Il Panorama dei rischi

Danni ai centri di elaborazione dati , ai sistemi, ai macchinari di: aziende di servizi , produttive, del credito, delle telecomunicazioni, dell'amministrazione pubblica.

Premessa:

Si anticipa che le informazioni contenute nel presente documento sono state modificate in modo da evitare il riconoscimento delle aziende colpite.

Purtroppo nessuna azienda colpita ha dato il consenso alla divulgazione dei dati e delle informazioni inerenti agli eventi alle quali è stata soggetta e pertanto il grado di modifica è proporzionale alla magnitudo dei danni e della dimensione dell'azienda, sono stati eliminati a questo scopo anche i paesi ove è avvenuto il fatto o dove risiede il sistema danneggiato.

Abbiamo cercato di eliminare le casistiche simili o identiche per dare un panorama il più possibile vario di quanto accade a nostra conoscenza, inoltre abbiamo eliminato i casi che hanno avuto grande rilevanza sui giornali per evitare ripetizioni (ma se i lettori desiderassero includerli , siamo aperti ai loro suggerimenti).

Inoltre invitiamo i lettori e i soci a inviare le loro casistiche perché riteniamo importante che le informazioni possano essere divulgate e scambiate al fine di accrescere la sensibilità degli operatori del settore verso i temi della sicurezza e della valutazione dei rischi che l'utilizzo delle nuove tecnologie comportano.

Ci riserviamo tuttavia di modificare quanto ricevuto in modo che non possa essere riferito ad una particolare azienda o ente o persona.

I casi sottoesposti sono, o sono stati, oggetto di polizze assicurative, o sono stati l'origine della spinta a ricercare una polizza assicurativa, o sono avvenimenti raccontati da clienti su casi di loro conoscenza e, successivamente alla prima pubblicazione, anche casi inviatici da soci e lettori che abbiamo ritenuto utile pubblicare.

Caso 1
In un'azienda a proprietà pubblica, a causa di un malfunzionamento del Back-up, una parte dei dati contabili e di fatturazione a utenti del servizio pubblico è andata persa (2 giorni di registrazioni).
Non essendo possibile, per varie ragioni (non ultima quella di ordine politico-industriale) emettere il rendiconto mensile a 45 milioni di utenti, viene deciso di emettere dei rendiconti per ciascuna operazione registrata (in tal modo è possibile recuperare quasi tutti i dati) , e di inviare in più a ciascuno degli utenti una lettera di spiegazione e scuse per il disservizio.
I costi dell'operazione (e quindi delle perdite) sono pari a 3 milioni di € (quasi totalmente indennizzati) a tali costi si sono aggiunti quelli delle lettere di scuse e spiegazione (1 milione); questa ultima parte dei costi non era assicurata ed è rimasta a carico dell'amministrazione (1 milione).

Caso 2
In un'azienda di servizi informatici per conto terzi (settore distribuzione), un'errata implementazione di un applicativo gestionale del controllo automatico dell'impianto di climatizzazione della sala principale, ha provocato una disfunzione nelle macchine dedicate a questo scopo; il problema si concretizzava con il congelamento delle schede di controllo delle macchine climatizzatrici. Queste ultime erano due gruppi identici per marca, modello e performance, e subirono l'identico problema. Le due macchine con le schede elettroniche congelate si fermavano andando in blocco. Fu chiamata l'assistenza della ditta costruttrice, che però non riusciva a districare la problematica informatica relativa ai chip interni alle schede; nei manuali di istruzione non vi era traccia delle informazioni necessarie per re-settare il software proprietario e determinati parametri evidentemente andati fuori registro. Fu proposto di smontare i macchinari e inviarli alla casa costruttrice (dato il tipo di macchine, in un altro continente), ma la proposta fu bocciata per i tempi biblici dell'operazione, per cui il male minore fu la soluzione scelta ala fine.

Si trattava cioè di continuare a lavorare sulle macchine in modo alternato, cioè in pratica accendere una macchina in alternativa all'altra con una frequenza tale che almeno una macchina potesse funzionare parzialmente per qualche ora prima di congelarsi, e così via fino a risolvere il problema.
Un giorno e mezzo di fermo totale, e successivamente un periodo di circa 50 giorni di inefficienza del sistema di climatizzazione nella sala dei computer centrali. Questi ultimi non sono stati danneggiati, ma hanno funzionato a regime ridotto per tutto quel tempo sviluppando un volume di calcolo pari al 35,45% del regime standard richiesto dalla loro attività. L'impatto su migliaia di punti vendita ha creato perdite reali ed immediate, dovute al fatto che il sistema è stato creato con lo scopo di poter assorbile punte enormi di richieste di calcolo in tempi estremamente ridotti, data anche la sua natura (per effetto di specifiche norme fiscali e erariali) di non poter assorbire le richieste e distribuire l'elaborazione in tempi differiti i cui risultati possono essere rilasciati a posteriori. In questo modo è stato calcolato, in base alla complessiva riduzione delle vendite, un calo di vendite di circa 27 milioni di $. Sono ancora aperte cause dei punti vendita nei confronti della società si servizi.

