AZIENDABANCA

Mensile

Data 03-2014
Pagina 44/45
Foglio 1 / 2

Garantire la continuità del business

LA CIRCOLARE 263 HA PREVISTO UNA SERIE DI ADEGUAMENTI IN TEMA DI BUSINESS CONTINUITY E DI DISASTER RECOVERY, CUI ANCHE GLI OUTSOURCER HANNO DOVUTO DARE RISPOSTA. MA LA RILEVANZA DEL SETTORE BANCARIO A LIVELLO DI SISTEMA PAESE NE FA ANCHE UN TARGET IDEALE PER AZIONI DI GUERRA INFORMATICA O CYBER ATTACCHI

In tema di Business Continuity, la Circolare 263 (la prima a evidenziare il ruolo dei servizi IT tra gli elementi su cui vigilare per la tutela del rischio) distingue due gruppi di banche: da un lato quelle che, in caso di problemi di operatività, non creerebbero rilevanti squilibri alla normale operatività del Sistema Paese, dall'altro quelle che, per le loro dimensioni o per le eventuali funzioni istituzionali che ricoprono, offrono servizi di carattere sistemico e devono pertanto ottemperare a un maggior numero di disposizioni per proteggere il funzionamento del Paese nel suo complesso. «Come erogatore di servizi di gestione dei sistemi informativi bancari, ci troviamo in una situazione ibrida – afferma Dario Bonavitacola, Responsabile della Direzione Infrastrutture Tecnologiche, Servizi e Sicurezza di Cedacri. In effetti, prese singolarmente le nostre banche clienti non possono essere considerate delle banche che erogano servizi sistemici, ma la prospettiva si ribalta nel momento in cui guardiamo al portafoglio complessivo dei nostri istituti: in questo caso, considerati come realtà integrata, arrivano ad avere un peso rilevante a livello nazionale, con oltre 2.700 sportelli sul territorio e volumi operativi gestiti pari a circa il 10% dell'intero sistema bancario italiano».

Dario Bonavitacola, Responsabile della Direzione Infrastrutture Tecnologiche, Servizi e Sicurezza di Cedacri

Come un operatore sistemico

La scelta, come outsourcer, è stata quella di perseguire una strategia di responsabilità che prende come riferimento le normative fissate per un operatore sistemico, adeguandosi a tutte le disposizioni imposte da Banca d'Italia. «Questa strategia conferma la nostra tradizionale attenzione alla qualità, con scelte che vogliono offrire ai clienti la certezza di poter contare su un servizio di business continuity di eccellenza – commenta Bonavitacola. Proprio per il nostro ruolo di outsourcer, ci siamo trovati già pronti a rispondere ad alcune delle richieste di Banca d'Italia. Ad esempio, per quel che riguarda la classificazione dei sistemi IT in termini di maggior o minor criticità per il business, come Cedacri disponevamo già di tale catalogazione per gestire al meglio i rapporti di fornitura con i nostri clienti. Ugualmente, eravamo già attrezzati all'origine per rispondere alle richieste di Banca d'Italia circa la corretta organizzazione della funzione IT – in termini di persone, processi e procedure – in un'ottica di business continuity».

Eguale potenza operativa: fatto

Ha preso invece il via nel 2012 l'adeguamento alla richiesta di equivalente potenza elaborativa fra il sito di produzione e quelli di business continuity e disaster recovery. «Nel 2013 abbiamo così raggiunto il risultato di aver portato a egual potenza elaborativa tutti e tre i nostri siti – spiega Bonavitacola – i siti di produzione e di business continuity di Collecchio (Parma) ottengono infatti ugual potenza elaborativa tramite un bilanciamento dei carichi tra i sistemi, mentre il sito di disaster recovery di Castellazzo Bormida (Alessandria) è stato potenziato attraverso nuovi apparati per essere equiparato ai primi due. Ci siamo trovati anche nella posizione di riuscire automaticamente ad ottemperare alle nuove norme relative alla locazione della struttura di disaster recovery, che deve essere oggi situata al di fuori delle aree metropolitane. Il nostro sito di Castellazzo si trova infatti distante dal contesto urbano, oltre a porsi in un'area geo-morfologica differente da quella dei siti emiliani, a garanzia di massima sicurezza in caso di catastrofe naturale».

I requisiti da operatore sistemico

Questo per quanto riguarda le norme comuni a tutte le banche: per gli istituti considerati come "sistemici" viene anche richiesto, in fase di disaster recovery, di ripartire con il primo servizio IT entro due ore dal disastro e di ripristinare tutti i servizi critici entro quattro ore. «Si richiede altresì che le persone impiegate nella gestione dello switch di disaster recovery siano diverse da quelle che operano nel sito di produzione – prosegue Bonavitacola. Cedacri è attualmente in grado di garantire ai propri clienti un ripristino dei servizi critici entro 4 ore e puntiamo in breve tempo a poter certificare anche la ripartenza del primo servizio in due ore. Sul tema della resilienza delle persone, il nostro sito di Castellazzo si avvale già oggi di un organico di professionisti, specializzati sia sui sistemi tecnologici che applicativi, del tutto distinto da quello operativo a Collecchio. Il percorso è stato intrapreso ancora prima che le disposizioni della Circolare 263 venissero finalizzate, ponendoci come un attore proattivo che anticipa le richieste del settore a sostegno della competitività dei clienti».

Strategie di sistema per la cyberwar

Restando sul tema sicurezza, c'è poi il filone delle misure da adottare per prevenire tipologie di rischio che nel nostro Paese fanno ancora pensare più a pellicole cinematografiche che a pericoli concreti, ma che dagli esperti vengono indicati come uno dei fronti caldi per il prossimo futuro: dalla cyberwar ad altri fenomeni di attacchi mirati, come il cyberhactivism, il settore bancario si troverà in prima fila sia per il suo ruolo all'interno del Sistema Paese sia per il valore simbolico di un attacco a un attore del mondo finanziario. «Quando si parla di cyberwar, cioè di macro-attacchi informatici condotti nei confronti di un determinato Paese a scopi bellici o geo-politici – precisa Bonavitacola –, dobbiamo essere consapevoli che le misure di contrasto vanno affrontate a livello di Sistema Paese, attraverso un coordinamento generale di tutti gli attori che possano essere potenzialmente coinvolti in attacchi di questa natura: un solo soggetto, davanti a un attacco di grande portata, difficilmente potrà resistere in autonomia».

E vigilanza attenta in caso di cyberattack

Diverso il caso dei cyberattack, che nascono appunto come volontà di estorcere informazioni (in quest'epoca facilmente convertibili in denaro) oppure con l'obiettivo di raggiungere una certa visibilità mediatica. «In questo secondo caso, come Cedacri, mettiamo in atto tutte quelle pratiche che ragionevolmente riteniamo possano metterci al riparo da eventuali attacchi – conclude Bonavitacola. In effetti, le nostre infrastrutture di collegamento informatico alla Rete sono ridondate al massimo per consentirci di difenderci da eventuali flussi di dati pericolosi, e siamo in costante coordinamento con le Forze dell'Ordine e la Polizia Postale con un duplice obiettivo: da un lato contribuiamo attraverso i nostri strumenti ad arricchire il bagaglio informativo delle istituzioni, coadiuvando la loro lotta quotidiana al crimine informatico, dall'altro riceviamo da parte loro alert puntuali quando i nostri sistemi possono divenire potenziale oggetto di attacchi, consentendoci di alzare le nostre misure di sicurezza quando il rischio si fa più concreto».

A.G.