Progetti e azioni per difenderci al meglio da attacchi cyber

Rocco
DE NICOLA
Scuola IMT – LUCCA
Direttore C3T - Centro di Competenza Cyber-security Toscano

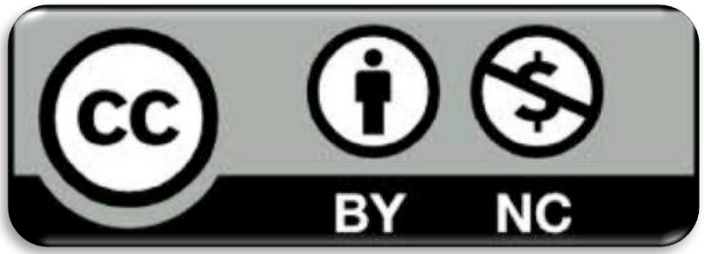
Confindustria Firenze
9 Aprile 2019

cini Cybersecurity National Lab

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

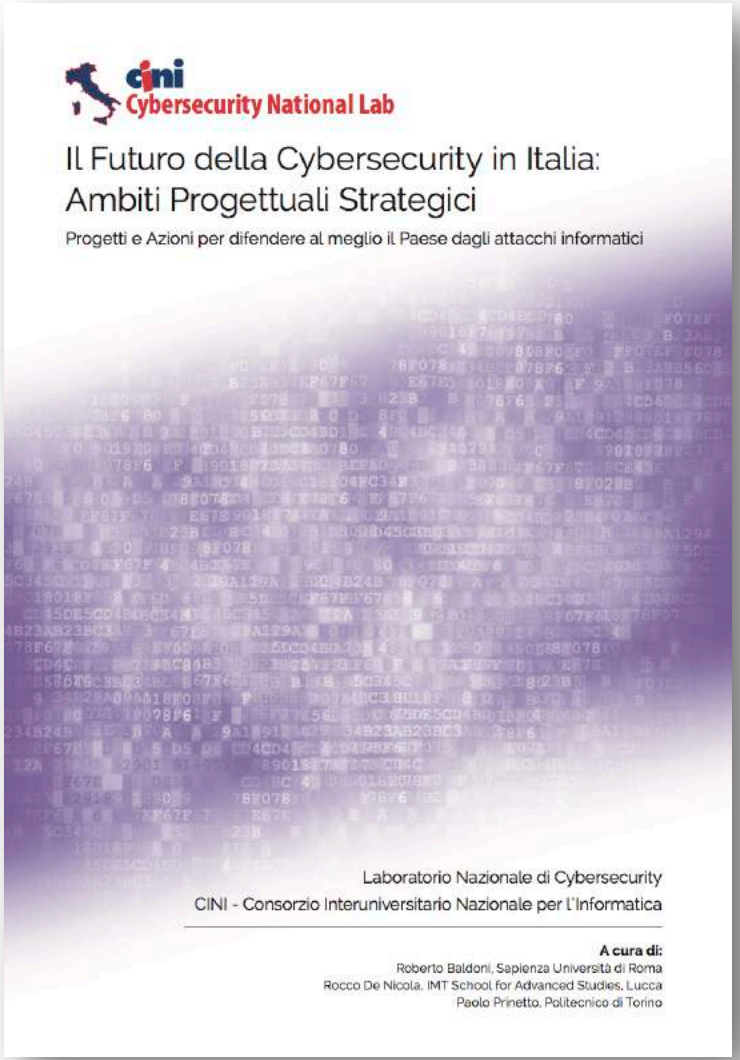


To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.



Roberto BALDONI
Rocco DE NICOLA
Paolo PRINETTO

cini
Cybersecurity
National Lab

cini
consorzio
interuniversitario
nazionale
per l'informatica

www.consorzio-cini.it

Cyberspace

- Quel complesso ecosistema 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]

- 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*"

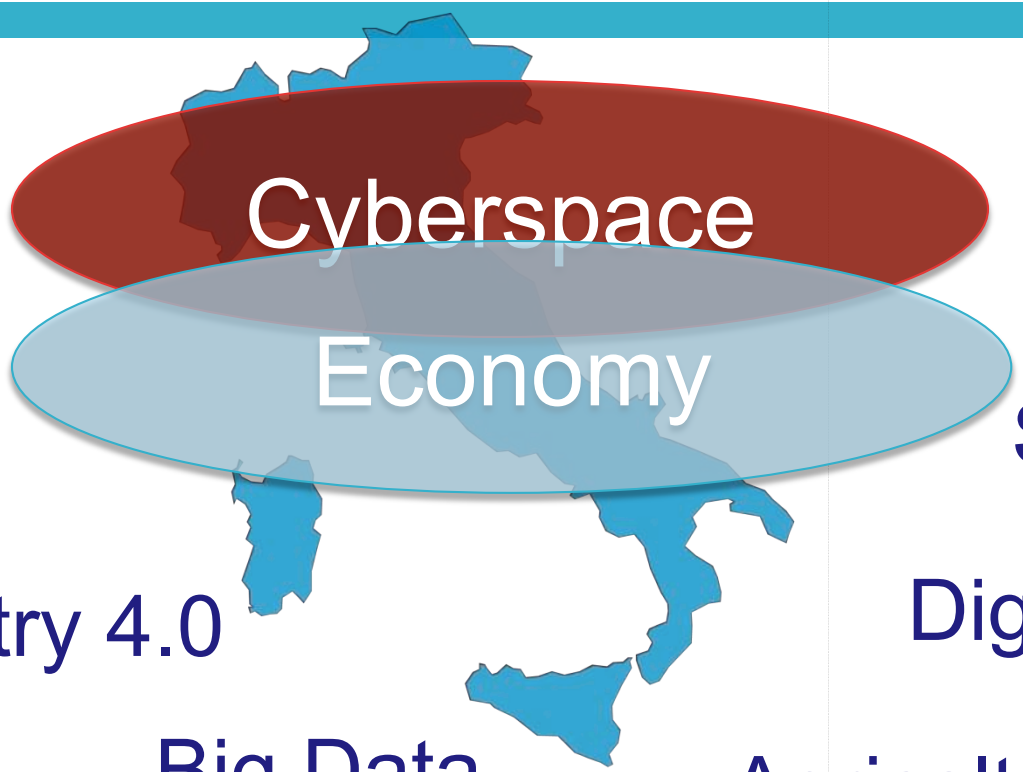
Cybersecurity

- Quella 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 arrivano dal cyberspace

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

- Protezione di **informazioni**
  - Memorizzate in un computer
  - Trasmesse su una rete
- Protezione di **Sistemi e Risorse**
  - Hardware – software - firmware
  - telecomunicazioni

Il cyberspace è pervasivo



IoT

Robotics

Drones

Smart Cities

Industry 4.0

Digital Currencies

Big Data

Agricolture 4.0

R.it | Sicurezza

Home | News | Speciali | Mobile | Social Network | Sicurezza | Prodotti | Interattivi | Video

102

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

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

"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".

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.

