ANDREA PIRAS

LA SPERANZA NON È UNA STRATEGIA

13

COMANDAMENTI PER LE PMI

PROTEGGERE IL BUSINESS, SENZA OSTACOLARLO

La cybersecurity non è più un lusso riservato alle grandi aziende. Oggi ogni impresa, piccola o grande, è un potenziale bersaglio. **Per una PMI, la sfida è doppia**: proteggere i propri sistemi **senza ostacolare il business, con budget limitati** e spesso un solo referente IT che deve fare da amministratore di sistema, tecnico helpdesk e guardiano della sicurezza.

Questo libro nasce con un obiettivo chiaro: offrire un approccio strutturato, concreto e sostenibile per rafforzare la sicurezza aziendale, anche in contesti con risorse minime. Qui troverai un piano chiaro di **13 settimane** — una per ciascun capitolo — per trasformare gradualmente la sicurezza della tua azienda in una difesa solida.

Ogni settimana lavorerai su un "comandamento" essenziale, con esempi, scenari reali, strumenti a basso costo e checklist operative. In tre mesi avrai costruito una base di sicurezza robusta e consapevole, senza paralizzare le operazioni quotidiane.

Ma il percorso non finisce qui: al termine delle prime 13 settimane, avrai completato il primo ciclo e sarai pronto a ricominciare, questa volta con maggiore consapevolezza e attenzione ai dettagli. Nei cicli successivi, ogni settimana dedicata a un comandamento sarà l'occasione per raffinare ciò che hai già implementato, introdurre nuove migliorie e rispondere alle minacce emergenti. Così, la sicurezza diventerà un processo vivo, in continua evoluzione, parte integrante della cultura aziendale.

Ecco una breve anteprima del percorso:

1. **Autenticazione Multi-fattore** – Come fermare gli accessi non autorizzati anche in caso di furto di password, e perché la MFA è il baluardo più semplice ma potente da adottare.

2. **Deny-by-default** – Impostare sistemi e applicazioni per bloccare tutto ciò che non è esplicitamente autorizzato, riducendo il rischio di software malevoli.

3. **Disattivazione macro** – Chiudere una delle porte d'ingresso preferite dal ransomware e impostare policy sicure in Office e strumenti simili.

4. **Privilegi minimi** – Perché "meno è meglio" quando si parla di permessi utente, e come ridurre l'impatto di un'eventuale compromissione.

5. **Hardening sistemi e network** – Applicare configurazioni di sicurezza di base per ridurre la superficie di attacco, senza dover acquistare hardware costoso.

6. **Monitoraggio file e uso USB** – Rilevare comportamenti anomali e prevenire esfiltrazioni di dati, anche con strumenti gratuiti o integrati.

7. **Patch regolari + MDR** – Automatizzare aggiornamenti e valutare un servizio Managed Detection & Response per monitoraggio continuo.
8. **Gestione Superficie di Attacco** – Identificare e mettere in sicurezza asset dimenticati o esposti in rete prima che lo facciano i criminali.
9. **Zero-Trust** – Dare accesso solo quando serve e solo a chi serve, riducendo al minimo i rischi di movimento laterale.
10. **Formazione personale** – Rendere i dipendenti un punto di forza e non un punto debole nella sicurezza aziendale.
11. **Backup cifrati** – Prepararsi al peggio assicurandosi di poter ripristinare i dati in modo sicuro e rapido.
12. **Segmentazione e cloud-first** – Separare reti e funzioni, sfruttando il cloud per semplificare e proteggere.
13. **Monitoraggio delle minacce** – Tenere un "orecchio teso" su nuove vulnerabilità e attacchi, con strumenti e fonti open source.

Questo non è un manuale da leggere e dimenticare: è un **piano di azione**. Se seguirai le settimane con costanza, alla fine del percorso avrai un'infrastruttura più sicura, un team più consapevole e processi più solidi, pronti a difendere la tua azienda dalle minacce di oggi e di domani.

BIOGRAFIA

Con una carriera di oltre 20 anni nell'IT e nella cybersecurity, Andrea Piras è un affermato leader nella sicurezza delle informazioni, noto per la combinazione di competenze tecniche e visione strategica. Iniziando alla fine del 2005 come collaudatore software, ha costruito solide basi nella qualità del software, un'esperienza che gli ha trasmesso un'attenzione meticolosa ai dettagli e la comprensione di come i sistemi possano fallire. Questa fase iniziale, focalizzata sui test, gli ha fornito una chiara consapevolezza dell'importanza di controlli rigorosi.

Sfruttando una formazione in informatica e una curiosità innata, nel periodo 2008-2013 ha lavorato sul progetto VEGA, vettore aerospaziale italiano. In questo ruolo ha maturato esperienza nella progettazione e nell'affidabilità dei sistemi, imparando ad applicare i principi di sicurezza alla protezione di asset critici. Questo periodo è stato fondamentale per sviluppare un approccio "system thinking" alla sicurezza: considerare gli ambienti IT aziendali come ecosistemi complessi e interdipendenti, che richiedono strategie di protezione olistiche.

Nel periodo 2013-2015 ha operato in contesti complessi come **System Administrator** per importanti aziende impegnate nella gestione del servizio idrico e del trasporto pubblico. In questo ruolo ha curato l'amministrazione e l'ottimizzazione di infrastrutture IT critiche, garantendo la continuità operativa di sistemi a supporto di servizi essenziali per la collettività. Le attività hanno incluso la gestione di server fisici e virtuali, reti aziendali e sistemi di sicurezza, l'implementazione di politiche di backup e disaster recovery, nonché il monitoraggio proattivo delle performance per prevenire interruzioni.

Nel 2018 è entrato in un ruolo dedicato all'analisi della sicurezza. Come analista e successivamente architetto della sicurezza delle informazioni, è stato responsabile della valutazione di minacce e vulnerabilità, della progettazione di soluzioni di sicurezza e dello sviluppo di architetture per proteggere le reti aziendali. Ha contribuito a progetti su larga scala riguardanti difesa di rete, gestione di identità e accessi e sviluppo sicuro del software, spesso fungendo da ponte tra i team tecnici e il management. Nel tempo, la sua capacità di tradurre questioni tecniche complesse in termini di business è diventata evidente, aprendo la strada a ruoli di leadership.

Ha assunto responsabilità nella gestione degli incidenti per diverse aziende di consulenza, guidando un Incident Response Team (IRT), e successivamente come CERT Manager, ha diretto le risposte a gravi incidenti di cybersecurity, da data breach a focolai di malware, coordinando team interfunzionali sotto pressione. In questo ruolo, oltre alla gestione tecnica del contenimento e del ripristino, ha fornito briefing esecutivi, gestito le aspettative degli stakeholder e implementato miglioramenti post-incidente. Questo incarico ha richiesto forti capacità di leadership e decisione,

nonché la competenza nello sviluppo e nell'applicazione di piani e procedure efficaci di risposta agli incidenti.

Un altro elemento distintivo del profilo dell'autore è l'impegno verso la formazione e il mentoring. Nel corso degli anni ha guidato decine di professionisti, supportandoli nello sviluppo di carriera e trasmettendo sia competenze tecniche sia consigli di leadership. Questa passione per la condivisione del sapere è una delle principali ragioni alla base della creazione di questo libro. Dopo aver osservato da vicino le difficoltà affrontate da chi aspira a ruoli di security manager, l'autore è stato motivato a raccogliere intuizioni e lezioni apprese in una risorsa strutturata. Scrivendo questo libro, unisce esempi pratici tratti dalla propria carriera al rigore accademico dei framework e degli standard, con l'obiettivo di preparare la prossima generazione di manager della sicurezza delle informazioni sia al successo nella certificazione, sia all'efficacia nel mondo reale.

SOMMARIO

1. AUTENTICAZIONE MULTI-FATTORE (MFA)

Immagina che **Marco**, titolare di una PMI, acceda al gestionale aziendale da casa usando solo username e password. Un hacker, tramite phishing, ruba le sue credenziali e le usa per entrare nei sistemi aziendali di sera, indisturbato. Uno scenario del genere purtroppo è comune: oltre l'80% delle violazioni di dati nel 2022 è avvenuto proprio grazie a password deboli o rubate. La soluzione? Implementare l'**MFA (Multi-Factor Authentication)** sugli accessi remoti. Con l'MFA, oltre alla password si richiede un secondo fattore di autenticazione (come un codice sullo smartphone), creando un doppio lucchetto per l'account. Questo semplice accorgimento "blocca il 99,9% degli attacchi agli account", secondo Microsoft, perché anche se un criminale indovina o ruba la password non potrà accedere senza il secondo fattore. In pratica, l'MFA funziona come un portiere che chiede un documento dopo aver già mostrato la chiave: se qualcuno ha solo la chiave (password) ma non il documento (secondo fattore), resta fuori.

Implementare l'MFA in una PMI è molto più semplice di quanto si possa pensare e non richiede né budget enormi né infrastrutture complesse. Oggi quasi tutti i servizi cloud e molte VPN la supportano già nativamente. Se ad esempio la tua azienda utilizza **Microsoft 365** o **Google Workspace** per la posta elettronica, puoi abilitare l'autenticazione a più fattori per tutti i dipendenti **senza costi aggiuntivi**. Lo stesso vale per l'accesso alla rete aziendale da remoto: la MFA può essere integrata facilmente anche con soluzioni già esistenti come **Duo Security** o **Microsoft Azure MFA**, e con sistemi compatibili con protocolli come RADIUS e LDAP.

Anche i gestionali online, specialmente quelli in abbonamento, offrono ormai quasi sempre la possibilità di attivare un secondo fattore di autenticazione dalle impostazioni di sicurezza. Le modalità possono variare: alcune aziende preferiscono usare app come **Microsoft Authenticator**, **Google Authenticator** o **Authy**, che generano codici temporanei validi solo per pochi secondi; altre optano per token hardware come **Yubikey** o **Feitian**, più adatti a scenari ad alta sicurezza; altre ancora scelgono le **notifiche push sullo smartphone**, che permettono di approvare o negare un accesso con un semplice tocco.

Per la maggior parte delle PMI, la soluzione più pratica resta comunque l'uso di app gratuite per smartphone: sono sicure, non comportano costi e sono già familiari a molti utenti, visto che vengono utilizzate anche per servizi personali come l'home banking o i social network. In questo modo si ottiene un livello di protezione elevato senza stravolgere le abitudini dei dipendenti e **senza mettere sotto pressione il budget aziendale**.

Scenario pratico: La **Ditta Alfa**, con 20 dipendenti, ha impostato l'MFA su VPN e posta elettronica dopo un tentativo di intrusione. Un dipendente aveva inavvertitamente divulgato la password in risposta a una finta email "dell'assistenza tecnica". L'attaccante ha provato ad accedere all'account remoto, ma si è trovato davanti la richiesta del codice MFA sul telefono – che ovviamente non aveva. Accesso negato. La violazione è stata sventata, e l'azienda ha compreso quanto questo "doppio controllo" sia essenziale per lavorare in sicurezza anche in smart working. Gli stessi dipendenti, magari inizialmente intimoriti dalla nuova procedura, si sono abituati rapidamente: in fondo molti di loro già usavano l'MFA per servizi personali (Facebook, home banking, ecc.), quindi applicarlo anche al lavoro è risultato naturale. Come ha dichiarato un esperto di cybersecurity di Microsoft, *"MFA oggi è un must, soprattutto con più persone che lavorano da casa… è uno dei modi migliori per fermare gli hacker, anche se hanno la tua password"*.

1.1 Strumenti consigliati

Per una PMI che deve proteggere accessi a desktop remoto o a una VPN aziendale, ci sono diverse opzioni facili da implementare e spesso gratuite. **Duo Security**, ad esempio, offre un piano base gratuito per un numero limitato di utenti e dispositivi, ideale per le realtà più piccole. **Microsoft Azure MFA** è invece integrato in molti abbonamenti Microsoft 365, quindi se già utilizzi la suite per email e documenti, probabilmente ce l'hai incluso senza saperlo.

I servizi cloud più diffusi, da **Dropbox** a **Slack**, da **Google Workspace** a **Microsoft 365**, permettono di attivare l'MFA con pochi clic, utilizzando semplici app di autenticazione. Queste app sono lo strumento più pratico per iniziare: si installano sullo smartphone, generano codici temporanei validi per pochi secondi e funzionano anche senza connessione internet.

Ecco una selezione di strumenti adatti alle PMI, ordinati per tipologia e facilità d'uso:

- **Microsoft Authenticator** – Gratuito, integrato con Microsoft 365 e Azure, supporta anche account non Microsoft.
- **Google Authenticator** – Gratuito, semplice, compatibile con la maggior parte dei servizi online.
- **Authy** – Gratuito, simile a Google Authenticator ma con backup cifrato dei codici su cloud, utile se si cambia o si perde il telefono.
- **Duo Security (Free Plan)** – Gratuito fino a 10 utenti, include notifiche push e report di accesso.
- **FreeOTP** – Open source, leggero, supporta token TOTP e HOTP.

- **Yubikey (hardware)** – A pagamento, ma molto sicuro e duraturo, consigliato per account critici come quelli amministrativi.

Indipendentemente dallo strumento scelto, l'implementazione dell'MFA richiede alcuni passaggi chiave. Prima di tutto, bisogna **registrare i dispositivi** di ciascun utente: in genere il loro smartphone personale o aziendale. Poi è necessario **formare il personale** spiegando come funziona il processo di login con secondo fattore, cosa fare se arriva una richiesta di autenticazione non attesa e come gestire i codici di recupero.

Questi codici, generati al momento dell'attivazione dell'MFA, sono fondamentali: servono come "chiave di scorta" in caso di smarrimento del telefono o sostituzione del dispositivo. Tenerli in un luogo sicuro (come una cassaforte aziendale o un gestore di password protetto) è una buona pratica che evita blocchi operativi.

Per una PMI con un solo referente IT, la scelta dovrebbe cadere su strumenti **a basso impatto gestionale**, con procedure di recupero semplici e una curva di apprendimento minima. Con questa impostazione, l'MFA diventa un alleato quotidiano, non un ostacolo, e protegge le risorse aziendali da uno dei vettori di attacco più comuni: il furto di credenziali.

1.2 Checklist operativo

- **Identifica gli accessi critici da proteggere con MFA:** posta elettronica, VPN, gestionali cloud, desktop remoto e qualsiasi login da fuori ufficio.
- **Abilita l'MFA su questi servizi:** verifica le guide del fornitore (es. Microsoft 365 > Security > MFA) e attiva l'autenticazione a due fattori per tutti gli utenti.
- **Scegli il secondo fattore adeguato:** app di autenticazione (preferibile), SMS (minimo indispensabile se altri metodi non sono possibili) o token hardware per utenti con esigenze speciali.
- **Comunica e forma il personale:** spiega perché arriva questa nuova misura ("è come una cassaforte con due chiavi") e fornisci istruzioni semplici per la prima configurazione (magari un breve vademecum illustrato).
- **Implementa gradualmente se necessario:** ad esempio, inizia dall'account dell'amministratore IT e dai dirigenti, poi estendi a tutti i dipendenti. In ogni caso, copri **tutti** gli account privilegiati immediatamente.
- **Testa la procedura di accesso:** verifica personalmente che ogni utente riesca a fare login con MFA e che i codici funzionino. Prevedi una procedura di emergenza (codici di backup stampati e custoditi, o un amministratore che può resettare l'MFA) per chi avrà problemi.
- **Rendi l'MFA obbligatorio nelle policy aziendali:** ad esempio, imposta che l'accesso VPN senza MFA è disabilitato. Molti servizi permettono di rendere il secondo fattore richiesto, non opzionale.

- **Mantieni aggiornati i contatti di recupero:** assicurati di avere email alternative o numeri di telefono aggiornati per ogni utente, nel caso in cui l'MFA vada resettato (ad esempio, un dipendente perde il cellulare).
- **Monitora i log di accesso MFA:** spesso le piattaforme registrano quando un secondo fattore fallisce. Un numero insolito di richieste MFA negate potrebbe indicare tentativi di intrusione (es. qualcuno ha la password ma non il token, e prova più volte). In tal caso, fornisci supporto al dipendente interessato e, se opportuno, forzate un cambio password.

Adottando l'MFA, stai mettendo un buttafuori all'ingresso digitale della tua azienda. È un piccolo passo – in molti casi gratuito – che rafforza enormemente la difesa senza gravare sull'operatività quotidiana.

2. DENY-BY-DEFAULT E WHITELIST

La **seconda regola aurea** è: *permettere solo al software esplicitamente approvato di funzionare nei sistemi aziendali*. Questo principio "deny-by-default" (nega tutto di default) è alla base del **software whitelisting** o allowlisting. Immagina il tuo computer aziendale come un club esclusivo: solo i programmi nella lista degli invitati possono entrare in esecuzione, tutti gli altri vengono respinti alla porta. Così facendo, anche se un dipendente scarica inavvertitamente un programma infetto da Internet, quel programma **non verrà eseguito** a meno che non sia stato prima inserito nella lista delle applicazioni consentite. Si tratta di una misura potentissima per bloccare malware sconosciuti: infatti, quando ben configurato, il whitelisting può **impedire l'installazione o l'esecuzione della maggior parte dei malware**. A differenza degli antivirus tradizionali (che funzionano a bloccare ciò che è riconosciuto come cattivo, lasciando passare tutto il resto), un sistema di allowlisting fa l'opposto – *blocca tutto tranne ciò che è riconosciuto come buono*.

Vediamo uno scenario concreto: in **PiccolaImpresa Srl**, un impiegato riceve via email un file eseguibile "InteressanteOfferta.exe". L'azienda senza whitelisting rischia grosso: basta un doppio click e, se l'antivirus non rileva nulla di noto, quel file (che magari è un ransomware zero-day) parte e cifra i documenti. Invece, con una policy di allowlisting attiva, Windows impedisce proprio l'avvio di "InteressanteOfferta.exe" perché non è nell'elenco dei programmi autorizzati. L'impiegato vede comparire un messaggio tipo "Operazione bloccata dall'amministratore". Nel frattempo il malware non è riuscito a entrare in azione. Questa è prevenzione proattiva. Non a caso il **NIST** (l'ente nazionale standard USA) afferma che un whitelisting configurato a dovere è uno dei metodi più efficaci per proteggere i sistemi da minacce note e sconosciute.

Come implementarlo in pratica in una PMI? Fortunatamente, gli strumenti esistono già dentro i nostri sistemi operativi. Se usi Windows, hai due funzionalità utili: **AppLocker** (sui Windows Pro/Enterprise) e **Windows Defender Application Control**

(WDAC) sui Windows 10/11, che permettono di creare liste di applicazioni consentite. In alternativa, esistono software di terze parti – alcuni anche in versione gratuita limitata – per controllare quali programmi possono girare. All'inizio può sembrare complesso: devi fare l'inventario dei software usati in azienda (Office, browser, gestionale, ecc.), configurarli come consentiti, e poi tutto il resto verrà bloccato. Un approccio graduale può essere utile: ad esempio, partire col mettere in whitelist i software aziendali principali e bloccare **tutto ciò che proviene da cartelle temporanee o di download**. Molti attacchi ransomware eseguono il payload dal profilo utente (es. cartella AppData/LocalTemp), dove per impostazione predefinita Windows lascia eseguire file. Includendo nelle regole di restrizione il divieto di esecuzione da queste cartelle, ottieni un effetto simile al whitelisting, riducendo drasticamente il rischio. CISA e FBI infatti consigliano di implementare **Software Restriction Policies (SRP)** per impedire l'esecuzione dei programmi dai percorsi comunemente usati dai ransomware (cartelle temporanee, di download, archivio compresso, ecc). Questa è una misura attuabile in poco tempo con l'Editor Criteri di Gruppo di Windows e richiede poca manutenzione.

Scenario pratico: La **Tipografia Bianchi** decide di applicare il principio "deny by default" dopo aver letto di un attacco subito dalla tipografia concorrente. Il responsabile IT crea con AppLocker delle regole semplici: permettere esecuzione solo da C:\Program Files (dove risiedono i software ufficiali installati) e bloccare eseguibili da percorsi utenti (Desktop, Download, Temp). Un mese dopo, un dipendente scarica un finto aggiornamento di Adobe Flash (in realtà un trojan) e prova ad avviarlo: Windows mostra un messaggio *"Questa app è stata bloccata dall'amministratore di sistema"*. Il dipendente, un po' scocciato, chiama l'IT, che immediatamente capisce di aver sventato un possibile contagio malware. La minima seccatura iniziale si tramuta in sollievo quando il responsabile spiega: "Guarda, quel file poteva essere un virus. Meglio bloccarlo, se invece ti serve un nuovo software faremo la procedura di approvazione".

Non ostacola il business? Un sistema di whitelisting *deve* essere calibrato bene per non intralciare il lavoro: bisogna assicurarsi che tutti i programmi necessari siano inclusi (compresi aggiornamenti, componenti aggiuntivi come plug-in del browser, ecc.). All'inizio potrebbe richiedere qualche aggiustamento – ad esempio, aggiungere alla whitelist un tool che era sfuggito – ma una volta stabilizzato, funziona in trasparenza. In compenso, offre un enorme beneficio: riduce quasi a zero la possibilità che software non autorizzato (malevolo o anche solo non conforme alle policy) venga eseguito sui PC aziendali. Questo significa meno infezioni, meno supporto tecnico per ripulire macchine infette e più tempo dedicato ad attività produttive.

