



ACQUA SICURA 4.0 ***la Cyber Security*** ***nei sistemi Scada***

Francesco Tieghi
ServiTecno SRL
ftieghi@servitecno.it

Antonio Allocca
A.T.I. SRL
a.allocca@acmotec.com

ServiTecno



Distributor
Intelligent Platforms





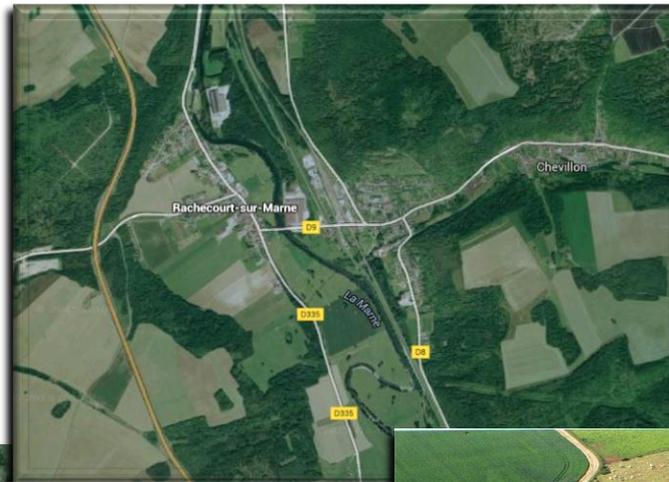
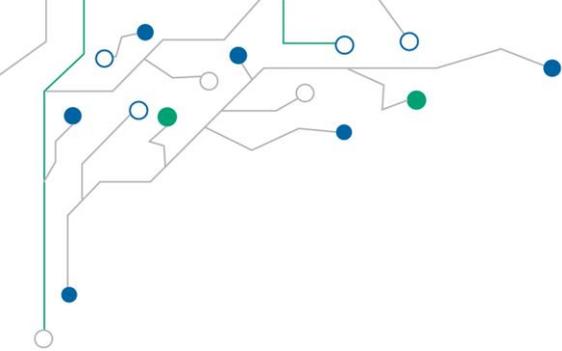
Indice della presentazione

Sicurezza: inquadramento del problema (ServiTecno)

1. Cos'è la sicurezza informatica
2. Un problema non facile da vedere
3. Eventi: fatti e numeri
4. Associazioni di settore

Sicurezza: in pratica (A.T.I.)

1. Valutazione del rischio
2. Minacce ed azioni preventive
 - organizzative
 - ambientali
 - tecniche
3. Conclusioni



RACHECOURT SUR MARNE, Francia - Alta Marna

piccolo paese nella Regione Champagne Ardenne,
meno di 1.000 abitanti ma un corso d'acqua
fondamentale da gestire per l'agricoltura della zona

I PALLINI BLU



Sono più di 13.000 gli indirizzi IP di Sistemi di Controllo (i pallini blu appunto con relativa porta, provider, luogo geografico e coordinate GPS) ai quali è possibile accedere senza particolari difficoltà o competenze tecniche.

TUTTO CIO' CHE PUO' ESSERE ATTACCATO LO SARA'

(Corollario alla legge di Murphy)



- **Italia:** nella **TOP 10** globale per **diffusione malware.**
- **Primi** in Europa per numero di **PC infetti e controllati** da Cyber criminali.
- **Non esiste una legge che obblighi a denunciare furti o altre attività.**

In Italia si può subire un'attacco senza denunciarlo o peggio...

SENZA ACCORGERSENE

TUTTO CIO' CHE PUO' ESSERE ATTACCATO LO SARA'

ICS-CERT MONITOR

September 2014 – February 2015

Assessments by Sector	2014				2015		Sept. – Feb. Totals
	September	October	November	December	January	February	
Chemical							
Commercial Facilities	2						2
Communications							
Critical Manufacturing							
Dams							
Defense Industrial Base			1		1		2
Energy	2	1	3	2		4	12
Food and Agriculture							
Government Facilities					2		2
Healthcare & Public Health							
Information Technology			1				1
Nuclear Reactors, Materials & Waste							
Water and Wastewater Systems	1	6		1	3	3	14
MONTHLY TOTALS	5	7	4	3	5	7	37 Total Assessments

CYBER ATTACK: IERI, OGGI E DOMANI

domenica24 casa24 moda24 food24 motori24 job24 stream24 viaggi24 salute24 shopping24 radio24

Abbonati subito!

NOVA24

Venerdì 10 Luglio 2015

HOME ITALIA MONDO NORME & TRIBUTI FINANZA & MERCATI IMPRESA & TERRITORI

Gadget Social Media Business Startup Innovazione Scienza Games App&Ent

Tecnologie Business

Aerei e borse a rischio hacker: Tecnicamente possibile, ma i precedenti sono pochi

di Biagio Simonetta 9 luglio 2015

HOME ITALIA MONDO NORME & TRIBUTI FINANZA & MERCATI IMPRESA & TERRITORI NOVA24 TECH PLUS24 RISPARMI

Analisi e Inchieste Macroeconomia Europa USA Americhe Medio Oriente e Africa Asia e Oceania

Mondo USA

Hacker cinesi all'attacco rubano 4 milioni di dati di dipendenti federali americani

