Tavola Rotonda «Danno e impatto nella cybersecurity: risposte di sistema»

Cybersecurity nelle Infrastrutture critiche: tipologie di rischio e risposte di sistema

Roma, 20 gennaio 2020

INDICE

Il contesto attuale di cybersecurity

I principali rischi del mondo in cui operiamo

Rischi legati al mancato presidio della supply chain e dei servizi offerti con infrastrutture esterne (es.: cloud computing)

Scenario di convergenza tra **criminalità informatica e criminalità tradizionale**

Superficie di attacco **ampliata**, in particolare da **nuove vulnerabilità** e minacce

Complessità ed eterogeneità del perimetro aziendale che incrementano il **rischio di inadeguatezza dei presidi**

Rischi legati al fattore umano favoriti da comportamenti errati nella quotidianità lavorativa

Evoluzione e complessità normativa che espone a **rischi legati alla conformità**

INTESA SANPAOLO

Il contesto attuale di cybersecurity

Il ruolo del fattore umano

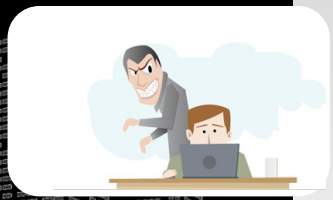
75% dei **data breach** è legato al **fattore umano**, che sia un attaccante malevolo o un errore umano

1 su 4 in particolare avviene a causa di un **«insider involontario»**, vittima di phishing o il cui device è stato rubato o perso*

Phishing in tutte le sue varianti: ricezione di **SPAM** o **raggiri** tramite mail, messaggi istantanei, SMS, ecc.

Malware: **programma malevolo** installato su un sistema senza che la vittima ne sia a conoscenza

Reti Wi-Fi: rischio di **condivisione di informazioni** non cifrate **su reti pubbliche o aperte**



Social Engineering: raccolta e sfruttamento di informazioni (es. codici riservati, password, dati personali) attraverso la **manipolazione** delle vittime

Social Network: **rischi legati alle informazioni condivise attraverso il loro utilizzo**, ad esempio violazioni di privacy o riservatezza in caso di breach ai danni dei social network

Perdita di dati o device: si mette **a la riservatezza di informazioni sensibili**, ad esempio lasciando un documento riservato sulla scrivania non presidiata

