IT Security & Standards

What do we need to defend us from
and, possibly, how?
Milan
27 September 2018

Mimmo Squillace
Presidenza@uninfo.it
mimmo_squillace@it.ibm.com

UNINFO

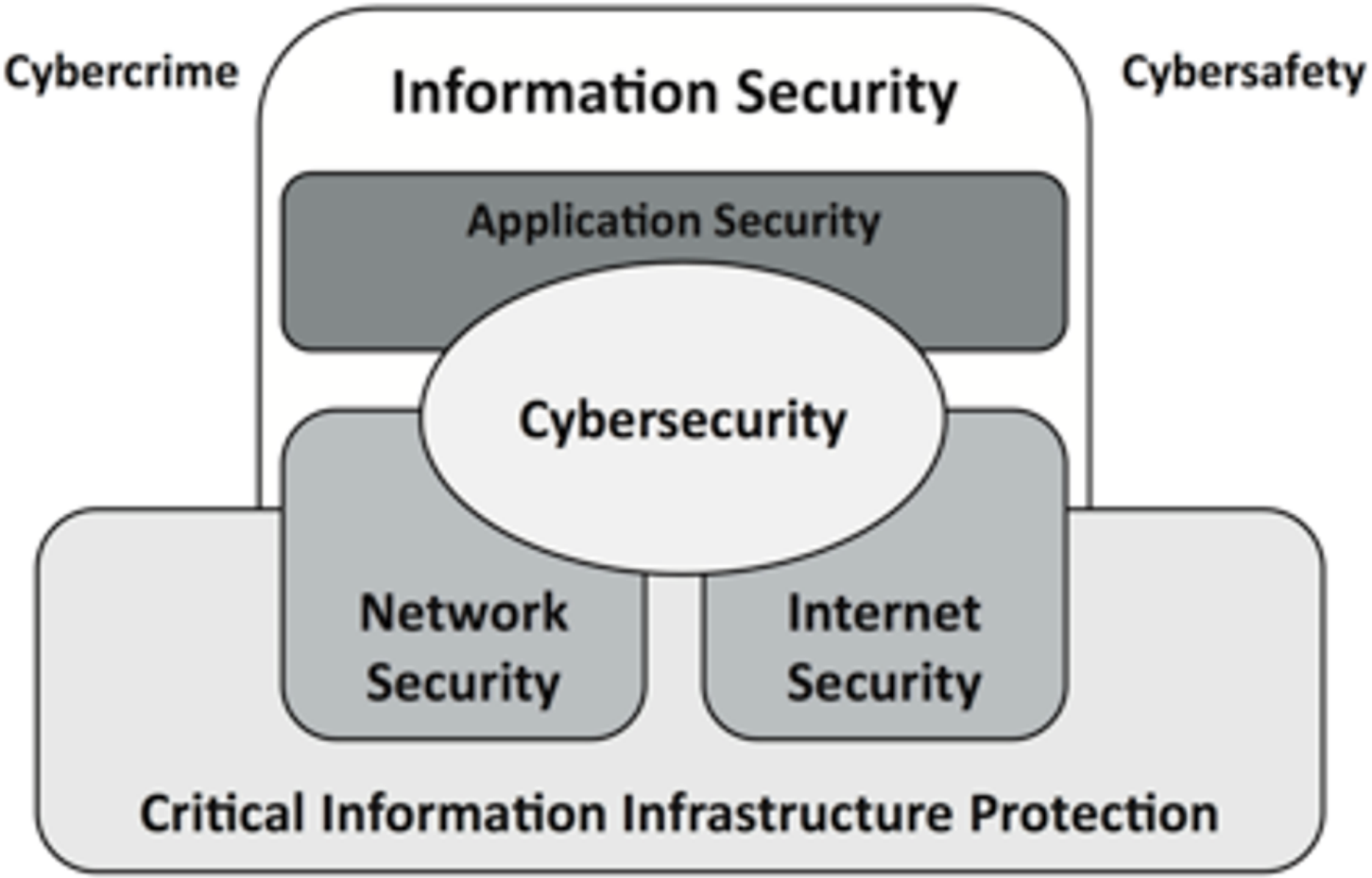
Mimmo Squillace

Technical Relations Executive – IBM Italia

Presidente UNINFO

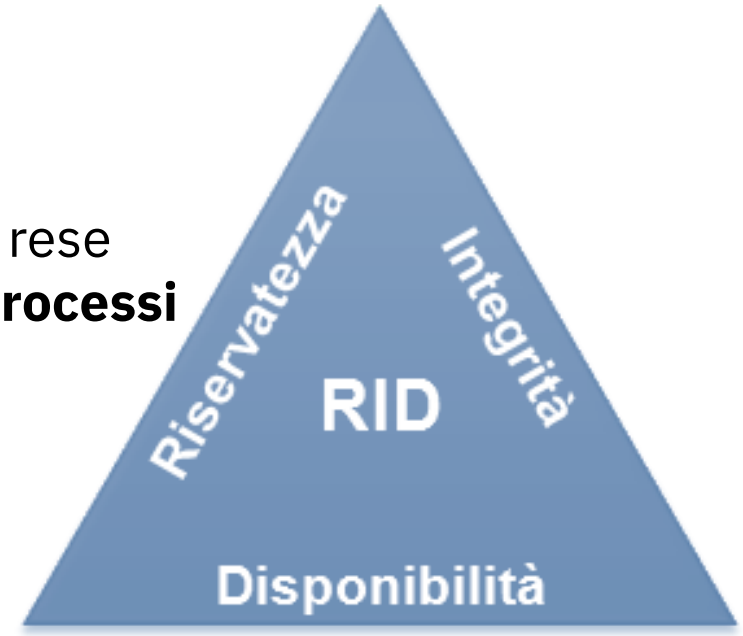
- *Sicurezza Informazioni*
- *Norme Tecniche*
- *UNINFO*

Information Security vs Cybersecurity



Sicurezza delle informazioni

Preservazione della **riservatezza**, dell'**integrità** e della **disponibilità** delle informazioni



Riservatezza

- Proprietà delle informazioni di non essere rese disponibili o divulgate a individui, entità o **processi** non autorizzati