5 giugno 2015

Tweet 26 Consiglia 71 +1 2



Un gruppo di hacker stranieri ha violato i dati personali di quattro milioni di dipendenti federali americani, tra quelli in servizio ed in pensione. Secondo i giornali e siti americani ci sarebbe dietro un gruppo di programmatori-pirata cinesi. L'attività sospetta è stata individuata ad aprile da parte

MEDIASET
TGCOM24

Panorama Motori Casa Assicurazione Giochi Cucina Scuola Me

HOME PRIMO PIANO SPORT SPETTACOLO TV PEOPLE DONNE LIT

Tgcom24 > Mondo > Attacco hacker a Sony, Usa dimostra responsabilità della Corea del Nord

19 gennaio 2015

Attacco hacker a Sony, Usa dimostra responsabilità della Corea del Nord

Secondo il New York Times, la Nsa è riuscita a infiltrarsi nella rete di Pyongyang ricostruendo i movimenti dei pirati informatici

06:38 - Gli Stati Uniti sono riusciti a stabilire le responsabilità della Corea del Nord nel micidiale cyber-attacco subito dalla Sony Pictures alla fine di novembre grazie ad una intrusione, che risale al 2010, della National Security Agency (Nsa) nel network informatico nordcoreano. Lo scrive il New York Times citando ex funzionari americani e di altri Paesi, nonché esperti informatici successivamente informati dell'operazione e un documento della Nsa.

HOME ITALIA MONDO NORME & TRIBUTI FINANZA & MERCATI IMPRESA & TERRITORI NOVA24 TECH PLUS24 RISPARMI

Analisi e Inchieste Macroeconomia Europa USA Americhe Medio Oriente e Africa Asia e Oceania

Mondo USA

Attacco hacker al sito dell'esercito Usa

8 giugno 2015

Tweet 59 Consiglia 39 +1 1

HOME ITALIA MONDO NORME & TRIBUTI FINANZA & MERCATI IMPRESA & TERRITORI NOVA24 TECH PLUS24 RISPARMI

Analisi e Inchieste Macroeconomia Europa USA Americhe Medio Oriente e Africa Asia e Oceania

Mondo USA

Attacco hacker al sito dell'esercito Usa

8 giugno 2015

Tweet 59 Consiglia 39 +1 1



Attacco hacker al sito dell'Esercito Usa (<http://www.army.mil/>) Il sito risulta (alle 22.30 ora italiana) inaccessibile e a rivendicare l'azione risulta essere stavolta il Syrian Electronic Army, che in un messaggio online critica il governo americano definendolo "corrotto", accusandolo di sostenere il terrorismo (anti-Assad) in Siria e invitando i cittadini statunitensi a non "ascoltarlo".

Hacking Team alza bandiera bianca: «Nostri software fuori controllo». Si teme per il terrorismo

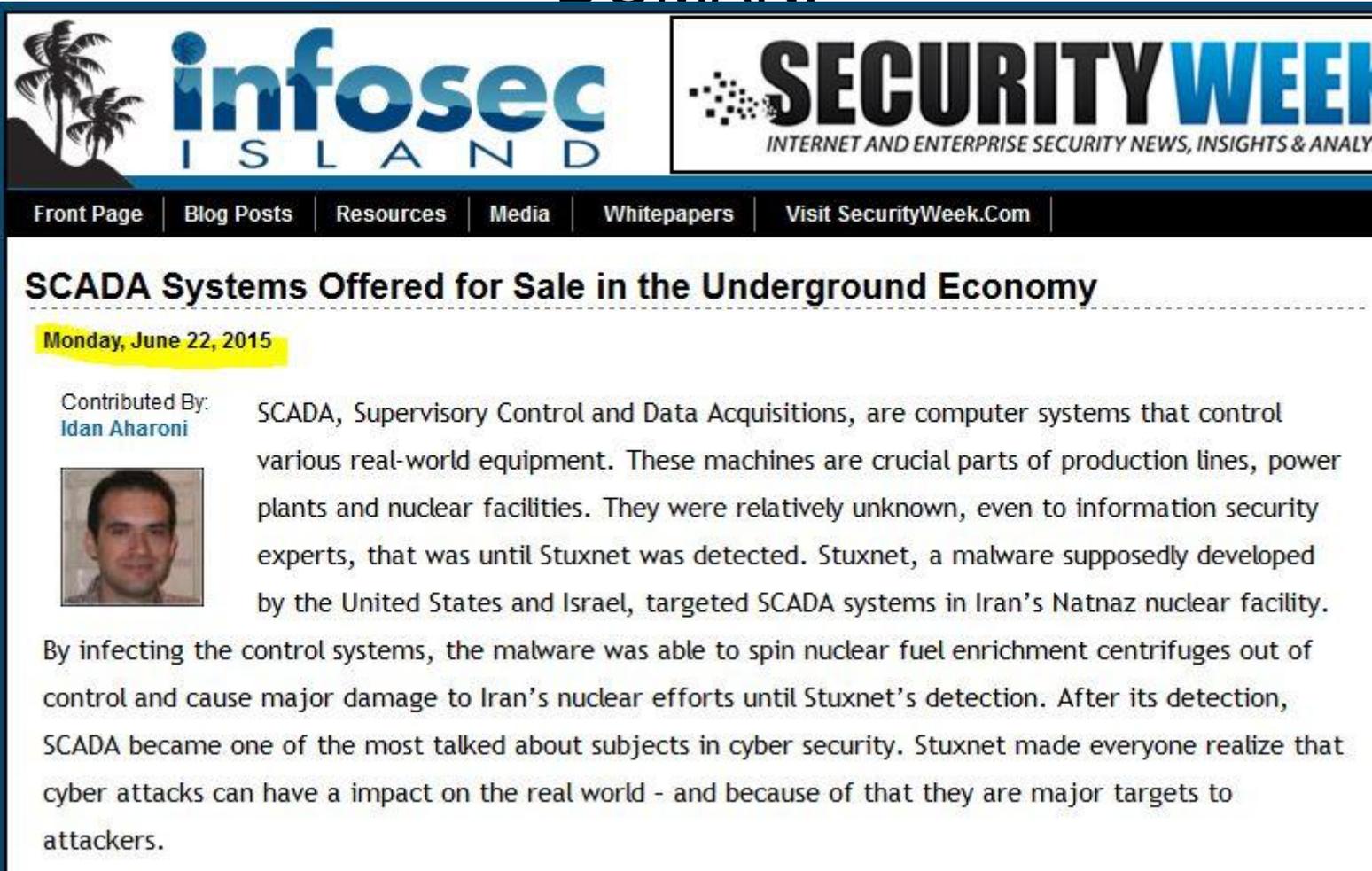
di Biagio Simonetta 9 luglio 2015 Commenti (6)

