T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2013
Berlin, 04. - 05.11.2013

Sicherheit von Produktionsanlagen, Automatisierungssteuerungen, Medizingeräten und kritischen Infrastrukturen

Risiken und Handlungsempfehlungen

Sascha Dubbel
Palo Alto Networks (Deutschland) GmbH

Agenda

- Warum auch Produktionsanlagen geschützt werden müssen
- Prominente Beispiele
- Mögliche Folgen
- Ein Blick auf SCADA
- Einzelmaßnahmen aus der IT-Sicherheit
- Organisatorische Handlungsempfehlungen
- Kombinierte und Effiziente Lösungen von Palo Alto Networks

Warum auch Produktionsanlagen geschützt werden müssen

Moderne Prozesssteuersysteme, Fertigungsanlagen und Medizingeräte basieren heute oft auf PC-Technik und Embedded System-Technologie. Sie sind daher leider keine “unverwundbaren Blackboxes” sondern vernetzte Komponenten mit unterschiedlichen Charakteristiken und auf verschiedenen Standarts basierend. Durch den technischen Wandel bedingt, nutzen Systeme zur Steuerung IP-Netzwerk-Kommunikation, isolierte Systeme findet man nur noch selten.

Anlagenparks entsprechen Computernetzwerken, die Computer sind nur nicht auf den ersten Blick sichtbar.

Kommunkationsanbindung

- Moderne Prozesssteuersysteme, Fertigungsanlagen und Medizingeräte verfügen heute über Kommunikationsschnittstellen die genutzt werden um Wartung, Monitoring und Integration in andere Anlagenbestandteile zu ermöglichen.
  - Direkte Einwahl über PSTN/ISDN
  - Anbindung über UMTS
  - Anbindung über TCP/IP
- Anlagen werden in vielen Fällen nicht vollständig von weiteren Benutzer-/Office-Netzen getrennt und sind somit darüber angreifbar.
- Anlagen werden teilweise auch ohne Schutz direkt an das Internet angebunden!

Welche Anlagen können betroffen sein?

- Produktionsanlagen
- Kraftwerkssteuerungen
- Photovoltaikanlagen
- Medizingeräte / Bildgebende Diagnose
- Klimatisierungssysteme
- Netzersatzanlagen (Notstrom)
- Kommunikationsanlagen
- Überwachungstechnik und Gefahrenmeldeanlangen
- Gebäudesteueranlagen (Licht/Luft)
- Zutrittskontrollsysteme
- Mautstationen
- Pumpwerke
- ….

Prominente Beispiel von Angriffen auf Anlagentechnik

heise online > News > 2011 > KW 2 > Stuxnet Gemeinschaftsprojekt der USA und Israels?

16.01.2011 14:27 « Vorige | Nächste »

Stuxnet Gemeinschaftsprojekt der USA und Israels?

vorlesen / MP3-Download

Dass in Stuxnet jede Menge Gehirnschmalz steckt, war schon länger klar. Ebenso, dass hier ein Expertenteam nicht einfach nur Windows-Exploits an Siemens-Fabrikationssteuerungen vorführt, sondern gezielt Zerstörungen an Zentrifugen zur Uran-Anreicherung beabsichtigt hat.

Der Bericht der New York Times hat nun viele Indizien zusammengetragen, die den Schluss nahelegen, dass Experten der USA und Israels Stuxnet innerhalb von zwei Jahren gemeinschaftlich entwickelt haben. Vermutlich hat Siemens dabei sogar unfreiwillig Schützenhilfe geleistet: Das Unternehmen hatte mit einer Forschungseinrichtung des US-Energieministeriums an einem Programm zum Schutz vor Cyberattacken zusammengearbeitet. Die aufgedeckten Sicherheitslücken (PDF) wurden dann bei der Entwicklung des Wurms berücksichtigt.

Prominente Beispiel von Angriffen auf Anlagentechnik

heise online > News > 2011 > KW 2 > Stuxnet Gemeinschaftsprojekt der USA und Israels?

16.01.2011 14:27 « Vorige | Nächste »

heise online > News > 2011 > KW 24 > Kritische Lücke in Industriesteuerungs-Software

19.06.2011 13:15 « Vorige | Nächste »

Kritische Lücke in Industriesteuerungs-Software

vorlesen / MP3-Download

Das ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), eine Behörde im US-Ministerium für Homeland Security, warnt (PDF) vor Sicherheitslücken in einer weltweit verbreiteten Steuersoftware für Industrieanlagen. Betroffen sind die Produkte ForceControl 6.1 und pNetPower 6 des chinesischen Herstellers Sunway, die weltweit in unterschiedlichen Branchen im Einsatz sind.