Caso 3
Una società di servizi informatici bancari a seguito di un errore del personale addetto nell'implementazione di una nuova piattaforma (in sostituzione del sistema principale di gestione dei conti correnti) crea un problema risolto in una giornata circa (su 3,5 milioni di conti); in pratica il mngnt decide di scaricare il nuovo software e ricaricare il vecchio software in produzione, risolvere il problema e poi ricominciare di nuovo la nuova installazione; l'operazione costa complessivamente 1,5 milioni di sole spese extra.

Caso 4
Era un'azienda finanziaria quotata nelle prime posizioni alla borsa di NY; un forte dissapore tra il responsabile dei servizi informatici e un suo programmatore dette luogo al licenziamento in tronco di quest'ultimo. L'attività informatica continuò per molti mesi; l'anno successivo, durante un'operazione di routine, in seguito ad un intoppo (un problema conosciuto e tranquillamente risolvibile con qualche artificio) e alll'avvio di una funzione raramente utilizzata, detta esecuzione ad un programma sconosciuto portò alla cancellazione di tutti i file, ivi compresi tutti i file di backup. Il danno subito di fu di circa 17 milioni di $ oltre a circa 1 milione di costi per le pubbliche relazioni.

Caso 5
Un ente pubblico la cui rete è costituita da moltissime sottoreti ha subito un crash down totale di 1 giorno e malfunzionamenti parziali per i giorni successivi per l'accumularsi di alcuni malware al suo interno. Il calcolo della perdita per l'ente pubblico, per le sole spese fisse su 10.000 postazioni di lavoro supera il milione e mezzo, mentre la somma delle spese per tutti gli interventi di disinfestazione su client e server ammonterà a quasi 1 milione di euro.

Caso 6
Un operatore di telefonia mobile a causa di un errore operativo di un addetto ai sistemi e ad un effetto di overwork del sistema si trova ad affrontare 24 ore di black out delle telecomunicazioni .
Danno stimato per la sola perdita di profitti 8-10 milioni di $.

Caso 7
Un malfunzionamento del sistema di controllo principale della regolazione dei flussi dei fluidi petroliferi (tramite condotte), mette in allarme la sicurezza informatica di un operatore di trasporti gas e si attiva un sistema di emergenza comprendente una squadra di operatori informatici nel campo della security.
Per 8 e più ore tutti gli sforzi sono concentrati nel riportare nella norma le regolazioni dei flussi del gas nelle condotte. I danni economici subiti e ulteriori dettagli non sono stati resi noti , l'informazione è giunta al mondo del web tramite l'esposizione in un convegno di Hacker in Germania da parte di un gruppo operante sui servizi "infrastrutturali", mentre da parte dell'azienda colpita e del governo del paese dove ha sede la corporate qualsiasi informazione è stata secretata.
Dato il tipo di prodotto ed il periodo dell'anno in cui è avvenuto il fatto si presume che i danni economici (per un'attività a variazione stagionale) siano stati ingentissimi.

Caso 8
Un azienda sanitaria riceve un macchinario con caratteristiche innovative che consente di operare tramite un robot che emette raggi ad alta energia in aree molto particolari tramite interventi non invasivi. La macchina è dotata di un sistema computerizzato che, tramite una scansione magnetica, compone in un quadro di coordinate spaziali la ricostruzione tridimensionale sia delle parti molli che della parte ossea del corpo del paziente, della parte ove occorre intervenire.
In questo modo è possibile operare con una precisione dell'ordine di milionesimi di millimetro.
Ovviamente la macchina è stata testata, o meglio è stata provata già in altri paesi con esiti incoraggianti. Nella fattispecie, la macchina in questione, nuova e appena installata, era soggetta (dopo i test di routine

della ditta installatrice e una serie di training al personale che doveva utilizzarla) al primo utilizzo pratico da parte del personale medico. Durante l'inizializzazione della stessa (operazione standard prevista ad ogni inizio di sessione di lavoro) un malfunzionamento della stessa ha prodotto una situazione non prevista. Il personale è ricorso prontamente alle istruzioni (software di supporto gestionale alle operazioni della macchina) sia video che cartacee, e seguendo le istruzioni ha eseguito delle operazioni speciali. Purtroppo l'errore nelle esposizioni delle istruzioni (note mal poste) e l'errore dell'operatore nel limitarsi ad eseguire un comando senza aver letto in modo approfondito tutte le istruzioni fino in fondo, ha determinato una rottura di una parte operativa della macchina e un errore nei settaggi. Chiamata l'azienda produttrice è sorta una diatriba notevole a seguito della comunicazione che la riparazione comportava dei costi pari ad 1/5 del valore dell'intera macchina. L'errore di impostazione del software sarà poi corretto nelle versioni successive (tuttavia la ditta produttrice continua ad asserire che nessun errore di software era presente nella macchina danneggiata); l'errore dell'operatore invece era considerato dalla cliente come una conseguenza dell'errore del produttore; per fortuna, comunque, nessun paziente è stato danneggiato altrimenti il danno corrispondente al milione sarebbe sicuramente lievitato a cifre molto più altre.

