Resilienza e Gestione del Rischio: antagonismo o complementarietà?

Due concetti che, finalmente, hanno sempre maggiore diffusione nel contesto ICT sono quelli di gestione del rischio e di resilienza. Molti vedono questi concetti, e le metodologie ed i processi associati, in opposizione, altri li vedono invece come complementari. Per approfondire il dibattito può essere utile ripartire dalle definizioni. Secondo Wikipedia, la resilienza è la capacità intrinseca di un sistema di adattarsi al cambiamento ovvero di adattarsi alle mutate condizioni d'uso e di modificare il proprio funzionamento prima, durante e in seguito ad un cambiamento o ad una perturbazione in modo da continuare ad offrire il servizio richiesto. La defizione della National Accademy of Science è simile perchè afferma che la resilienza è " la capacità di pianificare, prevedere e prepararsi ad assorbire, recuperare da, ed adattarsi a, eventi avversi". Il focus su singoli eventi è quello che differenza la resilienza dal disaster recovery, che ha impatti molto più vasti e devastanti sul sistema di interesse. La resilienza è ovviamente una proprietà emergente del sistema che non dipende da un singolo componente ma dalla interazione tra i diversi componenti che formano il sistema. Un sistema resiliente è in grado di offrire i propri servizi sia in condizioni previste che in condizioni impreviste. Ovvero, un sistema resiliente riesce ad offrire i propri servizi anche in condizioni che il progetto non ha saputo prevedere. Ovviamente, le prestazioni possono essere, per un tempo più o meno lungo, inferiori a quelle in condizioni normali. Vi sono più cause dell'incapacità di progettare ed adottare nel sistema strategie che evitino la caduta temporanea delle prestazioni, ma la root cause è la carenza di informazioni accurate e complete sul contesto del sistema.



Fig. 1 Curva delle prestazioni in funzione del tempo

La curva in fig. 1, da systemic2016, illustra alcuni comportamenti possibili di un sistema resiliente a seguito di un disturbo, raffigurato in rosso. Ad esempio, il disturbo può essere dovuto ad un guasto o ad un attacco malizioso. La possibilità di considerare sia guasti che attacchi come disturbi evidenzia che quando parliamo di resilienza non interessa distinguere tra safety e security. Il sistema descritto in figura ha una propria robustezza intrinseca che gli consente di resistere al disturbo per un tempo tre, poi le sue prestazioni iniziano a diminuire. Ovviamente, in un sistema ideale, tre ha sempre durata superiore al disturbo ma adottare una soluzione che soddisfi questo vincolo può essere, come discusso nel seguito, impossibile o, talvolta, non conveniente. Quando il sistema raggiunge il suo livello di prestazioni minimo, può evolvere in diversi modi. La curva D descrive il comportamento di un sistema non resiliente, che crolla definitivamente e non riesce più ad offrire il livello di servizio richiesto. Le altre tre curve descrivono tre comportamenti diversi ma tutti resilienti. Infatti, in ogni caso il sistema riesce ad offrire un livello di servizi superiore al minimo richiesto. Il sistema più resiliente è ovviamente quello descritto dalla curva A perché reagisc con un bounce-back grazie al quale le prestazioni ritornano al livello iniziale dopo un tempo tre+tra. Le curve B e C descrivono un sistema che utilizza o un ripristino parziale o un cambio di regime. In un cambio di regime, il sistema reagisce al disturbo adottando un nuovo comportamento, diverso da quello iniziale. Strategie di ripristino basate su un cambio di regime sono il risultato di strategie di resilienza ispirate a sistemi ecologici. Ad esempio, in questi sistemi alcuni componenti possono comportarsi in modo diverso dopo il disturbo, adottando algoritmi più semplici ma meno efficienti.