Beide Produkte besitzen Server-Komponenten zur Fernsteuerung, in denen spezielle HTTP- beziehungsweise UDP-Pakete einen Buffer-Overflow auslösen können. Angreifer könnten die damit gesteuerten Anlagen lahmlegen und dort vermutlich auch beliebigen Code einschleusen. Ein Exploit ist nach bisherigen Erkenntnissen noch nicht in Umlauf. Der Hersteller bietet seit einem Monat Patches für ForceControl und pNet Power an.

Prominente Beispiel von Angriffen auf Anlagentechnik

heise online > News > 2011 > KW 47 > Hacker zerstört Pumpe in US-Wasserwerk

heise online > News > 201 21.11.2011 10:23 « Vorige | Nächste »

16.01.2011 14:27

Stux

heise online > News >

19.06.2011 13:15

Kritische Lücke

vorlesen / MP3-Download

Das ICS-CERT (Indus
eine Behörde im US-M
Sicherheitslücken in ei
Betroffen sind die Proc
Herstellers Sunway, di

Beide Produkte besitz
spezielle HTTP- bezie
können. Angreifer kön
vermutlich auch belieb
Erkenntnissen noch ni
für ForceControl und

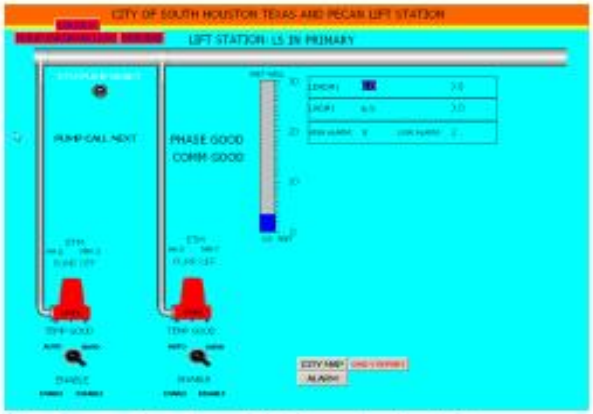
Dass
dass
Fabri
Uran-

Der B
Schlu
Jahre
unfrei
Forsc
Schut
Siche
berüc

Hacker zerstört Pumpe in US-Wasserwerk

vorlesen / MP3-Download

Offenbar ist es einem Hacker gelungen, über das Internet in die Prozessleittechnik eines Wasserwerks im US-Staat Illinois einzudringen. Laut US-Medienberichten gelang es ihm, eine Pumpe mehrfach ab- und anzuschalten und dadurch zu zerstören. Das wäre das erste Mal, dass Teile der kritischen Infrastruktur eines Landes über das Internet angegriffen und erfolgreich lahmgelegt worden sind.



Als Beweis seines Einbruchs hat der Hacker insgesamt fünf Screenshots des SCADA-Systems veröffentlicht.

Zwar nahmen das FBI und DHS im Anschluss an den Vorfall die Ermittlungen auf, spielten aber zunächst das Risiko herunter. Davon fühlte sich der mutmaßliche Hacker "prof" provoziert und drang kurz darauf in ein weiteres Wasserwerk ein, diesmal in Houston, Texas. Als Beweis veröffentlichte er Screenshots des Systems zur Visualisierung und Steuerung der Leittechnik (SCADA). In einem auf Pastebin veröffentlichtem Manifest gibt der Hacker an, auf die Sicherheitsprobleme bei SCADA aufmerksam machen zu wollen und wie leicht die Systeme zugänglich seien. Der Sicherheitszustand der nationalen Infrastruktur sei schlecht.

paloalto NETWORKS

Prominente Beispiel von Angriffen auf Anlagentechnik

heise online > News > 2011 > KW 47 > Hacker zerstört Pumpe in US-Wasserwerk

heise online > News > 201 21.11.2011 10:23 « Vorige | Nächste »

16.01.2011 14:27

Hacker zerstört Pumpe in US-Wasserwerk

heise online > News > vorlesen / MP3-Download

Stux

19.06.2011 13:15

Offenbar ist es einem Hacker gelungen, über das Internet in die Prozessleittechnik

vo

heise online > News > 2012 > KW 44 > ICS-CERT warnt vor Angriffen auf industrielle Steueru

Dass

Kritische I

30.10.2012 15:57 « Vorige | Nächste »

dass

vorlesen / MP3

Fabri

Das ICS-CERT

Uran-

eine Behörde i

Sicherheitslück

ICS-CERT warnt vor Angriffen auf industrielle Steuerungssysteme

Der B

Betroffen sind

vorlesen / MP3-Download

Schlu

Herstellers Sur

Jahre

Beide Produkte

Die Attacken auf industrielle Steuerungssysteme nehmen zu. Das Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) hat dazu eine Warnung herausgegeben, die vom Bundesamt für Sicherheit und Informationstechnik (BSI) unterstützt wird. Spezielle Tools und Suchmaschinen erleichtern auch unerfahrenen Angreifern die Attacken auf Maschinen und Geräte, die Relevanz für die Infrastruktur, wie etwa die Stromnetze, haben.

