Gli effetti della Digital Transformation sugli scenari della Cyber Security

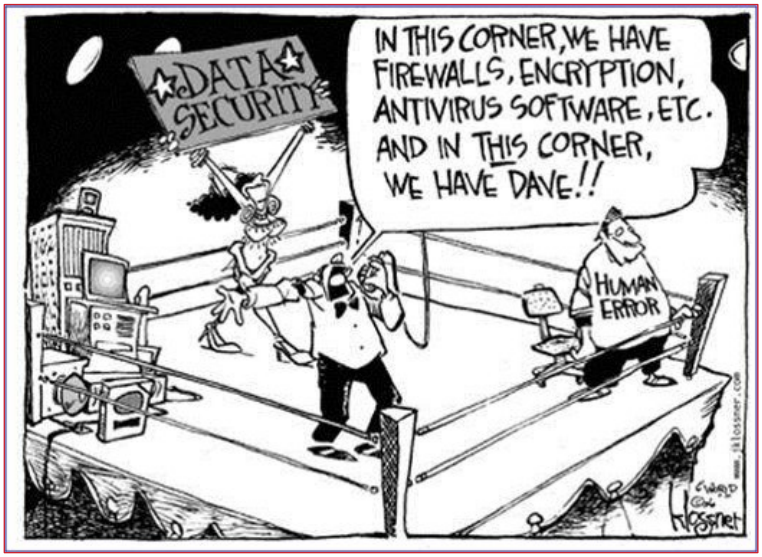
Roma, 4 luglio 2017

selta.com

I punti che vedremo

- Contesto
- Evoluzione
- Esigenze
- Offerta

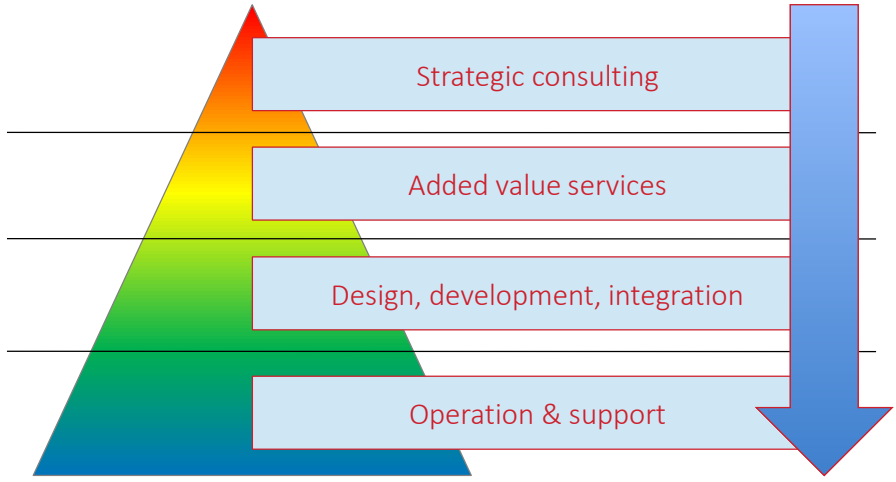
Il vero problema della cybersecurity



La nostra visione del problema

- Il **fattore umano** è il punto di attenzione fondamentale:
  - obiettivo di **attacchi specifici** (spearphishing, social engineering, …)
  - fonte di **errori**, commessi anche in buona fede
  - utilizzatore **ingenuo** di dispositivi potenti e connessi ma **intrinsecamente deboli**
- Occorre rafforzare questo anello debole:
  - depotenziando le minacce esterne ed interne
  - minimizzando le possibilità di errore
  - aumentando le capacità di prevenzione e detezione
  - potenziando le capacità di risposta e ripristino
- Le tecnologie sono un **valido supporto** ma la risposta alle esigenze di cybersecurity non può essere esclusivamente basata su di esse