Sicurezza

Safety

- Protezione della persona

Security

- Protezione del cyberspazio

Vulnerabilità

- La complessità del cyberspazio genera *vulnerabilità* a causa di:
  - Errori nei programmi
  - errori di progettazione dell'hardware
  - errate configurazioni
  - debolezze dei protocolli di comunicazione usati
  - …

Attacchi nel Cyberspace

- Le *vulnerabilità dei sistemi* e *delle persone* (*fattore umano*) sono sfruttati dai cyber-criminali per sferrare *attacchi*
  - esfiltrare dati
  - rubare soldi
  - arrecare danni
  - controllare in modo surrettizio
    - strutture,
    - servizi
    - intere nazioni
  - …

Le aziende tradizionali

- Il principio guida era la protezione (anche fisica) del perimetro della organizzazione
- Un perimetro sicuro garantiva la sicurezza dell'intera organizzazione
- IT e OT erano mondi del tutto separati

Le aziende in Industry 4.0

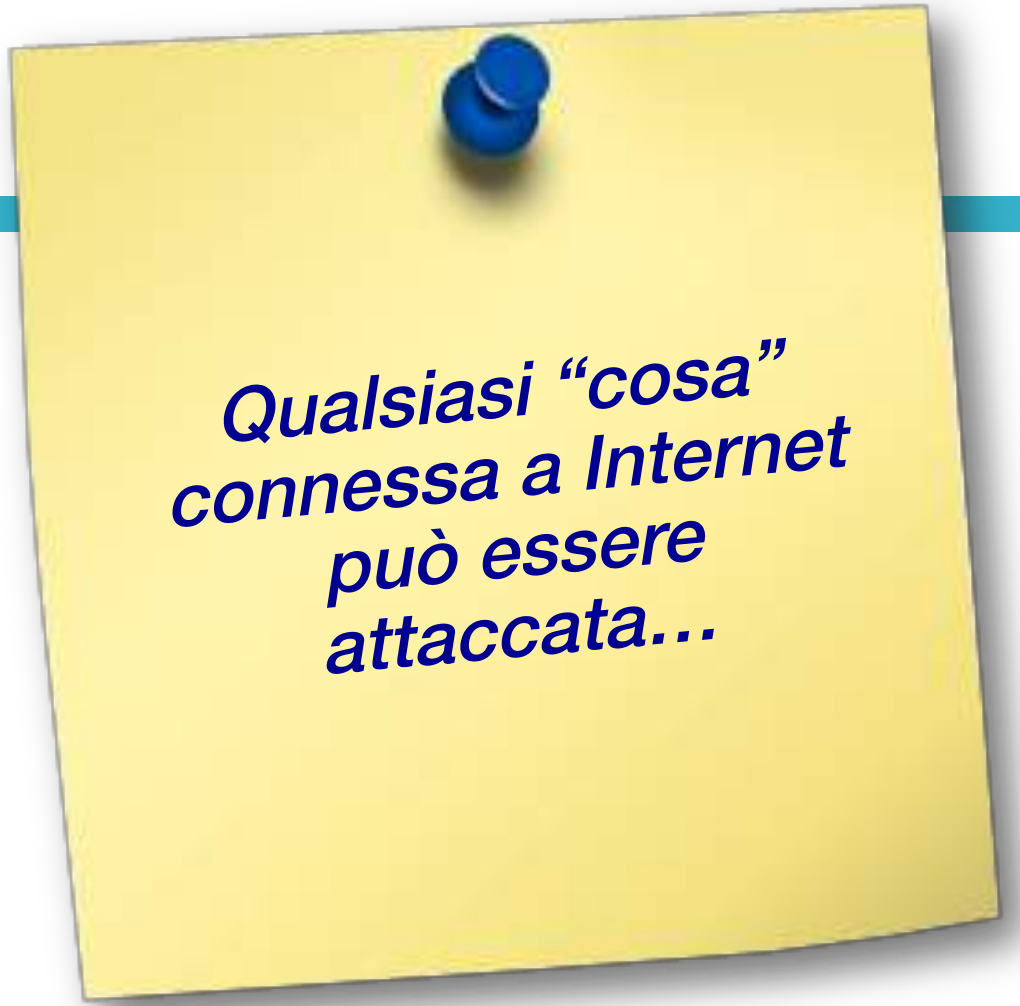
- Internet ha cambiato le aziende
- I processi di business si estendono oltre le “mura” aziendali
- Coincidenza di IT e OT

Le aziende in Industry 4.0

- Internet ha cambiato le aziende
- I processi di business si estendono oltre le "mura" aziendali

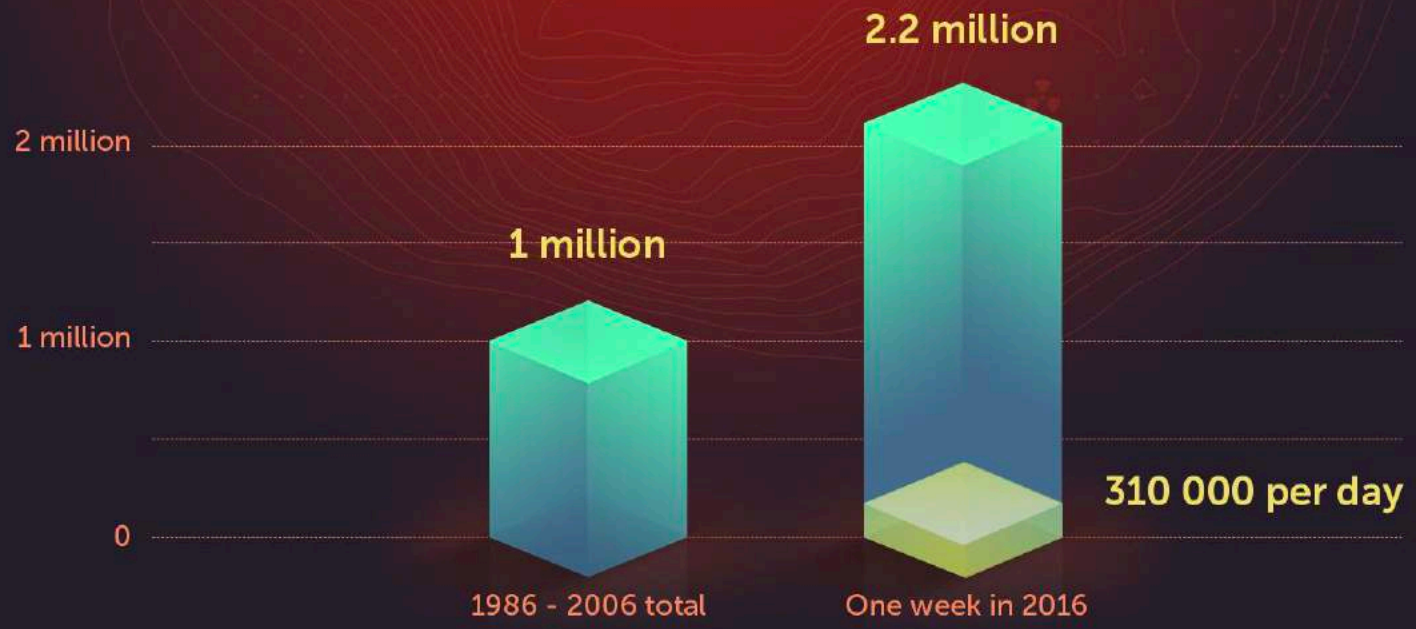
- Reti aziendali aperte a clienti, fornitori e partner
- Processi di business basati su reti pubbliche
- Web utilizzato per vendere e acquistare (B2B, B2C)
- Dati e applicazioni sul cloud
- Accesso remoto dei collaboratori

Caveat



CYBERTHREAT LANDSCAPE

Malware explosion *



* Kaspersky Lab database

Tutto è sotto attacco

[E. Kaspersky, 2018]

… sempre …

http://map.norsecorp.com/#/

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.

