Atti Convegno Cyber Crime Conference 2018 – Gianna Detoni

Author : Redazione

Date : 28 maggio 2018

Business Continuity: un’unica metodologia per ogni tipo di minaccia

Ringrazio gli organizzatori della Cyber Crime Conference per avermi invitata a parlare di questo tema, che probabilmente è il tema meno tecnologico della giornata, eppure importantissimo. Parlerò della Business Continuity, una metodologia imprescindibile per chiunque voglia utilizzare la parola “resilienza”. Senza un sistema di gestione della continuità operativa, infatti, nessuna delle vostre organizzazioni può dirsi resiliente.

Noi professionisti di Business Continuity diciamo che la nostra è una materia di buon senso. Gli inglesi chiamano il buon senso “common sense” e dicono “common sense is not so common”. E in effetti non è semplice far passare i concetti della continuità operativa. La sua metodologia è qualcosa che nel sistema anglosassone è dato ormai per scontato. Nel nostro sistema, invece, la prevenzione non è un elemento sempre presente. E essendo la Business Continuity una metodologia che pratica strategie di prevenzione, non è semplice fare in modo che entri nella nostra cultura. Ma noi abbiamo il dovere di modificare questa condizione. Il fatto che noi italiani sappiamo reagire e improvvisare meglio degli altri è la nostra iattura. Perché in realtà, non facendo prevenzione, molto spesso falliamo. Molto spesso questa nostra bravura nel reagire si risolve nel seppellire morti e vedere aziende che falliscono. Dobbiamo cambiare questo paradigma e diventare bravissimi anche nella prevenzione, non solo nella reazione.

Nel mio intervento farò molte provocazioni con l’obiettivo di stimolare tutti voi, che già conoscete la continuità operativa, ad approfondirla il più possibile e capire cosa potreste fare di più e meglio nella vostra organizzazione. La visione finale è quella di divulgare anche nel nostro paese una cultura di prevenzione, da cui noi tutti non possiamo che beneficiare.

Intitolo il mio intervento l'abuso della Business Continuity, perché molti sono convinti di avere già la Business Continuity, ma non è così. Hanno magari il Disaster Recovery e pensano di essere a posto in termini di continuità operativa. Ma Disaster Recovery e Business Continuity non sono sinonimi; se avete il Disaster Recovery e basta, non avete la continuità operativa. Il Disaster Recovery è solo uno dei piani a livello operativo del sistema di gestione della continuità operativa. Importantissimo, di fatto la prima azione di continuità operativa nata tanti anni fa, ma certamente non l'unica.

Con la convinzione che la Business Continuity si risolvesse con il Disaster Recovery, le organizzazioni hanno dato compito al dipartimento IT di provvedere alla continuità operativa. È molto ingiusto chiedere all'IT di dare una continuità operativa all'organizzazione perché l'IT specificatamente non ha e non deve avere alcun interesse nella gestione della continuità operativa. Non ne ha perché l'IT propone soluzioni di continuità operativa. Sono i professionisti ai quali noi dobbiamo dire qual è il problema perché ci forniscano una soluzione. Non possono dare una continuità operativa a tutta l'organizzazione. Sono i diretti titolari dei processi che devono invece stabilire qual è la continuità operativa per ognuno di essi.

