GRUPPO TIM
Cyber Security dello scambio dati nel soccorso tecnico e nelle emergenze
ISA - 5 ottobre 2017

Politiche di sicurezza delle infrastrutture informatiche:

l'approccio di Telecom Italia alla sicurezza della rete IP

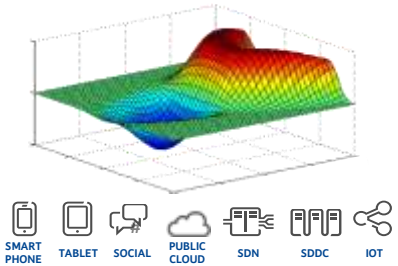
Sandro Dionisi
SECURITY – ICT Risk Management

TIM

Contesto e crescita del rischio Cyber

Nel 2017, «**Data fraud or theft and Cyber attacks**» sono tra i primi 10 rischi del Global Risk Report 2017 del World Economic Forum rispettivamente al 5° e 6° posto.

Sono i rischi percepiti con un livello molto elevato di probabilità di crescita (rispetto al 2016) e un impatto atteso sostanzialmente invariato 2017 vs 2016.



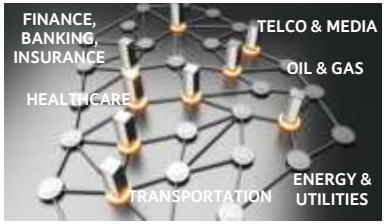
Aumenta la superfice esposta

Crollano i costi per organizzare attacchi

The Global Risk Report 2017

WORLD ECONOMIC FORUM

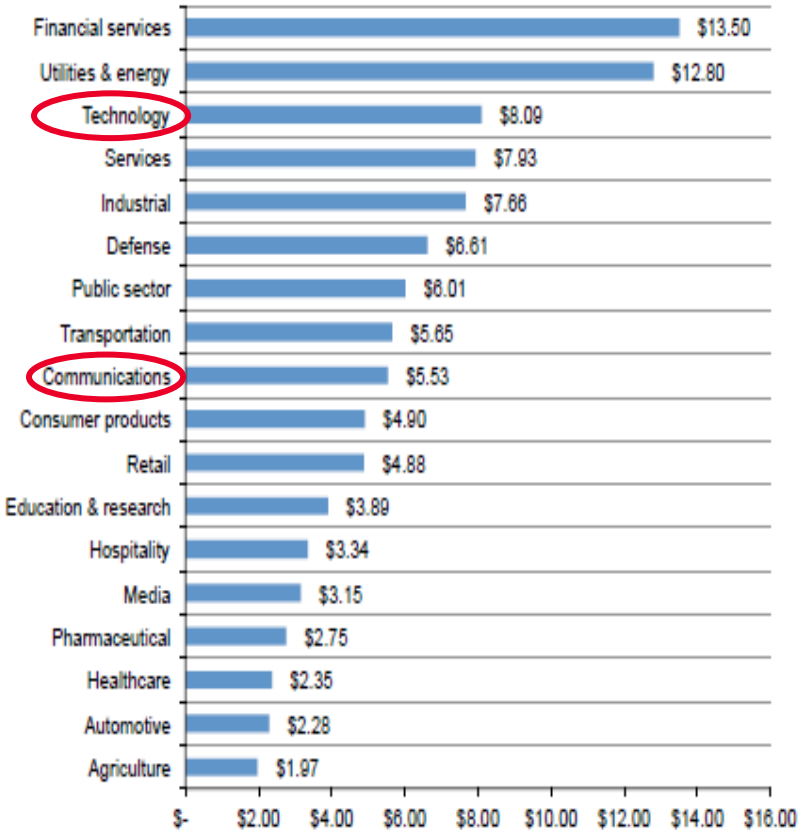
Aumenta la velocità di cambiamento
(sia a livello tecnologico sia delle competenze)



Interdipendenza delle Infrastrutture critiche

Anche dal punto di vista dei costi, gli incidenti di Cyber Security hanno un impatto considerevole in tutte le industry

Cybercrime: costo medio annuo per azienda nelle diverse industry (milioni di dollari USA)



Fonte: Ponemon Institute, *2015 Cost of Cyber Crime Study: Global*

SONY — RECORDS STOLEN 47,000 — STOCKS -1,7%

THE HOME DEPOT — RECORDS STOLEN 109M — STOCKS -2,4%

RECORDS STOLEN 83M — STOCKS -0,7%

ebay — RECORDS STOLEN 145M — STOCKS -0,7%

RECORDS STOLEN 110M — STOCKS -0,3%

Fonte: Bloomberg 2015

Le reti di telecomunicazione giocano un ruolo fondamentale nell'ambito delle infrastrutture critiche

Infrastruttura critica:

«*Un elemento, un sistema o parte di questo che è essenziale per il mantenimento delle funzioni vitali della società, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o distruzione avrebbe un impatto significativo a causa dell'impossibilità di mantenere tali funzioni*»

[Direttiva Europea 114/08 CE]

Tutte le infrastrutture critiche dipendono in maniera significativa dalle infrastrutture informatiche e di comunicazione

Le reti di telecomunicazione

Le reti di Telecomunicazione sono costituite da layer infrastrutturali diversi e interconnessi tra loro: Accesso (fixed/wireless), Trasporto, Core, Servizi e Applicazioni, Sistemi di Gestione

Alcuni numeri della Rete Telecom Italia

32 POP

~ 600 apparati Metro IP

~ 10000 centrali

~ 19000 siti radio

~ 98.000 Cabinet x FTTC

Le sfide per le infrastrutture di telecomunicazione

Per la sicurezza delle infrastrutture occorre tener conto dei tre diversi contesti:

IT

- *Molti servizi di rete sono gestiti e controllati da sistemi IT.*
  Anche in ambito Telco questi servizi stanno migrando su infrastrutture Cloud.