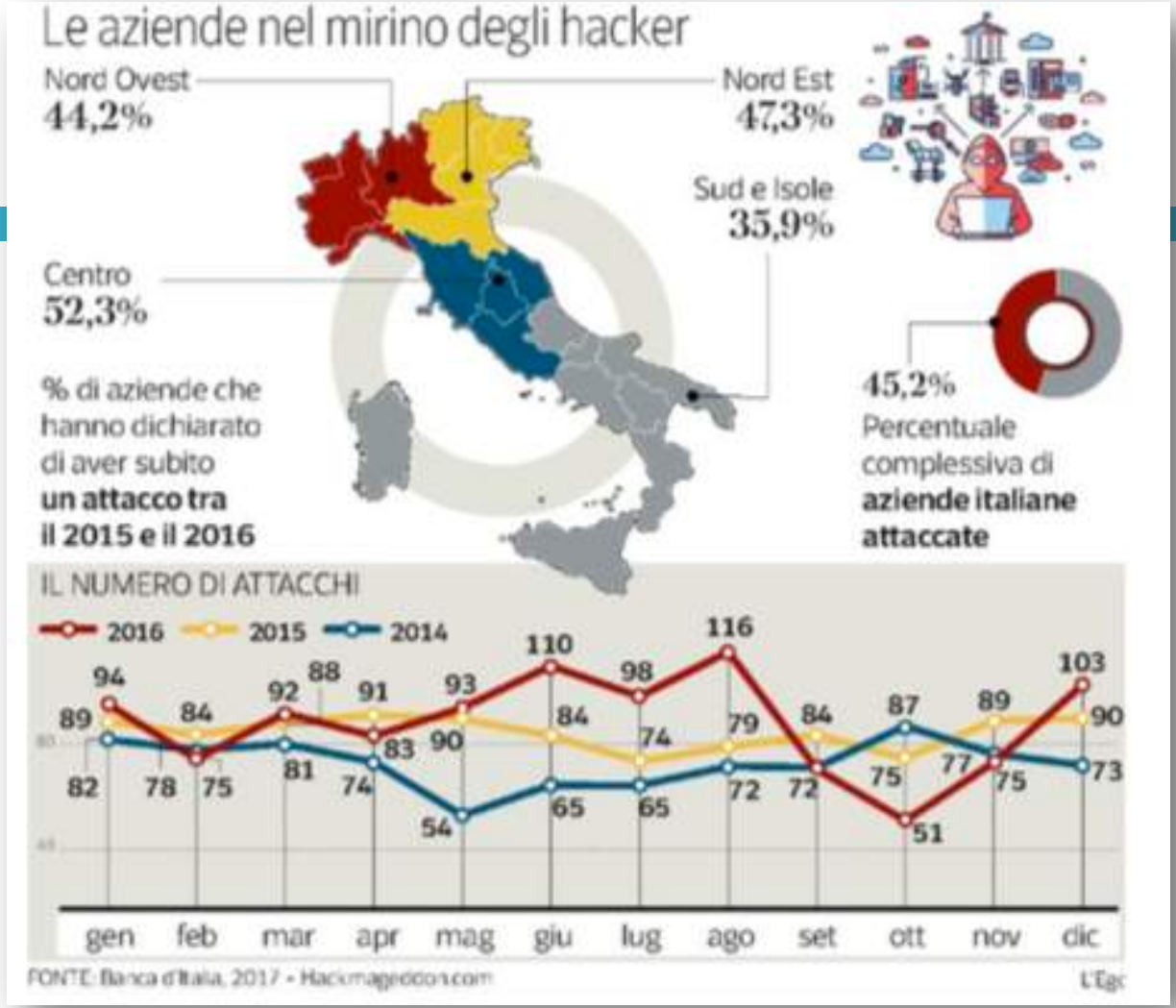
In the first six months, Java was the most common attack vector for hackers, but FireEye observed a surge in watering hole attacks using IE zero-days in the second half of the year.

Status

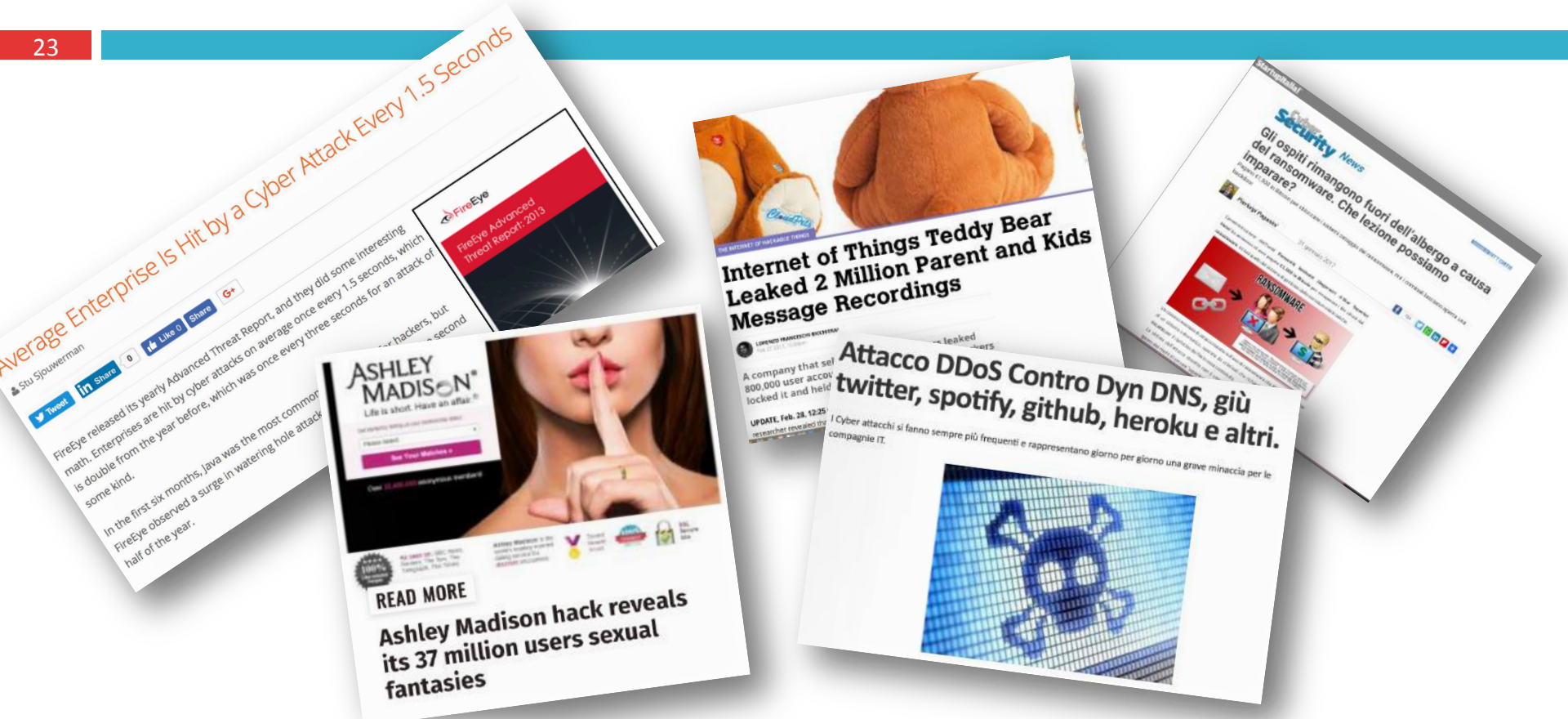
[Claudia Biancotti: "The price of cyber (in)security: evidence from the Italian private sector". *Questioni di Economia e Finanza 407*, Banca d'Italia, Dicembre 2017]

Tabella 1.1: Attacchi subiti da imprese italiane, settembre 2015–2016

Area geografica	
Nord Ovest	44.2
Nord Est	47,3
Centro	52,3
Sud e Isole	35,9
Numero di addetti	
20 – 49	42,7
50 – 199	48,4
200 – 499	56,0
500 e oltre	62,8
Intensità tecnologica	
Alta e medio-alta	48,8
Bassa e medio-bassa	43,8
Incidenza delle esportazioni sul fatturato	
Meno di 1/3	43,0
Tra 1/3 e 2/3	51,8
Più di 2/3	48,5
Percentuale sul totale delle aziende	**45,2**


Le aziende nel mirino degli hacker
Nord Ovest
44,2%
Nord Est
47,3%
Sud e Isole
35,9%
Centro
52,3%
% di aziende che hanno dichiarato di aver subito un attacco tra il 2015 e il 2016
45,2%
Percentuale complessiva di aziende italiane attaccate
IL NUMERO DI ATTACCHI
2016
2015
2014
94 84 92 88 91 93 110 98 116 79 84 87 89 90
89 82 78 75 81 74 83 90 54 84 65 65 74 72 72 75 77 75 73
103
51
gen feb mar apr mag giu lug ago set ott nov dic
FONTE: Banca d'Italia, 2017 - Hackmageddon.com

Alcuni esempi



SICUREZZA INFORMATICA

Hacker rubano 36 milioni di euro sui conti di 30 banche europee via sms

Colpiti anche clienti italiani. L'attacco attraverso un trojan dormiente sui Pc che si è trasferito sugli smartphone

(Foto web)

Oltre 36 milioni di euro, sui conti di 30 banche europee. Una cifra da capogiro. Rubata da un gruppo di hacker anche di clienti italiani. A darne notizia è stato il Financial Times nell'edizione online, rilevando che si tratterebbe del primo caso di furto che ha preso specificatamente di mira le procedure di sicurezza sui servizi

E se i prossimi attacchi informatici colpissero i satelliti artificiali?