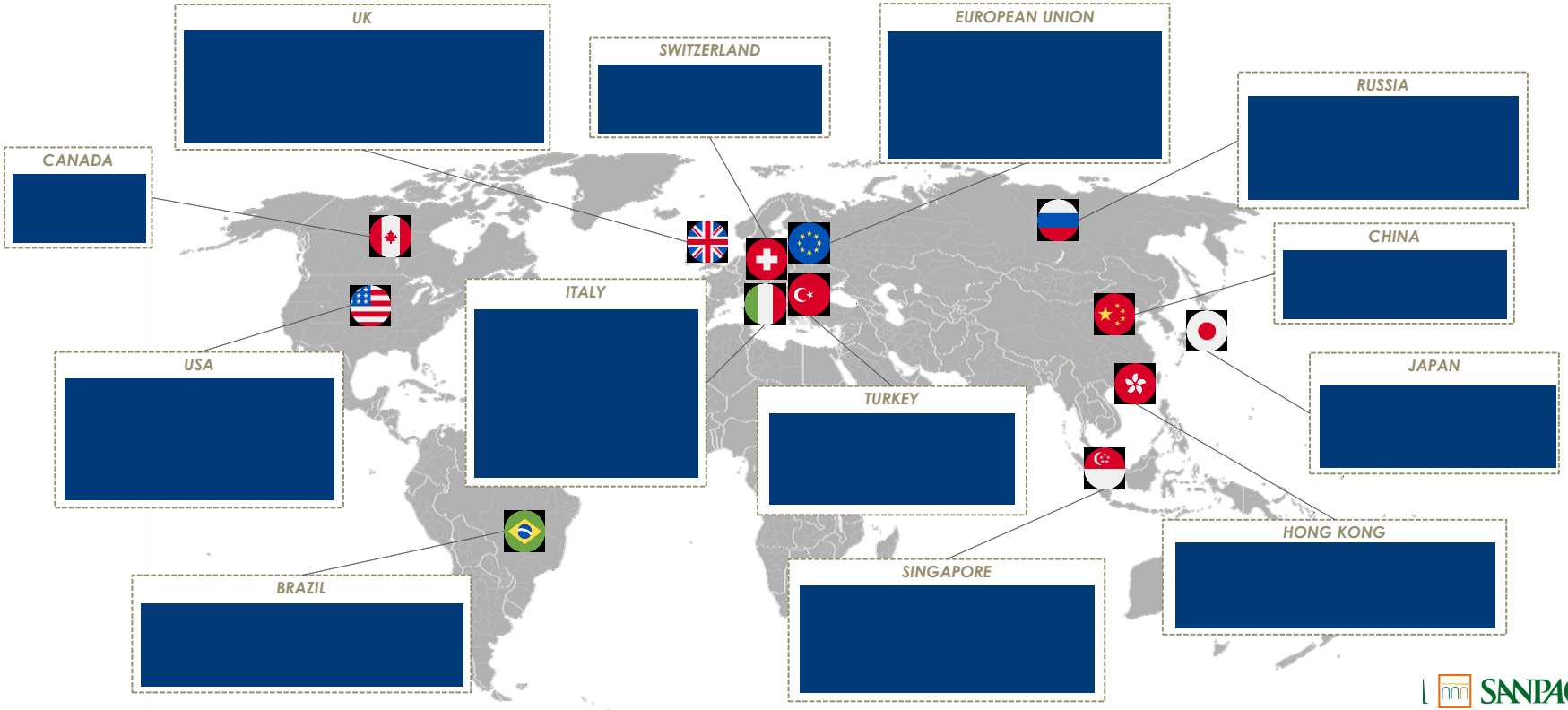
INTESA SANPAOLO

(*) Fonte: Cost of a Data Breach Report (2019) – IBM Security/Ponemon

Il contesto attuale di cybersecurity

La complessità dell'evoluzione normativa globale…

Rappresentativa



Il contesto attuale di cybersecurity

…e due tra le principali recenti normative a livello italiano

Decreto Legislativo n. 65 del 18 maggio 2018 «recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione», di **recepimento della Direttiva Europea NIS** (Network and Information Security).

Principali elementi

Emanazione di **linee guida e misure attuative da parte dell'autorità nazionale competente NIS** (ad esempio il Ministero dell'Economia e delle Finanze - MEF per il settore finanziario).

Legge n. 133 del 18 novembre 2019 recante «**Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica** e di disciplina dei poteri speciali nei settori di rilevanza strategica», conversione del D.L.105 (a cui ulteriori modifiche sono state apportate dall'articolo 27 del Decreto Legge n. 162 («Milleproroghe») in data 30 dicembre 2019).

Principali elementi

Le **misure attuative** della Legge n. 133 saranno definite **entro 10 mesi dall'entrata in vigore** della legge di conversione da parte del Presidente del Consiglio dei Ministri.

Il contesto attuale di cybersecurity

Focus: la situazione nel settore finanziario (**1** di 2)

KEY FIGURES

+11 % aumento del numero medio di incidenti di sicurezza per azienda.[1]

33 % dei costi di un data breach viene sostenuto a partire da un anno dopo l'incidente.[2]

I costi sono maggiori nel secondo e terzo anno ***soprattutto per settori fortemente regolamentati come healthcare e finance***.