- ***Minacce**: La migrazione verso infrastrutture Cloud espone le infrastrutture IT a nuove tipologie di minacce e l'estensione del perimetro IT ai Cloud Provider amplia la superficie d'attacco.*

Network

- *Il Telco ed in particolare la Rete è di fatto una delle **Infrastrutture Critiche** in grado di garantire il corretto funzionamento di numerose industrie (Energy, Utility, Finance…)*

- ***Minacce: resilienza** (attacchi DDoS), **intercettazione** delle comunicazioni, difficoltà nell'**individuazione e blocco del traffico malevolo** verso i clienti.*

Devices

- *Lo sviluppo dei device Mobili e la progressiva diffusione della **IoT** è la nuova frontiera dei servizi offerti dagli operatori Telco: **Smart Home, Smart Cities, Smart Industry, Automotive, …***

- ***Minacce:** i nuovi device IoT e i nuovi servizi che questi strumenti consentono di erogare sono largamente vulnerabili a diversi tipi di attacchi, la creazione della botnet MIRAI ne è la prova.*

Le infrastrutture evolvono grazie alle nuove tecnologie ….

Telco CLOUD

- Cloudcomputing
- Softwarizzazione delle funzionalità di rete (NFV&SDN)
- Piattaforme aperte (anche a SW di terze Parti) per la rapida implementazione di nuovi servizi

BIG DATA

Analisi dei dati real-time per ottimizzare l'esecuzione di servizi e per incrementare la capacità di previsione

IoT

Con l'incremento previsto di device M2M/IOT interconnessi, la maggior parte dei servizi (es. Smart Metering, Smart City, Connected Car) saranno senza interazione umana

MOBILITY

- Crescita esponenziale del traffico mobile
- Uso del terminale personale anche per il lavoro (BYOD)

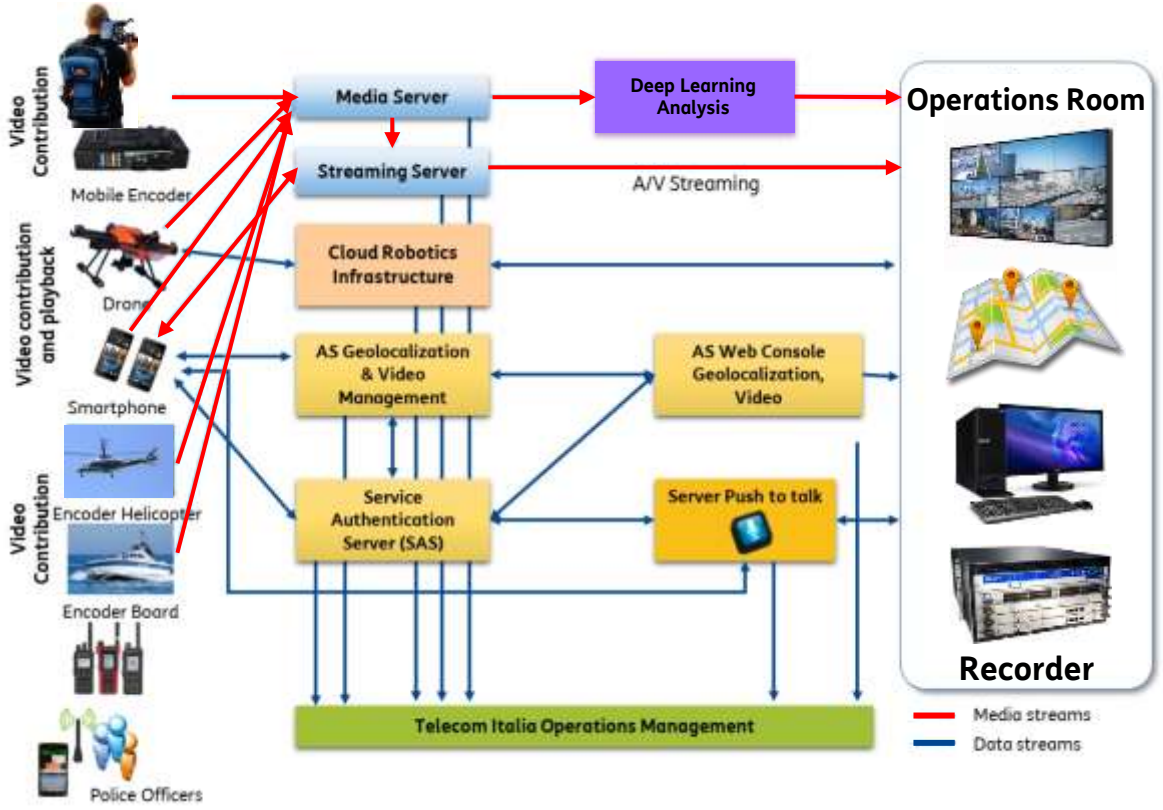
Nuove vulnerabilità e minacce dovute a: condivisione di risorse, servizi e funzionalità di rete, migrazione verso il paradigma «All IP», moltitudine di oggetti connessi che possono essere sia «target» sia «veicoli» di attacchi; disponibilità e gestione di molte più informazioni di rete da proteggere.

