Sicurezza fisica e Privacy nel GDPR

La protezione dei dati personali e aziendali oltre la cyber security come previsto dalle nuove regole europee

Un white paper Reportec

Sommario

Sicurezza fisica e Privacy nel GDPR 3

La riservatezza del dato 4

Sicurezza fisica e requisiti di privacy nel GDPR 6

L'importanza delle protezioni fisiche e il visual hacking 8

I Privacy Filter3M contro i visual hacker 10

Avvertenze
Pubblicato nel 2018

Sicurezza fisica e Privacy nel GDPR

La protezione dei dati personali e aziendali oltre la cyber security come previsto dalle nuove regole europee

Pensando alla protezione dei dati il pensiero si concentra soprattutto sulla sicurezza "logica" e sui rischi indotti dalle minacce del cyber crime, ma il GDPR (General Data Protection Regulation), che riguarda tutte le imprese, introduce alcune novità rispetto alla legislazione italiana e impone pratiche relative anche alla sicurezza fisica.

Il ritardo con cui le imprese italiane hanno approcciato il processo di compliance comporta ulteriori rischi.

In questo white paper evidenziamo alcune regole che potrebbero sfuggire ai responsabili della sicurezza dei dati, soprattutto perché il nuovo Data Officer (figura introdotta appunto dal GDPR), potrebbe, magari proprio per la pressione dell'imminente scadenza, concentrarsi sugli aspetti più "tradizionali", legati alla sicurezza logica, trascurando i requisiti richiesti dal GDPR in termini di sicurezza fisica.

Lo spirito su cui è basata la normativa è di ampio respiro, perché l'intenzione del legislatore è di ostacolare il più possibile i tentativi di elusione delle norme. Per questo, in particolare, non si fa riferimento a specifiche tecnologie, ma a pratiche da definire, adottare e perseguire. L'at-

La riservatezza del dato

Il filone d'interesse principale che ha portato all'emanazione del GDPR è quello relativo alla riservatezza del dato personale, dove per dato personale s'intende qualsiasi informazione correlata a una persona fisica o soggetto interessato. I dati personali possono dunque avere natura estremamente diversificata, da un nome, una foto, un indirizzo di posta elettronica, coordinate bancarie, post su siti di social network, informazioni mediche, o persino l'indirizzo IP di un computer. Altro aspetto importante riguarda la proprietà del

tenzione è anche sul fattore umano. In altre parole, le prassi aziendali e il comportamento dei dipendenti nell'utilizzo dei sistemi e degli impianti aziendali devono conformarsi alle esigenze di sicurezza, in base a precise policy.

La combinazione delle protezioni amministrative, informatiche e fisiche può contribuire a tutelare la sicurezza dei dati personali sensibili e dimostra l'impegno e il rigore di un'organizzazione nell'ambito della riservatezza dei dati.

Le imprese posseggono più dati sensibili di quanto immaginino. Anche piccole realtà possono trovarsi informazioni riguardanti i propri dipendenti e clienti che devono proteggere. Questo senza considerare la cosiddetta "digital transformation" e i big data che generano, cioè l'enorme quantità di dati che ciascun individuo produce quando chatta attraverso un'app dello smartphone, posta una foto su un social network, effettua un pagamento con la carta di credito e viene "intercettato", grazie a e-tag, web beacon, cookie e altri strumenti di monitoraggio. Lo sviluppo nel campo dell'intelligenza artificiale accresce la capacità di sfruttare le informazioni definendo profili dettagliati.

Raccogliere dati personali appartenenti a vari soggetti è un'attività normale per un'impresa, ma per l'impresa moderna diventa una necessità critica atta a garantire una sempre più adeguata relazione con gli attori della catena del valore e con i clienti in particolare.

D'altro canto, la riservatezza dei suddetti dati, prima ancora che un obbligo di legge, è cruciale per sostenere un rapporto di fiducia con clienti, partner e fornitori.