2.1 Strumenti consigliati

- **Windows AppLocker/WDAC:** per PMI con Windows Pro/Enterprise, permette di creare regole per consentire solo applicazioni firmate da fornitori fidati o presenti in determinate cartelle. Microsoft fornisce template di regole base.
- **Software Restriction Policies (SRP):** disponibile in Windows, consente di bloccare l'esecuzione in percorsi specifici. È una forma semplificata di whitelisting e può essere gestita via Criteri di Gruppo.
- **Antivirus con Application Control:** alcuni antivirus endpoint avanzati offrono moduli di controllo applicazioni (es. la funzione "Application Control" di alcune suite) che si avvicinano al whitelisting. Possono essere una soluzione intermedia se già inclusi nella licenza.
- **Soluzioni dedicate:** ThreatLocker, Ivanti Application Control, ecc., rivolte a PMI, che offrono interfacce semplificate per definire whitelist e bloccare eseguibili sconosciuti. Valuta costi e benefici, ma sappi che la logica di base è raggiungibile anche con strumenti gratuiti.
- **Monitoraggio iniziale in modalità audit:** molti sistemi di whitelisting consentono un periodo di "learning" in cui non bloccano nulla ma loggano quali programmi sarebbero stati bloccati. Questo aiuta a perfezionare la lista prima di applicare i blocchi effettivi.

2.2 Checklist operativo

- **Inventario software:** elenca tutti i software autorizzati e necessari in azienda (sistemi operativi, suite Office, browser, software gestionali, tool di produttività, ecc.). Non dimenticare script o macro legittime se usate (collegamento al Comandamento 3).
- **Implementa regole di base:** ad esempio, consenti esecuzione solo da cartelle di sistema note (Program Files, Windows) e blocca *tutto* da cartelle utenti e percorsi temporanei. Queste regole di base già fermano la maggior parte dei malware comuni.
- **Utilizza la modalità audit (se disponibile):** monitora per qualche giorno o settimana i log di whitelisting per vedere cosa verrebbe bloccato. Aggiungi in whitelist eventuali applicazioni aziendali che compaiono nei log (assicurandoti che siano lecite).
- **Applica il whitelisting in modalità enforcement:** una volta affinata la configurazione, attiva il blocco effettivo. Comunica agli utenti che se vedranno messaggi di blocco dovranno segnalarlo all'IT.
- **Definisci una procedura di approvazione software:** stabilisci come gestire richieste di nuovi software. Ad esempio, il dipendente compila una breve richiesta, l'IT valuta (sicurezza, licenza, utilità) e poi se approvato lo installa aggiungendolo alla whitelist.

- **Mantieni la whitelist aggiornata:** quando aggiorni un software esistente potrebbe cambiare il suo eseguibile o firma digitale, quindi verifica se serve adeguare la regola (soluzioni come AppLocker supportano regole per publisher, che restano valide anche con aggiornamenti minori della stessa azienda).
- **Monitora i log di blocco:** periodicamente controlla i tentativi di esecuzione bloccati. Se trovi molte voci, analizza: erano malware evitati? Erano tentativi legittimi bloccati per errore (in tal caso aggiusta la regola)?
- **Integra con altre difese:** il whitelisting non sostituisce del tutto l'antivirus (che serve comunque per altri tipi di minacce, es. macro malevole – vedi Comandamento 3). Usali in parallelo: se qualcosa sfugge alla whitelist, l'antivirus può intervenire e viceversa.
- **Sensibilizza gli utenti:** spiegando che se un programma viene bloccato non è "il computer rotto", ma una misura di sicurezza. Incoraggiali a richiedere assistenza invece di cercare vie traverse (es. non devono rinominare file o cambiare percorsi per aggirare i blocchi, ma contattare l'IT).

Con il deny-by-default, la tua PMI passa dalla difesa reattiva (bloccare i malware conosciuti) a quella proattiva (permettere solo ciò che è noto e sicuro). È un cambio di filosofia potente: riduce la superficie d'attacco e dà molta più tranquillità, perché sai che sui tuoi sistemi *gira solo ciò che hai scelto tu*.

3. DISATTIVAZIONE MACRO, PROTOCOLLI OBSOLETI, KEYLOGGER

Questo comandamento raccoglie una serie di misure "di pulizia" delle vulnerabilità interne: eliminare dal tuo ambiente quelle funzionalità o componenti tecniche che i malware sfruttano più spesso. Parliamo di tre cose in particolare: **macro Office**, **protocolli obsoleti** e **keylogger**. Sembrano elementi eterogenei, ma hanno un tratto comune: sono tra i vettori preferiti dai criminali per infilarsi nei sistemi, specialmente con ransomware.

3.1 Disattivare le macro (Office) non necessarie

Le macro VBA (Visual Basic for Applications) in Excel, Word, ecc. sono piccoli programmi che automatizzano compiti – utili in alcuni contesti, ma anche una porta d'ingresso per malware. Negli ultimi anni, tantissimi attacchi ransomware sono iniziati con un'email contenente un finto documento di Office che chiedeva di abilitare le macro per vedere il contenuto. Una volta abilitate, la macro eseguiva codice maligno: ad esempio scaricava ed eseguiva il ransomware vero e proprio. È un trucco così diffuso che la **National Cyber Security Centre (NCSC) britannica** ha dichiarato: *"l'unico modo efficace per proteggersi da macro malevole è disabilitare le*

macro in tutte le applicazioni Office e assicurarsi che gli utenti non possano riattivarle". Microsoft stessa, rendendosi conto del problema, ha cambiato impostazione predefinita: le versioni recenti di Office **bloccano automaticamente le macro nei file scaricati da Internet**, mostrando un banner di avviso. Tuttavia, non bisogna fare affidamento solo sulle impostazioni di default: è bene applicare policy aziendali esplicite. Se nella tua PMI **non usate macro legittime**, la scelta ideale è disabilitarle del tutto. Puoi farlo tramite criteri di gruppo o impostazioni di Office, selezionando "Disabilita tutte le macro senza notifiche". In questo modo, se arriva un documento furbetto che prova a far abilitare una macro, l'utente non vedrà neppure l'opzione per attivarla. Nel caso la tua azienda utilizzi qualche macro genuina (ad esempio un foglio Excel con macro contabili), adottate soluzioni come: firmare digitalmente quelle macro e configurare Office per eseguire solo macro firmate da voi, oppure utilizzare software alternativi per quell'automazione. L'obiettivo è **ridurre al minimo l'uso di macro**, specie nei documenti provenienti dall'esterno. Anche **CISA** nel suo vademecum #StopRansomware ribadisce: *assicurarsi che le macro in documenti Office ricevuti via email siano disabilitate*, perché gli attacchi ransomware le usano come vettore.

Scenario macro: La **Contabilità XYZ** riceve spesso fatture in Excel da fornitori. Un giorno ne arriva una con dicitura "Abilita contenuto per visualizzare correttamente i dati". Un'impiegata abilita la macro: in pochi secondi, sullo schermo compaiono messaggi di errore e tutti i file di rete diventano illeggibili, con estensioni strane – è partito un ransomware. Questo disastro si sarebbe evitato se le macro fossero state disattivate: quel click non avrebbe avuto alcun effetto e la macro malevola non sarebbe mai partita. Dopo l'incidente, Contabilità XYZ modifica le policy di Office e inizia a educare fornitori e dipendenti a *non usare macro nelle fatture*, preferendo formati come PDF o strumenti cloud per condividere dati.

3.2 Disabilitare protocolli obsoleti

I *protocolli* sono le regole di comunicazione tra computer. Alcuni protocolli datati, non sicuri o non più necessari rappresentano punti deboli che i cybercriminali sfruttano volentieri. Un esempio famoso è **SMBv1** – la vecchia versione del protocollo di condivisione file di Windows. Questo protocollo fu il bersaglio dell'attacco ransomware **WannaCry** nel 2017: il malware sfruttava una vulnerabilità di SMBv1 per diffondersi rapidamente in rete. Microsoft aveva già dichiarato deprecato SMBv1 e rilasciato una patch, ma molte organizzazioni non l'avevano disabilitato né aggiornato, subendo così l'infezione a catena. La lezione è chiara: se un protocollo non ti serve, o esiste una versione più sicura, **disattivalo**. Oggi SMBv1 non serve quasi a nessuno (SMB è arrivato alla versione 3); disabilitandolo, anche se un malware tenta quell'exploit, fallirà. Un detto tecnico recita: "**se non lo usi, chiudilo**". Questo vale per tanti servizi: vecchi protocolli di autenticazione (es. *NTLMv1*), vecchi protocolli di desktop remoto o telnet non cifrati, protocolli di stampa remota obsoleti, ecc. Fai una

ricognizione dei servizi attivi sui tuoi server e PC: hai porte aperte verso l'esterno per protocollo FTP vecchio stile? Spegni o restringi quegli accessi. Usi ancora SSL 3.0 o TLS 1.0 nelle comunicazioni? Disabilitali in favore di TLS 1.2/1.3. Ogni servizio superfluo in ascolto sulla rete è un possibile vettore di attacco. Molte campagne ransomware prendono di mira proprio porte aperte su servizi deboli (ad esempio l'RDP – Remote Desktop – senza MFA e patch, o VPN non aggiornate). Adotta quindi un principio di **"hygiene informatica"**: mantieni attivi solo i protocolli aggiornati e necessari, tutto il resto va tolto di mezzo. Questo spesso non costa nulla, se non un po' di tempo per verificare le configurazioni.

Scenario protocolli: La piccola **Agenzia Creativa Delta** aveva un vecchio NAS in rete che condivideva file usando SMBv1. Tutti i nuovi PC usavano SMBv2/3, ma quel NAS non era stato toccato da anni. Un ransomware di nuova generazione scansiona la rete interna, trova il NAS aperto su SMBv1, sfrutta un exploit stile EternalBlue e lo compromette, diffondendosi poi ai PC. Dopo l'incidente, Delta aggiorna il NAS e disabilita SMBv1 su tutti i dispositivi. Avessero fatto pulizia prima, il ransomware non avrebbe avuto vita facile; come notano gli esperti, *se SMBv1 è disabilitato, l'exploit EternalBlue non può colpire e WannaCry non può infettare via SMB*.

3.3 Rimuovere o bloccare keylogger

I **keylogger** sono programmi (o talvolta dispositivi hardware) che registrano di nascosto tutto ciò che viene digitato sulla tastiera, alla ricerca di password, numeri di carta e informazioni sensibili. Perché se ne parla in ottica ransomware? Perché spesso fanno parte del "kit" degli attaccanti: prima infettano con un trojan che include un keylogger, raccolgono credenziali e accessi interni, poi usano quelle credenziali rubate per propagarsi nella rete e lanciare il ransomware su più bersagli privilegiati. In sintesi, un keylogger è spesso uno **strumento di spionaggio iniziale** che prepara il terreno al colpo finale. Nel contesto di una PMI, potresti ritrovarti con un keylogger installato da: un malware scaricato (magari camuffato da software innocuo), un hacker che ha avuto accesso fisico a un PC e vi ha inserito una chiavetta keylogger, oppure un dipendente malintenzionato. Una volta in funzione, il keylogger invia periodicamente tutto ciò che cattura ai criminali (password digitate, messaggi, email, ecc.). Questo dà agli attaccanti le chiavi per muoversi lateralmente (ad esempio, se scoprono la password amministratore di sistema digitata dall'IT, ne approfitteranno per disabilitare antivirus o accedere ai backup, peggiorando gli effetti del ransomware).

Cosa fare? Innanzitutto prevenire l'installazione: le misure già descritte (whitelisting, niente privilegi admin per utenti normali, antivirus aggiornato) aiutano perché impediscono a un keylogger software di insediarsi. Inoltre, occhio all'aspetto fisico: un keylogger hardware è un piccolo connettore messo tra la porta della tastiera e il PC – basta dare un'occhiata dietro ai computer critici per assicurarsi che non ci siano dispositivi sconosciuti attaccati. Per il software, usare un buon anti-malware

aggiornato è fondamentale: molti keylogger noti vengono rilevati e bloccati. Abilitare la **protezione anti-keylogger** (alcune suite di sicurezza la includono) può aggiungere difese, ad esempio cifrando le battiture in modo che un keylogger registri solo testo inutile. Come prassi, riduci le occasioni in cui le credenziali vengono digitate manualmente: l'uso di un **password manager** aiuta perché auto-compila i login senza passare dalla tastiera per tutte le password salvate (il keylogger potrebbe non intercettarle). Per quelle che devi digitare, considera l'autenticazione a due fattori (che neutralizza l'uso di password rubate) – di nuovo vediamo come i comandamenti si rafforzano a vicenda: MFA, least privilege e whitelisting insieme rendono la vita difficile ai keylogger.

Scenario keylogger: La **TecnoImpresa** subisce un'infezione da trojan Emotet. Questo malware inizialmente dormiente ha incluso un modulo di keylogging: per giorni registra tutte le password inserite dal sistemista quando accedeva ai server. Con quelle credenziali, gli attaccanti ottengono privilegi Domain Admin e, senza farsi notare, disabilitano alcune protezioni e distribuiscono un ransomware su ogni macchina della rete con un colpo coordinato. È un attacco devastante. Analizzando a posteriori, l'azienda si accorge che qualche allarme dell'antivirus c'era stato, ma il trojan non era stato rimosso. Da questa lezione, TecnoImpresa adotta diverse contromisure: oltre a potenziare l'antivirus, implementa l'MFA per l'accesso ai server (così anche conoscendo la password, i criminali non avrebbero potuto loggarsi) e toglie i diritti amministrativi agli account quotidiani (il tecnico userà un account admin separato solo al bisogno). Inoltre, installa software anti-spyware su tutti i PC e periodicamente esegue scansioni manuali con tool come Malwarebytes anti-keylogger. Insomma, fanno "pulizia" sia delle infezioni esistenti sia potenziali.

3.4 Strumenti consigliati

- **Office Group Policy per macro:** nelle impostazioni di criteri di gruppo per Office (o nel cloud Admin Center per Microsoft 365) c'è la voce per disabilitare le macro. Imposta "Disable all macros without notification" per utenti che non ne hanno bisogno. Per chi ne ha bisogno, valuta "Disable with notification" più *Trusted Locations* rigorosamente gestite.
- **Bloccare macro Internet su Office vecchio:** se usi Office 2016/2019, applica l'aggiornamento di registro di Microsoft che blocca le macro provenienti da file Internet (simile al default Office 365).
- **Disabilitare WScript/HTA:** oltre alle macro, conviene disabilitare Windows Script Host (file .vbs) e gli *.hta* (Html Application) se non usati. Molti ransomware li sfruttano. Si può fare via registro di Windows (cambiando la chiave per WSH) o con GPO.
- **Verifica protocolli attivi:** usa comandi come netstat -an e sc query su Windows, o tool di network scanning, per vedere porte e servizi aperti. Disinstalla o disabilita servizi legacy (SMBv1 si toglie dalle Funzionalità

Windows). Aggiorna dispositivi di rete vecchi che supportano solo protocolli insicuri.

- **Firewall e IDS:** imposta il firewall (ne parliamo nel Comandamento 5) per bloccare tentativi di usare protocolli vietati. Esempio: regola che blocca traffico SMB in uscita verso Internet (nessun buon motivo per avere SMB su Internet di solito). Un IDS può allertare se rileva traffico di protocolli strani in rete interna (tipo un PC che improvvisamente fa da server Telnet).
- **Anti-keylogger software:** oltre all'antivirus tradizionale, ci sono programmi specializzati come SpyShelter o Zemana AntiLogger che monitorano attività di logging tastiera. Windows 10/11 con Defender for Endpoint ha protezioni contro keylogger conosciuti, assicurati che siano abilitate.
- **Password manager e 2FA:** come accennato, non sono strumenti anti-keylogger diretti ma mitigano l'impatto: un keylogger che cattura la master password del password manager trova comunque le password cifrate (e se hai 2FA sugli account, quelle password da sole non bastano). Quindi incoraggia il loro uso.
- **Formazione e controllo fisico:** includi nelle politiche che è vietato collegare dispositivi di input non autorizzati. Ogni tanto ispeziona fisicamente i PC importanti (server, computer amministrazione) per vedere se tra cavo tastiera e porta USB è stato inserito qualche apparecchio estraneo.

3.5 Checklist operativo

- **Disabilita macro Office:** applica policy aziendale per bloccare le macro Office su tutti i PC, a meno di approvazione esplicita. Distribuisci le impostazioni di blocco macro tramite Criteri di Gruppo o configurazione cloud (Intune).
- **Isola le eccezioni macro:** se alcune macro sono indispensabili, firma digitalmente quei documenti e configura Office per eseguire *solo macro firmate* di trust. Oppure valuta di convertirle in soluzioni più sicure (es. piccoli applicativi dedicati).
- **Comunica "No macro" via email:** avvisa dipendenti e partner esterni che per policy non dovrebbero inviare file Office con macro. Se arrivano, contattate l'IT prima di aprirli.
- **Mappa i protocolli utilizzati:** fai una lista dei servizi di rete necessari (es. condivisione file, RDP, SMTP, ecc.) e la versione sicura di ognuno. Poi identifica versioni vecchie ancora presenti (es. stampanti di rete che richiedono SMBv1) e pianifica la loro eliminazione o aggiornamento.
- **Disabilita protocolli legacy:** attraverso le impostazioni di sistema o di apparati, spegni SMBv1, SSL/TSL insicuri, protocolli di autenticazione vecchi (LANMAN, NTLMv1). In Windows, c'è uno strumento "Enable/Disable SMB1"

facile da usare. Controlla anche server Linux/unix per disabilitare Telnet, FTP non sicuro, SNMP v1, etc.

- **Aggiorna dispositivi e software datati:** spesso l'uso di protocolli vecchi è dovuto a apparecchiature non aggiornate (NAS, scanner di rete, ecc.). Applica aggiornamenti firmware o sostituiscili se non supportano protocolli moderni.
- **Implementa MFA sui servizi di amministrazione:** se proprio devi tenere esposto un servizio (tipo RDP o SSH per accesso remoto), almeno proteggilo con MFA e limitazioni di IP. Questo mitiga l'uso di eventuali credenziali catturate da keylogger.
- **Esegui scansioni anti-malware periodiche:** oltre alla protezione in tempo reale, fai scansioni complete fuori orario (anche con più prodotti on-demand) per scovare eventuali spyware o keylogger passati inosservati.
- **Controlla i processi in esecuzione:** ogni tanto, verifica se sui PC girano processi sospetti (i keylogger spesso hanno nomi falsi ma puoi notare comportamenti anomali, es. un processo che cerca di inviare dati in uscita di frequente).
- **Monitora traffico uscita (C2):** un keylogger software invia i dati raccolti a un server. Configura gli strumenti (firewall, IDS) per allertare su traffico verso destinazioni sconosciute o su protocolli inusuali sulla porta 80/443 (i keylogger a volte mascherano il traffico come HTTP/HTTPS verso certi server).
- **Sensibilizza sugli input non fidati:** nella formazione al personale, includi il rischio di dispositivi USB estranei (ad esempio, non collegare tastiere/chiavette trovate in giro) e in generale di non installare software non autorizzato (che potrebbe includere keylogger).

Con queste misure, stai **chiudendo diverse porte** in faccia al ransomware: niente macro trappola via email, niente facili exploit su vecchi protocolli, niente furto silenzioso di password via keylogger. Ogni varco tappato è un'opportunità in meno per l'attaccante e un livello di protezione in più per la tua azienda.

4. USARE PRIVILEGI MINIMI

Chi in azienda **usa il PC con diritti da amministratore**? Spesso, nelle piccole imprese, la risposta è: *"più o meno tutti"*. È comprensibile, per comodità: Windows chiede il permesso per certe operazioni e avere l'utente admin evita seccature. Ma questa comodità si paga carissima in termini di sicurezza. Il **principio del minimo privilegio** dice che ogni utente (o programma) dovrebbe operare con i privilegi minimi necessari. Tradotto: i dipendenti dovrebbero usare il PC con account standard, non come amministratori del sistema. Perché è così cruciale? Perché se un malware riesce a partire sull'account di un utente standard, avrà poteri limitati: magari potrà criptare i file di quell'utente, ma non potrà infettare componenti di sistema o

diffondersi facilmente ad altri nodi. Al contrario, se l'utente è amministratore, il malware ha in mano **le chiavi della città**: può installarsi come servizio di sistema, disabilitare l'antivirus, creare nuovi utenti con diritti elevati, insomma fare danni massimi.

Le statistiche confermano l'impatto enorme: uno studio di Cybersecurity ha trovato che oltre il 60% delle vulnerabilità critiche di Windows potrebbero essere mitigate semplicemente rimuovendo i diritti amministrativi agli utenti (in alcuni report si parla addirittura di percentuali attorno al 80-90% per certe categorie di minacce). L'US Small Business Administration raccomanda esplicitamente di applicare il principio di *least privilege*, ovvero *"nessun impiegato dovrebbe avere accesso amministrativo salvo quando assolutamente necessario"*, e chi ha un account admin dovrebbe usarlo solo lo stretto indispensabile. Allo stesso modo, CISA e FBI sottolineano che i ransomware spesso fanno leva su account con privilegi eccessivi; ridurre tali privilegi frena la possibilità di attacchi su larga scala.