Tweet 51 Consiglia 889 +1 15



«Abbiamo perso la capacità di controllare chi utilizza la nostra tecnologia. Terroristi, estorsori ed altri possono implementarla a volontà. Crediamo sia una situazione estremamente pericolosa, è ormai evidente che esiste una

CYBER ATTACK: IERI, OGGI E DOMANI



The screenshot shows a webpage header for SecurityWeek with navigation links: Front Page, Blog Posts, Resources, Media, Whitepapers, and Visit SecurityWeek.Com. The main article title is "SCADA Systems Offered for Sale in the Underground Economy" dated Monday, June 22, 2015, by Idan Aharoni. The article text discusses SCADA systems, their role in production lines and power plants, and the impact of the Stuxnet malware attack on Iran's nuclear facility.

infosec ISLAND

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Front Page | Blog Posts | Resources | Media | Whitepapers | Visit SecurityWeek.Com

SCADA Systems Offered for Sale in the Underground Economy

Monday, June 22, 2015

Contributed By:
Idan Aharoni



SCADA, Supervisory Control and Data Acquisitions, are computer systems that control various real-world equipment. These machines are crucial parts of production lines, power plants and nuclear facilities. They were relatively unknown, even to information security experts, that was until Stuxnet was detected. Stuxnet, a malware supposedly developed by the United States and Israel, targeted SCADA systems in Iran's Natanz nuclear facility.

By infecting the control systems, the malware was able to spin nuclear fuel enrichment centrifuges out of control and cause major damage to Iran's nuclear efforts until Stuxnet's detection. After its detection, SCADA became one of the most talked about subjects in cyber security. Stuxnet made everyone realize that cyber attacks can have a impact on the real world - and because of that they are major targets to attackers.

White Paper & Good Practice



Associazioni e Contatti



ENISA - European Network and Information Security Agency
Home About ENISA Our Activities Publications Press & Media Events Recruitment
you are here: home
Awareness Raising
CERT
Identity & Trust
Resilience
Risk Management
Stakeholder
ENISA - Securing Europe's Information Society
Every day we experience the Information Society. Interconnected networks touch our everyday lives, at home and at work. II computers, mobile phones, banking, and the Internet are the backbone of Europe's digital economy. That is why ENISA is working to ensure the Information Security for the EU and the Member States.
See ENISA's tasks and activities



CERT-SPC
COMPUTER EMERGENCY RESPONSE TEAM
Sistema Pubblico di Certificazione - CNIPA
Cerca nel sito
HOME BOLLETTINI RISORSE INIZIATIVE BLOG DOWNLOAD
Il CERT-SPC Missione del portale FAQs Contatti Responsabilità e Copyright



ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA
Dipartimento di Informatica e Comunicazione Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - tel. 347.231.9285 - fax 02.700.440.496
Home Formazione Eventi Pubblicazioni



Polizia di Stato
Chi siamo Le questurati
L'organizzazione Polizia delle comunicazioni



Clusit
Sicura mente
CHI SIAMO | SOCI | VETRINA SOCI | LINKS | VIRUS | WHITE PAPERS | ISCRIZIONE ALLA NEWSLETTER
COME ASSOCIARSI | STAMPA | ARCHIVIO | LEGALE | ASSICURAZIONI | INFORMAZIONI | AREA SOCI | AREA C.D.
ENGLISH
Eventi - News
Milano 14-16 Marzo 2011
SECURITY SUMMIT
Roma 9-10 Giugno 2010
Atti - Video - Foto
Milano 15-18 Marzo 2010
Atti - Video - Foto
FSE
ROSI
Premio Tesi
Inserito di MF 30 set 2010
La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per far fronte ai problemi della sicurezza informatica. Il CLUSIT nasce sulla scorta delle esperienze di altre associazioni europee per la sicurezza informatica quali CLUSIB (B), CLUSIF (F), CLUSIS (CH), CLUSSIL (L) che costituiscono un punto di riferimento per la sicurezza informatica nei rispettivi paesi da oltre 10 anni. Il CLUSIT è aperto ad ogni persona e organizzazione che manifesti un interesse per la sicurezza informatica.
OBIETTIVI
• **Diffondere** la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
• **Partecipare** alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello comunitario che italiano.
• **Contribuire** alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
• **Promuovere** l'uso di metodologie e tecnologie innovative.
Blog Clusit
Calendario Seminari 2011
Clusit Education
Calendario Seminari ed esami
Information Resources Online