Necessità di aggiornamento dei modelli di protezione preventiva, monitoraggio e rapida reazione.

…. così pure le applicazioni, che si fanno sempre più «demanding»

non soltanto in termini di prestazioni prettamente tecniche (velocità, latenza, copertura), ma anche in termini di resilienza (business continuity) e sicurezza dell'informazione.

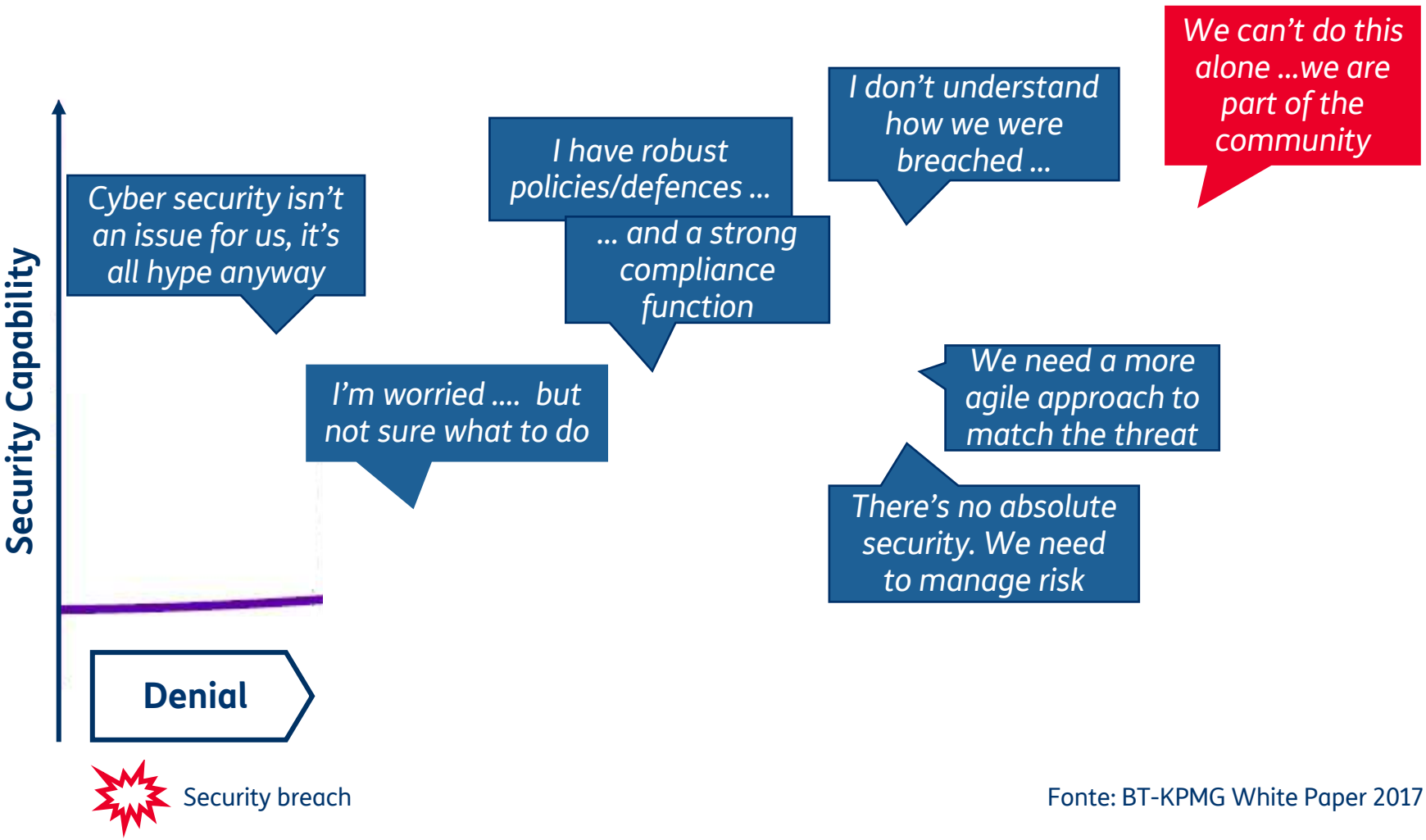
Ciò risulta particolarmente rilevante per l'applicazione, sempre più crescente, delle soluzioni tecniche (es. basate su LTE) e dei servizi (es. video, social media, cloud) nati per il mondo consumer anche ad ambiti con requisiti particolarmente stringenti di protezione cyber e di continuità di servizio (reti **mission-critical**), quali **Public Safety**, **Servizi di Emergenza**, **Controllo automatico del Traffico** e **Automotive**, **Industria 4.0**, **E-health**, …).