279 giorni per identificare e contenere un data breach, in media.[2]

+4,9% rispetto al 2018

FOCUS FINANCE

18,5M $ costo medio del cyber crime per le aziende del **settore finanziario**.[1]

+40% rispetto alle altre industry

17% degli **attacchi globali** nel 2018 ha interessate il **finance**, a parimerito col settore delle tecnologie.[3]

30% Il settore finanziario si riconferma al primo posto anche **in Europa** (EMEA) dove aumenta anche in percentuale sul totale degli attacchi

1. *Fonte: 2019 Cost of cyber crime Study – Accenture/Ponemon*

2. *Fonte: Cost of a Data Breach Report (2019) – IBM Security/Ponemon*

3. *Fonte: Global Threat Intelligence Report 2019 – NTT Security*

Il contesto attuale di cybersecurity

Focus: la situazione nel settore finanziario (**2** di 2)

Qualsiasi organizzazione (o persona) con un asset informatico e che utilizza tecnologie di comunicazione online è costantemente **esposta al cyber risk**, ma il **settore finanziario** è **particolarmente a rischio** in quanto:

- è un **settore critico**,
- è altamente **dipendente** dalle **informazioni e** dalle **tecnologie** come fattore abilitante di prodotti e servizi forniti
- le **organizzazioni** del settore finanziario sono **interconnesse** (tra di loro e con altri settori) attraverso i sistemi di pagamento
- i **prodotti e** i **servizi** forniti sono **time-critical** e potrebbero essere compromessi da eventuali attacchi cyber
- sempre più giurisdizioni introducono **normative e framework** per rafforzare la cybersecurity di settore e delle istituzioni.

Le Banche devono anche fronteggiare un numero sempre maggiore di minacce, considerando gli **impatti di un possibile incidente cyber** sia in termini di perdite finanziarie dirette, sia di **ramificazioni indirette a livello sistemico**

Risulta quindi fondamentale **sfruttare l'interconnessione in termini di collaborazione** per rispondere efficacemente al contesto attuale

INDICE

L'importanza della cooperazione

L'approccio olistico di Intesa Sanpaolo nella risposta ai crescenti rischi

Come Intesa Sanpaolo adottiamo un **approccio olistico** che mira a rafforzare la **resilience** e ad abilitare la **readiness** non solo a livello di **Gruppo**, ma anche di **Sistema Paese.**

L'importanza della cooperazione

La risposta di sistema attraverso lo stakeholder networking…

Network con gli stakeholder

La strategia di Intesa Sanpaolo mira a **sfruttare l'interconnessione** crescente e il fatto di essere un **anello importante della catena nell'ambito del Sistema Paese** per fare leva sulla collaborazione, l'infosharing e le risorse dei diversi player in modo da **garantire un livello comune di sicurezza e di innalzarlo per tutto l'ecosistema**

Reti di **stakeholder all'interno del Gruppo** (altre strutture aziendali, realtà del Gruppo, filiali, ecc.)

Partnership **privato-privato** con **stakeholder esterni** come associazioni, gruppi di lavoro di cybersecurity, peer di settore e non, ecc.

Partnership **pubblico-privato** con **stakeholder esterni** come regolatori, supervisori, istituzioni nazionali, europee e internazionali, ecc.

L'importanza della cooperazione

…e l'aumento di cyber culture ed awareness

Cyber culture ed awareness

A partire dal livello italiano, la cyber culture va creata e rafforzata attraverso **iniziative coordinate e mirate** a partire dalla **scuola primaria**, fino alla **formazione universitaria**

All'interno dell'azienda, le **iniziative di awareness** vanno previste e predisposte per tutti, dal **top management**, agli **esperti di sicurezza**, a **tutti** gli impiegati e i collaboratori

Inoltre, **una delle misure più importanti ed efficaci** nella prevenzione mitigazione di potenziali danni e impatti di cybersecurity è **l'aumento dell'awareness**.

La **cyber culture** va indirizzata come **priorità strategica** in tutte le aziende e le deve pervadere a tutti i livelli, estendendosi anche a client e terze parti e fornitori.

