Introduzione alla *Sicurezza*

Obiettivo della presentazione

- Introdurre il concetto di sicurezza
- Fornire una tassonomia

Indice

- Introduzione
- Dependability
- Safety
- Security
- Cybersecurity
  - sua rilevanza
- Conclusioni

Note

- Nel seguito introdurremo il concetto di Sicurezza utilizzando definizioni diverse, che partono da diversi punti di vista.
- Come vedremo, al termine italiano *Sicurezza* corrispondono in inglese termini diversi (principalmente *Safety* e *Security*, ma anche *Dependability*).

Definizioni

- Le slide nella quali in alto a destra è raffigurato un dizionario, come in questa, contengono delle *definizioni*.

Sicurezza (Security)

- L'assenza di quelle condizioni che possono causare la perdita di beni patrimoniali con conseguenze inaccettabili

[“Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems,”
NIST, Tech. Rep. NIST.SP.800-160 Volume 1, Nov. 2016:
https://doi.org/10.6028/NIST.SP.800-160v1]

Implicazioni pratiche

- È imperativo che l'ambito specifico della sicurezza debba essere chiaramente definito dalle parti interessate in termini di:
  - *beni* (asset) a cui si applica la sicurezza
  - *impatto* rispetto alle quali viene valutata la sicurezza.

Asset

- Qualsiasi bene o elemento di valore di proprietà di un individuo o di un’organizzazione.

Asset - classificazioni

- Un asset può essere:
  - *tangibile* (ad ed., un dispositivo fisico come hardware, piattaforma di calcolo, dispositivo di rete o qualsiasi altro componente tecnologico)
  - *intangibile* (ad es., dati, informazioni, software, marchi, copyright, brevetti, proprietà intellettuali, immagine o reputazione).

Impatto

- La perdita di un asset ha un *impatto* che ne riassume il valore, la criticità, la insostituibilità e il suo ruolo nel raggiungere obiettivi, mission e business dello stakeholder.

Rischio (Risk)

- Con il termine *rischio* si riferisce alla possibilità che si verifichi un evento negativo che comporti un danno (impatto).

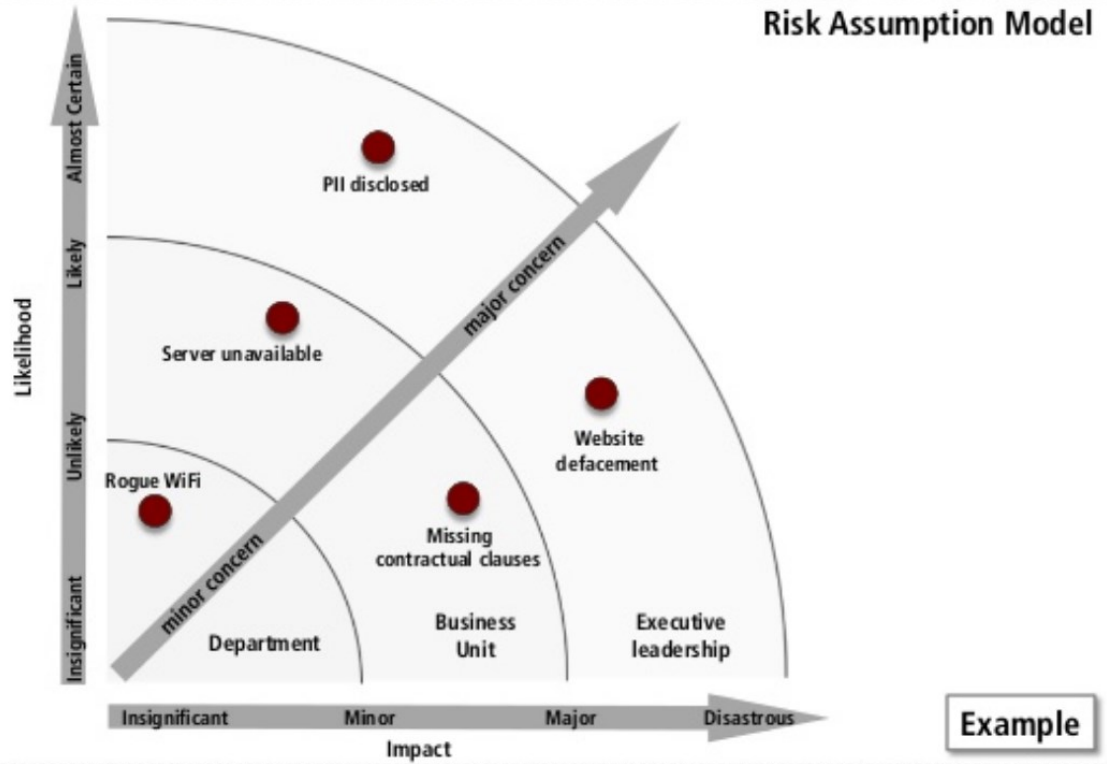
Risk = Likelihood x Impact

Cyber-risk

- Il termine *cyber-risk* si riferisce alla possibilità di danno (perdita finanziaria, interruzione di servizio o danno reputazionale) subito da un'organizzazione a seguito di un malfunzionamento dei suoi sistemi informatici.

Risk = Likelihood x Impact

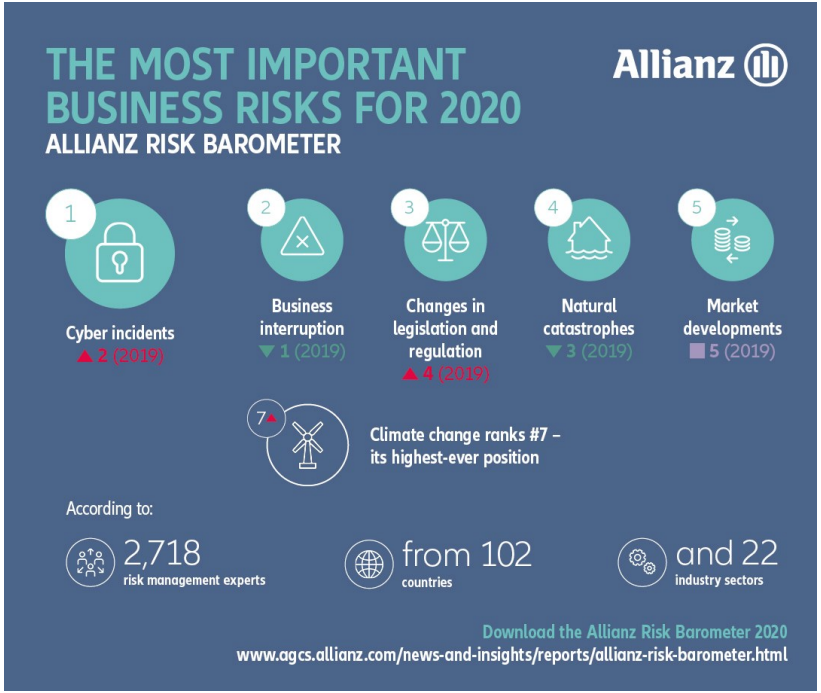
Risk-based prioritization



[https://www.slideshare.net/MarceloMartinsCISSPC/information-security-strategic-management]

Cyber-risk

La consapevolezza del cyber-risk è cresciuta rapidamente negli ultimi anni a causa sia dell'aumentata dipendenza dai servizi digitali che dal crescente numero di incidenti cyber di alto profilo.



