Cyber hygiene: che cos'è l'igiene informatica e perché tutte le aziende dovrebbero praticarla

Testi a cura
di Laura Zanotti - Fonte TechTarget

INDICE DEGLI ARGOMENTI

Cyber hygiene o igiene della sicurezza informatica come insieme di pratiche che vanno eseguite regolarmente per mantenere **in buona salute e sicurezza** dispositivi, reti, sistemi, identità, dati, utenti e organizzazioni. L'approccio può sembrare lapalissiano, fondandosi su **un'analogia tra le buone pratiche di igiene personale e le buone pratiche della sicurezza informatica.** Vero è che certe azioni preventive di igiene in entrambi i casi aiutano a mantenere l'integrità del sistema immunitario sia fisico che aziendale. Ad esempio, come lavare spesso le mani contribuisce ad arrestare la diffusione delle malattie, **seguire misure precauzionali di igiene informatica contribuisce a prevenire violazioni dei dati e altri incidenti di cybersecurity**. In entrambi i casi, infatti, se perseguite in modo costante e corretto ogni giorno, regole e procedure aiutano a preservare nel tempo un ottimo stato di salute.

1 DALLA CULTURA ALLA POSTURA DELLA SICUREZZA INFORMATICA

L'obiettivo dell'igiene informatica è proteggere da furti o attacchi le informazioni, soprattutto quelle sensibili o legate alla proprietà intellettuale di un'azienda. **Nel momento in cui la cyber hygiene viene applicata con costanza sia a livello di organizzazione che a livello di ogni singolo utente, è oggettivamente possibile ridurre le vulnerabilità e aumentare la postura della sicurezza informatica aziendale.** La postura della sicurezza di un'azienda si riferisce alla forza complessiva del suo programma di protezione informatica, definendo il suo posizionamento rispetto alla capacità di gestire le minacce esistenti ed emergenti. Mantenendo una buona igiene informatica, un'organizzazione riduce al minimo:

- il rischio di interruzioni operative (impatto sulla business continuity)
- la compromissione o la perdita dei dati (data breach intenzionale o non intenzionale)

2

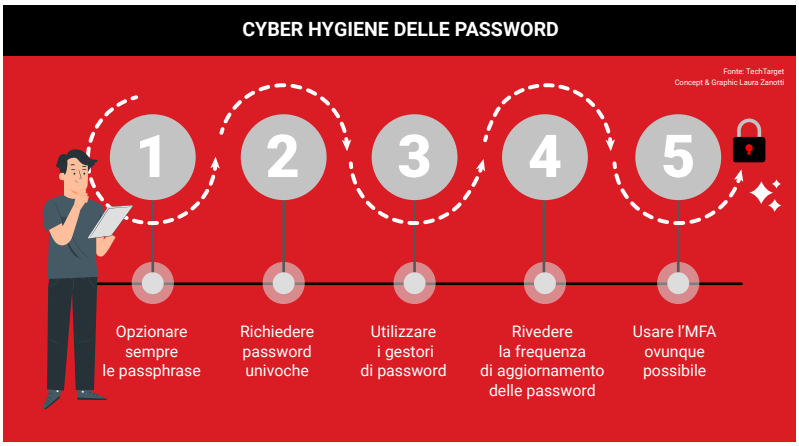
LE BEST PRACTICES DELLA CYBER HYGIENE

Come fanno notare gli esperti, è importante che l'onere dell'igiene informatica non ricada solo sui quadri, sugli analisti e sui tecnici della sicurezza IT. Il punto di partenza è una cultura aziendale più consapevole e quindi matura in relazione a una responsabilità condivisa della cybersecurity che diventa prioritaria per tutti i reparti e tutti gli utenti.

