RBB/LAB

ESTRATTO GRATUITO NEWSLETTER

Cybersecurity per le *PMI.*

Normativa, difese pratiche e intelligenza artificiale nel quotidiano.
Il piano in 4 trimestri per passare da esposti a difendibili e dimostrabili.

rbb-lab/estratto-44-pagine.md

nis2 · gdpr · ai-act

- **Piano completo dell'opera:** tutti i 28 capitoli delle 5 Parti
- **Cap. 1 integrale (Le PMI nel mirino):** l'economia degli attacchi, i casi italiani reali e i conti di ACME
- **Cap. 2 integrale (Anatomia di un disastro):** cronologia minuto per minuto ed euro per euro di un attacco
- **Cap. 3 integrale (Chi attacca e come):** gli accessi venduti a 900 dollari e la filiera RaaS
- **Cap. 28 integrale (La roadmap di 12 mesi):** il piano operativo 4×90 e le tre fasce di budget

difendibile e dimostrabile · piano 4×90 · 12 mesi · capitoli **28/28**

ENRICO RUBBOLI
RBB LAB · Product & Security Engineering · rbblab.com

ESTRATTO PARTE I + ROADMAP

RBB/LAB

Cybersecurity per le PMI

Estratto: Parte I integrale (Capitoli 1–3) e Capitolo 28 (La roadmap di 12 mesi)

ENRICO RUBBOLI

Cybersecurity per le PMI: normativa, difese pratiche e intelligenza artificiale nel quotidiano
Autore: Enrico Rubboli (enrico.rubbo.li) · Pubblicato da **RBB LAB** (rbblab.com) · Edizione 2026.
Questo documento contiene la Parte I integrale (Capitoli 1, 2 e 3) e il Capitolo 28 conclusivo dell'opera completa (28 capitoli, 300 pagine). Coerentemente con i metodi descritti nella Parte IV del volume, il libro è stato redatto e revisionato con il supporto di strumenti di intelligenza artificiale, sotto la verifica e la validazione finale dell'autore. In fondo al documento trovi le indicazioni per accedere al volume integrale (in formato digitale o cartaceo) con lo sconto riservato agli iscritti alla newsletter di RBB LAB.

PIANO COMPLETO DELL'OPERA · 28 CAPITOLI · 300 PAGINE

Cosa contiene il libro integrale e cosa trovi in questo estratto

01 · PARTE I · IL TERRENO DI GIOCO

- **Capitolo 1 · Le PMI nel mirino** ◆ INCLUSO NELL'ESTRATTO
- **Capitolo 2 · Anatomia di un disastro** ◆ INCLUSO NELL'ESTRATTO
- **Capitolo 3 · Chi attacca e come** ◆ INCLUSO NELL'ESTRATTO

02 · PARTE II · LA NORMATIVA, SENZA PANICO

- **Capitolo 4 · NIS2: rientrate nel perimetro?** (Edizione integrale)
- **Capitolo 5 · L'effetto a catena: quando i clienti scrivono la vostra politica di sicurezza** (Edizione integrale)
- **Capitolo 6 · Il GDPR in pratica** (Edizione integrale)
- **Capitolo 7 · L'AI Act, per le aziende che usano l'IA** (Edizione integrale)
- **Capitolo 8 · Le altre regole che contano** (Edizione integrale)
- **Capitolo 9 · Governance minima: chi fa cosa** (Edizione integrale)

03 · PARTE III · LA DIFESA PRATICA

- **Capitolo 10 · Il metodo: un'autovalutazione in una settimana** (Edizione integrale)
- **Capitolo 11 · Identità e accessi** (Edizione integrale)
- **Capitolo 12 · Email** (Edizione integrale)
- **Capitolo 13 · Endpoint** (Edizione integrale)
- **Capitolo 14 · Backup e continuità** (Edizione integrale)
- **Capitolo 15 · Rete e perimetro** (Edizione integrale)
- **Capitolo 16 · Le persone** (Edizione integrale)
- **Capitolo 17 · I fornitori e la catena di approvvigionamento** (Edizione integrale)
- **Capitolo 18 · Risposta agli incidenti** (Edizione integrale)
- **Capitolo 19 · Assicurazione cyber e budget** (Edizione integrale)

04 · PARTE IV · L'INTELLIGENZA ARTIFICIALE IN AZIENDA

- **Capitolo 20 · Shadow AI** (Edizione integrale)
- **Capitolo 21 · La policy sull'uso dell'IA** (Edizione integrale)
- **Capitolo 22 · Scegliere gli strumenti** (Edizione integrale)
- **Capitolo 23 · Gli LLM nel lavoro quotidiano, funzione per funzione** (Edizione integrale)
- **Capitolo 24 · Sicurezza degli LLM** (Edizione integrale)
- **Capitolo 25 · L'IA a supporto della funzione sicurezza** (Edizione integrale)
- **Capitolo 26 · LLM locali** (Edizione integrale)
- **Capitolo 27 · Conformità nell'uso dell'IA** (Edizione integrale)

05 · PARTE V · IL PIANO

- **Capitolo 28 · La roadmap di dodici mesi** ◆ INCLUSO NELL'ESTRATTO

01 · PARTE I

RBB/LAB

Il terreno di gioco

Perché una PMI manifatturiera italiana è il bersaglio più redditizio sul mercato criminale, quanto costa davvero un giorno di fermo e come funziona la filiera industriale degli attacchi.

CAPITOLI DI QUESTA PARTE

- **Capitolo 1:** Le PMI nel mirino
- **Capitolo 2:** Anatomia di un disastro
- **Capitolo 3:** Chi attacca e come

CAPITOLO 1

Le PMI nel mirino

> *Le PMI italiane vengono attaccate per calcolo economico, non per caso: questo capitolo illustra perché una piccola impresa manifatturiera rappresenta l'affare migliore sul mercato criminale e quanto costa quell'affare quando arriva il conto da pagare.*

La mattina dell'11 febbraio 2025 i macchinari della Alf DaFrè funzionavano perfettamente. Non c'erano stati incendi né allagamenti, e nessun ordine era sparito dai registri. A essersi fermato, nella notte tra il 10 e l'11 febbraio, era il server che comunica alle macchine cosa produrre durante la giornata. Gli aggressori sono entrati nei server aziendali e nel giro di pochi minuti hanno bloccato il server di produzione.[1]

Alf DaFrè produce mobili in provincia di Treviso e conta circa 350 dipendenti. La produzione è rimasta ferma per più di otto giorni, costringendo l'azienda a richiedere la *cassa integrazione*, l'ammortizzatore sociale che copre gli stipendi quando l'attività si interrompe.[1]

L'obiettivo di questo libro è proprio evitare quegli otto giorni di *cassa integrazione*. La notizia finita sui giornali, del resto, non riguardava dati rubati o hardware guasto, bensì 350 persone mandate a casa: quando l'IT (la tecnologia dell'informazione, i computer e i software che fanno funzionare un'azienda) di una fabbrica si ferma, la notizia riguarda i lavoratori. Un fallimento della sicurezza informatica, in Italia, arriva con un sussidio pubblico allegato. Il fallimento è privato; una parte del conto viene socializzata.

Non si tratta di un evento isolato. Nell'ottobre 2024 la Fraschetti, distributore di ferramenta e articoli per il giardinaggio di Frosinone, è stata attaccata nella notte tra il 9 e il 10 ottobre ed è rimasta ferma per tre settimane, ricorrendo allo stesso ammortizzatore sociale.[2] Nel settembre 2024 la Rothoblaas, azienda altoatesina che produce utensili e

[1] Il Post, «L'azienda veneta costretta a chiedere la cassa integrazione per un attacco informatico» (18 febbraio 2025). Alf DaFrè (produttore di mobili, Treviso, ~350 dipendenti): gli aggressori sono entrati nei server nella notte tra il 10 e l'11 febbraio 2025 bloccando il server di produzione in pochi minuti; produzione sospesa per oltre otto giorni, l'azienda ha richiesto la cassa integrazione. ilpost.it

[2] CyberSecItalia, «Fraschetti Spa, ransomware ferma la produzione per tre settimane» (28 ottobre 2025; l'attacco si è verificato il 9-10 ottobre 2024). Fraschetti S.p.A. (distribuzione ferramenta/giardinaggio, Frosinone) attaccata il 9-10 ottobre 2024; produzione sospesa per settimane; richiesta la cassa integrazione. cybersecitalia.it

materiali per l'edilizia, è stata colpita dal gruppo *ransomware* Akira (il ransomware è un software che cifra i file e chiede un riscatto per sbloccarli) attraverso lo sfruttamento di una vulnerabilità (un difetto noto del software usato per introdursi nel sistema), e la produzione si è fermata per giorni.[3] Giorni alla Rothoblaas. Tre settimane alla Fraschetti. Otto giorni e una richiesta di cassa integrazione alla Alf DaFrè. Tre settori, tre regioni, un unico schema: gli aggressori entrano, le operazioni si congelano, le persone restano a casa.

Questo schema non è sfortuna. È aritmetica.

L'aritmetica di un bersaglio

Spesso si dice: siamo troppo piccoli, troppo noiosi, nessuno perderebbe tempo con noi. Se però si mette da parte questa illusione e si guardano gli incentivi, il quadro cambia. Chi attacca le aziende non è un vandalo e, nella maggior parte dei casi, non è nemmeno un prodigio dell'informatica: è un business, con costi, margini e una preferenza netta per i bersagli che pagano bene e resistono poco. Nella savana la tigre non insegue la gazzella più forte: prende quella che resta indietro. Valutata su quel mercato, la PMI italiana è la gazzella che resta indietro. I motivi sono tre, tutti di natura economica.

Il primo motivo è il debito. Non quello che monitora la banca, ma il *debito di sicurezza*: la somma degli aggiornamenti di sicurezza mai applicati, delle password riutilizzate per anni su servizi diversi, del server che nessuno controlla, delle credenziali catturate molto tempo prima da un'email di *phishing* (un messaggio confezionato per spingere qualcuno a consegnare la propria password) e ancora funzionanti. Il debito è raramente plateale. È il server installato nel 2016 e aggiornato solo quando c'era tempo, è la password di amministratore condivisa da quattro persone perché cambiarla bloccherebbe un macchinario, è il backup che viene eseguito ogni notte, ma che nessuno si è mai preoccupato di verificare se effettivamente funziona. Ognuna di queste voci è il risultato di un'ora di tempo che qualcuno ha deciso di dedicare ad altro. Il totale si accumula su un bilancio che nessuno redige, e una notte viene riscosso, con gli interessi. Una porta lasciata aperta per cinque anni non significa aver vissuto cinque anni di sicurezza. Significa avere avuto una porta aperta per cinque anni.

Il secondo motivo è che i vostri dati si vendono. Una piccola impresa manifatturiera possiede un inventario sorprendentemente ricco, e in gran parte monetizzabile all'istante: liste di clienti con nomi, email e abitudini di pagamento, ordini aperti con importi e date, fatture con gli IBAN, specifiche di produzione, anni di posta elettronica. Dall'interno, nulla di tutto ciò sembra prezioso. Messo insieme, costituisce un kit per frodi costruite

[3] RaiNews TGR Bolzano, «Azienda altoatesina paralizzata da un attacco hacker» (26 settembre 2024). Rothoblaas (materiali per l'edilizia, Cortaccia) colpita dal gruppo ransomware Akira tramite lo sfruttamento di una vulnerabilità; produzione ferma per giorni; confermato dal global IT manager Stefan Trebo. rainews.it

su misura: chi conosce i vostri ordini aperti può scrivere al vostro cliente con l'importo esatto, il riferimento corretto e un IBAN leggermente diverso, e incassare una fattura che avete emesso voi. Questa è la *frode della fattura*, e non ha bisogno di dati segreti: ha bisogno di dati attuali. E ciò che l'acquirente non usa di persona finisce di nuovo sul mercato: molto spesso i dati vengono rivenduti nel dark web ad altri criminali o addirittura ad altre aziende concorrenti. Un ordine in corso rende una comunicazione fraudolenta indistinguibile da una vera.

Il terzo motivo è la posizione. La vostra rete è anche la porta d'accesso alle reti dei vostri clienti, e più grande è il cliente, più preziosa è la vostra porta. L'Italia ha già vissuto questo esperimento su larga scala. Intorno alle cinque e mezza del mattino dell'8 dicembre 2023, il venerdì che apre il ponte dell'Immacolata, un attacco ha colpito Westpole, un *cloud provider* (un'azienda di cui si noleggiano i server invece di gestirne di propri) appartenente al gruppo Cegeka, con data center a Roma e Milano.[4] LockBit 3.0 ha rivendicato l'attacco, e l'effetto domino si è abbattuto su PA Digitale, i cui servizi sono utilizzati da circa 1.300 enti pubblici, bloccando la fatturazione elettronica per i clienti di Dylog e Buffetti.[4] Aziende e uffici pubblici non hanno potuto emettere fatture durante un ponte nazionale a causa di un server di cui non avevano mai sentito parlare, situato in un armadio rack che non avevano mai visto. Il capitolo 17 analizza a fondo questo effetto domino. In questa sede, è sufficiente coglierne lo schema: un provider è una singola serratura che apre molte porte, e un fornitore è una porta verso ogni cliente che serve. La vostra azienda è la porta di qualcun altro, che lo abbiate pianificato o meno.