[https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020.html]

Protezione degli asset

- Alla luce di queste considerazioni, si devono progettare *protezioni* appropriate per garantire le prestazioni e l'efficacia del sistema di sicurezza contro la perdita di asset e le relative conseguenze.

Sicurezza

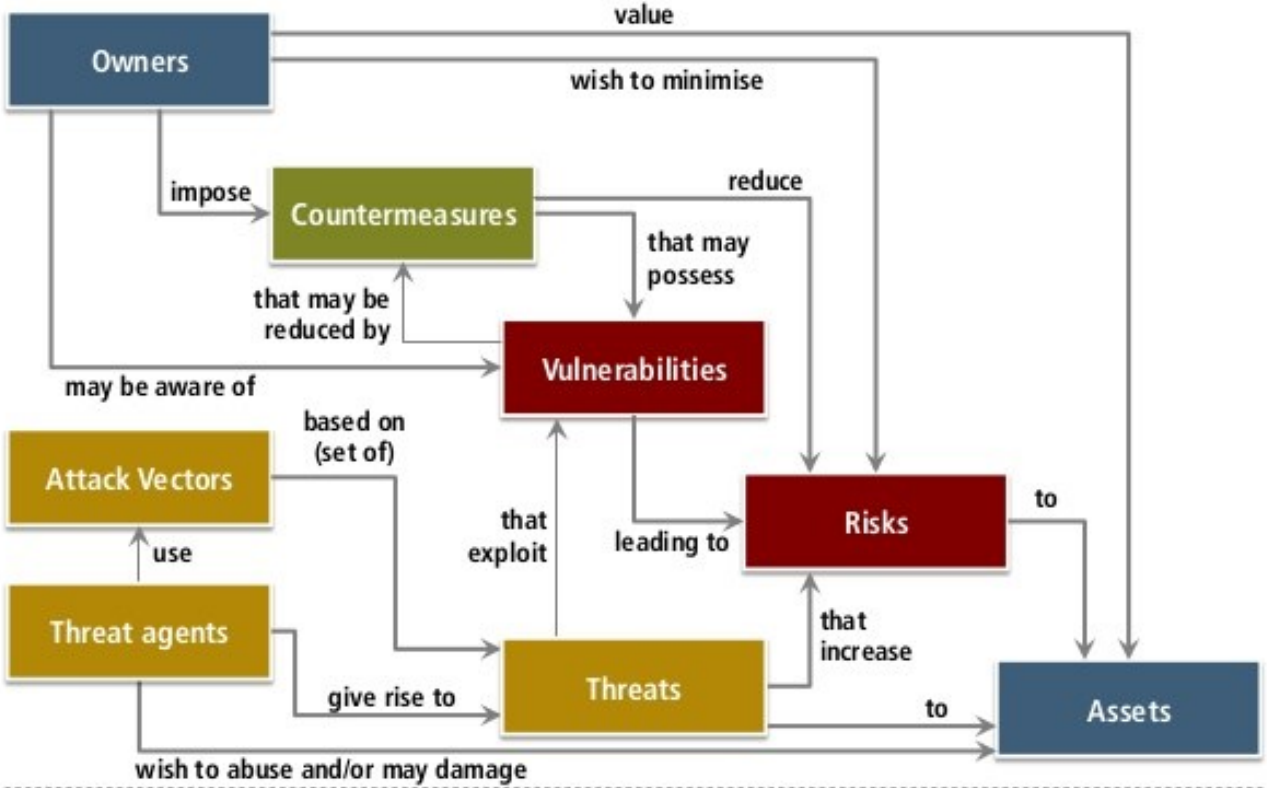
- Condizione oggettiva esente da *minacce* (*threats)*

Vulnerabilità

- *Debolezza* presente in una delle *componenti di un sistema* che può essere sfruttata da un attaccante per condurre un *attacco* contro il sistema stesso

Framework

Security Context



The elements of risk and their relationships according to ISO 15408:2005

Sicurezza, Minaccia

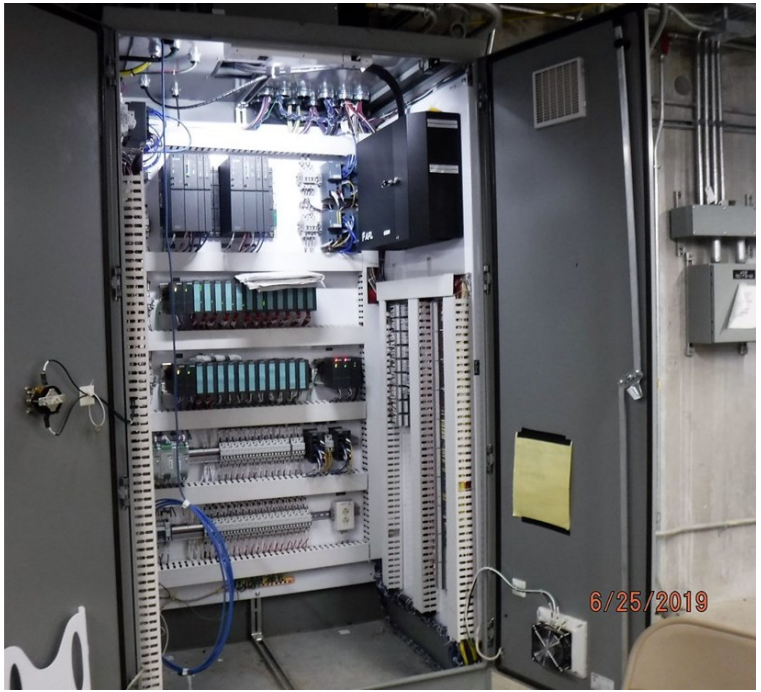
- Assumono significati diversi in ambiti diversi
- Nel seguito ci concentreremo esclusivamente su:
  - *IT - Information Technology*
  - *OT - Operational Technology.*

IT - Information Technology

- Si riferisce a tutto ciò che ha a che fare con la tecnologia informatica
- Si concentra sulla memorizzazione, il recupero, la trasmissione, la manipolazione e la protezione dei dati.

OT - Operational Technology

Sistemi Hardware e software che rilevano o causano un cambiamento attraverso il monitoraggio e/o il controllo diretto di dispositivi fisici, processi ed eventi all'interno di un'organizzazione.



