La (cyber) security ha bisogno di norme

D. (Mimmo) Squillace
presidenza@uninfo.it
mimmo_squillace@it.ibm.com

Mimmo Squillace

Technical Relations Executive – IBM Italia

Mimmo Squillace

Technical Relations Executive – IBM Italia

Presidente UNINFO

UNINFO e gli Standard

Sicurezza Informatica

Nemmeno a farlo apposta, ieri …

Ransomware Hits San Francisco Public Transit System, Asks for $73,000

By Catalin Cimpanu

November 28, 2016 04:15 AM 5

San Francisco CA
@SF_CA_RR

Follow

'You hacked' appears on Muni screens across San Francisco
rightrelevance.com/search/article…
1:47 AM - 27 Nov 2016

13 6

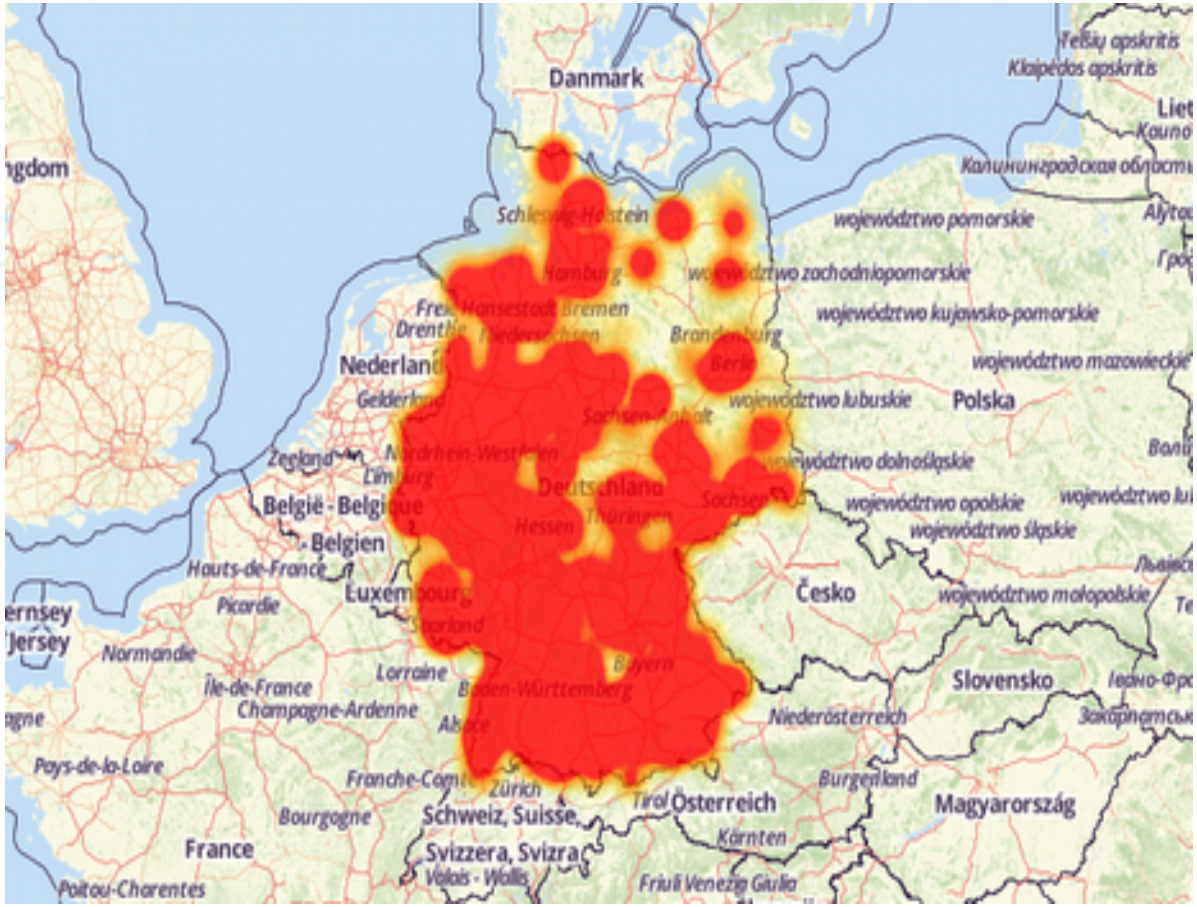
Source:
http://www.bleepingcomputer.com/news/security/ransomware-hits-san-francisco-public-transit-system-asks-for-73-000/