● 01 · PER IL MANAGER ◆ DECISIONE & BUDGET

La decisione che questo capitolo vi chiede di prendere non è un acquisto, ma una stima. Mettete su carta due valutazioni: quanto costa all'azienda una settimana di fermo produzione e quali dei vostri dati potrebbero, oggi, essere messi in vendita sul mercato nero. Ottenere queste risposte costa un pomeriggio di lavoro insieme a chi gestisce l'IT e a chi conosce il portafoglio ordini. Senza questi numeri, ogni decisione di sicurezza che prendete è un'ipotesi, e ogni offerta che riceverete da operatori di sicurezza verrebbe valutata senza un contesto chiaro. Avendoli, potrete distinguere una proposta seria da una semplicemente costosa, che è poi la differenza tra comprare protezione e comprare una messa in scena.

[4] Wired Italia, «Westpole, PA Digitale e il cyber domino che ha messo ko gli enti pubblici in Italia» (14 dicembre 2023). Attacco ransomware intorno alle 5:30 dell'8 dicembre 2023 contro il cloud provider Westpole (gruppo Cegeka), data center di Roma e Milano; effetto a cascata su PA Digitale (servizi usati da ~1.300 enti pubblici) e blocco dei servizi di fatturazione elettronica per i clienti Dylog e Buffetti; rivendicato da LockBit 3.0. wired.it

Un mercato con un suo listino prezzi

I dati sul crimine informatico mostrano un mercato in piena espansione, e l'Italia vi occupa una posizione sorprendentemente avanzata. Nel 2025 il nostro Paese ha registrato 507 incidenti significativi contro i 357 del 2024, con un aumento del 42%: parliamo del 9,6% degli incidenti significativi a livello mondiale, per una nazione che produce circa l'1% del PIL globale.[5,6] A livello mondiale, il numero di incidenti è cresciuto del 49% nel 2025. Il Clusit monitora anche la rapidità con cui questa frequenza accelera, e il balzo del 48,7% dal 2024 al 2025 è il più alto mai registrato, con una gravità media in costante aumento anno dopo anno.[5,6]

L'autorità nazionale rileva la medesima tendenza dal proprio osservatorio. Secondo l'ACN (Agenzia per la Cybersicurezza Nazionale), il suo CSIRT (Computer Security Incident Response Team, l'unità che assiste le vittime degli incidenti) ha gestito 2.729 eventi nel 2025, il 38% in più rispetto al 2024, con una media di 227 al mese; 615 di questi sono stati incidenti con un impatto confermato e hanno coinvolto 1.901 vittime uniche, il 50% in più rispetto all'anno precedente.[7]

Non tutto questo volume rappresenta un'attività a scopo di lucro. Il mese più intenso del 2025 è stato giugno, con 434 eventi, spinto dagli hacktivisti (gruppi che attaccano per una causa politica) attraverso attacchi DDoS (distributed denial of service, un servizio inondato di traffico fino al collasso): si tratta di una protesta condotta con un generatore di traffico, raramente il tipo di evento che blocca una linea di produzione.[7] Gli attacchi a scopo di lucro si muovono in modo più silenzioso e iniziano prima dell'effettiva intrusione. Nello stesso anno, l'ACN ha inviato 46.867 comunicazioni di allerta preventiva, ovvero avvisi a organizzazioni i cui sistemi esposti o compromessi erano già stati individuati.[7] Ognuna di queste comunicazioni è un campanello d'allarme che suona prima del furto.

[5] Clusit (Associazione Italiana per la Sicurezza Informatica), dati stampa dal *Rapporto Clusit 2026*: nel 2025 l'Italia ha registrato 507 incidenti significativi contro i 357 del 2024 (+42%), ovvero il 9,6% del totale mondiale, a fronte di circa l'1% del PIL globale; crescita globale degli incidenti +49% nel 2025; accelerazione della frequenza +48,7% (2024⟶2025), la più alta mai registrata; gravità media in aumento ogni anno. clusit.it

[6] Clusit, *Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2026* (rapporto completo). clusit.it

[7] ACN (Agenzia per la Cybersicurezza Nazionale), *Relazione annuale al Parlamento 2025*. Il CSIRT Italia ha gestito 2.729 eventi cyber nel 2025 (+38% sul 2024, media di 227/mese), di cui 615 incidenti con impatto confermato (+7%); 1.901 vittime uniche (+50%); picco di 434 eventi a giugno 2025 (campagna DDoS hacktivista); inviate 46.867 comunicazioni di allerta preventiva. documenti.camera.it (vedere anche acn.gov.it per il dato di riferimento del 2024: 1.979 eventi)

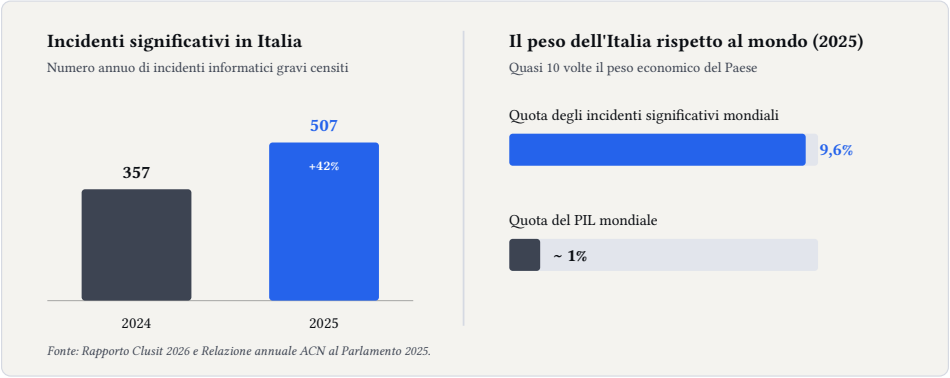

Figura 1.1: *Andamento degli incidenti informatici significativi: quota Italia vs mondo (dati: Clusit 2026; ACN, Relazione annuale 2025)*

Nella figura occorre osservare la percentuale, non i valori assoluti. Entrambe le curve salgono, ma la fetta italiana degli incidenti significativi mondiali si attesta al 9,6% a fronte di circa l'1% del PIL globale, sfiorando dieci volte il peso economico del Paese. È l'esatto contrario di ciò che suggerisce l'idea di essere «troppo piccoli».

C'è un altro elemento che i numeri non mostrano: chi si trova dall'altra parte. L'immagine del geniale adolescente che lavora da solo non sopravvive al contatto con il *ransomware-as-a-service*: gruppi organizzati come aziende, con decine di persone che si dividono compiti e ricompense. C'è chi scrive il software, chi vende l'accesso iniziale alle reti, chi esegue l'intrusione, chi conduce la trattativa e chi muove i soldi: ognuno incassa la propria quota, e c'è persino un banco di assistenza, perché anche i franchising criminali offrono un servizio clienti. Il capitolo 3 analizza a fondo questa filiera. Per riassumerla in una riga: quando il vostro server si ferma, le persone dall'altra parte del tavolo delle trattative stanno eseguendo un processo industriale, e questo processo ha un suo listino prezzi.

Nemmeno lo Stato è troppo grande

Anche le grandi dimensioni di un'azienda o di un ente non mettono al riparo. Prendiamo il GSE, Gestore dei Servizi Energetici: l'operatore statale al centro dei servizi energetici italiani, 714 dipendenti e oltre 16 miliardi di euro di incentivi erogati in un solo anno. Nella notte tra il 28 e il 29 agosto 2022, secondo i ricercatori, il gruppo BlackCat (noto anche come ALPHV) si è introdotto nei sistemi e ha copiato circa 700 gigabyte (GB) di dati prima

di andarsene.[8] Il GSE ha poi pubblicato la notifica richiesta dall'articolo 34 del GDPR (General Data Protection Regulation, la legge europea sulla privacy; l'articolo 34 obbliga un'organizzazione a informare le persone coinvolte quando una violazione le espone a un rischio elevato), relativa a rete, client, infrastruttura applicativa, file server e posta elettronica.[9] Un ente di proprietà statale, di rilevanza nazionale, eppure gli aggressori ne hanno svuotato gli scaffali.

Le dimensioni e la rilevanza nazionale non sono difese. La preparazione lo è.

L'aspetto della normalità

Questo per quanto riguarda i nomi finiti sui giornali. Ma come si presenta, statisticamente, l'azienda media? Il Cyber Index PMI, il rapporto nazionale sulla consapevolezza informatica delle PMI realizzato da Generali, Confindustria e Politecnico di Milano con il supporto dell'ACN, ha misurato nel 2024 una consapevolezza media di 52 su 100, su un campione di 1.005 PMI.[10] La terza edizione, del 2026, riporta un punteggio di 55 su 100: il 16% delle PMI è considerato maturo, il 14% principiante e il 70% si colloca in una fascia intermedia.[11] Una PMI su quattro ha subito un attacco nel 2025.[11] Anche il conto finale è stato stimato. Il costo medio di un attacco per una PMI italiana supera i 95.000 euro, mentre i casi peggiori oltrepassano i 300.000 euro se si calcolano i tempi di fermo, la perdita di dati e il danno d'immagine (dati Clusit 2025 riportati da KTS Finance).[12]

In questo contesto vi presentiamo ACME, l'azienda che farà da filo conduttore a questo libro. ACME S.r.l. è fittizia, ma costruita rigorosamente in scala: un'impresa manifatturiera del Nord Italia, circa 80 dipendenti, un fatturato di circa 18 milioni di euro, produttrice di componenti per la filiera meccanica e automobilistica. Il reparto IT ha risorse limitate: un collaboratore dedicato a tempo pieno e un secondo collega che divide il tempo tra l'informatica e altre attività. Questa seconda persona si occupa anche di mantenere in vita il software di produzione, dà una mano con la documentazione per la qualità e risponde di ogni stampante nell'edificio; la parola «sicurezza» non compare nella mansione di

[8] Reuters, «Ransomware group BlackCat behind Italy's GSE hacking, researchers say» (2 settembre 2022). Attacco nella notte tra il 28 e il 29 agosto 2022 al GSE (Gestore dei Servizi Energetici), operatore statale dei servizi energetici; rivendicato da BlackCat/ALPHV; rubati ~700 GB di dati. reuters.com

[9] GSE S.p.A., notifica di violazione dei dati ex art. 34 GDPR (colpiti rete, client, infrastruttura applicativa, file server e sistemi di posta elettronica). gse.it

[10] Generali / Confindustria / Osservatorio Cybersecurity & Data Protection (Politecnico di Milano) con il supporto dell'ACN, *Rapporto Cyber Index PMI 2024* (1.005 PMI intervistate): punteggio medio di consapevolezza cyber 52/100. public.confindustria.it

[11] Il Sole 24 Ore, «Rischio cyber, nel 2025 una Pmi su quattro ha ricevuto un attacco» (12 marzo 2026, terzo rapporto Cyber Index PMI, punteggio 55/100; PMI «mature» 16%, «principianti» 14%, 70% nei livelli intermedi). ilsole24ore.com

[12] KTS Finance, «Cyber Risk 2025: quanto costa un attacco informatico alle PMI italiane?» (14 ottobre 2025), citando dati del rapporto Clusit 2025: costo medio di un attacco cyber per una PMI italiana superiore a 95.000 euro; casi peggiori oltre i 300.000 euro (tempi di inattività, perdita di dati, danno reputazionale). ktsfinance.com

nessuno. La posta elettronica e i documenti si appoggiano a Microsoft 365; l'ERP (enterprise resource planning, il software che gestisce ordini, magazzino e fatture) è affidato a un provider locale. Tre grandi clienti, di quelli strutturati con uffici acquisti, invieranno presto dei questionari di sicurezza, perché sono obbligati a richiederli; il capitolo 5 spiega cosa fare quando arrivano. ACME non è negligente. ACME è normale. E la normalità è esattamente ciò che il mercato descritto poco fa sa come prezzare.

I conti di ACME: 18 milioni di euro di fatturato su circa 250 giorni lavorativi fanno circa 72.000 euro al giorno, cioè il costo di un giorno di fermo. Per una piccola e media impresa italiana la spesa media supera i 95.000 euro, cifra che supera una giornata intera di produzione ancor prima di calcolare un eventuale riscatto. Una settimana di blocco fa slittare ordini per circa 360.000 euro, e una parte di questi è persa per sempre: penali, spedizioni d'urgenza, clienti che iniziano in silenzio a qualificare un secondo fornitore. Il caso peggiore nazionale supera i 300.000 euro: una settimana di una normale azienda, prima di contare il riscatto.

02 · PER IL REFERENTE TECNICO ◆ ESECUZIONE & VERIFICA

Tre compiti per questa settimana, senza alcun acquisto necessario. Primo, mettete per iscritto l'incentivo dell'attaccante: quali informazioni si potrebbero rubare e rivendere, e a chi potrebbero servire. Contatti dei clienti, ordini aperti, fatture con IBAN, archivi di posta, specifiche di produzione, e per ciascuna voce dove vive. Secondo, trovate la data dell'ultimo aggiornamento di sicurezza applicato al server più vecchio dell'edificio e contate quanti account condividono la stessa password; appuntatevi entrambi i numeri, qualunque essi siano. Terzo, sedetevi per mezz'ora con il responsabile amministrativo e calcolate il costo di una giornata di fermo produzione: ordini bloccati, penali, personale inattivo. Questi tre risultati costituiscono la materia prima di ogni capitolo successivo.

