



Panel I

Securitatea sistemelor cyber-fizice, provocarea anilor viitori
pentru domeniul securității private
*Cyber-physical systems security, the challenge of the coming
years for the private security sector*

**Conferința națională a A.R.T.S.
PERSPECTIVE ÎN SECURITATEA
PRIVATĂ - VALOAREA SOCIALĂ A
SERVICIILOR DE SECURITATE**

București, 8 Iunie 2017

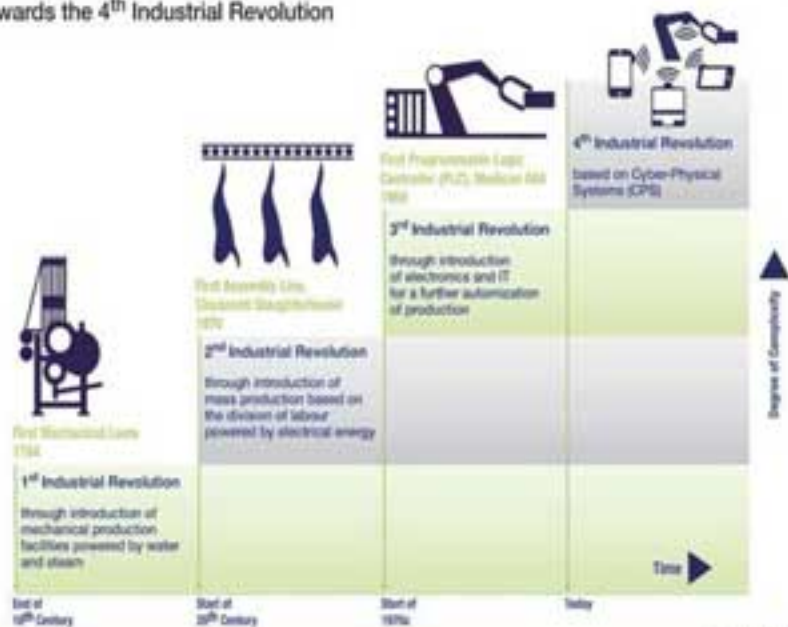
Crowne Plaza Hotel, Crowne Ballroom



Sisteme cyber-fizice

- Iminente schimbărilor aduse de omniprezența digitală și patrunderea tehnologiilor 'disruptive'
- a 4a revoluție industrială
- trecerea la procese inteligente 'smart'
- contribuția personală prin BYOD

Towards the 4th Industrial Revolution



Source: [24], [25]



Sisteme cyber-fizice

- Sisteme complexe capabile să controleze și să coordoneze procesele fizice și organizaționale la nivel local și global prin utilizarea tehnologiei informației și comunicațiilor

- transport inteligent
- energie inteligentă
- sănătate inteligentă
- producție inteligentă,
- orașe inteligente

Securitatea sistemelor cyber-fizice

- diversificare gama vulnerabilitati si amenintari
- atacuri si incidente complexe
- modificari de paradigma in modul de protectie
- cooperarea public-privat
- tehnologii avansate de culegere si procesare a datelor
- *evolutia solutiilor si serviciilor de securitate*
- *aplicarea modelelor de securitate reglementate*
- *capabilitatile si garantiile unui prestator de servicii de securitate*
- *raspunsul la atacuri si incidente de securitate*

Masa rotunda - subiecte

- analiza de risc si managementul riscului in SCF
- amenintari si atacuri in SCF
- atacuri combinate cyber-fizic
- gradul mare de inovare in atacurile impotriva SCF
- managementul incidentelor in SCF
- securitatea fizica a sistemelor cyber vs securitatea cibernetica a sistemelor de securitate fizica
- utilizarea tehnologiilor avansate de procesare a datelor in securitate – servicii inovative
- caracterizarea prestatorilor de servicii pt securitatea SCF
- cooperarea public privat in domeniul securitatii SCF