Caso 9

In un ospedale ottimamente attrezzato, la sezione medicina nucleare era situata negli scantinati e una particolare attenzione era stata dedicata al personale anche di supporto che poteva accedere al piano interrato. Durante un turno di riposo, la ditta delle pulizie, che normalmente mandava una persona che era stata istruita specificatamente dal personale addetto alle macchine, sostituiva questa persona momentaneamente malata con altra persona del loro staff.
La donna delle pulizie si sostitutiva alla persona malata, e con una grande macchina lava pavimenti procedeva alle pulizie del sotterraneo; le era stato detto di non entrare nelle stanze ove erano presenti le grandi macchine per le radiografie ma, nonostante l'avvertimento, la signora trovando una porta aperta entra a cavallo della macchina lava pavimenti industriale pensando di far bene; la macchina a risonanza magnetica era purtroppo rimasta accesa e l'enorme forza del magnetismo in funzione è risultata talmente potente da attirare improvvisamente la macchina lava pavimenti e con lei la sfortunata donna delle pulizie.
Risultato: macchina a risonanza magnetica distrutta all'80%, donna delle pulizie deceduta, macchina lava pavimenti distrutta, blocco da parte della magistratura del reparto ospedaliero e danno per l'ospedale di svariati milioni di €.

Caso 10

In una banca di medie dimensioni era stato creato un nuovo centro elaborazione dati; il progetto prevedeva la suddivisione del cuore pulsante in due sale macchine identiche e sincrone, in modo da evitare l'interruzione delle elaborazioni nel caso in cui in una delle due sale fosse sorto un problema.
Fabbricati ed impianti nuovi, macchinari nuovi, sistemi di protezione nuovi, tutto all'ultimo stato dell'arte in fatto di sicurezza e efficienza.
Dopo un primo periodo di test tutto è stato messo in funzione con la massima soddisfazione e senza alcun problema, per almeno 2 anni, dopodiché si è verificato un evento imponderabile. Un tubo a soffitto del canale principale del sistema antincendio a gas è esploso danneggiando una delle macchine principali e rendendola inservibile.
Fortuna vuole che la seconda sala fosse perfettamente in funzione e i danni sono stati limitati alla riparazione del computer colpito e del rifacimento dell'impianto A.I. a gas da parte della ditta produttrice. Se il danno fosse avvenuto 3 anni prima quando il CED era costituito da un'unica sala, dove i 2 computer in mirroring sincrono erano uno affiancato all'altro, è molto probabile che la banca avrebbe subito un ingente danno indiretto (di qualche decina di milioni) e delle spese da Disaster Recovery di emergenza a chiamata anch'esse milionarie.

Caso 11

Un porto container a gestione avanzata è in grado di garantire un tempo di carico/scarico dei container in transito inferiore al minuto e mezzo. Il volume di container depositati e in transito si aggira sui 30mila giornalieri e costituisce una delle principali fonti di reddito della zona.
La gestione avanzata è costituita da un sofisticato sistema informatico che recepisce ed integra le informazioni in arrivo da navi e traffico su gomma o ferro, raccoglie in un sistema efficiente le prenotazioni di carico e scarico, tempi e programmazioni con aggiornamenti in tempo reale di tutto il database sulla situazione e posizionamento di ogni container stoccato da caricare o scaricare sui mezzi di trasporto.
Una nuova release più performante del programma viene elaborata e messa in produzione , il sistema si impalla malamente e viene danneggiato anche il database (si perdono le posizioni e le informazioni di circa un migliaio di container), ma quello che è peggio è che non si riesce a trovare il mezzo di ritornare alla situazione pre-incidente. Navi vengono dirottate verso altri porti, code chilometriche sulle strade di accesso al porto container, treni merci fermi nelle stazioni; risultato: una riduzione del 24 % del totale merci in transito per la regione sul quale esiste il porto; i danni economici diretti sono quantificabili, ma quelli indiretti a terzi e da responsabilità assumono dimensioni incalcolabili. Dopo circa 3 mesi, durante i quali la situazione da fuori

controllo passa ad un controllo limitato e poi ad una normalizzazione, il porto torna ad una normalità, ma molti clienti hanno deciso di trasferirsi altrove e il recupero dei flussi di merci non tornerà, almeno per qualche anno ai regimi precedenti (il danno non è stato solo immediato, ma ha avuto anche strascichi per lunghissimo tempo).

Caso 12
Una sala principale situata in un bunker ad un piano interrato confinava con una proprietà di un terzo; a seguito della necessità di ristrutturare alcune parti dell'edificio di questo vicino viene aperto un cantiere nel cortile confinante l'ubicazione della sala macchine. Durante la sosta dei lavori edili un venerdì sera viene lasciato aperto un rubinetto dell'acqua e in breve la situazione si evolve in un allagamento, prima del cortile e successivamente di tutti gli interrati. La sala macchine è presidiata da un allarme antiallagamento che svolge regolarmente la sua funzione, tuttavia non erano mai stati testati i tempi di intervento, che poi al caso pratico si sono rivelati ampiamente insufficienti, e a tal punto che l'intervento dei tecnici ha solo constatato l'avvenuto spegnimento dei sistemi e vari fenomeni elettrici con danni anche consistenti ai back up dell'ultima settimana che era depositato in una saletta a parte, ma sempre nello scantinato. L'inesistenza di un sistema automatico di evacuazione dell'acqua, la progettazione errata dei percorsi dei cavi (nel sottopavimento anziché a soffitto), l'intervento a seguito dell'arme tardivo, hanno reso il danno molto consistente e di impatto economico significativo.