Architettura LTE PS (*)

(*) TIM è Partner Tecnologico della Polizia di Stato

La Sicurezza non è un progetto .....
è un percorso di continuo miglioramento!



Fonte: BT-KPMG White Paper 2017

Analisi del Rischio come step fondamentale per la protezione

La Cyber Security va intesa come un processo finalizzato alla protezione delle informazioni attraverso attività di prevenzione, rilevazione e risposta ad ***attacchi*** *provenienti dal cyberspazio (NIST)*

È l'insieme di attività, ruoli e responsabilità, approcci, metodologie e tecnologie, che aiutano ogni organizzazione a definire, implementare e migliorare costantemente una strategia di protezione adeguata a preservare tutto ciò che è dipendente dall'ICT e quindi **vulnerabile** e a **rischio**

Obiettivo: assicurare l'integrità e la difesa dalle **minacce** interne ed esterne con un approccio olistico

L'Analisi del Rischio consente di identificare e misurare il rischio associato ad un contesto tecnologico su cui incidono vulnerabilità e minacce che se attivate possono causare un danno e relativo impatto

Due tipici approcci alla protezione da attacchi cyber

Incidente di sicurezza

PROTEZIONE PREVENTIVA

Proteggere i sistemi mediante l'analisi del rischio e l'implementazione delle contromisure, verificandone la corretta esecuzione. Le contromisure in fase preventiva si estendono dalla fase di progettazione/sviluppo (**security by design**) a quella di esercizio (**monitoraggio continuo**)

PROTEZIONE REATTIVA

Cercando di minimizzare gli impatti a seguito di un incidente di sicurezza. Il **rischio residuo** derivante dalla implementazione delle contromisure in fase di test, infatti, non va considerato nullo.

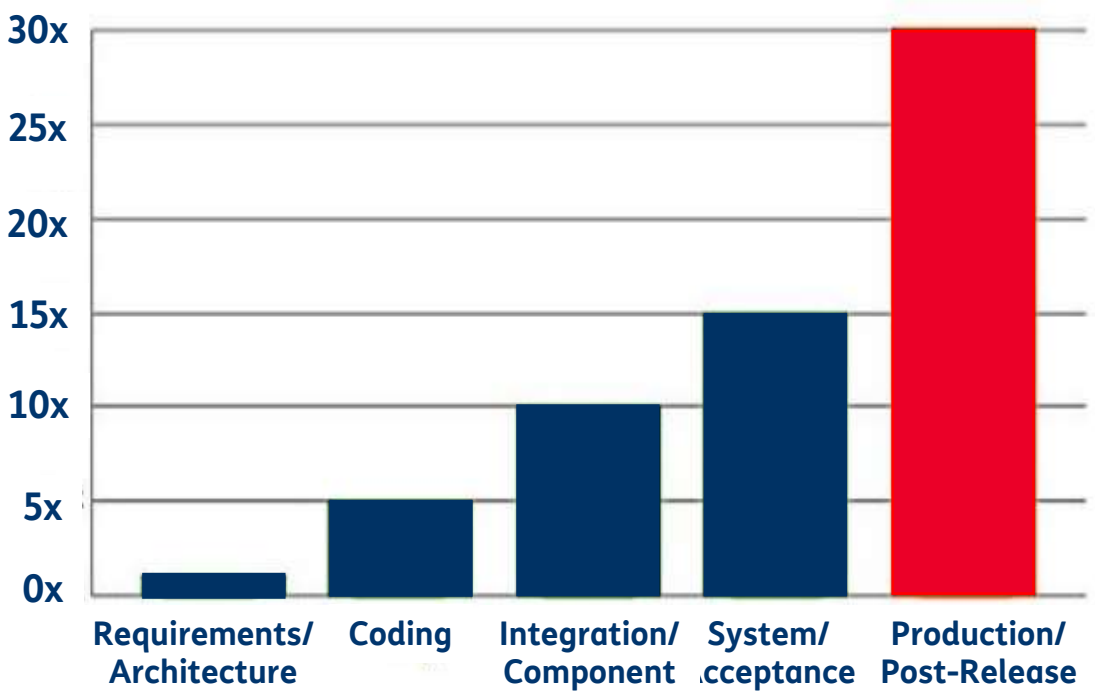
E' dunque necessario dotarsi di tutte le misure adeguate per reagire ad un eventuale incidente che vada ad insistere proprio su quel rischio specifico.

Attaccare è facile, difendersi è molto più complesso. È dunque necessario un approccio organizzativo security-oriented, in cui tutte le varie unità hanno uno specifico ruolo all'interno del processo e l'intera organizzazione è coinvolta nella gestione degli incidenti di sicurezza

L'importanza di intervenire in fase di progettazione

Progettare infrastrutture **nativamente sicure** garantisce una **maggiore efficacia** rispetto all'add-on delle contromisure su sistemi già rilasciati.

E' **economicamente più efficiente** rimuovere le vulnerabilità in fase di progettazione anziché gestirle in fase di esercizio.



The Economic Impacts of Inadequate Infrastructure for Software Testing (NIST)

*Esempio: ciclo di vita del **Software***

L'effort per la risoluzione di bug da sw già rilasciato incrementa in modo considerevole al susseguirsi delle fasi del ciclo di vita.