Safety, (Cyber)Security e Dependability

- Persone
- Ambiente
- Oggetti
- Computer
- Informazioni
- Cyberspace

Safety, (Cyber)Security e Dependability

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

Safety, (Cyber)Security e Dependability

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

Safety, (Cyber)Security e Dependability

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni

SECURITY

- Cyberspace

CYBERSECURITY

Safety, (Cyber)Security e Dependability

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni

SECURITY

- Cyberspace

CYBERSECURITY

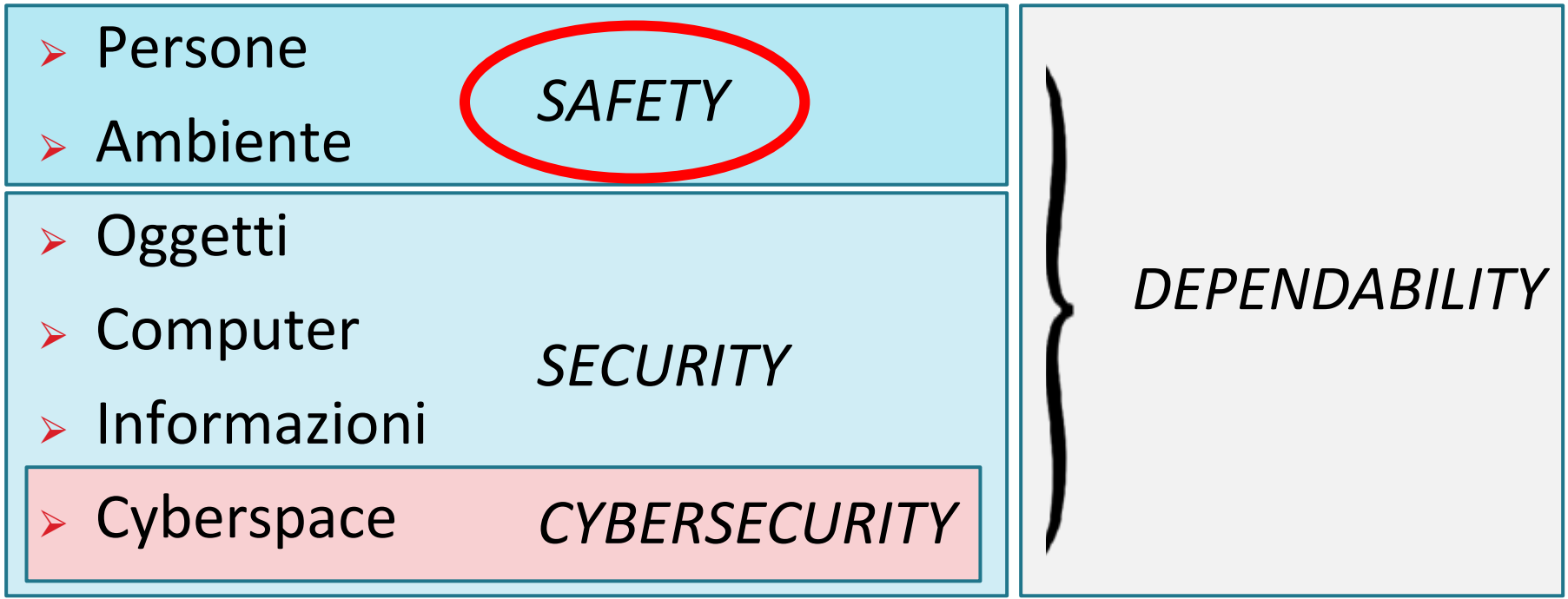
DEPENDABILITY

Dependability

- La misura in cui si può fare affidamento sul fatto che un determinato sistema esegua esclusivamente e correttamente i compiti definiti, in condizioni operative e ambientali definite, in un determinato periodo o istante di tempo.

["Industrial-Process Measurement and Control - Evaluation of System Properties for the Purpose of System Assessment", Part 5: Assessment of System Dependability, Publication 1069-5, Int'l Electrotechnical Commission (IEC) Secretariat, Feb. 1992]

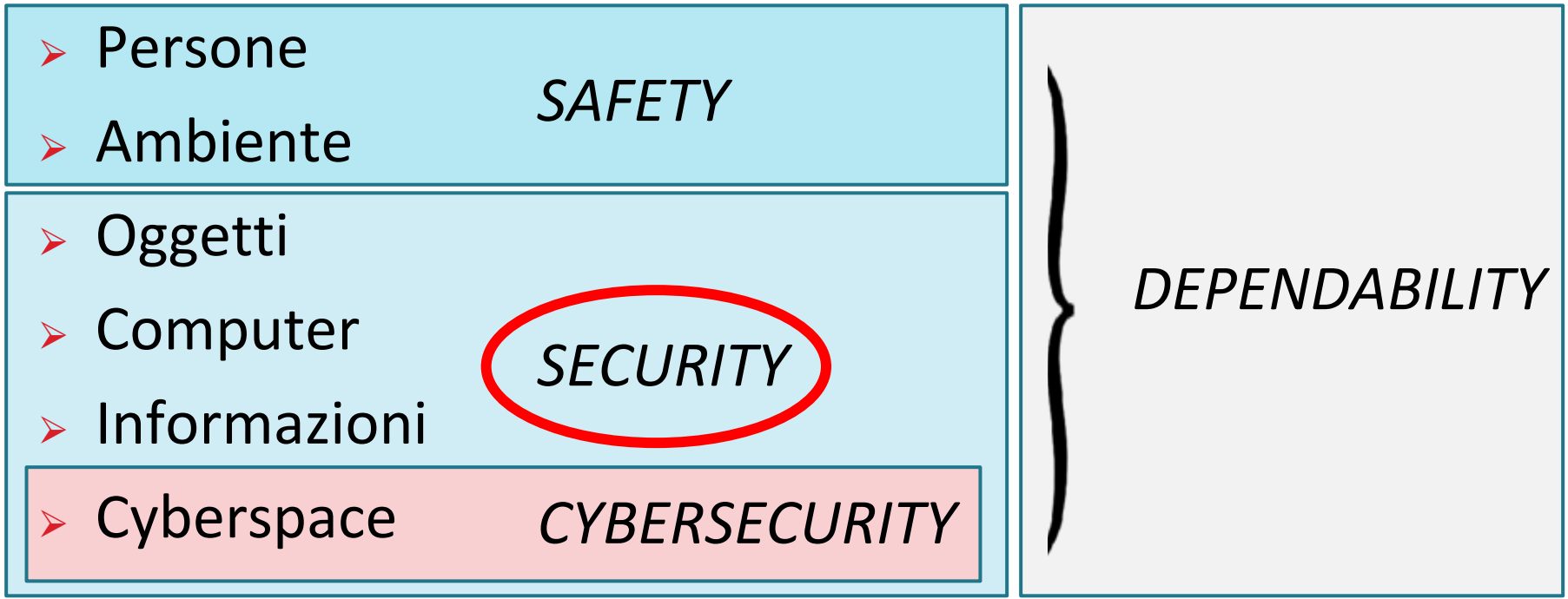
Safety, (Cyber)Security e Dependability



Safety

- Proprietà di un sistema che ne riflette la capacità di funzionare, normalmente o in modo anomalo, senza il rischio di causare lesioni o morte agli esseri umani e senza arrecare danni all'ambiente circostante.