Nemmeno a farlo apposta, ieri …

900,000 Routers Knocked Offline in Germany amid Rumors of Cyber-Attack

By Catalin Cimpanu

November 28, 2016 10:47 AM 0



Source: http://www.bleepingcomputer.com/news/security/900-000-routers-knocked-offline-in-germany-amid-rumors-of-cyber-attack/

UNINFO e gli Standard

Sicurezza Informatica

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

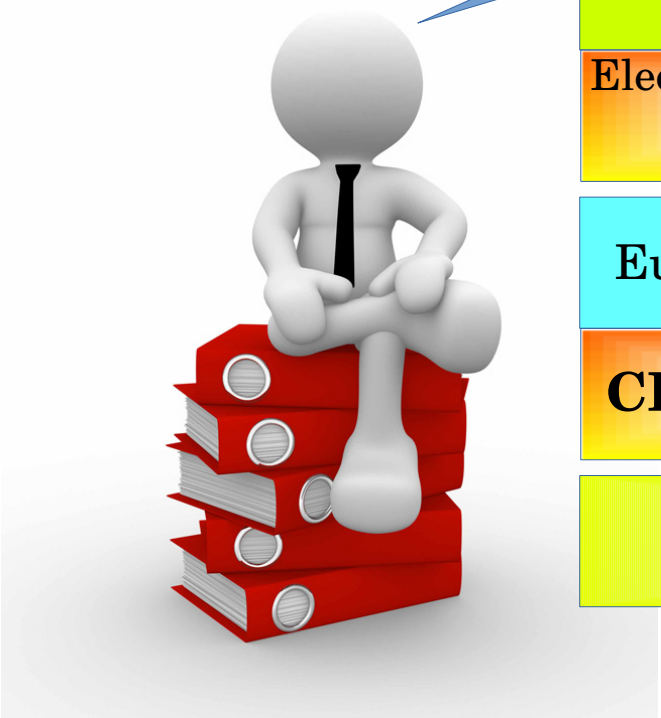
Una Norma Tecnica è un documento che descrive lo “stato dell’arte” di: un bene, un servizio, un processo, un sistema, ...

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.***

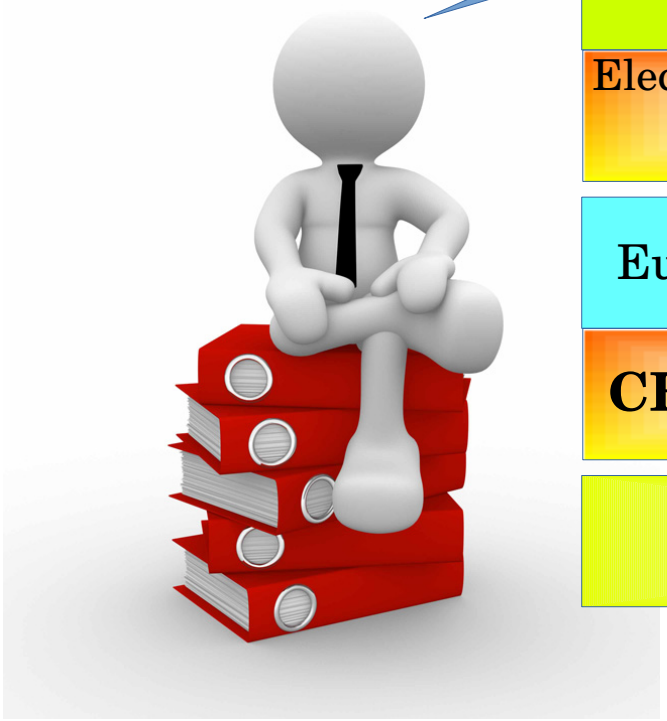
Chi sviluppa le Norme Tecniche?

Le Norme Tecniche sono sviluppate da:



International Standard Setting Organizations		
Electrotechnical **IEC** **JTC/1**	"All-others" **ISO**	Telecommunication **ITU**
European Standard Setting Organizations		
CENELEC	**CEN**	**ETSI**
National Standard Bodies		

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

W 3 C

I E T F & 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

Perchè sono importanti?

Interoperabilità
Definizione univoca
Sicurezza prodotti
Economie di Scala

Perchè sono importanti?

