Cybersecurity dei dati: protezione e controllo

Camera di Commercio Firenze
dal 1770 la casa delle imprese
punto impresa digitale
Sezione Regionale Toscana
Albo Nazionale Gestori Ambientali

Indice della lezione

01 — **Cybersecurity; cos'è e perché serve**

02 — **Le minacce più comuni**

03 — **Le misure essenziali di protezione**

04 — **Come rispondere a un attacco**

01

Cybersecurity; cos'è e perché serve

…mettere in sicurezza i nostri dati

Cybersecurity: definizione

La cybersecurity protegge il patrimonio digitale di un'organizzazione - dati, sistemi e persone - garantendo che le informazioni rimangano riservate, integre e disponibili.

Confidenzialità: I dati sono accessibili solo a chi è autorizzato.

Integrità: I dati non vengono modificati da soggetti non autorizzati.

Disponibilità: I sistemi e i dati sono accessibili quando servono.

Per una PMI significa concretamente: **sapere quali dati hai, chi vi accede, come sono protetti e cosa fare se qualcosa va storto**.

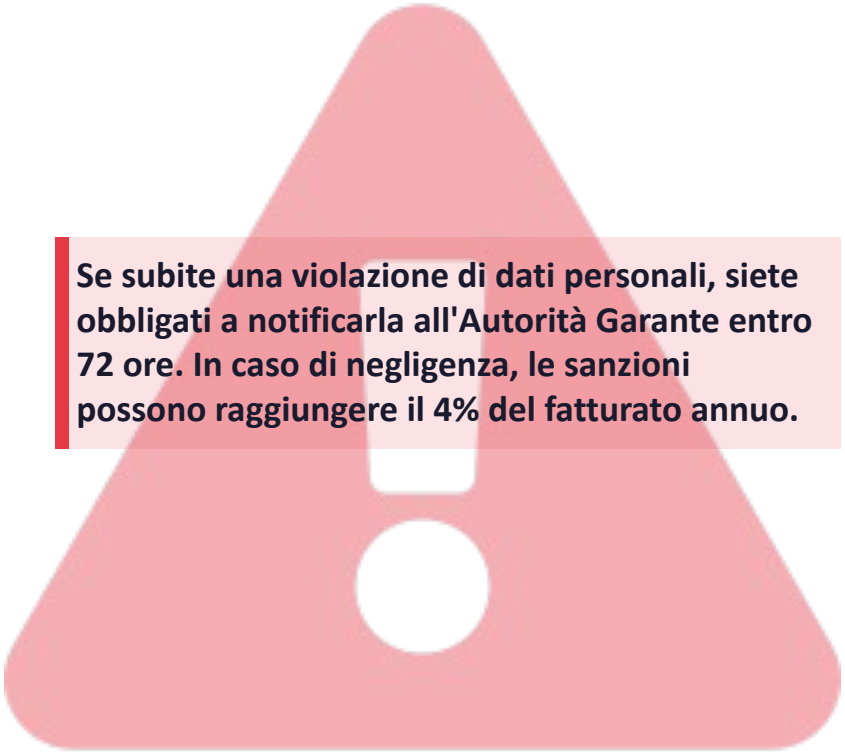
Non solo danni diretti: il GDPR

Tenere un registro dei trattamenti dati

Nominare un responsabile del trattamento

Adottare misure tecniche e organizzative adeguate

Informare i clienti su come vengono usati i loro dati



Se subite una violazione di dati personali, siete obbligati a notificarla all'Autorità Garante entro 72 ore. In caso di negligenza, le sanzioni possono raggiungere il 4% del fatturato annuo.

NIS2 e normative europee: cosa cambia per le PMI

Non tutte le piccole imprese sono obbligate direttamente, ma tante sono coinvolte attraverso la catena di fornitura.

Chi è obbligato direttamente

La NIS2 (D.Lgs. 138/2024) si applica alle imprese con più di 50 dipendenti o 10M€ di fatturato in settori critici: energia, trasporti, sanità, infrastrutture digitali, PA.