La domanda che vale la pena farsi

Resta un'obiezione legittima, e va presa sul serio. Di fronte a dati statistici così netti, che peso ha la decisione di un singolo proprietario? Dipende da quale domanda vi fate. «Ci colpiranno?» non ha risposta, e chi promette di darvela sta vendendo qualcosa. «Se ci colpiscono, cosa succede e quanto ci costa?» ha invece una risposta, ed è possibile calcolarla: si tratta di un elenco di scelte, ciascuna con un costo immediato e potenziali conseguenze molto più gravi in futuro. L'esito di un incidente grave è determinato dagli investimenti fatti o dalle vulnerabilità accumulate nel tempo. Valutare il rischio è più utile che tentare di prevedere l'evento, perché l'attacco dipende da fattori esterni, mentre l'impatto finale dipende dalle vostre decisioni.

Il capitolo 2 ripercorre la giornata del cyberattacco minuto per minuto, evidenziando i costi reali in ogni fase: la prima telefonata, le macchine bloccate, la trattativa, il ripristino. Il resto del libro rappresenta il piano per cambiare il finale di quella giornata. E inizia proprio dove si chiude questo capitolo: dall'aritmetica, non dalla paura.

Nessuno sceglie una vittima. Tutti leggono un listino prezzi.

SCHEDA RIASSUNTIVA DI FINE CAPITOLO RBB/LAB · RUNBOOK

01 · DECISIONI E BUDGET · PER IL MANAGER

- La decisione: smettete di chiedervi se siete un bersaglio e stimate invece quanto vi costa una settimana di fermo produzione e quali dei vostri dati si potrebbero vendere sul mercato nero.
- Cosa protegge: il budget. I soldi vanno dove indicano le reali probabilità di subire un attacco, e le offerte dei fornitori diventano confrontabili.
- Budget e tempi realistici: un pomeriggio con il vostro responsabile IT e il responsabile amministrativo. Questo capitolo non richiede alcun acquisto.

02 · CHECKLIST OPERATIVA · PER IL REFERENTE TECNICO

☐ Inventariare i dati vendibili (contatti dei clienti, ordini aperti, fatture con IBAN, archivi di posta elettronica, specifiche di produzione) e dove risiede ciascuna voce.

☐ Registrare la data dell'ultimo aggiornamento di sicurezza sul server più vecchio e il numero di password condivise o riutilizzate.

☐ Verifica: calcolare e definire formalmente, insieme all'amministrazione, il costo giornaliero del fermo produzione. Se questo dato non è disponibile, significa che la stima finanziaria del rischio non è stata fatta.

CAPITOLO 2

Anatomia di un disastro

> *Un martedì immaginario alla ACME S.r.l., minuto per minuto ed euro per euro, con i numeri reali alla mano: la richiesta di riscatto alle 7:40, il backup troppo accessibile, la negoziazione, il conto alla rovescia delle 72 ore che scorre in parallelo e i cinque momenti in cui la giornata avrebbe potuto prendere una piega diversa.*

Alle 7:40 di un martedì mattina di fine ottobre, alla ACME si accesero i primi computer e su uno degli schermi comparve un documento che nessuno aveva scritto. Chiara, in amministrazione, inserì la password e al posto del foglio di calcolo delle vendite lasciato aperto la sera prima trovò un file di testo: contattateci, pagate in bitcoin, non coinvolgete le autorità o il prezzo salirà. L'ERP (il software gestionale che governa ordini, magazzino e fatture) si bloccò su ogni postazione dell'ufficio senza riuscire a caricare i dati. In officina i macchinari continuavano a muoversi, perché eseguono programmi caricati localmente e non dipendono direttamente dai server; mancavano però gli ordini di produzione della giornata, salvati su un server che aveva smesso di rispondere. Alle 8:00 tre server aziendali mostravano lo stesso messaggio di riscatto.

Abbiamo già incontrato ACME nel primo capitolo: un'azienda manifatturiera del Nord Italia con circa ottanta dipendenti, 18 milioni di euro di fatturato e un reparto IT ridotto al minimo. L'azienda è fittizia, ma la cronologia che segue ricostruisce passo dopo passo come si svolgono davvero questi incidenti nelle PMI italiane, combinando dinamiche, tempi e costi tratti da casi reali.

Le settimane precedenti

Nessuno alla ACME aveva fatto nulla di insolito. Settimane prima, un venerdì pomeriggio, un dipendente aveva aperto un'email di phishing e inserito la propria password in una pagina identica alla webmail aziendale. Era una password unica, riutilizzata dal 2021. Da quel momento un attaccante era entrato nella rete senza farsi notare, limitandosi per settimane a osservare: aveva esplorato le cartelle condivise sui server, censito le macchine, individuato il database dell'ERP e i backup e verificato a quali risorse potesse accedere ciascun account. Stava studiando la pianta della casa mentre la famiglia guardava la televisione.

Secondo l'indagine globale Sophos condotta su aziende tra i 100 e i 5.000 dipendenti, la prima causa tecnica di intrusione è lo sfruttamento di una vulnerabilità nota, cioè un difetto del software che un normale aggiornamento avrebbe risolto.[1] Alla ACME il punto d'ingresso è stato invece una password sottratta tramite phishing: cambia la porta d'accesso, ma ciò che avviene dentro la rete è identico. Una volta entrato, la prima mossa dell'attaccante è sempre cercare i backup, l'unico strumento che può rendere inutile il blocco dei sistemi. E nella maggior parte delle aziende li trova accessibili.

Ore 8:15: la portata del danno

Alle 8:15 Marta, l'unica persona dedicata a tempo pieno all'IT, aveva chiaro il perimetro dell'incidente. Tutti i server mostravano la richiesta di riscatto, le cartelle condivise erano inaccessibili, il database dell'ERP era crittografato e i piani di produzione della giornata erano spariti. Continuava a funzionare solo la posta elettronica, perché Microsoft 365 risiede nei data center di Microsoft e non sui server aziendali bloccati durante la notte. L'attacco finale aveva impiegato pochi minuti; la preparazione aveva richiesto settimane.

Quello che sta succedendo ad ACME ricalca da vicino il caso reale della Alf DaFrè visto nel primo capitolo: anche lì l'attacco è scattato di notte, ha bloccato in pochi minuti il server che governa la produzione e ha fermato la fabbrica per oltre otto giorni, fino alla richiesta di cassa integrazione.[2]

Alle 9:00 anche Bruno, il titolare, aveva capito cosa fosse un ransomware, nel modo in cui lo scoprono quasi tutti gli imprenditori: trovandoselo in azienda. In Italia il 61% degli attacchi informatici arriva a crittografare i dati,[3] e la ACME era appena entrata in quella statistica. Il messaggio degli attaccanti chiedeva una somma a cinque cifre in bitcoin, con l'avviso che l'importo sarebbe raddoppiato ogni 48 ore.

Alle 9:30 Marta chiamò il fornitore locale che gestisce l'ERP. Il fornitore richiamò solo dopo pranzo: il contratto di assistenza, firmato anni prima, non prevedeva alcuna clausola

[1] Sophos, *The State of Ransomware 2025* (sondaggio su 3.400 responsabili IT e cybersecurity in 17 Paesi, organizzazioni da 100 a 5.000 dipendenti): costo medio di ripristino pari a 1,53 milioni di dollari escluso il riscatto (638.000 dollari per le organizzazioni da 100 a 250 dipendenti); vulnerabilità sfruttate come prima causa tecnica di intrusione; circa il 50% delle vittime ha pagato il riscatto; il 53% ha recuperato completamente l'operatività entro una settimana (35% l'anno precedente). assets.sophos.com

[2] Il Post, «L'azienda veneta costretta a chiedere la cassa integrazione per un attacco informatico» (18 febbraio 2025). Alf DaFrè (produttore di mobili, Treviso, ~350 dipendenti): gli aggressori sono entrati nei server nella notte tra il 10 e l'11 febbraio 2025 bloccando il server di produzione in pochi minuti; produzione sospesa per oltre otto giorni, l'azienda ha richiesto la cassa integrazione. ilpost.it

[3] Sophos, *The State of Ransomware in Italy 2026* (sondaggio indipendente dai fornitori; segmento italiano): il 61% degli attacchi in Italia ha crittografato i dati (media globale 56%); il 47% delle organizzazioni italiane ha pagato il riscatto e riavuto i dati (27% l'anno precedente); il 98% di coloro che hanno subito la crittografia dei dati li ha recuperati; i dati sono stati rubati anche nel 23% degli attacchi in cui i dati sono stati crittografati. assets.sophos.com

sulle emergenze né tempi massimi di risposta garantiti. Il capitolo 17 è dedicato proprio a come verificare e rinegoziare questi contratti.

Ore 11:00: i clienti e la scoperta sui backup

Alle 11:00 squillò il telefono in amministrazione: era il responsabile acquisti di uno dei tre grandi clienti della ACME. Sul loro portale le conferme d'ordine risultavano bloccate e chiedeva spiegazioni. Non avendo ancora informazioni certe, l'amministrazione diede una risposta evasiva, di quelle che pochi giorni dopo si è costretti a smentire. Prima della pausa pranzo l'ufficio acquisti del committente aveva già aperto una segnalazione interna di rischio fornitore sulla ACME: una procedura che nei grandi gruppi industriali può far scattare il blocco dei nuovi ordini, la revisione delle condizioni contrattuali e l'attivazione di un fornitore alternativo. La scheda veniva compilata unilateralmente dal cliente, senza che ACME avesse potuto fornire una propria versione dei fatti. Il capitolo 5 spiega come gestire in anticipo le richieste sulla sicurezza e le procedure di qualifica dei clienti strutturati, prima che sia un incidente a farle scattare.

Nel primo pomeriggio un contatto di Bruno fornì il recapito di una società specializzata in *DFIR* (digital forensics and incident response, gli specialisti che ricostruiscono come sono entrati gli attaccanti, quali sistemi hanno compromesso e se hanno ancora accesso alla rete). La prima telefonata seguì una procedura d'emergenza ben precisa: non pagate nulla per il momento, non cancellate nulla, non formattate né reinstallate i sistemi e date per scontato che ogni operazione eseguita su quei server sia visibile agli attaccanti. Poi, alle 14:30, arrivò la domanda che gli specialisti pongono sempre per prima:

Avete dei backup funzionanti?

Marta diede la risposta che danno quasi tutte le aziende: un *NAS* (network-attached storage, un dispositivo di archiviazione collegato alla rete locale nella sala server) copiava i server ogni notte e inviava ogni mattina una notifica di operazione completata. I rapporti risultavano regolari da anni. Avere una copia completata e riuscire davvero a ripristinarla, però, sono due cose diverse: nessuno in azienda aveva mai provato a recuperare nemmeno un singolo file da quel dispositivo, e il consulente DFIR lo sapeva bene.

La verifica tecnica durò fino alle 17:00. Il NAS accettava lo stesso account di amministratore di dominio che gli attaccanti avevano compromesso e usato sul resto della rete; la cartella dei backup era raggiungibile da qualsiasi PC dell'ufficio, incluso quello violato settimane prima. L'ultima copia integra risaliva a tre giorni prima; tutto ciò che seguiva era stato cancellato dagli intrusi. Non è un'eccezione: nel 94% degli attacchi ransomware i criminali cercano di compromettere i backup, e nel 57% dei casi ci riescono.[4] Un backup

[4] Sophos, *The State of Ransomware 2024*: il 94% delle organizzazioni colpite ha dichiarato che gli attaccanti hanno tentato di compromettere i backup; il 57% di questi tentativi ha avuto successo; il 70% degli attacchi ha comportato la crittografia dei dati. insight.com

accessibile con le stesse credenziali che aprono il resto della rete aziendale non è un backup: è solo un'altra cartella che viene cancellata o crittografata insieme ai server.

02 · PER IL REFERENTE TECNICO ◆ ESECUZIONE & VERIFICA

Tre verifiche da fare questa settimana, in quest'ordine. Primo: controllate dove vengono salvati i backup e quale account li esegue; se quello stesso account ha anche i permessi per modificarli o cancellarli, siete esattamente nella situazione di ACME e dovete separare subito i privilegi. Secondo: chiedete la data e il verbale dell'ultimo test di ripristino; se non esistono, mettete a calendario una prova di recupero entro la fine del mese (il capitolo 14 spiega la procedura passo dopo passo). Terzo: individuate fin d'ora il partner tecnico da chiamare in caso di incidente e assicuratevi che l'amministrazione e la direzione abbiano già approvato la procedura per attivarlo senza esitazioni.

Il conto, in tre voci

Vediamo ora quanto costa concretamente una giornata come questa. Il conto finale si divide in tre voci.

La prima voce è il fermo operativo. Come calcolato nel primo capitolo, 18 milioni di euro di fatturato su circa 250 giorni lavorativi corrispondono a circa 72.000 euro di produzione al giorno. Dieci giorni lavorativi per ripristinare i sistemi fanno slittare circa 720.000 euro di commesse: una parte viene consegnata in ritardo, ma una parte è persa per sempre tra penali, spedizioni d'urgenza e clienti che spostano gli ordini su un secondo fornitore. Nei casi reali che abbiamo visto i tempi di fermo non sono stati da meno: oltre otto giorni alla Alf DaFrè,[2] tre settimane alla Fraschetti,[5] a fronte di un costo medio nazionale che supera i 95.000 euro per attacco e oltrepassa i 300.000 euro nei casi più gravi.[6] Solo con il blocco della produzione, la ACME ha già superato entrambe le soglie.