unfrei

spezielle HTTP

Forsc

können. Angre

Schut

vermutlich auch

Siche

Erkenntnissen

berüc

für ForceContr

SCADA-Systems veröffentlicht.

der Hacker an, auf die Sicherheitsprobleme bei SCADA aufmerksam machen zu wollen und wie leicht die Systeme zugänglich seien. Der Sicherheitszustand der nationalen Infrastruktur sei schlecht.

paloalto NETWORKS

Wussten Sie…

- …dass eine der größten Explosionen in der Geschichte der Menschheit durch eine SCADA-Attacke verursacht wurde? Und zwar schon 1982!
- http://en.wikipedia.org/wiki/Siberian_pipeline_sabotage

paloalto NETWORKS

Bedrohungen im Großen: Moderner Terrorismus

Frankfurter Allgemeine

Politik

AKTUELL MULTIMEDIA THEMEN BLOGS ARCHIV MEIN FAZ.NET 50

Politik Wirtschaft Feuilleton Sport Gesellschaft Finanzen Technik & Motor Wis

Aktuell > Politik > Inland

Islamistischer Terrorismus

„Wir haben längst den Online-Dschihad“

11.02.2012 · Der „Dschihadismus 2.0“ ist längst Realität, sagt Verfassungsschützer Alexander Eisvogel. Im Interview spricht er über die Radikalisierung von Islamisten im Internet und die Gefahr eines Cyber-Angriffs.

paloalto NETWORKS

Bedrohungen im Kleinen: aus unserem Alltag

- Prozesssteuerungssystem dient als interne Tauschplatform der Azubies für Filme, Videos (…und ein Bischen Malware…)

- Chinesischer Peer-to-Peer Client auf Betriebsdaten-Erfassungs-Server entdeckt (…kleines Andenken an den netten chinesischen Praktikanten…)

- Wachschutz-Mitarbeiter installiert Spiele auf CNC Steuerkonsole… (…man muss sich ja irgendwie wachhalten…)

Ungeschützte Anlagen finden? Ganz einfach!

paloalto NETWORKS

Mögliche Folgen:

- Ausfall der Produktion
- Verhinderung der Einsatzfähigkeit der Mitarbeiter
- Fehler in den Produkten
- Verfälschung von Messergebnisse
- Zerstörung der Anlage oder von Anlagenkomponenten
- Umwelt-Unfälle wie Verunreinigung/Kontamination von Boden/Luft/Wasser
- Personenschaden (auch bei Medizingeräten!)
- Thermonukleare Kettenreaktionen