Alla Cybertech Europe di Roma, l'italiana Leonardo ha presentato insieme all'ESA nuove soluzioni per impedire che le reti spaziali di comunicazione e geolocalizzazione non cadano in mano dei cybercriminali

LEGGI ANCHE

Una falla nel protocollo di rete mette a rischio la sicurezza delle auto

MARCO TONELLI

R.it Cronaca

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

Lo leggo dopo | 30 settembre 2017

Gianfranco Dell'Alba

ROMA - Ci sono circa cinquecentomila euro che da un conto della Confindustria sono finiti in un conto estero di cui ancora non si conosce l'intestatario. Soldi evaporati, per ora. C'è una mail falsa da cui è cominciato tutto. C'è un dirigente dell'associazione degli industriali licenziato in tronco per un bonifico che non avrebbe dovuto fare. È successo in Confindustria ma sono centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail contraffatte (mail spoofing, le chiamano gli esperti del settore) da cui partono ordini per spostare denaro in ogni parte del mondo.

Hacker truffa con una mail falsa un dirigente di Confindustria: spariti 500mila euro

"Sposta subito mezzo milione su questo conto estero". Il finto ordine a firma della direttrice Marcella Panucci, ad eseguire il bonifico il dirigente livornese Gianfranco Dell'Alba

TRUFFE CONFINDUSTRIA HACKER

30 settembre 2017

Finding ways into a car's network

1 GAINING ACCESS

The first step requires gaining access to an electronic control unit that is in contact with an outside network. Some examples of these "attack surfaces" include:

Bluetooth
This technology is commonly used to pair phones and is nearly ubiquitous in modern cars.

Radio data system
Some radios need to process data to, for example, display the name of a song. This presents a vulnerabilty, as malignant code can be introduced.

Cellular and WiFi
Many cars are connected to cellular networks, and some are connected to the internet.

2 TAKING CONTROL

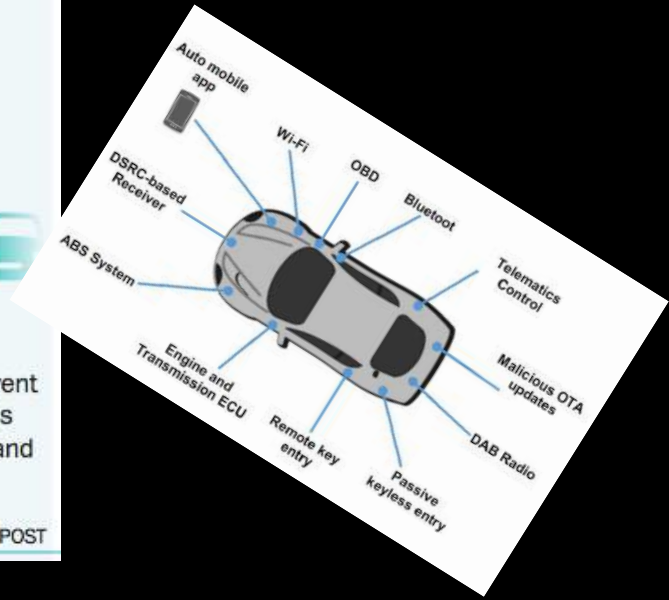
Once attackers find a way in, they can manipulate some safety-critical features:

Adaptive cruise control
A computer slows or speeds up the car depending on road conditions. These adjustments happen when the car is moving at high speeds.

Collision prevention
This system uses the car's sensors to engage the brakes when it senses a crash is imminent.

Lane-keep assist
Uses the car's sensors to prevent it from leaving its lane. It sends signals to the steering wheel and brakes.

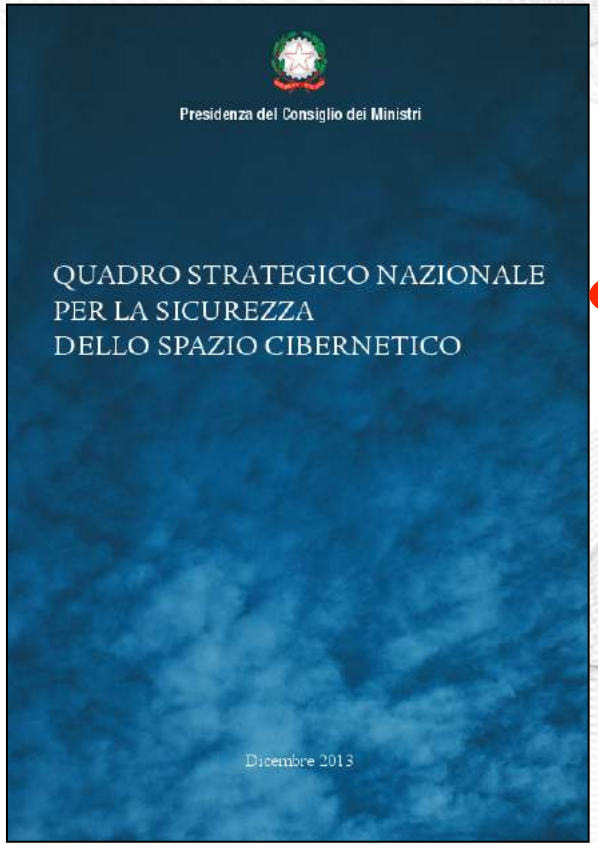
Source: "A Survey of Remote Automotive Attack Surfaces" LAZARO GAMIO, RICHARD JOHNSON AND DAWN CAI/THE WASHINGTON POST



Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc);
- *Cyber-espionage* (acquisizione indebita dati);
- *Cyber-terrorism* (con connotazione ideologica);
- *Cyber-warfare* (pianificazione e conduzione operazioni).

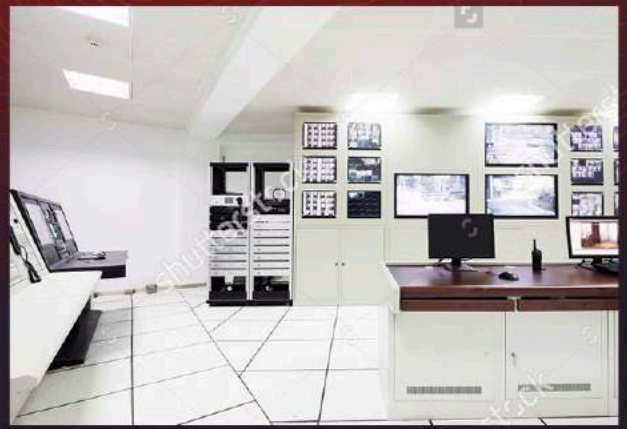


Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc);
- *Cyber-espionage* (acquisizione indebita dati);
- *Cyber-terrorism* (con connotazione ideologica);
- *Cyber-warfare* (pianificazione e conduzione operazioni).

TRADITIONAL AND ONLINE CRIME GROUPS ARE NOW WORKING TOGETHER



Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc);
- *Cyber-espionage* (acquisizione indebita dati);
- *Cyber-terrorism* (con connotazione ideologica);
- *Cyber-warfare* (pianificazione e conduzione operazioni).

ANALISI DELLA MINACCIA

ANALISI DELLA MINACCIA

Liaoning CV 16

USS TRUMAN

Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc);
- *Cyber-espionage* (acquisizione indebita dati);
- *Cyber-terrorism* (con connotazione ideologica);
- *Cyber-warfare* (pianificazione e conduzione operazioni).

