Cybersecurity della Conoscenza Operativa

22 Aprile 2026 · Confindustria Brescia · Cybersecurity Masterclass

Federico Cerutti
federico.cerutti@unibs.it

Executive Summary

In molte imprese, la continuità operativa non si rompe per un semplice difetto di rete o di software, ma perché si perde il sapere pratico che consente a processi, impianti e persone di funzionare quando il contesto reale si discosta dalla procedura. Questo sapere vive nelle configurazioni, nelle eccezioni sedimentate, nelle routine degli operatori, nei criteri di manutenzione e nei modi con cui si riconoscono e si risolvono i problemi ricorrenti. Una parte importante della cybersecurity contemporanea continua però a muoversi entro un paradigma che privilegia la protezione di dati, reti e sistemi IT. Questo approccio coglie solo una parte del rischio: nelle imprese, il problema è anche la dispersione, la distorsione e la perdita di coerenza della conoscenza operativa. L'impresa va quindi letta come un sistema dinamico di agenti umani e tecnologici, attraversato da flussi di conoscenze. Proteggere la cybersecurity significa proteggere la capacità dell'organizzazione di decidere, coordinarsi e agire attraverso OT, ERP, supply chain integrate, sistemi di AI, pratiche operative informali e strumenti di supporto decisionale.

La conoscenza come asset

Una linea produttiva non funziona solo perché esiste una procedura: funziona perché qualcuno sa quando seguirla, quando correggerla e quando sospenderla. In questo senso la distinzione tra informazione e conoscenza descrive livelli diversi di capacità operativa.

La cybersecurity tradizionale è stata sviluppata soprattutto attorno alla protezione di sistemi informativi, dati, asset digitali e continuità dei processi di supporto. Questa impostazione è coerente con i principali framework contemporanei di gestione del rischio cyber, che organizzano il problema intorno all'identificazione, protezione, rilevazione, risposta e ripristino di asset e funzioni essenziali.[1, 2, 3] Tale paradigma ha prodotto architetture, controlli e metriche indispensabili per gli ambienti IT, ma mostra dei limiti quando viene applicato a contesti produttivi.

Dato, informazione e conoscenza non sono sinonimi. Il dato è una rappresentazione simbolica. L'informazione è il risultato della sua interpretazione entro un contesto. La conoscenza è la capacità di agire efficacemente in una situazione concreta.[4, 2] Essa include esperienza, giudizio, sensibilità alle eccezioni e capacità di adattamento: regolazioni di macchina, compromessi tra qualità e tempi, interventi manuali su anomalie ricorrenti e conoscenza delle tolleranze reali dei materiali dipendono spesso da pratiche incorporate nell'esperienza degli operatori.[5, 2]

Una quota rilevante del rischio è quindi invisibile. Anche senza grandi esfiltrazioni di dati, un'organizzazione può essere vulnerabile alla perdita, all'alterazione o al deterioramento della propria conoscenza operativa.

L'impresa come sistema socio-tecnico di agenti

Per chi governa l'impresa, il problema non è un singolo asset digitale, ma la catena di decisioni attraverso cui un'anomalia viene interpretata e trasformata in azione. Un'azienda è infatti un sistema di agenti, attori eterogenei che interagiscono tra loro: individui, macchine con i loro software di controllo, software gestionali, sistemi di supervisione, fornitori esterni e, sempre più spesso, sistemi di AI.

Il comportamento complessivo del sistema azienda nasce quindi dall'interazione locale tra agenti che possiedono informazione e capacità decisionali parziali.[6, 7] L'azione organizzativa emerge da una catena di interpretazioni: un sensore segnala una deviazione; un sistema SCADA la presenta in una certa forma; un operatore la confronta con la propria esperienza; un responsabile decide se fermare, compensare o proseguire; un gestionale ricalcola priorità e sequenze. Il risultato dipende dalla qualità delle relazioni tra tutti questi passaggi.

Questa distribuzione della capacità operativa rende più difficile governare il rischio. Quasi mai esiste una rappresentazione completa di ciò che il sistema-azienda *conosce* e di come quella conoscenza venga trasformata in decisione. Anche quando le infrastrutture sono formalmente protette, possono restare vulnerabili le relazioni tra attori, le dipendenze implicite e i passaggi interpretativi.

L'introduzione di sistemi di AI accresce questa complessità, modificando sia il perimetro di attacco sia il modo in cui un errore può propagarsi. Tali sistemi producono classificazioni, raccomandazioni, sintesi e previsioni che entrano nei processi decisionali; il rischio è sia tecnico, che cognitivo, perché aumenta la possibilità di overreliance e di uso improprio dell'automazione.[8, 9] Ne deriva una maggiore opacità quando una parte della conoscenza utile all'azione viene mediata da questi modelli.

Fragilità della conoscenza operativa

La compromissione della conoscenza operativa non produce effetti uniformi: potrebbe tradursi in errori di processo, rallentamenti, inefficienze, degradazione della qualità o interruzioni della continuità operativa. Il tratto comune è la rottura della coerenza con cui il sistema azienda interpreta e governa la propria azione.