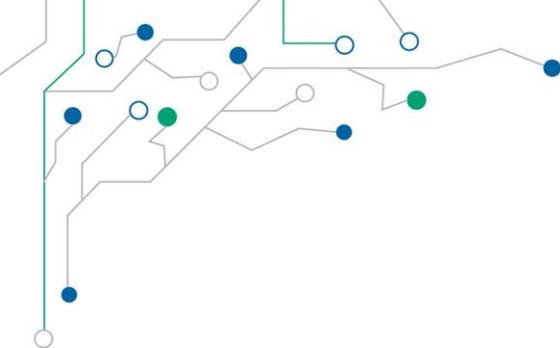
- Questure
- Reparti mobili
- Reparti prevenzione crimine
- Reparti volo
- NOCS
- Polizia stradale
- Polizia dell'immigrazione
- Polizia delle comunicazioni
- Polizia ferroviaria
- Polizia della montagna
- Polizia del mare
- Polizia scientifica
- Polizia di prevenzione
- Polizia dei giochi e delle scommesse
- Polizia a cavallo
- Cinefili



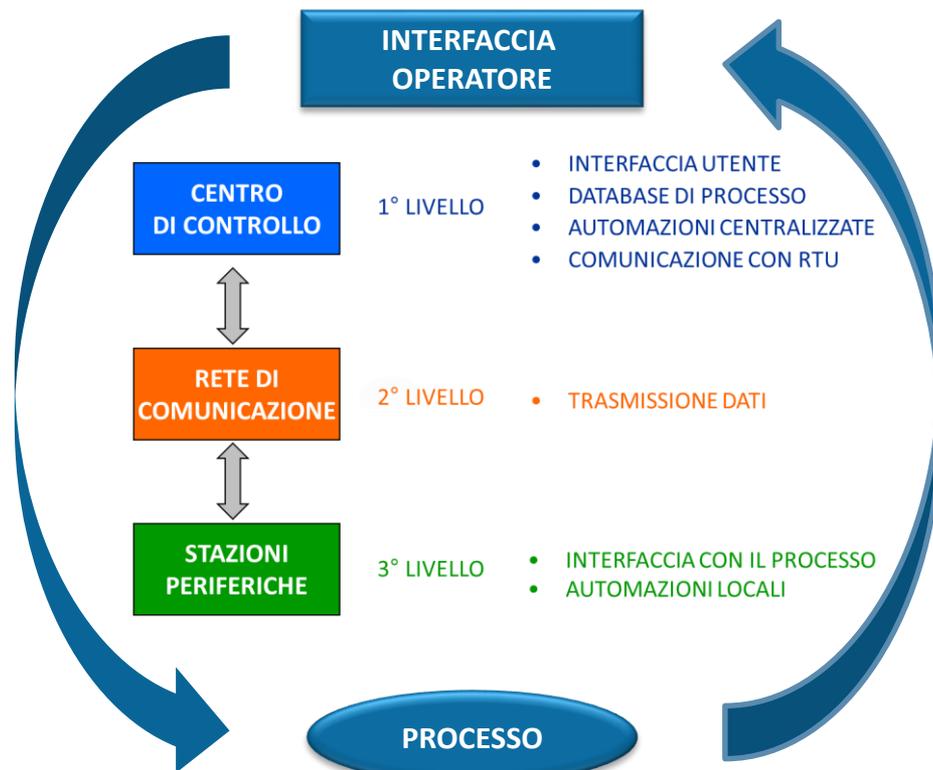
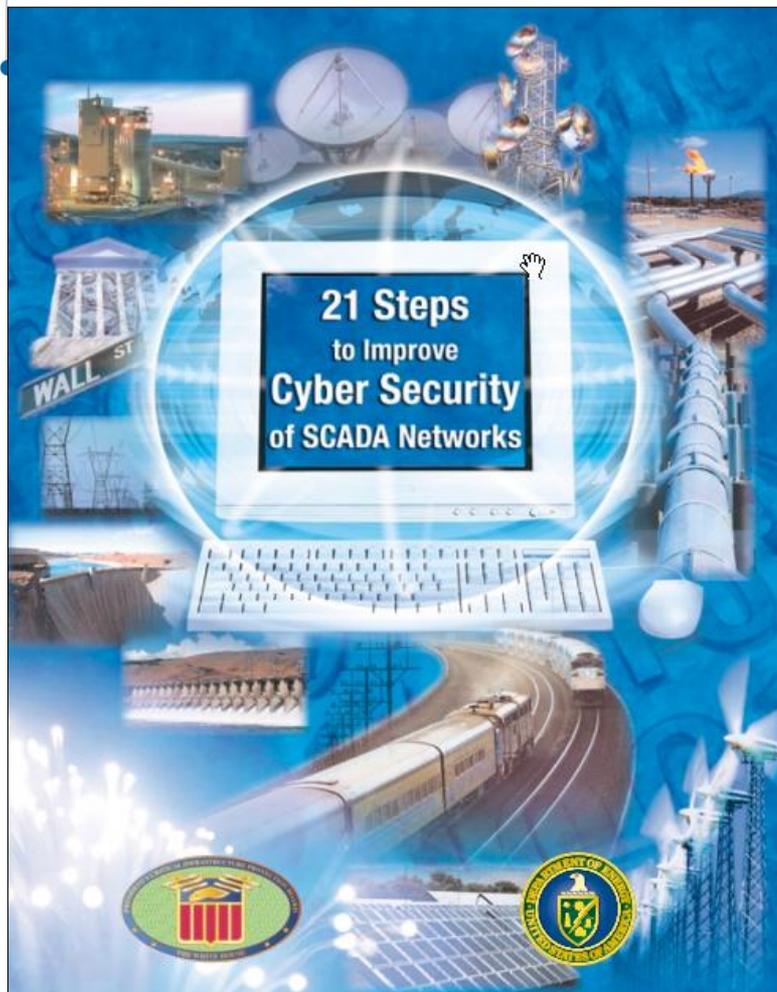
CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione Infrastrutture Critiche
Il C.N.A.I.P.I.C. è in via esclusiva incaricato della repressione dei crimini informatici organizzata o terroristica, che hanno infrastrutture informatizzate di natura critica e di rilevanza nazionale.
Il valore aggiunto che il Centro rappresenta, nel panorama della protezione delle Infrastrutture Critiche deriva:
- dalla realizzazione di una Sala operativa, disponibile 24 ore su 24 e 7 giorni su 7, in qualità di Punto di contatto univoco dedicato sia alle I.C., sia ad ogni altro attore, anche a livello internazionale, impegnato nella protezione delle I.C.;
- dai collegamenti telematici esclusivi, dedicati e protetti, tra il C.N.A.I.P.I.C. e le I.C., per il condiviso, reciproco e costante trasferimento dei dati e delle informazioni utili all'esercizio delle funzioni di valutazione, prevenzione e repressione delle minacce e dei crimini informatici.
Unità di analisi sul crimine informatico/Computer Crime Analysis Unit
CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Come la Postale smaschera i pedofili online
Nuova frontiera nell'addestramento online dei bambini