Cyber hygiene lato utenti

Parafrasando Voltaire, in un'azienda che opera nel migliore dei modi possibili, ogni singolo collaboratore o dipendente aiuta a mantenere una corretta cyber hygiene informatica, osservando una serie di comportamenti e procedure, in primis:

- Fare attenzione a non pubblicare informazioni personali che un malintenzionato potrebbe utilizzare per indovinare o reimpostare una password o per accedere in altro modo ad account privati.
- Essere consapevoli di quali informazioni personali sono già disponibili online, che i criminali informatici potrebbero utilizzare negli attacchi di ingegneria sociale.
- Evitare di cliccare su link sconosciuti
- Attivare le patch e fare aggiornamenti costanti
- Potenziare in modo significativo i filtri antispam
- Evitare il Wi-Fi pubblico
- Creare password complesse e univoche
- **Fare backup costanti**



Cyber hygiene lato organizzazione

Mantenere una buona igiene informatica è fondamentale ma tutt'altro che facile data l'ampiezza e la complessità degli ambienti IT. Per i professionisti della sicurezza aziendale significa **applicarsi costantemente a gestire un flusso infinito di comportamenti e attività importanti, a volte anche banali e proprio per questo, spesso trascurate.** Tuttavia, nelle aziende odierne, l'enorme volume di utenti, dispositivi e risorse, spesso distribuiti in ambienti ibridi e multi-cloud, rende estremamente difficile mantenere una corretta cyber hygiene.
Se è vero che il giusto framework di sicurezza IT e gli standard di sicurezza informatica possono aiutare offrendo un punto di partenza per l'organizzazione e la gestione di un programma di sicurezza utilizzando processi, politiche e pratiche consolidate per impostare e dare priorità alle attività di cyber hygiene è altrettanto vitale.

Backup – Eseguire regolarmente il backup dei file importanti in una posizione separata e sicura anche nel caso in cui la rete principale venga compromessa.

Firewall – Assicurarsi che firewall, WAF e router siano impostati e configurati correttamente per tenere i malintenzionati fuori dai sistemi privati.

Gestione delle patch – Installare tutti gli aggiornamenti software e le patch di sicurezza disponibili sui dispositivi di proprietà dell'azienda e su qualsiasi dispositivo personale utilizzato per lavoro.

Crittografia – Utilizzare la crittografia di ultima generazione per garantire la protezione dei dati aziendali sensibili, sia in transito che inattivi oggi e domani, considerando l'evoluzione dell'AI o del calcolo quantistico su cui anche il cybercrime ha iniziato a sperimentare.

Sicurezza dell'endpoint – Oggi, una pletora di dispositivi opera oltre il tradizionale perimetro di sicurezza aziendale. Endpoint, infatti non sono solo i pc, i laptop, gli smartphone o i tablet, ma anche i centralini intelligenti, le videocamere di sorveglianza, le installazioni interattive, i terminali POS e tutti i sensori smartificanti associati alla IoT. Dunque, per evitare di esporre sia gli stessi endpoint che la rete aziendale a un rischio di attacco, è fondamentale istituire un regime di policy e di soluzioni di monitoraggio e controllo tali da permettere di identificare, gestire e proteggere ogni possibile periferica connessa.

Software di sicurezza – Installare software di sicurezza, come antimalware e antivirus, per difendere i sistemi da software dannoso, inclusi virus, ransomware, spyware, worm, rootkit e trojan, assicurandosi non solo che il software sia configurato correttamente ma che vengano eseguite scansioni regolari per rilevare tutte le attività insolite.

Autenticazione e controllo degli accessi – L'autenticazione, o la conferma che un utente o un dispositivo è chi o cosa afferma di essere, è una parte fondamentale della cyber hygiene. La sicurezza stessa dipende dall'autenticazione e dal controllo degli accessi: la capacità di verificare e ammettere determinati utenti escludendone altri. I comuni meccanismi di controllo degli accessi includono il controllo degli accessi basato sui ruoli, che concede autorizzazioni di rete in base alla posizione formale di un utente in un'organizzazione, e il principio del privilegio minimo, che garantisce agli utenti l'accesso solo alle risorse di cui hanno assolutamente bisogno per svolgere il proprio lavoro. Per proteggere le proprie reti, le organizzazioni possono scegliere tra almeno sei tipi di autenticazione. La più rudimentale è l'autenticazione basata sulla conoscenza, che richiede a un utente di condividere credenziali prestabilite, come nome utente e password o PIN. MFA richiede due o

più fattori di autenticazione, come una password e un codice monouso inviato al cellulare o all'indirizzo e-mail dell'utente. L'autenticazione biometrica utilizza identificatori biologici, come la scansione delle impronte digitali o il riconoscimento facciale. Altri tipi di autenticazione includono single sign-on, autenticazione basata su token e autenticazione basata su certificato.