Invitati

- Cristian IORDAN – C.N. Cyberint
- Mihai GRADINARU – UTI, ROMSECA
- Adrian VILCIU – ARPIC
- Toma CAMPEANU - ANSSI
- Dan GAVOJDEA – CISCO
- Gabriel BADEA – FSS
- Lee St. John - ERNITEC
- Mihai BRANA - HONEYWELL



TOMA CAMPEANU



Asociația pentru Securitatea Sistemelor Informatice a fost înființată în 2012, ca un liant între sectorul public și mediul de afaceri

ANSSI este o organizație neguvernamentală, nonprofit, profesională și independentă.

Asociația reunește peste 50 de membri, companii având în total aproximativ 25000 de angajați



TOMA CAMPEANU



Mix fizic-cibernetice

Cele mai mari daune: MyDoom - 38.5 miliarde USD

Un vierme polimorf care se raspandea prin email si permitea atacatorului sa preia controlul calculatorului

Social media – 1.7 miliarde conturi active (aprox 2/3 total utilizatori)

600.000 conturi Facebook compromise zilnic

Like jacking /-Link jacking / Phishing

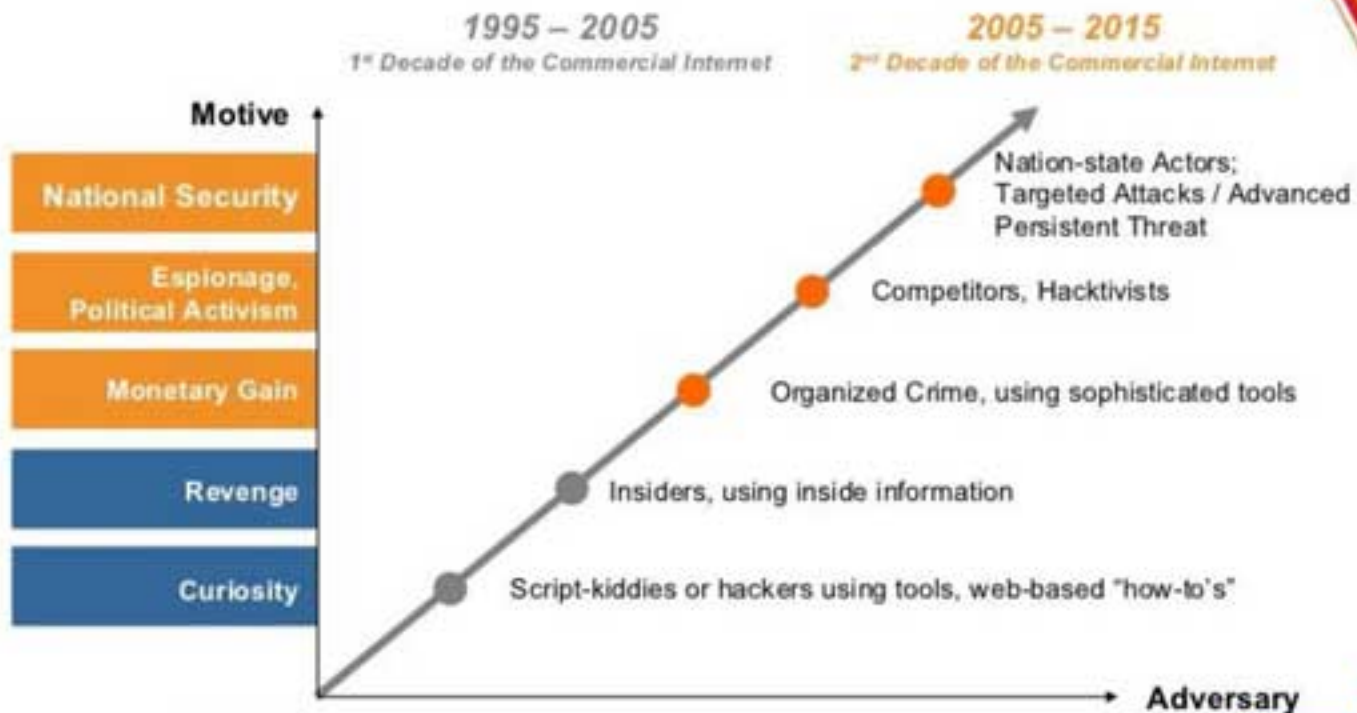
99% calculatoare au vulnerabilitati; 60% dintre angajati iau cu ei datele la plecare