La resilienza di un sistema può essere ottenuta integrando tre

strategie:

1. Ridondanza dei componenti, sia calda che fredda
2. Monitoraggio dei comportamenti sistema
3. Riconfigurazione.

Sostanzialmente, un sistema resiliente deve innanzitutto monitorare i propri componenti e reagire ad eventi quali fault, attacchi o malfunzionamenti che si manifestano come comportamenti anomali, che violano cioè le specifiche del sistema. Tipiche violazioni possono essere tempi di risposta lunghi a richieste degli utenti, timeout su accessi a database oppure improvvisi picchi di carico in sottoreti di solito non utilizzate. Questi eventi possono essere dovuti sia a guasti di server che gestiscono database o a malware che tentano di esfiltrare informazioni. La reazione del sistema all'anomalia utilizza la ridondanza del sistema, che deve essere stata introdotta in fase di progetto, per riconfigurare il sistema rimpiazzando i componenti non funzionanti. Ad esempio, tipiche riconfigurazioni sono la migrazione di una macchina virtuale da un nodo di un cloud ad un altro, l'attivazione di una versione di backup di un database oppure la modifica delle politiche di routing nel control plane di una software defined network. Questi esempi evidenziano, innanzitutto, come un sistema resiliente non debba necessariamente distinguere le cause di un disturbo ma sia interessato solo agli effetti, ovvero alla perdita di prestazioni. Unica caratteristica di interesse da questo punto di vista è se la causa dei disturbi sia temporanea o permanente perché le due situazioni richiedono strategie di riconfigurazione diverse. Altra caratteristica è la risposta automatica del sistema, che deve saper reagisce senza un intervento esterno. Infine, gli esempi citati evidenziano anche come l'adozione di soluzioni software aumenti la flessibilità del sistema e quindi la possibilità di riconfigurarne il funzionamento.

La breve disamina precedente dimostra che il costo della resilienza è dato dalla somma del costo dei componenti

ridondanti e da quello dei componenti per monitoraggio e riconfigurazione. Entrambi i costi comprendono sia quelli di acquisizione che quelli per esecuzione e gestione. È evidente come l'aumento sia non banale. Mentre il costo di acquisizione è fisso, un investimento fatto al momento della installazione e configurazione, quello per l'esecuzione e la gestione dei componenti deve essere pagato per tutta la vita del sistema. Un caso in cui il secondo costo è ridotto è quello di sistemi molto dinamici con significative variazioni del carico di elaborazione gestite mediante riconfigurazione dei componenti. In questo caso, il sistema comprende già componenti di monitoraggio e riconfigurazione. Pensiamo ad esempio ad un sistema dove il bilanciamento dinamico del carico di elaborazione attiva o congela delle macchine virtuali. In questo caso, il monitoraggio delle prestazioni e la riconfigurazione è insito nel sistema. La strategia di bilanciamento del carico risultante può essere vista come una prima, semplice resilienza rispetto al disturbo generato da variazioni non prevedibili nel carico di elaborazione.

Per evidenziare le differenze tra un approccio basato su analisi e gestione del rischio ed uno su resilienza, è sufficiente considerare che un sistema resiliente non è interessato alla specifica causa del disturbo. Invece, l'analisi e la gestione del rischio è focalizzata su individuare le possibili sorgenti di attacco o malfunzionamenti e caratterizzarle nel modo più adeguato. Vari passi dell'analisi del rischio, quali l'analisi delle minacce o quella delle vulnerabilità, devono raccogliere ed analizzare informazioni sulle sorgenti di attacco e sui difetti del sistema. Ad esempio, nel caso di un attaccante intelligente, l'analisi è interessata a capire, tra gli altri, le strategie di attacco che adotta, le informazioni di cui dispone e gli obiettivi strategici e tattici che si pone. Se, invece, stiamo considerando problemi di safety, informazioni importanti sono i tipi di guasto che si possono verificare e l'impatto di ognuno. Tutte queste informazioni vengono raccolte e

strutturate dall'analisi delle minacce, passo fondamentale di ogni analisi del rischio. Tanto più accurate le informazioni che questa analisi restituisce, tanto migliori saranno sia la valutazione del rischio sia la scelta delle contromisure da adottare per annullare o minimizzare il rischio per il sistema considerato. Senza informazioni accurate è, ad esempio, del tutto impossibile stimare il rischio in modo quantitativo o semi-quantitativo e quindi decidere se un certo investimento in contromisure è conveniente o meno.