Caso 13
Una società di telecomunicazioni propone dei servizi aggiuntivi ai propri clienti, tra i quali l'abbinamento ai servizi telefonici fissi con quello dei portatili; cioè, in pratica, è possibile addebitare i costi del cellulare sul contratto del fisso. Per rendere l'operazione molto semplice ed appetibile, vengono volutamente "semplificate" le operazioni di riconoscimento delle istruzioni al servizio automatizzato. Il crimine organizzato provvede a verificare il punto debole delle procedure e si inserisce nel sistema trasferendo ingenti costi di traffico telefonico (probabilmente vendendo in automatico tale potenzialità di traffico reperita dolosamente) ai conti degli ignari frodati. Alla resa dei conti, quando vengono richieste somme milionarie di recupero di traffico telefonico, la società di telecomunicazione si accorge del "buco" e provvede a trattare un accomodamento interno con i creditori; ai clienti restituisce conteggi depurati di tale abnorme traffico per un normale pagamento delle bollette.

Caso 14
Sembrerebbe incredibile, ma un danno ai dati è stato sofferto per il "peso"dei medesimi, espresso in chili ! in effetti, è proprio successo così: una scaffalatura mal progettata e peggio realizzata è crollata sotto il peso di migliaia di cassette, danneggiandone una certa quantità per effetto dell'urto nella caduta.

Caso 15
L'evoluzione dei sistemi informatici ha portato alla concentrazione, anche di peso per metro quadro dei macchinari principali coinvolti, sostituendo macchinari obsoleti con macchinari moderni; in una sala macchina si è verificato un "crollo" del sottopavimento flottante (evidentemente progettato in passato e al limite della portata media) con il risultato che alcune macchine nuove si sono danneggiate; è stato necessario smontare tutto il centro e rifare l'intero pavimento flottante e rimontare tutto. Tempi lunghi per un CED e danno notevole in tutti i sensi soprattutto per i periodi di mancato utilizzo (danno economico).

Caso 16
In un ospedale, un piccolo incendio che ha bruciato una piccola quantità di plastica ha prodotto fumo corrosivo che ha danneggiato i circuiti dei macchinari di analisi del sangue, di analisi cliniche, e altri macchinari medicali elettronici di laboratorio. Solo per effettuare lo smontaggio, la pulizia ed il rimontaggio è stato speso un importo significativo in rapporto al valore delle macchine colpite.

Caso 17
Il virus Config ha prodotto una pandemia in un sistema di qualche migliaio di unità collegate in rete. I tempi di intervento e di controllo per un sistema pubblico ha determinato danni ingenti (la loro stima però non è stata divulgata e non è dato di saperne di più in quanto non erano assicurati).

Caso 18
Una fabbrica ha un sistema automatizzato di reperimento ordini, produzione, confezionamento, e spedizione tramite robot. Un problema (software) di funzionamento del collo di bottiglia costituito dal robot di prelevamento del prodotto finito per il confezionamento dei colli e di consegna al reparto spedizione ha prodotto un fermo degli interi processi lavorativi, pari ad una settimana.

Caso 19
Una società finanziaria ha affidato a un impiegato esperto la gestione di alcuni portafogli, nell'ambito di limiti precostituiti e definiti nei processi operativi informativi. L'individuo ha provveduto a forzare i medesimi ai fini di ottenere sempre migliori risultati ad ogni fine mese di chiusura del bilancio di attività. Viene scoperto, dopo un periodo di alcuni anni, che l'ottimo impiegato aveva esposto l'azienda per cifre esorbitanti, e questo quando il volume delle perdite non poteva più essere nascosto tramite forzatura del sistema informativo.

Caso 20
Un paese del terzo mondo gestisce le proprie telecomunicazioni tramite un service esterno privato; il sistema è configurato con un modello misto cluster e cloud. L'errore di settaggi da parte di un operatore di un server produce un effetto domino che si trasmette a migliaia di server in tutto il paese. Il conseguente fermo produce un danno stimato in 140 milioni di $ complessivamente tra spese di revisione di tutti i server e perdite, spese extra dovute a costi di comunicazione alternativi durante il fermo, perdite economiche effettive. L'assicurazione in corso era in copertura per un capitale pari a meno del 10% dell'effettiva perdita subita, causa un errato assessment del rischio che aveva considerato il sistema completamente al sicuro da eventi informatici catastrofici.

Caso 21
Un errore di implementazione di una patch di aggiornamento del software messa in produzione blocca un sistema aeroportuale che gestisce 30.000 passeggeri al giorno e merci corrispondenti.
Il blocco totale dura un giorno e diversi sono i giorni necessari per smaltire l'arretrato accumulatosi nello smaltimento bagagli (con un incremento dei costi di spedizione, e delle perdite dei medesimi).

Caso 22
Un'azienda che produce il suo business con l'aggiudicazione di gare soffre di una riduzione degli esiti positivi con corrispondente riduzione del fatturato annuo. Ad un'indagine più approfondita del management si scopre che la flessione corrisponde all'uscita di uno dei principali agenti di vendita che si è messo in proprio. Denunciato il fatto alle autorità, l'indagine di polizia scopre che un programma spyware inserito nei computer dei dipendenti comunicava in real time alla concorrenza, in anticipo sulla data della gara, i piani di vendita e i prezzi che poi venivano comunicati (ecco perché i prezzi della concorrenza erano sempre inferiori a quelli dell'azienda colpita). L'Agente di vendita viene arrestato dopo aver scoperto l'indirizzo finale dove arrivavano le informazioni estorte dal programma dannoso, tuttavia la perdita di mercato e il profitto perduti non potranno essere rimborsati per mancanza di fondi del colpevole. Trattasi di un 30% del fatturato annuo.