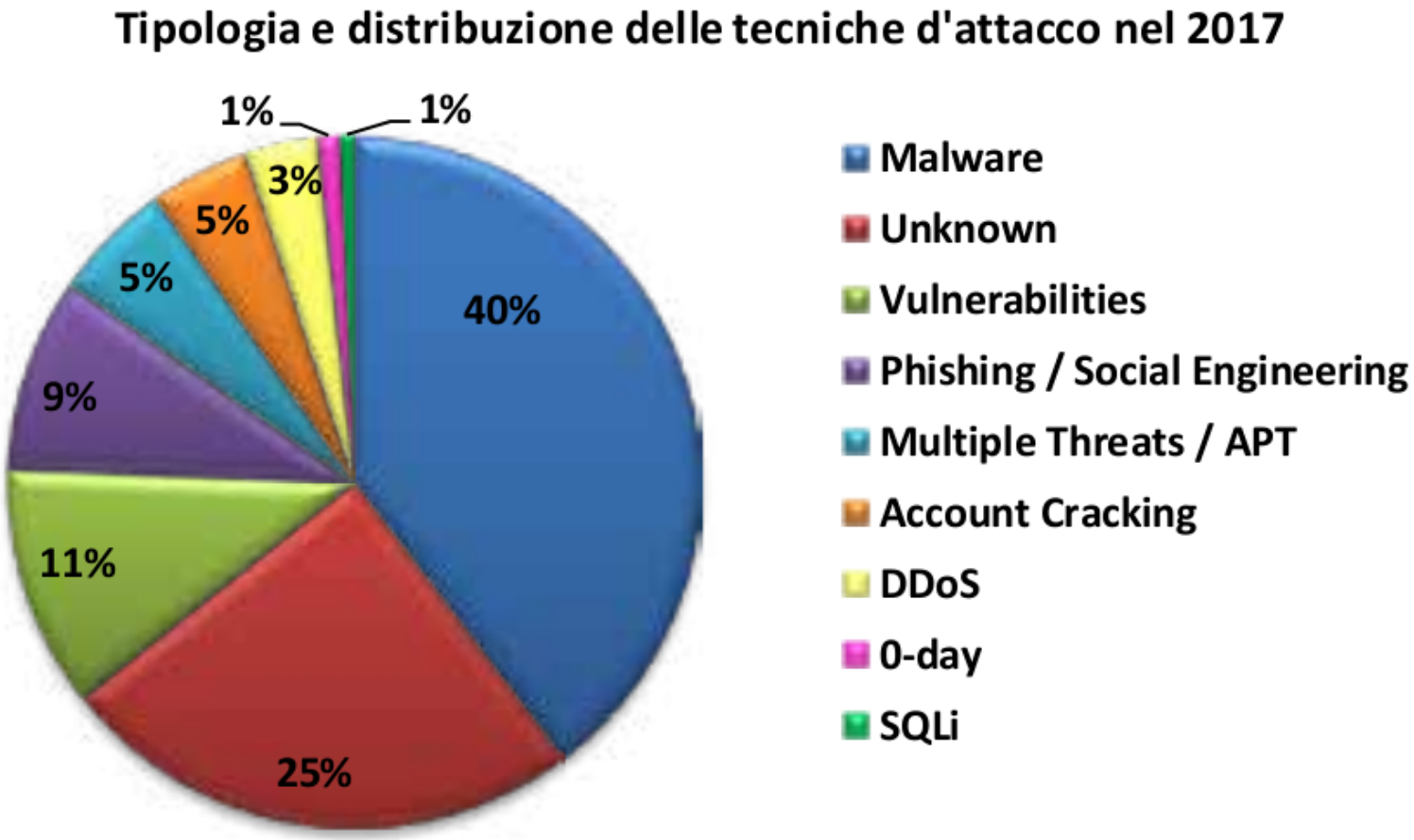
Integrità

- Proprietà relativa all'accuratezza e alla completezza

Disponibilità

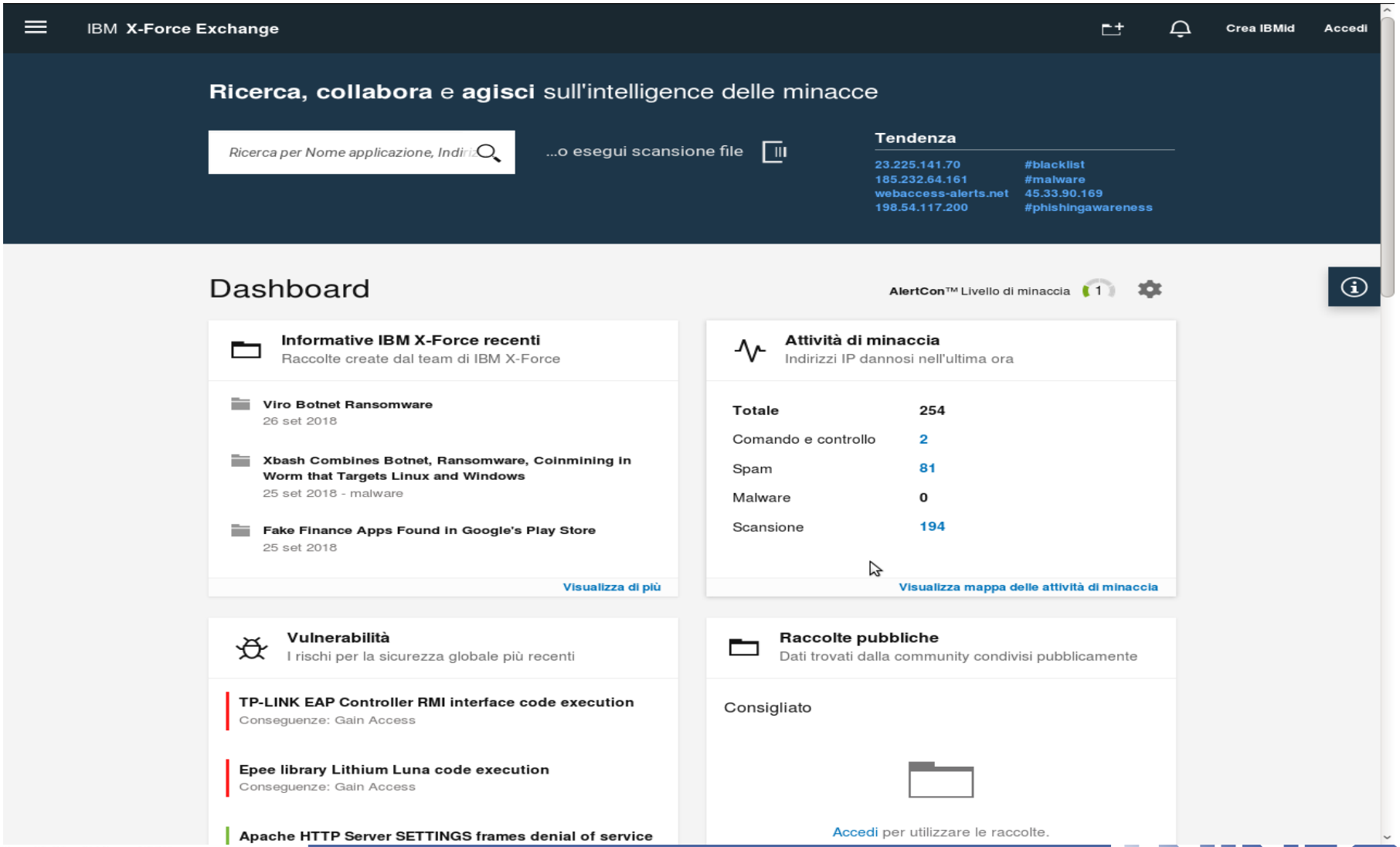
- Proprietà di essere accessibile e usabile