1 singur grup transnational: -1 miliard USD in 2 ani / 100 de banci / 30 de tari / spear phishing

68% din sumele pierdute nu pot fi recuperate



TOMA CAMPEANU





TOMA CAMPEANU



EUGDPR.org

The Regulation

The Process

More Resources

Our Partners

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

**TIME UNTIL GDPR ENFORCEMENT
UTC**

352:14:40:51

Days Hrs Mins Secs



- Infrastructura critica – sisteme complexe , eterogene, cu grad inalt de informatizare, de regula cu intindere geografica intinsa si cu impact asupra societatii si activitatii autoritatilor statului
- Protectia infrastructurii critice –un act de responsabilitate fata de societate si alti operatori

“The world will not be destroyed
by those who do evil, but by
those who watch them without
doing anything”
Albert Einstein



Deficiente

■ Securitate fizica

- nu sunt definite cerinte specifice
- nu este privita ca o activitate cu valoare adaugata
- menita sa raspunda unor cerinte legale

■ Securitate cibernetica

- nu este privita ca o necesitate
- legislatie deficitara
- lipsa competentelor la nivelul operatorilor



Provocari

- Cresterea amenintarilor de natura fizica si cibernetica
- Cresterea gradului de interdependenta
- Cresterea nivelului de integrare



Pasi de urmat

- Integrarea managementului securitatii fizice si cibernetice
- Redefinirea rolului managerului de securitate
- Standardizarea unor cerinte prin dezvoltarea unor proiecte de cercetare
- O mai buna comunicare intre actorii implicati – model EUCONCIP



- **Securitatea fizica este o parte intrinseca a protectiei retelelor informatice.**
 - ▷ APTs bazate inclusiv pe penetrare fizica in zona infrastructurilor hardware, racolarea insider-i, activitati de supraveghere informativa si culegere de informatii derulate in timp;
 - ▷ *Deci, cel putin in astfel de cazuri nu se poate vorbi de o securitate informatica reala, efectiva daca nu exista un nivel cel putin suficient al securitatii fizice si fara asigurarea unei protectii contrainformative eficiente in sensul clasic al cuvantului.*



▣ Internetul obiectelor

- Industria de Securitate se bazeaza din ce in ce mai mult pe solutii bazate pe comunicare IP;
- Consecintele unui atac cibernetic asupra unor sisteme de securitate izolate dar mai ales asupra unor retele de sisteme de securitate sau a unor centre de monitorizare si management alarme, pot atinge o magnitudine si o probabilitate peste norma.



GABRIEL BADEA – F.S.S

Terorism si Cyberterorism:

- ▷ Wannacry un atac cibernetic de proportii care insa a avut un efect devastator asupra retelei nationale de sanatate publica din Marea Britanie. 70 de Spitale din Anglia si Scotia au avut activitatea grav perturbata. Functiunea/Serviciul de primire urgente serios perturbat si el.
- ▷ In acelasi timp Marea Britanie se confrunta cu un val de atacuri teroriste.
- ▷ In contextul presiunii in crestere asupra ISIS este cazul sa se ia in calcul si scenarii de atacuri combinate...Ce s-ar fi intamplat daca in paralel cu incapacitarea NHS ar fi fost atacate cibernetic si alte structuri de raspuns in situatii de urgenta sau alte infrastructuri critice, si ce s-ar fi intamplat daca in acelasi timp ar fi avut loc si un atac de mari proportii precum atentatele teroriste de la Londra in 2005;