Come ci si protegge? Lavorare sui tre pillar fondamentali

- Security awareness
- Competenze chiave
- Formazione ed esercitazioni

- Analisi e valutazione rischio
- Monitoraggio
- Rilevazione e risposta
- Quadro normativo/procedurale

- Capacità di prevenzione, rilevazione e contrasto
- Soluzioni innovative per la Cyber Security
- Presidiare ambiti strategici (come 5G, UBB fisso, IoT)
- Presidio dell'evoluzione delle Minacce e Cyber Info-Sharing

Come ci si protegge? Il Framework Nazionale per la Cyber Security

Il **Framework Nazionale per la Cybersecurity,** allineato al *Framework for Improving Critical Infrastructure Cybersecurity* del NIST prende in considerazione tutti gli aspetti rilevanti (presidio organizzativo, ruoli, skills, processi e sistemi/soluzioni) e garantisce l'**adozione di un approccio coerente con la gestione del rischio cyber**.

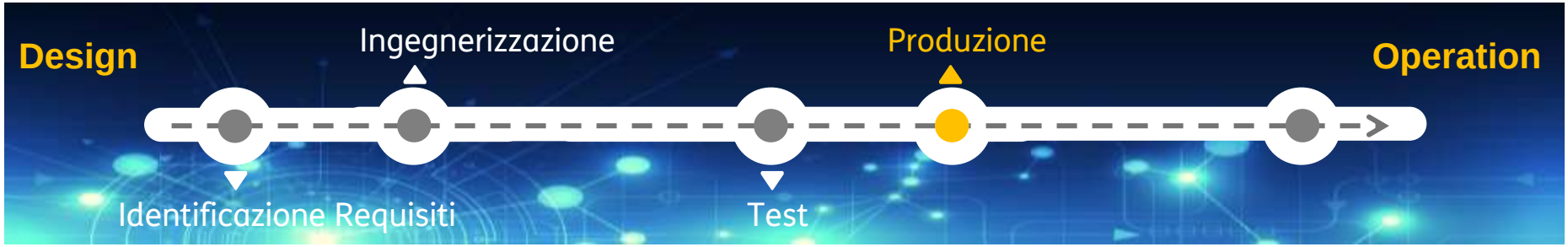
Si considera tale Framework come riferimento per la sua **diffusione, attualità e aderenza per le Infrastrutture Critiche**

Identify	Protect	Detect	Respond	Recover
Acquisire una conoscenza approfondita della organizzazione e asset per gestire efficacemente i rischi cyber sui sistemi, i dati e le competenze	Sviluppare e implementare adeguati meccanismi di difesa per assicurare la continuità operativa dei servizi erogati da infrastrutture critiche	Sviluppare e implementare le opportune attività per identificare possibili eventi di sicurezza	Sviluppare e implementare le opportune azioni di risposta a seguito di un evento di sicurezza	Sviluppare e implementare adeguati piani di resilienza e di ripristino del servizio a seguito di un evento di sicurezza

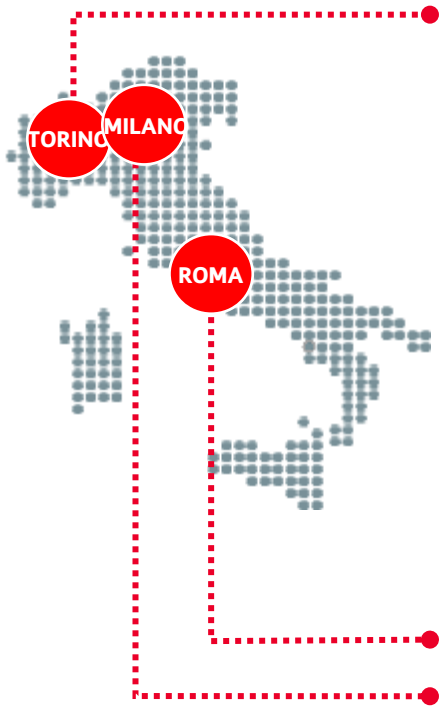
Applicazione dei principi del framework nella produzione di tecnologie

Un produttore di servizi e prodotti tecnologici implementa il framework di sicurezza dalla realizzazione sicura dei propri prodotti (software, servizi, infrastrutture tecnologiche) fino al suo esercizio attraverso un monitoraggio continuo

Security by design	Security Validation	Security Monitoring
Analisi delle minacce Analisi dei rischi Requisiti di sicurezza Sviluppo sicuro	Accertamento su presenza contromisure	Rilevazione e gestione eventi di sicurezza
Identify, Protect	Protect, Detect	Detect, Respond, Recover



Presidi TIM - Centri di competenza per la sicurezza logica



Security Lab

- Presidia l'**evoluzione delle minacce** con attività di **threat intelligence**
- Studia **soluzioni innovative** per la cybersecurity e identifica le **soluzioni di sicurezza** più idonee alle esigenze del Gruppo
- Svolge attività di **security testing** su apparati, dispositivi, soluzioni e piattaforme di sicurezza
- Partecipa ai **programmi di ricerca** della UE
- Sviluppa una **rete di relazione internazionale** con gruppi di standardizzazione, mondo open-source, Università, Vendor e altri Operatori