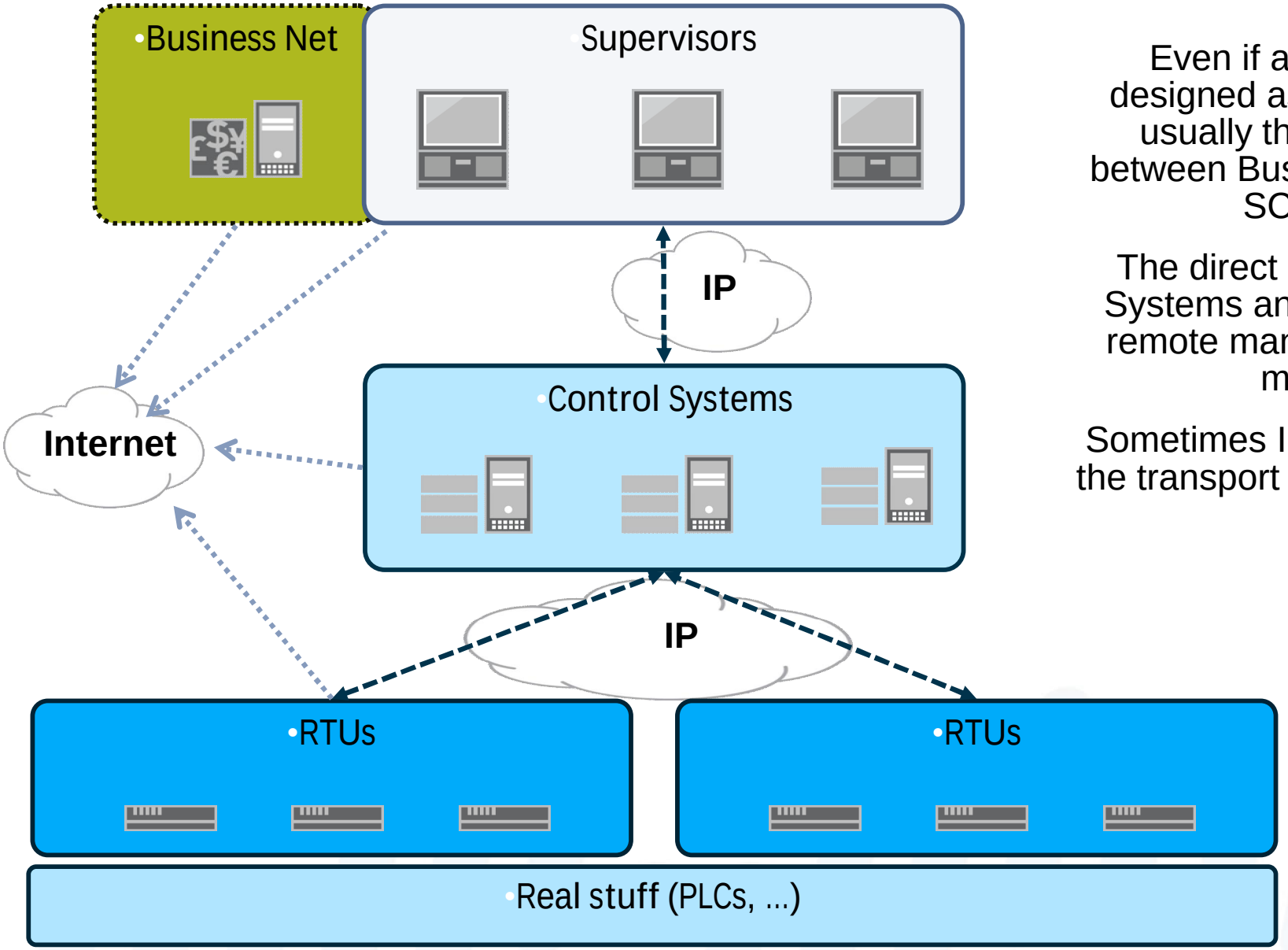
Über SCADA

- Laut Wikipedia:

  Unter **Supervisory Control and Data Acquisition** (**SCADA**) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems

  Die Kommunikation innerhalb von SCADA-Systemen erfolgt heute mehr und mehr auf der Basis von TCP-basierten Internettechniken. In der Feldebene spielen aber auch noch serielle Verbindungen in Form von Punkt-zu-Punkt-Kommunikationen und Feldbussystemen eine gewichtige Rolle, die wahrscheinlich auf absehbare Zeit erhalten bleiben wird.
  Die Standardisierung bei der Kommunikation ist noch nicht abgeschlossen. Versuche wie OPC beschränken sich häufig noch auf bestimmte Betriebssysteme, obwohl auch hier inzwischen ein Schritt in Richtung Betriebssystemunabhängigkeit (OPC XML-DA, OPC UA) gegangen wird. Häufig sind im Bereich SCADA noch herstellerspezifische oder geschlossene Lösungen anzutreffen. Aber offene Protokolle wie beispielsweise Modbus erfreuen sich wachsender Popularität. Über Gateways in Form eingebetteter Systeme lassen sich unterschiedliche Übertragungsprotokolle aneinander anpassen. Die Arbeitsplätze, an denen visualisiert wird, werden heute vermehrt über Ethernet oder drahtlose Netze, d.h. immer mehr auf Basis von TCP angebunden.

A typical SCADA Network



Even if a SCADA network is designed as an isolated network, usually there are many doors between Business Network and the SCADA network

The direct connection of Control Systems and RTUs to Internet for remote management is more and more frequent

Sometimes Internet is even used as the transport network between layers


www.guenter-pilger.de


Linie 1
Linie 2
ABB

SCADA-typische Probleme

- Keine durchgängige Standardisierung
- SCADA wurde ursprünglich für fest verdrahtete Kommunikationsverbindungen entwickelt, die Kommunikation erfolgt häufig nicht verschlüsselt und/oder signiert.
- Fehlende Authentifizierungsmechanismen
- Anlagen werden lange betrieben (20 Jahre und länger) ohne dass es zu Modernisierungen in der Steuerung kommt.
- Anlagenentwickler und Betreiber haben kein Fachwisse über IT-Sicherheit
- Systeme dürfen nicht gepatcht werden oder Upgrades werden aufgrund der Komplexität hinausgeschoben
- Anlagen werden nicht von anderen Netzwerkbereichen abgetrennt oder Netze wachsen „schleichend“ zusammen.

Organisatorische Maßnahmen

- Awarenes schaffen, auf Folgen hinweisen!
- Personal-Zu- und Abgänge insbesondere von Dienstleistern und Subunternehmern prüfen, Richtlinien zum Verhalten in Produktionsumgebungen festlegen und durchsetzen.
- Notfallmanagement Etablieren,
  - CISO muss jedem Produktionsleiter bekannt sein,
  - Probleme müssen einfach und Effizient gemeldet werden können
  - Notfallprozesse definieren und Dokumentieren
- Große Anlagen-Hersteller (z.B. Siemens) betreiben eigene Emergency-Response Team Center (sog. CERT): Zugang sicherstellen, Kooperation ermöglichen.
  - Alle Anlagen-Hersteller auffordern aktive Dienstleistungen zur Sicherheit anzubieten und Konzepte Auzuzeigen