Scenario negativo: la **Software Beta** aveva tutti i dipendenti con account locali amministrativi – "così possono installarsi i tool di sviluppo che gli servono senza aprire ticket", pensava il titolare. Un developer scarica senza pensarci un pacchetto npm infetto; quel malware sfrutta i permessi admin per insinuarsi nel sistema, avviarsi con Windows e da lì rubare credenziali di rete e fare movimenti laterali. In pochi giorni il dominio Windows dell'azienda è compromesso. Se quell'utente fosse stato standard, il malware avrebbe incontrato ostacoli ad ogni passo: per installarsi avrebbe dovuto richiedere privilegi (generando un prompt UAC che forse avrebbe insospettito lo sviluppatore), non avrebbe potuto accedere a zone sensibili del sistema né istallare driver nocivi. Insomma, il danno sarebbe stato contenuto o addirittura nullo.

Scenario positivo: la **Ditta Gamma** invece ha deciso che nessuno lavora con account amministrativi. Tutti i dipendenti usano account utenti semplici; l'unico admin è l'account del responsabile IT, che però lo utilizza solo per installazioni o configurazioni straordinarie. Un giorno, un dipendente del marketing clicca su un file strano e parte un trojan: prova a modificare impostazioni di sistema ma Windows chiede la password admin (che il marketing ovviamente non ha). Il malware rimane confinato, riesce solo a scaricare qualche file temporaneo ma non ad attivarsi in modo permanente. L'antivirus lo rimuove al successivo scan. L'azienda ringrazia la scelta di limitare i privilegi: l'infezione non ha avuto gambe per camminare.

4.1 Come implementarlo

tecnicamente, è semplice: quando configuri i PC, non aggiungere gli utenti normali al gruppo "Administrators". In un dominio Windows, assicurati che gli utenti siano solo nel gruppo Users. Se al momento tutti sono admin, pianifica una migrazione: crea per ciascuno un nuovo account standard (o converti il loro in standard) e mantieni un

account amministrativo separato – magari uno per l'IT e uno di emergenza – tenuto segreto. È importante che il management appoggi questa decisione, perché all'inizio qualche seccatura apparente c'è: l'utente non può installare autonomamente software o stampanti, ad esempio. Ma questo si può gestire con policy: l'IT può distribuire le stampanti in rete, e per i software definire una procedura (come visto nel comandamento whitelisting). A conti fatti, togliere i privilegi amministrativi agli utenti risolve molti problemi prima che nascano e riduce drasticamente le possibilità di installare malware di livello profondo.

Non dimenticare l'account *Administrator* di Windows: rinominalo e imposta una password robusta, oppure disabilitalo se non serve, per evitare che venga sfruttato (è un account noto, i malware spesso tentano brute-force su quello). E se usi server o servizi con utenti admin di default, cambia nome e password anche lì.

4.2 Strumenti consigliati

- **Gestione Utenti e Gruppi (Windows):** per rimuovere gli utenti dal gruppo Administrators locale. Puoi farlo manualmente su ogni PC o in modo centralizzato con criteri di gruppo (Restricted Groups) in un dominio.
- **Account separati per admin:** crea account dedicati per attività amministrative. Su Windows AD/Azure AD, gli account amministrativi dovrebbero essere distinti da quelli usati per email e lavoro quotidiano. Ad esempio: utente "m.rossi" per lavorare, "adm-rossi" per compiti IT con privilegi. Il secondo lo si usa solo dentro sessioni RDP/console dedicate o con "Esegui come amministratore" quando serve.
- **Strumenti di elevazione controllata:** se c'è il timore di rallentare il lavoro, esistono tool come **MakeMeAdmin** (uno script che dà temporaneamente diritti admin a un utente per tot minuti) o soluzioni di *Privilege Access Management* semplificate che forniscono elevazione "just in time" (collegamento al Comandamento 9). Questi tool aiutano l'IT a concedere rapidamente diritti su richiesta senza lasciare utenti sempre admin.
- **Audit dei privilegi:** usa gli strumenti di audit per identificare chi ha privilegi e dove. In un dominio Windows, ad esempio, controlla regolarmente i membri dei gruppi Domain Admins, Administrators locali delle macchine, ecc., e pulisci eventuali aggiunte indebite.
- **Controllo account utente (UAC):** mantieni attivo l'UAC su Windows al livello predefinito o più alto. Anche per gli amministratori, avere l'UAC attivo riduce la superficie (gli admin eseguono i programmi con token utente standard finché non elevano intenzionalmente). Non disattivarlo mai per comodità.
- **Server Linux/Mac:** anche su altri sistemi il concetto vale. Su Linux/Unix utilizza sudo con parsimonia e non far lavorare tutti come root. Su Mac, non usare l'account amministratore come predefinito per l'utente se non necessario.

4.3 Checklist operativo

- **Censimento degli utenti e privilegi:** fai un elenco di tutti gli account utente aziendali e verifica chi ha privilegi amministrativi (locali o globali). Attenzione agli utenti che, magari per installare un programma anni fa, erano stati promossi admin e mai rimossi.
- **Pianifica la revoca dei privilegi:** comunica con la direzione e spiega i benefici (maggiore sicurezza, riduzione infezioni, protezione dati). Ottieni supporto nel far capire al personale che questo cambiamento è per il bene dell'azienda.
- **Crea account amministrativi separati:** per ogni persona dell'IT (o consulente esterno) che necessita di privilegi, predisponi un account dedicato all'amministrazione. Questi account avranno password forti e possibilmente MFA.
- **Converti gli account utente a standard:** rimuovi gli utenti normali dal gruppo Administrators sulle loro macchine. In un dominio, assicurati che solo il personale IT sia in Domain Admins e simili. Esegui test su un paio di PC prima, per vedere se tutto funziona (alcuni software legacy potrebbero avere richieste particolari: in tal caso c'è da lavorare di fino con i permessi di file o registro per farli girare da utenti standard, ma è fattibile).
- **Comunica le procedure per installazioni:** informa che da ora in poi per installare nuovo software o fare cambiamenti di sistema, gli utenti dovranno contattare l'IT. Idealmente, accompagna la policy con un sistema snello di richiesta (un ticket o anche un messaggio istantaneo, purché l'IT risponda in tempi accettabili). L'obiettivo è evitare che percepiscano la cosa come "adesso non possiamo far più nulla", ma piuttosto "ora c'è più controllo, ma se ti serve qualcosa te lo facciamo avere in sicurezza".
- **Proteggi gli account admin:** quelli nuovi creati devono essere ben custoditi. Password forti, memorizzate in password manager o cassaforte digitale. Valuta di abilitarvi l'MFA se possibile (ad es. account admin di Microsoft 365 con app Authenticator).
- **Rinomina/disabilita account Administrator di default:** su ogni PC/Server Windows locale, rinomina l'utente Administrator e/o impostane uno molto lungo e complesso di password, oppure disabilitalo e usa altri account admin nominali.
- **Verifica applicazioni post-cambio:** controlla se applicazioni di gestione remota, agent di backup, ecc., necessitano di credenziali admin salvate. Meglio creare service account dedicati piuttosto che usare account personali admin.
- **Controlla gli effetti nel tempo:** monitora se la rimozione dei privilegi causa colli di bottiglia o se compiti quotidiani restano fluidi. Ad esempio, se scopri che i commerciali non riescono più ad aggiornare un plugin CRM perché

serve admin, studia una soluzione sicura (magari l'IT può aggiornarlo per tutti in rete). In generale, risolvi caso per caso, ma **non tornare indietro sulla policy** – di solito pochi inconvenienti iniziali si risolvono e il beneficio di lungo periodo è enorme.

- **Audit periodico dei privilegi:** fai ogni 3-6 mesi un controllo: nessun nuovo utente dovrebbe essere admin. Se scopri eccezioni (magari qualcuno in emergenza è stato messo admin e poi ci si è dimenticati di toglierlo), correggi subito. Questo controllo regolare garantisce che il principio di least privilege resti applicato nel tempo.

Adottando il minimo privilegio, ottieni due risultati: limiti la capacità di azione di eventuali malware e al contempo riduci anche errori umani (un utente senza permessi non può *accidentalmente* disinstallare un software di sicurezza o modificare impostazioni critiche). I criminali informatici sanno bene che i privilegi elevati sono la chiave per colpire in grande stile – togliendoglieli, li costringi a faticare molto di più (spesso troppo, spingendoli a rinunciare o accontentarsi di accessi limitati). Come dice una massima tra gli esperti: *"togliendo i privilegi admin, togli il carburante al ransomware"*.

5. HARDENING SISTEMI E NETWORK

Se pensiamo alla sicurezza informatica come alla protezione di un castello, spesso ci concentriamo sul **tenere chiuso il portone** per impedire ai nemici di entrare (il traffico in entrata). Ma c'è un altro aspetto cruciale: **sorvegliare anche le uscite segrete e le comunicazioni verso l'esterno**. Il traffico in uscita da una rete aziendale è spesso trascurato, e invece i cybercriminali ne approfittano. Dopo essersi infilati nella rete, la prima cosa che fanno i malware è provare a *telefonare a casa*, cioè a contattare server esterni per scaricare comandi o inviare dati rubati. Se lasciamo tutto aperto in uscita, è come dare al ladro le chiavi per scappare con il bottino. Una strategia di sicurezza robusta per una PMI deve prevedere **blocchi (o filtri) sulle porte e sul traffico in uscita** non necessario, oltre a chiudere le porte d'ingresso non presidiate.

Facciamo un esempio: in **Alfa Srl** un PC viene infettato da malware. Appena entrato, il malware cerca di collegarsi al suo server di comando e controllo (C2) su Internet per ricevere istruzioni (ad es. "scarica il ransomware e cifrali tutti"). Se l'azienda ha un firewall che permette solo il traffico web su porta 80/443 e blocca tutto il resto, il malware potrebbe trovarsi con le mani legate se prova porte insolite. Anche se usa la porta 443 (quella del HTTPS) per uscire, un firewall con filtro potrebbe analizzare le richieste e bloccare quelle verso domini noti come malevoli. In molti casi, quando il malware non riesce a contattare il server remoto, l'attacco abortisce o rimane limitato. Inoltre, limitando il traffico in uscita, puoi anche **impedire esfiltrazioni di dati**: supponiamo un ransomware provi a spedire all'esterno gigabyte di documenti

(per la doppia estorsione), ma trova solo la porta web aperta e magari con controllo di contenuti: potresti accorgerti e intervenire prima che vada a segno.

Dall'altro lato, **bloccare le porte non necessarie in entrata** è una pratica storica di buon senso: se la tua azienda ha un server web pubblico sulla porta 443, non c'è motivo per cui debbano essere aperte dall'esterno anche la porta 3389 (RDP) o 445 (SMB), etc. Ogni porta aperta è un bersaglio che attira i bot degli hacker 24/7. Quindi, chiudi tutto ciò che non serve e proteggi con regole stringenti ciò che deve rimanere aperto. Ad esempio, se per emergenza devi tenere aperto RDP sul server, limita l'accesso solo a specifici IP di trust (magari l'IP statico di casa tua) e comunque mettici davanti l'MFA (vedi Comandamento 1).

5.1 Focus sul traffico in uscita (Egress Filtering)

Molte PMI sottovalutano questo aspetto pensando "finché ho l'antivirus sto a posto". Ma la mancata attenzione al traffico in uscita è il tallone d'Achille di tante reti aziendali. I firewall vengono configurati per bloccare l'esterno che entra, ma spesso lasciano passare tutto l'interno che esce, **senza monitoraggio**. I criminali lo sanno e sfruttano questo "side door": magari entrano con phishing (che non viene bloccato dal firewall perché è traffico inizialmente legittimo verso l'interno) e poi una volta dentro usano la libertà di uscita per fare danni. Se invece concentri l'attenzione anche sulle comunicazioni uscenti, puoi accorgerti per tempo di attività malevole e bloccarle. Ad esempio, se nessun PC dovrebbe contattare indirizzi IP strani in Russia, puoi mettere regole che blocchino quel traffico e allertino l'IT. Molti attacchi di ransomware noti coinvolgono infatti il *doppio furto*: prima i dati esfiltrati poi la cifratura. Impedire l'esfiltrazione può risparmiarti la seconda parte del ricatto. Inoltre, bloccare chiamate verso i server di comando e controllo dei malware spesso significa **neutralizzarli** sul nascere: come un ladro chiuso nel caveau senza poter comunicare, non sa come muoversi e rimane intrappolato finché lo scopri.

Scenario concreto: alla **Gamma & Co.** un dipendente apre un allegato infetto. Il malware tenta di collegarsi a un server su porta 8080 per scaricare il resto del codice maligno, ma il firewall aziendale ha una regola "nega tutto in uscita tranne web e mail". Quella richiesta viene bloccata. Subito scatta un alert al pannello di controllo del firewall: "Tentativo di connessione uscente bloccato verso IP sconosciuto su porta 8080 dal PC di Mario". L'IT contatta Mario, isola il suo PC e scopre il malware prima che abbia potuto fare altro. Gamma & Co. si salva da un potenziale attacco grazie a una politica di egress filtering. Viceversa, la **Delta Srl** non aveva restrizioni: il loro malware è riuscito a comunicare tranquillamente col suo server C2, scaricare l'exploit per muoversi in rete e infine lanciare il ransomware su 10 PC. A posteriori, Delta vede nei log che per ore un PC aveva dialogato con un indirizzo IP esterno strano, su porta 4444, ma nessuno stava guardando e non c'era blocco.

5.2 Implementazione pratica

la maggior parte dei router/firewall attuali (anche quelli "all-in-one" forniti dagli ISP alle aziende) permettono di creare regole di firewall per traffico uscente. Un approccio semplice è: **blocca tutto eccetto** alcune destinazioni/porte note. Ad esempio, consenti solo: navigazione web standard (porta 80/443) verso qualunque destinazione, DNS solo verso i server DNS affidabili, posta SMTP solo verso il server dell'ISP o servizi noti, e poco altro di specifico (ad esempio se hai un software che deve collegarsi a un certo servizio cloud su porta non standard, lo autorizzi esplicitamente). Tutto il resto – *deny*. Questa è la filosofia "**deny by default**" applicata alle connessioni di rete (si sposa con la whitelist software del Comandamento 2). Certo, all'inizio potresti dover aggiungere qualche eccezione man mano che scopri necessità (es. il gestionale deve fare FTP a un certo server, quindi apri quell'uscita specifica). Ma alla fine otterrai un profilo di traffico molto più pulito e controllato.

Inoltre, puoi utilizzare funzionalità di **Threat Intelligence sul firewall**: molti firewall UTM anche piccoli includono elenchi di IP e domini malevoli noti (aggiornati dal fornitore). Attivando questi filtri, se un PC tenta di contattare un C&C (Comando e Controllo) conosciuto, viene bloccato immediatamente. È come avere una lista nera dinamica di destinazioni pericolose. Non costa in genere extra, basta abilitare l'opzione se c'è.

5.3 Strumenti consigliati

- **Firewall hardware/UTM:** se hai un firewall dedicato (SonicWall, Fortinet, WatchGuard, etc) sfrutta le policy di egress filtering. Molti hanno procedure guidate per impostare regole di base ("Blocca tutto tranne HTTP/HTTPS/DNS").
- **Router ISP avanzati:** alcuni router evoluti (tipo FRITZ!Box o apparati Cisco/Juniper small business) permettono regole simili. Controlla la documentazione; in mancanza, valuta l'upgrade a un dispositivo che lo consenta.
- **Firewall software su PC:** Windows Firewall su ogni client può anche filtrare l'uscita. In ambienti senza un firewall centrale, puoi tramite Criteri di Gruppo distribuire regole di Windows Firewall che blocchino ad esempio tutte le porte tranne alcune. È meno efficace di un firewall perimetrale (perché ogni PC può teoricamente cambiare le proprie regole se è admin, ma noi abbiamo tolto admin agli utenti!), però aggiunge un livello.
- **DNS filtrato (Protective DNS):** un metodo efficace e semplice per controllare traffico web malevolo è usare un servizio DNS pubblico con filtro. Ad esempio **Quad9** o **Cloudflare Gateway** o **OpenDNS**: questi resolver DNS non risolvono i nomi di dominio maligni noti. Così, se il malware prova a contattare *badserver.evil.com*, il DNS non glielo trova proprio, e la

connessione fallisce. Attiva uno di questi DNS sui client o a livello di router. CISA e NSA raccomandano vivamente l'uso di DNS protettivi per bloccare sul nascere malware e phishing.

- **Proxy web con filtro URL:** se la tua PMI ha la necessità di controllare nel dettaglio la navigazione web, un proxy con filtro può bloccare categorie (es. siti per adulti, o siti noti per malware). Esistono soluzioni cloud per PMI (Cisco OpenDNS, zScaler small business, etc.) che fungono da proxy filtri senza dover installare nulla on-prem.
- **Monitoraggio e logging:** qualunque sia la soluzione di firewall, assicurati di **loggare** il traffico bloccato in uscita e controllarlo regolarmente. Ad esempio, se noti tentativi di connessione a Tor (uscite verso tanti IP random su porta 9001, tipico di Tor), potresti scoprire che un malware sta cercando di usare Tor per comunicare. O se un PC tenta di contattare decine di IP in paesi con cui non hai affari, magari è segnale di un'infezione.
- **Geo-blocking (con cautela):** alcuni firewall permettono di bloccare traffico da/a certi Paesi. Se la tua PMI opera solo in Italia, potresti bloccare tutte le connessioni in ingresso da altri Paesi e magari in uscita verso nazioni notoriamente fonti di attacchi (Russia, Nord Corea, ecc.). Non è infallibile (gli attaccanti usano proxy in tutto il mondo), ma riduce un po' la superficie. Tuttavia, attenzione a non bloccare servizi cloud globali che magari risiedono all'estero. Questa misura va soppesata bene.

5.4 Checklist operativo

- **Mappa il traffico necessario:** elenca i servizi interni che richiedono comunicazioni esterne. Es: web browsing (porta 80/443) per tutti; posta SMTP (porta 587?) verso server mail; VPN verso filiale (porta specifica); software particolari (es. un software gestionale che fa ftp su un server della banca). Questa mappa ti serve per sapere cosa autorizzare.
- **Chiudi porte non usate in entrata:** configura il firewall per accettare dall'esterno *solo* ciò che serve al business (ad esempio, porta 443 per il sito web aziendale). Tutto il resto – RDP, database, file sharing – deve essere chiuso o accessibile solo via VPN. Se hai servizi web interni, considera di metterli dietro una VPN o almeno dietro autenticazione robusta.
- **Implementa regole *deny* in uscita:** sul firewall perimetrale (o su ciascun PC via Windows Firewall) crea una regola generale che blocchi ogni traffico uscente, e poi definisci eccezioni permesse: DNS verso server DNS autorizzati; HTTP/HTTPS verso Internet (eventualmente solo dai PC che ne hanno bisogno, per esempio il server non dovrebbe navigare su siti esterni se non per update); SMTP verso server posta; NTP verso server orario, ecc. In caso di dubbi, inizia bloccando solo le porte conosciute come pericolose (es. blocca tutte le porte TCP/UDP sopra 1024 tranne quelle usate) e poi affina fino ad arrivare al modello whitelist completo.

- **Attiva il filtro DNS:** imposta sui dispositivi l'uso di un DNS filtrante come Quad9 (configurabile sul router per comodità). Testa che la navigazione funzioni e prova un sito noto malevolo (Quad9, ad esempio, redirige a una pagina di blocco).
- **Blocca IP malevoli noti / Tor:** se il tuo firewall ha la feature, abilita blocco automatico di IP/domini malevoli. Inoltre, se non c'è ragione di usare Tor in azienda, blocca le connessioni verso nodi Tor noti. Questo può prevenire che malware usino Tor per comunicare.
- **Limita velocità e quantità in uscita:** se possibile, metti anche limiti di traffico in uscita anomali. Ad esempio, se un PC generalmente invia pochi MB al giorno su Internet, e improvvisamente prova a inviarne 100GB (tipico di esfiltrazione), un controllo di *Data Loss Prevention* o semplicemente un alert di soglia può avvisarti. Alcuni firewall UTM hanno la funzione DLP integrata.
- **Monitora i log di blocco:** stabilisci una routine (settimanale magari) in cui guardare gli eventi di traffico uscita bloccato. Se noti tentativi ripetuti da un PC verso destinazioni strane, indaga subito su quel PC: potrebbe essere segno di malware che tenta senza successo di chiamare casa. Meglio trovarlo *prima* che magari riesca a comunicare (non è detto che tutti i canali siano bloccati – un malware potrebbe adattarsi e provare a usare HTTPS su porta 443 per mimetizzarsi).
- **Aggiorna le regole man mano:** se un nuovo software o servizio è introdotto in azienda, ricordati di aggiornare di conseguenza il firewall. Ad esempio, passi a una nuova piattaforma cloud? Assicurati che le sue chiamate siano permesse (magari forniscono un elenco di endpoint/IP da consentire). Mantieni un documento delle regole con annotazioni sul perché di ciascuna eccezione.
- **Testa la sicurezza dall'esterno:** puoi fare un port scanning della tua rete pubblica (ci sono servizi online come ShieldsUP, o usare nmap da fuori) per vedere quali porte risultano aperte. Dall'interno, potresti usare tool come telnet o nc per provare a raggiungere porte esterne non consentite e assicurarti che vengano bloccate.
- **Isola la rete in caso di incidente:** predisponi un piano: se comunque avviene un'infezione, come reagire lato rete? Ad esempio avere VLAN separate (vedi Comandamento 12) e possibilità di scollegare rapidamente la rete da Internet o segmenti tra loro. Questo come misura contenitiva estrema.