SOC Security Operation Center

- Presidia il **monitoraggio 24x7 della sicurezza** delle Reti Pubbliche di Telecom Italia, dei Data Center, delle Reti Di Gruppo, dei PC e dei Server
- **Centro integrato** che somma le funzionalità di CERT e di SOC
- E' in **continuo e stretto contatto** con tutte le Operations di TIM
- Collabora con realtà CERT/SOC nazionali e itz

3,4 Tbit/s
di traffico analizzato statisticamente per rilevazione DDoS

415.000
query/s DNS analizzate statisticamente

6.000
dispositivi di rete IP con configurazione sicura e controllata

168.000
identità

1.800
apparati di rete più critici monitorati

10.000
apparati di rete con accesso tramite AAA

79.000
PC/Server protetti con antivirus

Presidi TIM - Best practice tecniche e processive

TIM in coerenza con quanto ridefinito di recente dal **DPCM di Febbraio 2017** (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali) e in attesa della definizione del quadro normativo di riferimento - **recepimento Direttiva NIS** (Network Information Security) e del **Decreto Attuativo per la D.Lgs 70/2012** incentrata sulla Resilienza degli operatori TLC

Utilizza le Linea Guida di ENISA come riferimento per gli obiettivi di controllo, le misure e **Best Practice** da adottare per valutare, raggiungere e monitorare la conformità al D.lgs 70/2012 (resilienza)

Continua evoluzione **di un'estesa infrastruttura di sicurezza** costituita da contromisure che operano a **livello di rete** e da contromisure attive sui **singoli sistemi o infrastrutture**

Collabora con gli **Organi preposti al contrasto delle minacce cyber** (Cert Nazionale, DIS e CNAIPIC), con partecipazione strutturata a iniziative quali "Tavolo delle Imprese" c/o DIS e "Tavolo tecnico" c/o Cert-Nazionale

Ha in essere un insieme di **flussi di comunicazione con le Istituzioni** utilizzati anche per la gestione di eventi significativi di sicurezza cyber

Conclusioni (1/2)

Il modello di business delle Telco va sempre più trasformandosi da un **modello chiuso** ad un **modello aperto**, volto a soddisfare la customer experience, la diffusione di nuovi contenuti e servizi e la crescita esponenziale del traffico dati

NFV + SDN

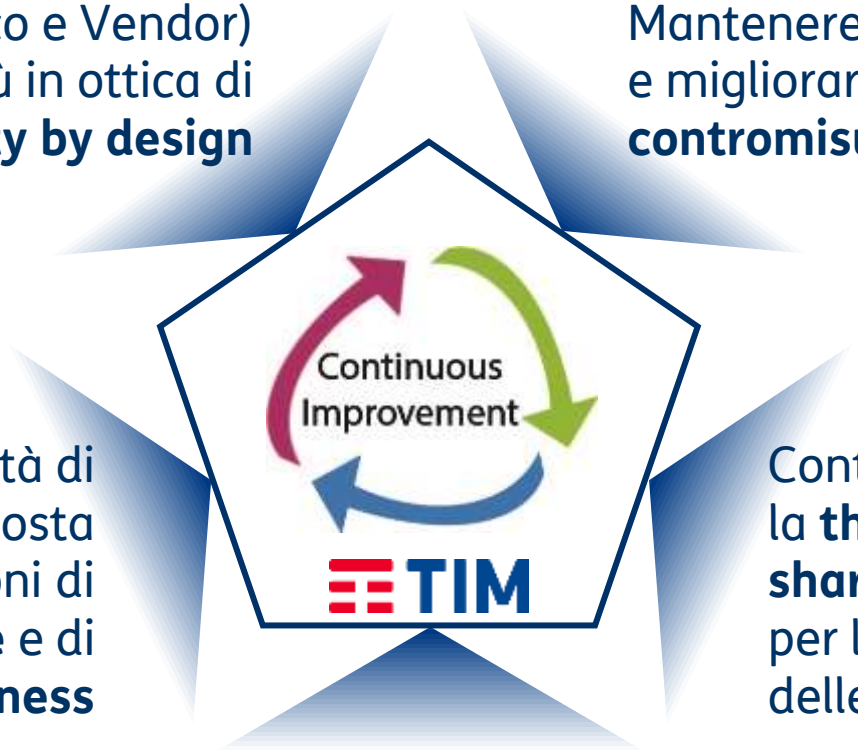
Le nuove tecnologie come il **Telco Cloud**, i **Social Media** e i **Big Data** faciliteranno la transizione da soluzioni di rete ove solo le persone sono connesse a quelle in cui le comunicazioni riguarderanno anche gli oggetti verso le persone e gli oggetti verso gli oggetti

D'altra parte:
l'abbattimento del costo computazionale necessario per effettuare gli attacchi e la **diffusione/disponibilità di strumenti** abbassano notevolmente gli skill necessari ad effettuare gli attacchi che possono trovare maggiore diffusione anche grazie alla introduzione delle nuove tecnologie, della sempre **maggiore IP-zzazione** e di nuovi modelli di business (ad es legati a 5G, IoT,...)