La catena di fornitura

Anche se non sei obbligato, i tuoi clienti grandi lo sono. Richiedono sempre più spesso requisiti minimi di sicurezza ai fornitori come condizione contrattuale. La NIS2 arriva alle PMI attraverso la supply chain.

GDPR + NIS2: quando si sovrappongono

Un attacco ransomware che coinvolge dati personali attiva entrambe le normative. GDPR: notifica al Garante entro 72 ore. NIS2: notifica all'ACN. Due obblighi, una sola violazione.

Cyber Resilience Act

In vigore da ottobre 2024. Riguarda chi produce o vende prodotti con componenti digitali connesse. Rilevante per PMI manifatturiere con macchinari, sensori o dispositivi IoT.

Dove si trovano questi dati?

PC e laptop

Locali, spesso senza backup

Smartphone

Email, foto, documenti aziendali

Cloud

Google Drive, Dropbox, OneDrive

Casella email

Anni di comunicazioni sensibili

Gestionale

Clienti, fatture, fornitori, pagamenti

Sito / e-commerce

Dati di accesso clienti

Quanti dati ha la vostra impresa?

Dati clienti

- Nome, indirizzo, email
- Storico acquisti
- Metodi di pagamento

Dati fornitori

- IBAN e coordinate bancarie
- Contratti e prezzi
- Credenziali portali

Dati aziendali

- Dati fiscali e bancari
- Accessi software gestionali
- Dati dipendenti

Dati operativi

- Email e comunicazioni
- Documenti e offerte
- Credenziali accessi web

Cybersecurity = Rischio d'impresa

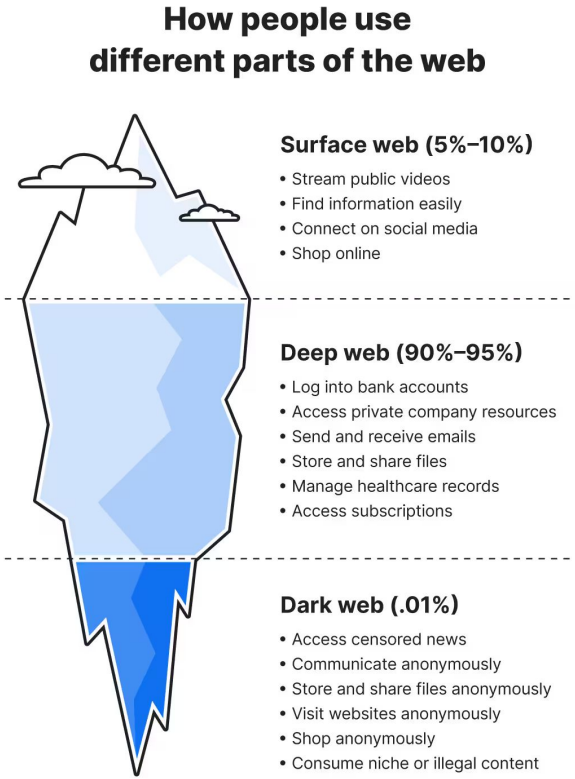
Rischi che già gestisci

- Furto / rapina
- Incendio
- Inadempimento clienti
- Guasto impianti

Rischi digitali (stesso livello!)

- Blocco attività
- Perdita dati clienti
- Furto identità digitale
- Danno reputazionale

Quanto valgono i tuoi dati



IBAN + credenziali bancarie	**€ 500 – 2.000**
Lista clienti con email	**€ 100 – 400**
Credenziali email aziendale	**€ 50 – 200**
Accesso a e-commerce	**€ 200 – 1.000**

Conosci ciò che devi proteggere

Non si può proteggere ciò che non si conosce. Il primo passo è fare **l'inventario degli asset della propria impresa.**

Dispositivi	Dati critici	Software e servizi	Persone e accessi
· PC e notebook	· Archivio clienti	· Gestionale/ERP	· Chi ha accesso a cosa
· Smartphone aziendali	· Dati contabili	· Email aziendale	· Dipendenti con privilegi admin
· Tablet	· Contratti	· Cloud storage	· Fornitori con accesso ai sistemi
· Stampanti e scanner	· Credenziali di accesso	· Sito web e e-commerce	· Ex dipendenti (verificare!)
· Dispositivi IoT	· Dati personali dipendenti	· App di pagamento	· Account condivisi

Non tutto ha lo stesso peso: come assegnare le priorità

Con risorse limitate, proteggere tutto allo stesso modo significa non proteggere niente davvero. La priorità si assegna in base a due criteri.
Priorità = Impatto × Probabilità - proteggi prima ciò che fa più male se compromesso e che è più esposto a una minaccia.

