

CYBER RISK

Le nuove minacce connesse alla rivoluzione digitale e le risposte del mercato assicurativo

Ascoli Piceno – 10/05/2018

Relatore: Igor Poletti – Responsabile Tecnico Ariostea Broker S.r.l.

Premessa

Hardware o dati?

Nell'era di massima diffusione della *office automation* Risk Manager, Esponenti Aziendali e Broker hanno concentrato le proprie attenzioni su strumenti di tutela dedicati all'hardware, inteso come contenitore/elaboratore dei dati, e la stessa impostazione della polizza Elettronica ricalcava questo sentimento diffuso.

Server, workstation e laptop avevano costi non trascurabili per le aziende e periodi di ammortamento lunghi, per cui il vero rischio era rappresentato dalla perdita della macchina, più che dalla ricostruzione del dato.

La rivoluzione digitale ha cambiato le regole del gioco ed il dato è diventato più importante dell'hardware.

I Cyber Risk sono oggi in cima alle preoccupazioni dei Risk Manager, le grandi multinazionali dispongono di programmi assicurativi già orientati in tal senso, ma sussistono ancora grandi differenze tra USA ed Europa e la domanda di copertura tra le aziende medio-piccole non è ancora decollata.

Il mercato assicurativo si trova in una fase di transizione, dovendo adeguare la propria visione ed adattare l'offerta di prodotti ad un mondo in continua evoluzione.

Cyber Security

Non esiste ad oggi una definizione esaustiva di Cyber Security, al contrario è invece certo quello che dovrebbe essere il suo scopo ovvero:

*«proteggere tutti quegli **asset materiali ed immateriali** che possono essere aggrediti tramite il “cyberspazio” ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l’assurance e la business continuity di tutta l’infrastruttura digitale a supporto»*

Ciò che certo è che assicurati ed assicuratori si trovano di fronte ad un rischio nuovo ed emergente con poco più di 30 anni di storia alle spalle.

Rischio nuovo - Hostcount

«Il Cyber Risk si è evoluto insieme ad internet»

Con il termine host (nodo ospitante) si intende ogni terminale collegato, attraverso link di comunicazione, ad una rete informatica.

Nel 1981 gli host connessi erano 213

DAL 2000 AL 2013

109,574 
numero host connessi

1,000,000,000 
numero host connessi

2017

7,500,000,000 
Popolazione mondiale

3,700,000,000 
Persone connesse a internet

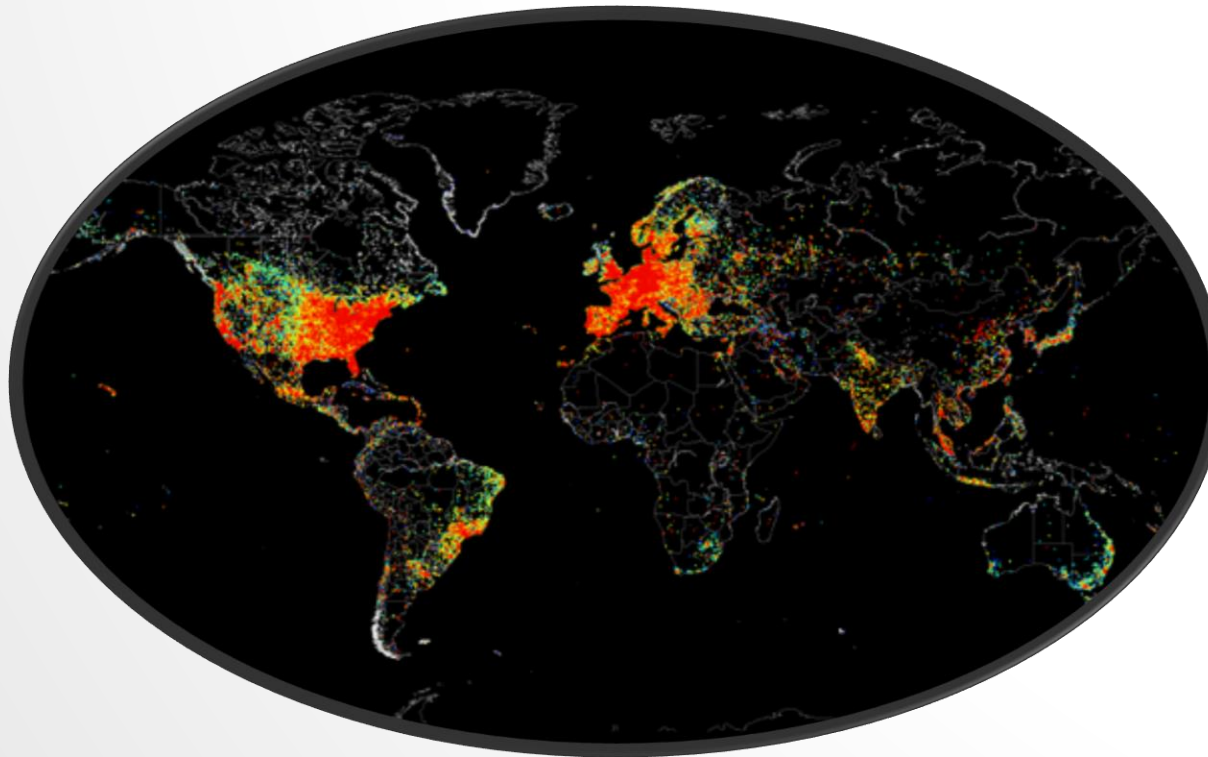
Una crescita esponenziale così rapida ha fatto emergere livelli di vulnerabilità spesso sottovalutati