La seconda voce è il costo di gestione e risposta all'incidente, che quasi nessuna PMI mette a budget perché nessuno pianifica di dover acquistare questi servizi: le perizie forensi necessarie per assicuratori, legali e Garante della privacy; l'assistenza legale specializzata; la ricostruzione da zero dei server compromessi, di cui non ci si può più fidare; le ore di straordinario notturno del personale interno distolto dal proprio lavoro abituale. A livello globale l'indagine Sophos rileva un costo medio di ripristino di 1,53 milioni di dollari (riscatto escluso), che scende a 638.000 dollari per le aziende tra i 100 e i 250 dipendenti.[1]

[5] CyberSecItalia, «Fraschetti Spa, ransomware ferma la produzione per tre settimane» (28 ottobre 2025; l'attacco si è verificato il 9-10 ottobre 2024). Fraschetti S.p.A. (distribuzione ferramenta/giardinaggio, Frosinone) attaccata il 9-10 ottobre 2024; produzione sospesa per settimane; richiesta la cassa integrazione. cybersecitalia.it

[6] KTS Finance, «Cyber Risk 2025: quanto costa un attacco informatico alle PMI italiane?» (14 ottobre 2025), citando dati del rapporto Clusit 2025: costo medio di un attacco cyber per una PMI italiana superiore a 95.000 euro; casi peggiori oltre i 300.000 euro (tempi di inattività, perdita di dati, danno reputazionale). ktsfinance.com

Per una realtà delle dimensioni di ACME la spesa diretta di consulenza e ripristino è più contenuta, nell'ordine delle decine di migliaia di euro, ma arriva tutta insieme e fuori budget. La stessa indagine rileva che solo il 53% delle aziende colpite riesce a tornare pienamente operativo entro una settimana:[1] significa che quasi la metà impiega più di sette giorni, mentre il fermo continua a costare 72.000 euro al giorno.

● 01 · PER IL MANAGER ◆ DECISIONE & BUDGET

La decisione più urgente non riguarda il ransomware in sé, ma la gestione della prima ora. Stabilite oggi chi ha l'autorità di dichiarare l'incidente, chi contatta la società di DFIR, chi gestisce le comunicazioni con i clienti e chi quelle con il Garante, assegnando in anticipo un budget di emergenza per le prime verifiche; il capitolo 18 vi guida a condensare queste scelte in un piano operativo di una sola pagina, realizzabile in un pomeriggio. Definirlo a mente fredda costa una riunione interna. Improvvisarlo il giorno dell'attacco significa dover cercare e contrattare consulenti d'urgenza nel pieno del blocco produttivo, con fornitori che sanno perfettamente che non avete alternative. Con un fermo fabbrica da 72.000 euro al giorno, organizzare in anticipo la prima ora d'intervento è l'investimento più redditizio che l'azienda possa fare.

La terza voce è il riscatto. I numeri parlano chiaro: a livello globale circa metà delle organizzazioni colpite decide di pagare.[1] In Italia ha pagato il riscatto e riottenuto i dati il 47% delle aziende colpite, in netto aumento rispetto al 27% dell'anno precedente,[3] mentre il 98% di chi ha subito la crittografia è riuscito in qualche modo a recuperare i file (pagando o tramite backup).[3] Pagare di solito permette di ricevere la chiave di sblocco, ma non chiude l'incidente: nel 23% degli attacchi con crittografia i criminali hanno anche rubato una copia dei dati,[3] e nessuna chiave di decrittazione cancella il vostro portafoglio ordini o i vostri progetti dai server di chi li ha sottratti. Il riscatto, insomma, è solo una delle voci del danno, spesso non è nemmeno la più alta, ma è l'unica su cui gli attaccanti impongono un conto alla rovescia.

La trattativa e la scadenza delle 72 ore

Nella realtà una trattativa ransomware non somiglia a ciò che si vede nei film. Non ci sono telefonate: il messaggio di riscatto rimanda a una chat sulla rete Tor (raggiungibile solo con un browser specifico) e lo scambio segue una procedura commerciale standardizzata. Gli attaccanti dimostrano di poter sbloccare i sistemi decrittando gratuitamente un paio di file a scelta dell'azienda; provano il furto dei dati mostrando schermate degli ordini aperti o di documenti interni; infine avanzano una richiesta economica calibrata sul fatturato stimato della vittima e sugli eventuali massimali della sua polizza assicurativa. Le aziende che scelgono di trattare si affidano spesso a un *negoziatore* (un consulente specializzato nel condurre queste comunicazioni). Qui occorre avere ben chiara la dinamica economica:

il negoziatore è pagato dalla vittima, ma il suo obiettivo pratico è trovare una cifra su cui l'attaccante accetti di chiudere l'accordo. La scadenza delle 48 ore, la minaccia di raddoppiare l'importo e il timer che scorre nella pagina di chat non sono vincoli tecnici: sono strumenti di pressione commerciale studiati per spingervi a pagare prima che i vostri tecnici abbiano capito se è possibile ripristinare i sistemi in autonomia.

Mentre scorre il timer degli attaccanti, parte una seconda scadenza, questa volta fissata dalla legge. Quando vengono sottratti dati personali, come confermato dai primi rilievi forensi alla ACME, il GDPR (General Data Protection Regulation, il regolamento europeo sulla protezione dei dati) impone di notificare la violazione al Garante per la protezione dei dati personali entro 72 ore dal momento in cui l'azienda ne viene a conoscenza. Sono tre giorni, da cui vanno sottratte le ore già impiegate per capire cosa è stato compromesso. Il capitolo 6 illustra nel dettaglio la procedura di notifica; il punto critico, nelle prime ore dell'emergenza, è che la scadenza legale e l'estorsione corrono in parallelo: dall'altra parte della chat ci sono gruppi criminali che gestiscono decine di trattative al mese, mentre l'azienda si trova ad affrontare per la prima volta contemporaneamente il fermo della produzione e gli adempimenti verso l'autorità di controllo.

Entra poi in gioco un terzo soggetto, che alla ACME avevano quasi dimenticato: la compagnia assicurativa. L'azienda aveva stipulato una polizza cyber, rinnovata per tre anni guardando solo l'importo del premio. In caso di sinistro, però, l'assicurazione impone i propri periti forensi e il proprio negoziatore, verifica che quanto dichiarato nel questionario di assunzione corrisponda al vero ed esamina con attenzione le clausole di esclusione: server non aggiornati o l'assenza di autenticazione a più fattori (MFA, un secondo controllo oltre alla password che impedisce l'accesso anche se la credenziale viene rubata) possono invalidare la copertura proprio nel momento del bisogno. Il capitolo 19 spiega come analizzare queste polizze prima di firmarle. Il giorno dell'incidente vale invece una regola operativa semplice: contattare l'assicurazione prima di autorizzare qualsiasi intervento o pagamento, per non perdere il diritto al rimborso.

È la stessa sequenza che abbiamo visto nel primo capitolo su scala molto più grande con il caso del GSE: dopo l'intrusione della notte tra il 28 e il 29 agosto 2022 e il furto di circa 700 gigabyte di dati,[7] anche l'operatore statale ha dovuto isolare i sistemi e pubblicare la notifica formale prevista dall'articolo 34 del GDPR, elencando gli ambienti compromessi (rete, postazioni di lavoro, infrastruttura applicativa, file server e posta elettronica).[8] Che si tratti di un grande ente nazionale o di una PMI manifatturiera da ottanta dipendenti, i passaggi tecnici e legali dopo l'impatto sono gli stessi.

[7] Reuters, «Ransomware group BlackCat behind Italy's GSE hacking, researchers say» (2 settembre 2022). Attacco nella notte tra il 28 e il 29 agosto 2022 al GSE (Gestore dei Servizi Energetici), operatore statale dei servizi energetici; rivendicato da BlackCat/ALPHV; rubati ~700 GB di dati. reuters.com

[8] GSE S.p.A., notifica di violazione dei dati ex art. 34 GDPR (colpiti rete, client, infrastruttura applicativa, file server e sistemi di posta elettronica). gse.it

L'altro finale

Un caso reale documentato in provincia di Bergamo mostra come può concludersi la stessa giornata quando le difese essenziali sono già state predisposte. Un'azienda manifatturiera lombarda viene colpita dallo stesso tipo di ransomware: gli attaccanti entrano nella rete e dopo 47 minuti avviano la crittografia dei sistemi. Quello che non riescono a toccare è la copia di sicurezza della notte precedente, salvata su un *backup immutabile*, cioè uno spazio di archiviazione che nessun account, nemmeno l'amministratore di sistema, può modificare o cancellare prima di una scadenza prefissata. I tecnici verificano l'integrità dei dati su server isolati dalla rete aziendale e completano il ripristino in circa quattro ore. Non è stata una questione di fortuna né di budget fuori portata: la differenza l'ha fatta una decisione presa mesi prima, spendendo poche centinaia di euro all'anno per uno spazio di backup separato dalle credenziali di dominio e collaudando in anticipo la procedura di recupero.

Per la ACME l'incidente significa settimane di fermo; per l'azienda bergamasca si è risolto in mezza giornata. L'attacco era identico. A cambiare l'esito è stata una misura preventiva che ha tolto agli estorsori la loro principale leva di ricatto.

I cinque punti in cui si poteva fermare

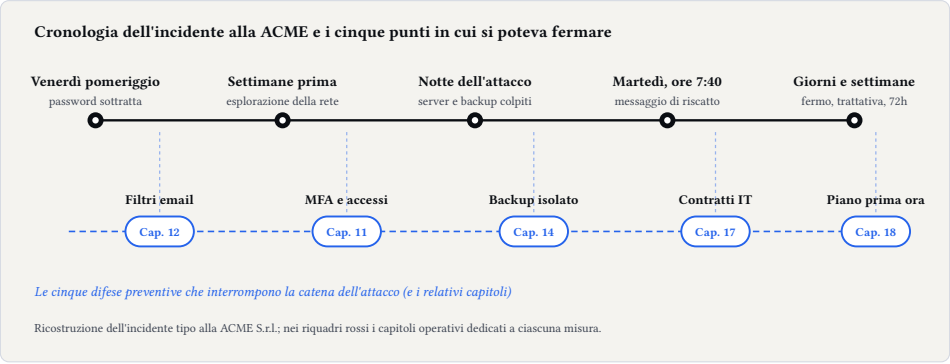

Figura 2.1: *La giornata come una catena, con i cinque punti in cui poteva spezzarsi*

Rileggendo l'incidente della ACME dall'inizio alla fine, emergono cinque passaggi decisivi. La buona notizia è che sarebbe bastato interromperne anche solo uno per evitare il blocco dell'azienda, e a ciascuno di essi è dedicato un capitolo operativo di questo libro:

- **L'email di phishing iniziale (capitolo 12):** come proteggere la posta aziendale e ridurre la probabilità che un messaggio fraudolento raggiunga i dipendenti.

- **La password riutilizzata e priva di secondo fattore (capitolo 11):** come introdurre un gestore di password e l'autenticazione a più fattori, rendendo inutilizzabile una credenziale rubata.
- **Il backup accessibile dalla rete (capitolo 14):** come isolare le copie di sicurezza dagli account amministrativi ordinari e verificarne l'efficacia con test di ripristino periodici.
- **Il fornitore ERP senza tempi di risposta garantiti (capitolo 17):** quali garanzie contrattuali e tempi di intervento richiedere ai fornitori informatici critici prima che si verifichi un'emergenza.
- **L'improvvisazione della prima ora (capitolo 18):** come preparare in anticipo un piano di risposta agli incidenti di una sola pagina, con ruoli, contatti e procedure già approvati.

Nessuna di queste cinque misure richiede tecnologie complesse o investimenti proibitivi per una PMI. Sono interventi ordinari che si pianificano nei mesi tranquilli, quando i sistemi funzionano e si può decidere con lucidità.

L'esito del martedì nero della ACME non è stato deciso quella mattina alle 7:40: è stato determinato dalle scelte rimandate nei mesi precedenti. Il messaggio di riscatto ha solo presentato il conto.

SCHEDA RIASSUNTIVA DI FINE CAPITOLO RBB/LAB · RUNBOOK

01 · DECISIONI E BUDGET · PER IL MANAGER

- La decisione: definire subito un piano di risposta agli incidenti di una pagina (chi dichiara l'emergenza, chi contatta il partner DFIR, il legale, l'assicurazione e i clienti) e pre-approvare il budget per il primo intervento.
- Cosa protegge: la continuità operativa dell'azienda (72.000 euro al giorno di produzione, per una realtà come ACME), il rispetto della scadenza legale delle 72 ore prevista dal GDPR e la capacità di gestire fornitori e controparti senza agire in preda al panico.
- Budget e tempi realistici: un pomeriggio di lavoro per redigere il piano; poche migliaia di euro all'anno per un accordo di intervento rapido (retainer) con un'azienda specializzata in DFIR; il test di ripristino dei backup può rientrare nel contratto di assistenza IT già attivo.

02 · CHECKLIST OPERATIVA · PER IL REFERENTE TECNICO

☐ Individuare dove risiedono i backup e verificare se l'account che li esegue ha anche i permessi per modificarli o cancellarli; in caso affermativo, separare subito le credenziali e configurare copie immutabili entro questo mese.

☐ Eseguire una prova di ripristino dal backup della notte precedente su una macchina isolata, misurando il tempo effettivo richiesto, e pianificare un test completo seguendo la procedura del capitolo 14.

☐ Verifica: assicurarsi che i riferimenti del partner DFIR e la procedura di attivazione siano condivisi con l'amministrazione e già approvati dalla direzione, così da poterli attivare immediatamente in caso di blocco.

