Vademecum sulla sicurezza IT in azienda: come implementarla

Piccola guida pratica per proteggere il proprio lavoro dai cybercriminali
e dagli incidenti IT con consigli operativi e checklist da conservare e consultare

Business Provider
COREUP

Come preservare dati sensibili, sistemi e know-how aziendale

Perché per un'azienda è fondamentale investire sulla sicurezza informatica (anche in ottica NIS2)?

Di seguito alcune considerazioni ed esempi che mettono in luce vulnerabilità e pericoli da cui è importante difendersi (per il bene dell'azienda e delle persone che collaborano con essa).
Partiamo dalla prossima entrata in vigore della ***direttiva europea NIS2 sulla sicurezza informatica*** *e ragioniamo sull'impatto che un incidente informatico potrebbe avere su tutta la catena di approvvigionamento:*

Supply Chain Attack

Obiettivo della NIS2 è creare un comune livello di cybersicurezza in tutti gli Stati membri dell'Unione. Per questo motivo la sicurezza IT in ottica NIS2 riguarda non solo le aziende identificate come "critiche" ma anche quelle che fanno parte della loro catena di approvvigionamento.
Se la **Vostra azienda** costituisce un anello della supply chain di un'azienda direttamente interessata dalla NIS2 e non garantisce alti livelli di sicurezza IT a clienti e fornitori, potrebbe ritrovarsi nella posizione di:

1. doversi adeguare agli standard su richiesta di un cliente o di un fornitore (nella migliore delle ipotesi);
2. essere sostituito da un altro partner commerciale che investe nella sicurezza informatica garantendo una certa resilienza.

Differenze della NIS2 rispetto alla NIS:

IMPORTANTE #1: Le aziende interessate dalla direttiva NIS2 devono compiere una serie di azioni per prepararsi al recepimento nell'ordinamento nazionale (17 ottobre) e alla successiva entrata in vigore. Da quel momento in poi gli organi dirigenziali di un'azienda saranno ritenuti DIRETTAMENTE RESPONSABILI in caso di attacchi e danni informatici. Non più una questione legata solo all'ambito IT, bensì un problema che coinvolge TUTTA L'AZIENDA.

IMPORTANTE #2: Viene introdotto un processo di vigilanza affidato ad autorità competenti che controllano lo stato delle misure reattive e proattive adottate dalle aziende al fine di garantire un elevato livello di cibersicurezza.

