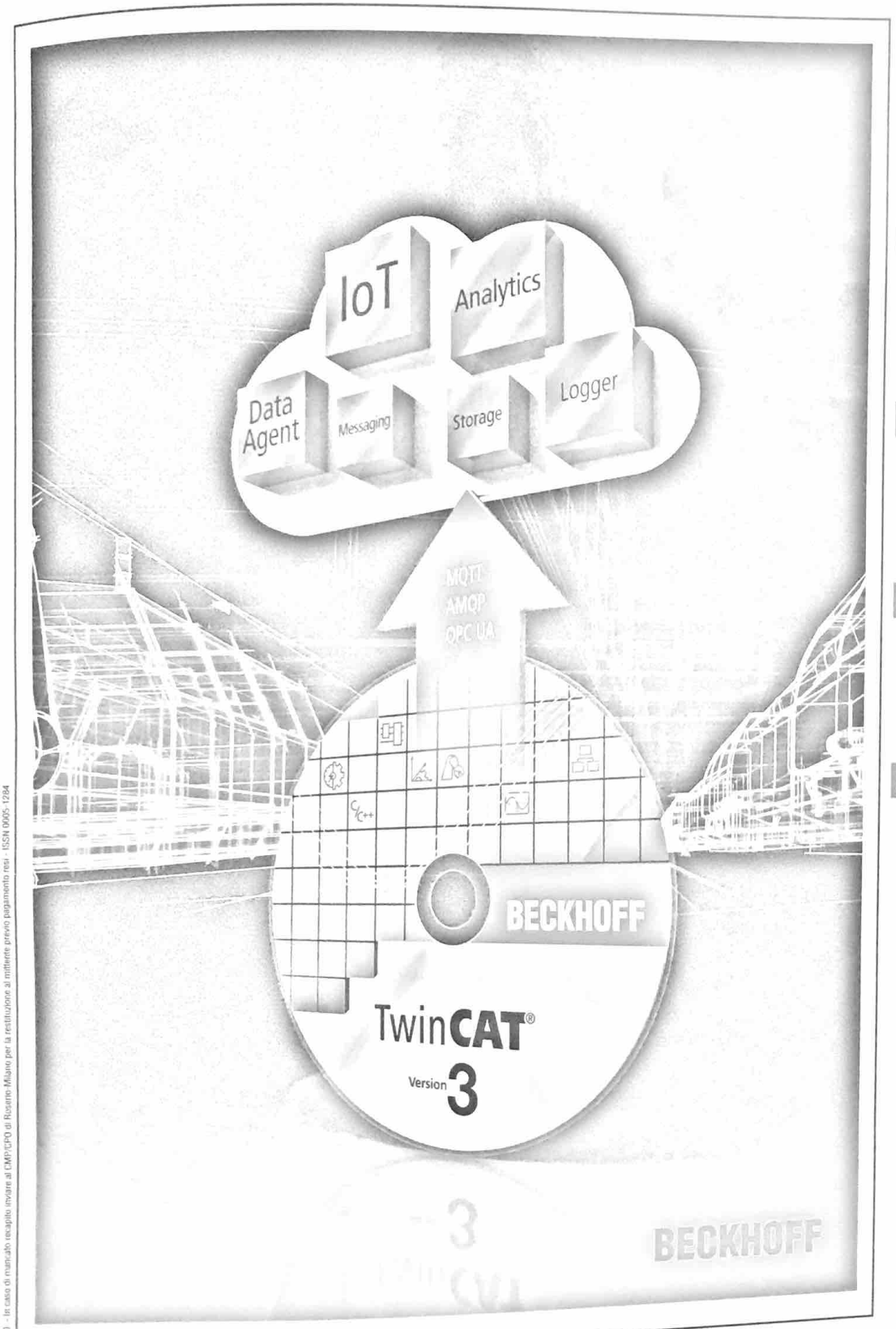
www.automazione-plus.i

AUTOMAZIONE E STRUMENTAZIONE

Elettronica Industriale

Maggio 2017
Anno LXV - N. 4



COVER STORY

Il mondo IoT con TwinCat 3

INDAGINE

Controlli decentrati per Industria 4.0

TECNICA

Cyber security nella gestione d'impresa

SPECIALE

Ethernet e le reti industriali

in questo numero

efficiency

FIERA MILANO MEDIA

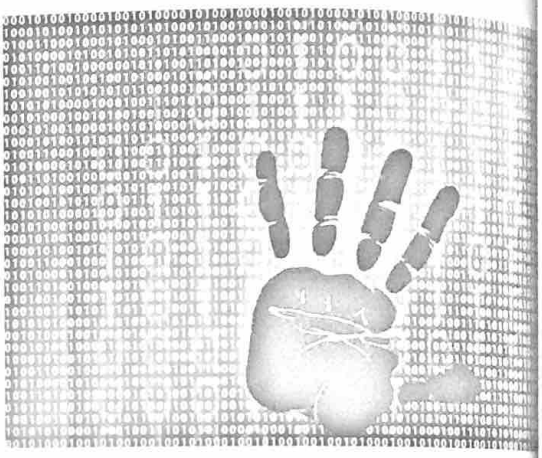
A.N.I.P.L.A. ASSOCIAZIONE NAZIONALE ITALIANA PER L'AUTOMAZIONE

50 - In caso di mancato recapito inviare al CMP/CPO di Rozzano Milano per la restituzione al mittente previo pagamento resi - ISSN 0005-1284

INDUSTRIAL CONTROL SYSTEMS E LE VARIABILI ORGANIZZATIVO SOCIOTECNICHE

Promuovere la cyber security negli ICS con l'analisi dei processi organizzativi

L'impatto delle azioni per fronteggiare la cyber security in ambito industriale è una opportunità ancora in parte da esplorare. Accanto ad una certa immaturità/incredulità da parte degli attori organizzativi che non prendono molto sul serio la sfida della sicurezza, si osserva il persistere di strategie ancorate a visioni manageriali che eludono le dimensioni sociali della sicurezza.



Alberto Zanutto