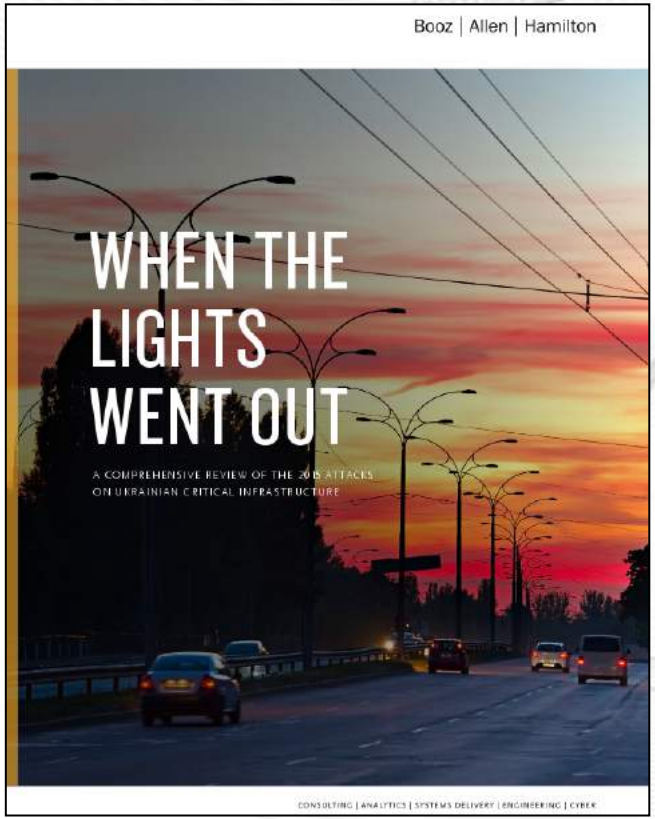

Estonia
Latvija
Latvia
Lietuva
Беларусь
Belarus
Україна
Ukraine
Moldova
România
Romania
Србија
Serbia
България
Bulgaria
France
España
Spain
Portugal
Ελλάς
Greece

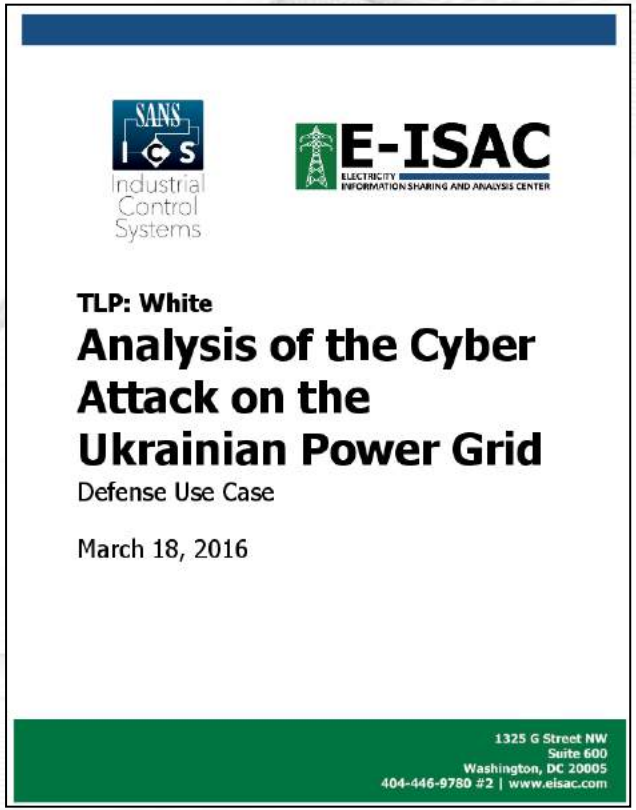
Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc);
- *Cyber-espionage* (acquisizione indebita dati);
- *Cyber-terrorism* (con connotazione ideologica);
- *Cyber-warfare* (pianificazione e conduzione operazioni).

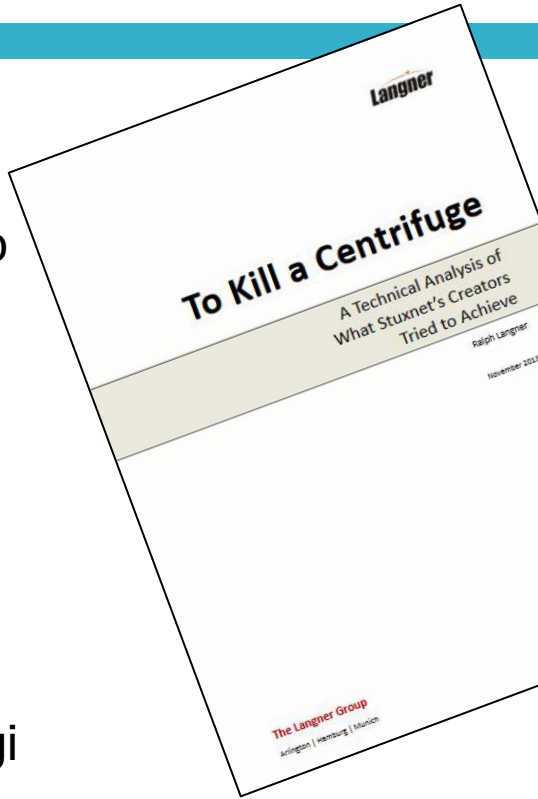
ANALISI DELLA MINACCIA



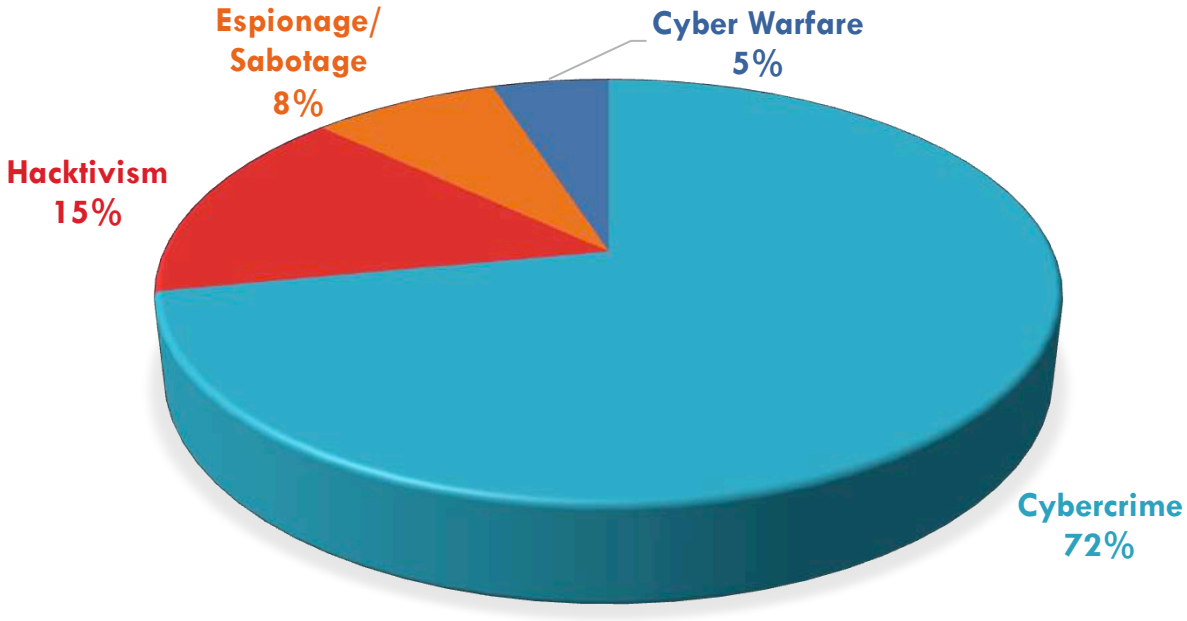


Stuxnet: un attacco fisico

- A giugno 2012 viene anticipato che il presidente Obama ha ordinato un cyber-attacco contro l'Iran.
- L'attacco è stato condotto con il worm Stuxnet che è passato da un sistema Windows ai controllori SCADA (*Supervisory Control And Data Acquisition*) utilizzati per il monitoraggio elettronico di una centrale nucleare iraniana.
- Il worm ha cambiato la velocità dei rotori in una centrifuga della centrale iraniana utilizzata per arricchire l'uranio.
- La compromissione è stato possibile grazie ad attività di ingegneria sociale e ad altre tecniche (mentre il rotore si riscaldava il "virus" mandava alla centrale operativa messaggi che confermavano che era tutto ok).