Criterio 1 — Impatto

Se questo asset venisse compromesso, quanto danno causerebbe?

CRITICO	Stop all'attività, danni irreversibili, sanzioni
ALTO	Perdita dati clienti, danni reputazionali significativi
MEDIO	Disagi operativi, costi di ripristino gestibili
BASSO	Inconveniente minore, rapidamente recuperabile

Criterio 2 — Probabilità

Quanto è probabile che questo asset venga attaccato o compromesso?

ALTA	Esposto su internet, password debole, non aggiornato
MEDIA	Accesso limitato ma non protetto con 2FA
BASSA	Accesso controllato, aggiornato, monitorato
MINIMA	Isolato dalla rete, accesso fisico controllato

Il registro minimo: uno strumento pratico e immediato

Non serve un software dedicato. Un foglio Excel con 4 colonne è sufficiente per iniziare. L'importante è farlo e tenerlo aggiornato.

Cosa	Chi lo usa	Dati critici che contiene	Livello di rischio
PC reception	Personale front office	Dati clienti, email	Alto
Gestionale ERP	Amministrazione, magazzino	Contabilità, ordini, clienti	Molto alto
Sito web WordPress	Fornitore web agency	Nessuno / Form contatti	Medio
Smartphone titolare	Titolare	Email, WhatsApp business, accessi	Alto
NAS ufficio	Tutti	Documenti, contratti, backup	Molto alto

02

Le minacce più comuni

Phishing, malware e tanti altri

Perché le PMI sono bersagli "facili"

- Nessun responsabile IT dedicato
- Budget scarso per la sicurezza
- Formazione dei dipendenti solitamente assente
- Software non aggiornati
- Backup irregolari o assenti

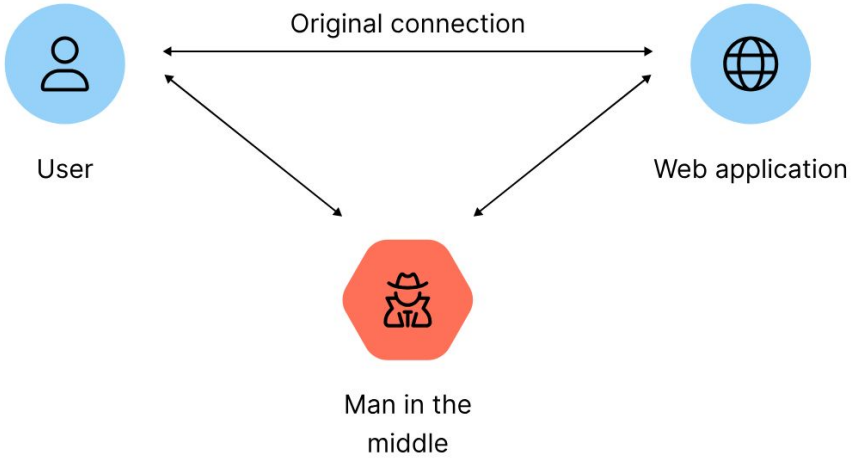
Il principio della serratura

I criminali non cercano la cassaforte più ricca. Cercano quella più facile da aprire.

Dal campo: il caso Man-in-the-Middle

⚠ Questo tipo di attacco colpisce ogni anno centinaia di PMI italiane

- **L'imprenditore**
  Riceve email dal suo fornitore: "Nuovo IBAN per i pagamenti".
- **L'attaccante**
  Si è inserito nella conversazione email e ha modificato l'IBAN.
- **Il risultato**
  16.000€ bonificati sul conto del criminale. Recupero quasi impossibile.