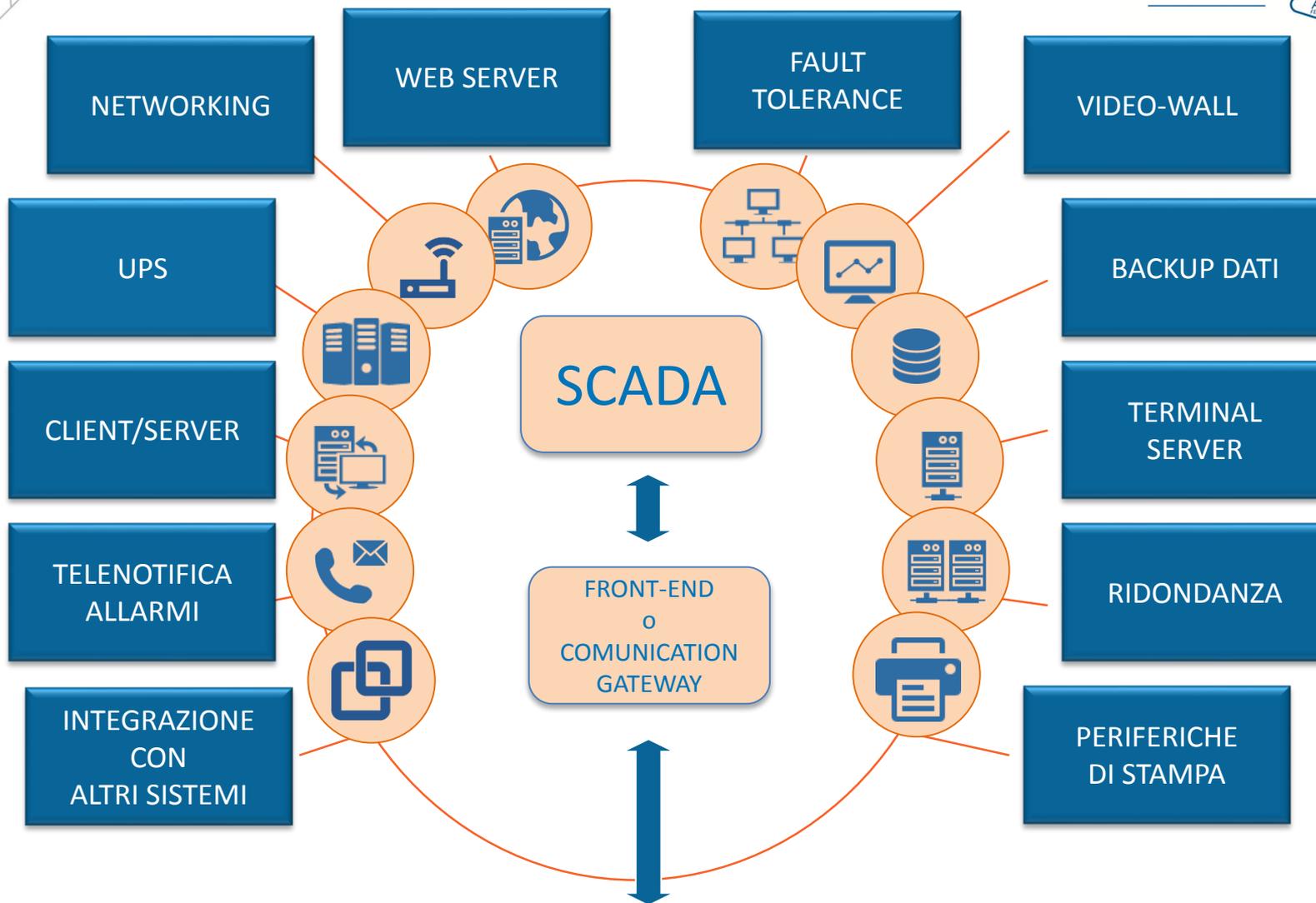


ASSOCIAZIONE ITALIANA
ESPERTI IN
INFRASTRUTTURE CRITICHE

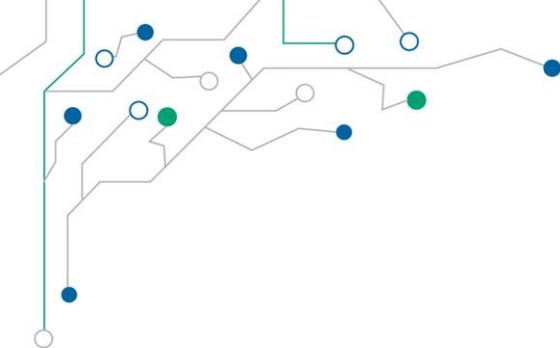


... IN PRATICA





2° LIVELLO – RETE DI COMUNICAZIONE



SICUREZZA INFORMATICA: DEFINIZIONI

La **sicurezza** può essere definita come
la "conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati".

In termini più semplici è: sapere che quello che avverrà non provocherà dei danni.

La sicurezza totale si ha in assenza di pericoli.

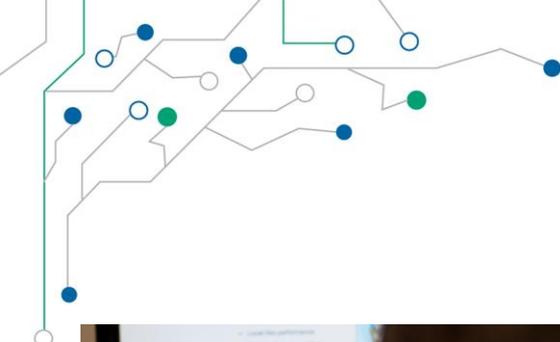
In senso assoluto, si tratta di un concetto difficilmente traducibile nella vita reale anche se l'applicazione delle *norme di sicurezza* rende più difficile il verificarsi di eventi dannosi e di incidenti.



Sicurezza informatica:

il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia dovuta ad eventi accidentali.

RISERVATEZZA – INTEGRITA' – DISPONIBILITA'