a richiesta di un'entità autorizzata

Da cosa ci difendiamo?



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

Da cosa ci difendiamo?

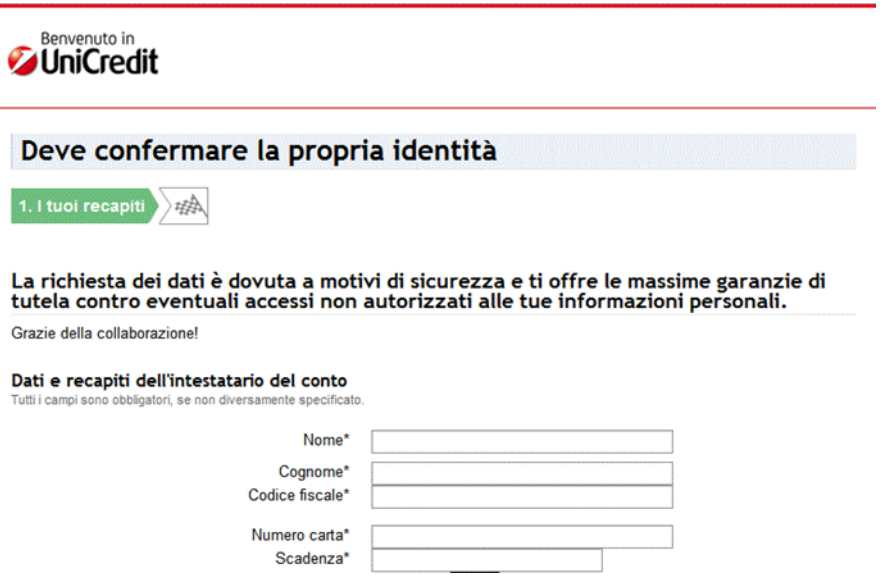


Da cosa ci difendiamo?