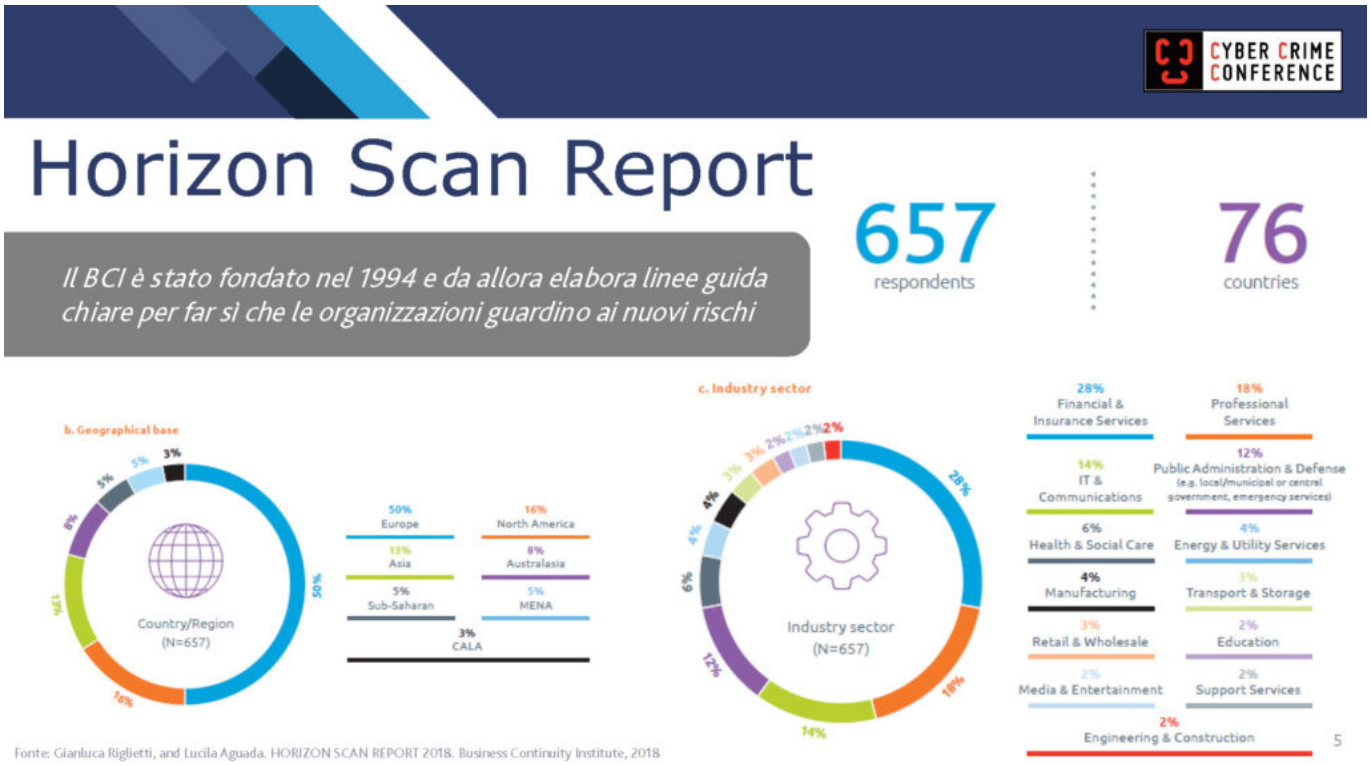
In generale, c'è un grande malinteso sulla Business Continuity. Ci sono persone che pensano che sia un buon Crisis Management, chi pensa sia un buon Disaster Recovery. In realtà, la continuità operativa è una metodologia olistica, trasversale, di cui fanno parte sia il Disaster Recovery che l'Emergency Management, il Crisis Management, la Resilienza Organizzativa e il Risk Management.

Soprattutto i titolari di prodotti, servizi, processi e attività devono capire la continuità operativa e analizzare gli impatti di una discontinuità sui propri prodotti, servizi, processi e attività. Non è un

tema che è praticato da un manipolo di tecnici che in una stanza fanno continuità operativa mentre tutto il resto dell'organizzazione fuori da lì fa danni. La Business Continuity è un cambiamento culturale, quindi tutta l'organizzazione deve capire quali possono essere i rischi di discontinuità. La discontinuità crea le interruzioni. Più le interruzioni sono gravi, più il danno è serio.

Quali sono le nuove sfide? La Cyber Resilience, la Data Protection. Noi che facciamo continuità operativa non ci vediamo niente di nuovo. Non nasce nel 2017 o 2018. La Data Protection è molto vecchia. Cosa c'è di nuovo rispetto al passato? Il GDPR è la novità che introduce sanzioni pesanti. Forse questo. Va benissimo, almeno le organizzazioni si sveglieranno sull'esigenza di dotarsi di qualcosa per proteggere i dati. Ma non è che fino al 25 maggio 2018 invece i dati potessero essere tranquillamente abusati senza ritegno. Le organizzazioni che hanno avuto data breach o ransomware hanno un problema reputazionale grave. Con il GDPR avranno anche un importante danno economico. Ma a livello di sostanza non è cambiato granché rispetto al passato.

Ogni nascono sempre più strumenti per difendere le organizzazioni. La difesa è dinamica perché le minacce sono dinamiche. Però la cultura di prevenzione rimane quella ed è sempre valida. Se si applica correttamente un sistema di gestione della continuità operativa, si è già attrezzati per fronteggiare tutte le nuove minacce, tutte quante. Da molti anni il Business Continuity Institute (BCI), ad esempio, fa questo report annuale, l'Horizon Scan Report, che dice qual è lo stato di preoccupazione e preparazione sui diversi rischi nelle organizzazioni di tutto il mondo. Il BCI intervista i Business Continuity Manager, coloro che sono responsabili della continuità e vedono tutte le interruzioni, di qualsiasi tipo. Non hanno problemi né riserve a fornire il dato di eventuali interruzioni rispetto alla percezione di minaccia.