Tipologie di minacce



Costi

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GU

Cybercrime costs the global economy $450 billion

Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

CNBC

Costi

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GU

Cybercrime costs the global economy $450 billion

Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

CNBC

PIL dell'Austria nel 2017
434 miliardi di $

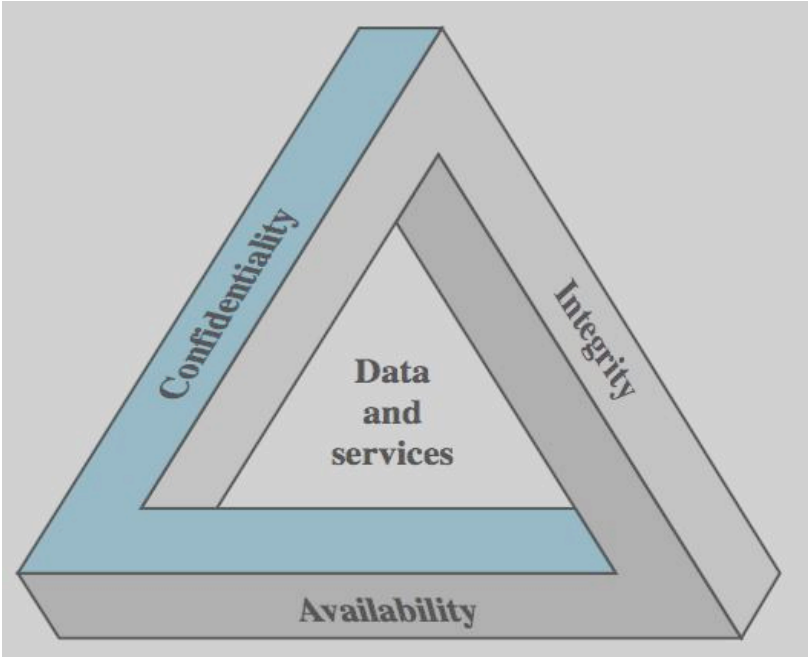
Pizzeria Google

La triade - CIA

- *Confidentiality, Integrity, Availability* formano quella che in gergo viene chiamata la triade CIA

- Riassumono gli obiettivi di sicurezza fondamentali per la protezione di informazioni, computer e reti

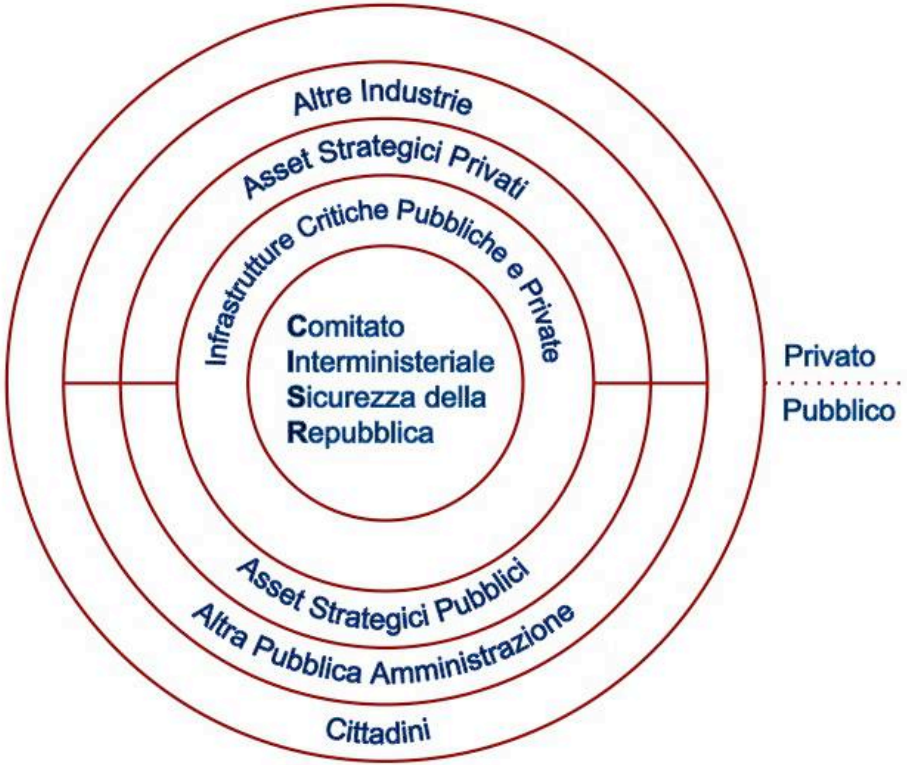
- Altri Obiettivi:
  - Authenticity
  - Accountability



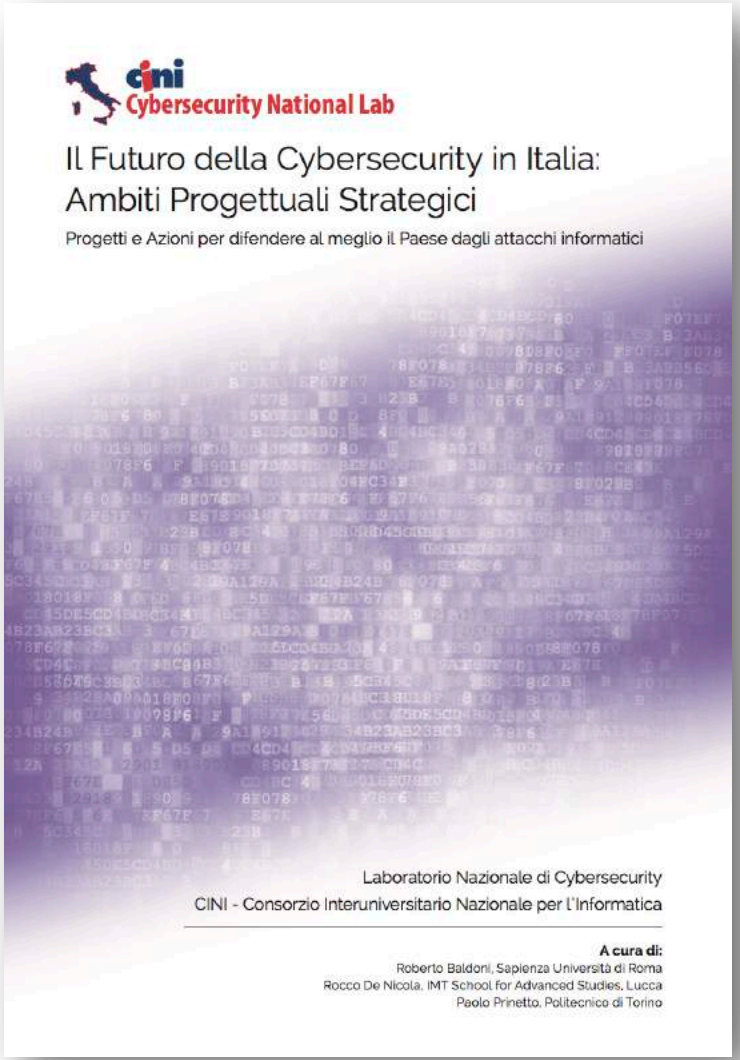
Che fare?