Il rischio Cyber è globale

Il rischio cyber è potenzialmente pandemico?

Il livello di interconnessione di device nel mondo rende il rischio Cyber globale perchè la velocità di connessione ed il numero di host amplificano il rischio di propagazione delle minacce attraverso la rete.

La concezione di rischio catastrofale non è più legata alla distanza degli enti, ma alla velocità delle infrastrutture digitali che consentono la connessione di diversi Host



Le zone a maggior concentrazione industriale sono quelle più esposte. La figura è la rappresentazione grafica di un ping lanciato da una macchina verso un numero indefinito di dispositivi connessi alla rete.

Una stessa singola minaccia cyber può colpire indifferentemente host collocati a decine migliaia di km di distanza gli uni dagli altri.

Definizione di rischio Cyber

Cyber Risk

Definire i rischi di tipo Cyber è semplice, perché se ne individua immediatamente il contesto, ma complesso vista e considerata la loro molteplicità e natura mutevole.

L'approccio alla valutazione ed individuazione della effettiva esposizione a rischi Cyber in una qualsiasi organizzazione deve essere di tipo «olistico», non potendosi fermare ad una analisi dei singoli processi interessati, ma dovendo piuttosto coinvolgere risorse tecniche, umane e fisiche per individuare, prevenire e correggere fattori di vulnerabilità verso i rischi Cyber.

L'ambiente nel quale si concretizza un cyber risk non è fisico, è logico, e questo elemento rende più difficile non solo la prevenzione, ma anche la gestione dell'emergenza, perché spesso quando l'evento si manifesta si è già del tutto consumato.

Il problema del mercato assicurativo è sostanzialmente quello di valutare la sottoscrizione del rischio Cyber secondo gruppi di elementi quali:

Aspetti attuariali

Fattori che determinano le condizioni alle quali un assicuratore può assumere assumere rischio

Aspetti di mercato

Fattori che influenzano la possibilità di proporre il rischio al mercato

Aspetti sociali

Fattori che condizionano la possibilità di proporre la copertura al mercato

Aspetti attuariali, di mercato e sociali

Aspetti attuariali

Criteri	Caratteristiche
Rischio/Incertezza	misurabile
Occorrenza dei danni	indipendente
Danno massimo	gestibile
Danno medio	moderato
Frequenza dei danni	elevata
Rischio morale/selezione avversa	non eccessivi

Aspetti di mercato

Criteri	Caratteristiche
Premio assicurativo	appropriato
Limiti di copertura	accettabili
Capacità del settore sufficiente	gestibile