Chi si occupa di cyber security nei sistemi industriali si trova a fronteggiare molte sfide. La prima di tutte è probabilmente il fatto che la consapevolezza su come i nostri comportamenti organizzativi siano collegati al rischio cyber è molto scarsa o addirittura volutamente sottaciuta. Le aziende sono poco o nulla interessate a condividere le informazioni sugli eventuali cyber attacchi ricevuti. Le statistiche ufficiali, fornite ad esempio dall'autority americana, non permettono di capire come è realmente la situazione visto che riesce a monitorare non più di qualche centinaio di casi per anno. E tuttavia gli esperti di sicurezza collezionano continuamente storie relative alla capacità degli hacker nel prendere il controllo di varie macchine e di generare danni a cose e a persone attraverso la loro attività.

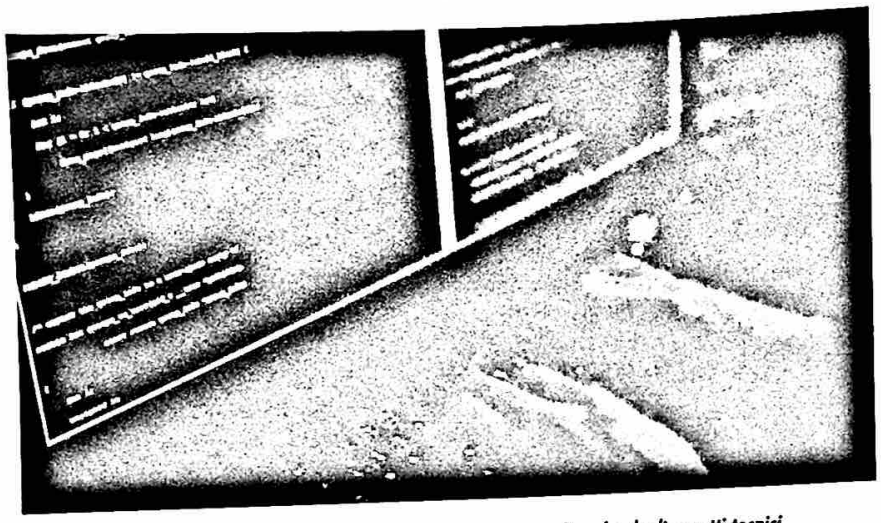
Come è possibile allora operare affinché le aziende riescano ad affrontare con maggiore capacità questi rischi? Cosa e come si deve controllare e verificare per fermare eventuali cyber attacchi nei vari siti industriali?

Molti dei problemi che si osservano nei siti industriali connessi attraverso i sistemi **Scada** (Supervisory Control Data Acquisition), anche noti come **Industrial Control Systems** (ICS) dipendono, come sostengono *Busby e Bennet* [2], dalle rappresentazioni che i singoli hanno del rischio e dalla percezione relativa ai processi sociali con cui si può alimentare il rischio.