Safety, (Cyber)Security e Dependability



Safety and Security

- La differenza tra safety e security non è solo nel tipo di bene esposto al rischio (fisico vs cyber), quanto nella *accidentalità* o *intenzionalità* della minaccia.
- **Safety:** la minaccia è un evento accidentale endogeno (ad es. fault di un componente) o esogeno (ad es. evento atmosferico, o rumore elettromagetico)
- **Security:** la minaccia è portata da un agente (umano) ostile.

Computer security

- Si occupa della prevenzione e del rilevamento di azioni non autorizzate da parte degli utenti di un sistema informatico

Computer security

- Si occupa della prevenzione e del rilevamento di azioni non autorizzate da parte degli utenti di un sistema informatico
- La definizione di *Autorizzazione* è cruciale
- Presuppone una *policy di sicurezza*, che dice chi (o che cosa) possa fare cosa

Computer security

- Insieme di misure e controlli mirati a garantire la *riservatezza*, *l'integrità* e la disponibilità delle risorse di un sistema di elaborazione, incluse hardware, software, firmware e dati in elaborazione, archiviati o trasmessi.

[The NIST Internal/Interagency Report NISTIR 7298
- Glossary of Key Information Security Terms, May 2013
(**NIST** = U.S. National Institute of Standards and Technology)]

Sicurezza delle informazioni

- Si occupa della sicurezza delle informazioni, indipendentemente dai sistemi informativi dai quali vengono trattate

Sicurezza delle informazioni

- Le informazioni sono più generali dei dati
- I dati veicolano informazioni
- Le informazioni possono anche essere rivelate senza rivelare dati (ad esempio, tramite riassunti statistici)
- Costituisce un diritto fondamentale: protezione di sé (possesso, ...)

Quotazioni dei dati nel Dark Web

- data di nascita, social security number
- informazioni su carte di credito
- social media account
- cartelle sanitarie

Quotazioni dei dati nel Dark Web

- data di nascita, social security number 3 $
- informazioni su carte di credito 75 ¢ - 40 $
- social media account 16 $ - 325 $
- cartelle sanitarie 500 $ - 1200 $

500,000+ Zoom accounts available for sale on the Dark Web

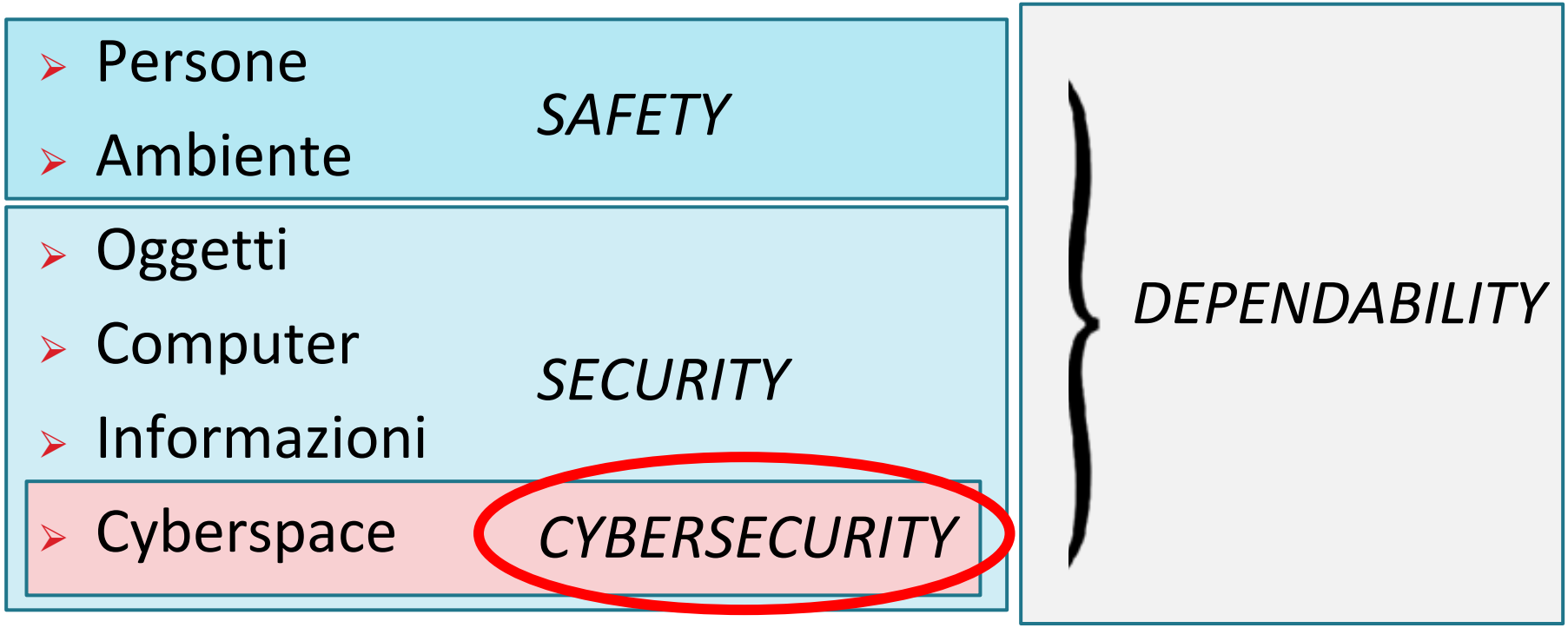
April 13, 2020 By Pierluigi Paganini

Zoom accounts are flooding the dark web, over 500 hundred thousand Zoom accounts are being sold on hacker forums.

Over 500 hundred thousand Zoom accounts are available for sale on the dark web and hacker forums. Sellers are advertising them for .0020 cents each, in some cases they are offered for free.

The huge trove of account credentials was not stolen by Zoom, instead, it appears the result of credential stuffing attacks that leverage records from third-party data breaches.

Safety, (Cyber)Security e Dependability



Cybersecurity

- Pratica che consente a una entità (organizzazione, cittadino, nazione, …) la protezione dei propri asset fisici e la *confidenzialità*, *integrità* e *disponibilità* delle proprie informazioni dalle minacce che provengono dal *cyberspace.*

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspace

- Quel complesso risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti a esso connesse

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:

Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali

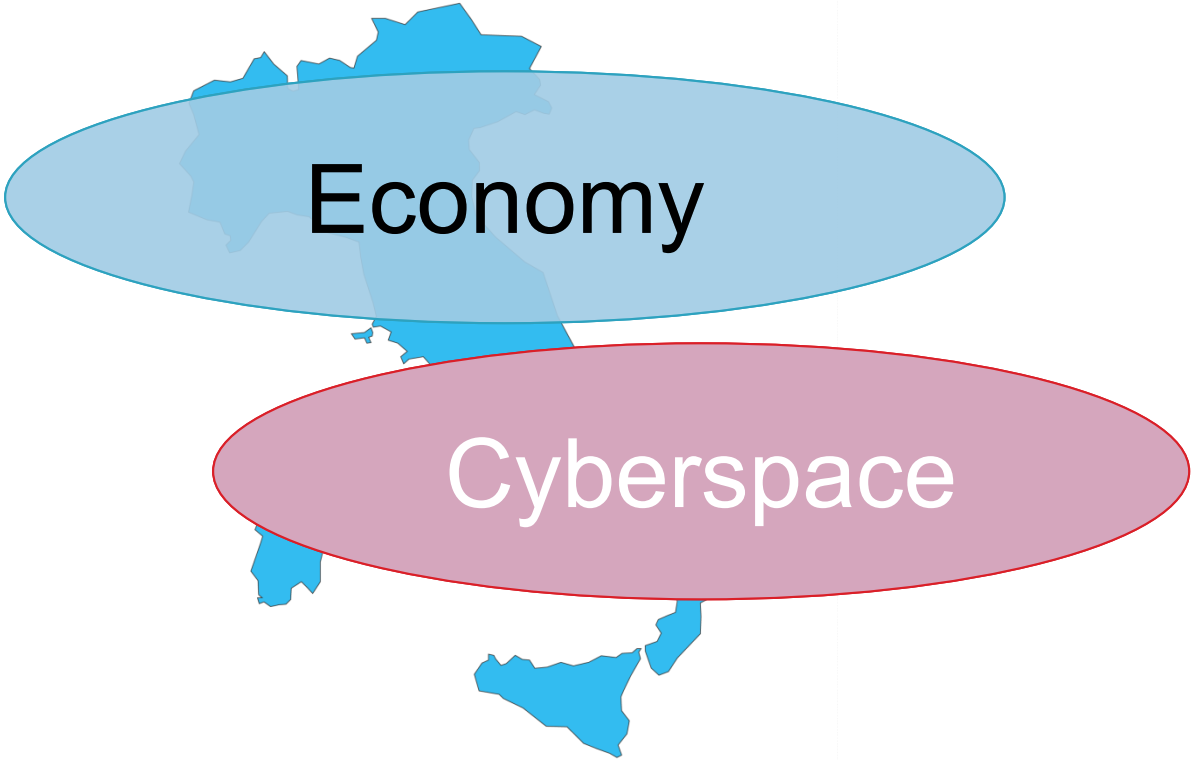
Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali
  - Internet pensata come strumento di collaborazione *friendly* e con servizi *best-effort*
  - …

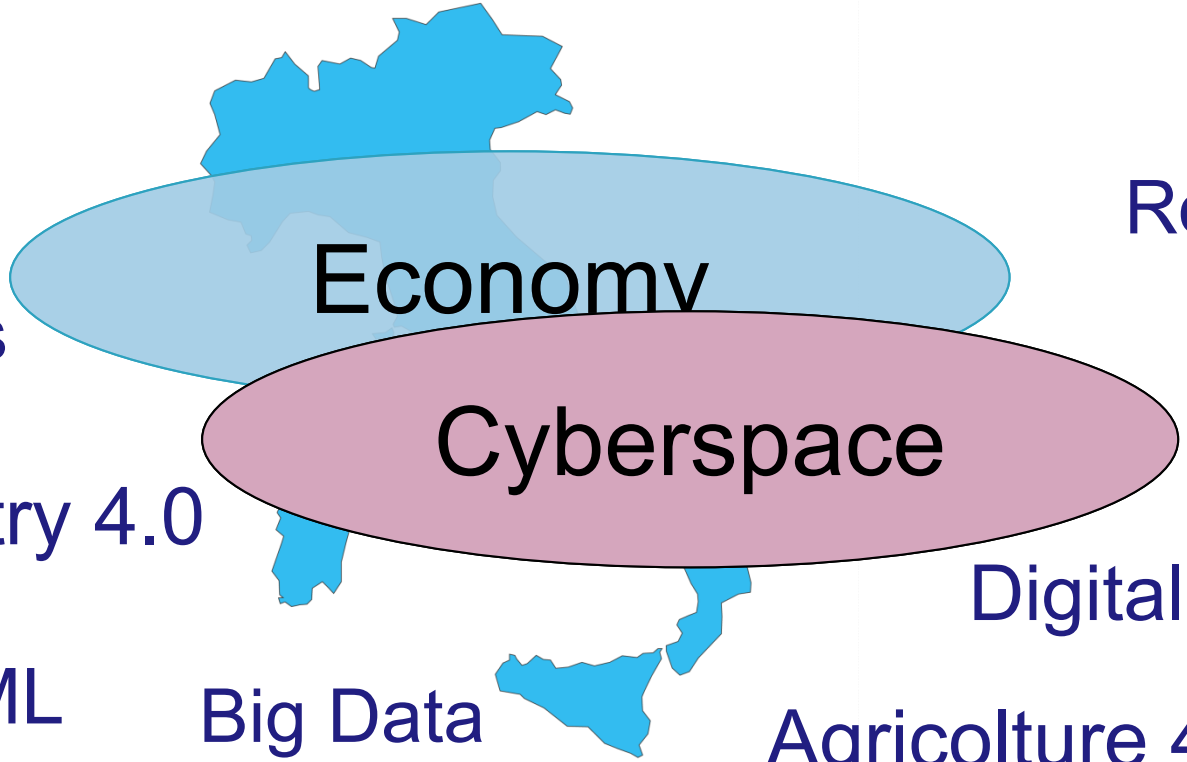
Cyberspace

- Ci consente di:
  - comunicare e interagire dovunque, in ogni momento
  - svolgere un maggior numero di attività per unità di tempo
  - memorizzare e gestire maggiori quantità di dati
  - superare le barriere spazio-temporali (frontiere comprese)

Pervasività del cyberspace



Pervasività del cyberspace



IoT

Drones

Industry 4.0

AI & ML

Big Data

Robotics

Smart Cities

Digital Currencies

Agricolture 4.0

Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito
- La complessità genera *vulnerabilità*

Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito
- La complessità genera *vulnerabilità*
- Le *vulnerabilità* sono sfruttate dai cyber-criminali per sferrare *attacchi*

Cyberspace & Cybersecurity

- Vulnerabilità e attacchi saranno oggetto del prossimo Modulo

Indice

- Introduzione
- Dependability
- Safety
- Security
- Cybersecurity
  - sua rilevanza
- Conclusioni

L'appello di Mattarella per la cybersicurezza: "Gli Stati hanno l'obbligo di difendere dagli attacchi web"

Il presidente della Repubblica Sergio Mattarella a Riga (Lettonia), in occasione del vertice Arraiolos (ansa)

"Non dobbiamo cadere nella trappola di pensare di potere irreggimentare i nostri concittadini orientandoli, ma stimolare la loro libertà e il loro spirito critico", così il capo dello Stato durante il meeting in Lettonia

13 Settembre 2018

" *Le conseguenze di attacchi informatici possono essere disastrose: sui sistemi informatici pubblici, sulle banche, sui sistemi elettorali, sui sistemi sociali e sanitari. E la possibilità che grandi gruppi criminali, o anche Stati con atteggiamento ostile, possa provocare questi danni disastrosi è davvero allarmante per tutti* ".