Aspetti sociali

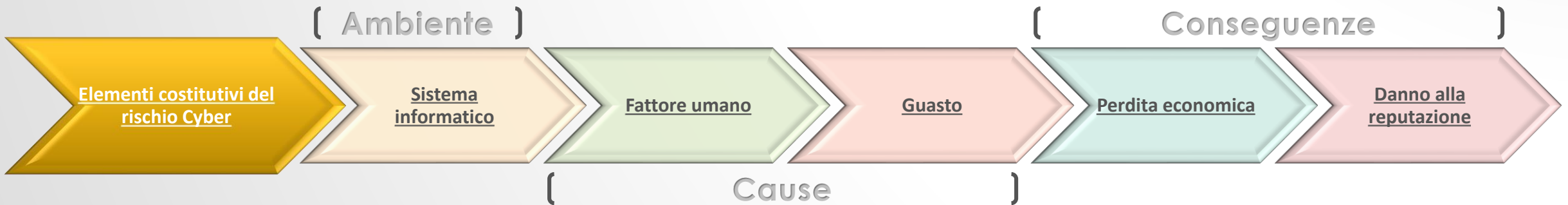
Criteri	Caratteristiche
Sistema pubblico	coerente
Sistema legale	permissivo

.....con quali conseguenze

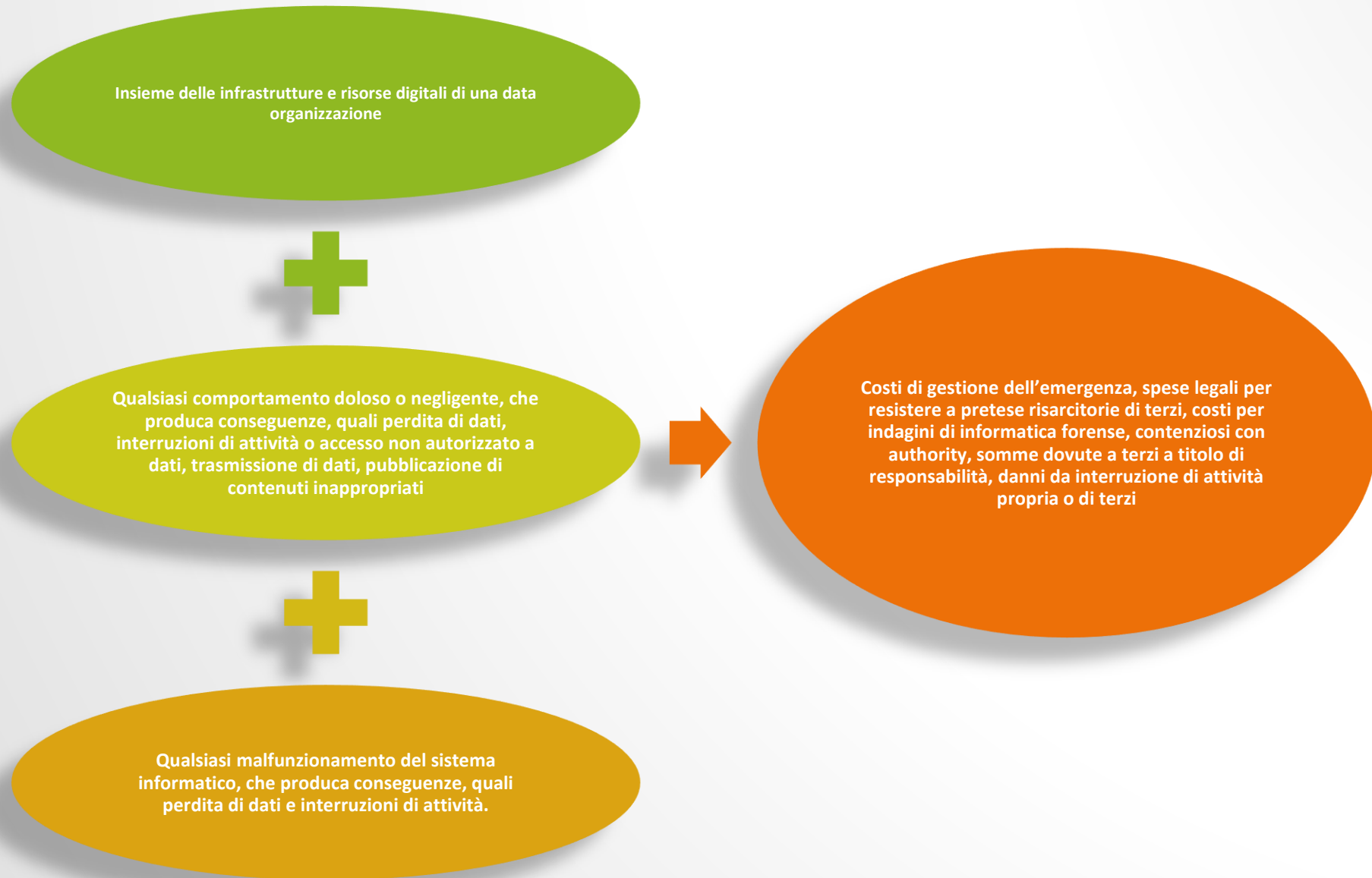
Aspetti attuariali	Fattori critici	Fattori moderati
	<u>Problemi di natura informativa</u>	<u>Rischio morale</u>
	<u>Complessità dei rischi ceduti</u>	<u>Prevenzione</u>
	<u>Rapida evoluzione dei rischi</u>	
	<u>Rischi emergenti</u>	
	<u>Esposizione occulta</u>	
	<u>Interdipendenza</u>	
Aspetti di mercato	Fattori critici	Fattori moderati
	<u>Carenza di riassicurazione</u>	<u>Massimali</u>
		<u>Scarsa diffusione</u>
Aspetti sociali	Fattori critici	Fattori moderati
	<u>Restrizioni legali</u>	<u>Frodi</u>