In sintesi, con una buona gestione delle porte e del traffico di rete, stai creando un muro di cinta più intelligente: non solo robusto verso l'esterno, ma anche capace di **intrappolare** il nemico se dovesse entrare. Come in un castello medioevale, hai i ponti levatoi sollevati (porte chiuse) e, anche se qualcuno scavalcasse, troverebbe

porte interne serrate e sentinelle pronte ad allarme se provasse a scappare col bottino.

6. MONITORAGGIO FILE E USB

Una mattina ti accorgi che sul server aziendale tutti i documenti Word hanno cambiato estensione in *.locked* e c'è una nota di riscatto. È successo di notte, e nessuno se n'è accorto in tempo. Ora immagina invece se avessi avuto un sistema che **monitorava i file**: appena un numero anomalo di file veniva modificato o criptato in breve tempo, avrebbe lanciato l'allarme, magari bloccando il processo sospetto. Monitorare lo stato dei file e l'uso di dispositivi USB può fare la differenza tra un attacco scoperto quando è troppo tardi e uno neutralizzato sul nascere.

6.1 Monitoraggio dei file (File Monitoring)

L'idea è di tenere d'occhio le **modifiche anomale ai file** nei tuoi sistemi critici. I ransomware spesso si rivelano perché all'improvviso iniziano a cifrare centinaia di file uno dopo l'altro. Un software di monitoraggio potrebbe rilevare questo pattern insolito di I/O disco. Windows 10/11 include una funzione chiamata **Controlled Folder Access** proprio pensata per questo: protegge cartelle specifiche (es. Documenti, Desktop, cartelle condivise) e impedisce alle applicazioni non autorizzate di modificarne i file. Se un processo tenta di criptare o alterare molti file protetti e non è in whitelist, Windows lo blocca e ti avvisa. È come un sistema immunitario che reagisce appena un processo tocca dati vitali senza permesso. Attivare Controlled Folder Access tramite Windows Security (sezione "Protezione da ransomware") è gratuito ed efficace, specie se abbinato al whitelisting applicazioni (Comandamento 2). Un'altra tecnica di **File Integrity Monitoring (FIM)** è utile su server: strumenti che calcolano periodicamente l'hash dei file importanti e segnalano se cambiano all'improvviso. Questo aiuta non solo contro ransomware ma anche per scoprire manomissioni (es. qualcuno modifica file di configurazione o installa backdoor). Molti sistemi di whitelisting o EDR hanno integrato un certo grado di FIM.

6.2 Monitoraggio dispositivi USB

Le chiavette USB e dischi esterni sono notoriamente una via di infezione e di esfiltrazione dati. Un dipendente distratto infila una chiavetta trovata in parcheggio – e boom, virus in rete. Oppure qualcuno copia dati aziendali riservati su un hard disk esterno per portarseli via. Limitare e sorvegliare l'uso delle USB è quindi cruciale. La soluzione più sicura è **bloccare del tutto le USB** (almeno l'archiviazione di massa) sui PC aziendali a meno di eccezioni specifiche. Questo si può fare via criteri di gruppo su Windows (impostando "Disattiva l'accesso a unità di archiviazione rimovibili" o permettendo solo a utenti autorizzati l'uso). Se bloccare al 100% non è

pratico (magari usate chiavette per trasferire dati ai clienti), almeno abilita la sola lettura e blocca l'esecuzione di programmi da USB. Puoi anche investire in **software di DLP (Data Loss Prevention)** che controlla l'attività USB: ad esempio, logga tutti i file copiati su dispositivi esterni e può impedire copie di file contenenti certe parole chiave o imponendo la crittografia automatica. Esistono soluzioni DLP entry-level adatte anche a PMI, spesso come parte di suite di sicurezza endpoint.

Monitorare l'uso USB significa anche ricevere un alert quando viene inserito un dispositivo non autorizzato. Alcuni antivirus endpoint lo fanno: "è stato collegato il dispositivo X al PC Y". Questo, se non altro, ti rende consapevole dell'evento. In un contesto piccolo, il solo sapere che un certo impiegato ha montato 3 chiavette in un giorno potrebbe spingerti a una chiacchierata (magari sta trasferendo dati aziendali?).

Scenario di infezione USB: la **Azzecco S.p.A.** aveva segmentato e protetto la rete, ma non considerato le USB. Un tecnico esterno, per comodità, usa la sua chiavetta per copiare un driver su un PC produzione. Quella chiavetta era stata infettata altrove da un worm, il quale appena collegato esegue il suo payload (approfittando dell'auto-run su quella macchina). Il worm entra nella rete isolata e comincia a diffondersi. Se Azzecco avesse avuto il blocco delle USB o anche solo avesse disabilitato l'auto-run, l'infezione sarebbe stata prevenuta. Dopo questo episodio, l'azienda ha rivisto la sua politica: USB vietate nei sistemi critici; se serve scambiare file, solo tramite canali controllati (server condiviso, trasferimento sicuro). Inoltre, ha implementato un sistema per cifrare automaticamente qualsiasi chiavetta autorizzata, così in caso di smarrimento i dati non sono leggibili.

Scenario di furto dati via USB: un dipendente insoddisfatto di **StudioGamma** decide di cambiare lavoro portandosi il database clienti. Collega di nascosto un hard disk USB e lo copia. StudioGamma però aveva un agent DLP attivo che immediatamente avvisa l'IT di un bulk copy non usuale. L'IT interviene prima che il dipendente possa uscire dall'ufficio col drive, e sventa il furto. Questo scenario sottolinea un altro lato del monitoraggio USB: non solo protezione da malware, ma anche da **insider threat**.

6.3 Strumenti consigliati

- **Windows Controlled Folder Access:** integrato in Microsoft Defender Antivirus (Win10 e Win11). Attivalo per proteggere cartelle come Documenti, Desktop, ecc. Puoi aggiungere percorsi di rete (cartelle condivise) nelle impostazioni di protezione ransomware. Ogni app non riconosciuta che tenta di modificare quei file verrà bloccata e segnalata.
- **Software anti-ransomware dedicati:** ce ne sono di standalone (es. Acronis Ransomware Protection, CyberReason RansomFree) che monitorano i file honeypot e comportamenti di cifratura. Molte suite AV hanno già funzioni anti-ransomware comportamentali. Assicurati che siano abilitate.

- **File Integrity Monitoring tools:** OSSEC (gratuito) o SolarWinds (commerciale) tra i tanti. Per un server critico, ad esempio, OSSEC può essere configurato per controllare certi file config e inviarti alert via email se cambiano.
- **Logging di accesso ai file su Windows:** abilita l'auditing su server file per loggare chi modifica/elimina i file (può aiutare a ricostruire eventi, e magari a notare accessi inusuali in tempo reale se integrato con un SIEM).
- **Group Policy per USB:** in ambiente Windows AD, usa le policy di **Device Installation Restrictions** per vietare l'installazione di unità USB non autorizzate. Puoi creare una whitelist di ID hardware (cioè specifiche pen drive aziendali) e bloccare tutto il resto. In alternativa, una GPO specifica in Configurazione Computer > Impostazioni di sicurezza > Criteri locali > Opzioni di sicurezza, c'è "Dispositivi: Impedisci l'accesso a unità di archiviazione rimovibili" – può essere impostata per sola lettura o blocco completo.
- **Software DLP leggero:** se investi un po', soluzioni come **Endpoint Protector**, **Teramind** o **Symantec DLP** (ci sono pacchetti per piccole aziende) permettono controllo fine sulle USB. Ad esempio, possono forzare la crittografia dei file copiati su USB, o impedire copie di tipi di file specifici.
- **Antivirus cloud con controllo dispositivi:** molte console cloud di antivirus per endpoint (es. Bitdefender GravityZone, Kaspersky Endpoint) includono la gestione centralizzata delle porte e dispositivi. Puoi da lì configurare policy: es. "blocca tutte le chiavette eccetto quelle cifrate con BitLocker" o "consenti solo mouse e tastiere, blocca storage".
- **Notifica uso dispositivi:** attiva se presente nel tuo AV/EDR l'opzione di notificare l'admin quando viene inserito un dispositivo USB. Alcuni la offrono via email o dashboard.

6.4 Checklist operativo

- **Abilita Controlled Folder Access (CFA):** su tutti i PC Windows10/11 con Defender. Vai in Sicurezza di Windows > Controllo delle app e del browser > Protezione da ransomware > abilita l'accesso alle cartelle controllate. Aggiungi eventuali percorsi di rete o percorsi personalizzati dove risiedono dati importanti. Testa che le normali attività (es. salvataggio file da Word) funzionino, e prova a eseguire un'app non consentita per vedere come viene bloccata e loggata.
- **Metti in whitelist le app sicure nel CFA:** potrebbe essere necessario aggiungere manualmente alcuni programmi aziendali affidabili alla lista Consenti di Controlled Folder Access, se vengono bloccati. Fallo preferibilmente centralmente via PowerShell/GPO/Intune.

- **Configura l'auditing di modifiche massicce:** se hai un SIEM o almeno la possibilità di script, crea un alert: "più di X file modificati in Y minuti su questa cartella = avvisa IT". Alcuni backup software hanno integrato un rilevamento di ransomware guardando il numero di file cambiati da un backup all'altro. Verifica se il tuo backup lo fa e abilitalo (Comandamento 11).
- **Blocca le unità USB esterne:** valuta la politica zero USB. Se fattibile, applicala via GPO come detto. Comunica ai dipendenti che per trasferire dati devono usare alternative (email cifrata, condivisone cloud aziendale come OneDrive/Google Drive, ecc.).
- **Se non blocchi, almeno limita:** imposta almeno "Deny execute" sulle USB. Su Windows puoi usare Applocker o SRP per vietare esecuzione di file da percorsi di tipo "removibile". Inoltre, disattiva l'**AutoRun/AutoPlay** per i dispositivi rimovibili su tutti i PC (c'è una GPO specifica): così se qualcuno inserisce una chiavetta con un virus autoeseguente, non partirà automaticamente.
- **Crittografia dispositivi autorizzati:** se proprio devono usare chiavette, fornisci chiavette aziendali cifrate (con BitLocker To Go, ad esempio). In questo modo, se vengono infettate da un PC esterno, un PC aziendale potrebbe non eseguirne il contenuto se non sblocca la chiave (e comunque se segui il blocco esecuzione, sei doppiamente protetto). Inoltre, se qualcuno copia dati aziendali su una USB cifrata, senza la password non potrà leggerli altrove.
- **Implementa logging utilizzo USB:** attiva sui client l'Auditing degli eventi di "installazione dispositivo" o usa il tuo antivirus/EDR per tenere traccia. Almeno, se succede un incidente, puoi vedere dal registro "chiavetta XYZ collegata al PC di Mario alle 15:30". Questo può dare contesto durante un'indagine.
- **Controlla fisicamente le porte critiche:** sui server e PC più importanti, potresti addirittura usare *physical port blocking*: esistono tappini di plastica con chiave per USB port che impediscono l'inserimento di dispositivi non autorizzati. È una misura più comune in ambienti ad alta sicurezza, ma se hai, ad esempio, un server di produzione che nessuno dovrebbe toccare, inserire quei blocchi fisici USB elimina il rischio di sviste.
- **Sensibilizza i dipendenti:** spiega perché le USB sono pericolose. Racconta storie (ce ne sono tante) di attacchi partiti da chiavette. Introduci una policy "Non collegare dispositivi USB personali ai PC aziendali" e fai capire che anche i gadget tipo caricabatterie USB possono essere alterati (BadUSB). È importante combattere la curiosità (es. chi trova una chiavetta e vuole vedere cosa c'è). Meglio consegnarla all'IT per analisi, se proprio.
- **Aggiorna i controlli con i risultati:** se noti dai log che un certo utente collega spesso chiavette, parlaci: è per lavoro? Ha necessità di trasferire file? Forse puoi offrirgli un canale più sicuro (come uno spazio cloud condiviso col

cliente invece di usare la chiavetta). Insomma, usa le info di monitoraggio per migliorare anche i processi lavorativi riducendo le tentazioni di usare supporti removibili.

Monitorando i file e l'uso delle USB, stai praticamente *installando delle telecamere e sensori di movimento* nel tuo sistema informatico. I ransomware e i ladri digitali lasciano tracce – file che cambiano, dispositivi collegati – e questi sistemi ti permettono di coglierli sul fatto. Non solo: spesso bloccano l'azione prima che degeneri (un po' come un antifurto che suona e ferma il ladro mentre sta forzando una porta). È un altro strato di difesa, complementare agli altri comandamenti, che aumenta notevolmente la resilienza della tua PMI agli incidenti cyber.

7. PATCH REGOLARI & SICUREZZA GESTITA CON MDR

"Se non è rotto, non aggiustarlo" – questo detto *non* vale in informatica. I sistemi potrebbero sembrarti funzionanti, ma nel frattempo nuovi buchi di sicurezza compaiono continuamente. Applicare le **patch regolarmente** è come fare manutenzione all'auto: se salti i cambi d'olio, prima o poi il motore grippa. Allo stesso modo, se non aggiorni software e sistemi, prima o poi un malware sfrutterà quella vulnerabilità lasciata aperta. Le statistiche sono allarmanti: nel 2022 circa **60% delle violazioni di dati e il 76% degli attacchi ransomware sfruttavano vulnerabilità note, per le quali esisteva già una patch disponibile ma non applicata**. Ciò significa che più di *metà* degli incidenti potevano essere evitati semplicemente tenendo aggiornati i sistemi! Ecco perché il patching regolare è un comandamento fondamentale.

Parallelamente, sappiamo che una PMI non può permettersi un Security Operations Center (SOC) interno con analisti 24/7 che monitorano gli allarmi. È qui che entra in gioco il **MDR (Managed Detection & Response)**, un servizio esterno che, semplificando, funge da *sentinella continua* sui tuoi sistemi. Pensa al MDR come un antifurto con la vigilanza privata: tu installi i sensori (software di monitoraggio endpoint) e c'è un team di esperti remoto che sorveglia gli allarmi giorno e notte, pronto a intervenire in caso di intrusione. Per una PMI con un solo IT manager oberato, avere un MDR significa non dover fare i turni di notte per controllare log ed essere avvisati immediatamente se qualcosa non va. **MDR fornisce alle PMI visibilità e risposta agli attacchi 24/7, grazie a esperti esterni e tecnologie avanzate, il tutto a costi molto inferiori a un team interno**.

Vediamo in pratica i due aspetti.

7.1 Patch regolari

Consiste nell'installare tempestivamente le correzioni di sicurezza rilasciate dai fornitori per sistemi operativi, applicazioni, firmware di dispositivi, ecc. "Regolare"

significa che devi avere un ciclo – tipicamente mensile – in cui verifichi e applichi gli aggiornamenti. Microsoft, ad esempio, rilascia patch ogni secondo martedì del mese (Patch Tuesday); altri fornitori hanno cadenze simili. Un buon processo di patch management prevede: tenere d'occhio gli avvisi (newsletter di sicurezza dei vendor, feed RSS, etc.), testare le patch critiche su un paio di macchine, quindi distribuirle su tutte. So che in una PMI il test formale è difficile – spesso si applica direttamente sperando che non ci siano problemi – ma almeno pianifica gli aggiornamenti in orari di basso carico e fai un backup prima (così se qualcosa va storto puoi ripristinare, vedi Comandamento 11). **Prioritizza le patch di sicurezza**: se esce la patch per una vulnerabilità attivamente sfruttata, non aspettare il mese prossimo, applicala subito. Un caso eclatante: la falla di Exchange "ProxyShell" del 2021 – c'erano patch disponibili, chi non le ha messe in fretta si è ritrovato i server compromessi in pochi giorni. Altro esempio: la vulnerabilità di Log4Shell (dicembre 2021) in una libreria Java diffusissima; le aziende che non hanno aggiornato le applicazioni Java con la versione fixata si sono esposte a attacchi gravi. Perciò, serve vigilanza continua.

Sfida budget/tempo: Microsoft Windows può fare aggiornamenti automatici, quindi approfittane – abilita Windows Update su PC e server (magari con rinvio di qualche giorno su server per evitare reboot in orari sbagliati, ma non rimandare di mesi). Per software di terze parti, ci sono strumenti gratuiti tipo **Ninite Updater** o **Patch My PC** (quest'ultimo ha un'edizione free integrabile in Microsoft SCCM) che aiutano a mantenere aggiornati browser, PDF reader, Java, ecc. Non trascurare i dispositivi di rete: il firmware del router, dell'access point Wi-Fi, ecc. Anche quelli vanno aggiornati, magari un paio di volte l'anno controlla sul sito del produttore.

Scenario patching: la **ACME Srl** non aggiornava regolarmente un server Linux esposto in rete. Un ransomware gang ha sfruttato una vecchia vulnerabilità di Apache Struts (come avvenne nel caso famoso di Equifax) e bucato il server, poi pivoting nella LAN. Danno enorme. Se ACME avesse fatto update mensili, quella falla sarebbe stata chiusa tempo prima. Dopo il fattaccio, ACME implementa un rigoroso calendario di patch: ogni secondo venerdì del mese, per due ore, i sistemi vengono aggiornati. Da allora, nessun incidente simile.

7.2 MDR (Managed Detection & Response)

Una volta messe in atto le misure preventive, hai comunque bisogno di sapere se qualcosa sfugge o se un attacco nuovo si infiltra. MDR è il tuo "occhio che non dorme mai". Tipicamente funziona così: scegli un fornitore di MDR, installi sui tuoi endpoint un agente (simile a un antivirus/EDR) che raccoglie eventi e comportamenti sospetti. Questi dati vanno al SOC del provider, dove algoritmi di AI e analisti umani li esaminano. Se viene rilevato qualcosa di anomalo – ad esempio, un processo che somiglia a un nuovo ransomware in azione – intervengono: possono allertarti immediatamente e a volte anche prendere azioni automatiche, tipo isolare la macchina dalla rete. Ad esempio, se alle 3 di notte di domenica un tuo server inizia a

lanciare un tool hacker (Mimikatz per rubare password), il MDR potrebbe bloccarlo sul momento e chiamarti (o seguire il piano di risposta concordato). Così lunedì mattina non trovi la rete già devastata, ma "solo" un incidente contenuto da analizzare.

I vantaggi per le PMI: Costi modulabili (paghi un canone per endpoint, di solito), nessun bisogno di assumere esperti di sicurezza difficili da trovare e mantenere, e soprattutto **copertura costante**. Come citato prima, *il MDR dà accesso a software all'avanguardia e a esperti attivi 24/7, alla portata di una piccola azienda*. Alcuni servizi MDR offrono anche guida proattiva – ad esempio, segnalano configurazioni da migliorare che hanno notato, o ti aiutano a rispondere a un incidente fornendo rapporti e supporto forense. In un certo senso, è come avere un *team di cybersecurity in outsourcing*.

Scenario MDR: la **XYZ Consulting**, con 50 dipendenti, sottoscrive un servizio MDR. Dopo qualche mese, una dipendente apre un PDF maligno ricevuto via email. L'antivirus base non lo riconosce; il malware comincia a esplorare la rete in silenzio. Ma l'agente MDR vede che quel processo PDF sta lanciando comandi anomali e comunica un alert. Gli analisti SOC osservano e in pochi minuti decidono che è un attacco in corso: attivano il blocco isolando il PC e avvisano il referente IT di XYZ, fornendo istruzioni per bonificare. Al mattino il dirigente IT trova già un rapporto dettagliato e la situazione sotto controllo. L'attacco è stato sventato senza impatto sul business, grazie alla guardia notturna degli esperti MDR.

7.3 Strumenti consigliati

- **WSUS o servizi di patch management:** se hai un ambiente Windows con più di qualche PC, potresti usare **WSUS** (Windows Server Update Services) che è incluso in Windows Server, per centralizzare e approvare gli aggiornamenti. In alternativa, servizi cloud come **Microsoft Intune** (in alcuni bundle Microsoft 365 Business) permettono di gestire patch dei device.
- **Automatizza le patch dove possibile:** per sistemi Windows singoli, lascia Windows Update su automatico (magari con orario di attivita personalizzato per evitare riavvii in momenti inopportuni). Per software come Adobe Reader, Chrome, ecc., abilita l'opzione "aggiorna automaticamente". Molti software ormai lo fanno in background. Laddove non c'è auto-update, considerare utilità di terze parti (Ninite, Chocolatey script).
- **Vulnerability Scanner periodico:** potresti utilizzare uno scanner (anche open source come **OpenVAS** o servizi online occasionali) per fare una scansione della tua rete e vedere se rileva vulnerabilità note. Questo aiuta a verificare se qualche patch ti è sfuggita.
- **Newsletter di sicurezza:** iscriviti agli advisory di sicurezza dei vendor chiave (Microsoft Security Bulletins, CERT-AgID in Italia, etc.) così ricevi in email gli avvisi di patch importanti.