L'appello di Mattarella per la cybersicurezza: "Gli Stati hanno l'obbligo di difendere dagli attacchi web"

Il presidente della Repubblica Sergio Mattarella a Riga (Lettonia), in occasione del vertice Arraiolos (ansa)

"Non dobbiamo cadere nella trappola di pensare di potere irreggimentare i nostri concittadini orientandoli, ma stimolare la loro libertà e il loro spirito critico", così il capo dello Stato durante il meeting in Lettonia

RELAZIONE DEGLI 007

L'appello di Conte ai cittadini: 'La cybersecurity diventi interesse di tutti'

di **Luigi Garofalo** | 28 Febbraio 2019, ore 13:31

Alla presentazione della Relazione sulla politica dell'informazione per la sicurezza 2018, Giuseppe Conte: 'La minaccia cibernetica può danneggiare le infrastrutture critiche e strategiche. La cultura della cybersecurity diventi interesse dei cittadini per incrementare il livello complessivo di sicurezza, anche se l'Intelligence è il custode della cybersecurity nazionale'.

Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"

Jean-Claude Juncker, presidente della Commissione europea (ansa)

Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity tra le priorità dell'agenda e propone un'Agenzia europea per la sicurezza

di ARTURO DI CORINTO

Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"

Jean-Claude Juncker, presidente della Commissione europea (ansa)

Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity priorità dell'agenda e propone un'Agenzia europea per la sicurezza

di ARTURO DI CORINTO

Priorità:

1. Agenda commerciale
2. Competitività
3. Clima
4. Cybersecurity
5. Immigrazione

Ue, Jean-Claude Juncker: "L'Europa non è pronta contro i cyberattacchi"

Jean-Claude Juncker, presidente della Commissione europea (ansa)

Nel suo discorso sullo Stato dell'Unione il presidente della Commissione europea mette la cybersecurity priorità dell'agenda e propone un'Agenzia europea per la sicurezza

di ARTURO DI CORINTO

Priorità:

1. Agenda commerciale
2. Competitività
3. Clima
4. Cybersecurity
5. Immigrazione

ITALIA SOTTO ATTACCO

(di Alessandro Rugolo) 20/11/18 - Da tempo l'Italia risulta essere nel mirino degli hacker, eppure, fino a ieri sembrava che nessuno fosse interessato. Ma questa volta è diverso.

Già da qualche giorno circolano voci su un attacco cyber che avrebbe colpito gli uffici giudiziari. Questa volta però alle voci seguono i fatti, e i fatti consistono nella **prima conferenza stampa tenuta dal professor Roberto Baldoni, vice direttore generale Cyber del Dipartimento delle informazioni per la Sicurezza**.

Questa volta l'attacco è andato a segno e sembra che siano in tanti ad essere preoccupati.

Difesa Online è invitata alla conferenza stampa, come le principali testate giornalistiche. Ci si trova tutti assieme ad aspettare l'arrivo del professor Baldoni, in una sala piccola ma splendida, con il soffitto completamente affrescato, di Palazzo Verospi in via dell'Impresa a Roma.

Perché occuparsene

- L’informatizzazione della società e la digitalizzazione di beni, merci e servizi, pubblici e privati, ci obbliga ad avere una grande attenzione verso la sicurezza degli asset informatici.

Perché occuparsene

Infrastrutture Critiche

Cybersecurity e infrastrutture critiche

- In un mondo sempre più digitalizzato gli attacchi informatici che suscitano allarme nella popolazione e causano danni ingenti all'economia mettono in pericolo la stessa incolumità dei cittadini quando colpiscono le reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti; cioè le infrastrutture critiche delle società moderne.

U.S. Critical Infrastructure Full of Security Holes

By Ann R. Thryft 06.04.2020 0

Share Post Share on Facebook Share on Twitter in

The coronavirus pandemic has spawned a huge increase in cyberthreats and attacks. While much of this is aimed at consumers, a lot has also targeted companies whose employees must now access critical infrastructure, such as industrial control systems (ICS) and operational technology (OT) networks, from home.

But that critical infrastructure, which keeps modern society going even during a pandemic, is seriously under-protected against cyberattacks, say recent reports from cybersecurity companies.

New: Security researchers say Triton, a powerful malware that once tried to blow up a Saudi chemical plant, has been found in a second facility.

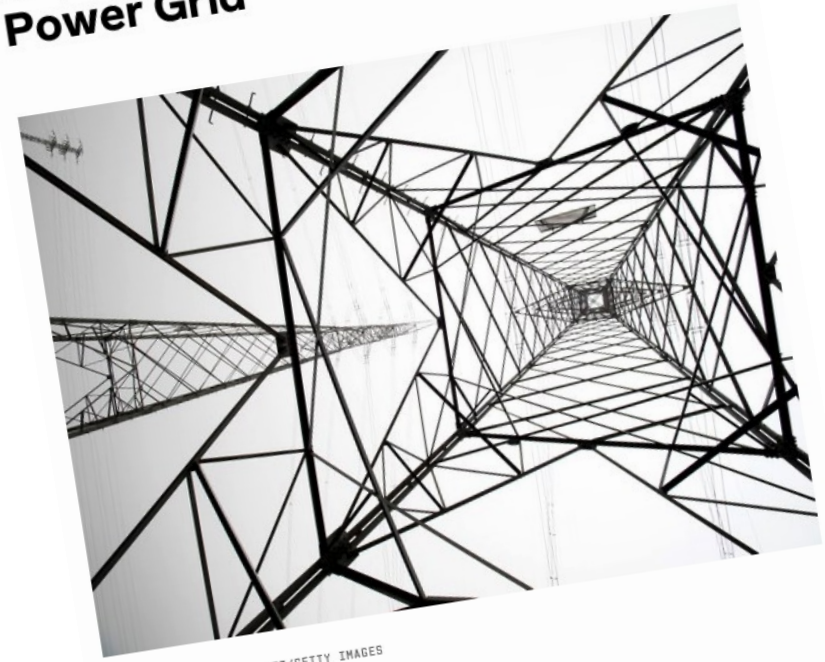
A powerful malware that tried to blow up a Saudi plant strikes again

A highly capable malware reportedly used in a failed plot to blow up a Saudi petrochemical plant has now been linked to a second compromised facility. FireEy...

techcrunch.com

2015, Dec. 23rd

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their

HACKING | Di Joseph Cox | gen 12 2016, 10:18am

La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.

Johannesburg residents left in the dark after a ransomware attack at City Power

July 26, 2019 By Pierluigi Paganini

South African electric utility City Power that provides energy to the city of Johannesburg, has suffered serious disruptions after a ransomware attack.

A ransomware infected systems at City Power, an electricity provider in the city of Johannesburg, South Africa, and some residents were left without power.

The energy utility informed its customers via Twitter of the ransomware attack that encrypted its network, including all its databases and applications.

Hackers targeted ICS/SCADA systems at water facilities, Israeli government warns

April 27, 2020 By Pierluigi Paganini

The Israeli authorities are alerting organizations in the water industry following a series of cyberattacks that hit water facilities in the country.

The Israeli government has issued an alert to organizations in the water sector following a series of cyberattacks that targeted the water facilities.