Le minacce principali

Data Breach

Furto di dati aziendali o di clienti

Credential Stuffing

Credenziali rubate usate in automatico per accedere ai tuoi account

DoS / DDoS

Sovraccarico del sito o dei servizi fino a renderli irraggiungibili

Malware

Software malevolo che si installa sul dispositivo

Ransomware

Blocca i file e chiede un riscatto in denaro

Phishing

Email false che rubano credenziali o denaro

Come rispondiamo: il 51% del traffico internet non è umano

Ogni giorno la tua impresa è raggiunta da traffico che non hai invitato e che non vedi. Non è fantascienza, è la normalità di qualsiasi dispositivo o sito connesso a internet.

51%

del traffico internet globale è generato da bot automatizzati

Bot 'buoni' — 17%

Crawler di Google, strumenti di monitoraggio, aggregatori di prezzi. Fanno parte del funzionamento normale del web.

Bot 'cattivi' — 34%

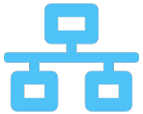
Scansionano siti alla ricerca di vulnerabilità, tentano accessi con password comuni, raccolgono email per spam. Attivi 24 ore su 24.

Perché riguarda la tua PMI

I bot non scelgono le vittime — scansionano tutto ciò che è connesso. Un sito non aggiornato o un pannello admin con password debole vengono trovati automaticamente.

La "superficie di attacco" di una PMI

Ogni dispositivo o servizio connesso è un potenziale punto di ingresso per un attacco.



Router / Wi-Fi

Rischio: Alto

Email aziendale

Rischio: Alto

PC

Rischio: Alto

Gestionale / ERP

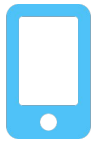
Rischio: Medio

Sito web

Rischio: Medio

Cloud storage

Rischio: Medio



Smartphone

Rischio: Medio

Stampanti / IoT

Rischio: Medio/Basso

Gli impatti concreti di un attacco

Perdita economica diretta

Bonifico errato, riscatto ransomware, costo ripristino sistemi

Perdita di dati

File irrecuperabile, anni di documentazione aziendale persi

Fermo attività

Da ore a settimane di interruzione operativa

Danno reputazionale

I clienti vengono a sapere della violazione

Il fattore umano: l'anello più debole e più importante

Il **95%** degli incidenti informatici ha origine da un comportamento umano: un clic sbagliato, una password debole, un allegato aperto.

Clic su link di phishing

L'email sembrava autentica — il dipendente non era stato formato a riconoscerla

Password debole o condivisa

Nessuno aveva spiegato le regole e le conseguenze

Allegato malevolo aperto

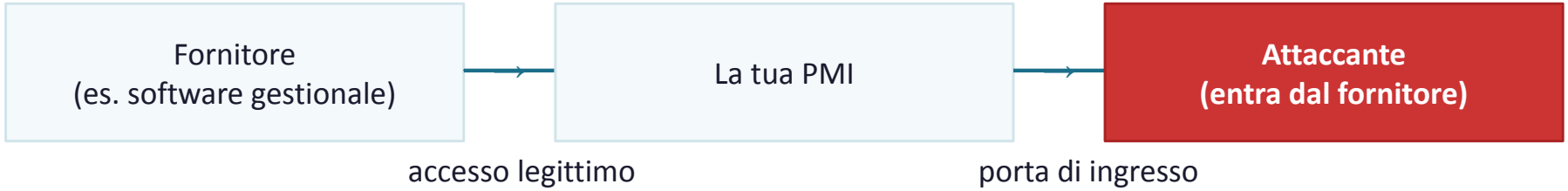
Un file PDF o Word con macro: senza formazione, il rischio non è riconoscibile

Ingegneria sociale subita

Il 'titolare' che chiede un bonifico urgente — senza procedura di verifica, ci si fida

I fornitori: un rischio spesso sottovalutato

Il 29% degli attacchi alle PMI avviene tramite un fornitore o un partner con accesso ai sistemi aziendali. La catena di fornitura è parte della tua superficie di attacco. (Report Clusit 2026)



Le domande da porsi per ogni fornitore con accesso ai tuoi sistemi:

- ➔ A quali dati e sistemi ha accesso questo fornitore? L'accesso è strettamente necessario, o potremmo limitarlo?
- ➔ Esiste un contratto che prevede obblighi di sicurezza?
- ➔ Siamo avvisati in caso di incidente sul lato del fornitore?