L'AUTORE
A. Zanutto, Lancaster University, Security Department, UK

Gli aspetti sociali e organizzativi

In questi anni, seguendo l'analisi di *Hansen e Nissenbaum* [3], abbiamo attraversato almeno tre pulsioni. Da un lato sono stati enfatizzati i processi di 'hyper-securitization' dove deve prevalere la procedura e il protocollo che permette l'accesso sicuro ad ogni cosa. Dall'altro abbiamo spesso preso atto di come molte pratiche quotidiane siano ignare dei più elementari principi di tutela della sicurezza e come terzo fenomeno abbiamo dato sempre più spazio alla iper tecnicizzazione. Con quest'ultima modalità nei fatti il management delle imprese punta sempre con più convinzione sull'adozione di tecnologie per rispondere al rischio dei cyber attacchi. Tuttavia ai più attenti non sarà sfuggito come in questi anni si siano consolidati alcuni modi 'tipici' nell'affrontare la cyber security nei contesti industriali. Ad esempio *Buzan* (2004) evidenzia come i discorsi pubblici siano sempre più orientati ad esagerare il rischio di attacco e a contemplare l'adozione di contromisure efficaci. Ma in ogni caso tutti i discorsi pubblici richiamano come motivazione principale il rischio di un possibile imminente e grave disastro. Si mobilizza cioè uno 'spettro' del passato per indicare i rischi presenti per il futuro. Si instaura così un processo costruzionista che spinge a mettere in agenda un tema che deve essere affrontato con urgenza dal management. Questa dimensione sociale, che incide così tanto nel decidere le agende a livello decisionale, è determinante anche nello



Un approccio razionale alla Cyber Security deve tenere conto, oltre che degli aspetti tecnici, anche di quelli sociali ed organizzativi

sviluppo di buone pratiche a livello di organizzazioni. I processi che possono davvero aiutare ad affrontare questi possibili eventi dipendono, infatti, principalmente dalle capacità 'sociali' delle persone che lavorano nelle organizzazioni. Ad esempio *Busby e Bennnet* [2] affermano che l'apertura mentale degli addetti al lavoro sul campo e sulla possibile scena del rischio permette di elevare il grado di protezione delle organizzazioni. Le organizzazioni, infatti, non sono luoghi in cui tutto è prevedibile e affrontabile con le migliori risorse a disposizione dell'impresa. Molto spesso il diverso ruolo degli operatori, le culture di lavoro locali, il mancato coordinamento tra i settori in caso di variazioni nei programmi di lavoro ecc., generano situazioni che *Turner* [4] definisce 'disgiuntive' e quindi difficili da gestire se si verifica un disastro imprevisto. I diversi punti di vista attingono a diversi bagagli di conoscenze e generano una diversità di interpretazione dei possibili indizi di un cyber attacco. Anche se, ricorda *Weick* [5], non c'è nessuna difficoltà tecnologica che possa essere paragonata al peso che può avere un modello organizzativo. Il richiamo al ruolo della divisone del lavoro nelle organizzazioni riposiziona è ancora una volta una questione chiave nell'avviare un risk management organizzativo. A questo proposito, l'equipe di ricerca dell'*Università di Lancaster* era interessata a mettere in risalto le azioni 'invisibili' collegate alla sicurezza, quelle che non fanno parte dello stock previsto dai protocolli e dalle linee guida. L'equipe era interessata alle pratiche quotidiane da cui la cyber sicurezza dipende senza che le persone lo sappiano. L'attenzione è stata posta a questo riguardo, in particolare, sulle azioni volte a riconoscere, gestire e trasmettere le informazioni di possibili attacchi o volte a gestire attività ordinarie per verificare se e in che modo gli operatori tengono presente il rischio di attacchi informatici.

Il lavoro di ricerca

L'attività di campo è durata circa due anni e ha coinvolto imprese in Regno Unito e Italia di diversa grandezza e diversa cultura della sicurezza informatica. In particolare, guardando principalmente ai **manager** e agli **operatori della sicurezza**, abbiamo potuto rappresentare con sufficiente dettaglio come agiscono questi attori organizzativi.

I manager sono apparsi abbastanza consapevoli e realisti rispetto ai possibili attacchi, e hanno chiaro come può essere grave l'impatto sul business. Allo stesso tempo è emerso che i cyber attacchi non sono per loro una priorità connessa alla vita quotidiana ma soprattutto a eventi molto particolari per cui non hanno un forte committment ad agire per proteggere le proprie aziende in modo ordinario. Spesso si muovono, solo dopo aver avuto eventi di attacchi e aver realizzato di essere molto a rischio. Spesso hanno delegato tutto ad una persona o ad un piccolo team cui chiedono di proteggere tutto l'insediamento produttivo. Queste persone, a loro volta, sembrano formate in modo non specifico e di solito sono esperti IT che si autoformano attraverso letture, passaparola e convegni specialistici.