Perché occuparsene

Infrastrutture Critiche

Imprese

Cybersecurity e imprese

- Un attacco informatico di successo potrebbe anche rappresentare un momento di non ritorno per la credibilità di un’azienda, lo sviluppo del suo business, la capacità di vendere prodotti utili in un regime di sana concorrenza.

Average Enterprise Is Hit by a Cyber Attack Every 1.5 Seconds

Stu Sjouwerman

FireEye released its yearly Advanced Threat Report, and they did some interesting math. Enterprises are hit by cyber attacks on average once every 1.5 seconds, which is double from the year before, which was once every three seconds for an attack of some kind.

In the first six months, Java was the most common attack vector for hackers, but FireEye observed a surge in watering hole attacks using IE zero-days in the second half of the year.

Perché occuparsene

Infrastrutture Critiche

Imprese

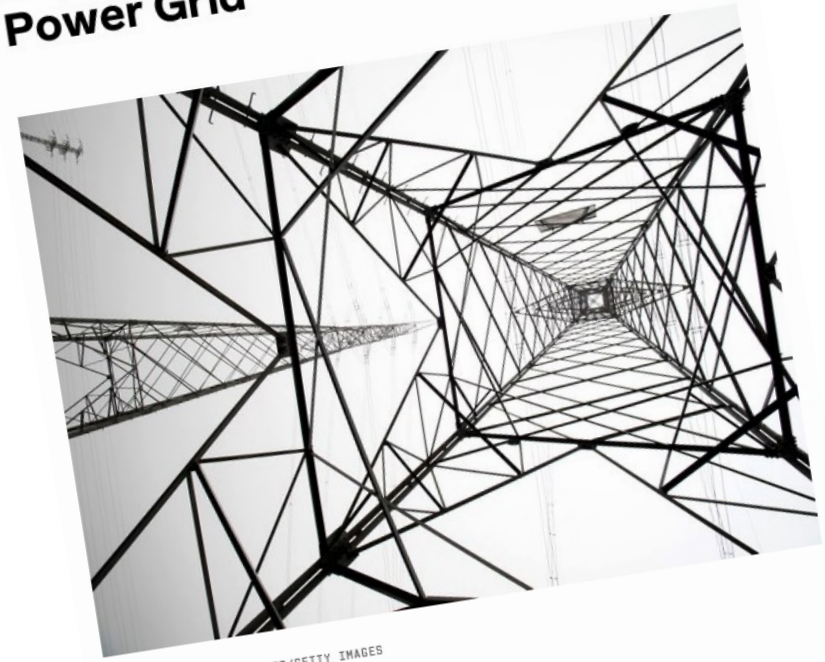
Sistema Paese

Cybersecurity e Sistema Paese

- Un attacco informatico riuscito potrebbe destabilizzare il mercato azionario e sprofondare interi paesi nel caos, oppure bloccare i rifornimenti di gas in inverno o il ciclo dei rifiuti urbani: che scenario politico ne conseguirebbe?

23 dic 2015

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their

HACKING | Di Joseph Cox | gen 12 2016, 10:18am

La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.

Perché occuparsene

Infrastrutture Critiche

Imprese

Sistema Paese

Diritti

Cybersecurity e Diritti

- La sicurezza informatica oggi coincide con la sicurezza dei dati e delle informazioni che ci definiscono come cittadini, elettori, lavoratori, consumatori.
- Se la sicurezza di dati e informazioni viene meno, a risentirne è la nostra privacy, che è la precondizione per esercitare il diritto d'opinione, d'espressione, di cronaca, d'associazione, di movimento, d'impresa, alla proprietà.

I campi della Cybersecurity

- La Cybersecurity sta diventando un elemento importante nella vita quotidiana
- Tuttavia, le conoscenze fondamentali su cui si sta sviluppando sono frammentate e, di conseguenza, può essere difficile orientarsi.

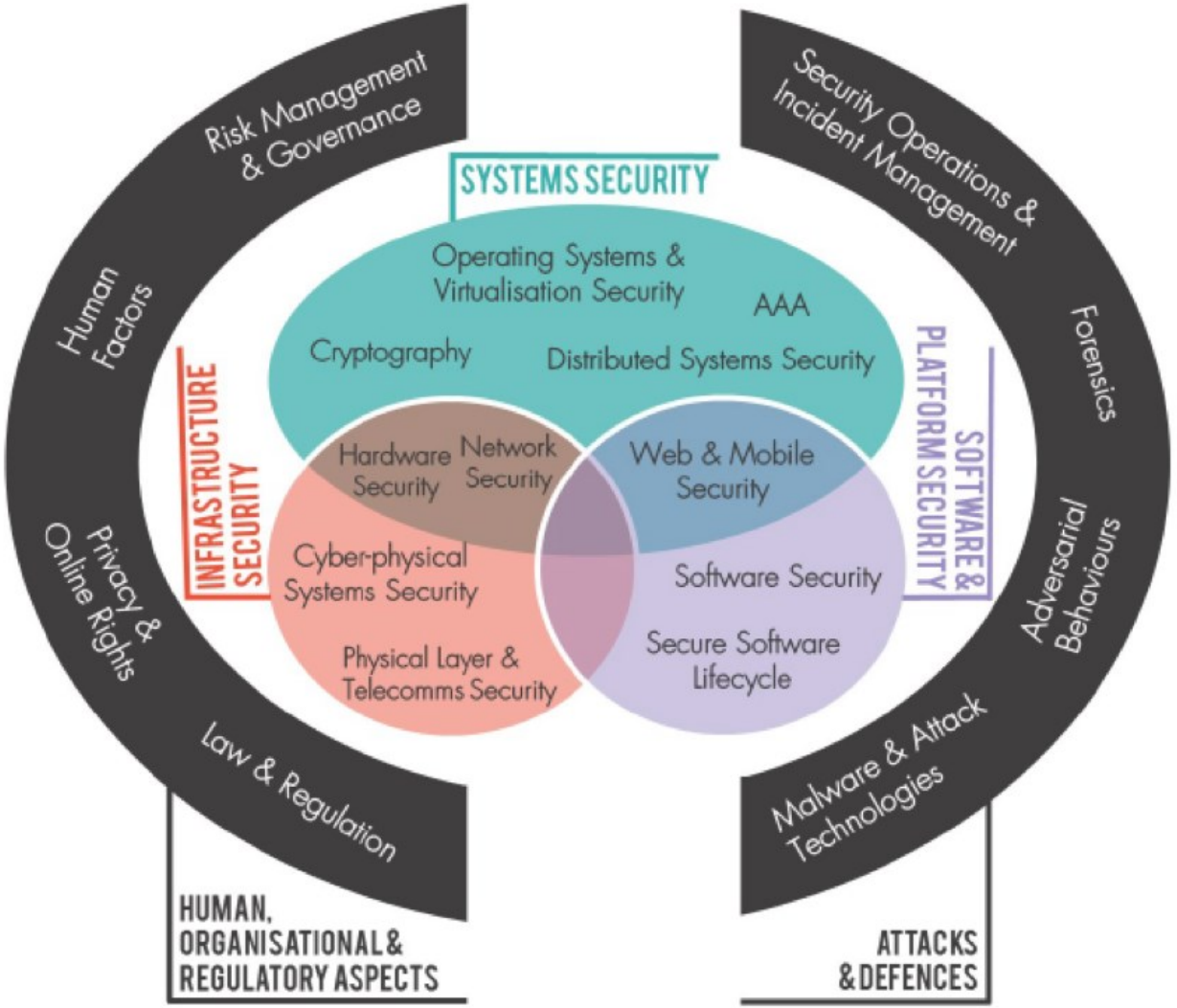
The Cyber Security Body of Knowledge (CyBOK)