Politica password – Le password semplici o riciclate sono praticamente un invito aperto agli hacker. La creazione di una policy per le password aziendali aiuta a preservare la sicurezza aziendale stabilendo regole, requisiti e aspettative sulle credenziali degli utenti.

Strategia di backup integrata alla governance aziendale – Sviluppare una strategia programmata dei backup a livello aziendale garantisce che le informazioni mission-critical vengano regolarmente duplicate e archiviate in un luogo sicuro. Molti esperti, in base alla criticità dei dati, consigliano di seguire la regola del backup 3-2-1, che richiede l'archiviazione di tre copie dei dati su due diversi tipi di supporto, ad esempio cloud, disco e nastro, e la conservazione di una copia fuori sede.

Broker di sicurezza per l'accesso al cloud (CASB) – Qualsiasi organizzazione che si affida a IaaS, PaaS o SaaS dovrebbe prendere in considerazione l'implementazione di un CASB come parte della propria strategia di igiene informatica. Il software CASB facilita le connessioni sicure tra gli utenti finali e il cloud, applicando le policy di sicurezza aziendali relative all'autenticazione, alla crittografia, alla prevenzione della perdita di dati, alla registrazione, agli avvisi, al rilevamento di malware e altro ancora. Un CASB offre a un'organizzazione una maggiore visibilità sull'utilizzo da parte dei dipendenti delle applicazioni basate su cloud, nonché un maggiore controllo sulla sicurezza dei dati basati su cloud.

Gestione delle risorse di sicurezza informatica – Per proteggere le risorse IT, bisogna prima sapere che esistono. Proprio per questo è opportuno inserire la gestione delle risorse di sicurezza informatica, un sottoinsieme della gestione delle risorse IT (ITAM) che prevede la scoperta, l'inventario, la gestione e il monitoraggio delle risorse di un'organizzazione con l'obiettivo di proteggerle. Anche perché il volume e la varietà sbalorditivi delle risorse IT nelle aziende odierne rendono logisticamente impossibile rintracciarle manualmente tramite fogli di calcolo o database. Inoltre, entità effimere o virtuali di breve durata come macchine virtuali, microservizi e container significano che la superficie di attacco aziendale si contrae e si espande di minuto in minuto.

Liste consentite/bloccate – Controllare quali applicazioni, siti Web e indirizzi e-mail gli utenti possono e non possono utilizzare. Nel primo o nel secondo caso, le liste sono due metodi per presidiare meglio gli accessi. Mentre la lista consentita fornisce un elenco selezionato di applicazioni, processi e file a cui gli utenti possono accedere, la lista bloccata fornisce un elenco a cui gli utenti non possono accedere.

Gestione del registro di sicurezza – Un programma di sicurezza informatica è valido solo quanto la sua capacità di riconoscere attività inappropriate o sospette nell'ambiente IT. Il che non significa che sia facile. Le migliori pratiche per la gestione dei registri di sicurezza includono la registrazione e l'archiviazione degli eventi corretti, la garanzia dell'accuratezza e dell'integrità dei registri, l'analisi dei dati di registro per identificare i problemi e l'utilizzo di strumenti di registrazione per gestire il volume degli eventi.

Monitoraggio della sicurezza – È bene scansionare regolarmente o continuamente la rete alla ricerca di minacce e vulnerabilità, come le porte aperte che

gli hacker potrebbero utilizzare nei loro attacchi. In questo senso è opportuno utilizzare strumenti come SIEM o scanner di vulnerabilità. La scansione e il monitoraggio frequenti migliorano notevolmente l'igiene informatica. Segnalano sia le potenziali minacce attive che i punti deboli a cui gli aggressori potrebbero accedere.

Segmentazione della rete – La segmentazione della rete limita la distanza che i criminali informatici possono percorrere se riescono a entrare in una rete, contribuendo a mitigare il danno e la portata di un attacco.

Formazione sulla consapevolezza della sicurezza – I responsabili IT non possono ottenere una buona igiene informatica da soli. Hanno bisogno del supporto e del coinvolgimento degli utenti finali in tutte le loro organizzazioni, compresi quelli con poca esperienza o interesse per la sicurezza informatica. Educare i dipendenti sul ruolo cruciale che svolgono nella mitigazione del rischio informatico costruendo un efficace piano di formazione sulla sicurezza informatica è un'altra best practice cruciale della cyber hygiene. I programmi di formazione sulla consapevolezza della sicurezza più efficaci trovano nuovi modi per coinvolgere i dipendenti nelle pratiche fondamentali di sicurezza informatica. Gli utenti finali possono quindi mettere alla prova le loro nuove conoscenze con questo quiz sulla consapevolezza della sicurezza.

