung unseres Rufs im Markt führen?

Generell gilt: Eine genauere Analyse liefert präzisere Ergebnisse.

Fazit

Wer sensible Bereiche im Unternehmensnetz schützen will, hat zwei Möglichkeiten: Entweder man setzt auf konventionelle IT-Sicherheit, die aber künftig bei Weitem nicht mehr ausreichen wird. Oder man trennt und separiert sensible Netzwerke, damit sie nicht mehr miteinander verbunden sind. Der Angreifer muss dann für jedes System neue Entwicklungszeit auf sich nehmen. Es ist wichtig, dass Unternehmen verstehen, dass eine Sicherheitsrichtlinie und -architektur nicht alle potenziellen Sicherheitsangriffe und -verstösse vollständig unterbinden kann. Durch Implementierung eines Pakets aus unterschiedlichen Lösungen kann das Risiko jedoch beträchtlich minimiert werden.

Links

- **Stuxnet:** http://de.wikipedia.org/wiki/Stuxnet
- **On-Access-Scanner:** http://de.wikipedia.org/wiki/Dropper

Angaben zum Autor

Righard Zwienenberg ist Chief Research Officer beim norwegischen Antiviren-Hersteller Norman. Er ist Mitglied der CARO (Computer Antivirus Research Organization), Mitbegründer des AVED (Anti Virus Emergency Distribution Network) sowie Präsident der Anti-Malware Testing Standards Organization (AMTSO). Zu seinen Spezialgebieten gehören die Bedrohung durch Cyberterrorismus sowie der Schutz von Unternehmen und individuellen PC-Nutzern.

Norman Data Defense Systems AG, 4052 Basel
info@norman.ch