MINACCE e AZIONI PREVENTIVE



MINACCE di tipo ORGANIZZATIVO

mancanza di
consapevolezza

mancanza di
policy per la
sicurezza

gestione accessi
al sistema
limitatamente
regolati

nessuna
procedura per
gestione
password

formazione
del
personale

procedure per
cambio
configurazioni

procedure
per accesso
ai sistemi

procedure
per gestione
password

AZIONI PREVENTIVE

MINACCE e AZIONI PREVENTIVE

MINACCE di tipo AMBIENTALE

discontinuità
alimentazione
elettrica

eventi meteo
eccezionali, incendi,
esplosioni

vandalismi, furti

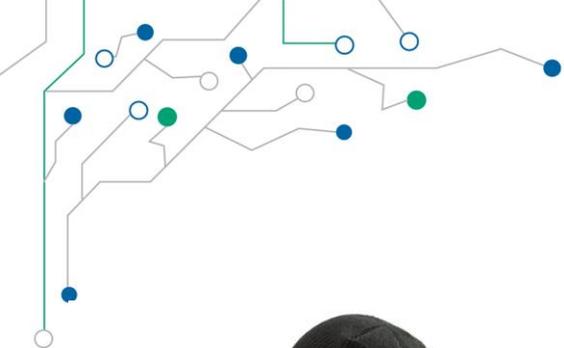
protezione
elettrica

disaster recovery

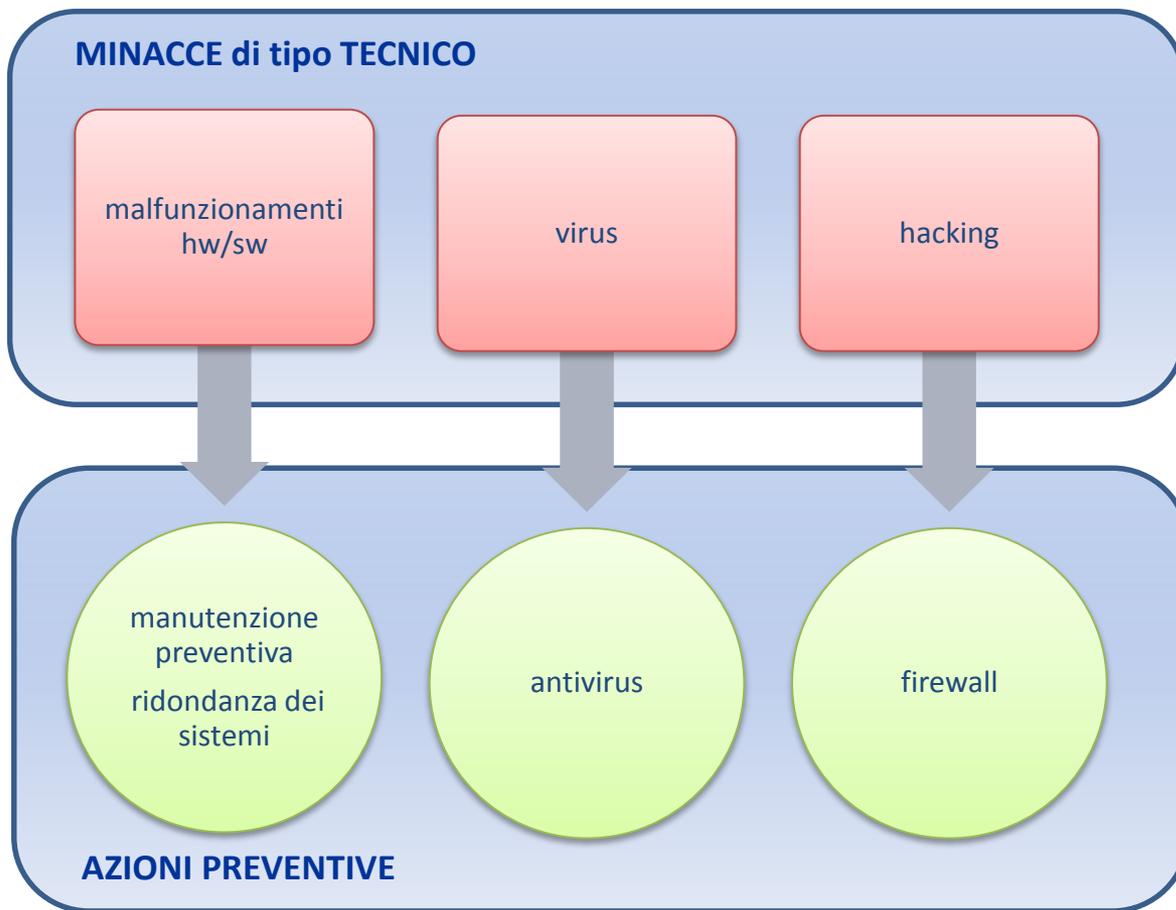
protezione locali
controllo accessi
videosorveglianza

AZIONI PREVENTIVE





MINACCE e AZIONI PREVENTIVE





MINACCE e AZIONI PREVENTIVE