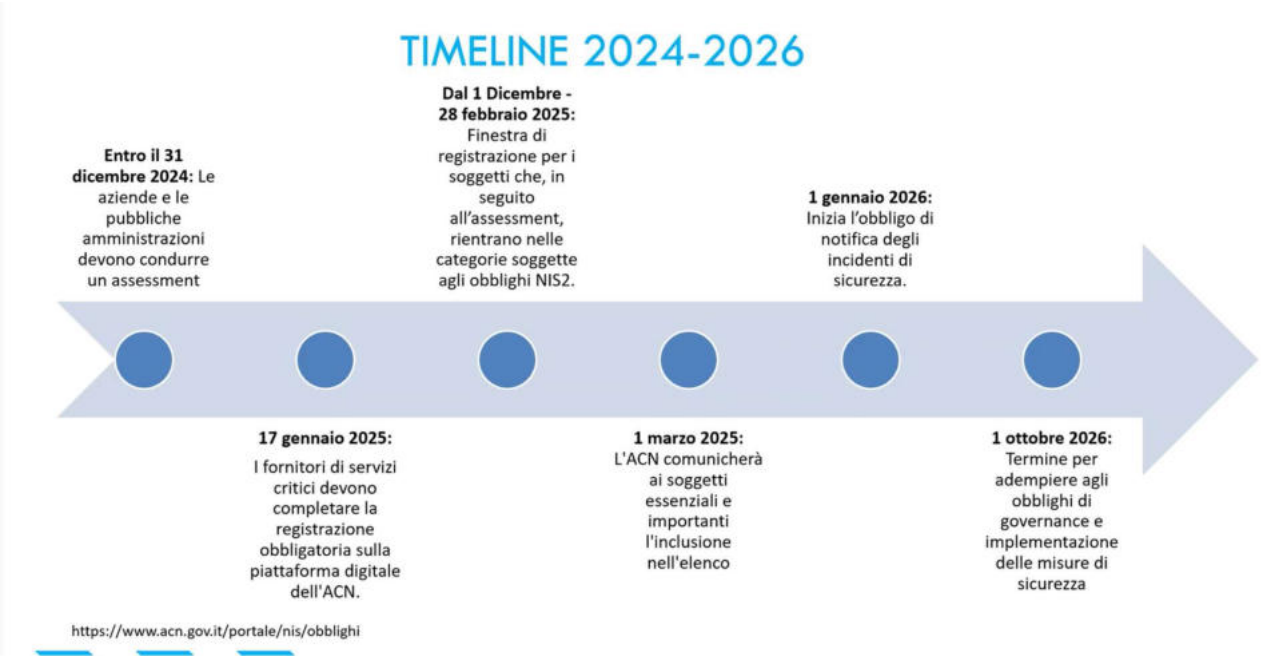

Figura 1 - NIS2: le prossime date importanti

T. 030.4194040
M. info@coreup.it
W. www.coreup.it

Possibili scenari che potrebbero mettere a rischio l'attività dell'azienda

SE AD ESSERE ESPOSTI/ATTACCATI SIETE VOI: L'azienda potrebbe ritrovarsi nella posizione di dover comunicare a clienti e fornitori che alcuni dei loro dati sensibili sono stati rubati o che, a causa di un incidente informatico, gli impianti sono fermi e la produzione subirà un rallentamento che causerà inevitabilmente ritardi a cascata su tutta la catena di approvvigionamento. Potrebbe anche profilarsi una situazione nella quale un cliente o fornitore chieda un risarcimento danni per l'impatto che l'incidente informatico può avere avuto sull'attività. Oltre alle perdite finanziarie, vanno inoltre sempre considerati i danni d'immagine. Essere percepita dai partner commerciali come una realtà "poco sicura" non giova di certo alla salute del brand.

SE AD ESSERE ESPOSTO/ATTACCATO È UN VOSTRO CLIENTE O UN FORNITORE: L'azienda potrebbe ricevere la comunicazione da un cliente o da un fornitore rispetto a un attacco hacker che li ha colpiti mettendo a repentaglio anche il vostro lavoro, i dati e il know-how aziendale. Questo potrebbe causare fermi e ritardi, ma affrontare una comunicazione del genere sapendo di aver già agito preventivamente per proteggere l'azienda, è sicuramente lo scenario migliore per arginare i danni. Dato che non si può controllare costantemente lo stato di sicurezza IT delle aziende con cui si lavora, la scelta più lungimirante è sempre quella di proteggersi direttamente e al meglio, facendo affidamento sui propri sistemi di difesa (firewall, Nas, antivirus, servizi di MSP per il monitoraggio costante dell'infrastruttura IT, formazione del personale interno, e molto altro ancora).

Esempi di attacchi hacker:

1. **Esempio di phishing:** 2018, Tecnimont, Italia. L'azienda leader nel campo dei servizi e delle soluzioni innovative integrate di ingegneria e costruzione per l'industria petrolchimica e fertilizzanti è stata truffata per 17 milioni di dollari con una semplice e-mail proveniente (in apparenza) da un superiore che ordinava un bonifico. La mail era però artefatta (con una lettera in più o in meno nell'indirizzo), e tuttavia presa sul serio. A distanza di poco tempo un altro manager del Gruppo si vede recapitare una mail con la richiesta di un altro bonifico di 5 milioni che viene eseguito perché la mail risultava firmata dal direttore finanziario in persona: peccato che l'indirizzo e-mail avesse una vocale in meno. Oltre ad aver avviato un procedimento disciplinare interno, l'azienda si rivolge alla Procura di Milano che però respinge la richiesta di sequestro conservativo dei residui soldi bloccati perché nessuno dei segmenti criminosi si è svolto in Italia.