CAPITOLO 3

Chi attacca e come

> *Dietro un attacco ransomware non c'è un genio solitario, ma una filiera criminale specializzata: gli intermediari vendono accessi alle reti aziendali al prezzo di un portatile, gli affiliati noleggiano il software d'attacco in franchising, i negoziatori e i riciclatori si spartiscono il riscatto e i dati rubati vengono rivenduti per anni. Questo capitolo ricostruisce ogni passaggio di questa catena e mostra come le difese di base rendano l'attacco antieconomico fin dall'ingresso.*

Su un forum del *dark web* (la parte di internet raggiungibile solo tramite appositi software di anonimizzazione, che un normale browser non può aprire), nella sezione in cui gli accessi alle reti aziendali si comprano e si vendono come auto usate, compare un annuncio di questo tipo:

Azienda manifatturiera, Europa occidentale. Fatturato stimato tra i 10 e i 50 milioni. Accesso iniziale tramite servizio di accesso remoto, credenziali verificate e funzionanti, privilegi di amministratore inclusi. Prezzo: 900 dollari. Escrow accettato.

Nella stessa bacheca scorrono decine di inserzioni analoghe: un'azienda di logistica, un gruppo di cliniche private, un'impresa edile, il fornitore di una compagnia aerea. Le voci della scheda sono sempre le stesse: settore, area geografica, fascia di fatturato, tipo di accesso offerto e prezzo richiesto. Forum criminali come Exploit, XSS e RAMP ospitano migliaia di annunci di questo genere, e i ricercatori che li hanno catalogati hanno calcolato un prezzo medio di vendita poco superiore ai 2.700 dollari.[1] L'inserzione riportata qui sopra è un esempio ricomposto a scopo illustrativo, ma ciascuna delle sue voci ricalca fedelmente il formato standard usato in queste compravendite.[1,]

Non ci sono dossier segreti, figure incappucciate o geni dell'informatica curvi su tre monitor: c'è solo una scheda standardizzata in un catalogo online, archiviata tra una contestazione sulla commissione di *escrow* (il servizio di deposito a garanzia gestito dal forum, che trattiene il denaro finché l'acquirente non conferma che le credenziali

[1] Rapid7, *2025 Initial Access Brokers Report*: analisi delle inserzioni degli initial access broker (IAB) sui forum Exploit, XSS e RAMP; il prezzo base medio di una vendita di accesso è poco superiore ai 2.700 dollari, con la maggior parte delle transazioni nella fascia tra 500 e 1.000 dollari; il 71,4% delle vendite include già un livello di privilegio e circa il 10% raggruppa vettori di accesso multipli e/o privilegi in un unico pacchetto; le inserzioni si concentrano in larga misura su aziende occidentali, con una selezione dei settori merceologici prevalentemente opportunistica. rapid7.com

funzionano) e una guida su come convertire i proventi in valuta corrente. Soprattutto, chi ha pubblicato la scheda non è la stessa persona che una notte lancerà la crittografia sui server dell'azienda descritta: l'autore dell'annuncio è un intermediario, e il suo unico mestiere consiste nel trovare una via d'ingresso nella rete e rivenderla.

Per un consiglio di amministrazione o per il titolare di una PMI italiana, leggere una di queste inserzioni è molto più istruttivo che leggere la cronaca di un attacco sui giornali. Mentre le notizie raccontano l'emergenza a disastro avvenuto, l'annuncio di vendita mostra con freddezza contabile come viene valutata un'impresa sul mercato nero e quanto poco basta per metterla in catalogo.

Il mercato degli accessi aziendali

Nel lessico della sicurezza informatica questo intermediario è chiamato *initial access broker* (IAB): un criminale la cui intera attività consiste nell'ottenere un primo accesso abusivo a una rete aziendale per poi cederlo ad altri gruppi. Il broker non gestisce l'estorsione, non sviluppa il codice del ransomware e non comunica mai con la vittima: si limita a entrare, verificare che l'accesso ottenuto sia stabile e rivendibile e pubblicare l'offerta.

Ciò che viene messo in vendita nelle inserzioni è quasi sempre un elemento tecnico molto semplice: una credenziale funzionante, un sistema esposto su internet e privo degli ultimi aggiornamenti di sicurezza, un accesso al portale VPN o un account con diritti di amministratore. Nel 71,4% delle compravendite l'acquirente riceve già un certo livello di privilegio sulla rete, non il semplice profilo di un utente ordinario;[1] circa il 10% dei lotti raggruppa inoltre più punti d'ingresso o più account privilegiati in un unico pacchetto.[1] Il prezzo varia in base a ciò che quelle credenziali permettono di controllare: le inserzioni oscillano in genere tra i 500 e i 3.000 dollari, e nella metà dei casi non superano i 1.000 dollari. La media complessiva sale a poco più di 2.700 dollari solo perché alcune reti di grandi dimensioni vengono vendute a cifre molto elevate,[1] ma la maggior parte delle transazioni si chiude nella fascia tra i 500 e i 1.000 dollari.[1]

Con la cifra necessaria per acquistare un singolo portatile, un attaccante compra le credenziali per entrare in una rete aziendale che collega ottanta postazioni di lavoro.[1] Ancora più rilevante è la tendenza registrata a partire dal 2024: i broker hanno preso di mira un numero crescente di aziende di dimensioni più contenute, abbassando di conseguenza i prezzi delle inserzioni. Di fronte a grandi gruppi industriali sempre più protetti, gli operatori del mercato criminale non hanno ridotto l'attività: si sono spostati verso le PMI, dove le barriere d'ingresso sono più basse.

Come fanno i broker a procurarsi questi accessi? Esattamente attraverso le vulnerabilità che abbiamo già incontrato nei primi due capitoli: una password sottratta con un'email di phishing come quella che ha aperto la rete della ACME, un difetto noto su un server o un

firewall a cui nessuno ha applicato la *patch* disponibile da mesi, oppure una credenziale rubata anni prima e ancora valida perché riutilizzata su più servizi. Il lavoro del broker consiste nell'individuare queste aperture prima degli altri, verificare che la password o la falla funzionino ancora e fissare un prezzo di vendita.

Il modello RaaS: il ransomware in franchising

Quando l'inserzione trova un compratore, entra in scena una seconda figura professionale: l'*affiliato*, cioè l'operatore che acquista l'accesso dal broker, penetra nella rete della vittima, esplora le cartelle, sabota i backup, esfiltra i documenti e avvia la crittografia dei server. Nella maggior parte dei casi l'affiliato non sviluppa in proprio il software di attacco, ma noleggia una piattaforma di *ransomware-as-a-service* (RaaS): una formula organizzata come un franchising, in cui un gruppo centrale scrive il codice del ransomware, gestisce l'infrastruttura di pagamento e recluta gli affiliati, mentre questi ultimi conducono le intrusioni sul campo e trattengono la quota maggiore del riscatto versando una percentuale ai gestori della piattaforma. Esiste persino un servizio di assistenza tecnica interna che risponde alle richieste di supporto degli affiliati durante le operazioni.[2] Le analisi di settore confermano che il RaaS è oggi il modello operativo dominante tra i grandi gruppi di estorsione informatica.[2]

Questa divisione dei compiti segue la stessa logica economica di qualsiasi rete in franchising. Chi sviluppa il software moltiplica i propri ricavi reclutando nuovi affiliati anziché eseguire personalmente le intrusioni; l'affiliato aumenta il numero di attacchi comprando accessi già verificati dai broker anziché cercarli da zero; nessun componente della filiera ha bisogno di padroneggiare più di un singolo passaggio.[2] Anche la sigla del gruppo RaaS viene gestita come un marchio commerciale: il sito nel dark web su cui vengono pubblicati i file sottratti (*leak site*) e la fama stessa dell'organizzazione servono a intimidire la vittima successiva e a convincerla che la minaccia è concreta. LockBit, l'organizzazione RaaS che ha rivendicato l'attacco al cloud provider Westpole visto nel primo capitolo, bloccando la fatturazione elettronica e i servizi di centinaia di enti pubblici durante il ponte dell'Immacolata del 2023, è l'esempio più noto di questo modello.[3]

[2] Flare via BleepingComputer, «Ransomware as a Service and the Strange Economics of the Dark Web» (27 marzo 2024): il RaaS è il modello organizzativo dominante tra i grandi gruppi ransomware; il gruppo centrale sviluppa il codice, gestisce l'infrastruttura e recluta gli affiliati sui forum del dark web; gli affiliati eseguono le intrusioni e distribuiscono il ransomware, mentre le trattative sono spesso condotte dalla piattaforma RaaS. bleepingcomputer.com

[3] Wired Italia, «Westpole, PA Digitale e il cyber domino che ha messo ko gli enti pubblici in Italia» (14 dicembre 2023). Attacco ransomware intorno alle 5:30 dell'8 dicembre 2023 contro il cloud provider Westpole (gruppo Cegeka), data center di Roma e Milano; effetto a cascata su PA Digitale (servizi usati da ~1.300 enti pubblici) e blocco dei servizi di fatturazione elettronica per i clienti Dylog e Buffetti; rivendicato da LockBit 3.0. wired.it

Un aspetto specifico di questa ripartizione dei ruoli chiarisce quanto abbiamo visto accadere durante l'incidente della ACME nel secondo capitolo. Nel modello RaaS le trattative con l'azienda colpita vengono spesso condotte direttamente dalla struttura centrale della piattaforma, non dall'affiliato che ha eseguito l'intrusione.[2] Chi scrive nella finestra di chat sulla rete Tor è quindi, di frequente, un negoziatore professionista che lavora per i gestori del servizio RaaS, non l'operatore tecnico che ha violato i server. Il conto alla rovescia che raddoppia l'importo richiesto dopo 48 ore non dipende dall'umore dell'attaccante né da informazioni particolari sulla vittima: è una leva standard di pressione commerciale, applicata centinaia di volte su imprenditori che si trovano invece a subirla per la prima volta.

La spartizione e il riciclaggio del riscatto

Il percorso del denaro riflette fedelmente l'organizzazione della filiera. Quando la vittima paga il riscatto in criptovaluta, la somma viene ripartita secondo quote prefissate: il broker è già stato saldato al momento della cessione dell'accesso iniziale, la piattaforma RaaS trattiene automaticamente la propria commissione e l'affiliato incassa il resto. A quel punto subentra un ulteriore segmento specializzato, dedicato al riciclaggio dei proventi: i fondi vengono frazionati e fatti transitare attraverso catene di portafogli digitali (*wallet*) per ostacolare i tracciamenti, fino ai servizi di cambio che li convertono in valuta corrente trattenendo una propria percentuale. Nulla viene improvvisato: nel momento in cui una richiesta di riscatto compare sullo schermo di un'azienda in Lombardia o in Veneto, ogni anello della catena conosce già in anticipo la propria quota.

Quando l'impresa colpita incarica un negoziatore esterno, come abbiamo visto nel secondo capitolo, la trattativa si inserisce dentro questo meccanismo economico: da un lato il consulente pagato dalla vittima per prendere tempo e trovare una cifra su cui chiudere l'accordo, dall'altro l'operatore della piattaforma RaaS che gestisce l'incasso seguendo tariffe e scadenze prestabilite.[2]

Il mercato secondario dei dati rubati

La crittografia dei server serve a paralizzare l'operatività nell'immediato, ma la copia dei file sottratti alimenta un mercato secondario che dura molto più a lungo. Come già rilevato nel secondo capitolo, in Italia il furto dei dati accompagna la crittografia dei sistemi nel 23% degli attacchi ransomware.[4] Ciò che viene copiato dai server aziendali viene rimesso in circolazione in due fasi: prima la pubblicazione di un campione di

[4] Sophos, *The State of Ransomware in Italy 2026* (sondaggio indipendente dai fornitori; segmento italiano): il 61% degli attacchi in Italia ha crittografato i dati (media globale 56%); il 47% delle organizzazioni italiane ha pagato il riscatto e riavuto i dati (27% l'anno precedente); il 98% di coloro che hanno subito la crittografia dei dati li ha recuperati; i dati sono stati rubati anche nel 23% degli attacchi in cui i dati sono stati crittografati. assets.sophos.com

documenti sul *leak site* del gruppo per costringere la vittima a pagare, poi la vendita dell'intero archivio ad altri criminali. Anagrafiche clienti, ordini aperti, fatture con IBAN e anni di corrispondenza via email costituiscono, come visto nel primo capitolo, la base informativa perfetta per costruire frodi sui pagamenti mirate contro i clienti stessi dell'azienda colpita.

Dal punto di vista di chi acquista questi archivi sul mercato nero, il loro pregio principale è la durata nel tempo. I documenti aziendali non perdono validità in pochi giorni: un archivio di fatture, listini e contratti sottratto nel 2024 può essere sfruttato ancora a distanza di anni, perché per rendere credibile una richiesta fraudolenta di cambio IBAN basta disporre di riferimenti commerciali e contatti amministrativi reali, che nelle aziende restano invariati a lungo. Rivenduti a pacchetti, riorganizzati e incrociati con i dati provenienti da altre intrusioni, i file rubati continuano a generare rischi di truffa molto tempo dopo che l'azienda ha ripristinato i propri server.

Accanto agli archivi aziendali completi, sugli stessi forum si vendono a prezzi ancora più bassi gli *stealer log*: pacchetti di dati raccolti dai malware *infostealer*, programmi che infettano un singolo computer e rastrellano in automatico tutte le password salvate nel browser, i cookie e i token di sessione attiva. Una singola credenziale estratta da uno di questi archivi viene scambiata per pochi centesimi, perché il guadagno dei venditori si regge sui grandi volumi. Tuttavia, una password aziendale catturata nel 2023 e mai modificata o riutilizzata su più servizi resta una porta aperta: prima o poi un broker la individua, verifica che consente ancora l'accesso alla rete dell'impresa e la trasforma in un'inserzione da centinaia di dollari, senza che l'attesa gli sia costata nulla.