- Sviluppare una buona *difesa*
- A livello:
  - personale
  - nazionale
  - transnazionale

Organizzare la difesa



- Organizzare la difesa tramite:
  - Condivisione delle informazioni
  - Riduzione dei tempi di transito
  - Velocità di risposta
  - Gestione della risposta ai livelli appropriati



Roberto BALDONI
Rocco DE NICOLA
Paolo PRINETTO

cini
Cybersecurity
National Lab

cini
consorzio
interuniversitario
nazionale
per l'informatica

www.consorzio-cini.it

Outline

- Scenari
- Ambiti progettuali e Azioni
- Raccomandazioni

Struttura

1. Ruolo e impatto della cybersecurity
2. Ambiti progettuali
3. Impatto sugli assi portanti
4. Iniziative all'estero
5. Raccomandazioni

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Internet Nazionale*
- *Rete Nazionale di Data Center*
- *Rete di Centri di Competenza*

Rete di Centri di Competenza

La difesa contro gli attacchi cyber richiede la realizzazione di un complesso mosaico - l'eco-sistema cyber nazionale - che deve coinvolgere diversi soggetti e attori coordinati tramite una politica nazionale cyber.

Organizzati a diversi livelli

- *Nazionale*
- *Territoriale*
- *Verticale*

In evidenza: le strutture

Centro Nazionale

per Ricerca e Sviluppo in Cybersecurity

- Struttura centralizzata, multi-disciplinare, con adeguata massa critica senza scopo commerciale
- Assiste il Governo in analisi, ricerca, progettazione e scouting tecnologico
- Coinvolge ricercatori e investitori pubblici e privati (nazionali)
- Coopera con centri di eccellenza sparsi sul territorio nazionale

In evidenza: le strutture

Centro Nazionale

per Ricerca e Sviluppo in Cybersecurity

- Struttura centralizzata, multi-disciplinare, con adeguata massa critica senza scopo commerciale
- Assiste Governo per analisi, ricerca, progettazione e scouting tecnologico
- Coinvolge ricercatori e investitori pubblici e privati (nazionali)
- Coopera con centri di eccellenza sparsi sul territorio nazionale

Centri Territoriali

di Competenza in Cybersecurity

- Servizi e Consulenza alle imprese per protezione di asset fisici e virtuali
- Gestione di osservatori locali per condividere informazioni sugli attacchi
- Supporto a gestori di infrastrutture, imprese e PA locali per certificazioni
- Progetti di ricerca e trasferimento tecnologico di interesse strategico
- Attività di formazione permanente per imprese, PA locali e cittadini

In evidenza: le strutture

Centri Verticali

di Competenza in Cybersecurity

- Nascono dalla necessità di alcuni settori specifici (energia, trasporti, sanità, finanza, etc.), di disporre di centri ad hoc per lo sviluppo di attività dedicate:
  - CERT e contrasto al cybercrime
  - Cyber Range
  - Centri di ricerca
  - Laboratori di certificazione
- Istituiti da stakeholder pubblici, privati o da iniziative pubblico-privato
- Servono a proteggere filiere produttive nazionali e/o specifici distretti industriali
- Richiedono chiarezza di obiettivi per evitare sovrapposizioni e sprechi di risorse

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Sicurezza di applicazioni e servizi*
- *Analisi dei malware e banca dati nazionale delle minacce*
- *Anticipare la risposta ad attacchi cibernetici, sociali e fisici*
- *Analisi forense*
- *Gestione del rischio sistemico*
- *Difesa attiva*

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Sicurezza di applicazioni e servizi*
- *Analisi dei malware e banca dati nazionale delle minacce*
- *Anticipare la risposta ad attacchi cibernetici, sociali e fisici*
- *Analisi forense*
- *Gestione del rischio sistemico*
- *Difesa attiva*

In evidenza: l'anello debole

Attacchi

- Fake News: L'uomo viene attaccato tramite la rete, si sfrutta la pervasività, la velocità della rete e … l'ignoranza degli utenti
- Social Engineering: le strutture in rete vengono attaccate usando l'uomo per acquisire informazioni utili allo scopo

In evidenza: l'anello debole

Attacchi

- Fake News: L'uomo viene attaccato tramite la rete, si sfrutta la pervasività, la velocità della rete e … l'ignoranza degli utenti
- Social Engineering: le strutture in rete vengono attaccate usando l'uomo per acquisire informazioni utili allo scopo

Difese

- Cultura e Spirito Critico: Non esistono *pallottole d'argento*: serve dubitare, chiedersi a chi serve, cercare le fonti, …
- Conoscenza Tecnologica: Bisogna essere coscienti dei pericoli a cui si è esposti e ai quali si può esporre altri: servono

  cyber-hygiene e media literacy

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Architetture Hardware*
- *Crittografia*
- *Biometria*
- *Tecnologie quantistiche*
- *Intelligenza Artificiale*
- *Blockchain e Distributed Ledger*

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Architetture Hardware*
- *Crittografia*
- *Biometria*
- *Tecnologie quantistiche*
- *Intelligenza Artificiale*
- *Blockchain e Distributed Ledger*

In evidenza: Proteggere le informazioni

Strumenti

- Crittografia per proteggere dati e garantire riservatezza; usata molto prima di Internet e ancora molto importante
- Blockchain per certificare azioni in rete in assenza di entità centrali attraverso libri mastro distribuiti:
  - può rappresentare una nuova rivoluzione

In evidenza: Proteggere le informazioni

Strumenti

- Crittografia per proteggere dati e garantire riservatezza; usata molto prima di Internet e ancora molto importante
- Blockchain per certificare azioni in rete in assenza di entità centrali attraverso libri mastro distribuiti:
  - può rappresentare una nuova rivoluzione

Rischi

- Pensare che una buona crittografia sia sufficiente a garantire sicurezza.
- Attacchi di forza bruta ai dati cifrati sfruttando le capacità computazionali dei (futuri?) computer quantistici.
- Attacchi di massa coordinati alle blockchain da potenze straniere con grandi capacità computazionali

Nuovo Strumento: Intelligenza Artificiale

Minacce

- Generazione automatica di testo per
  - fake news
  - phishing
  - false identità
- Avvelenamento dell'ambiente di apprendimento
- Induzione a dialoghi offensivi tramite chatbot

Nuovo Strumento: Intelligenza Artificiale

Minacce

- Generazione automatica di testo per
  - fake news, phishing, fake identity
- Avvelenamento dell'ambiente di apprendimento
- Induzione a dialoghi offensivi tramite chatbot

Difese

- Diffusione dei principi etici e consapevolezza dei rischi per la sicurezza derivanti dall'IA.
- Automazione della scoperta di vulnerabilità.
- Condizionamento del campo di battaglia

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Infrastrutture wireless*
- *Cloud*
- *Algoritmi*
- *Internet of Things*
- *Industrial Control Systems*
- *Robot*

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Infrastrutture wireless*
- *Cloud*
- *Algoritmi*
- *Internet of Things*
- *Industrial Control Systems*
- *Robot*

In evidenza: le “cose”

IoT

- *Internet of Things* (IoT) rappresenta le “cose” connesse in rete e in grado di comunicare tra di loro, o con altri sistemi, senza intervento umano
- L’*Impresa 4.0* dipende molto da sistemi IoT e da sistemi di controllo industriali ICS e *SCADA* connessi alla rete

In evidenza: le “cose”

IoT

- *Internet of Things* (IoT) rappresenta le “cose” connesse in rete e in grado di comunicare tra di loro, o con altri sistemi, senza intervento umano
- L’*Impresa 4.0* dipende molto da sistemi IoT e da sistemi di controllo industriali ICS e *SCADA* connessi alla rete

Rischi

- Gli IoT e i nuovi servizi hanno accresciuto a dismisura la *superficie di attacco* e introdotto nuove vulnerabilità
- I sistemi ICS e SCADA sono per lo più progettati senza considerare le vulnerabilità introdotte dalla rete

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Protezione dei dati personali e GDPR*
- *Formazione*
- *Sensibilizzazione e cyber-hygiene*
- *Gestione del rischio cyber per le imprese*
- *Certificazioni sostenibili*

2. Ambiti progettuali

- Infrastrutture e Centri
- Azioni abilitanti
- Tecnologie abilitanti
- Tecnologie da proteggere
- Azioni orizzontali

- *Protezione dei dati personali e GDPR*
- *Formazione*
- *Sensibilizzazione e cyber-hygiene*
- *Gestione del rischio cyber per le imprese*
- *Certificazioni sostenibili*

In evidenza: il capitale umano

Un recente studio di Intel ha analizzato la disponibilità di esperti di cyber-security in vari paesi

- L'82% dei partecipanti riporta una carenza di professionalità in cybersecurity all'interno della loro organizzazione.
- Il 30% ammette che la loro organizzazione è stata vittima di furti di dati e intrusioni per la mancanza di personale qualificato.