GABRIEL BADEA – F.S.S

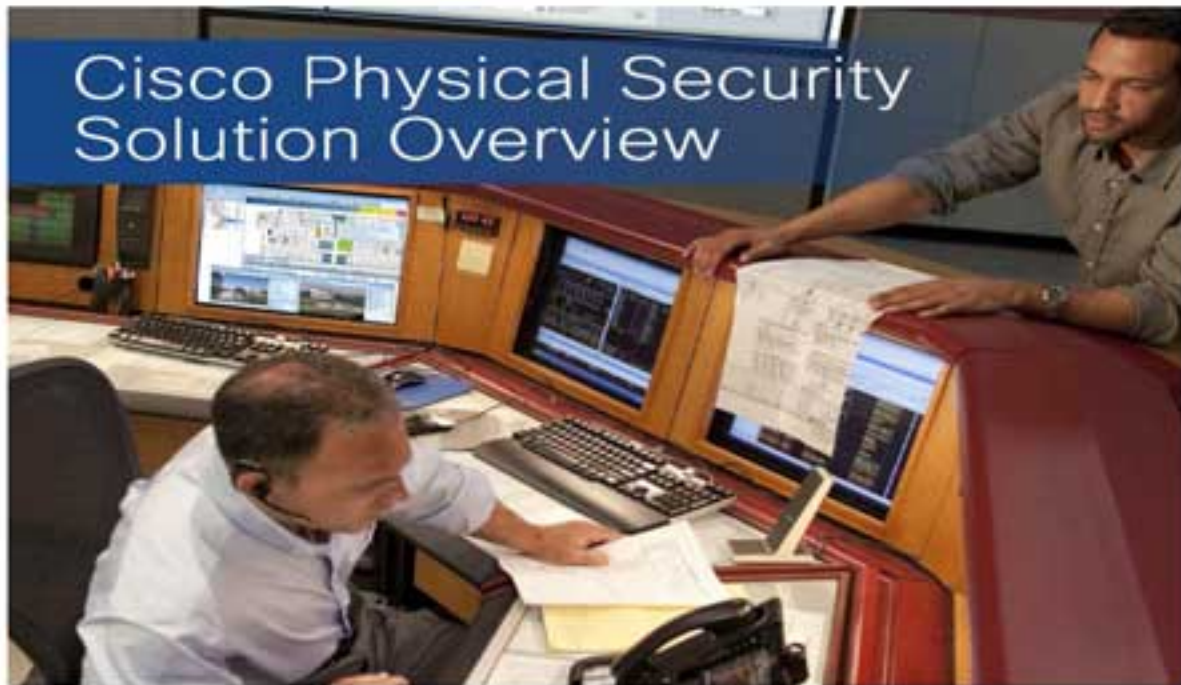
- ▷ ISIS are o divizie de Cyberwar;
- ▷ De asemenea se pune intrebarea daca nu cumva sumele platite in bani virtuali (bitcoin) care sunt dificil de urmarit nu sunt folosite pentru finantarea activitatiilor teroriste;

Avand in vedere criticalitatea sigurantei retelelor informatice, statul (institutiile competente) ar trebui sa joace un rol mult mai activ in cybersecurity inclusiv in mediul privat sau sa creeze avantaje fiscale celor care investesc in cyber security;

Cybersecurity ca o activitate comerciala nu numai ca nu este eficace dar starneste si controverse; Statele si companiile ar trebui sa-si puna resursele in comun pentru a crea si implementa strategii efective de aparare in infrastructurilor informatice care sa fie accesibile tuturor;