I **clienti** e più in generale i **cittadini** devono essere **formati e sensibilizzati sulle tematiche di cybersecurity** con campagne di awareness ad hoc

INDICE

Le principali iniziative di Intesa Sanpaolo

La cooperazione e l'infosharing

Rappresentativa

Iniziative a livello italiano

- **CERTFin: CERT (Computer Emergency Response Team) italiano per il settore finanziario**, guidato dall'Associazione Bancaria Italiana (ABI) e da Banca d'Italia
- **Cyber Security Framework italiano**, per fornire alle **organizzazioni pubbliche e private un approccio volontario omogeneo**

Iniziative globali

- Partecipazione a tavoli di lavoro internazionali come il **Financial Stability Board**
- Iniziative di **information sharing** con altre infrastrutture critiche e con le forze dell'ordine per gestire le minacce cyber ed essere in linea con quanto richiesto dalle diverse normative per le istituzioni finanziarie (Financial Market Infrastructures) a livello globale (i.e.: **"OF2CEN[1]" project**)
- Collaborazioni con organismi **internazionali in ambito finanziario e di Cybersecurity** come FS-ISAC[2], Carnagie Endowment, FIRST[3], etc.

Iniziative a livello europeo

- Collaborazione con la **European Banking Federation** (EBF): analisi della **regolamentazione** e rappresentazione della **posizione del settore bancario europeo**; ad esempio contribuzioni per le tematiche di cybersecurity al **gruppo di lavoro Cloud Banking Forum** di EBF
- **Collaborazioni con associazioni come** AFME - Association for Financial Markets in EU, ENISA, Europol, etc.
- Collaborazione con la **European Cyber Security Organization** (ECSO): attraverso **partnership privato-pubblico** con la Commissione Europea, per rafforzare la cyber resilience e la cyber security, anche definendo priorità di investimento e allocazione di fondi per contribuire al raggiungimento di un **Digital Single Market europeo cyber-sicuro**

[1] Online Fraud Cyber Centre and Expert Network

[2] Financial Services Information Sharing and Analysis Center

[3] Forum of Incident Response and Security Teams

Le principali iniziative di Intesa Sanpaolo

Un esempio di partnership privato-privato

Nel corso del 2019, Intesa Sanpaolo ha aderito ad **accordi per collaborazioni di tipo privato-privato** tra organizzazioni che condividono le stesse sfide in ambito cybersecurity.

Le **partnership privato-privato sono un complemento efficace a quelle di tipo pubblico-privato** e mirano a diventare acceleratori / facilitatori nello sviluppo di capacità nazionali per far fronte alle minacce nel cyberspace.

Altri vantaggi potrebbero emergere **in ambito supply chain**, considerato che le organizzazioni condividono spesso gli stessi fornitori, che beneficerebbero a loro volta di un **approccio comune e condiviso** alla cybersecurity da parte dei loro clienti.

Nello specifico, il Gruppo di Lavoro coinvolge diverse grandi aziende italiane che hanno deciso di indirizzare le prime attività operative sui seguenti ambiti:

1. **Condivisione di Indicatori di Compromissione** (IoC) attraverso accordi e piattaforme automatiche:
    a. formalizzazione della collaborazione con la firma congiunta di un documento condiviso,
    b. adozione di una tassonomia condivisa per Tecniche, Tecnologie e Procedure (TTP) in termini di *IoC data model*
    c. uso di una piattaforma di infosharing per la condivisione degli IoC
2. Iniziative di **formazione ed awareness** su **temi specifici di interesse** (come ad esempio le tecniche di social engineering) e **TTP utilizzati dagli attaccanti**
3. **Esercizi comuni di cybersecurity** (Incident handling, Capture the flag, Red Team vs. Blue Team, ecc.)
4. Condivisione di informazioni per individuare **best practice** anche a livello di **modello organizzativo e skill professionali** di riferimento