È da parecchi anni che il cyber attack è al primo posto in questo report tra le minacce più temute. Se vi ricordate, non siamo mai stati tranquilli da questo punto di vista, anche se oggi se ne parla sempre di più. I white hacker hanno sempre allertato sui potenziali denial of service, problemi coi pirati informatici e così via. La seconda minaccia dopo i cyber attack è il data breach.

Tra le interruzioni effettive, invece, i cyber attack stanno al quarto posto, non al primo. Al primo ci sono i problemi di interruzione IT o alle telecomunicazioni. Al secondo problemi climatici. Al terzo posto ci sono le interruzioni alle infrastrutture critiche. Tema dolentissimo perché in Italia nessuna infrastruttura critica ha la Business Continuity. Non c'è un'infrastruttura critica sulla quale noi contiamo che abbia un sistema di gestione della continuità operativa o un Business Continuity Manager. Noi dobbiamo contare che tutti i componenti che concorrono alla nostra resilienza facciano la loro parte. Il tema della Business Continuity, invece, non è sentito a livello governativo e politico. Noi non possiamo come privati chiedere conto alle grandi società di energia, telecomunicazioni e trasporti di seguire un sistema di gestione della continuità operativa, dev'essere imposto a livello governativo. E questo ancora non c'è. C'è la volontà di qualcuno all'interno di queste organizzazioni a introdurre la Business Continuity in un mondo in cui non c'è grande sensibilità sull'argomento, ma non c'è la giusta informazione. Mi occupo di continuità da tantissimi anni e da tantissimi anni parenti e amici mi chiedono di spiegare cosa faccio. Sul momento capiscono subito, poi dopo qualche mese me lo richiedono di nuovo. Questo perché non viene praticata, non fa parte della nostra cultura. Il rischio lo capirebbero tutti, ma la Business Continuity non fa parte della nostra cultura, quindi non viene percepita.

C'è anche un'inerzia organizzativa misurata dal Business Continuity Institute all'interno del Report. È interessante vedere come le organizzazioni arrivano ad accorgersi di aver avuto un problema di natura cyber. La maggior parte se ne accorge grazie all'IT, ma il tempo di latenza è rilevante, mentre a volte lo veniamo a sapere addirittura dai nostri clienti. Il problema dell'allerta è molto importante.

Perché implementare allora un sistema di gestione della Business Continuity? Il sistema di gestione passa attraverso tutte le fasi, non solo quella di gestione del rischio ma anche quella di sensibilizzazione. Ci sono sei fasi complessive nel sistema di gestione:

- Istituire la policy e delineare un programma;
- Radicare la cultura di continuità operativa all'interno dell'organizzazione. Troppo spesso la BC dipende dall'illuminazione del manager del momento, il manager successivo non è illuminato e taglia tutto. Se la continuità è nel DNA dell'organizzazione, questo problema non sussiste. L'incorporazione si fa tramite formazione e sensibilizzazione;
- Fare l'analisi, che è il cuore e fondamento del sistema di gestione della BC. Si tratta dell'analisi d'impatto (BIA) che può avere un'interruzione su tutti i nostri prodotti, servizi, processi e attività urgenti. La cosa fondamentale da capire è che nel Risk Management quello che si fa è calcolare probabilità per impatto, mentre nella BIA do per scontato che l'incidente succeda e analizzo le conseguenze su tutto ciò che è urgente. Inoltre, nell' analisi di impatto non importa quale sia la causa. A prescindere dalla causa, mi posiziono dopo l'interruzione. Quindi un'organizzazione che fa bene Risk

Management e poi fa anche la Business Continuity diventa davvero molto resiliente. È fondamentale capire che una senza l'altra è monca;

- Dopo l'analisi viene la progettazione. Solo dopo l'analisi, infatti, abbiamo una giustificazione logica per investimenti onerosi per l'organizzazione. Prima di implementare bisogna progettare, fare dunque sinergia in tutta l'organizzazione per progettare soluzioni di continuità – che possono essere tecnologiche, formative, o altro. Tutti abbiamo commesso l'errore di implementare di pancia, passando direttamente al punto 5. In questo modo non avremo mai un'analisi che porti al Top Management una giustificazione logica per gli investimenti che si fanno;
- Nell'implementazione – solo lì – si scrivono i piani;
- Ma è come non aver fatto nulla se non si fa la convalida. I fornitori di Disaster Recovery raccontano che su 100 organizzazioni che hanno da loro il Disaster Recovery, solo 20 lo testano. Le altre 80 fanno vedere che hanno messo lì qualcosa, ma non fanno alcun test. Perché i test sono rischiosi, dicono. Ma se è rischioso fare i test, quanto lo è non farli?