Accessi locali e remoti per manutentori e fornitori.

Ricordiamoci di censire tutti gli accessi, controlliamoli e soprattutto proteggiamoli in modo adeguato!

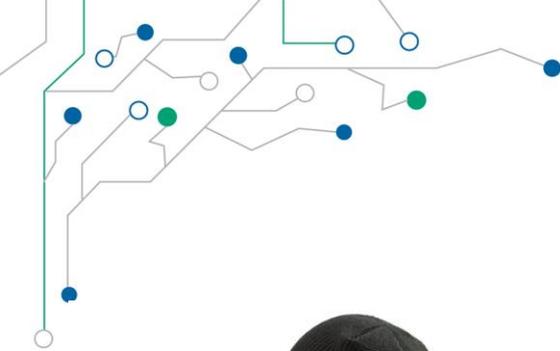
VPN: Virtual Private Network ~~Virus Propagation Network~~

Documentazione e Back-up.

Dove sono? Sono aggiornati?

Sono una risorsa per limitare i danni da malfunzionamenti e rotture.





MINACCE e AZIONI PREVENTIVE



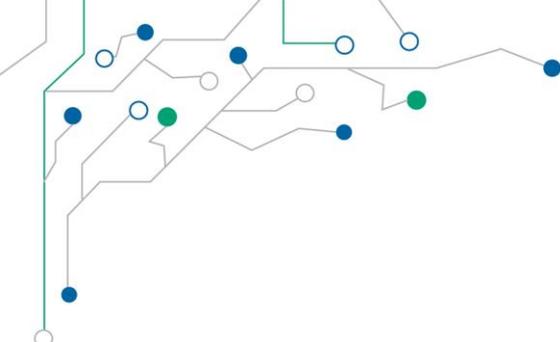
PERIODICA ANALISI DI HW E SW

può essere utile ad identificare potenziali criticità e programmare per tempo aggiornamenti.

ANTIVIRUS

mancano totalmente ?
non sono previsti ?
non sono compatibili con le applicazioni ?
le signature sono vecchie di mesi: a cosa serve ?
le patch di sicurezza, di quando sono ?
aggiornate all'ultima fermata dell'impianto ?