Il nostro approccio top-down

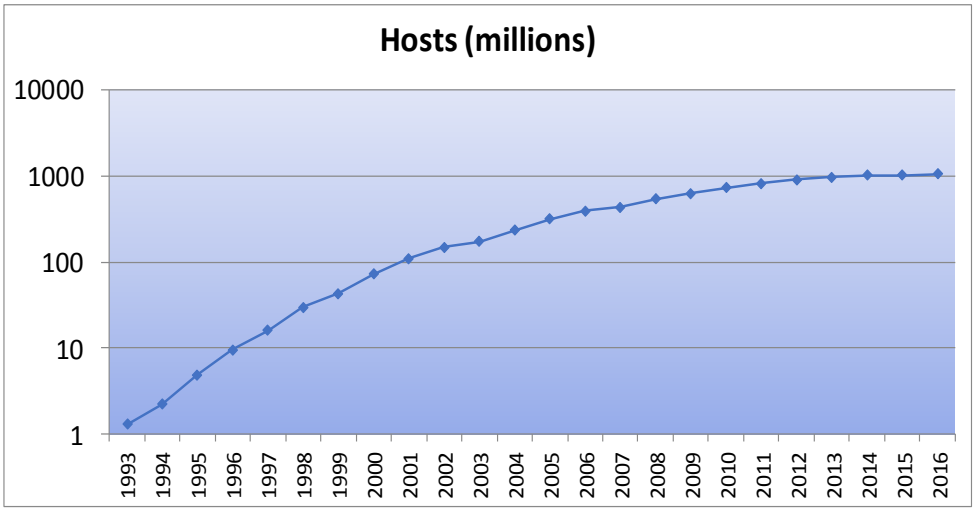


Cyber Team

- **Obiettivo**: opera all'interno della MU CS&IS per rispondere in modo strategico, unitario e integrato alle nuove minacce cibernetiche
- **Vision**: sicurezza come fattore abilitante e valore competitivo
- **Mission**: aiutare i Clienti a proteggere i propri asset materiali ed immateriali contro le nuove minacce cibernetiche, per mantenere alta la capacità di perseguire i propri obiettivi strategici
- **Target**: difesa, infrastrutture critiche, grandi organizzazioni
- **Attività**: sviluppo di prodotti e soluzioni, consulenza strategica, servizi a valore aggiunto, scouting ed integrazione di prodotti innovativi

Un mondo sempre più complesso

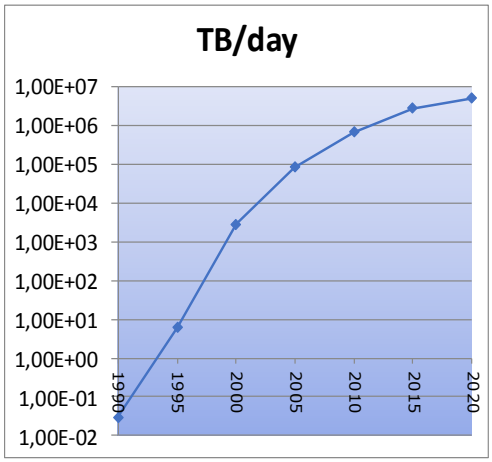
Crescita di Internet, 1993-2016



Source: Statista, 2017

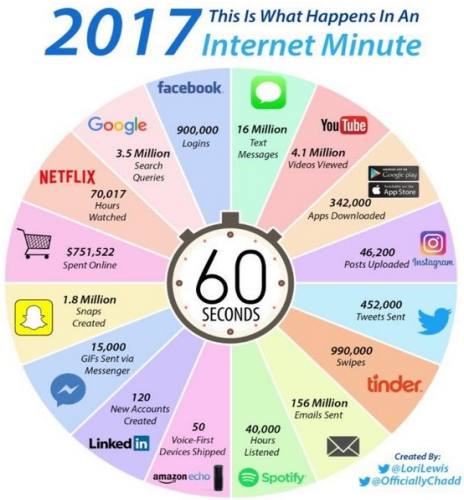
Crescita del traffico, 1990-2020

Year	TB/day	F_{1990}
1990	0.03	1
1995	6	$2.0 \cdot 10^2$
2000	2,800	$9.3 \cdot 10^4$
2005	81,000	$2.7 \cdot 10^6$
2010	672,000	$2.2 \cdot 10^7$
2015	2,680,000	$8.9 \cdot 10^7$
2020	5,000,000	$1.7 \cdot 10^8$