2. **Esempio di attacco attraverso telefono**: 2023, MGM Resorts, USA - È bastata una telefonata di pochi minuti per mandare al tappeto questo colosso da 33 miliardi di dollari: gli hacker hanno contattato l'helpdesk dell'azienda fingendo di essere un dipendente e chiedendo di resettare la password del profilo utente. L'attacco ha minato i sistemi di prenotazione, le chiavi elettroniche delle camere, i bancomat e le slot machine. La causa principale di questo disastro è stata la mancanza di una strategia di difesa dagli attacchi cibernetici, sottovalutando quindi i rischi a cui l'azienda era esposta.

3. **Esempio di attacco malware ransomware**: Virus "WannaCry", 2017 - Il virus ha infettato oltre 200.000 computer in 150 paesi diversi e ha richiesto un riscatto in bitcoin per sbloccare i dati crittografati fruttando ai cybercriminali circa 100.000 dollari – cifra modesta se si pensa alla portata mondiale dell'attacco. Questo attacco ransomware ha sfruttato una vulnerabilità del sistema operativo Windows: il virus, una volta entrato nei sistemi operativi, ha cominciato a criptare i file sul computer, rendendoli inaccessibili. Poi, gli utenti attaccati si sono visti recapitare una richiesta di riscatto con pagamento in bitcoin per ripristinare l'accesso ai dati.

4. **Esempio di attacco tramite chiavetta usb infetta:** 2010, Stabilimento nucleare in Iran - I sistemi della centrale nucleare non erano collegati a Internet, per motivi di sicurezza. La centrale è però stata ugualmente attaccata da un virus che, per sferrare l'attacco, doveva essere eseguito su un computer, poiché doveva modificare uno dei file di configurazione per eseguire il suo codice all'interno della centrale stessa. Allora come è stato possibile? Attraverso i dipendenti dell'azienda: probabilmente qualcuno ha lasciato cadere una chiavetta USB infetta vicino a un addetto della centrale, che l'ha trovata e ha avuto la brillante idea di collegarla al suo computer per vederne il contenuto. Una volta all'interno della rete, il malware si è diffuso.

Business Provider COREUP

LA GESTIONE DEL RISCHIO

Proteggere le nostre informazioni vuol dire analizzare le situazioni e gli ambiti in cui sono trattate e **valutare i rischi di sicurezza associati.**

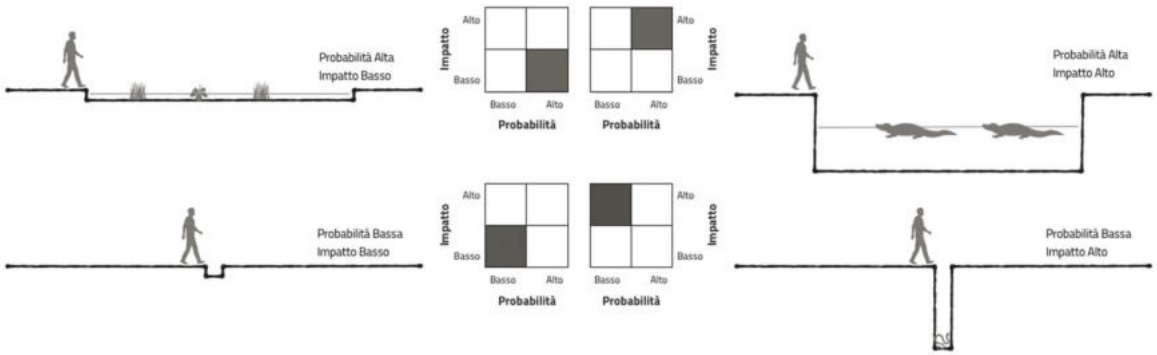

Figura 2 - La possibilità che le minacce digitali compromettano l'integrità dei sistemi operativi, di dati e delle reti va calcolata ad analizzata con gli strumenti giusti, come il Vulnerability Assessment.