03

Misure essenziali di protezione

Cosa fare per proteggere i dati

La difesa non è (solo) una questione tecnica

Il 95% degli incidenti informatici ha origine da un errore umano o da una procedura mancante e non da una tecnologia insufficiente.

Strumenti avanzati - Antivirus, EDR, ecc - utili ma non sufficienti da soli

Controlli tecnici — Password, backup, aggiornamenti, firewall

Processi e governance — Regole, responsabilità, politiche scritte

Cultura e formazione — Le persone sono la prima linea di difesa

L'identità digitale: il bersaglio preferito degli attaccanti

Il furto di credenziali è alla base dell'80% delle violazioni informatiche. Username e password sono la porta d'ingresso a tutto.

Phishing

Un'email convincente porta il dipendente a inserire le proprie credenziali su un sito falso

Data breach

Le credenziali vengono rubate da un altro servizio in cui si usa la stessa password

Keylogger/Malware

Un software malevolo registra ogni tasto premuto e invia le password agli attaccanti

Ingegneria sociale

L'attaccante si finge il titolare o l'IT e chiede le credenziali direttamente al dipendente

Nota !!! Una sola credenziale compromessa può dare accesso all'intero sistema aziendale se non ci sono controlli aggiuntivi.

Come ci proteggiamo?

Governance

Una policy minima, responsabilità definite e procedure scritte riducono gli errori evitabili

Accessi e password

Minimo privilegio, password sicure, 2FA attivo, passphrase, password manager

Backup 3-2-1

3 copie, 2 supporti, 1 offsite. Testare mensilmente. Backup non testato = backup inutile

Aggiornamenti

Automatici per OS e browser. Mensili per software. Niente software senza supporto