Come per ogni altro rischio, ci sono due tipi di difese: tecnologica – fondamentale – e il resto dell'organizzazione, che spesso non viene considerata. C'è quindi un altro grande malinteso, che è anche una mancanza di correttezza nei confronti del Top Management. Voi esperti di difesa tecnologica sapete che uno dei punti fermi è che puoi erigere tutte difese che vuoi, ma non è mai sufficiente e può sempre succedere qualcosa. Un attacco cyber può andare a buon fine anche con le migliori soluzioni tecnologiche. Spesso può capitare con un banale errore umano. Se non diciamo al Top Management che a prescindere da tutto quello che noi spendiamo in tecnologie c'è il rischio di essere penetrati, il Top Management pensa: "ho speso tanto, allora sono a posto." Ma se invece si dice la verità, che esiste la possibilità che l'attacco vada comunque a buon fine, è possibile prepararsi alle conseguenze. Per questo esiste la Business Continuity. Da sempre abbiamo fatto riflettere le organizzazioni che qualcosa può succedere. Chi non è preparato avvisa i clienti dopo che questi l'hanno già scoperto da altri, creando un danno reputazionale altissimo.

Prepariamoci dunque a dovere per le conseguenze. È fondamentale gestire ogni aspetto, curare il fattore umano con formazione e sensibilizzazione. Voi probabilmente conoscete il caso di TV5, che è andata in nero per ben quindici minuti. Con un'impennata di ascolti, tra l'altro, durante l'interruzione. Qualche giorno dopo venne fuori che questo giornalista di TV5 aveva rilasciato un'intervista con le password d'accesso su un post-it attaccato sulla parete alle sue spalle. Agli hacker è bastato molto poco in quel caso. Nessuna tecnologia può nulla in questi casi. Noi possiamo aver preparato tutto ma se non abbiamo curato il fattore umano tutto è inutile. Non possiamo licenziare le persone se non le abbiamo formate. Dobbiamo formare le persone e fargli comprendere l'importanza del tema.

L'impegno del Top Management e le percentuali di organizzazioni che riportano un grande coinvolgimento dei vertici è salito negli ultimi tempi. Possiamo dire che il tema della Business Continuity è diventato un tema caldo. Anni fa ne parlavo con i rappresentanti delle organizzazioni e mi guardavano con uno sguardo "blank", tipo "non so di cosa stai parlando", ma oggi la situazione è cambiata, lo sguardo dell'interlocutore è diventato colpevole, del tipo "sì, lo so, dovrei farlo, ma ora non ho soldi, non ho tempo, non ho le risorse adeguate. Devo

fare il GPR, ci penso dopo il 25 maggio". Almeno c'è la consapevolezza che c'è un buco.

Negli anni ho visto una proliferazione di analisi diverse, come data protection, impact assessment, travel impact assessment, cyber risk impact analysis… Se voi avete una buona analisi d'impatto, le coprite tutte. Stabilire Recovery Time Objective e Recovery Point Objective è fondamentale per capire se in caso di attacco cyber verranno disattesi. È inutile che facciamo un obiettivo di tempo di recupero di 4 ore se poi in caso di attacco cyber sono due settimane. Dobbiamo stabilirlo con accuratezza. In questa metodologia tutto si può fare tranne ignorare di avere dei problemi. Quando ci sono dei problemi, nella fase di implementazione della continuità operativa emergono tutti. La Business Continuity è molto potente come metodologia organizzativa.

Il piano cyber è uno dei piani specialistici della continuità operativa, come gestire un attacco cyber è un piano di crisi particolare. Se le organizzazioni non sanno riprendersi velocemente da un attacco cyber, non sono resilienti.

Nessuna disciplina può dire di avere l'egemonia sulla Resilienza Organizzativa, perché la resilienza è costituita da diverse discipline, tra cui l'Emergency Management, il Disaster Recovery, il Risk Management, la Business Continuity, tante altre ancora. Nessuna di queste discipline ha l'egemonia sulla Resilienza Organizzativa, ma tutte sono fondamentali. Non c'è dunque resilienza senza continuità operativa.

Gianna Detoni, BCI Italy Forum Leader