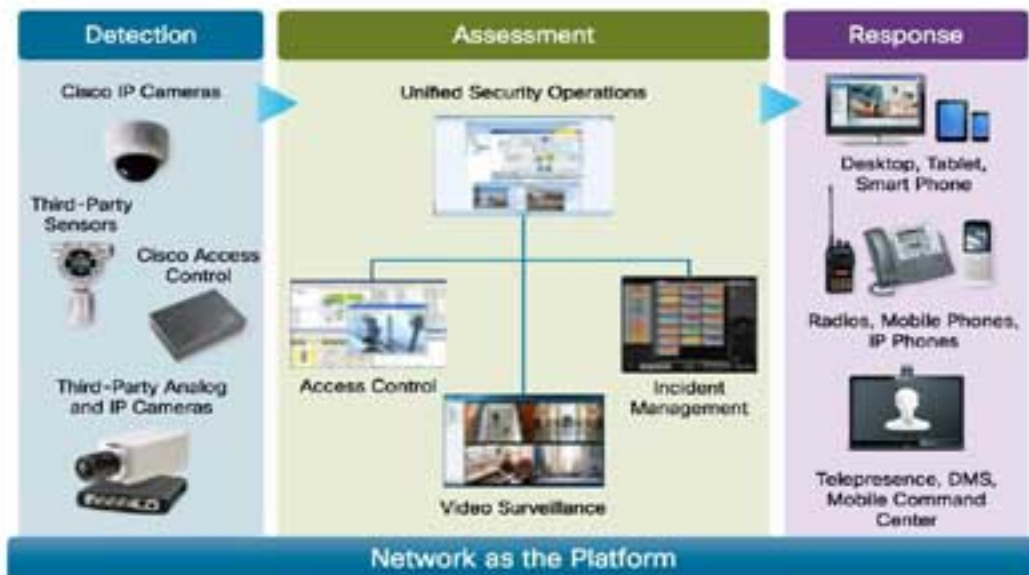
Cisco Physical Security Solution Overview



Solutie

The Solution

Unlike non-integrated point products, Cisco solutions provide end-to-end support to quickly detect incidents, correlate and prioritize key information, enabling faster and more effective collaboration among incident response personnel. Using the network as an open, scalable platform for integrating security helps to increase operational flexibility, improve protection capabilities, and reduce both risk and cost of ownership.





Going Digital = Smart Security? The "HOW" vs the "WHY"

UTi



=HOW?

- =Along with technological progress
- =Carefully consider risks!

=WHY?

- =Because of technological progress?
- =Carefully consider real needs!





Even in 2017 Technology Should Come Last Smart Security is Still First About People



Not even the 5th Industrial Revolution should change the priorities in Security:

1. People
2. Proceses
3. Technology

Cyber and Physical Security for Cyber-Physical Systems, Internet of Things, Smart Systems of Systems

... but Security by People. What people?

Smart People



Planning for Smart Security

The "WHY" vs the "HOW"; IT vs Security

UTi



=WHY?

- =Rapidly evolving risk spectrum
- =Smarter criminals; open and connected society
- =IT Technology introduces vulnerabilities & risks
- ... but also IT makes it possible & easier