Lösungsansätze der IT-Security: Systembezogen

- Systembasierte Maßnahmen leider oft nicht gangbar:
  - Patches sind nicht mehr verfügbar ☒
  - Lokale Virenscanner beeinträchtigen die Systemstabilität ☒
  - Host-Firewalls/Host IPS könnten ebenfalls nicht berücksichtigte und unerwünschte Nebenwirkungen mit sich bringen ☒
  - Application-Whitelisting könnte eine Option sein (wird im Banken-Umfeld z.B. auf Geldautomaten erfolgreich genutzt); aber tiefer Eingriff ins System ☒
  - Software-Lösungen sind für alte Betriebssysteme nicht mehr lieferbar ☒
  - Intrusive Vulnerability Scans werden gescheut, da Systeme abstürzen können ☒
  - Systeme sollten möglichst gehärtet ausgeliefert werden, unnötige Dienste müssen unbeding deaktiviert sein um den Angriffsvektor zu minimieren ☒
- Andere Maßnahmen
  - Versiegelung/Verschluss von physikalischen Schnittstellen ☑
  - Physikalische Zugangskontrollen ☑

Lösungsansätze der IT-Security: Netzwerkbasiert

- Netzbasierte Ansätze
  - Netzwerk-Firewalls müssen Verwaltungsnetzte zwingend von Produktionsanlagen isolieren. ☑
  - Produktionsanlagen dürfen nicht direkt vom öffentlichen Internet aus zugänglich sein ☑
  - Netzwerkbasierter Virenschutz auf SMB/CIFS sinnvoll ☑
  - Weitere Segmentierung zwischen IP-basierten Anlagenkomponenten kann bei kritischen Infrastrukturen sinnvoll sein. ☑
  - Wartungszugänge müssen ggf. über Authentifizierungsmechanismen geschützt ☑
  - Zugriffe auf Anlagen sollten auf die jeweils notwendige Applikationen beschränkt werden. ☑
  - Netzwerk Intrusion Prevention Systeme sollten verwendet werden um bekannte Angriffe zu unterbinden ☑

Die Lösung: Netzwerk-basierter Schutz

Effektive Netzwerk-basierte Schutzmechanismen

- Segmentierung der angeschlossenen Netze ohne Einbußen im Hinblick auf Datendurchsatz und Paketlatenz
- Eine granulare Überwachung und Kontrolle der Applikationen und Protokolle ist unabhängig von den genutzten Ports, z.B. Siemens Factory-Link, OPC, BACnet, iec-60870-5-104 , Video-TS (MPEG Streams), etc.
- Wartungszugänge über HTTP können über eine eigene Portalseite Authentifiziert werden (LDAP, Windows Domain, Radius etc).
- Die Firewall kann vorhandene Router ersetzen (L3 Modus), als Switch transparent fungieren (L2) oder einfach als Transparente Brücke in eine bestehende Verbindung eingeschliffen werden.
- Passive Überwachung im TAP/Mirror Modus: Traffic analysieren und alarmieren
- Eine Hardware-beschleunigte Stream-basierte AV-Engine prüft auf bekannte Virensignaturen (Latenzfrei!), auch CIFS/SMB Verbindungen

Integriertes Netzwerk-IPS

- Überwachung und den Schutz der Anlagen gegen bekannte Verwundbarkeiten, Exploits …

34675	Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	High	
34674	Siemens Tecnomatix FactoryLink SCADA VRN Server Directory Traversal Vulnerability	High	
34672	Interactive Graphical SCADA System Remote Buffer Overflow Vulnerability	High	CVE-2011-1567
34671	Interactive Graphical SCADA System Directory Traversal Vulnerability	Low	CVE-2011-1565
34669	Interactive Graphical SCADA System Directory Traversal Vulnerability	Low	CVE-2011-1566
34668	Interactive Graphical SCADA System Remote Buffer Overflow Vulnerability	High	CVE-2011-1567
34667	Interactive Graphical SCADA System Format String Vulnerability	High	CVE-2011-1568
34662	Interactive Graphical SCADA System Remote Buffer Overflow Vulnerability	High	CVE-2011-1567