- Servizi MDR sul mercato: ce ne sono diversi rivolti alle PMI. Qualche nome: Arctic Wolf, CrowdStrike Falcon Complete, Microsoft Defender Experts/Microsoft MDR (se sei nell'ecosistema MS), Sophos MDR, SentinelOne Vigilance, ecc. Anche alcuni provider locali offrono MDR brandizzato. Confronta un paio di offerte per capire costi e livello di servizio.
- **MDR integrato con EDR:** se hai già investito in un EDR (Endpoint Detection & Response) di fascia alta, vedi se offrono un add-on MDR. Ad esempio, se hai licenze di SentinelOne endpoint, puoi attivare a pagamento il loro team Vigilance. Questo semplifica l'implementazione, poiché hai già gli agent installati.
- **Contratto chiaro e playbook:** quando scegli MDR, discuti e definisci insieme il *playbook* di risposta: vuoi che blocchino attivamente o solo avvisino? Chi contattano e come (telefono, email) in caso di incidente? Quali ore/giorni coperte (molti offrono 24/7 come standard). Assicurati di essere a tuo agio con le procedure e di avere persone reperibili loro fornite per emergenze.

7.4 Checklist operativo

- **Crea un inventario di software/hardware:** elenca tutti i sistemi operativi, software applicativi, dispositivi di rete, etc. per poter tracciare cosa devi patchare. Non dimenticare i "dimenticati" (stampanti, IoT, centralini VoIP…) – se hanno firmware aggiornabile, includili nel piano.
- **Stabilisci un calendario patch:** es. "ogni primo venerdì del mese patch PC, ogni terzo venerdì patch server" oppure simile. Comunica agli utenti che in quelle finestre potrebbero esserci riavvii o brevi downtime (così lo sanno e non protestano troppo).
- **Abilita gli aggiornamenti automatici critici:** su PC client conviene lasciare auto-update attivo e solo gestire quando applicarli (puoi usare criteri per posporre di qualche giorno al massimo). Su server, se vuoi più controllo, notifiche manuali ma esegui comunque entro pochi giorni dal rilascio.
- **Aggiorna applicazioni di terze parti:** non fermarti al sistema operativo. Controlla aggiornamenti per Office, per Java, per i browser, per software di produttività o verticali. Molti problemi di sicurezza derivano da componenti di terze parti (si pensi a Log4j, OpenSSL, ecc.). Mantieni anche questi aggiornati all'ultima versione stabile.
- **Documenta patch e riavvii:** tieni un log di quando hai patchato cosa. Utile per vedere se qualcosa è rimasto indietro e anche per riferimento in caso di audit o assicurazione cyber.
- **Monitora notizie di exploit attivi:** se senti al TG o su siti specializzati di una nuova vulnerabilità critica *attivamente sfruttata* (ad esempio, un "zero-day"

in Windows), esci dalla routine e patcha immediatamente fuori programma. Meglio un piccolo disservizio ora che un attacco riuscito domani.

- **Test di vulnerabilità periodici:** se possibile, ogni 6 mesi fai fare (anche a un consulente esterno) una scansione di sicurezza o un piccolo penetration test. Ti darà la lista di cose da mettere a posto (a volte patch dimenticate o configurazioni errate). Questo serve anche come verifica indipendente dell'efficacia del tuo processo di patching.
- **Valuta e scegli un servizio MDR:** analizza le esigenze della tua PMI. Quanti endpoint hai? Hai solo PC e server on-prem o anche cloud (es. workload su AWS/Azure da monitorare)? Contatta fornitori e chiedi prove gratuite o demo. Molti MDR offrono un trial di 30 giorni. Durante il trial, guarda come funziona il loro portale, la qualità dei loro alert.
- **Implementa l'agente MDR sui dispositivi:** una volta scelto, distribuisci l'agente su tutti i sistemi (può sostituire l'antivirus tradizionale se è un EDR avanzato, oppure affiancarsi). Assicurati che tutti i computer critici siano coperti (compresi eventuali laptop remoti, server virtuali, ecc.).
- **Concorda le procedure di risposta:** discuti con il MDR provider: qual è la soglia di allarme, come vieni coinvolto tu, hanno autorità di isolare macchine automaticamente? Ad esempio, potresti dire: "Se rilevate ransomware, isolate subito e poi chiamatemi; se rilevate una cosa minore, mandatemi un ticket e aspetto mie istruzioni". Avere playbook condivisi riduce i tempi di reazione durante un vero incidente.
- **Integra le notifiche MDR nel flusso IT:** assicurati di ricevere gli avvisi MDR sul canale più comodo (email di lavoro, sms sul cellulare, chiamata). Imposta regole per non perderli (ad esempio, mail d'allarme marcate come importanti). Inoltre, fai in modo di avere reperibilità: se sei l'unico IT e vai in ferie, chi sarà contattato? Indica magari un backup (può essere un dirigente informato del minimo necessario per contattare il fornitore in emergenza).
- **Rivedi i report MDR regolarmente:** i servizi MDR spesso forniscono report mensili sullo stato di sicurezza, con statistiche di attacchi bloccati, vulnerabilità rilevate, ecc. Dedica tempo a leggerli: possono evidenziare punti deboli (es: "abbiamo visto tentativi di exploit su quella macchina con software non aggiornato") e raccomandazioni su misure aggiuntive. Approfitta della loro expertise – stai pagando anche per dei consigli!
- **Continua a fare backup e hardening:** MDR non sostituisce altre misure come backup (Comandamento 11) e segmentazione (Comandamento 12). È un complemento. Anche con MDR, mantieni sempre le best practice: in caso un attacco passasse, avrai i backup; in caso qualcosa sfugga all'analisi MDR, le difese di base (MFA, whitelisting, ecc.) possono comunque mitigare.

In sostanza, questo comandamento unisce la **disciplina delle patch** con la **sorveglianza attiva MDR** per creare un ciclo continuo di protezione. Le patch

chiudono le porte conosciute prima che i criminali le sfruttino; MDR sorveglia le porte nuove o i tentativi di sfondamento e reagisce in tempo reale. Così, anche con una squadra IT minima, la tua PMI può raggiungere un livello di sicurezza paragonabile a organizzazioni ben più grandi. È davvero un caso in cui tecnologia e servizio compensano la mancanza di "teste" sul campo, permettendoti di dormire sonni più tranquilli.

8. GESTIONE SUPERFICIE DI ATTACCO

Sai davvero quanti e quali "ingressi" ha la tua azienda verso Internet? Il cosiddetto **Attack Surface Management (ASM)** riguarda proprio questo: identificare e tenere sotto controllo tutti gli asset digitali esposti esternamente che appartengono alla tua organizzazione, compresi quelli dimenticati o non ovvi. Perché gli hacker li cercano attivamente – un server test dimenticato, una vecchia pagina web non aggiornata, un sottodominio aperto – e sfruttano il primo punto debole che trovano. Molte PMI pensano di avere "il sito web e basta" online, ma poi magari scoprono che c'è anche un vecchio sito di test accessibile, o un servizio cloud attivato da qualcuno senza avvisare l'IT, o ancora record DNS attivi non più in uso.

Il mantra qui è: **non puoi proteggere ciò che non conosci**. Quindi, devi metterti nei panni dell'attaccante e scandagliare la tua presenza online per scovare ogni asset – e successivamente assicurarti che ciascuno sia sicuro o venga spento.

Cosa sono questi asset "nascosti" esterni? Esempi:

- Nomi a dominio registrati dall'azienda (compresi quelli vecchi non più usati).
- Sottodomini DNS attivi (es. old.crm.azienda.it che magari punta a un server decommissionato).
- Server cloud dimenticati accesi su AWS/Azure/GCP. A volte, durante un progetto, qualcuno apre una VM o un servizio PaaS per test e poi se ne scorda.
- Servizi web non evidenti: ad esempio, un'interfaccia di amministrazione di un router accessibile via internet perché nessuno l'ha chiusa; una pagina di login di WordPress all'indirizzo nomesito.it/wp-admin se il tuo sito è WordPress; un database Elasticsearch esposto pubblicamente perché per default ascoltava su tutte le interfacce.
- Indirizzi IP pubblici assegnati all'azienda (spesso il range che l'ISP ti dà). Magari su uno di quegli IP qualcuno ha aperto tempo fa un servizio FTP per un cliente e poi se n'è dimenticato, ed è rimasto senza manutenzione.

Gli attaccanti scandagliano in continuazione internet alla ricerca di queste cose. Sfruttano motori come **Shodan** o **Censys** (che indicizzano dispositivi e servizi esposti) e fanno ricerche sulle aziende. Ad esempio, se la tua PMI si chiama PIPPO,

cercheranno sottodomini tipo vpn.pippo.it, mail.pippo.it, ecc., e vedranno se rispondono.

8.1 Implementare ASM su misura di PMI

La buona notizia è che esistono diversi **tool gratuiti o economici** per fare discovery di asset. Ad esempio, **OWASP Amass** è un tool open-source che fa enumerazione di DNS e subdomain, utile per scoprire sottodomini dimenticati. Puoi usarlo per trovare tutti i *.tuaazienda.com. Poi c'è **Nmap** per scansionare i tuoi IP pubblici alla ricerca di porte aperte. Anche un semplice Google dork, cercando "site:tuaazienda.com" può rivelare pagine indicizzate che non sapevi di avere. Strumenti online come Shodan permettono di inserire il nome dell'azienda o IP e vedere che servizi risultano. Ci sono pure servizi commerciali entry-level: alcuni offrono un report gratuito (come Attaxion nel snippet, con "free external asset discovery report"). L'importante è fare periodicamente questa "ricognizione esterna".

Scenario comune: la **Startup X** lancia un nuovo sito per un prodotto, spostando il dominio principale su un nuovo server, ma dimentica di spegnere il vecchio sito (ancora raggiungibile magari su old.startupx.com). Quel vecchio sito ha una falla non patchata. Un attaccante la scopre e entra nel vecchio server, da lì trova credenziali che funzionano ancora su sistemi interni e colpisce. Tutto ciò, anche se il nuovo sito era sicuro, è avvenuto dal "fantasma" dimenticato online. Un semplice scan DNS avrebbe rivelato la presenza di old.startupx.com e l'azienda avrebbe potuto eliminarlo prima che fosse troppo tardi.

Scenario ASM positivo: Impresa Beta decide di adottare un approccio ASM fai-da-te. Il responsabile IT utilizza strumenti open-source per scansionare la presenza web: scopre un sottodominio sconosciuto test.beta.it che punta a un server di test rimasto acceso. Inoltre, Shodan rivela che sull'IP della sede risponde un servizio remoto sulla porta 8000 (era un server di telecamere di sorveglianza). Grazie a queste scoperte, Impresa Beta mette in sicurezza o chiude questi servizi inattesi: il server di test viene spento e rimosso, il sistema di telecamere viene messo dietro VPN. In futuro, l'IT pianifica scansioni trimestrali per vedere se appare altro (ad esempio quando lanciano nuovi servizi, per verificare che non rimangano porte aperte non documentate).

8.2 Strumenti consigliati per ASM di base

- **Motori di ricerca speciali: Shodan** e **Censys** – inserendo il nome del dominio aziendale possono mostrare host e servizi collegati. Ad esempio, Shodan query: hostname:"azienda.com" potrebbe elencare i sistemi noti.
- **OWASP Amass:** strumento CLI per enumerazione DNS e port scanning rudimentale, utile per scoprire sottodomini e mappare la rete.

- **Nmap:** il celebre port scanner. Esegui una scansione sui tuoi indirizzi IP pubblici (che puoi chiedere al tuo ISP quali sono) con nmap -sV -O <IPrange> per vedere che porte/servizi risultano aperti e la versione (ottimo per scoprire quell'FTP dimenticato o RDP aperto).
- **SecurityTrails / VirusTotal:** siti web che elencano record DNS noti e sottodomini storici. Su SecurityTrails puoi mettere un dominio e vedere sottodomini e vecchi DNS. VirusTotal ha una sezione Intelligence per DNS as well.
- **Google dorking:** come detto, cerca su Google varie combinazioni: site:tuodominio.com, intitle:"Index of /" tuodominio (per vedere se ci sono directory listing aperte), nomeazienda su pastebin (per vedere se ci sono fughe di dati indicizzati).
- **SAS di base (External Attack Surface Scanners):** ci sono servizi cloud gratuiti come **Firefox Monitor** o **HaveIBeenPwned** per controllare se le email aziendali sono comparse in breach (così sai se cambiare password di certi account). O anche strumenti di scanning come **Intruder** o **Pentest-Tools** che offrono trial per scansioni esterne.
- **CISA Cyber Hygiene (per USA):** se la tua azienda operasse negli USA, CISA offre scanning gratuiti dell'infrastruttura (vulnerability scanning). In Italia, il CERT nazionale offre a volte servizi simili per infrastrutture critiche; per PMI generiche c'è meno, ma puoi informarti su iniziative regionali.

8.3 Checklist operativo

- **Recupera l'elenco domini e IP:** fai una lista dei domini che l'azienda possiede (anche non attivi) e degli IP pubblici assegnati. Se non sei sicuro degli IP, chiedi all'ISP un riepilogo o usa un servizio come bgp.he.net cercando l'AS della tua azienda (se ha un proprio AS) o il nome. Anche siti come SecurityTrails possono dare gli IP storicamente collegati al tuo dominio (es. IP del sito attuale e precedente).
- **Esegui enumerazione DNS:** con uno strumento (Amass o servizi online) ottieni la lista dei sottodomini attivi. Controlla ognuno: quello che non riconosci va indagato. Se trovi old, test, dev ecc., verifica se corrispondono a server reali e decidi se vanno chiusi.
- **Scansiona gli IP per servizi aperti:** usa Nmap o affini per vedere quali porte rispondono su ciascun IP. Documenta i risultati: per ogni porta/servizio aperto, chiediti: "lo aspettavo? È autorizzato?". Se no, chiudi quella porta sul firewall o disabilita il servizio. Se sì, assicurati che sia aggiornato e messo in sicurezza (per esempio, se vede https aperto su un IP che corrisponde al portale VPN SSL aziendale, ok, ma controlla che il software VPN sia patchato e con MFA).

- **Esamina i risultati Shodan/Censys:** vedi se segnalano qualcosa che la tua scansione non ha colto, come certificati SSL noti su sottodomini. Shodan può mostrare versioni di software, prendi nota di eventuali vecchie versioni (es. “Apache 2.4.1” obsoleto -> patchalo).
- **Fai pulizia di ciò che non serve:** qualsiasi asset non usato = spegnilo. Siti web vecchi: se ti servono per archivio, mettili offline (anche un backup su disco), ma non lasciarli online. Macchine cloud non utilizzate: spegnile per risparmiare costi e ridurre rischio. Record DNS orfani: rimuovili (eviti attacchi di takeover di subdomain).
- **Proteggi quello che rimane:** gli asset esterni inevitabili (sito pubblico, VPN gateway, server mail, ecc.) devono essere fortificati: patch, config sicura, test di penetrazione se possibile. Questo rientra negli altri comandamenti (patching, MFA su accessi, etc.).
- **Ripeti periodicamente la ricognizione:** mettiti un promemoria ogni 3 mesi per rifare almeno una scansione sommaria: magari nel frattempo qualcuno in azienda ha registrato un nuovo dominio per marketing, o un nuovo servizio è stato pubblicato senza che tu fossi coinvolto. Uno scanning trimestrale ti permette di scoprirlo e integrarlo in sicurezza.
- **Monitora i certificati e menzioni online:** puoi usare servizi come **CRT.sh** per vedere quando viene emesso un certificato per un tuo dominio (utile per scoprire sottodomini nuovi). O mettere Google Alert sul nome dell’azienda nel caso venga citata in contesti hacker (ad esempio forum di leak).
- **Coinvolgi l’azienda:** fai sapere ai colleghi che l’IT deve essere informato quando si attiva qualcosa di nuovo online (es: se marketing vuole un nuovo sito evento e registra dominio, che lo dicano). Crea una procedura interna: “Catalogo degli asset digitali” e aggiornatelo di pari passo col business.
- **Considera servizi ASM professionali se cresce la complessità:** se la tua PMI diventa più grande e si muove molto sul cloud, valutare soluzioni attacco superficiale as a service può aiutare (ti danno un portale dove vedi costantemente i tuoi asset, punteggi di rischio, avvisi di nuove esposizioni). Alcuni nomi: Palo Alto Xpanse, Microsoft Defender EASM, Rapid7, ecc. Ma per realtà piccole spesso non è necessario, un po’ di script e buona organizzazione bastano.

Con l’ASM stai in pratica accendendo la luce su tutto il perimetro esterno dell’azienda. Invece di lasciare agli hacker la sorpresa di trovare un porticina aperta, la trovi tu e la chiudi o la sorvegli. È un lavoro investigativo che richiede metodo, ma le PMI che lo adottano riducono enormemente i rischi di quei tipici attacchi “di opportunità” dove l’attaccante colpisce perché ha trovato qualcosa di facile. Diventi un bersaglio molto meno facile perché **sai cosa hai esposto e provvedi a metterlo in sicurezza**.

9. ZERO-TRUST E "JUST IN TIME" (JIT)

Il modello di sicurezza tradizionale era a "mura e fossato": dentro la rete aziendale tutti (o quasi) si fidano, fuori no. **Zero Trust** ribalta questo concetto: *non fidarti di niente e nessuno di default, verifica sempre, concedi solo i permessi minimi e se necessario*. In pratica, Zero Trust è un insieme di principi architetturali che includono molti punti di cui abbiamo già parlato (MFA ovunque, segmentazione, least privilege, monitoraggio continuo). Qui focalizziamo sull'aspetto "**just-in-time (JIT)**" e "just-enough-access (JEA)" per gli accessi privilegiati. Significa che se qualcuno ha bisogno di un accesso elevato o a una risorsa critica, gli viene concesso **solo nel momento in cui serve e solo per la durata necessaria**, poi l'accesso viene revocato automaticamente.

Immagina un amministratore IT che ha i diritti Domain Admin 24/7 sul dominio Windows (situazione classica): se il suo account viene compromesso anche solo per un attimo, gli hacker hanno massimi privilegi in ogni momento. Con un approccio JIT, quell'amministratore userebbe il suo privilegio solo quando ne ha bisogno: ad esempio tramite un sistema che "eleva" il suo account per 1 ora per fare una certa attività, poi lo riporta a utenza normale. Così se un attaccante rubasse le sue credenziali al di fuori di quella finestra, non potrebbe fare danni perché non sarebbero più admin.

Zero Trust in senso lato vuol dire anche *non fidarsi della rete interna*: ogni accesso a un'applicazione va autenticato e autorizzato come se venisse da Internet, ogni dispositivo che si connette deve essere verificato (è un PC aziendale conforme o un laptop sconosciuto?). Questo riduce i movimenti laterali: se un malware infetta un PC, non è che può automaticamente parlare con tutti gli altri – dovrà comunque superare controlli di identità e device per accedere alle risorse.

Vediamo un caso pratico: **Azienda Alfa** senza Zero Trust: un dipendente una volta loggato in VPN entra in rete e può contattare liberamente tutti i server di produzione senza ulteriori controlli. Se quel dipendente viene attaccato, l'hacker in VPN ha campo libero su tutto il dominio. **Azienda Beta** con Zero Trust: ogni volta che il dipendente in VPN cerca di accedere al server di produzione o a un'app, deve passare per un gateway che verifica chi è, se ha MFA valido, se il suo device è aggiornato e autorizzato, e concede accesso solo a quella specifica risorsa. Il malintenzionato, anche rubando la sessione VPN, troverebbe altre barriere (MFA richiesto di nuovo, device trust mancante) e non riuscirebbe a muoversi liberamente.

9.1 Implementazione JIT/PAM in PMI

Un modo semplice è quanto già discusso: usare account admin separati e loggarsi con essi solo quando serve (questo è già una forma manuale di JIT). Ma esistono strumenti per automatizzare: ad esempio, **Azure AD Privileged Identity**

Management (PIM) se usi Microsoft 365/Azure, permette di rendere gli account amministrativi "eligibili" ma non attivi; quando devi fare una modifica admin, attivi il ruolo admin tramite PIM (magari con una giustificazione e un secondo fattore), usi il ruolo per 1 ora poi scade. Così normalmente non sei admin. Questo riduce la finestra temporale di esposizione. Altri strumenti di Privileged Access Management (PAM) per PMI includono soluzioni come **Delinea (Thycotic) PAP** che fornisce vault di password e rilascio just-in-time di credenziali ad alti privilegi. Se questi nomi suonano complessi per una PMI, l'idea chiave è: nessun utente (nemmeno il CEO o l'IT) dovrebbe avere accessi illimitati per default, a meno che non stia effettivamente svolgendo un compito che lo richiede *in quel momento*.