Caso 23
Una corrispondenza interna di una grande azienda farmaceutica crea allarme negli amministratori: dati molto riservati sono stati divulgati anche a personale di livello inferiore (sul network interno tramite un'e.m.). Si cerca di trovare il responsabile, si cerca di verificare se sono stati violati luoghi informatici protetti da sistemi di riconoscimento avanzati; il pericolo che formule protette da segreto, possano essere esportate, copiate e vendute al mercato alternativo dei farmaci illegali è reale. Le ricerche sono tutt'ora in corso. Ovviamente sono stati avvisati gli organi competenti, ma si procede anche a indagini affidate ad esperti ed i costi sono elevati. Purtroppo le triangolazioni delle telecomunicazioni passanti da paesi che non ottemperano alle disposizioni internazionali sulle telecomunicazioni e agli obblighi Interpol hanno interrotto le ricerche nelle telecomunicazioni.

Caso 24
Una perdita dai tubi a soffitto del riscaldamento di acqua calda (per corrosione) cola su un UPS situato in uno scantinato di un centro elaborazione dati e la macchina si danneggia irreparabilmente essendo composta da due unità indipendenti, ma in un'unica macchina. Il centro di elaborazione è stato arrestato per un giorno dopodiché si è provveduto ad un allacciamento provvisorio di emergenza con un sistema temporaneo in affitto, con costi imprevisti e pesanti.

Caso 25
In un palazzo alto un CED è stato trasferito interamente in altra località a causa di un collasso in atto delle strutture portanti del palazzo; le vibrazioni della strada veloce a grande scorrimento costruita a fianco hanno determinato la situazione di emergenza. Poiché la ditta non era dotata di un centro speculare sito in un'altra località, né di un disaster recovery a freddo presso terzi, ha dovuto acquistare il servizio in emergenza pagando costi elevatissimi per evitare di fermare per giorni l'attività aziendale.

Caso 26
Durante il trasferimento con una gru di un sistema dal 20° piano di un grattacielo al truck in attesa al piano stradale, il gancio della gru cede e la macchina principale si sfracella al suolo. Perdita del macchinario per 15 milioni di $ e dei dati per qualche milione (solo i dati dell'ultima settimana). La Banca non era assicurata

per l'evento, il vettore non aveva un assicurazione corrispondente, la gru non era assicurata per una cifra del genere, il danno è stato praticamente quasi interamente assorbito dalla banca.

Caso 27

In un grande centro elaborazione dati vi sono molte salette separate, ognuna con i suoi sistemi di protezione e allarme, con separazioni di pareti mobili non a prova di incendio. Una sala è occupata da una nuova società la quale trasporta i propri apparecchi, server e mainframe. Durante il trasporto delle apparecchiature con i muletti da parte degli operai addetti al trasloco un operaio urta violentemente con il gomito una cassettina fissata a parete contenente il pulsante di attivazione manuale del sistema antincendio a gas, anche se protetto da vetro (rotto per il colpo del gomito dell'operaio). La scarica si attiva e occorre procedere alla ricarica dell'intero parco bombole con il relativo costo. La polizza incendio non ha risarcito le spese né il danno alle macchine già presenti e funzionanti nella sala, non era in vigore una polizza informatica, il danno è stato assorbito dalla Società di servizi.

Caso 28

In un centro elettronico di grande importanza (duplicato interamente in due palazzi differenti nella medesima località), ovvero appena insediato ex novo da circa 2 anni, alla prova del diesel generatore elettrico di emergenza si sviluppa un incendio nei locali dove è situato il motore. Fortunatamente non vi è stata interruzione di servizio in quanto si trattava solo di una prova "a caldo" e per prudenza il circuito era mirrorato in sincronia con la rete standard.
Il danno si è limitato alla sola operazione di smontaggio e pulitura della centralina di controllo della macchina. Si è appurato che l'origine era dovuta ad un falso allarme della centralina elettronica che ha provocato un surriscaldamento del circuito (scheda), evidentemente non installata nel modo corretto. Immaginate cosa sarebbe successo in caso di vero allarme con richiesta di attivazione immediata del diesel di emergenza. Un incendio nella sala del motore, il fermo dell'alimentazione ai sistemi, la perdita dei dati in corso di elaborazione, l'arresto delle attività controllate dal sistema (con potenziali danni a cascata nelle località ove risiedono i meccanismi controllati a distanza). Una eventuale distruzione totale di un settore produttivo non sarebbe stata da escludere.

Caso 29

In un centro elaborazione dati di media grandezza l'attivazione intempestiva di un interruttore generale ha provocato un immediato ed inatteso fermo generalizzato dell'intero parco macchine (l'interruttore non era duplicato e non era bypassabile) con perdita di tutti i dati in elaborazione nelle macchine, nei sistemi di back-up, nelle librerie sorgenti, l'interruzione dei server di telecomunicazione dati, centralino telefonico, etc… All'accadere del fatto, il medesimo interruttore si è guastato irreparabilmente. La ripresa dell'attività ha richiesto un certo tempo in quanto la sostituzione dell'interruttore non rientrava tra le SLA delle società di servizio di manutenzione elettrica. Ha richiesto inoltre un certo tempo la restaurazione dei dati da vecchie copie di sicurezza, che ha aggravato il fermo di alcune macchine principali. E' in corso uno studio per duplicare tale interruttore con by-pass automatico in caso di guasto. L'intera attività è ripartita solo dopo 4 giorni, non considerando gli strascichi di attività a minore impatto di business.