Esistono ovviamente strategie per condurre analisi accurate gestendo la eventuale incertezza nelle informazioni disponibili. Ad esempio, l'uso di intervalli invece che di valori puntuali permette di trattare informazioni che possono essere affette da errori. In taluni casi, l'incertezza viene rappresentata mediante delle probabilità. Un possibile esempio è il successo o fallimento di un attacco o alla presenza di una particolare vulnerabilità in un componente. Un metodo fondamentale per una valutazione accurata del rischio anche in presenza di distribuzioni di probabilità è il metodo Monte Carlo perchè permette di raggiungere valutazioni accurate al prezzo di esperimenti ripetuti. In altri sistemi, l'incertezza non è dovuta a mancanza di informazioni ma è epistemica, cioè dovuta alla non completa comprensione di alcuni fenomeni. In questi casi, l'incertezza è generata dalla indisponibilità di un modello adeguato a spiegare i fenomeni di interesse. Ad esempio, non disponiamo ancora di modelli adeguati per descrivere alcuni fenomeni fisici o particolari comportamenti umani. Tipico esempio è la catena di motivazioni che spingono un utente a clickare su un link di phishing o a rispondere ad una mail dalla Nigeria. Spesso non sappiamo risolvere l'incertezza epistemica mediante le probabilità proprio per la nostra insufficiente conoscenza del fenomeno. Questa è l'incertezza a cui si riferisce, per altri motivi e con altri fini, la celebre frase su "Unknown unknowns" di Donald Rumsfeld, ciò che non sappiamo di non sapere.

È bene sottolineare che talvolta l'incertezza su un sistema non può essere risolta semplicemente raccogliendo dati sul comportamento passato del sistema e confrontandolo con quello attuale per scoprire eventuali anomalie. Molte anomalie strutturali vengono scoperte solo al verificarsi di specifici eventi che hanno impatti severi e possono verificarsi con probabilità estremamente bassa, ma non trascurabile. Un esempio è la storia del tacchino che viveva tranquillo perché nell'ultimo anno tutti lo avevano accudito e che solo nel giorno del Ringraziamento scopre la vulnerabilità sistemica che lo coinvolge. Questo problema, segnalato da N.S. Taleb nei suoi libri ed articoli a partire dal celeberrimo Black Swan, è legato ad una distribuzione di probabilità che tende asintoticamente a zero, ad esempio all'aumentare del possibile impatto. Il problema è che la distribuzione di probabilità non raggiunge lo zero abbastanza velocemente, perché ha una thick tail. Se una distribuzione di probabilità di questo tipo regola un certo fenomeno, raccogliere informazioni storiche non solo è inutile, ma anche fuorviante e l'unica strategia possibile per una analisi del rischio è un approccio proattivo che focalizzi il metodo Monte Carlo su alcuni eventi di interesse. Ad esempio, per studiare l'effetto di guasti multipli si può assumere che alcuni guasti siano già avvenuti ed analizzare il comportamento del sistema al verificarsi dei guasti successivi. Questa analisi produce informazioni utili a minimizzare rischi catastrofici anche quando la catena degli eventi corrispondente ha probabilità minima.

Nonostante il grande numero e la flessibilità degli strumenti a disposizione per gestire informazioni poco accurate o incerte, è sicuramente vero che in alcuni sistemi, o meglio in particolari contesto di utilizzo, l'incertezza domina. Ad esempio, alcuni sistemi, per vincoli legali o geografici, non possono essere manutenuti o aggiornati. Per questi sistemi non è possibile, ad esempio, ripetere con una frequenza prefissata l'analisi del rischio per adeguare le contromisure. In questi contesti, ed in tutti quelli in cui non si sanno descrivere le

minacce ed i loro obiettivi, un approccio basato su resilienza può essere preferibile.