Elementi costitutivi di un Cyber Risk

Per rischio Cyber si intende qualsiasi rischio di perdita finanziaria, disturbo o danno alla reputazione di un'organizzazione in conseguenza di guasto dei suoi sistemi informatici.



Manifestazione di un Cyber Risk



Non solo «Cyber»

«conosci te stesso»

Vulnerabilità infrastrutture IT

La vulnerabilità delle infrastrutture informatiche è spesso legata ad una carenza di conoscenza del sistema di funzionamento o ad una sua crescita non controllata. Si tratta di un problema che affligge sia le organizzazioni medio piccole che quelle di grandi dimensioni. Se in casa lasciamo una porta o una finestra aperta questa vulnerabilità è visibile, non altrettanto si può dire per un device connesso alla rete, qui le porte aperte sono decine, ma non ce ne accorgiamo.

Vulnerabilità Risorse Umane

Un altro potenziale punto di debolezza è costituito dalle risorse umane in organico. Molti degli attacchi vedono utilizzate tecniche di social engineering, situazioni nelle quali per il completamento dell'attacco vengono impiegate tecniche psicologiche per cercare di ottenere informazioni od istigare le vittime a comportamenti vantaggiosi per l'attaccante.

Nel processo di individuazione e classificazione della vulnerabilità di una organizzazione (vulnerability assessment) è estremamente importante identificare anche la presenza di elementi critici nell'ambito delle gerarchie di accesso alla piattaforma IT.

L'orientamento del mercato assicurativo

Il mercato assicurativo fornisce risposte differenti, ma con due approcci ben distinti nella classificazione dei prodotti

Danni propri (First Party Damages)

Danni a terzi (Third Party Damages)

Le competenze richieste al mercato per la sottoscrizione dei rischi spesso riguardano differenti linee di business

Prodotti Multiline

Infedeltà/Crime

Polizze di responsabilità civile

D&O/E&O

Copertura spese legali

Property

RC professionali

Lo standard di offerta che si sta consolidando è quello di polizze modulari – stand alone che offrono un buon livello di copertura sia per quanto riguarda i danni propri che i danni a terzi.