Caso 30

La scoperta da parte di un operatore di sala di un mini-bug nel sistema contabile ha indotto l'operatore ad inserire nel sistema dei codici che trasferivano i resti contabili del calcolo dei rimborsi di tassazione su stipendi dei dipendenti (migliaia), quando dal calcolo comparivano decimali oltre la seconda cifra, su un file specifico. Quest'ultimo poi disponeva il trasferimento degli importi ad altro file collegato con un conto "fornitore" fasullo creato per l'occasione tramite un web bank, che procedeva successivamente ad inviarlo ad una banca estera in automatico. Poiché non vi erano rilevazioni di errori nei conti aziendali e nei controlli fiscali, il meccanismo fraudolento ha potuto funzionare per un periodo sufficientemente lungo da maturare una cifra milionaria. Fino al momento in cui per un errore di consegna i supporti dei dati sono stati consegnati ad un'altra ditta, i cui tecnici si sono accordi dello scambio (tipologia e macchina identici, e sistemi molto simili); infatti all'inserimento del supporto per la lettura dei dati il sistema più avanzato della loro ditta, ha segnalato l'anomalia prodotta dalla modifica dei sorgenti con un'allerta immediato. Alla riconsegna dei supporti al giusto indirizzo ha fatto seguito la comunicazione di quanto scoperto per caso e da lì sono partiti i controlli approfonditi che hanno scoperto la frode dell'operatore che nel frattempo aveva già lasciato l'azienda. Condannato in contumacia il medesimo non ha restituito il maltolto ed è tuttora ricercato. L'importo del danno economico sofferto è stato stimato tra i 4 e i 6 milioni di €, non coperto da nessuna polizza di assicurazione in vigore in quanto quella casistica (frode informatica) non era stata prevista nell'analisi di rischio dai responsabili dell'azienda.

Caso 31

Un enorme impianto chimico produce sostanze (semilavorati) destinati ad essere inviati ad altre fabbriche del gruppo per la produzione dei prodotti finiti. Il ciclo dell'impianto è controllato da PLC e da sofisticati sistemi di controllo, e i residuati della lavorazione sono costituiti da gas che necessitano di essere bruciati ad alte temperature per ottemperare alle norme antinquinamento. Alla fine dell'intero processo i residuati finiscono in un forno che alimenta una caldaia per la produzione di vapore ad alta temperatura e pressione necessaria ai processi produttivi. I fumi che fuoriescono sono controllati da sonde che riportano ad un sistema informatico di controllo che registra i valori e la composizione chimica dei gas combusti per controllare che siano all'interno dei parametri fissati per legge. Una piccola modifica ai comandi del sistema di controllo, per ottenere maggiore flessibilità nei controlli, ha determinato una staratura dell'intero sistema, che aveva anche il compito di regolare le temperature dei gas combusti che accedevano ai filtri finali prima della liberazione in atmosfera dei residui dai gas combusti. In questo modo il surriscaldamento dei filtri mal controllato ha sviluppato con il tempo un incendio che ha danneggiato irreparabilmente sia i filtri che alcune saldature della caldaia. Il processo produttivo a questo punto viene interrotto in emergenza, si ricorre al tentativo disperato di trovare sul mercato internazionale un macchinario con caratteristiche similari, per continuare la produzione almeno parzialmente per evitare ulteriori spese di fermo e ripartenza dell'intero impianto. I tempi di rimpiazzo della parte distrutta (caldaia e filtri) risulteranno biblici (4 mesi), il tentativo maldestro di modificare il software che regolava i parametri di controllo ha prodotto effetti devastanti e alla fine il danno sugli utili da mancata produzione per il gruppo supererà i dieci milioni di €.

