QUOTIDIANO ENERGIA
www.quotidianoenergia.it

ALTRE NOTIZIE RICERCA E INNOVAZIONE ROMA 4 NOVEMBRE 2016

Sicurezza utility: la tecnologia c'è, manca una cultura condivisa

Innovazione e servizi evoluti per un nuovo modello di gestione e controllo globale delle infrastrutture

di Tommaso Perelli*

Il settore delle utility sta vivendo un processo di profonda trasformazione trainato dal contesto macroeconomico e regolatorio, dalla crisi dei tradizionali modelli di business e dalla diffusione di nuove tecnologie. Questi trend stanno influendo in modo sempre più rilevante sulla percezione del concetto di sicurezza e controllo nelle multiutilty, cambiandone il paradigma storico. Il tema è stato al centro del seminario organizzato il 27 ottobre da Agici in collaborazione con DAB Sistemi Integrati, dal titolo ***"Il valore della sicurezza per le multi utility. Innovazione tecnologica e servizi evoluti per un nuovo modello di gestione e controllo globale"***. All'appuntamento, riservato ai partner dell'Osservatorio M&A Utilities, sono intervenuti in qualità di relatori: Santi Maurizio Grasso (DAB si), Alessandro Manfredini (A2A), Francesco Ceccarelli (Enel), Giorgio Morello (Smat). Di seguito le principali questioni emerse durante i lavori.

Le aziende multiutility sono detentrici di infrastrutture critiche costituite da un insieme di reti complesse e per questo risulta fondamentale che esse garantiscano la continuità del servizio offerto. Inoltre, l'introduzione di soluzioni innovative per la sicurezza e la gestione da remoto delle reti complesse delle multiutility favorisce l'ottimizzazione dei costi correlati agli aspetti di *security*, una migliore *governance* della sicurezza e può fornire strumenti addizionali di gestione delle *operations*.

Molti operatori hanno approcciato questi temi solo di recente e le modalità di adozione più diffuse seguono un modello non integrato e poco sofisticato. La situazione attuale riflette il ritardo nell'adozione di soluzioni innovative e di processi strutturati.

Lo scenario rispetto a questi temi presenta aspetti diffusi che possono rappresentare punti di debolezza per le *utility* italiane:

1. Criticità intrinseche delle strutture produttive tipiche di questo settore:

molteplici siti distribuiti su territori ampi, anche molto diversificati;
effetto domino di eventuali problemi sulle infrastrutture dovute a eventi imprevisti, provenienti anche dall'esterno;
notevoli impatti economici e sociali in caso di mancata erogazione dei servizi e di tempi di risposta lunghi;
incremento dei rischi dovuti alla liberalizzazione dei mercati e ad una sempre maggiore interconnessione delle reti.

2. Oggi molte strutture hanno un presidio fisico limitato o nessun presidio, data anche l'impossibilità di un presidio puntuale.

3. Elevati costi associati alla *security* delle infrastrutture, dovute a:

necessità di vigilanza e presidio dei siti operativi;
strutture organizzative di *security* non standardizzate e non integrate;
elevata probabilità di subire danneggiamenti delle infrastrutture (furti, vandalismo);
mancata produzione e fermi impianti, con eventuali ritardi nel ripristino delle operatività;
elevati danni immagine connessi alla tipologia di servizi erogati;

sottrazione di dati sensibili o sabotaggio tramite *cyber attack* a danno degli interessati o a favore di terze parti.

4. Ridotta *governance* di ciò che succede realmente nei singoli siti operativi dovuta alla ridotta conoscenza e integrazione delle informazioni o alla eccessiva disponibilità di dati non utilizzati efficacemente.

La soluzione per ottimizzare la gestione delle attività di sicurezza e di controllo si compone di molteplici aspetti. La sfida attuale per la *security* aziendale si basa soprattutto sulla capacità di **prevenzione**, data la rapidità con cui si evolvono le minacce, i metodi di attacco, i relativi livelli di sofisticazione (es. cyber threats) e l'elevato tasso di impatto sul raggiungimento degli obiettivi di business. Se il paradigma storico si basava su un tipo di approccio "reattivo", la sfida attuale si fonda sulla capacità di averne uno **proattivo** e **condiviso**. Questo approccio deve essere pervasivo, coinvolgendo ed essendo condiviso da tutti i livelli aziendali. I singoli componenti della struttura organizzativa devono farsi parte attiva, essere responsabilizzati e consapevoli. L'obbiettivo finale a cui si deve tendere è quello di garantire all'organizzazione la capacità di dare risposte forti e tempestive a segnali deboli e imprevedibili. Gli elementi chiave sui quali si basa un approccio di questo tipo sono sintetizzabili in:

1. La capacità di **iniziativa** , cioè non farsi sorprendere da eventi inaspettati, raccogliere ed interpretare adeguatamente "segnali deboli", valutare i trend delle minacce e analizzare precisamente i punti deboli dell'organizzazione;

2.La capacità di **condivisione**, favorendo il dialogo tra tutti i livelli dell'organizzazione, la conoscenza del business e gli obiettivi strategici dell'azienda nel suo complesso e l'analisi del contesto esterno di riferimento;

3. La capacità di **integrazione** delle informazioni, connessa in molti aspetti alla condivisione, permettendo l'utilizzo multidisciplinare delle informazioni tra le diverse realtà aziendali e i diversi aspetti di sicurezza fisica, della *cyber security* e telecontrollo

4. La capacità di **responsabilizzare**, definendo ed applicando un modello di comportamento orientato alla sicurezza che non sia solamente un insieme di regole, promuovendo una formazione del personale che miri all'insegnamento di una mentalità piuttosto che di procedure standard.

5. La capacità di **misurare**; dando per scontata l'importanza di raccolta di dati anche complessi. Bisogna essere in grado di sapere definire, misurare e monitorare indicatori di performance, finalizzati ad un incremento costante dell'efficienza.

Il grado di specializzazione o standardizzazione dei processi di *security* deve essere adattato alla complessità organizzativa. Tanto più è semplice, tanto più le competenze possono essere concentrate. Tuttavia, in organizzazioni più complesse, la forma ottimale è quella della rete basata su nodi distinti, che consente una migliore personalizzazione degli interventi e una maggiore velocità di risposta.

Ulteriori aspetti da sottolineare per la loro importanza quando si parla di sicurezza delle multiutility sono i temi di gestione dei rischi e della gestione di emergenze e situazioni di crisi. Chi gestisce la security deve garantire efficacia ed efficienza di tutto il processo di "*security risk management*", dal monitoraggio e valutazione integrata dei rischi fino alla loro gestione attiva e assicurazione. Per quanto riguarda la gestione efficiente di situazioni di emergenza (procedure predefinite) e di crisi (strategie non prevedibili), l'obiettivo deve essere quello di assicurare rapidità ed efficacia dei processi decisionali e di comunicazione interna/esterna per la gestione di qualsiasi evento in grado di pregiudicare la sicurezza delle persone, la continuità del servizio pubblico e dell'operatività aziendale, l'ambiente, gli asset, l'immagine e la reputazione, in modo da minimizzare l'impatto sul valore aziendale, sugli *stakeholder* e il tempo di ripristino dell'operatività. Anche in questi casi la definizione di processi strutturati, interconnessi, facilmente condivisibili e l'adozione di tecnologie innovative incrementano notevolmente i benefici.

In conclusione, si può affermare che le tecnologie disponibili sono già in grado di far fronte a queste necessità, mentre ampi margini di miglioramento si possono ottenere sulle risorse umane e sulla diffusione di una cultura condivisa.

***Agici**