Implementazione Zero Trust di base: Non serve comprare subito costose piattaforme. Inizia estendendo il concetto di "verifica continua" dappertutto. Ad esempio:

- Abilita l'MFA *anche* per accessi interni alle applicazioni sensibili, non solo dall'esterno (molti servizi cloud lo fanno di default; per app interne, valuta identity federation con Azure AD o simili per avere MFA anche internamente).
- Rendi minimi i privilegi come abbiamo fatto (Comandamento 4) – Zero Trust = zero fiducia implicita negli utenti.
- **Micro-segmenta**: limita quale rete o utente può parlare con quale servizio (collegato a Comandamento 12).
- **Logga e monitora** tutte le attività: in Zero Trust si assume che prima o poi l'attaccante entri, quindi devi poterlo individuare da comportamenti anomali (es. utente marketing che tenta di accedere al server contabile, come mai?).
- **Gestione dispositivi**: implementa se possibile un controllo su quali dispositivi accedono alle risorse. Ad es., permetti accesso a file condivisi solo se il PC è parte del dominio e aggiornato. Molte PMI stanno adottando strumenti di MDM (Mobile Device Management) leggeri o soluzioni come Microsoft Intune che assicurano compliance dei dispositivi.

Scenario Zero Trust: la **SoftwareGamma** ha dipendenti in smart working e adotta Zero Trust Network Access (ZTNA) invece della VPN classica. In pratica, i dipendenti per accedere alle applicazioni aziendali vanno su un portale sicuro, fanno login MFA, e vengono connessi specificamente all'app richiesta (ad esempio database CRM) senza mai avere accesso all'intera rete. Un hacker che rubasse le credenziali troverebbe comunque l'MFA come ostacolo e, anche superandolo ipoteticamente, vedrebbe solo quell'app specifica, non l'intera LAN. Questo confinamento riduce di molto i danni potenziali.

9.2 Strumenti consigliati

- **Azure AD + PIM:** se hai Microsoft 365 Business Premium o E5, hai Azure AD P2 che include Privileged Identity Management. Ottimo per gestire amministratori con JIT.
- **Vault password con checkout temporaneo:** soluzioni come **KeePass** in locale (se ben gestito) o servizi come LastPass Enterprise / 1Password Business hanno funzioni di condividere password admin solo quando richiesto. Ad esempio, l'IT tiene le credenziali dei server in un vault; se un tecnico deve accedervi, prende la password e la rotazione automatica può cambiarla dopo.
- **Google BeyondCorp / Cloud Identity:** se siete ecosistema Google, loro spingono la loro architettura Zero Trust (BeyondCorp). Magari overkill per PMI, ma alcune funzionalità di Context-Aware Access su Google Workspace permettono di limitare accesso in base a posizione/device.
- **Okta o altri IdP con adaptive MFA:** un Identity Provider esterno come Okta, OneLogin, JumpCloud, può unificare login e applicare policy zero trust (es. re-authenticate utente se il contesto cambia, come se improvvisamente da Milano la sessione appare in Brasile, scatta nuova verifica). Sono servizi a pagamento, ma per PMI con molte app cloud può valere la pena per centralizzare la gestione identità e applicare regole uniformi.
- **Soluzioni ZTNA emergenti:** alcuni firewall (Zscaler, Cloudflare for Teams) offrono servizi che rimpiazzano la VPN con accesso zero trust alle singole applicazioni interne. Ad esempio, Cloudflare Access consente di mettere dietro una sorta di proxy le tue applicazioni web interne e farle accedere solo con login IdP (Identity Provider) e criteri. Può essere interessante se hai molte risorse on-prem e utenti remoti.
- **Attitudine "Assume Breach":** più che uno strumento, è un mindset. Adotta pratiche di simulazione attacco (es. lancia un finto attacco interno e vedi se i controlli zero trust lo fermano). E preparati: se un aggressore interno c'è già (breach), come lo limiti? Zero Trust è come compartimentare una nave: se una stiva prende acqua, le paratie impediscono affondamento.

9.3 Checklist operativo

- **Analizza i flussi di accesso attuali:** mappa chi accede a cosa e da dove. Identifica punti deboli: ad esempio, utenti in LAN che accedono a server critici senza reautenticazione; account amministrativi sempre attivi; dispositivi personali dei dipendenti che accedono a risorse aziendali senza controlli. Questi saranno i target iniziali per Zero Trust.
- **Implementa MFA ovunque possibile:** se ci sono applicazioni interne senza MFA, valuta di metterle dietro una soluzione di identity (p. es. Azure AD App Proxy, che permette di richiedere login Azure AD+MFA prima di inoltrare

all'app interna). Per servizi legacy non integrabili, almeno gestisci l'accesso di rete (solo da IP specifici o PC aziendali).

- **Rivedi i privilegi e ruoli:** applica il principio di *just-enough-access*. Chi deve vedere un certo dato, lo vede, ma nulla di più. Questo può voler dire creare nuovi ruoli nelle applicazioni con permessi più granulari. Spesso nelle PMI tutti sono "admin" di un software per comodità: correggi questo, dai utenti normali e uno o due admin veri.
- **Attiva JIT per admin:** se hai Azure AD PIM, usalo. Altrimenti, pratica manuale: tieni account admin disabilitati e abilitali solo quando servi tu (lo so, manuale ma già efficace). Oppure adotta un tool leggero come PowerShell script che aggiunge temporaneamente un utente al gruppo Administrators Domain per 1 ora e poi lo rimuove. Ci sono script community per farlo.
- **Segmenta risorse (microsegmentation):** (collegato al Comandamento 12) Crea regole firewall interne per limitare chi parla con chi. Ad esempio: i PC utenti non devono mai contattare direttamente il server database – devono passare attraverso l'applicazione server. Quindi blocca la porta DB dal segmento utenti. In Zero Trust, di base *"deny all lateral movement"* finché non è esplicitamente autorizzato.
- **Verifica i dispositivi:** se puoi, implementa una forma di controllo dispositivo per le risorse sensibili. Ad esempio, attiva BitLocker su tutti i portatili (così Zero Trust fisico: se rubano un pc, i dati sono cifrati). Usa Intune (se M365) per almeno marcare i dispositivi aziendali ed eventualmente condizionare accessi (Conditional Access) solo a device conformi (antivirus attivo, disco cifrato, etc.). In mancanza di MDM, potresti fare controlli manuali periodici e inserire clausole di policy (es. "non accedere al gestionale da PC personali non approvati").
- **Mai fidarsi di sessioni lunghe:** configura time-out brevi per applicazioni critiche. Se un'utente è loggato al CRM e resta inattivo 15 minuti, fai sì che debba riloggarsi. Questo riduce finestre in cui una sessione compromessa può essere sfruttata.
- **Log e anomaly detection:** potenzia il logging su autenticazioni e accessi. Zero Trust implica monitoraggio costante. Se hai un sistema MDR (Comandamento 7), concorda con loro l'analisi di comportamenti strani di utenti validi (es. un dipendente marketing che prova ad aprire 100 file in cartella HR in 5 minuti – può essere qualcuno che usa sue credenziali impropriamente).
- **Formazione Zero Trust:** spiega in azienda che verranno introdotte misure extra di verifica non per sfiducia verso di loro, ma per protezione. Ad esempio, se chiedi di rifare login più spesso o di usare il telefono per MFA anche in ufficio, contestualizza dicendo che è per prevenire che un eventuale intruso interno possa muoversi liberamente. La cultura zero trust deve essere compresa per non generare boicottaggi o tentativi di aggirare.

- **Aggiorna procedure accesso fornitori/terze parti:** se hai consulenti esterni che accedono ai sistemi, applica anche a loro Zero Trust: account dedicati, attivati solo quando serve (JIT), con scadenza. Ad esempio, il consulente IT ha un account che abiliti giusto il giorno che deve fare manutenzione e poi disabiliti. Non lasci account dormienti attivi.
- **Misura i progressi:** Zero Trust completo è un ideale, ma man mano che implementi parti (MFA qui, segmentazione là, JIT su ruoli) verifica l'effetto. Vedi se gli utenti iniziano davvero a avere solo ciò che serve (nessuno oltrepassa più risorse che non deve). Se possibile, conduci un piccolo test: fai provare a un dipendente esperto di accedere a risorse a cui non dovrebbe e vedi se i controlli lo fermano.

Abbracciando Zero Trust e JIT, la tua PMI adotta una postura "paranoica sana": *"Non mi fido finché non ho verificato"*. Questo limita drasticamente i movimenti di un eventuale attaccante interno e riduce l'impatto di account compromessi. Per te, amministratore, può voler dire un po' più di attenzione nella gestione quotidiana (accendere accessi quando servono, controllare dashboard di sicurezza), ma il beneficio è enorme in termini di resilienza. In un mondo dove gli attacchi diventano sempre più sofisticati, Zero Trust è diventato il nuovo gold standard – tanto che governi e grandi aziende lo stanno adottando in massa. Farlo anche in piccolo, con gli strumenti adeguati, significa portare la tua sicurezza a un livello superiore, proiettato nel futuro.

10. FORMAZIONE PERSONALE

Abbiamo parlato di molte tecnologie e politiche, ma non dimentichiamo mai che **la prima linea di difesa (o di falla) sono le persone**. Secondo un celebre rapporto Verizon, nel 2022 **l'82% delle violazioni ha coinvolto il "fattore umano"** – errori, credenziali rubate, phishing riusciti, comportamenti scorretti. Puoi avere il miglior firewall e antivirus, ma se un dipendente apre la porta al nemico cliccando dove non deve, tutto può essere vano. Ecco perché la **formazione del personale** in materia di cybersecurity è un comandamento imprescindibile.

Cosa significa in pratica formazione? Non parliamo di trasformare tutti in tecnici informatici, ma di instillare **consapevolezza**: riconoscere un'email sospetta, capire perché una chiavetta USB trovata potrebbe essere un cavallo di Troia, scegliere password robuste (o meglio usare un password manager), non farsi ingannare da telefonate di finti tecnici, e così via. È far sì che ogni collaboratore diventi una sorta di "sensore di sicurezza" anziché un anello debole.

10.1 Argomenti chiave da coprire

- **Phishing:** spiegare cos'è, mostrare esempi reali, dare indicazioni su come riconoscerlo (mittente strano, errori grammaticali, urgenza sospetta, link mascherati). Questo riduce la probabilità che clicchino link malevoli o inseriscano credenziali in siti fake.
- **Allegati pericolosi:** insegnare a diffidare di allegati non attesi, soprattutto .exe, .zip con password, documenti Office che chiedono di abilitare macro. Incoraggiare a verificare col mittente con una telefonata se sembra sospetto.
- **Uso di password e MFA:** enfatizzare di non riutilizzare password aziendali per siti personali, di usare password manager fornito dall'azienda se disponibile, e ovviamente la buona pratica dell'MFA ovunque (già imposto tecnicamente ma far capire perché, per evitare resistenze).
- **Navigazione web sicura:** suggerire di evitare siti pirata/streaming illegale sul PC aziendale (spesso veicolo di malware), stare attenti a pop-up e truffe online (ad es. finte finestre "il tuo computer è infetto, clicca qui").
- **Social engineering generale:** raccontare casi in cui qualcuno chiama fingendo di essere dell'IT chiedendo la password (devono sapere che l'IT **non chiederà mai la password in chiaro**), o finti corrieri che chiedono di inserire credenziali su un link. Fornire semplici regole: *"quando in dubbio, chiedi all'IT prima di fare qualunque cosa"*. Meglio una domanda in più che un incidente.
- **Uso corretto degli strumenti di lavoro:** includi policy su installazione di software (non installare programmi senza autorizzazione), su uso di cloud personali (non caricare file aziendali su Google Drive personale, ad esempio, senza permesso), su come trattare dati sensibili (GDPR docet).
- **Cosa fare se sospetta un problema:** importantissimo! I dipendenti devono sentirsi a loro agio nel segnalare un possibile incidente o errore. Devono sapere a chi rivolgersi subito (es: "chiama il responsabile IT immediatamente se pensi di aver aperto un malware o se il PC si comporta in modo strano"). E assicurali che non saranno puniti per aver ammesso un errore – meglio saperlo subito e mitigare.

10.2 Modalità di formazione

Non serve organizzare costosissimi corsi in aula (anche se un seminario annuale con un esperto ospite può essere utile). Puoi fare cose agili:

- **Bollettini mensili via email:** una mail breve con una pillola di sicurezza ("Questo mese vediamo come riconoscere un falso SMS del corriere..."). Mantienilo leggero e non tecnico.
- **Poster e infografiche in ufficio:** un poster vicino alla macchinetta del caffè con "Le 5 regole d'oro per email sicure" può tenere alta l'attenzione.

- **Sessioni brevi in riunione:** ogni tot, prendi 15 minuti di una riunione aziendale per raccontare un caso reale (magari una truffa successa a un'azienda nota, di solito attirano l'attenzione). Le storie concrete restano più in mente.
- **Simulazioni di phishing:** esistono piattaforme (es. KnowBe4, PhishingBox) o puoi farle tu artigianalmente, che inviano finti phishing al personale per testare e insegnare. Ad esempio, mandi a tutti una mail fasulla abbastanza credibile; chi clicca viene indirizzato a un breve messaggio "Era un test di phishing, ecco cosa potevi notare per evitarlo...". Queste simulazioni vanno fatte con tatto, non per punire ma per educare (magari un concorso: chi non clicca mai in 6 mesi riceve un piccolo premio simbolico, e chi sbaglia ripete training).
- **Coinvolgimento attivo:** magari nomina alcuni "Security Ambassador" tra i vari reparti – persone un po' più sensibili al tema che aiutino i colleghi e facciano da punto di riferimento.
- **Aggiornamenti costanti sulle minacce emergenti:** se c'è notizia di una truffa diffusa (es. ondata di email che fingono fatture da ENEL con allegato virus), avvisa subito i dipendenti "Guardate che sta girando questa mail, fate attenzione e non apritela se la ricevete". Mostrare reattività li fa sentire protetti e li abitua a stare all'erta.

Scenario di successo: alla **Contoso Inc.**, dopo un paio di anni di programma di awareness, un impiegato riceve una mail sospetta che sembra dal CEO che chiede un bonifico urgente. In passato forse qualcuno l'avrebbe eseguito per paura reverenziale; ora quell'impiegato ricorda la formazione ("verificare sempre richieste finanziarie fuori routine") e telefona al CEO – il quale casca dalle nuvole e ringrazia per aver bloccato una probabile frode (Business Email Compromise). Un altro esempio: la stagista in amministrazione riceve un file .xls che chiede macro, lei immediatamente pensa "uh, ci hanno detto che le macro sono pericolose" e non le abilita, inoltrando la mail all'IT per verifica. L'IT conferma che era Emotet. Ecco, due incidenti evitati grazie alla prontezza degli utenti.

10.3 Strumenti e risorse per formazione

- **Kit di sensibilizzazione gratuiti:** il sito di **CISA** ha materiale (poster, infografiche) in inglese; l'**ENISA** (agenzia europea) pubblica ogni anno contenuti per il Mese Europeo della Sicurezza Informatica (ottobre). Organizzazioni come **Sans** offrono newsletter come "Ouch! Security" (anche tradotta in italiano a volte).
- **Video e corsi online brevi:** su piattaforme come YouTube trovi video semplici sul phishing, magari usarne alcuni durante una sessione interna. Oppure creare tu un breve screencast mostrando un esempio di phishing reale ricevuto (ovviamente anonimizzando).

- **Gamification:** si possono fare piccoli quiz ogni tanto con premio: tipo, invii un quiz di 5 domande (es. “Come riconosci un sito web sicuro?”) e chi risponde correttamente entra in estrazione per un buono regalo. Così li incoraggi a partecipare attivamente.
- **Policy scritte ma leggibili:** fornisci un documento di “Policy di sicurezza informatica per dipendenti” che non sia legalese, ma chiaro e con esempi: è una base su cui fare formazione e anche uno strumento di riferimento.
- **Supporto di direzione:** assicurati che il management supporti queste iniziative, partecipando essi stessi (se il capo per primo segue la formazione, tutti capiranno che è importante). E che diano tempo: ad esempio, dedicare quell’ora per un workshop non venga visto come tempo perso, ma come investimento.

10.4 Checklist operativo

- **Stabilisci un programma annuale:** pianifica con anticipo alcune attività in modo da coprire i temi principali. Es: Q1 phishing, Q2 password/MFA, Q3 protezione dati, Q4 sicurezza fuori dall’ufficio (remote working). Pianificalo come faresti per qualsiasi formazione obbligatoria (tipo sicurezza sul lavoro).
- **Ottieni supporto del top management:** presenta ai dirigenti le statistiche sugli attacchi e come l’errore umano pesa. Spiega che anche loro sono bersagli (il phishing ai CEO ad esempio, chiamato “whaling”). Ottenuto l’accordo, fai magari firmare da loro un messaggio di endorsement: “Tutti i dipendenti devono partecipare a questo sforzo per tenere l’azienda al sicuro…”.
- **Sviluppa materiale adatto alla tua realtà:** se la tua PMI è nel settore sanitario, porta esempi di phishing su temi sanitari; se in industriale, esempi di finte email di fornitori di componenti. Più è calato nella realtà dei lavoratori, più sarà efficace.
- **Esegui una sessione di kick-off dal vivo:** se possibile, un incontro iniziale con tutti (anche via webinar) dove spieghi perché la sicurezza è responsabilità di tutti, racconti qualche aneddoto, e presenti il programma. Questo serve a creare consapevolezza iniziale.
- **Usa simulazioni di phishing etico:** se decidi di fare campagne simulate, informane la direzione e magari il responsabile HR (per gestire feedback nel caso qualcuno si offenda di essere “ingannato”). Dopo ogni simulazione, invia a tutti (non solo a chi è caduto) un’analisi dell’email phishing e i segnali per riconoscerla, in modo che tutti imparino.
- **Monitora i progressi:** ci sono metriche semplici: % di dipendenti che fanno corsi e quiz, % di click al phishing (che idealmente calerà col tempo), numero di incidenti reali dovuti a errori umani (si spera zero se la formazione funziona). Condividi qualche risultato nei meeting (es. “questo trimestre 0

click su 3 email simulate, bravissimi!" oppure "abbiamo ridotto del 50% i casi di richieste strane segnalate, segno che c'è più attenzione").

- **Rendi la formazione continua:** non pensare sia una tantum. La sicurezza evolve e l'attenzione scema col tempo se non rinnovata. Prevedi refresh annuali e aggiornamenti quando ci sono nuove minacce.
- **Crea un clima aperto:** ringrazia sempre un dipendente che segnala qualcosa di sospetto, mai ridicolizzarlo. Crea fiducia: meglio chiamare per nulla che tacere un malware per paura. Puoi istituire un canale diretto (tipo un email sicurezza@azienda o un gruppo Teams) dove possano inviare dubbi su email strane ecc., garantendo risposte rapide.
- **Allinea la formazione con le policy:** se hai policy interne (es. "divieto di usare Dropbox personale per dati aziendali"), assicurati di spiegarne il perché nella formazione. Le persone rispettano più volentieri le regole se ne capiscono la ragione e le conseguenze.

In sintesi, la formazione del personale trasforma ogni collaboratore da potenziale bersaglio a **parte attiva della difesa**. La cultura della sicurezza diventa parte della cultura aziendale. Questo comandamento è forse il più "umano" ma, combinato con le contromisure tecniche, è quello che **cementa veramente** la sicurezza a 360 gradi. Un dipendente attento può fermare un attacco dove la tecnologia magari non l'ha intercettato immediatamente, oppure può evitare proprio che succeda (non cliccando, non inserendo password in giro). Come recitava uno slogan: *"La sicurezza inizia da te"* – in una PMI tutti devono poterlo dire. E con un buon programma di awareness, lo diranno.

11. BACKUP CIFRATI REGOLARI

Immagina il peggior scenario: nonostante tutte le difese, un ransomware riesce a colpire e cifra i tuoi file aziendali. A video compare la richiesta di riscatto: "Paga 50.000€ entro 5 giorni o i tuoi dati andranno persi per sempre". Cosa fai? Se hai seguito questo comandamento, la risposta è semplice: **ripristino i backup e mando al diavolo i criminali**. Avere backup aggiornati, integri e possibilmente offline significa che anche nella peggiore delle ipotesi non sei in balia degli estorsori. Non è un caso che un mantra della cybersecurity sia *"Backup, backup, backup!"*.

Ma attenzione, i backup oggi devono essere fatti con criterio, altrimenti rischiano anch'essi di essere cifrati dal ransomware o rubati da un attaccante. Ecco perché parliamo di **backup regolari e cifrati**. Approfondiamo:

11.1 Backup regolari

Stabilisci una frequenza adeguata alle esigenze. Per la maggior parte delle PMI, un backup giornaliero dei dati critici è un buon punto di partenza. Se generi molti dati (es.

database in continuo aggiornamento), valuta backup orari o replicazione continua, ma per molti basta una volta al giorno la notte. L'importante è essere disciplinati e **automatizzare**: se conti sul backup manuale, prima o poi salta. Usa software di backup o script pianificati. E non limitarti ai file: se hai macchine server virtuali, considera backup dell'intera VM; se hai email in cloud, valuta backup delle caselle (sì, anche Microsoft 365/Google hanno opzioni di backup di terze parti perché il loro "backup" è limitato a versioning breve, e non copre cancellazioni malevole su lungo periodo).