Conclusioni (2/2)

Operare (Telco e Vendor) sempre più in ottica di **security by design**

Mantenere/rafforzare **controlli** e migliorare **l'efficacia delle contromisure**



Evolvere le capacità di rilevazione e di risposta attraverso soluzioni di **security intelligence** e di **context awareness**

Continuare a potenziare la **threat intelligence e lo sharing di informazioni** per l'identificazione rapida delle nuove minacce

Sviluppare **soluzioni innovative** e **adeguare le soluzioni tecnologiche** a protezione da minacce «nuove» e da quelle «tradizionali»

occorre farsi trovare sempre <u>pronti</u>,
ricordando che ….

Proverbio malese

“Solo perché il fiume è tranquillo non significa che siano andati via….
… i coccodrilli !”

Grazie

sandro.dionisi@telecomitalia.it

TIM

Back up

CyberAttack: diverse motivazioni ma un contesto (*il CyberSpace*) e strumenti di lavoro comuni (*Trojan, BotNet,...*)

MOTIVAZIONE ATTACCO	DESCRIZIONE	ESEMPI DI VIOLAZIONE/ABUSO
CYBER CRIME	• interessi **personali** o scopi **criminali** • raggiungimento di un **profitto economico**	• Truffe telematiche, • Ransomware; • Frodi bancarie operate su canali web e Mobile
CYBER ATTIVISMO	• **motivazioni socio-politiche;** • Finalità di **protesta** e/o **attenzione** su specifiche tematiche	• Denial of Service (DoS); • Raccolta illecita (mediante attacchi APT) e diffusione di Dati e Informazioni classificate • Defacing di siti Web
CYBER SPIONAGGIO	• Operazioni di **intelligence** • scopo di ottenere l'**accesso a informazioni riservate, sensibili e strategiche**	• Raccolta informazioni aziendali segrete; • Intercettazione comunicazioni telematiche (comunicazioni, messaggi, uso dei sistemi Social)
CYBER WARFARE	• Attacco informatico effettuato da parte di uno **stato nei confronti di un altro**	• Danneggiamento di sistemi informatici militari o dalle aziende responsabili di servizi infrastrutturali (acqua, luce, telecomunicazioni)

Un estratto degli strumenti usati dalle comunità criminali

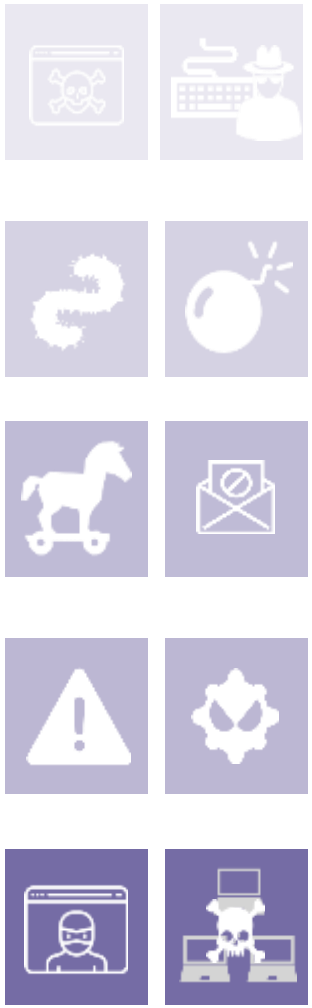
Virus
Malware che una volta attivato è in grado di replicarsi e infettare sistemi operativi, file e singoli documenti.

Worm
Malware auto-replicabile in grado di auto-propagarsi e infettare tutti i sistemi connessi su una stessa rete.

Trojan
Malware impiegato per effettuare intercettazioni, rubare informazioni sensibili ed effettuare operazioni sui sistemi.

Vulnerabilità 0Day
Vulnerabilità di applicazioni non ancora divulgate o per le quali non è ancora stata distribuita una patch.

Exploit
Esecuzione di codice malevolo che sfrutta una o più vulnerabilità con lo scopo di acquisire privilegi amministrativi



Keylogger
Strumento in grado di intercettare, in forma nascosta, le digitazioni effettuate sulla tastiera del dispositivo.

DDoS
Attacco mirato a rendere indisponibile un servizio mediante un sovraccarico di richieste verso il sistema target.

Spam
Comunicazioni indesiderate e ripetute da parte di mittenti sconosciuti usati anche per diffondere malware.

APT (Advanced Persistent Threat)
Attacco di difficile identificazione finalizzato a guadagnare punti di accesso a una rete per un lungo periodo di tempo.

Botnet
Rete di computer “zombie” infettati da un malware e controllati in via remota e nascosta da un attaccante.