Una filiera industriale guidata dal margine

Chi c'è dunque, concretamente, dietro la tastiera? Non figure isolate o personaggi da romanzo, ma ruoli operativi rigidamente separati. Gli sviluppatori scrivono il codice di crittografia senza mai entrare nella rete di un'azienda; gli affiliati eseguono le intrusioni senza dover scrivere una riga di software; gli addetti alle chat conducono le trattative senza occuparsi della parte tecnica; i riciclatori movimentano e convertono le criptovalute; i broker, come abbiamo visto, si limitano a trovare e vendere la prima credenziale d'ingresso e vengono pagati prima di tutti gli altri. I gruppi RaaS reclutano gli affiliati direttamente sui forum del dark web, aprendo discussioni pubbliche in cui pubblicizzano condizioni contrattuali, percentuali trattenute e servizi di supporto.[2] Quei forum funzionano come vere piattaforme di commercio elettronico, dotate di servizi di *escrow*, procedure di risoluzione delle dispute e punteggi di reputazione: un broker che vende credenziali non funzionanti compromette l'affidabilità del proprio account, che per la sua attività vale molto più di una singola vendita.[1]

Conoscere questa struttura non serve a soddisfare una curiosità, ma a prevedere con precisione il comportamento degli attaccanti. Un'attività organizzata su base industriale ottimizza il rendimento rispetto allo sforzo richiesto: standardizza le operazioni ripetitive, assegna un prezzo a ogni risorsa e abbandona i bersagli che richiedono troppo lavoro rispetto al possibile incasso. Un hacker solitario può ostinarsi su un obiettivo perché lo considera una sfida tecnica; una filiera che lavora a margine attacca ciò che rende e passa oltre non appena incontra un'azienda che fa salire i costi e i tempi dell'intrusione. Chi siede dall'altra parte della chat non segue impulsi imprevedibili: applica una procedura commerciale basata su costi, tempi e listini.

Perché un'azienda ordinaria finisce in catalogo

Se riportiamo il profilo della ACME dentro questi cataloghi, l'annuncio con cui si è aperto il capitolo descrive esattamente la sua situazione alla vigilia dell'incidente: settore manifatturiero, Europa occidentale, fascia di fatturato tra i 10 e i 50 milioni di euro, accesso con diritti di amministratore tramite una porta di collegamento remoto. Sul forum la sua scheda comparirebbe tra quella di un mobilificio trevigiano come la Alf DaFrè e quella di un'officina meccanica bresciana, identica nel formato e proposta a un prezzo accessibile a qualsiasi affiliato.[1,] Nessun elemento della ACME farebbe spiccare quell'annuncio rispetto alle centinaia di inserzioni simili: per gli operatori del mercato non conta l'eccezionalità della vittima, ma la facilità di accesso. Un'azienda produttiva non preparata rappresenta l'investimento più redditizio in bacheca, perché unisce liquidità reale all'interno e poca resistenza all'esterno.

Le statistiche sulle inserzioni dei broker confermano infatti che le aziende colpite si concentrano in larga misura nei Paesi occidentali e che la distribuzione per settore merceologico dipende dalle occasioni trovate aperte più che da una selezione strategica.[1,] La notorietà del marchio non è una voce del modulo di vendita; la fascia di fatturato sì. Per questo motivo la convinzione di essere troppo piccoli o troppo poco conosciuti per interessare agli attaccanti non offre alcuna tutela: l'anonimato dell'impresa non ferma il broker, mentre la fascia delle piccole e medie aziende rappresenta, dal 2024, proprio il segmento di mercato in più rapida espansione.

● 01 · PER IL MANAGER ◆ DECISIONE & BUDGET

Fate un esercizio pratico che richiede un'ora di tempo e nessuna spesa. Scrivete la scheda che un broker compilerebbe oggi sulla vostra azienda usando le voci standard del mercato nero: settore, area geografica, fascia di fatturato, punti di accesso esterni esistenti (la VPN, gli account di amministratore, il collegamento usato dal fornitore che gestisce l'ERP) e quali archivi avrebbero un valore commerciale se venissero copiati. Questo esercizio produce due risultati immediati: vi abitua a valutare la sicurezza con gli stessi criteri economici di chi attacca e vi consegna l'elenco preciso delle esposizioni che i capitoli operativi della Parte 3 vi aiuteranno a chiudere una per una.

Rendere l'attacco antieconomico

Se ogni elemento necessario per preparare un attacco viene comprato su un mercato, ciascuno di questi elementi ha un costo di acquisizione, e quel costo può essere alzato. Tutta la strategia di difesa illustrata in questo libro parte da questo principio economico. Un broker ha convenienza a confezionare e pubblicare un'inserzione solo finché può procurarsi l'accesso rapidamente e a basso costo; difendersi significa quindi rendere troppo costoso acquisire le credenziali e i punti d'ingresso nella vostra rete.

Ogni capitolo della Parte 3 interviene su un passaggio preciso di questa filiera:

- **Svalutare le credenziali rubate (capitolo 11):** introdurre un gestore di password e l'autenticazione a più fattori (MFA, il secondo controllo richiesto al momento dell'accesso) blocca l'attaccante anche quando un dipendente consegna la propria password a una pagina di phishing, rendendo la credenziale rubata inutilizzabile da sola.
- **Chiudere i canali di phishing (capitolo 12):** configurare correttamente le protezioni della posta elettronica riduce alla radice il numero di messaggi fraudolenti che raggiungono le caselle aziendali.
- **Eliminare le falle esposte (capitolo 13):** stabilire una cadenza regolare per gli aggiornamenti di sicurezza (*patch*) chiude le vulnerabilità sui sistemi esposti prima che un broker possa individuarle e metterle in vendita.
- **Neutralizzare l'impatto finale (capitoli 14, 17 e 18):** predisporre backup immutabili che la crittografia non può alterare, imporre per contratto tempi certi di risposta ai fornitori informatici e preparare il piano per la prima ora d'emergenza toglie agli estorsori la leva con cui bloccano l'azienda.

Tradotto nei conti del broker, un'impresa il cui accesso iniziale costa più tempo e denaro di quanto frutterebbe la sua vendita sul forum non finisce in catalogo: non per riguardo, ma per mancanza di margine.

Dietro gli attacchi che fermano le PMI non c'è quindi alcun genio informatico contro cui sarebbe vano difendersi. Nel primo capitolo abbiamo riassunto il crimine informatico come un processo industriale dotato di un proprio listino prezzi; ora ne abbiamo visto ogni componente: broker di accesso iniziale, piattaforme RaaS in franchising, affiliati, negoziatori, riciclatori e rivenditori di dati, ciascuno remunerato dal passaggio successivo. È una filiera commerciale, e qualsiasi filiera commerciale si inceppa quando acquisire la materia prima smette di essere conveniente.

02 · PER IL REFERENTE TECNICO ◆ ESECUZIONE & VERIFICA

Usate la scheda del broker come lista di controllo per verificare le esposizioni dell'azienda. Primo: elencate tutti i punti di accesso remoto raggiungibili da internet (VPN, desktop remoto, pannelli di amministrazione di server e apparati) e indicate quali sono già protetti da autenticazione a più fattori (MFA). Secondo: contate gli account con privilegi di amministratore e segnalate ogni credenziale condivisa o password riutilizzata su più servizi. Terzo: verificate lo stato degli aggiornamenti di sicurezza sul server più datato e sul firewall perimetrale. Verifica: esaminate i tre elenchi insieme a chi coordina l'IT o al fornitore esterno e stabilite quali esposizioni possono essere chiuse entro questo mese. Se nessun punto d'ingresso viene messo in sicurezza, l'azienda presenta già tutte le condizioni cercate dai broker, e il capitolo 11 indica da dove cominciare per intervenire.

SCHEDA RIASSUNTIVA DI FINE CAPITOLO

RBB/LAB · RUNBOOK

01 · DECISIONI E BUDGET · PER IL MANAGER

- La decisione: valutare l'azienda con gli stessi criteri usati dagli intermediari del crimine informatico. Dedicare un'ora a compilare la scheda che un broker scriverebbe sulla vostra impresa (settore, fascia di fatturato, accessi remoti esposti, archivi rivendibili) e usarla per stabilire l'ordine di priorità degli investimenti in sicurezza.
- Cosa protegge: l'efficacia del budget. Poiché gli attacchi funzionano come una filiera commerciale, le risorse vanno concentrate sulle misure che chiudono i punti d'ingresso cercati dai broker, a partire da gestione degli accessi, protezione della posta elettronica e aggiornamenti di sicurezza.
- Budget e tempi realistici: un'ora di lavoro con il referente IT e con chi gestisce il portafoglio ordini, senza alcun acquisto immediato; gli interventi operativi iniziano nei capitoli dall'11 al 14.

02 · CHECKLIST OPERATIVA · PER IL REFERENTE TECNICO

☐ Censire ogni punto di accesso remoto esposto (VPN, desktop remoto, pannelli di amministrazione) e verificare quali dispongono dell'autenticazione a più fattori (MFA).

☐ Contare gli account con diritti di amministratore, segnalare le password condivise o riutilizzate su più servizi e annotare lo stato degli aggiornamenti di sicurezza del firewall e del server più vecchio.

☐ Verifica: abbozzare la potenziale inserzione dell'azienda partendo dai dati raccolti. Se i campi relativi ai punti di accesso e ai privilegi amministrativi si compilano con troppa facilità, la loro messa in sicurezza diventa la prima priorità operativa, affrontata nel capitolo 11.

DAL PROBLEMA AL PIANO D'AZIONE · CAPITOLI 4–27

Come si chiudono le cinque porte viste nella Parte I

Nei primi tre capitoli hai visto perché una PMI manifatturiera come la **ACME S.r.l.** finisce nel mirino, come si svolge minuto per minuto la giornata di un attacco ransomware e quanto poco costa ai gruppi criminali comprare l'accesso iniziale alla rete aziendale. Nell'edizione integrale del libro (300 pagine), le tre parti centrali guidano il manager e il referente tecnico a costruire tutte le difese necessarie:

- **Parte II · La normativa, senza panico (Capitoli 4–9):** il test in 10 domande per sapere se rientrate nella NIS2 (d.lgs. 138/2024); come rispondere in una mattinata ai questionari Excel da 60 domande dei grandi clienti e negoziare gli allegati contrattuali; la procedura GDPR per le 72 ore; l'AI Act visto da chi compra software; l'organigramma della sicurezza con le 5 policy di una pagina e la riunione trimestrale di un'ora.
- **Parte III · La difesa pratica (Capitoli 10–19):** l'autovalutazione di 5 giorni senza acquisti; gestore di password e MFA; configurazione SPF/DKIM/DMARC e regole antifrode IBAN; EDR e crittografia dei portatili; backup immutabili 3-2-1-1-0 e test di ripristino; segmentazione della rete in 4 zone; formazione anti-phishing e test all'help desk; le 5 clausole per i fornitori IT/ERP; il piano di risposta agli incidenti di una sola pagina; come leggere e negoziare la polizza cyber.
- **Parte IV · L'intelligenza artificiale in azienda (Capitoli 20–27):** il sondaggio anonimo per far emergere la Shadow AI; la policy del semaforo dei dati (Verde/Giallo/Rosso); la scelta delle licenze aziendali; i flussi LLM per reparto; la difesa da prompt injection indiretta e deepfake; quando e come installare un modello LLM locale in azienda per i dati riservati; il prospetto unico di conformità GDPR + AI Act.

*Per permetterti di vedere subito il quadro d'insieme dell'intero percorso, nelle pagine seguenti trovi **integralmente anche il Capitolo 28 conclusivo**, che condensa tutti gli interventi del libro nella **Roadmap operativa di 12 mesi (4×90)**.*

05 · PARTE V

RBB/LAB

Il piano

La roadmap operativa di dodici mesi divisa in quattro trimestri per portare l'azienda da esposta a difendibile e dimostrabile.

CAPITOLI DI QUESTA PARTE

- **Capitolo 28:** La roadmap di dodici mesi

CAPITOLO 28

La roadmap di dodici mesi

> *L'intero percorso del libro condensato in un piano operativo di una pagina e in un calendario di quattro trimestri: dalla messa in sicurezza di accessi e backup fino al fascicolo delle evidenze pronto per clienti, assicuratori e autorità, con un indicatore misurabile aggiunto a ogni trimestre e tre opzioni di budget realistiche. L'obiettivo non è un bollino di conformità formale, ma portare l'azienda da una condizione esposta a una condizione difendibile e dimostrabile, partendo da una prima convocazione in agenda per lunedì prossimo.*

Numeri e calendario

Per un'azienda delle dimensioni di ACME S.r.l. un giorno di fermo costa circa 72.000 euro di produzione bloccata, e il danno medio di un attacco informatico a una PMI italiana supera quella cifra prima ancora di considerare un eventuale riscatto. I capitoli precedenti hanno spiegato dove si aprono i punti di vulnerabilità, come operano gli attaccanti e quali requisiti impongono le normative, i clienti strutturati e le compagnie assicurative. Questo capitolo conclusivo traduce quelle analisi in un calcolo economico e in un calendario operativo.