Per questo accade spesso qualcosa che assomiglia alla solita 'polvere nascosta sotto il tappeto'. I responsabili della sicurezza sono invitati a proporre soluzioni al management ma con moderazione, perché troppi investimenti non sono possibili e in ogni caso un sistema che produca un eccesso di alert da gestire, ad esempio dovuti a traffico anomalo o ad intrusioni nei data center, possono mettere in difficoltà l'organizzazione e questo può mettere in discussione gli incentivi che potrebbero essere collegati alla numerosità degli alert stessi.

Un altro aspetto di complessità è l'indisponibilità degli ingegneri delle linee produttive ad accettare qualsiasi filtro o limite tecnologico rispetto ai loro obiettivi di produzione. Accade così che spesso anche semplici dispositivi di protezione all'accesso nei luoghi di produzione vengano rimossi per semplificare i percorsi o per arieggiare un ambiente o semplicemente per poter modificare l'attività di un PLC con immediatezza. In ogni caso, ogni anomalia in questi contesti è rappresentata come meccanica o comunque funzionale al processo dei macchinari e non ad un eventuale tentativo di attacco via network. Nemmeno è dato per scontato che le nuove apparecchiature installate come i sistemi Scada prevedano sempre filtri o dispositivi per la cyber sicurezza. Infatti, spesso i capitolati non includono questa funzionalità e quindi i fornitori, anche se competenti e capaci di fornire dispositivi predisposti a questo tipo di scopo, non li introducono perché perderebbero gli appalti per i maggiori costi documentati.

La ricerca sul campo non ha permesso di trovare significative pratiche volte ad apprendere dall'esperienza su questi argomenti. Danni meccanici anomali, alert e mancati aggiornamenti software, sono gestiti in modo isolato senza una ricognizione sequenziale e comparata. Questo porta ad avere una visione contraria alle logiche della learning organization. Ogni operatore tende a considerarsi isolato e a dover applicare e replicare le regole senza alcuna percezione delle complessità sociali ed organizzative cui concorrono.

In generale poi, è diffusa l'idea di non 'turbare' macchinari complessi con port scanning o con simulazioni di attacchi, perché c'è un mescolamento continuo di vecchie pratiche e vecchie attrezzature che convivono con nuove pratiche e nuove attrezzature di cui è difficile conoscere tutti i dettagli e di cui è difficile prevedere le reazioni in seguito alle varie tecniche di simulazione. Il risultato è che nessuno oggi riesce a prevedere nelle proprie organizzazioni gli esiti effettivi di un eventuale cyber attacco. Infine, piuttosto che avviare processi virtuosi nelle organizzazioni che possano ridurre il rischio e mitigare gli effetti dei cyber attacchi, il management preferisce affidarsi a buone polizze assicurative assumendo il rischio come inaffrontabile attraverso strategie di gestione.

Conclusioni

L'esito principale di questa ricerca è dunque aver osservato che è quasi assente una riflessione 'sociotecnica' intorno alle produzioni e alle gestioni dei sistemi di mitigazione o detecting dei cyber attacchi. Solo un lavoro continuo di mapping delle pratiche quotidiane, delle rappresentazioni degli addetti e di analisi delle pratiche 'invisibili' permette alle organizzazioni di tenere sempre attivo un lavoro sulla cyber security. Un processo che potrebbe mutuare gli apprendimenti organizzativi maturati attraverso le pratiche di analisi della safety. Infatti, anche per quel tipo di materia il lavoro più consistente è stato quello di portare la safety ad essere parte delle azioni di management e così sono diventate piano piano oggetto di apprendimento organizzativo. La difesa dei contesti ICS non può che essere nuovamente il frutto di un lavoro continuo per definire i flussi di azione dei soggetti in combinazione con le tecnologie utilizzate e generare così ulteriore apprendimento organizzativo.

Riferimenti

[1] J. S. Busby, R. E. Alcock. "Risk and Organizational Networks: Making Sense of Failure in the Division of Labour." *Risk Management 10*, no. 4, pp. 235-56, 2008.

[2] J. S. Busby, S. A. Bennett. "Analysing the risks of individual and collective intentionality". *Journal of Risk Research. 11*, 6, pp. 797-819. 23, 2008.

[3] L. Hansen, H. Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly 53*, no. 4, pp.1155-75, 2009.

[4] B. Turner. "A Personal Trajectory Through Organization Studies", *Research in the Sociology of Organizations*, Volume 13, pp. 275-301, 1995.

[5] K. E. Weick. "Foresights of Failure: An Appreciation of Barry Turner", *Journal of Contingencies and Crisis Management 6*, no. 2, pp. 72–75, 1998.