Interoperabilità
Definizione univoca
Sicurezza prodotti
Economie di Scala

1 Norma EN:

- equivale a 33 Norme Nazionali
- consente l'accesso ad un mercato di 650 milioni di persone

I settori di attività di UNINFO

Ingegneria del SW

Informatica Medica

eBSF

Sicurezza informatica

Tecnologie Additive

“Traffico”

“MPEG”

Automazione Ind.

APNR-ICT

Blockchain

"Tecnologie abilitanti per l'I4.0"

- JTC/1-WG 9 "*Big Data*"
- JTC/1-WG 10 "*IoT*"
- JTC/1-WG 11 "*Smart City*"
- JTC/1-SC 38 "*Cloud*"

UNINFO e gli Standard

Sicurezza Informatica

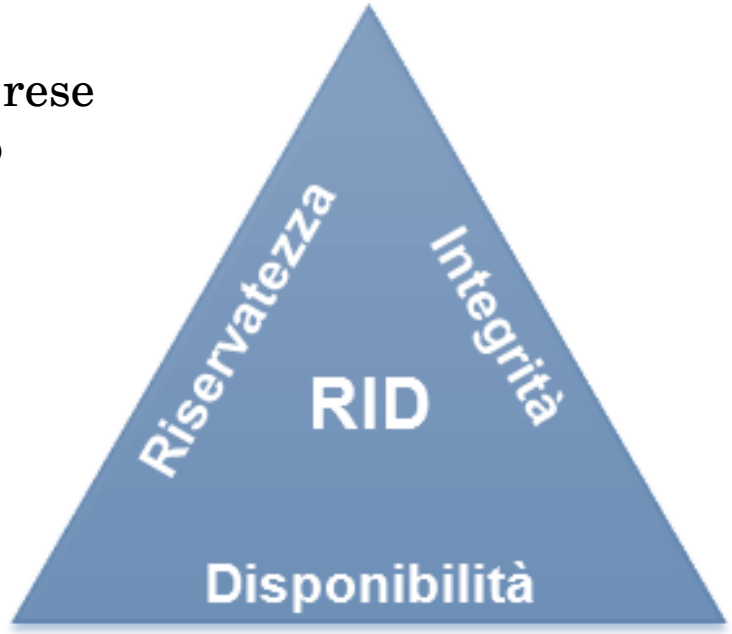
Sicurezza di cosa? Intendiamoci …

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?

Da cosa ci difendiamo?

Top Threats 2015	Assessed Trends 2015
1. Malware	↑
2. Web based attacks	↑
3. Web application attacks	↑
4. Botnets	↓
5. Denial of service	↑
6. Physical damage/theft/loss	→
7. Insider threat (malicious, accidental)	↑
8. Phishing	→

Top Threats 2015	Assessed Trends 2015
9. Spam	↓
10. Exploit kits	↑
11. Data breaches	→
12. Identity theft	→
13. Information leakage	↑
14. Ransomware	↑
15. Cyber espionage	↑

Da cosa ci difendiamo?

Amministrazione e contabilità

- Accesso ai conti aziendali
- Dati personali dei dipendenti
- Budget e dati finanziari

Presenza web

- Siti vetrina o e-commerce
- Posta elettronica
- Accesso remoto a file e sistemi

Management

- Strategie aziendali
- Legale rappresentanza

Progettazione

- Specifiche di prodotto / disegni
- Know-how aziendale

Commerciale

- Dati dei Clienti

Produzione

- Sistemi tecnologici

Da cosa ci difendiamo?

Attacchi web-based

Amministrazione e contabilità

- Accesso ai conti aziendali
- Dati personali dei dipendenti
- Budget e dati finanziari

Presenza web

- Siti vetrina o e-commerce
- Posta elettronica
- Accesso remoto a file e sistemi

DoS

Phishing

Management

- Strategie aziendali
- Legale rappresentanza

Malware Sabo-taggio

Progettazione

- Specifiche di prodotto / o
- Know-how aziendale
-

Cyber spionaggio

Furto identità

Commerciale

- Dati dei Clienti

Produzione

- Sistemi tecnologici

DoS

Ma a noi interessa davvero?

Ma a noi interessa davvero?

Familiarizziamo con termini quali:

- Phishing
- Ramsonware o cryptolocker
- Men-in-the-middle
- Malware
- DoS (Denial of Service)
- Botnet

Ma a noi interessa davvero?