11.2 Backup cifrati

Quando salvi dati di produzione in un backup, stai di fatto creando una copia completa delle tue informazioni – se finisse nelle mani sbagliate sarebbe un disastro di pari livello. Quindi **crittografa i backup**. Molti software di backup permettono di impostare una password di cifratura per i set di backup. Così, anche se un attaccante rubasse i tuoi file di backup, senza la chiave non potrebbe leggerli. Questo è vitale soprattutto per backup portati offsite o su cloud. Ad esempio, se metti i backup su un disco USB che porti fuori sede, cifra quel disco (BitLocker To Go è ottimo per questo). Se usi un servizio cloud tipo Amazon S3 per backup, abilita la cifratura lato server e/o cifra prima di inviare.

Offline/offsite backups (la regola 3-2-1): spesso citata: *3 copie dei dati, su 2 media diversi, 1 offsite*. Questo perché se tieni tutti i backup accanto ai dati originali, rischi di perderli in uno stesso evento (incendio, allagamento, furto). E se i backup sono sempre online e accessibili dalla rete, un ransomware moderno proverà a cancellarli o criptarli (ci sono varianti che cercano unità di rete e backup connessi). **CISA** raccomanda espressamente backup **offline e isolati** dalla rete proprio per prevenire ciò. Quindi, prevedi almeno una copia dei backup che non sia raggiungibile dal normale accesso di sistema: ad esempio, un disco USB che dopo il backup vien scollegato e messo in cassaforte, o backup su nastro (ancora utilizzati in certi contesti proprio per la loro immunità a malware online), o backup su cloud con credenziali separate non note sul network locale.

11.3 Test dei backup

avere backup è fantastico, ma **saperli ripristinare** è altrettanto importante. Troppe storie di aziende con backup corrotti o incongruenti scoperti solo quando servivano. Programma dei test periodici: scegli alcuni file a caso e provane il restore; o meglio, fai una simulazione di disaster recovery su una macchina isolata – tipo prendi l'ultimo backup server contabilità e prova a montarlo su una VM di test, vedi se funziona. Questo esercizio dà confidenza e scopre eventuali problemi.

Scenario positivo (con backup): la **Delta Srl** subisce un attacco ransomware venerdì notte. Lunedì mattina i file sul server sono cifrati, ma loro hanno backup offline fino a venerdì 18:00. Dopo aver bonificato i sistemi dall'infezione, avviano il ripristino dei

dati di venerdì sera: in poche ore tornano operativi, perdendo giusto mezza giornata di lavoro (che possono reinserire a mano). Nessun riscatto pagato, i criminali restano a bocca asciutta e Delta Srl riparte quasi indenne.

Scenario negativo (senza backup): la **Omega SAS** invece non faceva backup seri da mesi ("ci penseremo più avanti..."). Colpiti dallo stesso ransomware, perdono tutto il database clienti, anni di documenti, e l'unica speranza è pagare. Pagano il riscatto, ma i criminali – sorpresa – non forniscono una decrittazione completa o magari se ne vanno con i soldi e basta. Omega non riesce a recuperare i dati, perde clienti e viene pure multata perché aveva perso dati personali dei clienti. Un vero disastro, tutto perché non c'era un backup.

11.4 Strumenti per backup PMI

- **Software di backup dedicati:** ce ne sono gratuiti e commerciali. Ad esempio **Veeam** ha una Community Edition gratuita (fino a 10 istanze) molto valida, che fa backup di VM, server fisici e workstation. **UrBackup** open-source per file server. **Windows Server Backup** integrato in Windows Server per backup locali. Scegli in base a esigenze; l'importante è configurare pianificazioni automatiche e verificare le notifiche di successo/fallimento.
- **Backup su cloud**: servizi tipo **Backblaze**, **Acronis Cloud Backup**, **Carbonite** offrono spazi cloud e software per fare backup sicuri su loro datacenter (spesso con cifratura e versioning). Hanno costi mensili ma togli il pensiero di dove tenere i backup offsite. Attenzione solo alla banda: assicurati di avere una linea abbastanza veloce se devi mandare tanti GB su cloud regolarmente.
- **Backup su NAS con snapshot immutabili:** se hai un NAS (Synology, QNAP...), sfrutta la funzione di snapshot. Alcuni NAS permettono di creare copie di backup di sola lettura immodificabili per X giorni. Così anche se un ransomware accede al NAS, non può alterare le snapshot. Occhio però: il NAS deve essere anch'esso ben protetto (utente admin del NAS con MFA e non accessibile dalla rete dei PC).
- **Cifratura backup:** BitLocker per dischi USB, oppure nei software di backup imposta password di encryption. Usa una password robusta e conservala in luogo sicuro (se la perdi, perdi i backup!). Se usi cloud, spesso puoi scegliere di tenere tu la chiave di cifratura (così nemmeno il provider può leggere i dati).
- **Rotazione supporti:** se usi dischi esterni, adotta almeno 2 o 3 dischi in rotazione (es. backup dispari su Disco A, pari su Disco B, e uno Offsite C come ciclo settimanale). Così se un disco si guasta o viene compromesso, hai gli altri. Non tenere i dischi sempre connessi.
- **Backup di Microsoft 365/Google Workspace:** attenzione, molti pensano "è nel cloud, è al sicuro". Vero che Microsoft e Google hanno alta disponibilità, ma se un attaccante cancella o cifra file su OneDrive di un utente, quelle

cancellazioni si sincronizzano. Ci sono soluzioni specifiche (Spanning Backup, Veeam O365, etc.) per fare backup delle mailbox e file cloud su altro storage, con retention lunga. Valuta di implementarle per poter recuperare email o file di mesi fa se rimossi.

11.5 Checklist operativo

- **Identifica i dati critici:** cosa va assolutamente salvato? Esempi: cartella documenti e contratti, database gestionale, caselle email, configurazioni server, codice sorgente, ecc. Fai la lista di questi dataset e dove risiedono.
- **Scegli la strategia di backup per ciascuno:** potrebbe essere diversa. Esempio: file server e database su NAS – backup giornaliero su disco USB + replica su cloud; caselle email – backup settimanale su cloud con tool X; VM server – snapshot locali + copia offsite settimanale. Documenta lo schema.
- **Automatizza e pianifica:** configura i job di backup nel software scelto. Pianifica in orari non lavorativi se possibile. Attenzione all'encryption: imposta subito la password di cifratura nel job.
- **Implementa offsite/offline:** se fai backup su supporti fisici, assicurati che almeno una copia sia fuori dall'edificio (puoi portarla tu a casa in cassaforte, o usare cassette di sicurezza, o scambio con partner). Se su cloud, è offsite di natura, ma considera di mantenere credenziali separate per l'area backup cloud (non lasciarle memorizzate in un PC che può essere infetto).
- **Verifica notifiche di esito:** abilita le email di report del backup. Ogni giorno dovresti ricevere "Backup completato con successo" oppure avviso di errore. Se c'è un errore, indaga e risolvi immediatamente (disco pieno? file in uso? vedi cause e correggi). Non ignorare i log di backup.
- **Testa i ripristini periodicamente:** segnati ogni mese di fare almeno un test di restore piccolo: prendi un file a caso da backup e prova a ripristinarlo in una cartella temporanea – verifica che sia leggibile. Ogni trimestre/semestre fai un test più completo: es. simula che un server è perso, prova a ripristinare su un'altra macchina virtuale con il backup completo. Questo esercizio rivela se i tempi di ripristino sono accettabili e se ci sono passi mancanti (documentali la procedura di recovery durante il test, così se mai dovrai farlo sul serio sei già pronto con le istruzioni passo-passo).
- **Aggiorna/ruota le unità di backup:** dischi e nastri non durano in eterno. Sostituisci supporti ogni tot anni (nastri LTO ogni 5 anni, dischi magari ogni 3-4 se in continuo utilizzo) per evitare che al bisogno siano guasti.
- **Proteggi l'accesso ai backup:** limita fortemente chi può accedere alle console di backup o ai dispositivi backup. L'account amministratore del backup server dev'essere diverso da quello di produzione (così un malware che prende admin del dominio non ha per forza accesso all'ambiente backup). Se i backup sono su NAS, mettili in una share accessibile solo al servizio di backup, non montata come drive dagli utenti normali.

- **Cifra i backup fuori sede:** ribadiamo, se porti un disco fuori dall'azienda, cifralo. Anche un banale zip protetto con password forte è meglio di niente se devi trasferire alcuni file.
- **Segmenta rete di backup:** se possibile, isola il traffico di backup su VLAN dedicata o rete management. Meno un ransomware "vede" i tuoi repository di backup, meglio è.
- **Considera backup offline periodici:** ad esempio, masterizza su DVD o salva su un disco USB che poi scolleghi, almeno i dati vitali una volta al mese. È rudimentale ma garantisce una versione inaccessibile ai malware futuri.
- **Prevedi un piano di ripristino:** oltre al backup in sé, scrivi un piano di Disaster Recovery: priorità di cosa ripristinare (es. prima il server contabilità, poi la condivisione file meno critica, ecc.), chi decide attivazione DR, dove reperire hardware sostitutivo (es. una lista di contatti per noleggiare server se i tuoi sono inutilizzabili). Anche come contattare partner in emergenza se serve supporto. Questo piano può sembrare esagerato, ma anche poche linee guida aiutano molto quando sei sotto stress post-incidente.

CISA e altri enti ribadiscono: *backup offline e testati regolarmente sono la chiave di resilienza*. Con essi, anche un attacco grave diventa recuperabile. E ricorda: i backup servono non solo contro ransomware, ma anche contro errori umani (cancellazioni accidentali), guasti hardware, calamità naturali. Sono il tuo paracadute. Volare col paracadute dà molta più tranquillità che senza – allo stesso modo, condurre il business sapendo di avere copie sicure dei dati ti permette di fronteggiare i rischi con fiducia, e magari strappare condizioni migliori in assicurazioni cyber (che spesso chiedono: "avete backup offline?" come discriminante). Dunque, nessun compromesso su questo comandamento: se ancora non l'hai implementato, fallo diventare priorità uno.

12. SEGMENTAZIONE E CLOUD-FIRST

In un'azienda non segmentata, un aggressore che entra in un punto (es. PC reception) può muoversi lateralmente ovunque: server, dispositivi vari, macchine di produzione. La **segmentazione di rete** crea barriere interne – suddivide l'infrastruttura in zone isolate o con comunicazione strettamente controllata. È come avere compartimenti stagni: se uno viene compromesso, l'attacco resta confinato lì, **limitando i danni**. Inoltre facilita la gestione: politiche di sicurezza adattate a ogni segmento, meno traffico inutile che congestiona (migliora performance).

Parallelamente, l'approccio **cloud-first** significa privilegiare soluzioni cloud per nuovi servizi (e migrare quelli esistenti quando conveniente), così da ridurre la complessità on-premise. Per una PMI con poca IT staff, usare il cloud spesso semplifica gestione e sicurezza: i provider cloud investono enormi risorse in sicurezza di base, patching

infrastruttura, alta disponibilità. Questo non esime dal configurare bene, ma elimina tanta fatica di mantenere server locali. Ad esempio, passare da un server email interno a Microsoft 365 riduce il rischio di dover patchare Exchange (quanti attacchi perché le PMI non aggiornano Exchange…). Adottare cloud storage (OneDrive, Google Drive) al posto di un NAS esposto può essere più sicuro (con MFA, versioning integrato in caso di ransomware, ecc.). Inoltre, il cloud facilita il lavoro remoto e la resilienza (dati replicati geograficamente).

12.1 Segmentazione pratica per PMI

Non serve un data center con VLAN complesse – anche con router di fascia media si possono creare reti separate: ad esempio, una rete per i PC ufficio, una per i server, una per i dispositivi IoT/guest. Regole firewall interne poi decidono cosa può comunicare. Ad esempio: i PC ufficio possono accedere al server database solo tramite l'applicazione sul server applicativo, ma non direttamente alla porta DB. Le stampanti Wi-Fi stanno in una VLAN isolata accessibile dai PC ma che non può accedere ai server. Un esempio elementare: **rete ospiti** separata dal resto con solo uscita internet, così un device ospite infetto non tocca la LAN aziendale. Anche bancomat a parte, se arriva un consulente attacca il suo laptop sulla guest Wi-Fi.

In pratica, molti router tipo FRITZ!Box offrono già "guest network" isolata; altri come Ubiquiti ed i firewall UTM permettono VLAN. La configurazione può essere fatta gradualmente: prima isolando le macro-zone (ufficio vs produzione vs guest). Se hai apparecchiature particolari (es. macchine CNC con PC integrati un po' obsoleti), mettile in rete segregata, con accesso solo dal PC dell'operatore e magari dal PC dell'IT per manutenzione, ma che non hanno accesso a Internet aperto.

Segmentazione è anche **network segmentation by accounts**: ad esempio, su un server, crea share a cui solo reparti specifici accedono, non un unico calderone di file condivisi con permessi globali. Se un ransomware colpisce un utente, almeno cifrerà solo la share del suo reparto, non tutta l'azienda (in combinazione con i permessi minimi).

Scenario segmentazione: la **Ditta Elettrica** segmenta la rete in 3 VLAN: amministrazione, produzione (macchine PLC) e guest. Un crypto-malware arriva via phishing ad un PC amministrazione e prova a propagarsi. Grazie alle regole di segmentazione, il PC infetto non può "vedere" le macchine PLC nella VLAN produzione né accedere ai server SCADA, quindi il ransomware non impatta l'impianto produttivo (che spesso usa protocolli legacy e sarebbe andato giù). Il danno è confinato ad un paio di PC amministrativi poi ripristinati. Avessero avuto rete piatta, il malware avrebbe potuto infettare i PLC Windows-based e fermare l'impianto – danno potenzialmente milionario evitato con qualche regola di firewall interno.

12.2 Cloud-first per PMI

Non significa buttare tutto in cloud indiscriminatamente, ma valutare seriamente soluzioni SaaS o cloud-managed per ogni nuova esigenza. Ad esempio: devi mettere un CRM? Meglio uno SaaS online (Salesforce, Dynamics 365) che installare un server fisico in sede da mantenere. Devi ampliare storage? Forse conviene comprare licenze aggiuntive di OneDrive/SharePoint e mettere lì i file, piuttosto che un nuovo file server. Ovviamente considera costi ricorrenti, ma spesso per PMI i piani business di Microsoft/Google già includono pacchetti full (email, storage, collaboration) molto più sicuri e manutenuti di qualsiasi cosa on-prem improvvisata.

Un altro aspetto del cloud-first è **usare il cloud come DR/backup** (già trattato in Comandamento 11). Ad esempio, avere VM replicate su cloud che puoi accendere se i server fisici locali sono giù.

Attenzione: il cloud va configurato in sicurezza (MFA su account cloud, controlli di accesso Zero Trust – vedi Comandamento 9). Non è automaticamente un toccasana: se lasci bucket S3 pubblici con dati sensibili, è un disastro. Quindi adotta il cloud con competenza o con consulenza dove serve.

Scenario cloud-first: la **Contabilità SRL** aveva un vecchio server contabile on-prem che richiedeva costante manutenzione e rischi di guasto (e attacchi, se non patchato). Decidono di migrarlo ad una soluzione cloud ERP. Il carico sull'IT interno cala drasticamente: niente più patch mensili di SQL Server, niente backup manuali – il provider cloud gestisce tutto (naturalmente scelto con criterio, con contratti di sicurezza e backup). Anche durante la pandemia, i dipendenti accedono al gestionale da casa senza dover prima dover usare VPN, perché è SaaS. La produttività aumenta e l'IT locale si concentra su altre attività di miglioramento invece di spegnere incendi. In più, spostando quell'asset in cloud, riducono la superficie esposta in sede (meno porte, meno servizi esposti). Un attaccante non trova più quel server vulnerabile in azienda perché non c'è proprio – è altrove e presidiato da specialisti.

12.3 Strumenti consigliati

- **Firewall/VLAN:** se hai uno switch manageable, puoi definire VLAN separate per gruppi di porte. Se no, investi in un router firewall multi-sottorete (ce ne sono di economici tipo Mikrotik, Ubiquiti EdgeRouter, Draytek, etc., che con poche centinaia di euro danno funzionalità di segmentazione). Anche i sistemi Wi-Fi mesh moderni spesso hanno VLAN separate per guest vs main.
- **Access Control Lists (ACL):** su apparecchi di rete imposta ACL che limitino ad es. VLAN X può solo contattare IP Y sulla porta Z. Ad esempio: VLAN IoT (telecamere) può mandare stream video al server NVR, ma non può raggiungere Internet o altre VLAN.

- **VPN interne:** se hai sedi distaccate, piuttosto che farle una grande LAN unica, collegale con VPN site-to-site e mantieni segmenti di rete per sede. Così se una sede è infetta, non arriva lateralmente all'altra senza passare per firewall centrali che possano bloccare.
- **Cloud identity e gestione centralizzata:** adottare cloud spesso implica centralizzare identità in Azure AD/Google. Questo può semplificare gestione utenti (SSO su varie app).
- **Migrazione servizi graduale:** non serve tutto in una volta. Fai assessment: quali servizi on-prem generano più costi/rischi? Email e file server spesso sono i primi candidati per il cloud. Pianifica migrazione quando possibile (es. contratto licenze da rinnovare, hardware obsoleto da cambiare – magari invece di nuovo server fisico, passi a cloud).
- **Sicurezza del cloud:** strumenti come Cloud Security Posture Management (CSPM) per PMI, ad esempio i controlli di sicurezza integrati in Microsoft 365 (Secure Score) e Google (Security Center) – tienili d'occhio per migliorare la configurazione.
- **Edge computing ma segregato:** se hai necessità di mantenere qualche server locale (per latenze o dati critici), isolalo e proteggilo bene, e magari sincronizzalo col cloud per backup. Il concetto cloud-first non esclude di avere nulla in locale, ma rende la "first choice" il cloud, lasciando on-prem solo quando strettamente necessario.
- **Pianifica costi:** il cloud sposta spese CAPEX (hardware) in OPEX (abbonamenti). Fai un business case: a volte può costare un po' di più su lungo termine, ma includi nel calcolo i risparmi di manodopera IT, di energia, di spazi, e soprattutto di rischi mitigati. Spesso per PMI i piani cloud PMI sono abbordabili e l'eliminazione di rogne tecniche li ripaga.

12.4 Checklist operativo:

- **Segmenta per tipologia e sensibilità:** definisci i segmenti che hanno senso per la tua azienda. Ad esempio: Rete Ufficio (PC dipendenti), Rete Server, Rete Guest, Rete Produzione (macchinari / IoT). Ogni rete avrà un indirizzamento IP diverso (es. 192.168.10.x, 192.168.20.x, etc.).
- **Configura VLAN sullo switch/router:** implementa queste reti separate e sposta i dispositivi nelle VLAN corrette (magari bisogna riorganizzare cavi su switch se non è managed per assegnarli a VLAN statiche). Attiva la Wi-Fi guest isolata per ospiti.
- **Imposta regole di inter-VLAN firewalling:** di default, blocca tutto il traffico da una VLAN all'altra, poi crea eccezioni. Esempio: VLAN Ufficio può accedere a Server DB (IP X) sulla porta 3306; VLAN Produzione può essere raggiunta dal PC di Controllo specifico ma non dai client comuni; Guest VLAN nessun accesso alle altre VLAN.