- …und überwachung typischer Aktionen

31668	SCADA Modbus Write Request to a PLC Attempt	Low	
31667	SCADA Modbus Read Request to a PLC Attempt	Low	
31666	SCADA DNP3 Write Request to a PLC Atetmpt	Low	
31665	SCADA DNP3 Miscellaneous Request to a PLC Atetmpt	Low	
31664	SCADA DNP3 Disable Unsolicited Response Attempt	Low	
31663	SCADA DNP3 Warm Restart Attempt	Low	

paloalto NETWORKS

Kontrolle über Botnetze

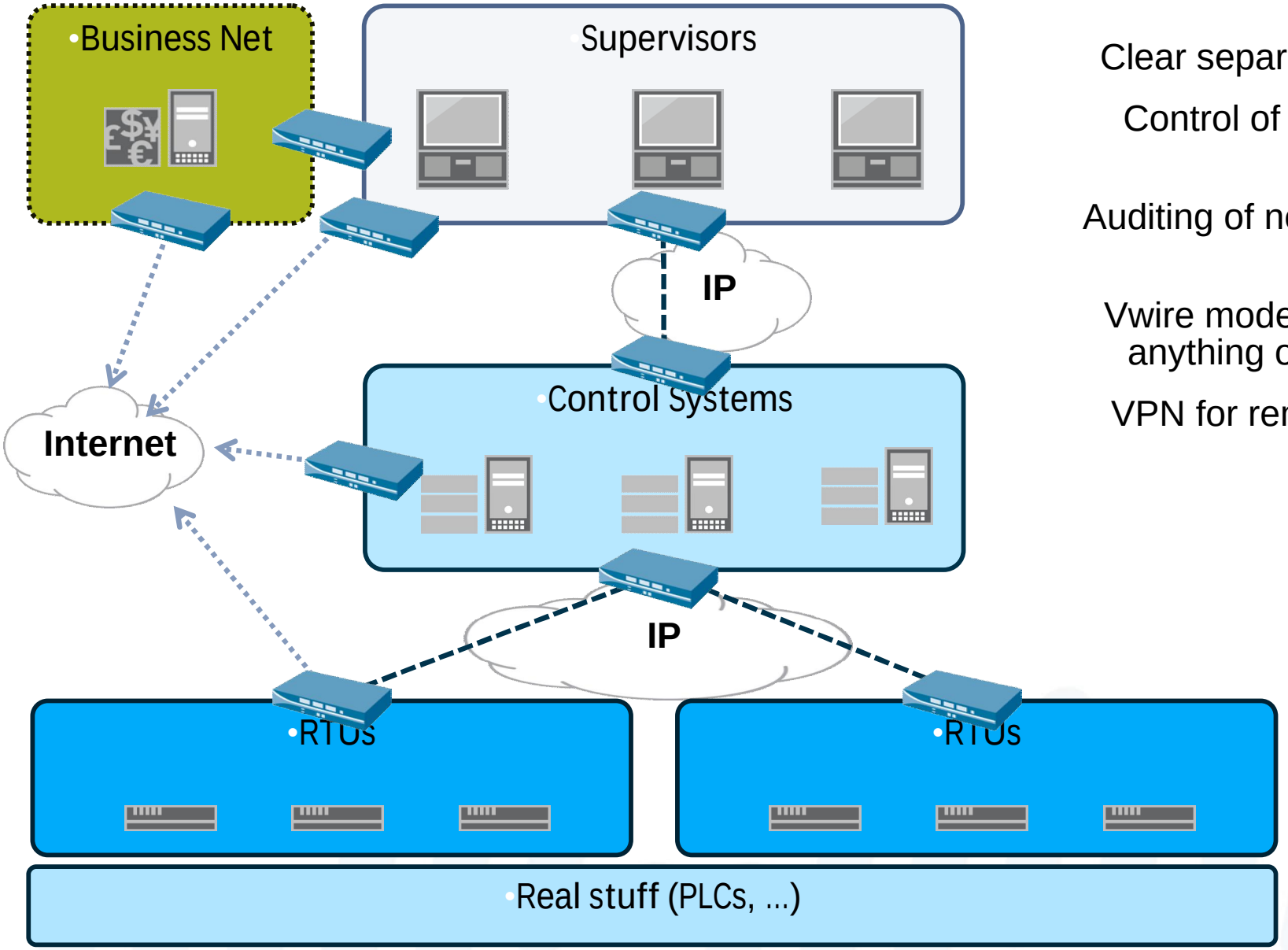
- Sichtbarkeit und Kontrolle über Botnetze:

  Anhand von Signaturen und generischen Engines erhöhen den Schutz vor Botnetz-Aktivitäten. So kann nicht nur der Command & Control Verkehr hunderter Botnetz-Varianten wie z.B. Stuxnet erkannt und blockiert werden sondern auch anhand des Netzwerkverhaltens sogar bisher unbekannte Botnetze identifiziert werden.