Gli attacchi hacker possono bloccare la produzione per giorni: cosa comporta questo per la tua azienda?

RIFLESSIONE: Ogni attacco hacker è **sempre** ramificato perché un solo colpo danneggia diversi ambiti contemporaneamente:

1. Produzione ferma = forti perdite finanziarie
2. Furto e perdita di dati sensibili = anche se non si può (ancora) dare un valore economico a ogni singolo dato, indubbiamente si crea un danno indotto (finanziario e di immagine)
3. Richiesta di riscatto = una questione etica e finanziaria da gestire con estrema cautela
4. Ripristino dei sistemi = costo del lavoro di chi dovrà occuparsi di riportare tutto alla normalità
5. Danno d'immagine = un'azienda che viene percepita dai partner commerciali e dai clienti come non sicura subisce sicuramente un calo della fiducia
6. Rischio per la stabilità economico-finanziaria: un attacco cyber comporta costi e perdite che possono essere così ingenti da mettere in ginocchio un'attività.

❓ **È possibile circoscrivere i danni derivanti da un attacco informatico?**
✅ Sì, ecco come:

A. Diffusione dell'**igiene informatica** e della **cultura del rischio IT** formando il personale e i collaboratori dell'azienda (esistono delle piattaforme dedicate alla formazione su questi temi, lo sapevi?) – a tal proposito, nelle pagine successive troverete 2 comode checklist da conservare!
B. Investimenti sulla **sicurezza IT** con sistemi di sicurezza adeguati (NAS, Firewall, antivirus, e altro ancora)
C. Monitoraggio proattivo e costante dell'infrastruttura di rete per intervenire tempestivamente in caso di attacchi o problemi informatici (**servizi MSP**)
D. **Test periodici** per il controllo del livello di sicurezza IT (Vulnerability Assessment e Penetration Test)
E. **Assicurazione** informatica

Igiene informatica: una guida pratica con checklist per tenere al sicuro i tuoi dati sensibili

L'**igiene informatica** (cyber hygiene) comprende le buone prassi da seguire per ridurre al minimo i rischi derivanti dall'utilizzo di sistemi informatici per preservare l'integrità e la sicurezza dei dati sensibili.

L'igiene informatica come cultura aziendale: perché?

Si tratta di un insieme di semplici regole e routine che aiutano a tenere al sicuro ed efficienti i nostri dispositivi informatici. Sempre più spesso si parla di **cultura** rispetto alla **sicurezza informatica aziendale**: l'applicazione di buone norme di comportamento responsabile e proattivo in azienda, formando e informando i collaboratori su rischi e pericoli cyber, è il primo "antivirus" che funziona davvero per contrastare possibili attacchi esterni.

Inoltre, è bene ricordare che il pericolo non arriva solo da fuori, dato che molto spesso i sistemi IT aziendali riscontrano problemi a causa di un errore umano di una risorsa interna all'organizzazione. Sono cose che possono capitare, ma se nella cultura aziendale entra l'igiene informatica come step imprescindibile, i danni possono essere evitati o circoscritti.

Da una cultura aziendale consapevole sulla cybersecurity nasce quindi una responsabilità condivisa che evolve in priorità per tutti i reparti, gli utenti e i collaboratori, a ogni livello.

Quali problemi evita la cyber hygiene?

Applicare costantemente le pratiche di igiene informatica permette di evitare e/o mitigare:

1. Violazioni della sicurezza (minacce hacker, phishing, malware, virus)
2. Perdita di dati: senza un backup ricorrente si corre il rischio di perdere per sempre dati sensibili importanti in seguito a un attacco hacker o un virus
3. Vulnerabilità del dispositivo a causa di software non aggiornati e antivirus obsoleti (i programmi obsoleti possono infatti contenere vulnerabilità che gli hacker sono in grado di sfruttare)

Quindi, mantenendo una buona igiene informatica, un'organizzazione riduce al minimo il rischio di interruzioni operative così come la compromissione o la perdita dei dati (data breach intenzionale o non intenzionale).