Phishing …

- ✔ Creazione di un sito web più possibile similare a quello legittimo
- ✔ Invio indiscriminato (se mirato si tratta di spear-phshing) di email contraffatte che portano l'utente verso il sito web contraffatto
- ✔ Raccolta di credenziali valide degli utenti tramite sito web contraffatto
- ✔ Riuso delle credenziali raccolte sul sito legittimo / su altri siti per transazioni illecite


UniCredit S.p.A. <noreply@www.unicredit.it>
31 agosto 2012 12:44
Reparto Informazioni e Sicurezza: Account Limitato
UniCredit
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

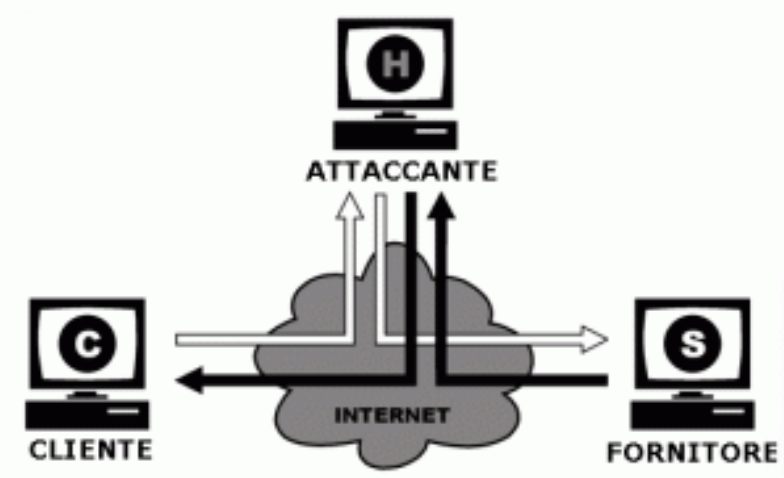

Benvenuto in UniCredit
Deve confermare la propria identità
1. I tuoi recapiti
La richiesta dei dati è dovuta a motivi di sicurezza e ti offre le massime garanzie di tutela contro eventuali accessi non autorizzati alle tue informazioni personali.
Grazie della collaborazione!
Dati e recapiti dell'intestatario del conto
Tutti i campi sono obbligatori, se non diversamente specificato.
Nome*
Cognome*
Codice fiscale*
Numero carta*
Scadenza*

Cryptolocker

- ✔ Apertura di allegato di email infetto o consultazione di sito web con contenuti malevoli
- ✔ Cifratura dei contenuti del disco locale e dei dischi di rete acceduti
- ✔ Richiesta di riscatto in Bitcoin (o altra valuta non tracciabile) per avere le chiavi di decifratura da parte del malware entro 3 o 4 giorni di tempo

Men-in-the-middle

- ✔ Compromissione o registrazione di dominio di posta elettronica di un fornitore
- ✔ Apertura di un conto ponte che non desti sospetti
- ✔ Invio di email per richiesta di modifica del conto registrato per i pagamenti verso un cliente
- ✔ Incasso del bonifico e spostamento di denaro su conto off-shore



Crypto-Miner

- ✔ Si sfruttano i computer infetti per “minare” le criptomonete
- ✔ NON ci si accorge praticamente di nulla (a meno di un rallentamento a volte vistoso…)
- ✔ Esiste anche la versione detta “mining-web” in cui viene iniettato nel **browser** il codice infetto

Computer World del 12/3/1

Solo “computer”? Uhmmm

WIRED

Hackers Remotely Kill a Jeep on the Highway.
– Wired, July 2015

Tech Insight: Hacking The Nest Thermostat
– Dark Reading, Aug 2014

The Hacker News
Security in a serious way

100,000 Refrigerators and other home appliances hacked to perform cyber attack
– The Guardian, Feb 2013

GIZMODO

Philips Hue Light Bulbs Are Highly Hackable
– Gizmodo, Aug 2013

WIRED

Millions of Kwikset Smartkey Locks Vulnerable to Hacking, Say Researchers– Wired, Aug 2013

Come ci difendiamo ...