Le polizze modulari

Un evento Cyber potenzialmente può generare:

- Perdite patrimoniali dirette
- Maggiori costi
- Perdite patrimoniali dovute ad interruzione di attività
- Responsabilità civile verso terzi
- Costi di emergenza
- Costi di difesa

La polizza Cyber presenta tendenzialmente una struttura modulare, articolata su differenti sezioni di garanzia, che variano a seconda della Compagnia ma che sostanzialmente sono riconducibili alle seguenti aree:

Area Responsabilità civile

Privacy

Responsabilità da Media

Area Perdite patrimoniali dirette

Danni da interruzione di esercizio

Cyber Extorsion

Area costi per gestione eventi

Costi per mitigazione

Incident Response

Spese legali

Le caratteristiche delle polizze modulari










Processi esposti a rischi Cyber






Sono comunemente esposte al Cyber Risk le organizzazioni che integrano i seguenti processi/servizi nel proprio ambito, indipendentemente da quale che sia il settore di riferimento:








Cyber Risk – Fattori di rischio e cattive abitudini

-  Spending review in strutture ICT
-  Scarsa alfabetizzazione informatica delle risorse umane
-  Assenza di policy (scritte o meno) interne in materia di sicurezza ICT
-  Ampio utilizzo di programmi freeware o di dubbia provenienza
-  Utilizzo dei propri account social su macchine collegate in rete aziendale
-  Gestione «libertina» delle password
-  La sindrome del «doppio click».....

Pillole Cyber Risk (USA)

-  Il costo medio di ripristino in seguito ad un attacco Cyber è di 690.000 \$ per small business ed oltre \$ 1.000.000 per aziende medium-sized business
-  Si stima che il 60% delle aziende colpite da un Cyber attack chiudano entro 6 mesi dall'evento
-  In USA chi rinnova o sottoscrive una polizza CR cerca sostanzialmente copertura per data breach , Cyber Extortion e sanzioni comminate da Regulator di settore
-  Preferibilmente si acquista una copertura stand alone, per il segmento small business molti sottoscrittori offrono estensioni su altre polizze
-  Il principale ostacolo per la diffusione di queste polizze viene individuato nella carenza di comprensione del testo di polizza

Pillole Cyber Risk (Italia)

-  La diffusione di coperture è limitata al 5% delle aziende
-  Il 40% delle imprese italiane ha subito un evento negli ultimi 5 anni
-  Furto di dati dei clienti ed interruzione di esercizio sono percepiti come gli eventi a maggior impatto potenziale
-  Meno del 60% delle imprese hanno implementato audit per il controllo della vulnerabilità
-  Almeno il 70% delle aziende concordano sul fatto che un malfunzionamento del sistema IT impatterebbe in modo trasversale molteplici processi aziendali (produzione, logistica, acquisti, vendita)

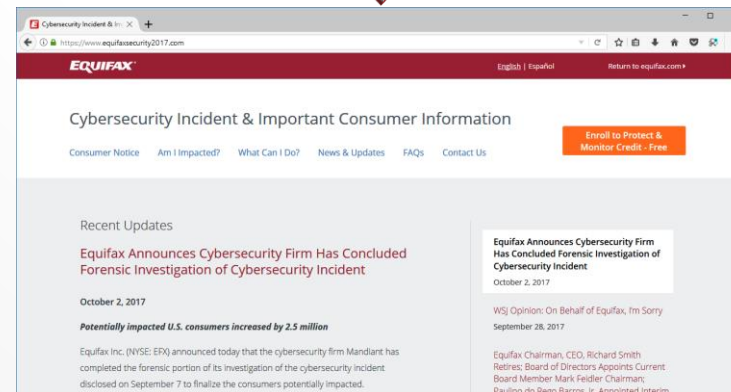
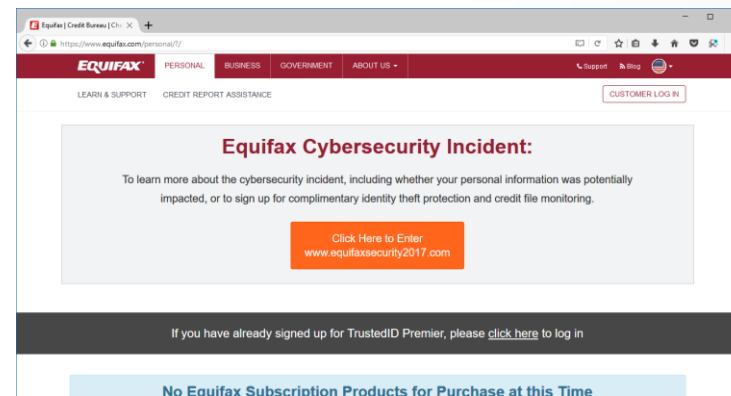
Case History