Checklist cyber hygiene per gli utenti

- Aggiorno regolarmente i sistemi e i software:
  - Aggiorno regolarmente le app, i browser Web, i sistemi operativi, l'antivirus e il firmware per usare le versioni più recenti che hanno corretto eventuali problemi di sicurezza;
  - Ho configurato gli aggiornamenti automatici del software;
  - Elimino le app che non uso più;
  - Scarico le app solo da fonti affidabili o ufficiali;

- Scelgo password sicure e complesse, da modificare periodicamente:
  - Evito di usare la stessa password per account diversi
  - Cambio le mie password regolarmente
  - Le mie password sono lunghe almeno 12 caratteri
  - Le mie password sono composte da una combinazione di lettere maiuscole e minuscole, simboli e numeri
  - Le mie password non sono ovvie, ad esempio non contengono numeri in sequenza ("1234") o informazioni personali facili da indovinare per qualcuno che mi conosce, come la mia data di nascita
  - Evito di condividerle le mie password con altri
  - Uso uno strumento per la gestione delle password per generare, archiviare e gestire tutte le mie password in un unico account online sicuro

- Attivo l'autenticazione a più fattori;

- Proteggo la mia privacy:
  - Disconnetto i profili personali al termine della navigazione facendo il logout;
  - Non pubblico informazioni private sui social (indirizzo di casa, immagini private, numero di telefono o i numeri delle carte di credito);
  - Non partecipo a quiz, giochi o sondaggi sui social media che chiedono informazioni personali sensibili;
  - Presto attenzione alle autorizzazioni che accetto per tutte le app che uso;
  - Utilizzo una password o un PIN per tenere computer e smartphone bloccati;
  - Non divulgo informazioni private quando uso il Wi-Fi pubblico (cercando di evitare il più possibile l'utilizzo di un Wi-Fi pubblico ma se proprio non posso so che devo usare una rete privata virtuale VPN);

  - Per ogni transazione online controllo che si passi da un sito Web sicuro = URL che inizia con https:// e non con http://, e presenza dell'icona del lucchetto a sinistra della barra degli indirizzi;

- Ricorro alla crittografia per cifrare i dati, rendendoli così inutilizzabili in caso di esfiltrazione;
- Faccio attenzione a non pubblicare informazioni personali che potrebbero ricondurre facilmente a una password (es. data di nascita propria e/o dei figli).
- Non clicco su link sconosciuti
- Controllo sempre il mittente delle e-mail in arrivo e non aprire allegati se non si è certi della bontà del messaggio
- Potenzio i filtri antispam
- Faccio backup costanti
- Prima di buttare o vendere un dispositivo, verifico di aver pulito il disco rigido per evitare che altri possano accedere alle mie informazioni personali

Quante di queste cose fai già regolarmente o quali invece devi integrare nella tua routine lavorativa?

T. 030.4194040
M. info@coreup.it
W. www.coreup.it

Checklist cyber hygiene per l'azienda

A livello aziendale mantenere una corretta **cyber hygiene** non è affatto semplice. Il flusso dei comportamenti da tenere e gli aspetti da controllare sono davvero molti, soprattutto se pensiamo a realtà frammentate in cui si lavora in luoghi e fusi orari diversi, da **remoto** e con un volume importante di utenti e dispositivi connessi contemporaneamente. Ecco perché, sempre più spesso, le aziende scelgono un partner strategico esterno che le aiuti nel completare tutte quelle procedure di routine (che richiedono tempo) utili al mantenimento della **sicurezza degli ambienti IT**. Stiamo parlando degli **MSP** (Managed Service Provider) che si occupano di monitoraggio proattivo e costante dell'infrastruttura IT per supportare il lavoro degli IT Manager interni e studiare un **programma strategico di cybersecurity**.