Caso 32

Una società di servizi IT avvia un progetto per l'unificazione delle credenziali per l'accesso alla posta elettronica con altre in uso per l'accesso ai servizi applicativi presenti nella propria Server Farm, al fine di garantire una maggiore semplicità d'uso a tutti gli utenti. Per rendere possibile la fase di sincronizzazione (ovvero della transizione tra l'utilizzo delle vecchie credenziali e quelle nuove, pur garantendo la continuità del servizio), si attiva a titolo sperimentale un collegamento tra il sistema di posta e il database centralizzato delle utenze, pur lasciando la possibilità tecnica, agli utenti coinvolti in questa sperimentazione, di continuare ad accedere al sistema di posta elettronica anche attraverso il database centralizzato, utilizzando le parole chiave del loro programma originario. In questa fase del progetto non si è avuta evidenza di una criticità, ovvero che non tutte le credenziali contenute nel database centralizzato rispondevano ai necessari requisiti di sicurezza. Tale situazione si era verificata come conseguenza della migrazione, avvenuta anni prima di un database il cui ambiente originario conteneva tali credenziali quali completamento all'uso di un certificato elettronico su smart card. In particolare, mentre l'utilizzo congiunto della smart card e delle credenziali era necessario per l'utilizzo degli applicativi, l'accesso ai servizi di posta elettronica era possibile mediante il solo utilizzo delle credenziali. Le credenziali di accesso originariamente assegnate agli utenti erano costituite dal numero di matricola degli stessi, con user ID e password uguali. La maggior parte degli utenti non ha mai modificato queste impostazioni iniziali. Tempo dopo l'attivazione del suddetto programma di unificazione, la società di servizi IT riceve segnalazione da parte di importanti clienti (per numero di collegamenti) che la possibilità di utilizzo dell'autenticazione verso la propria casella di posta era stata individuata ad alcuni utenti DI di altra azienda. La società di servizi IT si attiva quindi a controllare il log degli eventi del servizio di posta elettronica, riscontrando n. 13 collegamenti attuati attraverso "altra azienda" nell'ultimo recente periodo. Di questi, solo due avrebbero potuto non essere avvenuti da parte del legittimo assegnatario della casella di posta, ed entrambi erano relativi ad un medesimo personal computer che risultava assegnato ad un'utenza diversa da quelle usate per l'accesso alle due caselle di posta. A seguito di quanto emerso, i clienti che si sono ritenuti danneggiati formalizzano la sospensione dei pagamenti per le attività complessivamente svolte dalla società di servizi IT (anche se diverse rispetto al servizio di posta elettronica) per un totale di svariati milioini di €, manifestando il proposito di rivalersi sia per i danni di immagine subiti, sia per le ulteriori azioni a fronte di eventuali ricorsi e/o segnalazioni di terzi. Successivamente la società di servizi IT riconosceva alle clienti "a titolo di indennizzo per il disservizio" causato, una riduzione dei corrispettivi dovuti per le attività previste nel contratto di appalto relativamente all'anno in corso. Il relativo importo è l'oggetto del risarcimento da parte degli assicuratori.

Caso 33

E' un'azienda che produce food operando principalmente nel mercato italiano e marginalmente in quello estero. L'attività che comprende l'intero ciclo di lavorazione delle materie prime conta un fatturato annuo complessivo inferiore a 30 milioni di €. Il danno è riconducibile a un attacco informatico a causa di ignoti subito dall'Assicurata. In tale circostanza il server internet dell'Assicurata veniva sottoposto a molteplici interrogazioni informatiche esterne, generate automaticamente da un server estero, che provocavano la saturazione della banda internet riservata inibendone la connettività nonché generando una quantità abnorme di dati che, memorizzati dal sistema, venivano riversate nei dispositivi di back-up presenti, saturandone la memoria disponibile. Il malfunzionamento del sistema informatico veniva rilevato solamente il lunedì successivo, alla ripresa dell'attività lavorativa e, riscontrando alcuni problemi di connettività alla rete internet, veniva in un primo tempo attribuito al malfunzionamento della rete della società di

telecomunicazioni. Solo dopo l'intervento dei tecnici di quest'ultima veniva riscontrata l'anomala attività esterna ed il malfunzionamento riscontrato veniva attribuito ad un attacco di tipo DoS (Denial of Service). Le successive indagini eseguite del personale di un'impresa specializzata in sicurezza informatica, hanno ricondotto l'origine dell'attacco ad un server estero ubicato nell'area di un paese estero esotico, le cui interrogazioni però sono rimaste tutt'oggi senza seguito.

Caso 34
Diverse case di servizi informatici (relativamente a messaggi di posta elettronica, foto pubblicitarie o geografiche,stradali, e informazioni personali di libero accesso sui siti) sono in questo momento soggette alle azioni di controllo.
Si sono scoperti "errori " negli script del software che era stato in un primo luogo predestinato per un utilizzo di rilevazione "geografica" e successivamente utilizzato per altri applicazioni senza le opportune correzioni.
I costi per rivedere tutti i dati con software di controllo che cancellino automaticamente quelli ricadenti all'interno delle leggi della privacy dei vari paesi, si preannunciano piuttosto elevati (milioni di $ per cancellare un volume di dati stimato inferiore ad un terabyte, ma sparso in migliaia di server in giro per il mondo).

Caso 35
Una attività medicale è stata soggetta ad una condanna da parte di un giudice per aver reso possibile la divulgazione ai familiari del tipo di malattia che aveva colpito il paziente.
Nella fattispecie il riconoscimento è stato fatto tramite il tipo di principio attivo utilizzato e indicato nei file relativi alla persona in questione.
Per i soli "interessi affettivi lesi" di questa unica persona il danno è stato quantificato in 15.000€.

Caso 36
In uno stato la campagna elettorale è stata attuata anche inviando a ciascun elettore una lettera con contenuti promozionali, inclusi gadget, coupon e una specie di riffa a premi. Il tribunale ha ricevute denunce per il tipo di promozione, ed ha indagato in quanto l'elenco era stato composto con una selezione di persone bisognose o comunque in difficoltà economica troppo precisa. In tribunale il responsabile inquisito è stato accusato di aver avuto accesso illecito ad elenchi contenuti nei file dell'assistenza pubblica. La condanna proposta in qualche anno di reclusione è ancora in corso di discussione a livelli superiori di giudizio. A questo si aggiunge una collaterale azione giudiziaria per scoprire se i dati sensibili sono stati solo strafugati o se per effettuare l'operazione è stato necessario "bucare" il sistema dell'amministrazione pubblica, nel qual caso i responsabili della gestione dei sistemi informatici sarebbero indagati per cattiva gestione dei sistemi sotto l'aspetto della privacy.