Consideriamo l'OT, dove la protezione della conoscenza operativa si misura soprattutto nella capacità di governare sistemi ereditati nel tempo e chiamati a restare disponibili mentre evolvono con estrema cautela.[10] Qui il rischio assume forme sottili: una variazione minima nei parametri di

processo, una deriva nella taratura o un ritardo nella manutenzione possono produrre, nel tempo, un peggioramento di qualità, efficienza, sicurezza o durata dei componenti, rendendo difficile per l'organizzazione ricostruire i nessi causali.[11]

Passiamo alle supply chain digitali, nelle quali sistemi come ERP, MES e piattaforme gestionali fortemente personalizzate diventano il supporto di un coordinamento costruito nel tempo. In molte imprese queste architetture sono il risultato di anni di adattamenti incrementali, sviluppi locali, parametrizzazioni, integrazioni poco documentate e prassi operative sedimentate. La loro efficacia non dipende soltanto dal software in quanto tale, ma anche da una conoscenza pratica detenuta da key user, consulenti, responsabili di funzione e operatori amministrativi. Se questa conoscenza viene compromessa o riconfigurata in modo errato, i danni sotto forma di ritardi, scarti, errori di pianificazione e decisioni incoerenti possono emergere anche in assenza di una classica violazione dei dati.[12, 13, 14]

Infine, nei sistemi con componenti di AI, la vulnerabilità non riguarda soltanto la disponibilità o l'integrità dell'infrastruttura, ma soprattutto la qualità della conoscenza che questi sistemi restituiscono. Quando dati degradati o input manipolati entrano nei modelli, gli errori possono ripetersi e propagarsi nei processi pur in presenza di sistemi formalmente *funzionanti*. In questo senso, la cybersecurity si sovrappone sempre più alla capacità di verificare come la conoscenza venga prodotta, mediata e usata.[15, 16]

Vettori di compromissione

I principali vettori di compromissione non colpiscono solo dati o infrastrutture, ma la conoscenza operativa che consente all'organizzazione di interpretare il contesto e mantenere coerenza nell'azione. Il rischio entra quando questa conoscenza esce dal sistema, si deforma o viene affidata a strumenti che non ne garantiscono la verifica.

Una parte rilevante del rischio emerge dalla dispersione non intenzionale di conoscenza operativa. Operatori, tecnici e manutentori che descrivono anomalie, condividono parametri o trasmettono schermate di supervisione possono diffondere frammenti che, una volta aggregati, rendono ricostruibili logiche di processo. L'uso non governato di strumenti di AI generativa (*shadow AI*) per analizzare problemi, tradurre procedure o ottenere supporto tecnico introduce ulteriori canali di esposizione, trasferendo informazioni sensibili al di fuori del perimetro aziendale.[16, 8] Analogamente, l'interazione con fornitori remoti, piattaforme collaborative e servizi digitali esterni può facilitare il passaggio di configurazioni e conoscenze senza una piena consapevolezza del loro valore.[13]

Accanto alla dispersione, assumono rilievo la distorsione della conoscenza e gli interventi sulle configurazioni operative. I processi possono essere alterati da istruzioni obsolete, interpretazioni errate, adattamenti locali non controllati o suggerimenti prodotti da sistemi di AI non adeguatamente verificati; al tempo stesso, aggiornamenti software, cambi di versione, manutenzioni, sostituzioni di componenti o riconfigurazioni di rete possono modificare equilibri consolidati senza che ne sia pienamente compreso l'impatto sistemico. In entrambi i casi, l'organizzazione continua a operare su basi apparentemente coerenti, ma progressivamente disallineate rispetto alla realtà del processo produttivo e alla conoscenza storica che ne ha guidato l'evoluzione.[15, 16]

Infine, la crescente delega decisionale a dashboard, sistemi di monitoraggio, modelli predittivi e strumenti di AI introduce un livello ulteriore di vulnerabilità. La fragilità si sposta dalla protezione dell'infrastruttura alla qualità dell'interpretazione. Il sistema può continuare a funzionare producendo decisioni plausibili, ma inappropriate, rendendo il deterioramento meno evidente e più difficile da attribuire a una causa specifica.[16, 9]

Governare la conoscenza operativa

Ne deriva un'agenda che precede la scelta degli strumenti. La priorità è mappare il know-how critico, individuare i punti singoli di fallimento, documentare le eccezioni davvero rilevanti, governare l'uso di *shadow AI* e degli scambi con l'esterno, e verificare la recuperabilità della conoscenza tacita e la tenuta dei processi di ripristino.

Acronimi

AI Artificial Intelligence
ERP Enterprise Resource Planning
IT Information Technology
MES Manufacturing Execution System
OT Operational Technology

Riferimenti

[1] Ikujiro Nonaka e Hirotaka Takeuchi. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. OUP, 1995.
[2] ISO. *Knowledge management systems – Requirements*. International Standard ISO 30401:2018. 2018.
[3] NIST. *The NIST Cybersecurity Framework (CSF) 2.0*. 2024.
[4] Thomas H. Davenport e Laurence Prusak. *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press, 1998.
[5] Michael Polanyi. *The Tacit Dimension*. London: Routledge & Kegan Paul, 1966.
[6] Nancy G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: The MIT Press, 2011.
[7] Edwin Hutchins. *Cognition in the Wild*. Cambridge, MA: The MIT Press, 1995.
[8] ENISA. *Artificial Intelligence Cybersecurity Challenges*. 15 Dic. 2020.
[9] Raja Parasuraman e Victor Riley. "Humans and Automation: Use, Misuse, Disuse, Abuse". In: *Human Factors* 39.2 (1997), pp. 230–253.
[10] Keith A. Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Yan Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule e Michael Thompson. *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82 Rev. 3. 28 Set. 2023.
[11] Ralph Langner. "Stuxnet: Dissecting a Cyberwarfare Weapon". In: *IEEE Security & Privacy* 9.3 (2011), pp. 49–51.
[12] Ramin Vandaie. "The Role of Organizational Knowledge Management in Successful ERP Implementation Projects". In: *Knowledge-Based Systems* 21.8 (2008).
[13] ENISA. *Good Practices for Supply Chain Cybersecurity*. 13 Giu. 2023.
[14] NIST. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST Special Publication 800-161 Rev. 1. 2022.
[15] NIST. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. 2023.
[16] NIST. *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. NIST AI 600-1. 2024.