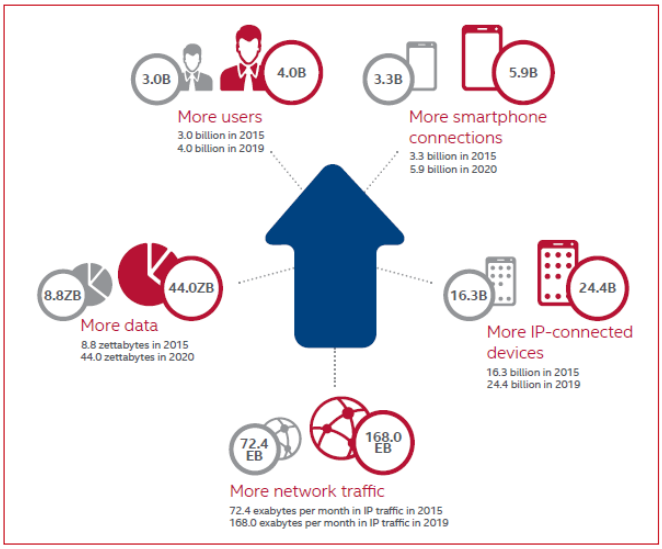
Fonte: Cisco VNI, 2011, 2015

I numeri di Internet, oggi e domani



- **Oggetti**: nel 2019 i dispositivi connessi in Rete saranno un numero pari a tre volte e mezza la popolazione della Terra.
- **Traffico**: il traffico IP nel 2015 è stato di 72,4 HByte al mese. Nel 2019 sarà di 168,0 HByte al mese. (1 HByte = 1018 Byte, ossia un milione di TByte).
- **Utenti**: erano 3 miliardi nel 2015, saranno 4 miliardi nel 2019.

Aumento della superficie d'attacco



Fonte: McAfee Labs, 2015

Esigenze di protezione

Il cyberspace non è un'isola

- Il cyberspace non è una dimensione a parte, ma l'insieme connesso di tutti i sistemi e le reti del pianeta:
  - le minacce cyber sono globali e pervasive, e il loro bersaglio non è il cyberspace in sé ma sono le infrastrutture del «mondo reale», il cosiddetto **dominio cyber-fisico**
- Il cyberspace è spesso considerato «terra di nessuno» per via dell'assenza di confini evidenti e della mancanza di una chiara giurisdizione:
  - è piuttosto una sorta di «portale» che consente a chiunque di proiettare la sua presenza e le sue attività nel cuore dei sistemi di un'altra nazione senza dover attraversare alcun reale confine: il cyberspace **non è uno spazio topologico**
- Il rapporto costo-benefici di un attacco terroristico o di una campagna criminale di tipo cyber diventa sempre migliore perché è sempre più facile raggiungere il bersaglio desiderato e sfruttarne le vulnerabilità

Una minaccia più subdola e sofisticata

Minaccia tradizionale	Minaccia cyber
Azione evidente, puntuale e diretta	Azione nascosta, elusiva ed indiretta
Intrusione	Infiltrazione
Approccio opportunistico «mordi e fuggi»	Approccio finalizzato alla permanenza
Obiettivi immediati o di breve periodo	Obiettivi di medio e lungo periodo
Ottenimento di beni o servizi	Ottenimento di informazioni
Focus soprattutto su reti e dispositivi	Focus soprattutto su persone e processi

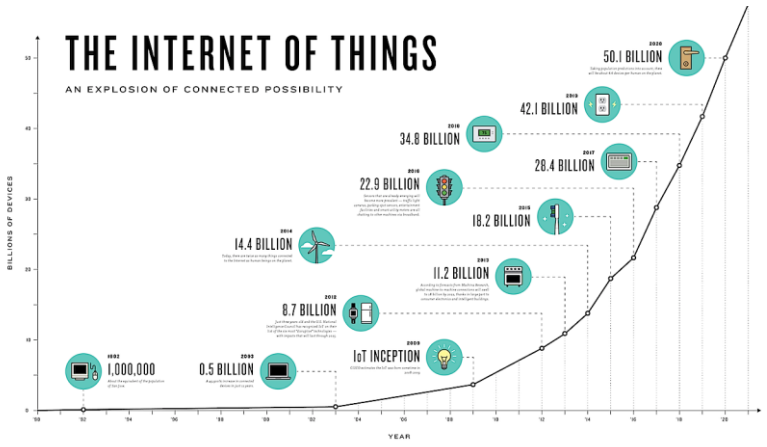
Il caso dei sistemi SCADA (1/2)

- I sistemi SCADA sono da sempre progettati per essere **safe** ma non **secure**
- La sicurezza nel mondo SCADA è tradizionalmente stata basata su:
  - il fatto che i sistemi **non fossero accessibili da reti esterne** (*isolation*)
  - il fatto che i sistemi fossero molto **specifici, complessi e oscuri** (*security by obscurity*)
- Poi è arrivato Stuxnet:
  - mirato al Siemens Simatic S7-300 (SO WinCC e PCS 7)
  - propagato sia off-line (USB key) che on-line (rete locale)
  - rimasto attivo per mesi fino a che non è uscito all'esterno per errore
  - per rilasciare la patch Siemens ha impiegato 675 giorni!