- Alta formazione — Fornire strumenti tecnici e metodologici fondamentali della cybersecurity con corsi di laurea e lauree magistrali, master universitari, programmi di dottorato

- Ricerca di talenti — Ricercare giovani talenti da indirizzare verso una carriera in cybersecurity, attraverso sfide informatiche e simulazioni in ambienti virtuali

In evidenza: il capitale umano

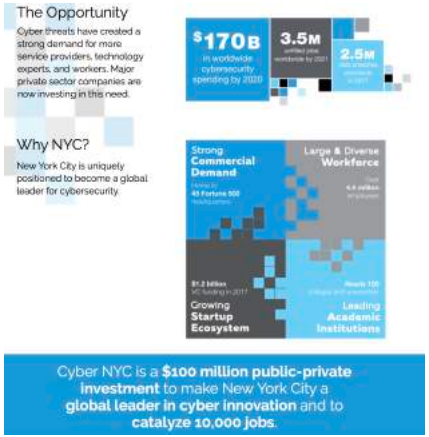
- Formazione continua — Garantire formazione professionale continua per tutte le professioni che devono affrontare problematiche di cybersecurity.
- Addestramento — Consolidare e migliorare le capacità operative degli operatori preposti al contrasto e alla gestione degli incidenti informatici
- Educazione di base — Insegnare elementi di cybersecurity in tutte le scuole, da quando i giovani iniziano a connettersi alla rete.
- Sensibilizzazione dei cittadini — Trasmettere a tutti concetti base di quella che viene ormai comunemente chiamata *cyber-hygiene*
- …..

Formazione e professionalità

Un recente studio di Intel ha analizzato la disponibilità di esperti di cyber-security in vari paesi

- L'82% dei partecipanti riporta una carenza di professionalità in cybersecurity all'interno della loro organizzazione.
- Il 30% ammette che la loro organizzazione è stata vittima di furti di dati e intrusioni per la mancanza di personale qualificato.

- 2016: prevista una carenza di due milioni di posti di lavoro entro il 2019
- 2018 prevista una carenza di tre milioni e mezzo di posti di lavoro entro il 2021



3. Impatto sugli assi portanti

- Democrazia
- Energia
- Finanza
- Trasporti
- Industria
- Turismo e cultura
- Comunicazione e stampa
- Cyber social security

3. Impatto sugli assi portanti

- Democrazia
- Energia
- Finanza
- Trasporti
- Industria
- Turismo e cultura
- Comunicazione e stampa
- Cyber social security

5. Iniziative all'estero

- Canada
- Cina
- Francia
- Germania
- Regno Unito
- Singapore
- USA

In evidenza: Due pillole

Germania

- Nel 2017, il governo Tedesco e la Saarland hanno istituito un centro di ricerca sulla cybersecurity a Saarbruecken.
- Il centro assorbirà i 200 ricercatori di un centro esistente e punta ad ospitare più di 500 ricercatori in tutte le aree della sicurezza informatica.

Gran Bretagna

- Nel 2011 il governo della Gran Bretagna ha lanciato un'iniziativa per individuare le capacità di ricerca universitaria in cybersecurity esistenti del paese. Ad oggi 14 università sono riconosciute come centri di eccellenza, e specificamente finanziate.

Un anno dopo …

Istituzioni

- Roberto Baldoni Vice Dir. Generale DIS (Dipartimento Informazioni e Sicurezza) con delega Cyber
- Nucleo Sicurezza Cibernetica di coordinamento tra Ministeri chiave
- Recepimento NIS (Network and Information Security)
- Implementazione CVCN (Centro di Valutazione e Certificazione Naz.)

Un anno dopo …

Ricerca e Formazione

- Cyberchallenge.it
  - una realtà non solo nazionale
- Centri di Competenza Cybersecurity
  - In Toscana C3T, altri seguiranno
- Framework 2.0 – GDPR
- Progetto Europeo Pilot Cybersecurity: SPARTA
- Rete di Cyber Range con specializ-zazioni (IoT, Energia, Droni, PA, …)

Ricerca e Formazione

- Collaborazioni su Awareness e Formazione
  - Confindustria Digitale (Curricula Framework 2.0 ed altro)
  - Polizia Postale e Biblioteche di Roma (condivisione materiale awareness)
  - Master e Master Executive con aziende
  - Regioni (Master per DPO)

Un progetto del
Laboratorio
Nazionale di Cyber-
security del CINI

Supportato da
Nucleo Sicurezza
Cibernetica
e
Dipartimento
Informazioni e
Sicurezza

cini
Cybersecurity
National Lab

www.consorzio-cini.it

Obiettivi

CYBER CHALLENGE
CyberChallenge.IT

- Scoprire e valorizzare i talenti informatici dei giovani (16-23 anni) che studiano in Italia
- Ridurre la carenza di forza lavoro orientando i giovani verso lo studio dell'informatica e della sicurezza informatica.
- Costituire una squadra nazionale di *cyber defender* per partecipare a competizioni internazionali annuali, come lo *European Cybersecurity Challenge*. (ECSC)

Un po’ di storia

Edizione	Nodi	Totale	Ragazze	Scuole Superiori
2017	1	683	80	57
2018	8	1.866	168	583
2019	18	3.203	373	1.341


Università di Bologna


Centro di Competenza Cyber. Toscano


Link Campus University di Roma


Politecnico di Milano


Politecnico di Torino


Sapienza Università di Roma


Università degli Studi del Sannio


Università degli Studi di Bari Aldo Moro


Università degli Studi di Cagliari


Università del Salento


Università della Calabria


Universitò degli Studi di Genova


Universitò degli Studi di Napoli Parthenope


Universitò degli Studi di Padova


Università di Camerino


Università di Perugia


Università di Pisa


Università Politecnica delle Marche

Un Centro Regionale per la Cybersecurity

- Nato come progetto di collaborazione tra cinque istituzioni di ricerca in Toscana
- Dopo la firma di un accordo con la Regione Toscana per collaborazioni in materia di sicurezza informatica.

Governance

C³T
CENTRO DI COMPETENZA
CYBERSECURITY TOSCANO

- Comitato di Indirizzo
  con un delegato del Rettore/Direttore/Presidente di ogni istituzione.

- Comitato Tecnico Scientifico
  con un rappresentante per ciascun dipartimento/istituto coinvolto

- Direttore
  nominato dal comitato direttivo, rappresenta pubblicamente il centro e coordina le attività dei due comitati

www.c3t.it

C³T
CENTRO DI COMPETENZA
CYBERSECURITY TOSCANO

C³T svolge attività di ricerca e trasferimento tecnologico nel campo della sicurezza dell'informazione con l'obiettivo di informare, sensibilizzare e rispondere alle esigenze di

- Piccole e medie imprese
- Enti pubblici
- Professionisti
- Cittadini

su come riconoscere, capire e reagire alle minacce alla sicurezza informatica

Domini Applicativi

C³T
CENTRO DI COMPETENZA
CYBERSECURITY TOSCANO

- Infrastrutture Critiche
  IMT Lucca, Univ. Pisa, Univ. Firenze, Univ. Siena, CNR
- Protezione dei Dati
  IMT Lucca, Univ. Pisa, Univ. Firenze, Univ. Siena, CNR
- Difesa Nazionale e Legislazione
  Univ. Pisa
- Istituzioni Finanziarie
  IMT Lucca, Univ. Pisa
- Protezione dei dati personali
  IMT Lucca, Univ. Pisa, Univ. Firenze, Univ. Siena, CNR
- Catene di Distribuzione
  Univ. Pisa
- Trasporti e Logistica
  Univ. Pisa, Univ. Firenze, CNR

Domande?