	Confidence	Source Address	Source User	Description
1	2	10.157.0.13	impressive\corent...	Repeatedly visited (14) the same URL "208.75.76.32/"
2	2	10.157.0.50	impressive\fleur.s...	Repeatedly visited (50) the same URL "165.235.45.6/"
3	2	10.157.1.11	impressive\justin...	Repeatedly visited (528) the same URL "208.81.185.220/"
4	2	10.157.1.111	impressive\tom.pi...	Repeatedly visited (48) the same URL "24.32.110.104/"
5	2	10.157.1.125	impressive\lore.gi...	Repeatedly visited (48) the same URL "221.11.172.31/crossdomain.xml"
6	2	10.157.1.27	impressive\julie.c...	Repeatedly visited (48) the same URL "216.38.57.37/openads/www/delivery/ajs.php?zon 1&loc=http:/www.lyricsmania.com/lyrics/hollywood_undead_lyrics_7318/swan_songs_lyr sourceid=navclient&hl=de&ie=UTF-8&rlz=1T4TSEA_deCN329CN330&q=Hollywood+Und
7	2	10.157.1.42	impressive\cleme...	Repeatedly visited (48) the same URL "8.3.241.71/idle/K57mYD8rcF6OyU5T/20"
8	2	10.157.10.1	impressive\alicia....	Repeatedly visited (48) the same URL "64.215.167.80/"
9	2	10.157.10.215	impressive\elodie...	Repeatedly visited (338) the same URL "130.150.237.19/"
10	2	10.157.11.124	impressive\lisa.fr...	Repeatedly visited (47) the same URL "207.46.113.89/"
11	2	10.157.12.133	impressive\sophie...	Repeatedly visited (48) the same URL "211.234.243.144/cacheupdate/cacheupdate.asp"

paloalto NETWORKS

Firewall for segmentation



Clear separation between layers

Control of access from and to Internet

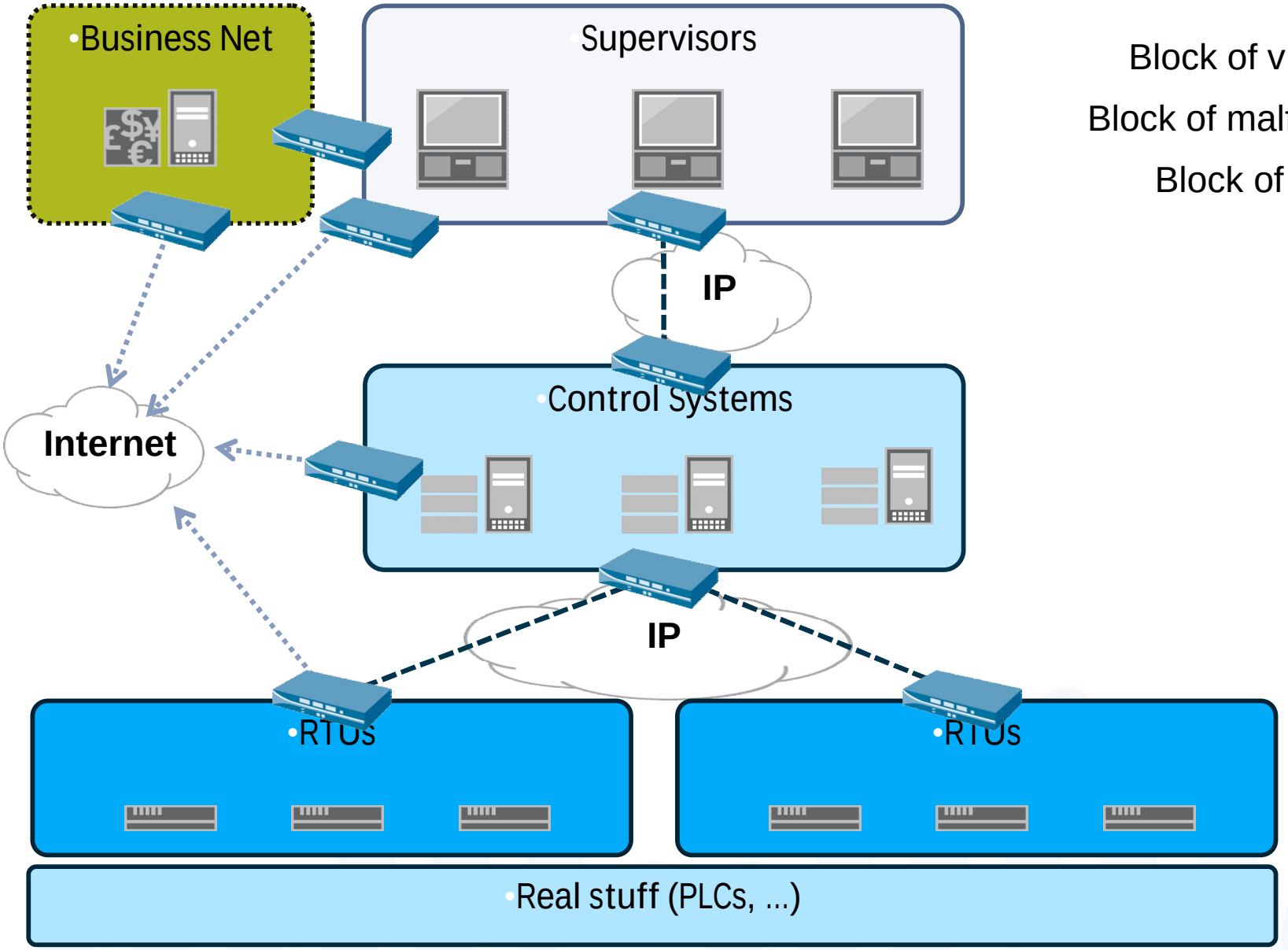
Auditing of network traffic between zones