Phishing su Internet Banking

- ✔ 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

http://www.sonicwall.com/phishing/

Ma a noi interessa davvero?

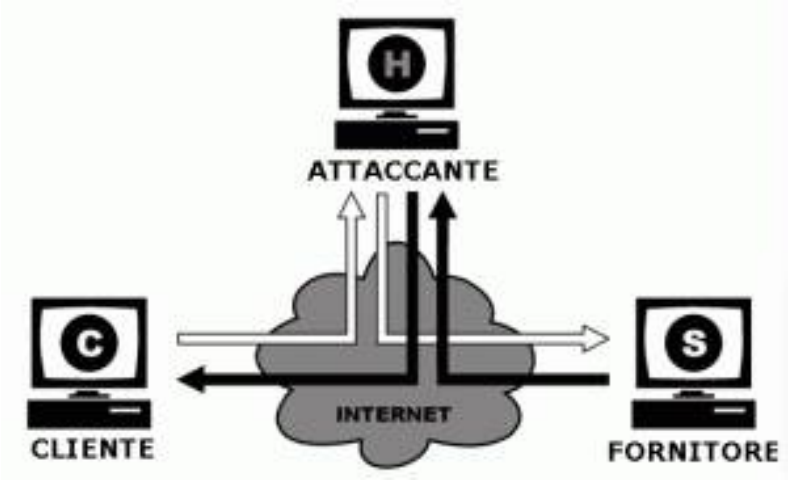
Cryptolocker

- ✔ 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

Ma a noi interessa davvero?

Attacco per finto bonifico

- ✔ 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



Ma a noi interessa davvero? [PMI]

AssetProtection. PMI sotto attacco: Cryptolocker e Cryptowall ancora in azione

Cryptolocker: Decine di casi in Abruzzo

Sicurezza: phishing e ransomware continuano a crescere

Cinesi all'attacco delle PMI Italiane

Clienti di PMI svizzere nel mirino degli attacchi di phishing

Aziende truffate tramite intercettazione email

Ma a noi interessa davvero? [PMI]

D: Si sente parlare poco di attacchi alla sicurezza delle PMI, come mai?

D: Noi non abbiamo mai avuto problemi di questo tipo™, perché?

D: Quelle per la sicurezza informatica non sono altre spese inutili?

Ma a noi interessa davvero? [PMI]

D: Si sente parlare poco di attacchi alla sicurezza delle PMI, come mai?

R: Le PMI tendono ad essere vittima di attacchi generalizzati e a non subire danni come una grande azienda. Pochi danni = poco risalto sui mass media

D: Noi non abbiamo mai avuto problemi di questo tipo™, perché?

R: Due cause sono quelle più plausibili:

- avete avuto MOLTA fortuna
- non ve ne siete mai accorti

D: Quelle per la sicurezza informatica non sono altre spese inutili?

R: Le spese fatte a caso o per mettere a posto i danni tendono ad essere inutili, un sensato livello di protezione è anche economicamente efficace.

Ma a noi interessa davvero? [IoT]

