Banche e Sicurezza 2021

Plenaria C

Milano – 25 Maggio 2021

Principali differenze ed integrazioni BC / Op.Res..

BUSINESS CONTINUITY «*Capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident*»

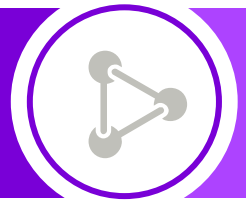
- Approccio reattivo
- Eventi ad alto impatto e bassa probabilità di accadimento

OPERATIONAL RESILIENCE «*The ability of an enterprise to deliver critical operations through disruption*»

- Approccio preventivo
- Estensione ad eventi a minor impatto ma alta probabilità di accadimento

..e Digital Op.Res

SUPPLY CHAIN



Sempre più vendor e terze parti interconnesse, sempre più integrate nei processi aziendali, connesse e dislocate in tutto il mondo

NEW CHANNEL

Digitalizzazione e remotizzazione di processi e servizi che richiedono l'implementazione di nuovi canali resilienti

NEW WAY OF WORK

Il remote working richiede nuovi sistemi ed una rete resiliente per chi lavora da remoto

NEW THREATS

Sempre nuove modalità di attacchi cyber esacerbate dalla digitalizzazione dei servizi e dei nuovi modelli di lavoro

Risulta necessario includere all'interno del proprio scope di Continuità Operativa lo SCENARIO CYBER

- ***BIA dei servizi digitali***
- ***Risk assessment applicativi***
- ***Scenario Cyber all'interno del BCP***
- ***Blue&Red teaming***

Il ruolo di Sicurezza nella Op.Res – Contesto

I cyber attack sono oggetto di una **crescita costante** negli ultimi anni **così come le conseguenze** che portano sulle aziende che colpiscono. Gli attacchi possono mettere a repentaglio la stessa sopravvivenza dell'azienda sia per interruzione dei servizi erogati, che per le conseguenze economiche e reputazionali che possono causare. Il rischio di cyber attack è stato classificato tra i top risk anche nell'ultimo report del World Economic Forum

Le Disposizioni di Vigilanza 285/13 citato lo scenario di "**attacchi informatici su larga scala**" tra quelli da includere nel business continuity plan destinato ai processi a rilevanza sistemica (regolamento lordo, accesso ai mercati, servizi di pagamento a larga diffusione, gestione della liquidità)

La gestione di questo scenario richiede una **forte integrazione** tra le strutture che si occupano di business continuity, quello che gestiscono gli "eventi cyber" e le strutture realizzative IT per l'implementazione delle necessarie azioni di prevenzione / contenimento

Le migliori pratiche da attuare per la prevenzione e il contenimento di questi eventi vengono identificate in contesti che si occupano di **proteggere informazioni e processi operative ritenuti particolarmente critici**. L'integrità e la disponibilità degli strumenti e dei dati di supporto sono infatti ritenuti i fattori chiave

La valutazione di questo scenario consente peraltro di sviluppare i **meccanismi di reporting integrati con le strutture di IT e Operational Risk Managememt**, nonché di rispondere in modalità omogenea alle periodiche richieste ECB in ambito cyber attack / business continuity

Il ruolo di Sicurezza nella Op.Res – Key Pillars

01

Caratterizzazione dello scenario

Gli attacchi informatici hanno peculiarità che li differenziano dai tradizionali scenari di Continuità Operativa per tipologia di cause (volontarie) e variabilità di natura / obiettivo

02

Soluzioni preventive e di contenimento

Fronteggiare attacchi informatici richiede l'implementazione di soluzioni preventive e di contenimento differenti rispetto ai tradizionali scenari di Continuità Operativa

03

Monitoraggio continuo

Fronteggiare attacchi informatici richiede l'implementazione di servizi di monitoraggio continuo per l'analisi e la correlazione degli eventi e l'indirizzamento tempestivo di ogni anomalia

04

Integrazione emergency / crisis mgmt

I processi di emergency / crisis management devono essere integrati con le procedure di Security Incident Management. I Team di gestione delle crisi devono essere integrati

05

Integrazione business continuity plan

Il piano di continuità operativa deve includere processi per la gestione in ordinario e in emergenza dello scenario di Cyber Attack così come avviene per gli altri scenari

06

Collaudo e certificazione

Gli eventi di cyber attack devono essere soggetti ad attività di collaudo e certificazione analogamente a quanto avviene per le altre tipologie di eventi trattati in ambito continuità' operativa

Thank You!