Merck, multinazionale settore del settore farmaceutico e life science è stata colpita nel mese di giugno 2017 da ransomware (Not Petya) che ha di fatto bloccato tutte le postazioni di lavoro.

L'impatto economico del danno è stimabile in circa 275 mln €, di cui 135 di mancati guadagni (previsione di Verisk Analytics PCS)

NOT PETYA è un software di tipo «ransomware» che dopo la sua installazione blocca la macchina chiedendo un riscatto. Il software è in grado di diffondersi autonomamente in un sistema. L'infezione avviene attraverso una mail con allegato apparentemente innocuo (.doc, .xls, .ppt) che una volta aperto avvia un «dropper», ovvero un programma che scarica il «malware» vero e proprio nella macchina e la infetta.

Equifax è una delle tre principali agenzie USA di monitoraggio dei crediti «consumer» è stata oggetto di un attacco Hacker iniziata nel maggio 2017, ma scoperta solo al termine di luglio e resa di pubblico dominio all'inizio di settembre. Circa 145 milioni sono stati gli utenti interessati.



Underwriting e mercato

Russ Johnston, CEO of QBE North America, noted, "Most major cat exposures tend to have a season. To the extent you have sophisticated models, the market can expect events and project magnitudes. Cyber does not have a season and can cross multiple lines of business and customer segments."

Pat Ryan CEO of Ryan Specialty Group "These two claims [Merck and Equifax] illustrate how vulnerable the market is to cyber losses and how huge the losses can be, especially as the plaintiffs' bar will try to wrap as many parties as possible into them,"

La vulnerabilità del mercato assicurativo è sintetizzabile in due concetti:

- Diverse LOB potenzialmente interessate da un unico evento
- Esposizione catastrofica non correlabile e fortemente influenzata da elementi soggettivi

2015

\$ 1.000.000.000

2016

€ 1.350.000.000

2017

\$ 2.000.000.000

Stima 2027

\$ 20.000.000.000

Dei rischi sottoscritti oggi a livello mondiale la quota USA di mercato è stimabile approssimativamente nel 90%

Cyber Crime – i settori più colpiti

Attaccati

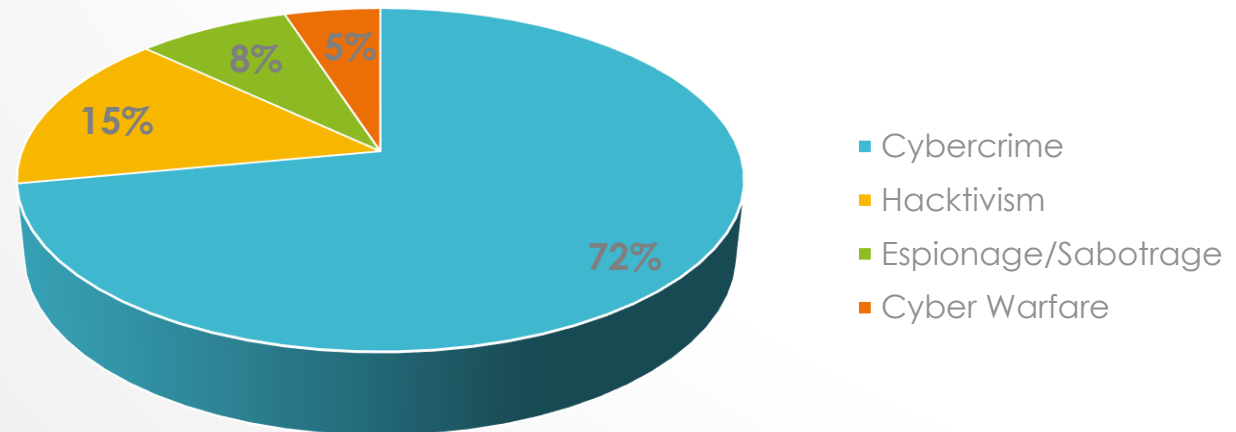
- Sanità (+102% cyber attack nel 2016)
- GDO (+70% cyber attack nel 2016)
- Financial Institutions (+64% cyber attack nel 2016)
- Infrastrutture «mission critical» (+15% cyber attack nel 2016)