Caso 37
Un'impresa multinazionale è sotto inchiesta per una denuncia interna effettuata all'autorità di controllo del paese dove opera. Nonostante la difesa dei legali dell'impresa è notorio che una consistente fetta di corporate (aziende con più di 20 mila dipendenti), circa il 41 percento, ha assunto personale specializzato nell' "analizzare" le e.m. e i contenuti della posta in uscita, in evidente contrasto con le disposizioni legislative nazionali e accordi internazionali. Quasi la metà delle corporate esistenti ha subito "perdite" importanti di informazioni che hanno portato a licenziamenti (il 26% di queste ha proceduto in tal senso) verso i colpevoli. Se il 14% di tali aziende lamenta addirittura la pubblicazione sulla rete di informazioni ritenute riservate, si capisce perché l'allerta è scattato anche se il prezzo è poi quello di ritrovarsi in contrasto con le disposizioni sulla privacy. Seguiamo gli sviluppi di questo processo perché potrebbe fare da esempio e portare la questione in sede politica al fine di modificare le leggi sulla privacy.

Caso 38
Una grande azienda nel campo della distribuzione ha subito una condanna, commutata in una sanzione pecuniaria di poco inferiore ai 100k€, per non aver informato correttamente la clientela dell'uso che avrebbe fatto dei dati forniti al momento dell'adesione dei clienti al programma di fidelizzazione, sulla pagina web del proprio sito. Alla sanzione si è aggiunta l'intimazione entro breve di rielaborare tutti i dati in possesso della clientele, in modo che l'attività in corso di classificazione degli utenti in base alle abitudini di acquisto potesse essere fermata e ricondotta a quanto previsto per legge in assenza di esplicito consenso degli utenti. La stima del danno per queste spese extra e delle perdite collegate all'arresto della strategia di "profilazione" e "marketing" della clientela sono ancora da stimare.

Caso 39
Una imprecisa imputazione dei parametri di settaggio di un sistema antincendio automatico ha costituito l'origine di una danno causato dall'errato funzionamento del sistema automatico di estinzione , con danni inerenti non solo al costo della ricarica del sistema medesimo, ma ad un temporaneo fermo del

funzionamento della sala degli elaboratori per le necessarie operazioni di pulizia e verifica funzionale,il tutto ha generato spese e perdite ingenti.
Poiché l'origine del danno è stato il funizonamento erroneo del SAI dovuto ad un errore nel flusso dei dati di gestione remota la polizza incendio in corso non ha pagato.

Caso 40
Durante un lavoro di routine di consolle il tecnico che aveva in carico il reperimento tramite interrogazioni del sistema, di informazioni necessarie allo stabilire future esigenze di ampliamento del sistema medesimo, a seguito di un errore di imputazione delle istruzioni ha inavvertitamente modificato alcuni piccoli parametri di gestione del sistema di archiviazione generale determinando una perdita di informazioni quantificabile in una misura superiore a 1500 Tera. La stima del danno non è ancora stata quantificata perché dipenderà dal costo medio di ricostruzione e reperimento delle informazioni perse o danneggiate (illeggibili). Sono inoltre in corso investigazioni per capire come mai nonostante tutti i controlli incrociati di sistema sia stato possibile che nessun avviso di emergenza abbia messo in allerta il personale di controllo , né da parte dei sistemi automatizzati ,ne da parte degli addetti al controllo "manuale" tramite le dash-board.

Caso 41
A seguito di un errore, i tecnici adibiti ad un test sull'impianto di estinzione a gas, appena installato in sala macchine di una grande azienda, invece di eseguire il test (che prevede la disattivazione delle valvole di rilascio delle scariche di gas) in modo corretto su tutte le valvole, hanno dimenticato di disattivarne una. Il risultato è stato che al momento dell'attivazione (che doveva essere in bianco) la valvola aperta ha determinato l'effettivo rilascio del gas e come conseguenza anche il rilascio di tutte le altre valvole (per effetto di una doppia sicurezza nel sistema contro i malfunzionamenti).
A seguito del rilascio di tutte le scariche il gas è fuoriuscito effettivamente in sala macchine. A seguito della fuoriuscita del gas, a sistema informativo in funzione , circa il 40 % dei dischi dell'intero sistema si sono rotti completamente, interrompendo ovviamente il funzionamento dell'intero Centro Elaborazione Dati.
Con la ricostruzione di quanto successo si è capito che il danno ai dischi è stato causato da un ultrasuono prodotto solo dal sibilo del gas fuoriuscito dalle testine.
Dopo l'incidente la ditta produttrice delle testine ha cambiano forma alle testine e pagato il danno procurato. Tuttavia non è dato di sapere quante testine siano ancora in giro in Centri elaborazione dati sparsi per il mondo con quel tipo di testina e, poichè i test vengono effettuati in fase di progettazione dell'impianto (door fan test) a locali vuoti e poi sempre a freddo, non ci saranno frequenti casi simili. Tuttavia il rischio esiste fino a che tali testine non verranno sostituite.

Riccardo Scalici
Socio Fondatore del Clusit
Senior Underwriter Dir.Technical Lines
ACE European Group Ltd
riccardo.scalici@acegroup.com