FOCUS: ANALISI

Analisi di Rischio

- Definizione minacce
- Identificazione vulnerabilità

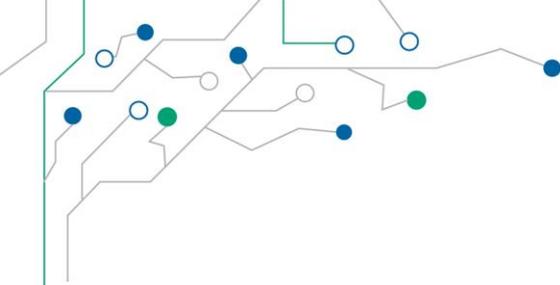
Analisi di Sistema

- Architettura funzionale e fisica
- Interfacce interne ed esterne

Analisi di sicurezza

- Definizione perimetri di intervento
- Definizione azioni preventive





RISCHI

Rischio
n°1

sovraccarico

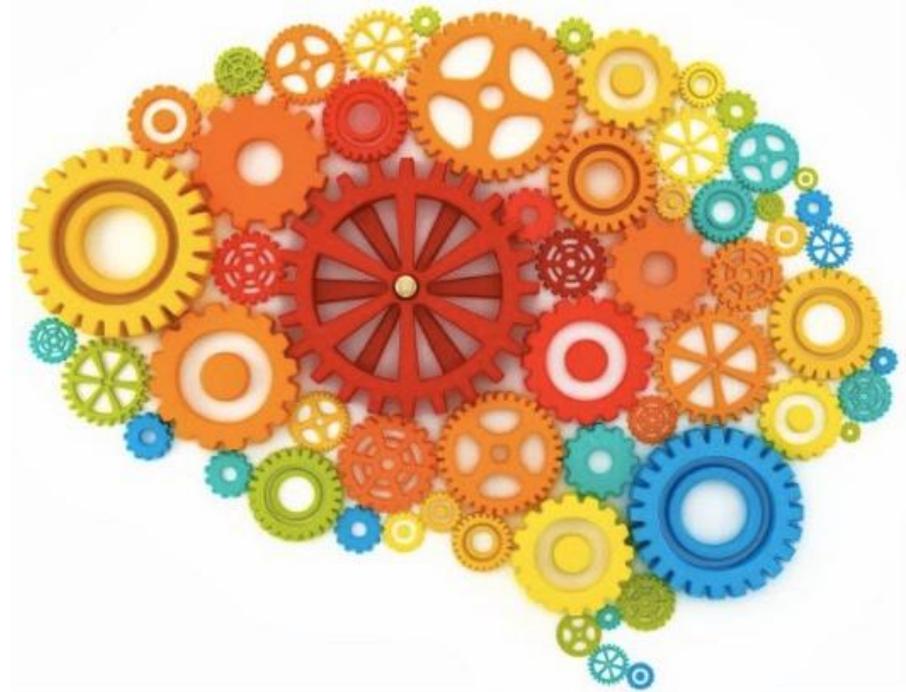


Rischio
n°2

creatura
meravigliosa



**SEMPLICITA'
APPARENTE vs.
COMPLESSITA'
REALE**



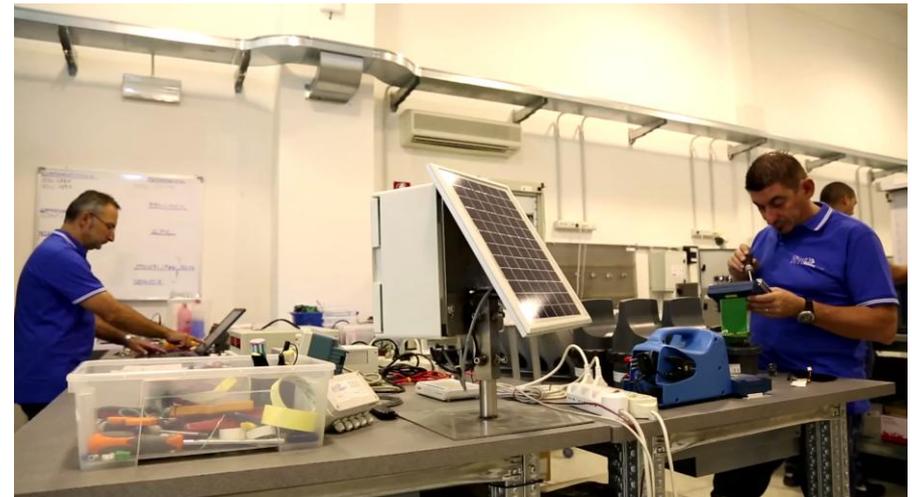
**Aumento della
complessità reale a
fronte della semplicità
apparente.**



Il ruolo del **system integrator** TELECONTROLLO e CUCINA



- ✓ La varietà degli ingredienti non è sufficiente per garantire il risultato.
- ✓ Mischiando buoni ingredienti non sempre ottengo un buon risultato.
- ✓ I cibi preconfezionati.
- ✓ Il fattore di scala.
- ✓ Gli obiettivi del padrone di casa.



Soluzioni per la sicurezza dei sistemi di telecontrollo-infrastrutture critiche



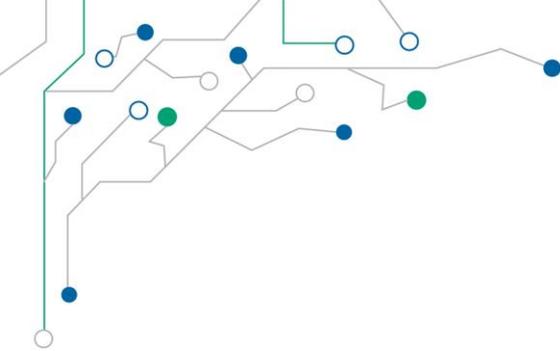
Minaccia

organizzativa
fisica
informatica

	X			X	X		X	X	X	X
X		X	X	X		X				X
		X	X			X		X	X	X

Azione correttiva





GRAZIE PER L'ATTENZIONE !

Enzo Maria Tieghi
ServiTecno SRL
etieghi@servitecno.it

ServiTecno



Distributor
Intelligent Platforms

Antonio Allocca
A.T.I. SRL
a.allocca@acmotec.com