Vwire mode, no need to change anything on SCADA systems

VPN for remote access to sites

paloalto NETWORKS

Threat Prevention for protection



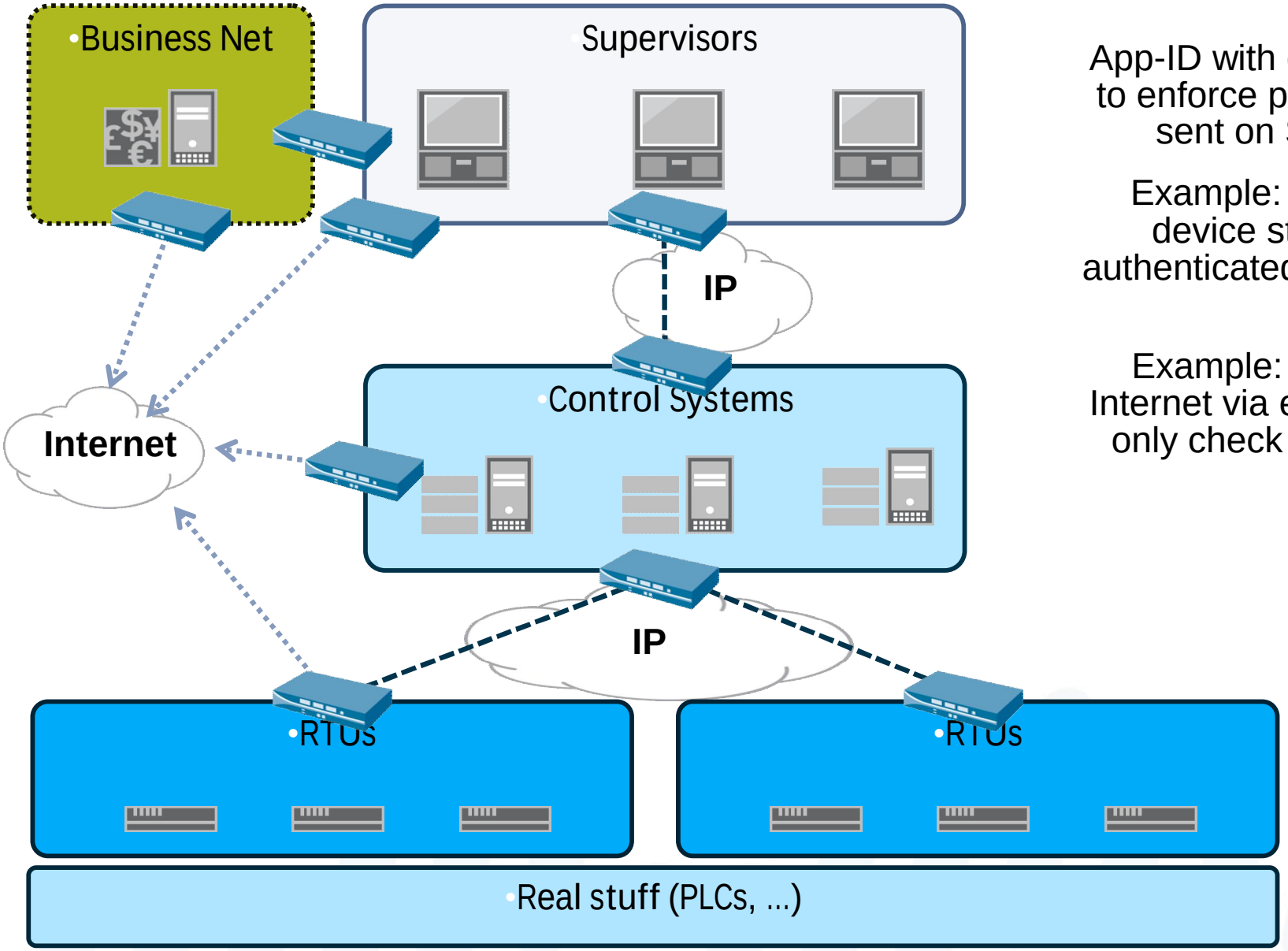
Block of vulnerability exploits

Block of malformed SCADA traffic

Block of SCADA malware

paloalto NETWORKS

App-ID for L7 enforcement



App-ID with command recognition to enforce policies on commands sent on SCADA protocols

Example: everyone can read device status only specific authenticated users can set device status

Example: users coming from Internet via encrypted tunnels can only check device status (read-only)

paloalto NETWORKS

Vielen Dank!

paloalto NETWORKS
the network security company™

Sascha Dubbel
sdubbel@paloaltonetworks.com