Riduciamo la lunghezza delle nostre mura e consolidiamole

- ✔ Dove sono le informazioni aziendali?
- ✔ Chi vi deve poter accedere?
- ✔ Possono essere accentrate e messe sotto controllo?

Come ci difendiamo ...

Riduciamo la lunghezza delle nostre mura e consolidiamole

Facciamo un'analisi del rischio in base al nostro business!

- ✔ Dove sono le informazioni aziendali?
- ✔ Chi vi deve poter accedere?
- ✔ Possono essere accentrate e messe sotto controllo?

Come ci difendiamo ...

Adottiamo misure di **igiene informatica** su tutti i sistemi aziendali.
Parliamo di misure di:

- ✔ Antimalware
- ✔ Autenticazione
- ✔ Aggiornamento
- ✔ Backup
- ✔ Cifratura
- ✔ Limitazione della connettività
- ✔ Limitazione dei privilegi

Come ci difendiamo ...

Esempio: gestiamo correttamente l'autenticazione ai sistemi

Come ci difendiamo ...

Informiamo e formiamo
periodicamente il nostro personale:

- ✔ su cosa devono fare per stare in sicurezza (v. uso delle password)
- ✔ su cosa non devono fare per evitare le minacce (v. phishing)
- ✔ sul perché la sicurezza delle informazioni è importante (v. giornata odierna)

Come ci difendiamo ...

I temi da toccare sono diversi e coinvolgono non solo i tecnici (o i fornitori) informatici ma tutta l'azienda, ognuno per il suo.

Per essere efficaci è necessario un **APPROCCIO COMPLESSIVO** alla sicurezza e ..., vista la complessità dei temi, non è necessario inventarselo da capo

Norme Tecniche

***s**tandard o **S**tandard?*

Una Norma Tecnica è un documento che descrive lo “stato dell’arte” di: un bene, un servizio, un processo, un sistema, …

Una Norma Tecnica è un documento che descrive lo “stato dell’arte” di: un bene, un servizio, un processo, un sistema, …

Sviluppato presso un Ente di Normazione in maniera ***trasparente*** *e* ***democratica,*** *approvato in maniera* ***consensuale*** *ed adottato su* ***base volontaria.***

Chi sviluppa le Norme Tecniche?

Le Norme Tecniche possono essere:

International Standard

European Standard

National Standard

Le Norme Tecniche sono sviluppate da:

International Standard Setting Organizations

Electrotechnical	“All-others”	Telecommunication
IEC JTC/1	ISO	ITU

European Standard Setting Organizations

CENELEC	CEN	ETSI

National Standard Bodies

Fora Consorzi

W3C

IETF & IEEE

Gli Enti di Normazione italiani sono:
CEI ed UNI

COMITATO ELETTROTECNICO ITALIANO

Quando si parla di UNI si intende il Sistema UNI

CTI
Termotecnica

CIG
Gas

CUNA
Automobili

UNICHIM
Chimica

UNSIDER
Ferro e Metalli

UNIPLAST
Materie Plastiche

UNINFO "fa" gli Standard per l'ICT

CTI
Termotecnica

CIG
Gas

CUNA
Automobili

UNICHIM
Chimica

UNSIDER
Ferro e Metalli

UNINFO
Informatica

UNIPLAST
Materie Plastiche

SW Enginering

eHealth

Blockchain

eBSF

“MPEG”

Industry 4.0

“Traffic”

APNR-ICT

Additive Tecnologies

IT Security

Industrial Automation

Perchè sono importanti le norme?