- CyBOK Version 1.0 © Crown Copyright, The National Cyber Security Centre 2019
- Rilasciato con Open Government Licence: https://www.nationalarchives.gov.uk/doc/open-government-licence/

The Cyber Security Body of Knowledge (CyBOK)

- Il CyBOK è suddiviso in 19 aree di conoscenza di alto livello (Knowledge Areas), raggruppate in 5 categorie:
  - *Human, Organisational, and Regulatory Aspects*
  - *Attacks and Defences*
  - *Systems Security*
  - *Software and Platform Security*
  - *Infrastructure Security*

CyBOK: categorie



Glossario relativo alla Cybersecurity

- https://csrc.nist.gov/Glossary

Lettura consigliata

Indice

- Introduzione
- Dependability
- Safety
- Security
- Cybersecurity
  - sua rilevanza
- Conclusioni

Safety vs Security

- Le varie dimensioni della dependability possono avere requisiti contrastanti...

Apertura automatica delle porte

Requisity di Safety

Le porte si devono aprire quando una vettura si capovolge.

Apertura automatica delle porte

Requisity di Safety

Le porte si devono sbloccare quando una vettura si capovolge.

Soluzione

Installare dei sensori di pressione sul tetto della vettura.

Apertura automatica delle porte

Requisity di Safety

Le porte si devono sbloccare quando una vettura si capovolge.

Soluzione

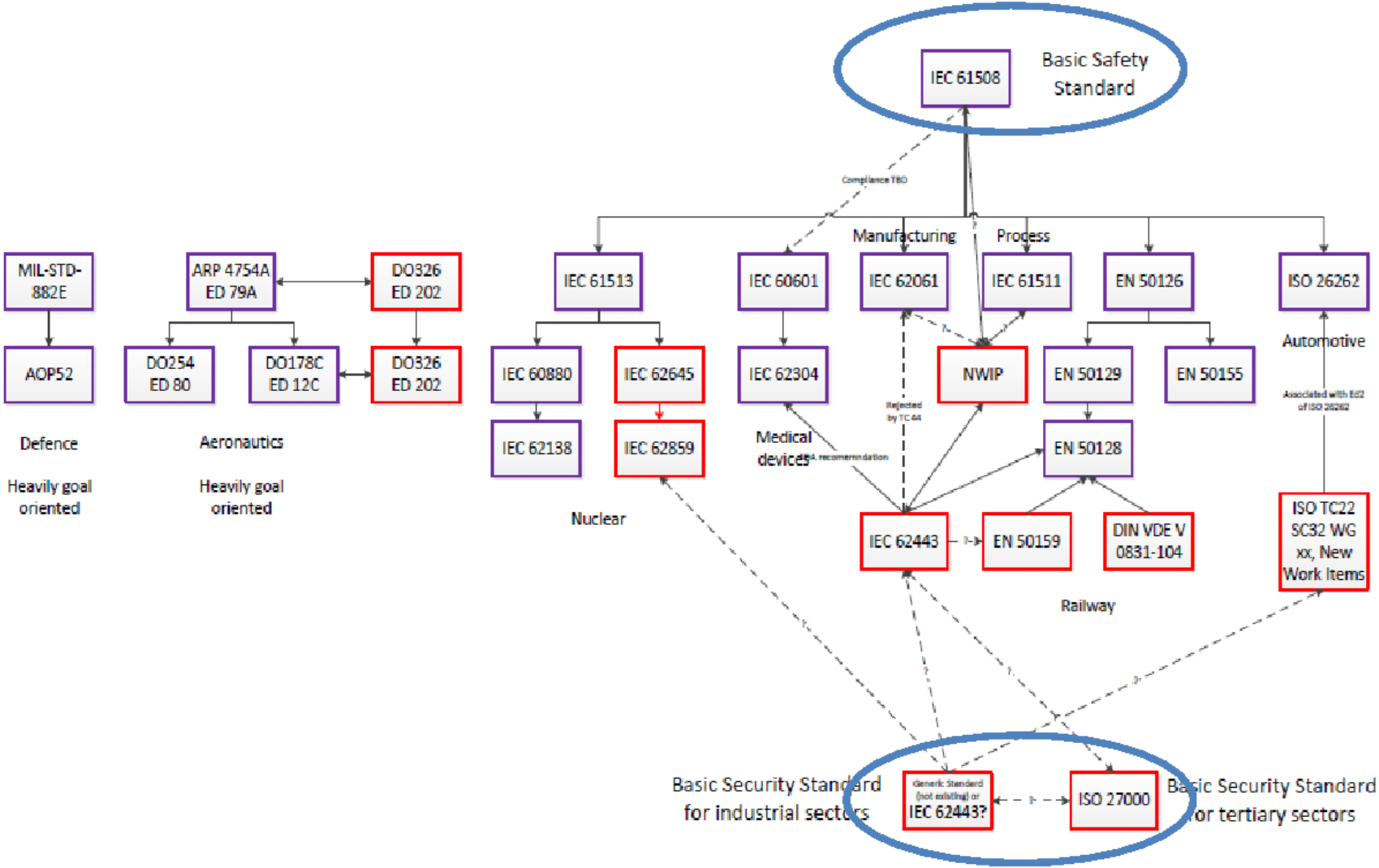
Installare dei sensori di pressione sul tetto della vettura.

Questa soluzione ha gravi conseguenze sulla sicurezza

Ingresso non autorizzato saltando sul tetto della vettura.

Il ruolo degli Standard

- Ciononostante, si è raggiunta una significativa convergenza dei vari standard...


IEC 61508
Basic Safety Standard
Compliance TBD
MIL-STD-882E
ARP 4754A ED 79A
DO326 ED 202
AOP52
DO254 ED 80
DO178C ED 12C
DO326 ED 202
Defence
Heavily goal oriented
Aeronautics
Heavily goal oriented
Manufacturing
Process
IEC 61513
IEC 60601
IEC 62061
IEC 61511
EN 50126
ISO 26262
Automotive
IEC 60880
IEC 62645
IEC 62304
NWIP
EN 50129
EN 50155
Rejected by TC 44
Associated with Ed2 of ISO 26262
IEC 62138
IEC 62859
Medical devices
EN 50128
Nuclear
IEC 62443
EN 50159
DIN VDE V 0831-104
ISO TC22 SC32 WG xx, New Work Items
Railway
Basic Security Standard for industrial sectors
Generic Standard (not existing) or IEC 62443?
ISO 27000
Basic Security Standard for tertiary sectors