L'orizzonte di lavoro è di dodici mesi, divisi in quattro trimestri. Un'azienda che all'inizio del percorso si trova esposta arriva a fine anno in una condizione difendibile e dimostrabile: protetta da presidi tecnici ben definiti e in grado di esibire a qualsiasi verificatore esterno la prova documentata che quei controlli sono attivi. L'obiettivo non è dichiararsi semplicemente «conformi», un termine spesso abusato che dà l'illusione di un adempimento definitivo. I criteri visti nel capitolo 4 stabiliscono gli obblighi normativi in base a due soli parametri, il settore di attività e la dimensione dell'impresa, per determinare se l'azienda rientra o meno nel perimetro del decreto NIS2. Nessuna normativa rilascia però un *bollino* che certifichi una volta per tutte la fine dei lavori. Nella sicurezza informatica un simile attestato non esiste, e chi lo promette vende solo carta. Ciò che conta sono le evidenze verificabili, raccolte in un fascicolo operativo e aggiornate nel tempo.

Un orizzonte di dodici mesi è la misura realistica per completare la transizione senza paralizzare l'attività ordinaria. Il primo trimestre non può contenere il progetto di segmentazione della rete, così come il quarto trimestre è il momento peggiore per accorgersi

che le copie di backup non si ripristinano. La sequenza degli interventi non è arbitraria: ricalca l'ordine della lista delle prime 10 priorità definita il venerdì della settimana di autovalutazione del capitolo 10, che le Parti 3 e 4 hanno sviluppato punto per punto. Anche lo strumento per governare l'avanzamento dei lavori è già pronto: la riunione trimestrale di un'ora introdotta nel capitolo 9, in cui quattro indicatori operativi vengono verificati insieme al titolare e messi a verbale con la sua firma. Questa roadmap non aggiunge nuove procedure: scandisce trimestre per trimestre gli interventi che vanno a popolare gli indicatori di quella riunione. L'intero programma entra in una sola pagina: quattro righe per i trimestri e tre colonne per indicare gli interventi previsti, l'indicatore di verifica e il responsabile incaricato. Un piano operativo per una PMI che richieda più di una pagina rischia di restare lettera morta.

Dal giorno 1 al giorno 90: accessi e copie di backup

Il primo trimestre unisce il programma di trenta giorni sulle identità del capitolo 11 e quello sui backup del capitolo 14, eseguiti in sequenza. Si parte con i quattro venerdì del primo mese: il gestore di password aziendale introdotto con due sessioni pratiche di mezz'ora; l'autenticazione a più fattori (MFA) attivata su ogni account esposto verso l'esterno o accessibile da remoto; gli account di amministratore separati da quelli utilizzati ogni giorno per leggere la posta; i sistemi di backup isolati su credenziali dedicate che nessun account di dominio può aprire. Seguono il pomeriggio dedicato alla revisione dei permessi secondo il principio del privilegio minimo, l'adozione della lista di controllo per revocare gli accessi ai dipendenti in uscita e la formalizzazione della regola 3-2-1-1-0 per i backup: tre copie dei dati, su due supporti differenti, di cui una conservata fuori sede, una immutabile che nessuna credenziale aziendale può modificare o cancellare e zero errori nelle verifiche di integrità. Il trimestre si chiude con il passaggio che la maggior parte delle imprese trascura: il primo test di ripristino cronometrato su una macchina isolata, con il recupero effettivo di un file o di un sistema reale e la verbalizzazione del risultato.

La spesa viva parte da poche centinaia di euro: i canoni del gestore di password per un'azienda di ottanta dipendenti si attestano su poche migliaia di euro all'anno, una frazione trascurabile rispetto al costo anche di una sola ora di fermo produttivo, mentre per una realtà di venti persone bastano poche centinaia di euro. Tutto il resto del lavoro nel primo trimestre richiede solo configurazioni, firme e pomeriggi già pianificati. Nessuna attività di questi primi novanta giorni richiede consulenti esterni, procedure d'acquisto complesse o nuovi server. Il programma del capitolo 11, che rappresenta l'intervento con il miglior rapporto tra sforzo richiesto e riduzione del rischio dell'intero libro, mantiene questo primato per tutto l'anno: è il modo più rapido ed economico per chiudere le porte d'ingresso più sfruttate dagli attaccanti.

Al novantesimo giorno sono pronti i primi due indicatori per il prospetto trimestrale del capitolo 9: la percentuale di account protetti da autenticazione a più fattori e la data dell'ultimo test di ripristino, con l'indicazione dei dati effettivamente recuperati. Quando queste due voci riportano valori verificati, l'azienda si colloca già sopra la media delle PMI italiane: una password sottratta non basta più per entrare nei sistemi e il blocco di un server richiede un pomeriggio di ripristino anziché trasformarsi in una crisi aziendale. Nella maggior parte delle imprese concorrenti nessuno dei due indicatori è mai stato misurato.

01 · PER IL MANAGER ◆ DECISIONE & BUDGET

La decisione riguarda il calendario prima ancora del budget. Approvate la scansione dei quattro trimestri, assegnate tre nomi al piano (chi esegue gli interventi, chi firma i documenti, chi presenta gli indicatori durante la riunione trimestrale) e scegliete l'opzione di spesa in base alle reali disponibilità dell'azienda, non ai cataloghi dei fornitori: si va da poche centinaia di euro affiancate dal lavoro interno fino alle licenze per utente, un secondo router e l'accordo di *retainer* per la risposta agli incidenti (DFIR). Cosa protegge, sul piano industriale: la continuità produttiva da 72.000 euro al giorno, i pagamenti aziendali esposti alle frodi via email e i contratti con i grandi clienti che hanno già iniziato a inviare i questionari di qualifica. Quanto tempo richiede alla direzione: un'ora di riunione a trimestre, quattro volte all'anno, più l'approvazione dei pomeriggi operativi distribuiti nel piano.

02 · PER IL REFERENTE TECNICO ◆ ESECUZIONE & VERIFICA

Redigete il piano di una pagina in un'ora. Impostate quattro righe per i trimestri riportando le attività nell'ordine descritto in questo capitolo, con un indicatore di verifica e un responsabile nominativo per ciascuna riga. Stampatene due copie: una da conservare nel cassetto insieme al piano di risposta agli incidenti, l'altra da tenere nella sala riunioni in cui si svolge il riesame trimestrale. Verifica: assicuratevi che il punteggio iniziale del questionario di trenta domande del capitolo 10 sia registrato prima di avviare gli interventi e che la convocazione per il primo lunedì sia già stata inviata.

Dal giorno 91 al giorno 180: posta elettronica, dispositivi e strumenti di IA

Il secondo trimestre mette in sicurezza due canali critici: la posta elettronica e le postazioni di lavoro. Si comincia dalla posta. I tre record di autenticazione del capitolo 12 (SPF, DKIM e DMARC) vengono pubblicati inizialmente in modalità di monitoraggio e portati gradualmente alla politica di blocco (*reject*) dopo alcune settimane di analisi

dei report: attivare il blocco totale fin dal primo giorno senza verificare i flussi rischia infatti di fermare anche le fatture e le comunicazioni legittime inviate dall'azienda. Si attivano e si configurano correttamente i filtri anti-phishing già inclusi nel canone della piattaforma di posta. Si firmano poi le due regole amministrative sui pagamenti: qualsiasi modifica delle coordinate bancarie va confermata telefonicamente chiamando il numero già presente in anagrafica, i bonifici sopra una soglia prefissata richiedono una doppia autorizzazione e su fatture e comunicazioni a clienti e fornitori viene inserita l'avvertenza fissa: *non comunichiamo mai variazioni di IBAN tramite email.* Si passa quindi alle macchine seguendo il capitolo 13: installazione del software EDR su tutti i server e i computer censiti nell'inventario; calendario degli aggiornamenti (patch) a partire dai due server più datati; assegnazione di un responsabile e di una scadenza di verifica a ogni riga dell'inventario; attivazione della crittografia del disco sui portatili con salvataggio delle chiavi di recupero nel gestore di password aziendale; regolamentazione dell'uso degli smartphone personali per l'accesso alla posta di lavoro.

In questo stesso trimestre trova posto un intervento che potrebbe sembrare prematuro e che invece è urgente: il sondaggio interno anonimo sugli strumenti di intelligenza artificiale effettivamente usati dai dipendenti e la policy di una pagina con la scheda a semaforo dei dati, descritti nei capitoli 20 e 21. L'inserimento nel secondo trimestre è intenzionale: l'uso non autorizzato di strumenti di IA (*shadow AI*) non aspetta che l'azienda completi il resto del piano, e ogni settimana priva di regole chiare è una settimana in cui i dati riservati dei clienti rischiano di essere caricati su piattaforme esterne governate dalle condizioni contrattuali di terzi. La policy occupa una singola facciata A4, la sessione di formazione per il personale richiede mezza giornata e nessuna delle due attività comporta costi vivi.

Al giorno 180 si aggiunge il terzo indicatore del prospetto trimestrale: la percentuale di patch installate entro la finestra temporale prestabilita, un dato che si ricava direttamente dall'inventario senza lavoro aggiuntivo. Il record DMARC è ora impostato in modalità di blocco e verificabile dall'esterno con qualsiasi strumento gratuito, poiché si tratta di un parametro pubblico che anche clienti e assicuratori possono controllare in autonomia. La scheda a semaforo sull'uso dell'IA è firmata e illustrata al personale, con il foglio presenze e l'elenco datato degli strumenti autorizzati già archiviati nel fascicolo delle evidenze. Da questo momento entra stabilmente nella routine trimestrale anche la verifica di quindici minuti descritta nel capitolo 12 sulle regole di inoltro automatico della posta: le istruzioni nascoste che copiano i messaggi verso un indirizzo esterno, usate dagli attaccanti per continuare a leggere le comunicazioni aziendali anche dopo aver compromesso una sola casella email.

Dal giorno 181 al giorno 270: rete, persone, fornitori e piano d'emergenza

Il terzo trimestre è il primo che richiede un investimento economico diretto, laddove l'opzione di budget scelta lo preveda. Si parte con la segmentazione della rete del capitolo 15: suddivisione dell'infrastruttura in zone separate, elenco delle regole del firewall scritto in modo chiaro e leggibile, accesso del dispositivo di teleassistenza dei fornitori e della rete wifi per gli ospiti limitato esclusivamente alle risorse necessarie, verificando l'isolamento con prove di connessione dalla rete ospiti verso le macchine di produzione (prove che devono dare esito negativo). Si prosegue con la formazione del personale del capitolo 16: sessioni mirate per mansione anziché corsi generici annuali, pulsante di segnalazione attivo sul programma di posta, regola di non punibilità per chi segnala un errore letta direttamente dal titolare che l'ha firmata, adozione delle tre liste di controllo per la gestione del personale e avvio della prima simulazione di phishing, valutata in base alla rapidità con cui i dipendenti segnalano l'email sospetta e non contando solo chi ha cliccato sul link. Sul fronte della filiera, si applicano le verifiche del capitolo 17: invio delle cinque domande di controllo a ogni fornitore informatico critico, archiviazione delle risposte e inserimento delle clausole di sicurezza al momento del rinnovo contrattuale, sfruttando la simmetria della catena di fornitura, poiché le garanzie che la ACME S.r.l. richiede al proprio partner ERP coincidono con quelle che i suoi tre principali clienti richiedono alla ACME. Si redige infine il piano di risposta agli incidenti del capitolo 18: una pagina divisa in sei sezioni con i nomi dei responsabili, stampata su carta e collaudata con la prima simulazione a tavolino di due ore sullo scenario del martedì d'attacco, correggendo entro la settimana stessa ogni punto che si riveli carente.

Al giorno 270 il terzo trimestre consegna tre evidenze concrete. La prima è l'esito positivo dei test di isolamento tra i segmenti di rete. La seconda costituisce il quarto indicatore del prospetto trimestrale: la percentuale di segnalazione e il tempo medio di reazione registrati nella simulazione di phishing, mentre la percentuale di clic resta nel pannello tecnico di Marta come dato diagnostico per orientare la formazione e mai come metro di giudizio individuale. La terza è il verbale datato della simulazione a tavolino, archiviato nel fascicolo delle evidenze: l'esercitazione serve infatti a verificare la tenuta pratica del foglio, facendo emergere il numero di emergenza cambiato dopo l'acquisizione di un fornitore, il sostituto in ferie negli stessi giorni del titolare o i tempi di notifica che non coincidono con quelli firmati nell'allegato contrattuale del cliente. Individuate attorno a un tavolo di riunione, queste incongruenze si correggono in pochi minuti; scoperte la mattina di un attacco, riproducono esattamente il blocco operativo visto nel capitolo 2.

Dal giorno 271 al giorno 365: le verifiche esterne e il bilancio dell'anno

Nel quarto trimestre il lavoro svolto viene messo a disposizione dei valutatori esterni e verificato internamente. Per la polizza cyber del capitolo 19, il questionario di assunzione viene compilato in un'unica sessione attingendo direttamente al fascicolo delle evidenze, in modo che ogni risposta trovi riscontro in un documento datato: dichiarare misure solo pianificate significa infatti firmare un contratto che la compagnia potrà contestare al momento del sinistro. Si ripete poi il questionario di autovalutazione del capitolo 10: le stesse trenta domande, calcolando il punteggio con lo stesso criterio basato sul conteggio delle risposte negative e affiancando il nuovo risultato al punteggio iniziale registrato dodici mesi prima. Una singola rilevazione fotografa solo il punto di partenza; è il confronto tra due misurazioni omogenee a distanza di un anno a dimostrare i progressi compiuti. Il fascicolo di qualifica del capitolo 5 arriva alla prima revisione annuale: nell'arco di un mese ogni documento viene riletto, aggiornato e ridatato. Per le aziende che rientrano nel perimetro del decreto NIS2 visto nel capitolo 4 si apre inoltre la finestra annuale sulla piattaforma dell'ACN: la registrazione o l'aggiornamento dei dati tra il 1° gennaio e il 28 febbraio, da fissare in agenda con un responsabile nominativo fin dal giorno in cui si approva il piano. A questo punto l'adempimento sul portale è una formalità amministrativa, perché l'elenco delle misure tecniche e organizzative richieste dal decreto corrisponde al percorso già attuato durante l'anno. Infine, la lista di controllo del capitolo 27 completa il registro degli utilizzi dell'IA, spuntando e datando i cinque requisiti previsti per ciascuna voce e programmando il riesame semestrale all'interno di due delle quattro riunioni trimestrali dell'anno successivo.