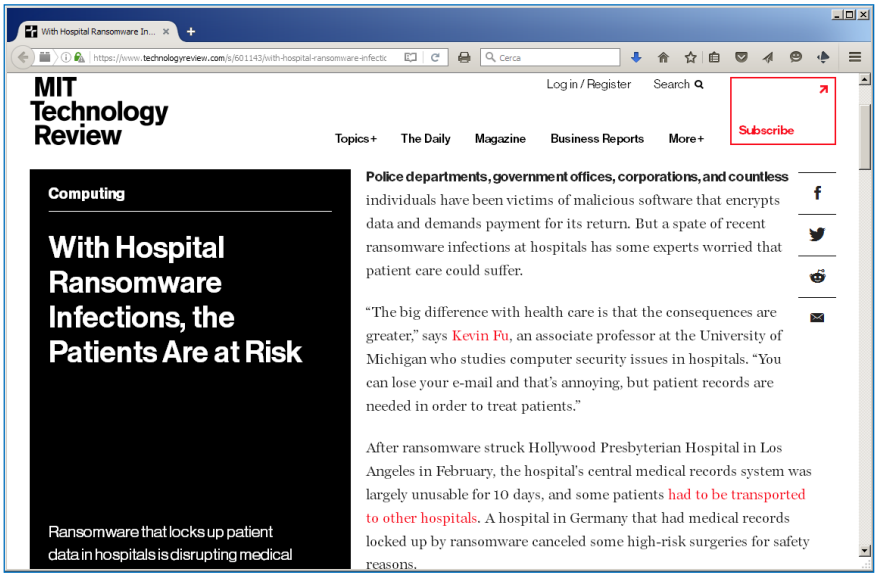
Il caso dei sistemi SCADA (2/2)

- Le vecchie assunzioni di «sicurezza» non sono più valide:
  - i sistemi SCADA sono generalmente connessi, e spesso a reti non sicure
  - i sistemi e i protocolli SCADA attuali sono intrinsecamente insicuri
  - la conoscenza delle architetture e dei protocolli SCADA non è più un «segreto professionale» di pochi addetti ai lavori
- Il risultato: malware «generici» che prendono di mira i sistemi SCADA
- **Industroyer** (CrashOverride), responsabile di attacchi alle centrali energetiche Ucraine (dicembre 2016):
  - implementa direttamente i protocolli IEC 60870-5-101, IEC 60870-5-104, IEC 61850, e OLE for Process Control Data Access (OPC DA)
  - è in grado di lanciare attacchi DoS contro i sistemi Siemens SIPROTECT, sfruttandone una nota vulnerabilità (CVE-2015-5374)

L'Internet delle cose (IoT) e i nuovi rischi



Ricatti ai soggetti deboli



With Hospital Ransomware In...

https://www.technologyreview.com/s/601143/with-hospital-ransomware-infectic

Cerca

MIT Technology Review

Log in / Register Search

Subscribe

Topics+ The Daily Magazine Business Reports More+

Computing

With Hospital Ransomware Infections, the Patients Are at Risk

Ransomware that locks up patient data in hospitals is disrupting medical

Police departments, government offices, corporations, and countless individuals have been victims of malicious software that encrypts data and demands payment for its return. But a spate of recent ransomware infections at hospitals has some experts worried that patient care could suffer.

"The big difference with health care is that the consequences are greater," says Kevin Fu, an associate professor at the University of Michigan who studies computer security issues in hospitals. "You can lose your e-mail and that's annoying, but patient records are needed in order to treat patients."

After ransomware struck Hollywood Presbyterian Hospital in Los Angeles in February, the hospital's central medical records system was largely unusable for 10 days, and some patients had to be transported to other hospitals. A hospital in Germany that had medical records locked up by ransomware canceled some high-risk surgeries for safety reasons.

Cosa facciamo

Il valore della sinergia

- Competenze multidisciplinari
- Capacità di progettazione, sviluppo, integrazione
- Sinergia col nostro CE.VA. (centro di valutazione accreditato Common Criteria)
- Sinergia coi nostri laboratori TEMPEST accreditati
- Sinergia con la divisione aziendale che produce sistemi SCADA
- Sinergia con partner e produttori italiani ed esteri
- Prodotti sviluppati e costruiti in Italia
- Intero range di offerta, dal livello network alla consulenza strategica

La nostra offerta

Strategic consulting	Added value services	Design, development & integration	Operation & support
• Audit & assessment • Roadmap design • Policies & processes • Risk assessment & management • Governance & compliance • Security & privacy	• Vulnerability assessment • Threat intelligence • Penetration testing • Application security • Business process review • Awareness building • Training & coaching	• Security architectures • Business continuity & disaster recovery • SIEM & log management • Identity management & access control • Content management • Data Loss Prevention • Convergent security	• Incident response • Crisis management • Malware analysis • Digital forensics • Digital investigations

22

I nostri principali clienti

THALES

LEONARDO

LFoundry

elt

SpecTec

TELESPAZIO
a LEONARDO and THALES company

23

I nostri principali partner

SELTA

Linking The Future

selta.com