Interoperabilità
Definizione univoca
Sicurezza prodotti
Economie di Scala

In più, 1 Norma EN:

- equivale a 33 Norme Nazionali
- da accesso ad un mercato di 650 milioni di persone

Norme Tecniche Sicurezza Informatica

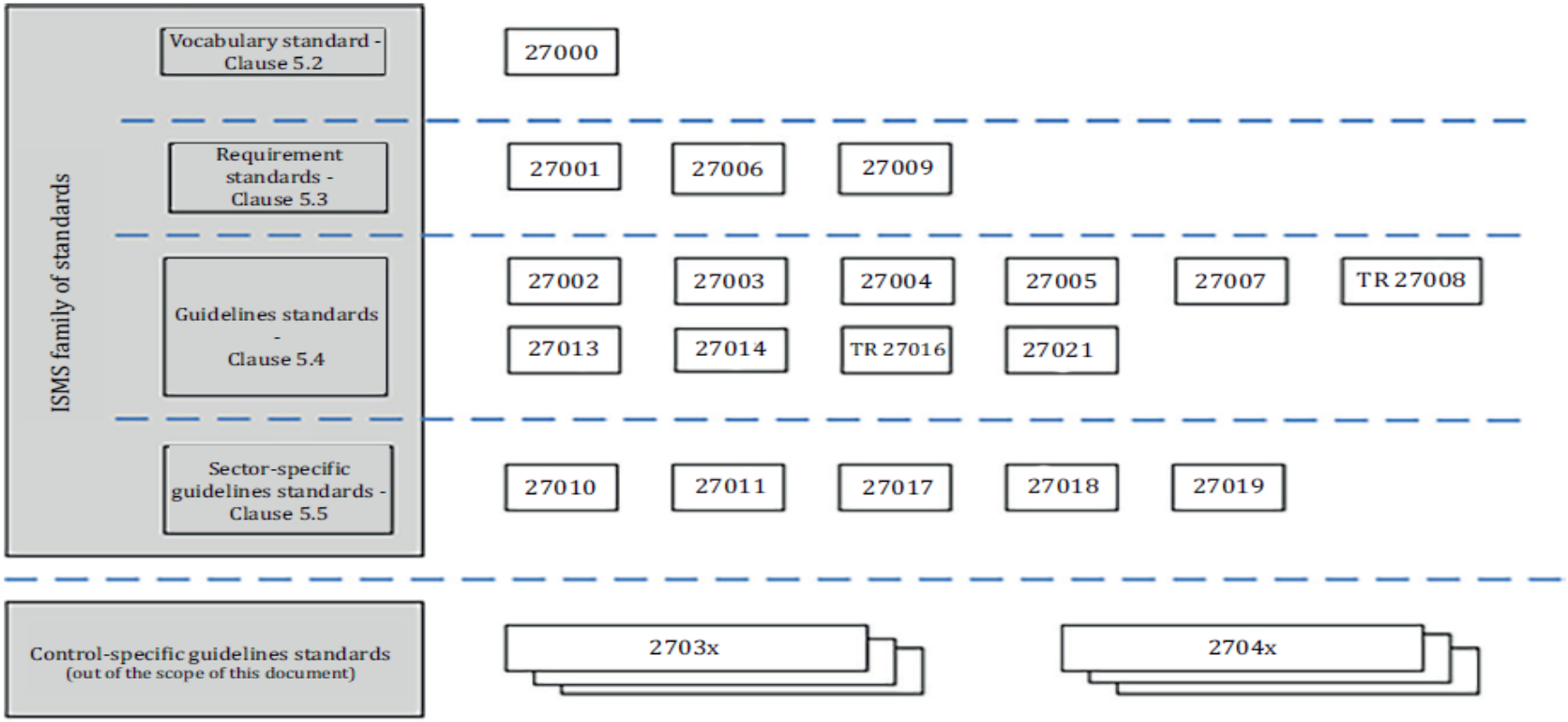
UNI CT/510 “Sicurezza Informatica”

Norme del sottocomitato 27 di ISO/IEC JTC 1 (150+)

- Sistemi di gestione per la sicurezza delle informazioni (27001, 27002)
- Linee guida per i sistemi di gestione (2700X)
- Linee guida di settore (2701X)
- Linee guida per la sicurezza (2703X-2704X)
- Certificazione della sicurezza dei prodotti (15408, 18045)
- Autenticazione e biometria (2476X)
- Protezione dei dati personali (291XX)
- Crittografia (979X, 18033)
- Modelli di maturità ICT (21827)

ISO/IEC 2700x

Si parla in genere di **famiglia delle norme ISO 2700x** intendendo un set ampio di standard.