Ecco alcune delle attività più importanti che l'azienda in primis deve compiere regolarmente per tenere alti i livelli di **sicurezza** contro il **furto** di dati sensibili e del know-how aziendale:

1. Eseguire regolarmente il Backup per salvare i file importanti in un luogo separato e sicuro.
2. Assicurarsi che il Firewall sia configurato correttamente per tenere i malintenzionati fuori dai sistemi privati.
3. Installare gli aggiornamenti software e le patch di sicurezza disponibili sui dispositivi.
4. Usare la crittografia per garantire la protezione dei dati aziendali sensibili.
5. Monitorare e controllare tutti gli endpoint: non solo pc, smartphone o tablet, ma anche i centralini intelligenti, le videocamere di sorveglianza, i terminali POS.
6. Installare software di sicurezza, come antimalware e antivirus.
7. Richiedere l'autenticazione e controllare gli accessi. Non solo il PIN ma anche l'autenticazione a più fattori (come, ad esempio, un codice monouso inviato sul cellulare dell'utente).
8. Adottare una politica delle password che stabilisca regole e requisiti sulle credenziali degli utenti (lunghezza, tipi di carattere, etc).
9. Inventariare, controllare e gestire tutte le risorse IT: solo così è possibile identificare una ipotetica superficie di attacco su cui potrebbero atterrare i malintenzionati.
10. Controllare applicazioni, siti Web e indirizzi e-mail che gli utenti possono e non possono utilizzare.
11. Monitoraggio regolare e costante della rete alla ricerca di minacce e vulnerabilità.
12. Segmentare la rete per limitare la distanza che i cyber criminali possono percorrere se riescono a entrare in una rete.
13. Formare ed educare tutti i collaboratori dell'azienda (non solo il reparto IT) sulla consapevolezza della sicurezza per mitigare il rischio informatico.
14. Pianificare una strategia di gestione degli incidenti e delle crisi informatiche. Dato che le conseguenze di un attacco possono includere perdite finanziarie, interruzioni operative, multe normative e danni alla reputazione, l'azienda deve contare su un sistema che combini competenze esecutive, tecniche, operative, legali e di pubbliche relazioni.

Figura 3 - Come si configura un'analisi delle vulnerabilità e del rischio informatico.

T. 030.4194040
M. info@coreup.it
W. www.coreup.it

MSP (Managed Service Provider): monitoraggio e risposta agli incidenti

Un MSP assicura un supporto costante, una gestione proattiva e un monitoraggio continuo dell'ambiente informatico per limitare problemi, disservizi e tempi di fermo.

Come funziona l'assistenza proattiva?
Grazie ai servizi gestiti da un MSP (Managed Service Provider) all'azienda viene garantito il **monitoraggio** costante e la **manutenzione** sempre aggiornata sulla sua **infrastruttura IT**.
È un approccio che tende a **prevenire** e a limitare il pericolo di fermi aziendali. Molto spesso i dipendenti dell'azienda non si rendono nemmeno conto del problema perché grazie al **monitoraggio 24/7 della rete IT** è lo stesso MSP ad intervenire da remoto, senza bisogno di essere allertato dal cliente. Questo tipo di approccio è possibile solo scegliendo un partner tecnologico esperto, con le migliori competenze IT necessarie in quel momento. La gestione proattiva permette, quindi, di valutare e intervenire in tempi brevi per scongiurare eventuali down-time.

Vantaggi:

- Gestione, monitoraggio e manutenzione IT della rete 24/7
- Continuità operativa garantita
- Prevenzione dei guasti tecnici e riduzione (o addirittura azzeramento) dei disservizi della rete
- Riduzione al minimo dei tempi di non funzionamento (down-time)
- Assistenza telefonica e da remoto illimitata
- Rete IT più sicura e sempre aggiornata
- Unico referente IT: risparmio di tempo/denaro
- Personale altamente qualificato senza dover assumere figure dedicate
- Gestione diretta dei fornitori (Software House, Hardware, etc)
- Zero sorprese di spesa: comodo contratto a tariffa fissa
- Rinnovo parco macchine e periferiche con comoda formula noleggio

---

Siamo a disposizione per mettere al sicuro il vostro lavoro.

Luca Belotti
CEO di Core Up Srl