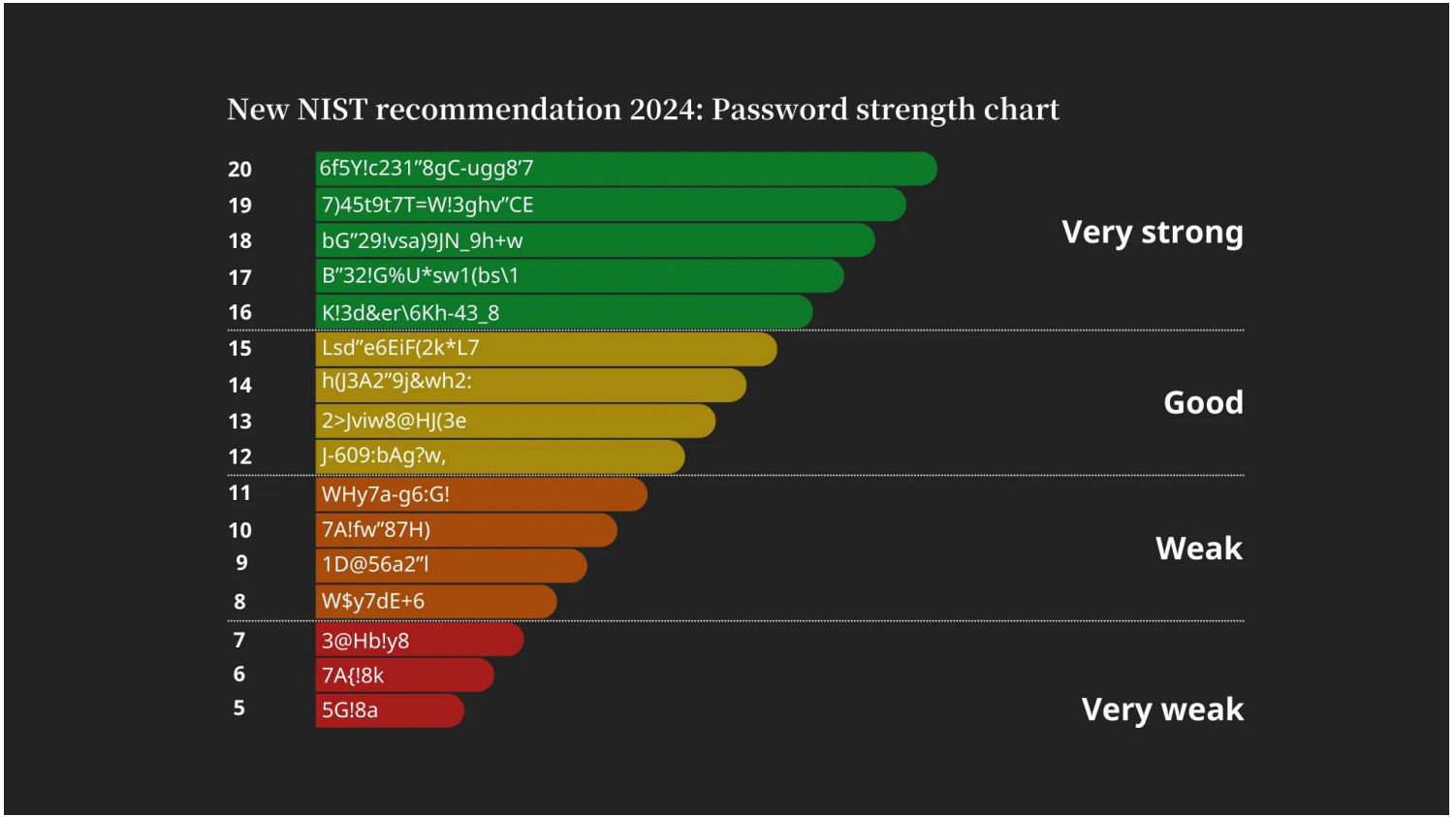
Rete e dispositivi

Firewall attivo, WPA2/3, rete ospite separata, antivirus aggiornato, PIN su mobile

Fattore umano

Formazione, dipendenti, cultura aperta

Lunghezza password



04

Come rispondere a un attacco

Accorgersi “in tempo” se qualcosa non va

DETECT: Come accorgersi che qualcosa non va

La maggior parte degli attacchi lascia tracce. Il problema è che senza abitudine a riconoscerle, vengono scambiate per problemi tecnici ordinari.

PC lento o che si comporta in modo strano

Uso anomalo della CPU, processi sconosciuti in esecuzione, cursore che si muove da solo

Impossibile accedere a file o account

File cifrati, estensioni cambiate, messaggi di riscatto - segnali classici di ransomware

Colleghi che ricevono email strane 'da te'

L'account email è compromesso - qualcuno invia messaggi usando la tua identità

Traffico di rete anomalo

Upload massivi di dati, connessioni a IP sconosciuti, rallentamento improvviso della connessione

Avvisi dell'antivirus ignorati o disattivati

Un malware può disattivare le difese - un antivirus che smette di funzionare è un segnale

Accessi in orari o luoghi insoliti

Login in orari insoliti, accesso dall'estero, account usato da un IP mai visto prima

RESPOND: I primi 30 minuti sono critici

Come reagisci nei primi 30 minuti determina l'entità del danno. La regola d'oro: isola prima, indaga dopo.

1 **ISOLA**

Disconnetti il dispositivo dalla rete - cavo e Wi-Fi. Non spegnerlo: potresti perdere prove. Non continuare a usarlo.

2 **NOTIFICA**

Chiama il tuo riferimento IT o il fornitore. Avvisa il titolare o il responsabile. Non mandare email dal sistema compromesso.

3 **DOCUMENTA**

Annota tutto ciò che vedi: messaggi di errore, orario, cosa stavi facendo. Fotografa lo schermo. Ogni dettaglio è utile.

4 **VALUTA**

Quali dati erano su quel dispositivo? Chi altro potrebbe essere coinvolto? Il problema è limitato o si è diffuso?

5 **SEGNALA**

Se sono coinvolti dati personali: notifica al Garante entro 72 ore (GDPR). Se sei soggetto NIS2: notifica all'ACN entro 24 ore.