In generale aumentano gli attacchi con finalità Cybercrime del 9,8% e del 117% quelli con finalità Cyber Warfare

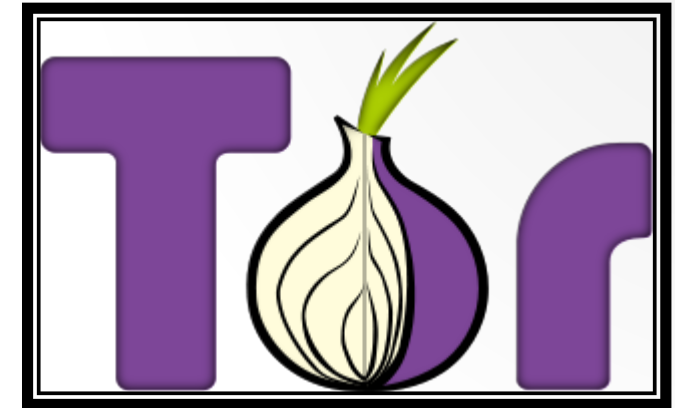
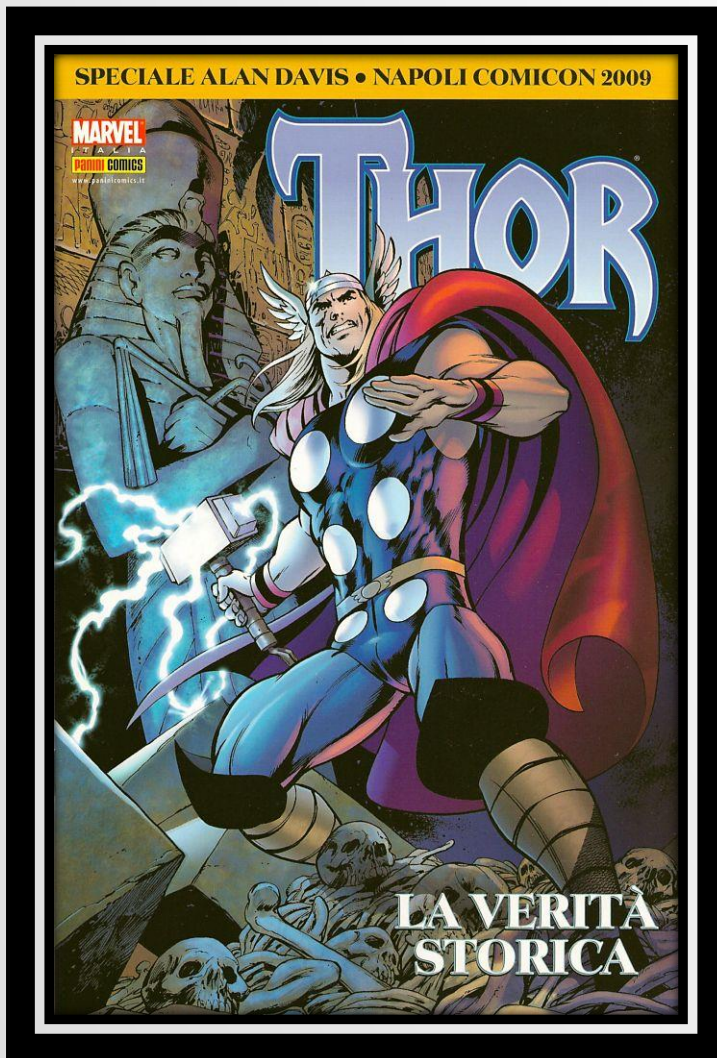
Aumento del 1.166% di attacchi basati su tecniche Phishing e Social Engineering.