Concluso il primo ciclo di dodici mesi, il calendario diventa una routine operativa ricorrente: un test di ripristino dei backup a trimestre; una simulazione di phishing a trimestre; una simulazione a tavolino sul piano di risposta agli incidenti una volta all'anno; quattro riunioni trimestrali di direzione con l'analisi dei quattro indicatori; un mese all'anno dedicato all'aggiornamento del fascicolo delle evidenze; la ripetizione annuale del questionario di trenta domande confrontata con il punteggio dell'anno precedente; l'aggiornamento tra gennaio e febbraio sul portale ACN per le imprese soggette alla NIS2. La sicurezza informatica non ha un traguardo definitivo perché le minacce e i sistemi aziendali continuano a cambiare: un'azienda che considera il giorno 365 come un punto d'arrivo definitivo inizia gradualmente a perdere terreno, lasciando invecchiare procedure e controlli un documento non aggiornato alla volta.

Tre opzioni di budget per lo stesso piano

Lo stesso piano di una pagina può essere attuato con tre diversi livelli di budget; ciò che conta è scegliere fin dall'inizio con realismo la variante sostenibile per l'azienda.

La variante a budget zero investe il tempo interno prima del denaro e si concentra sul blocco fondamentale costituito da identità e backup, che raccoglie gli interventi a costo quasi nullo. I canoni del gestore di password rappresentano l'unico esborso diretto di questa opzione, pari a poche centinaia di euro all'anno per una piccola impresa. L'autenticazione a più fattori è già inclusa senza costi aggiuntivi nel piano di posta elettronica aziendale e attende solo di essere attivata. Il record DMARC richiede l'inserimento di poche righe di testo nella configurazione DNS del dominio che l'azienda già possiede. Le cinque policy richiedono poche ore di redazione ciascuna, la formazione si svolge in sessioni interne di mezz'ora, il test di ripristino richiede solo un cronometro e una macchina isolata, mentre una simulazione di phishing può essere preparata internamente da un collega utilizzando un messaggio verosimile. Occorre però avere ben chiaro cosa viene rinviato scegliendo il budget zero: il software EDR (poiché soluzioni open-source affidabili su questa scala sono rare e cercare scorciatoie fa solo perdere tempo), gli apparati dedicati per la segmentazione della rete, l'accordo di *retainer* con una società di DFIR e la possibilità di negoziare riduzioni sul premio assicurativo grazie a un presidio tecnico completo. Il budget zero è un punto di partenza valido, non una soluzione definitiva: mantiene invariato l'ordine di priorità del piano e ne rallenta soltanto la velocità di esecuzione. La scansione triennale delineata nel capitolo 19 resta valida per ogni variante: il primo anno è dedicato alla chiusura dei varchi principali a basso costo, il secondo agli investimenti infrastrutturali e il terzo alle eventuali certificazioni richieste e ripagate da un cliente strutturato o da un bando di gara. Un'azienda che quest'anno parte a budget zero non è fuori strada: percorre lo stesso itinerario con un anno solare di scarto, mettendo comunque in sicurezza fin da subito gli accessi più critici.

La variante a budget minimo rappresenta lo scenario di riferimento adottato in questo libro e il percorso seguito dalla ACME S.r.l.: licenze per utente per il gestore di password e per il software EDR sulle postazioni, un secondo router di fascia economica per isolare la rete ospiti e i dispositivi connessi non gestiti, e l'accordo di *retainer* con una società di DFIR che in caso di attacco consente di attivare gli specialisti con una telefonata anziché dover negoziare un contratto d'urgenza. Anche in questo scenario non servono progetti complessi o consulenze continuative: basta approvare un acquisto mirato a trimestre e rispettare le scadenze fissate a calendario.

La variante basata sui fornitori esterni delega l'esecuzione tecnica, ma mai la titolarità delle decisioni. All'esterno si possono affidare il monitoraggio continuo, l'installazione delle patch e la gestione tecnica della piattaforma di posta: le cinque domande del capitolo 17 diventano in questo caso i livelli di servizio contrattuali (SLA), definendo chi installa gli aggiornamenti, entro quali tempi, con quale preavviso e con quali report di verifica. Ciò che non può mai essere delegato all'esterno sono invece le responsabilità di direzione: la firma delle policy, poiché il decreto NIS2 esaminato nel capitolo 4 attribuisce gli obblighi di governance direttamente agli organi di amministrazione; i verbali delle riunioni trime-

strali e della simulazione annuale a tavolino; la verifica degli indicatori operativi. Un fornitore esterno può gestire gli strumenti tecnici, ma spetta sempre all'azienda verificare che quei controlli stiano effettivamente funzionando.

Il fascicolo che risponde a ogni verifica

A fine anno il fascicolo delle evidenze impostato nel capitolo 5 ha raggiunto la sua forma completa. Raccoglie in modo ordinato tutti i documenti prodotti nei quattro trimestri, senza lasciare spazio all'improvvisazione: le cinque policy firmate e datate; i registri dei test di ripristino, con una riga per ogni prova e l'indicazione dei file recuperati; i prospetti trimestrali con la percentuale di patch installate nei tempi previsti; i report delle simulazioni di phishing con percentuale e tempi di segnalazione; i verbali delle simulazioni a tavolino; le risposte dei fornitori critici e le relative clausole contrattuali; la policy sull'uso dell'IA insieme al registro dei trattamenti aggiornato; il piano di risposta agli incidenti stampato con i recapiti di emergenza; i punteggi del questionario di autovalutazione di trenta domande, con il risultato iniziale e quello di fine anno affiancati. Ogni documento riporta un numero di versione e una data certa, perché in sede di verifica una dichiarazione priva di data resta un'opinione, mentre una pagina datata e firmata costituisce un'evidenza.

Questo unico fascicolo permette di rispondere con la stessa base documentale a quattro interlocutori diversi, ciascuno con le proprie scadenze. Il primo è il cliente strutturato del capitolo 5: il questionario di qualifica fornitori, che in precedenza richiedeva una settimana di rincorse tra gli uffici, si evade ora inviando un'email con gli allegati già pronti. Il secondo è la compagnia assicurativa del capitolo 19, il cui questionario di assunzione trova per ogni risposta un documento interno di riscontro. Il terzo è l'ente di certificazione, nel momento in cui diventa conveniente affrontarne i costi: come visto nel capitolo 8, una certificazione formale si acquisisce quando è richiesta e ripagata da un cliente o da un bando di gara, e fino a quel giorno è lo stesso fascicolo delle evidenze a dimostrare l'affidabilità dell'azienda durante gli audit. Il quarto è l'autorità di controllo: la registrazione e le scadenze NIS2 del capitolo 4, così come i registri GDPR del capitolo 6, attingono tutti alle stesse pagine. La stessa raccolta di documenti risponde sia alle qualifiche commerciali della filiera sia agli obblighi di legge. Inoltre il vantaggio operativo cresce nel tempo: compilare il secondo questionario di un cliente richiede una mattinata, il terzo una semplice email, e la proposta di rinnovo della polizza a marzo arriva quando gli indicatori sono già aggiornati. L'impianto documentale si costruisce una volta sola e continua a ripagare lo sforzo iniziale a ogni verifica successiva.

Il primo lunedì

Il programma inizia di lunedì, e la prima azione non è un acquisto, un'analisi tecnica o la stesura di una policy: è una convocazione in agenda. La settimana di autovalutazione del capitolo 10 (cinque sessioni mattutine, due persone coinvolte, nessun acquisto consentito fino a venerdì) parte lunedì prossimo; l'invito va inviato oggi, indicando i due nominativi e bloccando gli orari sul calendario prima che le urgenze quotidiane offrano un pretesto per rimandare. Tutto ciò che abbiamo descritto in questo capitolo, dai quattro trimestri agli indicatori, dalle opzioni di budget fino al fascicolo delle evidenze, dipende da quel primo appuntamento fissato in agenda. Tra dodici mesi l'azienda disporrà di un sistema di controlli documentato e pronto a rispondere alle verifiche esterne, oppure si ritroverà semplicemente con un anno in più alle spalle e la stessa esposizione di oggi: a fare la differenza è una riunione convocata per tempo. Nella maggior parte degli attacchi alle PMI nessuno sceglie la vittima per il nome che porta sull'insegna: le scansioni automatiche cercano varchi aperti e gli estorsori colpiscono dove entrare costa meno fatica. Dodici mesi di lavoro su questa roadmap non cambiano l'economia del crimine informatico, ma cambiano ciò che un attaccante o un verificatore esterno trovano quando esaminano la vostra azienda: accessi protetti, backup isolati e collaudati, indicatori misurati e documenti firmati con una data certa. Siete partiti da una condizione esposta; chiudete questo percorso con un'azienda difendibile e dimostrabile. Il piano occupa una sola pagina. Stampatela.

SCHEDA RIASSUNTIVA DI FINE CAPITOLO RBB/LAB · RUNBOOK

01 · DECISIONI E BUDGET · PER IL MANAGER

- La decisione: approvare il calendario dei quattro trimestri assegnando i responsabili a ciascuna voce e scegliere l'opzione di budget; il piano occupa una sola pagina e parte con una convocazione in agenda, non con una fattura.
- Cosa protegge: la continuità operativa da 72.000 euro al giorno, i pagamenti aziendali esposti alle frodi via email e la capacità di rispondere con prove documentate ai questionari di qualifica dei clienti, ai rinnovi assicurativi e alle verifiche delle autorità.
- Budget e tempi realistici: poche centinaia di euro più il lavoro interno nella variante a budget zero; licenze per utente (gestore di password ed EDR), un secondo router e l'accordo di *retainer* DFIR nello scenario di riferimento del libro; in entrambi i casi, dodici mesi di percorso e un'ora di riunione a trimestre.

02 · CHECKLIST OPERATIVA · PER IL REFERENTE TECNICO

☐ Predisporre e stampare il piano operativo di una pagina: quattro righe per i trimestri, le attività nell'ordine stabilito dal capitolo, un indicatore di verifica e un responsabile nominativo per ciascuna riga.

☐ Registrare il punteggio iniziale del questionario di trenta domande del capitolo 10 prima di avviare gli interventi del primo trimestre.

☐ Verifica: accertarsi che al giorno 90 siano compilati i primi due indicatori trimestrali (percentuale di copertura MFA e verbale del test di ripristino superato) e che al giorno 365 il questionario di trenta domande venga ricompilato con gli stessi criteri, affiancando il risultato finale al punteggio di partenza.

RBB/LAB

OFFERTA RISERVATA ISCRITTI NEWSLETTER

Passa all'edizione integrale (28 capitoli · 300 pagine)

Hai appena letto la Parte I e la Roadmap conclusiva del Capitolo 28. Per avere tutte le procedure operative, i modelli di policy di una pagina, le checklist dei Capitoli 4–27, le clausole per i fornitori e i protocolli sull'intelligenza artificiale, puoi richiedere l'opera completa con lo sconto riservato agli iscritti alla newsletter:

01 · DIGITALE INTEGRALE

Edizione PDF / eBook

Volume completo di 300 pagine con tutti i 28 capitoli, le 8 figure operative, l'indice interattivo e tutte le schede riassuntive.

◆ **Sconto iscritti nella mail di benvenuto**

02 · LIBRO CARTACEO + PDF

Edizione Stampata 17×24 cm

Il volume fisico da scrivania da condividere con direzione e referente tecnico, con download immediato dell'edizione digitale integrale.

◆ **Disponibile su Amazon e da RBB LAB**

◆ VUOI ACCELERARE L'ESECUZIONE IN AZIENDA CON RBB LAB?

Quando il reparto IT è già assorbito dall'operatività quotidiana o un cliente soggetto a NIS2 chiede evidenze documentate entro 30 giorni, **RBB LAB** affianca la direzione e il referente tecnico con quattro interventi a perimetro e tempi definiti:

- **01 · Sprint Fotografia & Piano 4×90 (5 giorni):** autovalutazione guidata dei sistemi, calcolo del costo di fermo e roadmap annuale.
- **02 · Pacchetto Qualifica Fornitori & NIS2:** costruzione del Fascicolo delle Evidenze, compilazione questionari clienti e revisione clausole.
- **03 · Collaudo Indipendente Backup & Ripristino:** verifica dell'isolamento delle copie e test reale cronometrato su macchina isolata.
- **04 · Governance IA, Art. 4 AI Act & LLM Locali:** censimento Shadow AI, formazione obbligatoria con registro firmato e modelli IA on-premise.

RBB LAB · rbblab.com · enrico.rubbo.li · Usa il link nella mail della newsletter per riscattare lo sconto o prenotare una call.