La Sicurezza del dato, sia fisica sia logica non si limita agli aspetti tecnici, perché è estremamente importante il cosiddetto "fattore umano". Prassi aziendali, operatività e comportamenti degli utilizzatori di sistemi e impianti debbono essere conformati alle esigenze di sicurezza attraverso la creazione di policy aziendali e relative procedure di utilizzo/fruizione delle infrastrutture digitali e telematiche, considerando che le procedure aziendali devono essere concepite per bilanciare i diritti della persona e l'operatività aziendale.

dato stesso. Dopo circa tre anni di discussione in seno alla commissione europea che ha preparato il regolamento, si è tirata una somma, che non ha soddisfatto tutti ma sancisce due punti fermi:

- i dati personali appartengono agli individui e non alle imprese;
- i cittadini hanno diritto alla privacy dei loro dati.

La riservatezza di questi deve essere dunque garantita, mentre per l'utilizzo dei dati da parte delle aziende è stato definito uno "strumento": la pseudonimizzazione. In pratica si tratta di sostituire i record con degli pseudonimi, in modo che non siano riconoscibili né riconducili al soggetto cui si riferiscono. In questo nodo i dati possono essere usati per analisi e altri scopi di natura statistica.

Ovviamente, se si vogliono sfruttare i dati, per esempio per le strategie di marketing, le imprese devono disporre di tutti i permessi necessari, ma devono anche fare in modo che gli operatori non compromettano la riservatezza dei dati.

Si presenta il problema della condivisione dei dati lungo la filiera operativa, con set di dati che vengono trasmessi a vari reparti o a fornitori esterni, per esempio al fine di pagare un collaboratore, condurre ricerche di mercato, lanciare una campagna di marketing via e-mail o per tracciare il grado di coinvolgimento dei clienti. Operazioni di questo tipo rappresentano un rischio di utilizzo improprio o non autorizzato dei dati personali. Anche perché l'impresa potrebbe avere il diritto di usare quei dati, ma l'operatore potrebbe non essere a conoscenza di come e perché ne è venuto in possesso e come e perché i dati siano stati originariamente raccolti, né potrebbero comunicare tali informazioni ad altri operatori lungo la filiera.

Sicurezza fisica e requisiti di privacy nel GDPR

Dando per scontato che le prassi nell'utilizzo dei dati siano esplicate conformemente alla legge, bisogna porre attenzione a ulteriori rischi che riguardano anche restrizioni fisiche.
Pure in questo caso, il regolamento, non esplicita strumenti tecnologici, ma suggerisce attente analisi, affinché sia garantita la massima protezione: in altri termini si deve poter dimostrare di aver pensato a tutto e predisposto adeguate misure di mitigazione, se non totale eliminazione del rischio.
In generale, poiché spetta all'impresa garantire la riservatezza questo significa che il responsabile del Trattamento dei Dati, come anche l'incaricato del trattamento, devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio.

La DPIA

Una DPIA (Data Protection Impact Assessment) consiste in una valutazione dell'impatto in caso di violazione. Prevista nell'articolo 35 e nelle Premesse 83-84 del GDPR, si tratta di una stima richiesta per attività ad alto rischio che aiuta le organizzazioni a determinare l'origine, la natura, la particolarità e la gravità dei rischi e ad attuare le misure appropriate per ridurre tali rischi, come per esempio mediante crittografia.
Nel valutare i rischi per la sicurezza dei dati, occorre prendere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione, la perdita o l'alterazione accidentale o illecita, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, memorizzati o altrimenti elaborati che possono portare a danni fisici, materiali o immateriali.

Gli articoli 24 e 32 del GDPR

Nel GDPR "rischio" è la parola chiave: in sostanza, si rende necessaria un'analisi dei rischi che permetta di definire le adeguate contromisure di sicurezza tecniche e organizzative

Le imprese italiane non sono pronte per il GDPR, anche se partivano avvantaggiate