Fonte: ISO/IEC 27000:2018

ISO/IEC 27001

Sistema di Gestione per la Sicurezza delle Informazioni (**SGSI o ISMS**).

- Applicabile **a realtà di ogni dimensione**
- Quasi **20 anni** di esistenza sul mercato
- Ambito definibile a piacimento
- Approccio ciclico (**PDCA**)
- Costituisce un framework completo
- Dice **cosa** fare, **non come** farlo
- Rivolto al miglioramento continuo
- È un **riferimento universale**

Norme Tecniche Industria 4.0 e IoT

Additive Technologies

Additive Technologies

JTC/1 SC41 Wearable

Additive Technologies

ISO184 & IEC65 + JWG21

JTC/1 SC41 “IoT”

JTC/1 SC38 “Cloud”

JTC/1 SC27 “IT Security”

JTC/1 SC42 “AI”

“Tecnologie abilitanti per Industria 4.0”

- JTC/1-WG 11 *“Smart City”*
- JTC/1-SC 38 *“Cloud”*
- JTC/1-SC 41 “IoT Te*chnologies*”
- CEN TC 225/WG 6 “IoT”
- ETSI M2M
- ETSI SM2M

ISO 184/IEC 65
JWG21

Smart Manufacturing Reference Model(s)

ISO/IEC JTC 1/SC 41 Internet of things and related technologies

Scope | Structure | Projects / Publications | Documents | Votes | Meetings | Collaboration Tools

Membership | Officers | Liaisons | Working Groups

Mr Domenico Mimmo Squillace

ISO/IEC JTC 1/SC 41 Subcommittee(s) and/or Working Group(s)

Label	Title
Working Groups	
WG 3	IoT Architecture
WG 4	IoT Interoperability
WG 5	IoT Applications
Advisory Groups	
AG 6	JTC 1/SC 41 Advisory Group
ad-Hoc Groups	
AHG 7	Study group on Wearables
AHG 14	Ad hoc group on Business Plan
AHG 15	Communication and outreach
AHG 16	Study Group on Reference Architecture and Vocabulary Harmonization
AHG 17	Study Group on Societal and human factors in IoT based services
AHG 18	Study Group on Integration of IoT and Blockchain
AHG 19	Study Group on Realizing Context Specific Solution / System Architecture based on IoT RA

Documenti di JTC/1 SC41 Pubblicati

- **ISO/IEC 30124:2018 Internet of Things (IoT) - Reference architecture**
- **ISO/IEC 20924:2018 Internet of Things (IoT) – Vocabulary**
- **ISO/IEC TR 22417:2017Internet of things (IoT) - IoT use cases**
- **16 norme “ereditate” da Sensor Networks**

Documenti di JTC/1 SC41 *Draft*

- **PNW JTC1-SC41-51 Internet of Things (IoT) – Application framework for industrial facility demand response energy management**
- **PNW JTC1-SC41-52 Internet of Things (IoT) - Requirements of IoT data exchange platform for various IoT services**
- **PNW JTC1-SC41-58 Internet of Things (IoT) - Compatibility requirements and model for devices within industrial IoT systems**
- **ISO/IEC 21823-1 Internet of Things (IoT) - Interoperability for IoT Systems - Part 1: Framework**
- **ISO/IEC 21823-2 ED1 Internet of Things (IoT) - Interoperability for IoT Systems - Part 2: Transport interoperability**
- **ISO/IEC 21823-3 ED1 Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability**
- **… Altri draft di norma**

Follow us on:
www.uninfo.it

https://www.facebook.com/UNINFO.it
https://twitter.com/uninfo_it
http://www.slideshare.net/uninfoit

Grazie dell'attenzione

Segreteria UNINFO
uninfo@uninfo.it