Ma questo non esclude comunque l'utilità di una valutazione e gestione del rischio perché questo aumenta la robustezza del sistema, e quindi il tempo tre di fig.1, in modo economicamente conveniente. Infatti, come ricordato, un approccio basato su resilienza è necessariamente più costoso in termini sia di componenti che di gestione dei componenti del sistema di uno basato sulla analisi e la gestione del rischio. Un'analisi del rischio che disponga di informazioni accurate o che sappia utilizzare anche informazioni incerte, permette di stimare tre in modo accurato e di gestire il rischio con un numero ridotto di interventi mirati, e quindi di per sé economici. Il numero di interventi, e quindi il costo della gestione del rischio, aumenta o, in un'altra prospettiva, il ritorno dell'investimento in sicurezza diminuisce al diminuire delle informazioni disponibili e/o della loro accuratezza. Il costo della gestione raggiunge il suo massimo, ed il ritorno dell'investimento il suo minimo, quando si vuole massimizzare la resilienza e non si vogliono utilizzare, o non si dispone di, informazioni su minacce e vulnerabilità.

Possiamo quindi concludere che un approccio che tenti di massimizzi la resilienza solo per evitare analisi o gestione del rischio non è certo una soluzione vincente o efficace. Una soluzione è vincente solo se sfrutta al meglio le informazioni disponibili, anche se non completamente accurate, e considera resilienza solo in presenza di gravi carenze nelle informazioni disponibili o dell'impossibilità di aggiornare il sistema. È comunque più semplice difendere un sistema dalle minacce ignote solo quando lo si è già difeso da quelle note. In questa prospettiva, l'analisi del rischio non è altro che il passo iniziale del progetto di un sistema resiliente.

Bibliografia

- Z. A. Collier, I. Linkov, J. H. Lambert, Four domains of cybersecurity: a risk-based systems approach to cyber decisions, Environment, Systems and Decisions, Dec. 2013, Vol. 33, 4, pp 469–470
- P. Lloret-Gallego, M. Aragüés-Peñalba, L. Van Schepdael, Lien et al, Methodology for the Evaluation of Resilience of ICT Systems for Smart Distribution Grids, Energies, Vol. 10, 9, 2017
- B. Plattner, D. Hutchison, J. P.G. Sterbenz (ed) Resilient and Survivable networks, Special Issue of Computer Networks, , June 2010 Vol. 54, 8, Pages 1243-1342
- T. Aven, E. Zio Knowledge in Risk Assessment and Management, Wiley, 2017
- National Institute of Standards and Technology, DRAFT Special Publication 800-160, Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, March 2018.

Articolo a cura di **Fabrizio Baiardi**

Laureato in Scienze dell'Informazione all'Università di Pisa.

E' attualmente è professore ordinario di Informatica presso l'Università di Pisa dove coordina il gruppo di ricerca sy ICT risk assessment and management. La sua attività di ricerca è focalizzata su strumenti e metodi formali l'automazione dell'analisi e la gestione del rischio.

Ha partecipato a numerosi assessment di sistemi ICT con particolare interesse per quelli con componenti SCADA.

Attualmente è responsabile scientifico del progetto Haruspex che ha prodotto una suite integrata di strumenti per analisi e gestione del rischio.

Una lista aggiornata delle pubblicazioni scientifiche sul progetto Haruspex e dei premi ricevuti si può trovare alla

pagina
http://www.di.unipi.it/~tonelli/securityteam/publications.php

F. Baiardi è stato presidente della laurea in Informatica Applicata e della laurea magistrale in Sicurezza Informatica dell’Università di Pisa.

E’ stato coinvolto in vari progetti nazionali ed europei sulla valutazione della qualità dei corsi di studio e di formazione superiore. Inoltre è valutatore di progetti di innovazione tecnologica per enti pubblici e fondazioni private nazionali ed europei.



https://www.ictsecuritymagazine.com/articoli/resilienza-e-gestione-del-rischio-antagonismo-o-complementarieta/