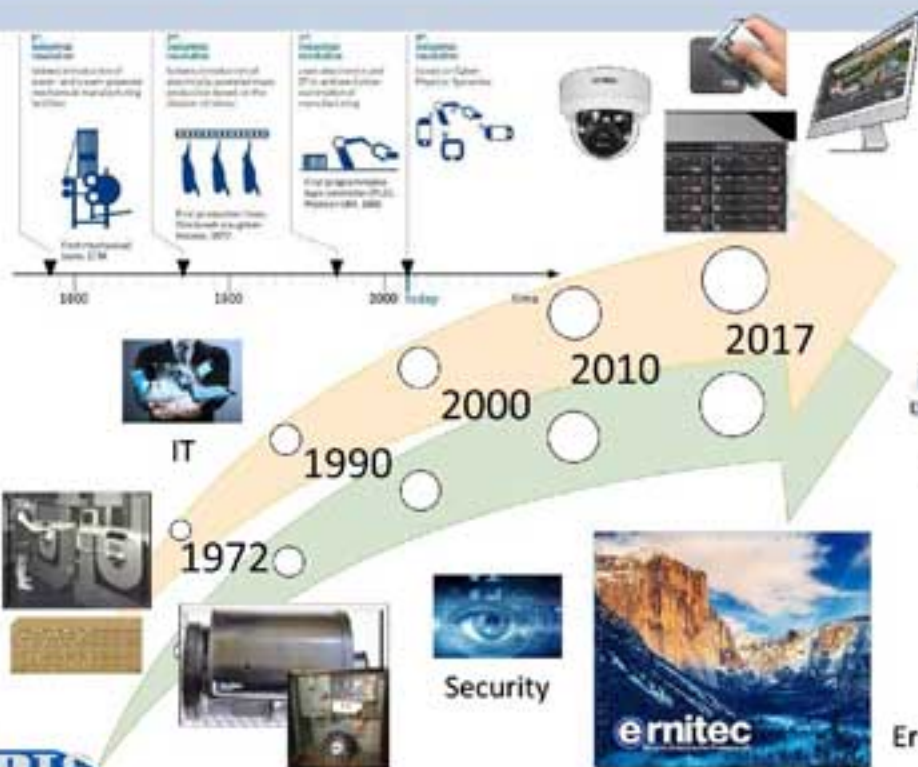
=HOW?

- =Use classical management processes but implement smart IT tools for process management
- =Treat Physical and Cyber risks management in an integrated approach
- =Make use (not abuse) of smart technologies ... but do not forget about **The People!**
- = Permanently observe and adjust for risk dynamics





Revolutions Impacting the Security Market Facing the Challenges of Disruptive Development



Physical & Cyber Security for the Cyber-Physical World



Fighting the last two
industrial revolutions



Ernitec of Denmark. Since 1972





From Analogue to IP Based CCTV & VMS From Video Surveillance to Digital Security

ernitec



=Cosmos IP Cameras - We have 3 Different Performance Bands to choose from. The SX Series is our entry level, resolutions range from 1080P to 6 mega pixel. The DX series is our Starvis low light range and PX Series which is our Ultra HD high resolution 4K Camera Range.

=Computing Hardware – Ernitec have been producing Servers and NVRs for the CCTV industry for over 10 years gaining a wealth of experience in the field and improving designs year on year.

=Video Management System - EasyView is a powerful open platform VMS system with unlimited expansion. EasyView is ideal for CCTV systems where integration Video Analytics, Access control and alarm systems combined with multiple vendor technology is demanded by the end user.



From Storing Video on Hardware to Securely Storing Video in the Cloud

ernitec

**ENCRYPTED CCTV
IN THE CLOUD**



**Ernitec IP Camera
Embedded Software**



BILLING PLATFORM

Mobile App





Access Control, Alarm System, Time & Attendance More Data for Enhanced User Awareness

ernitec



- Asgard is our new Access Control System
- Access Control with integrated Alarm System
- Time & Attendance
- Can be installed to Grade 4 Certification
- Large Range of Cards and Readers





Data Analytics & Fusion > Even More Data Going Digital for Enhanced Security

ernitec



- Video Content Analytics
- Integrated into EasyView

- Reporting Tools



- Trip Wire

- Custom Reports

- Tracking

- Audit Trail

- People Counting

- Alarms & Events

- Dwell Filter

- Bookmarks

- Removed Object

- Centralized Database

- ANPR

- Retail Event Research

- Speed Detection

- Any Web Browser

- Smoke

- People counting reports

- Fire

- ANPR analysis



... but higher level digitalization means:

- Higher Cyber- Risks
- Need for integrated

Cyber & Physical Security Approach



DISCUTII



Mulțumesc!

Aveți întrebări?
user@mail.me