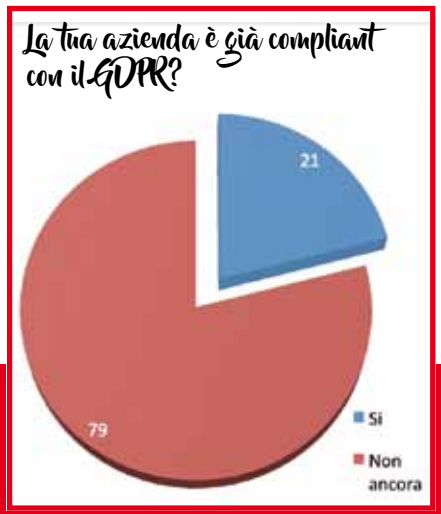
Le imprese italiane non sono ancora pronte per il GDPR, come mostrano diverse ricerche nazionali e internazionali (per esempio cfr.: "Rapporto Clusit 2018" o "Cambi di paradigma: Previsioni Trend Micro sulla sicurezza per il 2018") e un'inchiesta realizzata dalla redazione di Reportec nel gennaio 2018, che, pur senza pretese di rigorosità statistica nella metodologia e nella scelta del campione, fornisce un dato netto circa il ritardo nell'adeguamento. Peraltro, i risultati ottenuti, costituiscono una base di riflessione che ci permette d'integrare le opinioni espresse da numerosi esperti, sia in seno a società di ricerca qualificate, sia presso vendor del settore ICT, specializzati in sicurezza.

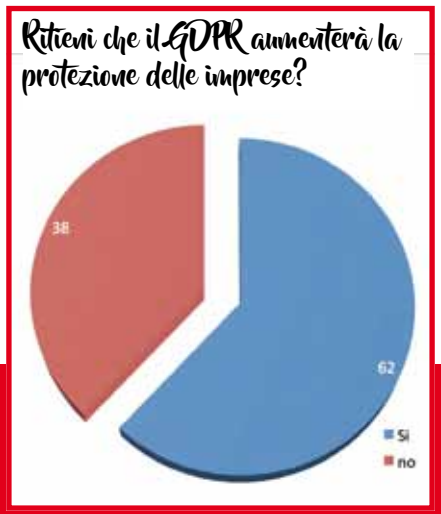
RENDERE SICURO IL PROPRIO AMBIENTE	*Proteggere i sistemi critici dall'ambiente IT generale*
	Ridurre la superficie di attacco e le vulnerabilità
	Rendere sicuro l'ambiente fisicamente
CONOSCERE E LIMITARE GLI ACCESSI	*Prevenire la compromissione delle credenziali*
	Gestire le identità e isolare i privilegi
RILEVARE E RISPONDERE	*Rilevare attività anomale sui sistemi o nelle transazioni dei dati*
	Pianificare la risposta agli incidenti e le notifiche sugli eventi dolosi

al fine di garantire la sicurezza del trattamento.
L'Articolo 24 del GDPR delinea la responsabilità di un'organizzazione nell'attuazione di "appropriate misure tecniche e organizzative" per garantire e dimostrare il corretto trattamento dei dati personali.
L'Articolo 32 compie un ulteriore passo in avanti spiegando che "nel valutare il livello di protezione appropriato, si dovrà tener conto dei rischi che sono presentati dall'elaborazione, e in particolare, dalla distruzione, perdita, alterazione accidentale o illecita, dalla divulgazione non autorizzata o dall'accesso a dati personali trasmessi, memorizzati o altrimenti elaborati".
Un aspetto importante di questo regolamento è l'enfasi sulla prevenzione degli accessi non autorizzati. Sotto questo aspetto la sicurezza fisica è essenziale. In particolare, si possono proteggere i dati contro le minacce umane interne ed esterne che mirano a sfruttare eventuali lacune all'interno delle strutture fisiche dell'organizzazione o dei suoi dipendenti. Queste operazioni includono la limitazione dei dati che possono essere osservati, sottratti o in altro modo ottenuti.

Il framework SWIFT

Il GDPR non è l'unico regolamento che include aspetti di sicurezza fisica nell'ambito della protezione dei dati: norme al riguardo sono state introdotte appena introdotte anche nel framework SWIFT (Society of Worldwide Interbank Financial Telecommunication), che riguarda strettamente il mondo finanziario e le transazioni economiche.
Per una maggiore garanzia è specificamente prevista nel framework la protezione fisica degli ambienti, anche per tenere al sicuro le credenziali degli operatori SWIFT. Si richiede, in particolare, oltre alla gestione delle identità, proprio di rendere sicuro l'ambiente fisicamente.