- **Testa la segmentazione:** verifica che dagli host delle varie reti (o con un portatile settato su quell'IP range) non si raggiungano servizi proibiti. E al contrario, che servizi essenziali funzionino (es. i PC devono stampare? La stampante deve stare in VLAN Ufficio o devi permettere quell'accesso cross-VLAN). Aggiusta finché la segmentazione non rompe il business legittimo ma blocca il resto.
- **Documenta la mappa di rete segmentata:** chiunque in futuro entri in azienda (anche tu stesso tra 6 mesi) dovrebbe poter capire: "Ah, i server sono qui e questi dispositivi possono parlarci…" In emergenza, sapere quali porte aprire o chiudere rapidamente può fare differenza.
- **Comunica ai dipendenti se cambia qualcosa:** ad esempio, se crei VLAN separate, potrebbero dover connettersi a un SSID diverso per guest, o magari notare che non vedono più la stampante se collegati a rete sbagliata. Spiega eventuali piccoli cambiamenti di abitudine (e.g. "Da ora se un consulente vuole stampare deve collegarsi al Wi-Fi Guest-Print e accedere a questa stampante di rete dedicata…"). Minimizza l'impatto utente.
- **Valuta trasferimento servizi al cloud:** fai un elenco di servizi interni (Email, File server, CRM, ERP, applicazioni varie). Per ciascuno, verifica se c'è una valida offerta cloud. Stima costi cloud vs costi attuali (inclusi costi occulti di manutenzione e rischi).
- **Stabilisci priorità cloud migration:** magari l'email/Office 365 è già in cloud (molti l'hanno fatto), il passo successivo potrebbe essere spostare i file su SharePoint/OneDrive. Oppure adottare un gestionale SaaS al rinnovo del vecchio. Pianifica un progetto alla volta. Non sovraccaricare il piccolo team IT con 10 migrazioni in parallelo; step by step.
- **Prepara il personale al cloud:** per esempio, se passi da file server a OneDrive/SharePoint, forma i dipendenti su come usare il nuovo sistema, i vantaggi (collaborazione, versione file), e le nuove regole (es. condivisione esterna soggetta ad approvazione…). L'adozione fallisce se le persone non sanno usarlo e mantengono vecchie abitudini (tipo continuare a salvare in locale).
- **Adegua la sicurezza al cloud:** ogni nuovo servizio cloud, assicurati subito: MFA abilitato, permessi corretti (non dare a tutti ruolo admin del nuovo CRM online, per dire), backup se necessario (come detto, SaaS in teoria ridondanti ma fai export dati ogni tanto), e contratti chiari (GDPR, compliance, etc).
- **Spegni il vecchio una volta migrato:** non tenere sistemi duplicati per troppo tempo per "sicurezza". Ad esempio, se hai migrato la posta su 365, spegni il vecchio server Exchange e dismettilo – lasciarlo acceso "in standby" è un rischio e una spesa. Idem per file server: decommissiona appropriatamente.
- **Rivaluta infrastruttura locale:** con più servizi in cloud, forse puoi semplificare la LAN: meno server = magari meno necessità di alcuni firewall interni. Ma mantieni le segmentazioni perché dispositivi e PC locali li avrai

sempre. Piuttosto, la segmentazione può facilitare l'integrazione col cloud: per es. isolando i server rimasti, puoi poi mettere un accesso Zero Trust per i dipendenti che devono raggiungerli (e quell'accesso è più facile da controllare se la rete è segmentata).

- **Aggiorna le politiche cloud-first:** definisci a livello direzionale che, per qualunque nuova esigenza software, verrà preferito il modello cloud a meno di ragioni contrarie (costo eccessivo o impossibilità tecnica). Così quando i reparti chiedono un nuovo strumento, subito valutate soluzioni SaaS. Questo evita di aggiungere nuovo debito tecnico on-prem.
- **Ottimizza costi nel tempo:** controlla periodicamente i costi cloud e l'utilizzo. Elimina risorse cloud non usate (account inutilizzati, spazio non necessario). Il cloud a volte porta spese fantasma se non monitorate. Una buona gestione assicura benefici senza sprechi.

In definitiva, combinare segmentazione interna e strategia cloud-first porta **duplice vantaggio**: la segmentazione isola eventuali infezioni, *impedendo che un singolo incidente comprometta tutto il network*; il cloud-first riduce la superfice d'attacco locale e delega parte della sicurezza di base a player specializzati (che possono investire milioni in protezioni che una PMI non potrebbe). Inoltre, il cloud semplifica il recupero in caso di disastro (se l'ufficio brucia, i tuoi servizi cloud sono ancora lì – i dipendenti possono lavorare altrove). Unendo i due concetti: la tua rete locale diventa più piccola, più semplice e ben segmentata; molti servizi girano in ambienti cloud sicuri e accessibili da ovunque; la gestione per te è più snella e la resilienza complessiva sale. Questo è esattamente l'obiettivo: **contenimento e semplificazione** – contenere i problemi, semplificare la sicurezza.

13. MONITORAGGIO DELLE MINACCE ESISTENTI

Nessuna PMI, da sola, può avere occhi ed orecchie ovunque nel cyberspazio. Ecco perché l'ultimo comandamento è: **fare squadra**. ISAC sta per *Information Sharing and Analysis Center*, ovvero centri settoriali o regionali per la condivisione di informazioni sulle minacce. In pratica, aderire a un ISAC (o comunque a reti di condivisione come CERT, gruppi di settore, ecc.) significa collegarsi con una comunità di altri soggetti simili a te e con enti di sicurezza, scambiandosi allerte e buone pratiche in tempo reale. Ad esempio, l'ISAC del settore finanziario (FS-ISAC) condivide avvisi di truffe bancarie emergenti alle sue banche membri. Per enti locali in USA c'è MS-ISAC (Multi-State ISAC). In Italia esistono gruppi come l'**ISAC in ambito sanitario** (HCIRC), nel campo energetico ecc., e per le PMI non settoriali ci si può affidare al CERT nazionale (il CSIRT Italia) o ad associazioni di categoria.

L'idea chiave: **networking informativo**. Se un attacco nuovo colpisce un'azienda in rete ISAC, questa avvisa subito le altre: "Attenzione, sta girando un phishing che sembra provenire da Agenzia Entrate con allegato .xls – non apritelo". Oppure:

“Abbiamo rilevato tentativi di exploit su VPN SonicWall con IP X Y Z, bloccateli se li vedete”. Ricevere questi avvisi permette di reagire *tempestivamente*, a volte prevenendo del tutto un incidente. Come consiglia CISA, aderire a info-sharing consente di ottenere informazioni critiche e servizi di supporto in tempi rapidi.

13.1 Cosa fare concretamente per una PMI

- **Unirsi a gruppi/community locali:** se c’è un ISAC per il tuo settore e aperto a membri privati, considera l’iscrizione. Alcuni richiedono requisiti o quote associative (spesso ne vale la pena se proteggono il tuo core business). Ad esempio, se sei un piccolo fornitore in ambito energia, potresti richiedere accesso al Energy ISAC per ricevere i loro bollettini.
- **Seguire CERT e CSIRT nazionali:** il **CSIRT Italia** pubblica sul suo sito alert di sicurezza e newsletter; anche l’**AGID-CERT** per PA. Iscriviti alle mailing list o feed RSS. Stessa cosa per **CISA** e l’**EUROPOL EC3** – hanno canali di allerta (CISA poi ha il programma Shields Up con consigli in momenti di crisi geopolitica).
- **Partecipare a community online:** su LinkedIn o forum tecnici ci sono gruppi di “IT Security Italia” dove professionisti condividono esperienze. Ovviamente filtra le info, ma può essere utile per annusare trend. Ci sono anche Slack/Discord di cybersecurity dove si discute di nuove vulnerabilità in tempo reale.
- **Collaborare con aziende partner:** se hai fornitori o clienti con cui puoi parlare di sicurezza, scambiatevi contatti per allertarvi reciprocamente. Es: il tuo fornitore software ti avvisa se uno dei suoi altri clienti subisce un attacco simile a te.
- **Iscriversi a portali di threat intelligence gratuiti:** esempi: abuse.ch (feed su indicatori malware), VirusTotal (puoi impostare notifiche se appare un malware col tuo nome di dominio per es.), molti vendor come Palo Alto, Fortinet pubblicano blog di minacce emergenti – segui quelli più rilevanti.
- **Eventi e conferenze locali:** partecipare occasionalmente ad eventi di sicurezza IT (anche online webinar) ti mette in rete con professionisti. Conosci altri IT di PMI, scambiate biglietti da visita – poter chiamare un collega in un’altra ditta per chiedere “anche a voi quell’email strana?” è prezioso.
- **Coinvolgere associazioni di categoria:** ad esempio Confindustria locale, CNA, Confartigianato – molte iniziano ad avere gruppi di lavoro su digitale e sicurezza. Unisciti per portare a casa conoscenze e magari training gratuiti.
- **Usare canali di polizia postale:** la Polizia Postale italiana diffonde avvisi su truffe in corso (sui social per es.). Tener d’occhio anche quelli.

Il concetto è simile al principio “l’unione fa la forza”. I criminali collaborano tra loro su forum clandestini, quindi anche i “buoni” devono fare fronte comune. Se tu vieni a

sapere di un nuovo malware targeting PMI manufacturing prima che arrivi a te, puoi prendere contromisure preventive (patch, sensibilizzazione dipendenti su quell'email truffa, ecc.).

Scenario: la **TecnoStartup** aderisce a un gruppo Cyber di aziende ICT in Italia. Un venerdì, un membro posta un alert: *"Abbiamo visto un ransomware nuovo propagarsi via RDP aperti, occhio a chi ha RDP esposti, patchate CVE-XXXX."* La TecnoStartup legge, realizza che effettivamente il loro server di test ha RDP aperto per un consulente, ancora con un bug non patchato. Corrono ai ripari (chiudono temporaneamente RDP e applicano patch). Poche ore dopo, arrivano scansioni massicce su quella porta in tutto il paese – ma loro hanno già sistemato. Hanno schivato il colpo grazie all'allerta condivisa.

Un altro esempio: il **Distretto Artigiano** locale ha un gruppo WhatsApp di responsabili IT: un giorno uno scrive "Ragazzi, sto vedendo email provenienti apparentemente da una ditta trasporti locale con allegato .xls, è un ransomware. Attenzione." Tutti avvisano immediatamente i loro utenti di non fidarsi di quell'email se arriva. Uno dei membri del gruppo poi trova quell'allegato e lo manda al CERT nazionale che conferma la minaccia e la diffonde. Questo micro-network ha arginato un attacco sul nascere.

13.2 Strumenti consigliati

- **Registrati al portale CSIRT-Italia:** contiene sezioni con indicatori di compromissione e avvisi.
- **MISP (Malware Information Sharing Platform):** alcune comunità usano MISP server per condividere indicatori di compromesso in modo strutturato. Non è qualcosa che una PMI mette in piedi da sé, ma potresti avere accesso a un MISP del CERT nazionale o di associazione e consultare i feed (con TI integrabile nel tuo SIEM/EDR).
- **Mailing list e newsletter di vendor:** anche iscriversi alle news di Microsoft Security, Cisco Talos, etc. porta informazioni: certo, sono globali e spesso tecniche, ma segnalano vulnerabilità o campagne attive.
- **Canali diretti con Forze dell'Ordine:** in Italia si può segnalare attacchi alla Polizia Postale (CNAIPIC per infrastrutture critiche). Stabilire un rapporto con loro (ad es. invitandoli a fare un talk in azienda o partecipando a eventi con loro) fa sì che in caso di attacco serio saprai subito a chi rivolgerti. In alcuni paesi la polizia invia alle aziende alert su truffe emergenti – vedi se localmente succede qualcosa di simile (a volte Confindustria smista comunicati di Polizia Postale).
- **Gruppi Trust**: nel tempo se entri in contatto con altri IT di fiducia, crea un piccolo gruppo email o chat con loro. Quel canale informale può essere rapido e schietto per scambi di info.

- **LinkedIn/Twitter:** segui profili di esperti di cybersecurity, CERT, agenzie. Ad esempio, il profilo Twitter di *CSIRT_IT*, *CISA Cyber*, *ZDNet security*, ricercatori noti. Spesso le breaking news di vulnerabilità appaiono lì in tempo reale (es. ricercatore X twitta "Attenzione, exploit di 0-day su Exchange in the wild").

13.3 Checklist operativo

- **Identifica l'ISAC o CERT rilevante:** a seconda del settore PMI. Se sei in un settore regolamentato (energia, sanità), verifica se esiste un ISAC. Contatta l'associazione di categoria per chiedere se hanno iniziative su cybersecurity.
- **Iscriviti a mailing list di allerta:** alcuni esempi: mailing list CERT-PA o CSIRT Italia, CISA Alert (ti manda email di advisory), FBI flash reports (a volte rilasciati per settori).
- **Partecipa ad incontri locali:** se senti di seminari gratuiti su cybersecurity organizzati da Camera di Commercio o associazioni, vai o mandaci il tuo IT. Oltre ad imparare, conoscerai gente con cui poi poter scambiare contatti.
- **Crea rubriche utili:** sul tuo telefono ed email tieni i contatti di riferimento: es. l'esperto IT dell'azienda vicina di cui ti fidi, il funzionario Polizia Postale locale (se sei arrivato a conoscerlo in un convegno, perché no), il CERT Nazionale (hanno email dedicata per segnalazioni). In caso di bisogno, non devi cercare in panico, hai già a chi rivolgerti.
- **Integra feed di intelligence:** se hai un sistema di log centralizzato o un SIEM, valuta di integrare qualche feed pubblico (es. IP di C2 noti, hash di malware attuali) così il sistema può avvisare se vede qualcosa di corrispondente. Molti EDR commerciali già lo fanno in backend, ma se hai soluzioni open potresti aggiungere manualmente feed di Abuse.ch (per esempio).
- **Contribuisci quando puoi:** networking non è solo prendere, ma anche dare. Se sventi un attacco nuovo o noti qualcosa di strano, condividilo (senza esporre dati sensibili). Ad esempio, informare il CERT se la tua azienda ha subito un tentativo di spear phishing molto mirato potrebbe aiutare altre. Ovviamente c'è il timore di reputazione, ma condividendo attraverso i canali giusti (anche in anonimato verso CERT pubblici) fai parte dell'ecosistema di difesa.
- **Stabilisci rapporti pre-crisi:** è psicologicamente più facile chiedere aiuto a qualcuno con cui hai già parlato prima in situazioni normali. Dunque, coltiva quei rapporti. Ad esempio, se sei membro di un ISAC, partecipa attivamente alle discussioni, presentati. Poi se mai avrai bisogno (es. "ragazzi, ho questo malware strano, qualcuno ne sa qualcosa?") otterrai risposte più rapide perché ti conoscono.
- **Monitora threat landscape:** senza esagerare (non devi stare h24 su Twitter), ma dedicare magari un'oretta a settimana a leggere un paio di articoli su minacce emergenti nel tuo settore ti tiene aggiornato e pronto. Magari

scoprendo nuovi trend puoi aggiornare anche la tua formazione interna (Comandamento 10) e dire "hey team, stanno aumentando gli attacchi via PEC false di fornitori, stiamo in campana".

In conclusione, questo comandamento riconosce che la sicurezza informatica è un gioco di squadra. Anche una piccola azienda può alzare di molto il suo livello di guardia se **si connette a una rete di allerta** più ampia. Le minacce evolvono in fretta, ma essere nel circuito delle informazioni ti dà quel vantaggio di tempo per prepararti. È come appartenere a un vicinato dove i vicini si avvisano a vicenda se c'è in giro un ladro: meglio che scoprirlo quando ce l'hai già in casa.

CONCLUSIONE

Abbiamo percorso i **13 comandamenti delle PMI in cybersecurity**, ognuno con il suo ruolo: dall'autenticazione robusta (MFA) alla disciplina tecnica (whitelisting, patching), dalle misure di contenimento (segmentazione, backup offline) alla componente umana (formazione, condivisione informazioni). Implementarli tutti può sembrare impegnativo, ma vanno visti come un programma di miglioramento continuo e integrato.

Molti di questi principi si rafforzano a vicenda: ad esempio, l'MFA e la formazione aiutano a ridurre il rischio di phishing; la rimozione dei privilegi e il deny-by-default limitano l'impatto se qualcosa sfugge; i backup e la rete di allerta ti danno resilienza e risposta rapida in caso di incidente. Insieme, costruiscono una difesa multilivello. E la bellezza è che **sono misure attuabili anche con risorse limitate**: spesso sfruttando funzionalità già presenti (sistemi Windows, soluzioni cloud esistenti, comunità di pratica gratuite) o richiedendo investimenti molto minori del costo di un attacco subito.

Per i titolari e manager di PMI, questi comandamenti non sono solo tecnicismi: sono **buone pratiche di gestione del rischio aziendale**. Un attacco grave può mettere in ginocchio un piccolo business; al contrario, un business protetto ispira fiducia ai clienti e partner (magari puoi persino comunicarlo come valore aggiunto: "i vostri dati sono al sicuro con noi, adottiamo le migliori pratiche di sicurezza informatica"). Inoltre, molte normative (GDPR, Direttiva NIS2 in arrivo per alcune imprese) richiedono misure adeguate di sicurezza – applicando questi comandamenti sei senz'altro sulla buona strada per la compliance.

Come usare questo manuale? Il metodo migliore è affrontare un capitolo alla settimana: leggi, analizza la tua situazione attuale in quell'area e metti subito in pratica almeno una delle azioni suggerite. Ogni capitolo contiene una checklist operativa: usala come mappa, procedendo un passo alla volta.

Dopo 13 settimane avrai completato il primo ciclo di interventi. A quel punto ricomincia dal primo capitolo: il contesto aziendale, le minacce e le tecnologie cambiano, e ogni giro ti permetterà di rafforzare e perfezionare ciò che hai già fatto. Puoi partire dalle misure più semplici e ad alto impatto (come l'autenticazione multifattore o i backup) e, man mano che prendi confidenza, passare a interventi più strutturali e strategici (come il whitelisting o l'adozione di un approccio Zero Trust). Coinvolgi fin da subito la direzione aziendale per ottenere supporto e risorse, e il personale per garantire adesione alle nuove policy e partecipazione attiva alla formazione. La sicurezza informatica non è un compito esclusivo dell'IT: è una responsabilità condivisa da tutta l'organizzazione.

Una proposta per il ciclo delle prime 13 settimane:

Settimana	Comandamento	Obiettivo della settimana	Azione chiave	Risultato atteso
1	Autenticazione Multifattore (MFA)	Proteggere gli accessi remoti	Attiva MFA su email, VPN, applicazioni cloud	Accessi protetti anche in caso di furto password
2	Deny-by-default	Limitare esecuzione software non autorizzato	Configura allowlist applicazioni	Riduzione rischio malware e programmi non approvati
3	Disattivazione macro	Eliminare un vettore di ransomware	Disattiva macro non firmate in Office	Riduzione drastica dei rischi da allegati malevoli
4	Privilegi minimi	Ridurre impatto di compromissioni	Rimuovi diritti admin locali inutili	Gli utenti non possono installare software malevoli
5	Hardening sistemi e network	Chiudere porte di attacco note	Disabilita servizi/protocolli obsoleti, configura firewall	Superficie di attacco ridotta
6	Monitoraggio file e uso USB	Individuare anomalie su dati e supporti	Installa tool di file integrity e blocco USB non autorizzati	Rilevamento rapido di copie o esfiltrazioni dati
7	Patch regolari + MDR	Aggiornare e monitorare costantemente	Abilita update automatici e valuta MDR	Vulnerabilità ridotte, sorveglianza 24/7
8	Gestione Superficie di Attacco (ASM)	Scoprire asset esposti	Usa tool ASM (anche gratuiti) per scansione	Mappa aggiornata degli asset esposti in rete
9	Zero-Trust	Limitare accessi superflui	Implementa policy di accesso "just in time"	Accessi ridotti al minimo indispensabile

Settimana	Comandamento	Obiettivo della settimana	Azione chiave	Risultato atteso
10	Formazione personale	Creare cultura di sicurezza	Organizza breve sessione su phishing e policy aziendali	Maggiore consapevolezza e riduzione errori umani
11	Backup cifrati	Garantire recupero dati sicuro	Configura backup cifrati e verifica restore	Ripristino dati sicuro in caso di incidente
12	Segmentazione e cloud-first	Contenere movimenti laterali	Segmenta rete e sposta servizi base in cloud sicuro	Maggiore isolamento e semplificazione gestione
13	Monitoraggio minacce	Restare aggiornati sui rischi	Attiva feed OSINT e alert su nuove vulnerabilità	Reazione più rapida a nuove minacce

Ricorda anche di **mantenere aggiornate** le tue conoscenze: le minacce evolvono, e quello che oggi è considerato sufficiente, domani potrebbe dover essere rafforzato. Ma se hai costruito basi solide con questi comandamenti, sarà più facile adattarsi. Avrai un'infrastruttura ordinata e monitorata, su cui applicare aggiornamenti e nuove misure con meno sforzo.

In un mondo digitale pieno di insidie, una PMI deve trovare un equilibrio tra protezione e operatività. Queste 13 regole d'oro mirano proprio a **proteggere il sistema senza ostacolare il business**: anzi, spesso ottimizzano i processi (pensiamo al cloud che rende il lavoro più agile, o al whitelisting che riduce incidenti e downtime). La sicurezza diventa un abilitatore, non un freno. Attraverso esempi pratici abbiamo visto che con un po' di ingegno e le giuste priorità anche una piccola azienda può respingere attacchi sofisticati e reagire prontamente alle crisi.

In conclusione, se implementerai questi comandamenti, potrai affrontare con maggiore serenità le sfide della cybersecurity. Non sarà facile né che potrai dormire completamente tranquilli – i rischi zero non esistono – ma certamente ridurrai drasticamente la probabilità di incidenti gravi e le loro conseguenze. E quando qualcosa accadrà, perché qualcosa prima o poi succede a tutti, tu non dovrai *improvvisare*: avrai una strategia, degli strumenti, una cultura aziendale pronta a fronteggiare la tempesta.

Come disse un esperto: *"Hope is not a strategy"* – sperare che non succeda nulla non è una strategia. Al contrario, **prepararsi è la strategia**. Con questi 13 comandamenti, la tua PMI sarà preparata. E potrai concentrarti sul far crescere il business, mentre le tue fondamenta digitali saranno robuste e ben presidiate. Buon lavoro e buona sicurezza!