RECOVERY: Ripristino e ritorno all'operatività

Il ripristino non è solo tecnico. È anche organizzativo e comunicativo. Un piano di recover riduce il downtime da settimane a ore.

Ripristina dal backup — **Tecnico**

Usa il backup più recente verificato. Segui l'ordine di priorità definito nel piano: prima i sistemi critici.

Ripulisci e riconfigura — **Tecnico**

Non ricollegare un sistema compromesso senza averlo ripulito. Reinstalla da zero se necessario.

Comunica internamente — **Organizzativo**

Aggiorna il team su cosa è successo, cosa è stato fatto e cosa devono fare. Evita il panico da disinformazione.

Comunica con clienti e fornitori — **Comunicazione**

Se i loro dati sono stati coinvolti, informali in modo chiaro e tempestivo. La trasparenza protegge la reputazione.

Documenta e analizza — **Apprendimento**

Scrivi cosa è successo, come si è risolto e cosa cambieresti. Questa analisi è la base per migliorare il piano.

Abbiamo visto cosa fare a mano e per fortuna la tecnologia aiuta

Detect, Respond e Recover richiedono attenzione, procedure e competenze. Ma esistono strumenti che automatizzano buona parte di questo lavoro - anche per le PMI.

Rilevamento automatico

Strumenti che monitorano continuamente e ti avvisano quando qualcosa non va - senza che tu debba guardare i log ogni giorno

Risposta assistita

Sistemi che bloccano automaticamente attività sospette prima che causino danni - guadagnare tempo è tutto

Intelligenza artificiale

La stessa tecnologia che potenzia gli attacchi viene usata in difesa per riconoscere comportamenti anomali che l'occhio umano non vede

L'Intelligenza Artificiale come alleata della difesa

La stessa tecnologia che potenzia gli attacchi viene usata in difesa. La differenza chiave: l'IA difensiva analizza in secondi ciò che un analista umano impiegherebbe ore a esaminare. Per le PMI senza team IT dedicato, è un moltiplicatore di capacità.

AI usata dagli attaccanti	AI usata in difesa
Genera phishing personalizzato e convincente	Rileva comportamenti anomali in tempo reale
Automatizza la ricerca di vulnerabilità	Correla migliaia di eventi per trovare pattern
Crea malware che si adatta per evadere i controlli	Blocca minacce mai viste prima (zero-day)
Produce deepfake per frodi BEC avanzate	Riduce i falsi positivi rispetto ai sistemi tradizionali

Caso studio: come va a finire (davvero)

Negozio articoli moto e bici con e-commerce, 7 persone, Toscana. 2023.

Lun 09:12	**Dipendente apre allegato PDF da 'fornitore'** L'email sembrava autentica - mittente noto, tono professionale. **Era malware.**
Lun 09:18	**Il ransomware inizia a cifrare i file in rete condivisa** In 6 minuti dall'apertura, tutti i file sulla rete condivisa vengono cifrati.
Lun 09:45	**Schermata di riscatto: 'Paga €4.500 in Bitcoin entro 72h'** Tutti i PC mostrano lo stesso messaggio. L'attività si ferma completamente.
Mar–Ven	**Tentativo di ripristino** Backup parziale e non verificato: 2 anni di dati persi definitivamente.
2 settimane	**Attività bloccata - e-commerce inutilizzabile** Ordini, persi, clienti non serviti, fatture non emesse.
Costo totale	**Stimato €33.000 tra perdita dati, fermo, consulenza tecnici, ordini persi**

Cosa sarebbe bastato per evitarlo

Antivirus aggiornato

Costo: € 50/anno per PC

Avrebbe bloccato il malware all'apertura

Backup automatico giornaliero e/o offline verificato

Costo: € 80 hard disk più 30min. a settimana

Ripristino completo in poche ore invece di settimane

Formazione bases

Costo: da 0 a 100€

Il dipendente avrebbe riconosciuto l'email falsa

Totale prevenzione:
con poco più di 100 euro e qualche ora di attenzione si sarebbe evitato un danno da 33.000 euro

Grazie per l'attenzione!

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Sezione Regionale Toscana
Albo Nazionale Gestori Ambientali