È bene ricordare che il GDPR è entrato in vigore nel maggio del 2016. Il parlamento Europeo ha concesso due anni di tempo per adeguarvisi.
Erroneamente, la data del 28 maggio 2018 è stata interpretata come quella in cui il nuovo regolamento sarebbe diventato operativo e, per molte imprese, rappresenta il momento in cui è semplicemente sufficiente dimostrare che si è cominciato ad attuare un piano per la protezione dei dati. In verità è la data in cui potrebbero essere applicate le prime sanzioni amministrative. Il rischio che si corre è di subire le pene pecuniarie, che arrivano a cifre molto elevate: 20 milioni di euro o fino al 4 per cento del fatturato globale annuo dell'azienda (a seconda di quale sia l'importo maggiore).
Uno spauracchio che non è servito ad accelerare i tempi per la compliance, nonostante che in Italia molte delle norme introdotte erano già previste.
Ciononostante, alcuni esperti consideravano due anni non adeguati per il recepimento dei complessi cambiamenti legali che

L'importanza delle protezioni fisiche e il visual hacking

Per quanto critica sia la sicurezza informatica, anche i controlli amministrativi e fisici a basso contenuto tecnologico sono ugualmente importanti e correlati alla cyber security, come dimostrano diverse analisi di esperti del settore. Sono in crescita, infatti (cfr Rapporto Clusit 2018"; "Cambi di paradigma: Previsioni Trend Micro sulla sicurezza per il 2018) i cosiddetti attacchi mirati, indirizzati su specifiche aziende con fini di spionaggio, sabotaggio o estorsione. Alla base di questi attacchi ci sono processi di analisi che studiano i punti deboli del "bersaglio" anche attraverso tecniche di social engeneering facilitate dalla diffusione di dispositivi mobili, smart working, open space, pratiche di BYOD (Bring Your Own Device).

Gli attacchi mirati iniziano tutti con una fase di ricognizione, il cui scopo principale è quello di ottenere informazioni e l'obiettivo primario sono credenziali di accesso cioè: user name e password di un utente aziendale. Negli attacchi tipici occorrono almeno tre fasi per ottenere tali credenziali, ma, grazie all'uso dei dispositivi mobili e del loro utilizzo in ambienti non protetti ne può bastare uno solo e con poco sforzo. Sta, infatti, prendendo piede il visual hacking come ci mostrano gli analisti (cfr "Public Spaces Interview Study" del Ponemon Institute).

Senza bisogno di strumenti informatici basta avvicinarsi al monitor di un collega, sbirciare lo schermo di uno smartphone poggiato sul bancone di un bar, osservare il monitor di un lavoratore mobile per ottenere le informazioni che servono.

L'indagine del Ponemon Institute rivela che l'87% dei sempre più numerosi "mobile worker" ha sorpreso qualcuno guardare il monitor del proprio notebook da dietro le loro spalle, in uno spazio pubblico.

Tre su quattro mobile worker intervistati dagli analisti di Ponemon affermano di essere preoccupati per questa minaccia, ma la consapevolezza di un problema è solo l'inizio, dopo occorre la soluzione. Eppure

il nuovo regolamento impone. In pratica i ritardi sarebbero da addebitarsi ad aspetti legali e amministrativi sul fronte business e non su quello tecnico, dove il rischio è trascurare le poche norme non previste in Italia, come quelle della protezione fisica.