+116% per malware

Attaccanti



Hacker e dintorni



TOR è l'acronimo di **The Onion Router** ed è un sistema di comunicazione attraverso internet basato su protocollo di rete di seconda generazione (Onion Routing).

La caratteristica di questo protocollo è quella di rendere anonime le comunicazioni attraverso i nodi che compongono la rete TOR (detti onion router), utilizzando un sistema di crittografia che consente a ciascun nodo di scoprire solo la posizione precedente e quella successiva del pacchetto di dati.

TOR è una darknet, ovvero una rete *navigabile* solo mediante l'impiego di un browser dedicato, altri esempi di darknet sono Freenet e I2P. Si tratta spesso di reti sperimentali o progetti accademici, alimentate dagli utenti, che rendono anonimi e garantiscono dalla censura.

Da dove nascono le minacce «I Black Market»

Tramite rete TOR è possibile accedere ai cosiddetti black market (Abraxas, Agora, Outlaw, Italian Darknet Community), siti nei quali è possibile acquistare software predisposto per perpetrare attacchi di tipo Cyber.

Le stime dei volumi di affari medi giornalieri calcolate su 35 black market ammontano circa € 300-500.000 al giorno

Listino prezzi

✓ <i>Record con informazioni personali di un utente</i>	<i>\$ 1</i>
✓ <i>Account Pay Pal e eBay</i>	<i>\$ 300</i>
✓ <i>Account per online banking</i>	<i>a partire da \$ 200</i>
✓ <i>Scansioni di documenti di identità (falsi)</i>	<i>da \$ 10 a \$ 35</i>
✓ <i>Documenti contraffatti</i>	<i>da \$ 200 a \$ 1.000</i>
✓ <i>Hacking di un account social</i>	<i>da \$ 200 a \$ 1.000</i>
✓ <i>Patente USA (falsa)</i>	<i>da \$ 100 a \$ 150</i>
✓ <i>Remote Access Trojan</i>	<i>da \$ 150 a \$ 400</i>
✓ <i>Source code di malware bancario personalizzato</i>	<i>da \$ 900 a \$ 1.500</i>
✓ <i>Noleggio di una Botnet per attacco DDoS (24h)</i>	<i>\$ 1.500</i>

Direttiva NIS

NIS «Network and Information Systems»






La direttiva, approvata dal Parlamento Europeo, il 6 luglio del 2016, ha lo scopo di incrementare il livello di sicurezza cibernetica (cyber security) nel territorio dell'Unione Europea.

Si tratta di uno strumento che intende:

- Obbligare gli stati membri ad adottare una strategia nazionale in tema di cyber security
- Creare un gruppo di cooperazione per agevolare lo scambio di informazioni tra stati membri, incrementando il reciproco livello di fiducia
- Creare un gruppo di intervento per la sicurezza informatica in caso di incidente
- Fissare obblighi di sicurezza e notifica per gli operatori di servizi essenziali e fornitori di servizi digitali
- Obbligare gli stati membri a designare autorità nazionali, punti di contatto unici e CSIRT (Computer Security Incident Response Team) con compiti connessi alla sicurezza della rete e dei sistemi informativi



Qualche spunto di riflessione

-  Quale è la reale percezione del rischio Cyber da parte del mercato?
-  La digitalizzazione dei servizi delle pubbliche amministrazioni e l'implementazione delle identità digitali
-  Industry 4.0
-  Il rischio Cyber è solo «corporate» o anche «retail»?
-  La supposta complessità delle polizze è un reale ostacolo alla loro diffusione?

Q&A