WIRED

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

DARKReading

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

Come ci difendiamo

Come ci difendiamo

Come ci difendiamo

Riduciamo la lunghezza delle nostre mura e consolidiamole

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

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

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

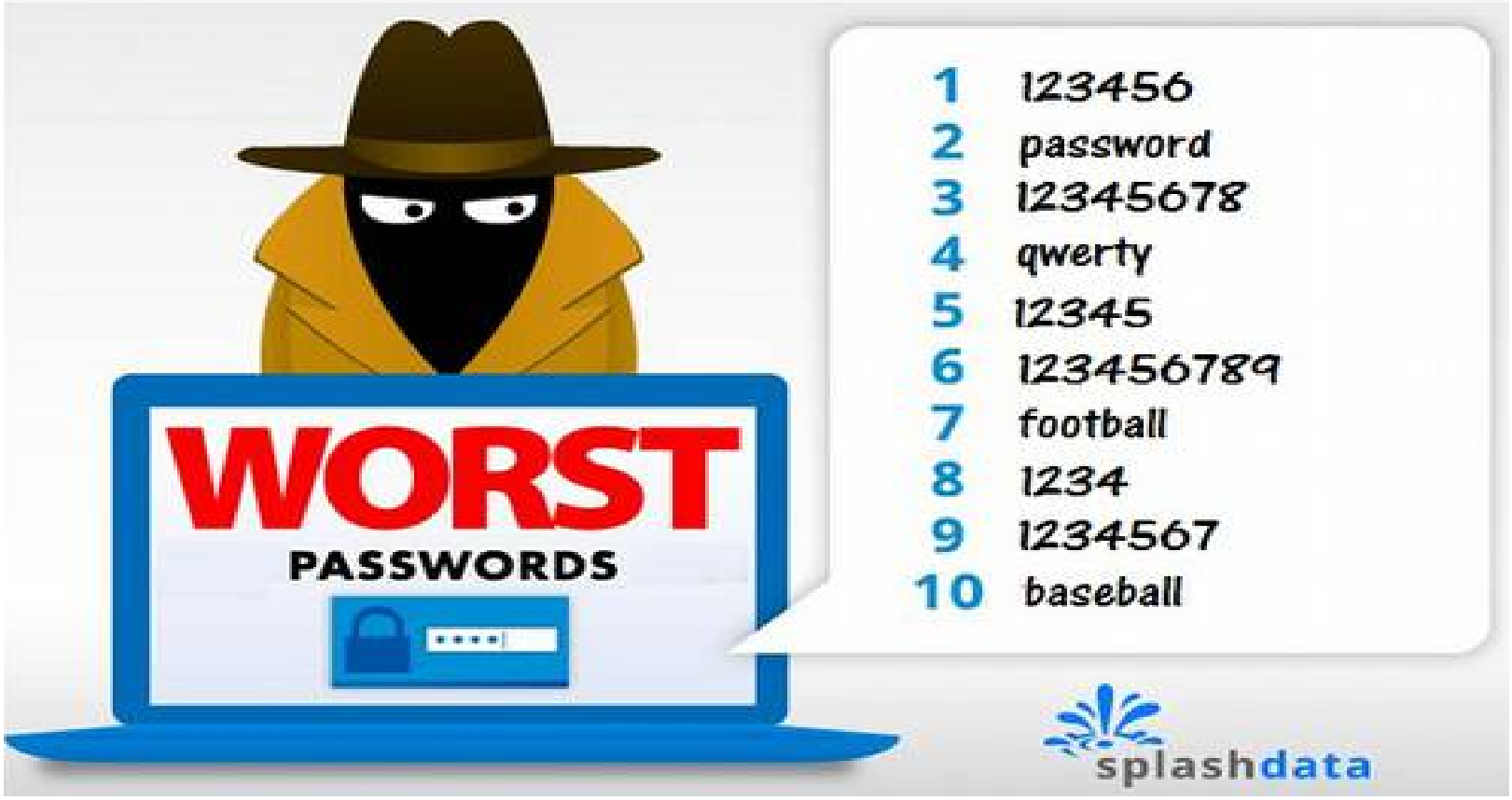
Come ci difendiamo

Adottando misure di **igiene informatica** su tutti i sistemi aziendali.

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

Come ci difendiamo

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, qualunque cosa produca!***

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

Come ci difendiamo

I temi da toccare sono diversi e coinvolgono non solo i tecnici (o i fornitori) informatici ma ***tutta l'azienda, qualunque cosa produca!***

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

UNINFO: Standard per la Sicurezza Informatica!

Attività di UNINFO

Attività di UNINFO

Norme di ISO/IEC JTC 1 SC27 “IT Security Techniques” (sono più di 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)

ISO/IEC 27001

Sistema di Gestione per la Sicurezza delle <u>Informazioni</u> (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 e certificabile

Analisi del rischio secondo ISO/IEC 27001:

Il vero "motore" della ISO/IEC 27001 è il processo di gestione del rischio relativo alla sicurezza delle informazioni, così specificato genericamente nella ISO 31000:

Definizione del contesto → Valutazione del rischio → Trattamento del rischio

Uno dei modi più diretti per effettuare un "trattamento del rischio" è quello di ridurlo ad un livello accettabile adottando dei controlli di sicurezza, dei quali la 27002 può essere considerata come un **esteso catalogo**.

ISO/IEC 27002:2013

Domande? Dubbi?

This work is licensed under the
Creative Commons Attribution- NonCommercial-NoDerivs 3.0 Unported License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0/

Grazie dell'attenzione

Follow us on: www.uninfo.it

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

Segreteria UNINFO
uninfo@uninfo.it

This work is licensed under the
Creative Commons Attribution- NonCommercial-NoDerivs 3.0 Unported License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0/