Alcuni dei *cyber attack* più rilevanti degli ultimi anni

#CyberWarfare

Worm

Stuxnet

Primo attacco rilevante sferrato nei confronti di Sistemi di Controllo Industriali **38K di macchine infette** (22K erano in Iran)

#CyberCrime

JPMorgan &Chase

Data Breach che ha compromesso dati dei client per **83Mln di accounts**

Data Breach

#CyberActivism

APT

Sony

Costi per le indagini e di rimedio per un ammontare di **$15Mln**

... to be continued

2010 2013 2014 2015

#CyberCrime

Adobe

;

Data Breach che ha compromesso **2.9Mln of IDs**

Data Breach

#CyberCrime

Data Breach

Target

Data Breach che ha compromesso **più di 40Mln di carte di credito**

#CyberWarfare

APT

Black Energy

Trojan sferrato nei confronti di tre centrali elettriche in Ucraina che ha disabilitato il servizio eletrico in **centinaia di migliaia di abitazioni** per molte ore

La rete di telecomunicazione può essere oggetto di varie tipologie di Rischi Cyber

Servizi Infrastrutturali

- **Garanzia** della **continuità del servizio** (es. attacchi **DDoS** in particolare su servizi come DNS)
- Esposizione ad **attacchi** anche molto **semplici** come ad es. **Mirai**

SS7 Rete di Segnalazione

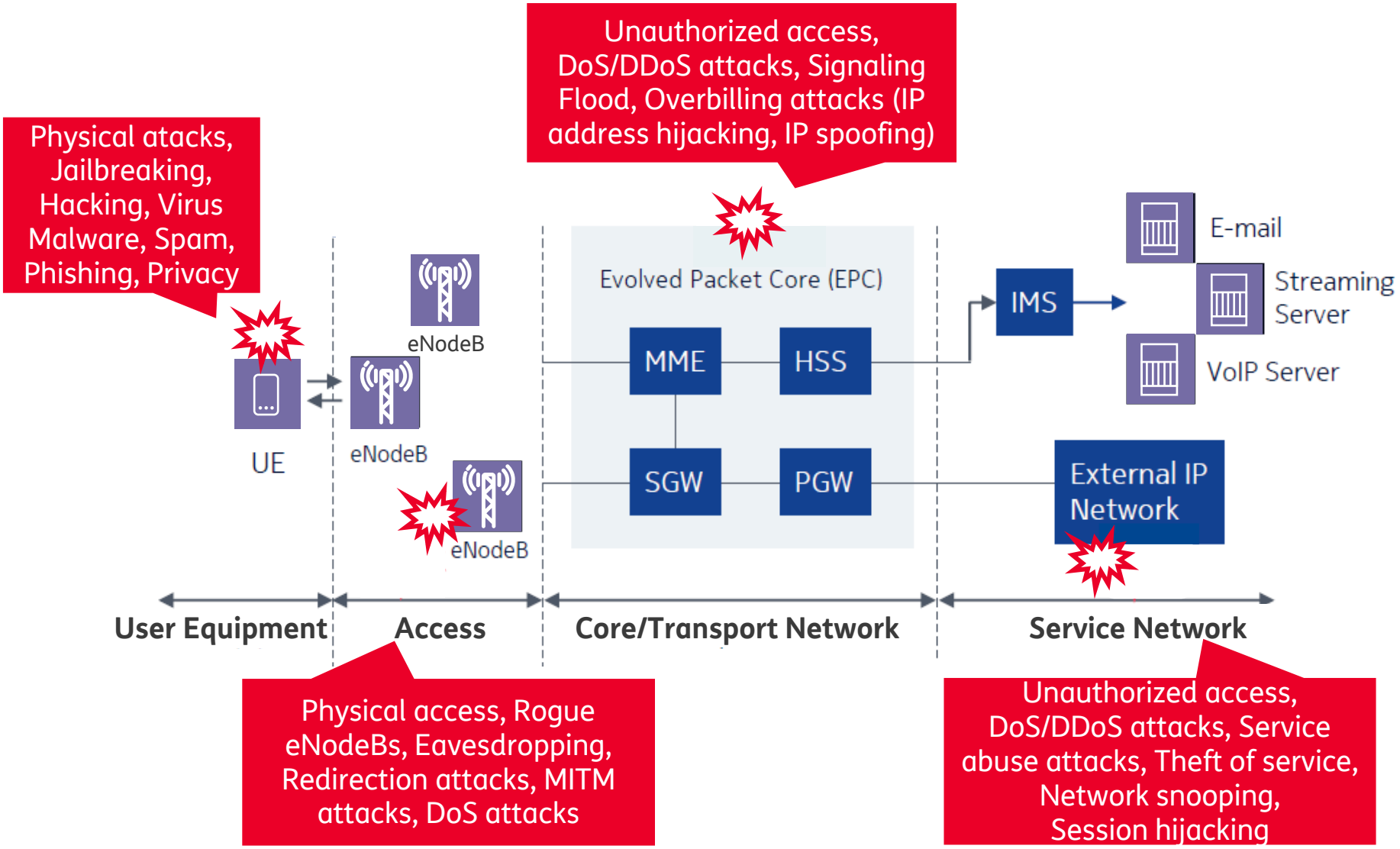
- Le **architetture ed i protocolli esistenti** lasciano aperte delle **vulnerabilità sulle comunicazioni** degli utenti
- A rischio sia le **comunicazioni** sia i **dati** utilizzati per abilitare i servizi di autenticazione (es. attacchi a Whatsapp e Telegram)

Network

Accesso

- La **maggiore accessibilità** determina una **maggiore superficie di esposizione** e **maggiore vulnerabilità**
- Nella Smarthome questi dispositivi saranno **gateway di decine di oggetti per user**
- Componente di **architettura IoT** più vicina all'**end user** (più esposto a **botnet ed agenti con worm**)

Possibili punti di attacco ad una rete di telecomunicazione: esempio 4G



Anche il comportamento umano può incrementare i rischi