Strategia di gestione e risposta agli incidenti – Se e quando un'organizzazione subisce un evento di sicurezza, ha bisogno di una risposta agli incidenti (IR) e di una strategia di gestione prestabilite per mitigare il rischio per l'azienda. Poiché le conseguenze di una violazione dei dati possono includere perdite finanziarie, interruzioni operative, multe normative, danni alla reputazione e spese legali, un team IR necessita

di una combinazione di competenze esecutive, tecniche, operative, legali e di pubbliche relazioni. Questo gruppo documenta chi, cosa, quando, perché e come del suo previsto IR, creando un piano che offrirà una direzione chiara in una crisi futura.

3

CYBER HYGIENE DELLA POSTA ELETTRONICA

Nonostante la crescente popolarità delle piattaforme di collaborazione, come Microsoft Teams e Zoom, la stragrande maggioranza delle organizzazioni fa ancora affidamento sulla posta elettronica come principale modalità di comunicazione. Di conseguenza, l'e-mail rimane un popolare vettore di attacco per i criminali informatici che la sfruttano per accedere alle reti e ai dati aziendali. Lo spoofing delle e-mail, ad esempio, è una tattica molto usata dal cybercrime per far sembrare che un messaggio provenga da una fonte attendibile (come un contatto personale o professionale o un noto sito Web di vendita al dettaglio).
Anche in questo caso **la cyber hygiene è indispensabile per impedire ai criminali informatici di ottenere l'accesso non autorizzato agli account di posta elettronica e al contenuto dei messaggi.** Anzi, secondo gli osservatori, stabilire una politica di sicurezza della posta elettronica efficace e aggiornata dovrebbe essere una priorità assoluta. Politiche informative, chiare e concise stabiliscono norme culturali e stabiliscono aspettative comportamentali sull'uso sicuro della posta elettronica.
È importante **delineare il rischio intrinseco della posta elettronica e dissipare qualsiasi falso senso di sicurezza che i dipendenti potrebbero avere** nell'usare questa tecnologia onnipresente. Dal punto di vista tecnico, i leader IT devono comprendere l'importanza dei principali protocolli di sicurezza e-mail e come possono aiutare a proteggere i messaggi aziendali.

4

CYBER HYGIENE: QUALI SONO I VANTAGGI

Le conseguenze di una violazione dei dati possono includere perdite finanziarie, sanzioni, tempi di inattività operativa, destabilizzazione organizzative, danni alla reputazione dell'organizzazione e responsabilità legali. La Cyber hygiene costituisce le fondamenta su cui sono costruite strategie di sicurezza informatica efficaci, promuovendo una cultura della sicurezza e contribuendo a un ambiente digitale più sicuro per tutti. Abbracciare l'igiene informatica è un passaggio fondamentale per proteggersi dalle minacce informatiche e garantire un futuro digitale sicuro e resiliente. Come si desume dalla lista di consigli di questo articolo, la cyber hygiene aiuta le aziende a raggiungere una sicurezza informatica ottimale. I vantaggi principali sono:

Sicurezza migliorata

Praticando una buona igiene informatica, le aziende possono migliorare la loro posizione di sicurezza complessiva e ridurre il rischio di essere hackerate o attaccate.

Riduzione dei costi

Adottare le pratiche di Cyber hygiene aiuta le aziende a risparmiare denaro riducendo la necessità di costose misure di sicurezza ed evitando multe o altre sanzioni per il mancato rispetto delle normative.

Reputazione migliorata

È probabile che un'azienda che dimostra una buona igiene informatica venga vista in modo più favorevole da clienti, partner e altre parti interessate. Ciò può portare a migliori vendite e opportunità di crescita.

Maggiore produttività dei dipendenti

Quando le aziende adottano pratiche di Cyber hygiene informatica, è meno probabile che i dipendenti subiscano tempi di inattività a causa di malware o altre violazioni della sicurezza. Ciò può portare a una maggiore produttività e a un minor numero di scadenze mancate.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