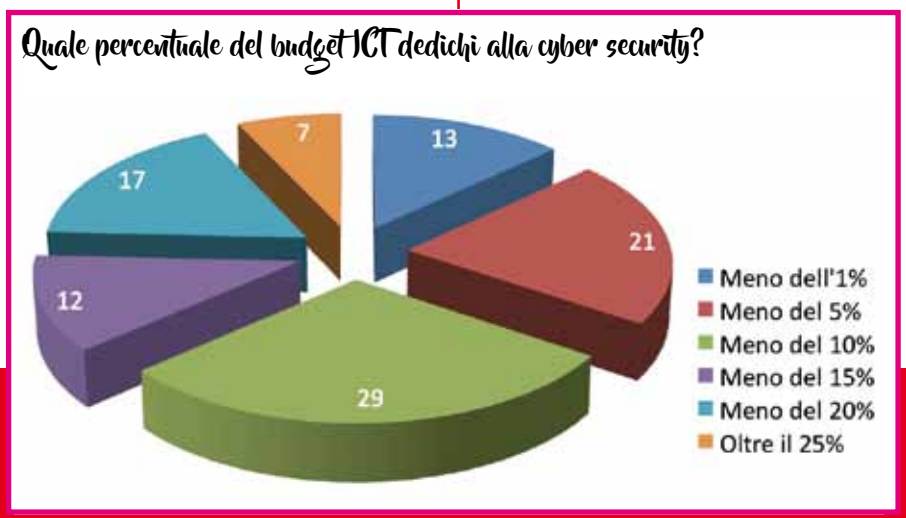
Lo stato d'adeguamento in Italia

L'inchiesta svolta dalla redazione di Reportec ha rilevato una crescita di attenzione nei confronti della sicurezza: attacchi devastanti come WannaCry nel 2017 e altri episodi legati alle estorsioni con il ramsonware hanno portato in televisione e sui tanti canali d'informazione il problema della sicurezza informatica. Sembra tuttavia prevalere la vecchia logica del "tanto a me non capita", visto i livelli bassi d'investimento in sicurezza.

Un'inchiesta della nostra redazione ha sondato il tema della conformità al regolamento europeo e quello della spesa per la struttura dedicata alla sicurezza informatica.

I risultati sono deludenti: Il 76% delle persone (specialisti ICT, security manager e business manager in oltre 200 imprese) che hanno risposto al sondaggio della redazione o che sono state intervistate direttamente, spende meno del 10% in sicurezza informatica, cioè meno dello stretto necessario, stando alle valutazioni effettuate dagli analisti del Gartner. Questi ultimi,

oltre la metà degli interpellati ammette di non fare nulla per proteggere le informazioni mentre lavorano in luoghi pubblici.
Sempre gli analisti di Ponemon, nei loro studi sul visual hacking hanno rilevato che il 91% degli attacchi visuali va a buon fine. Inoltre, il 52% dei dati sensibili di un'azienda perde la sua riservatezza poiché viene visualizzato da un impiegato interno non autorizzato.
Sono violazioni che possono portare a conseguenze gravi. Il GDPR impone che il rischio sia valutato e che siamo implementate delle contro misure.
Per determinare dove occorrono barriere fisiche, è necessario identificare i punti di accesso alle informazioni sensibili, a cominciare dalla reception dell'impresa per continuare oltre il mondo esterno: per esempio quanti sono i dipendenti che hanno bisogno di accedere alle informazioni sensibili in luoghi pubblici, spesso esposti alla vista di altri?
Sistemi di badge per avviare la stampa di un documento solo quando si è fisicamente vicino alla stampante consentono di avere maggior controllo dei dati impressi sulla carta. Naturalmente, occorre anche che i documenti cartacei siano conservati in una struttura riservata con tanto di controllo accessi. Neanche i trita documenti andrebbero lasciati senza protezione.
Come accennato anche le disposizioni open space degli uffici accrescono il rischio di visual hacking, perché sono rimosse le barriere fisiche.
I monitor andrebbero posizionati lontani da porte e finestre e posizionati in modo che lo schermo non sia visibile dai visitatori in un ufficio pubblico.
Per quanto riguarda la protezione dei dati visualizzati su un monitor esiste una soluzione tanto semplice quanto geniale, consistente in un filtro che si applica sullo schermo, oscurando la vista laterale. Si tratta del Privacy Filter di 3M.



infatti, ritengono che la suddetta quota occorra solo per la gestione ordinaria della sicurezza, come ci riportano gli esperti del Clusit. In altre parole potrebbe bastare a chi ha già messo in piedi una strategia per la security. Nella realtà, però, le imprese italiane sono ancora molto indietro: infatti, ben il loro 79% imprese ammette di non essere pronto per il GDPR.
In sostanza, dunque sono poco più del 20% le imprese che si sentono a posto con la nuova normativa ed è probabile che si tratti in massima parte delle più grandi o, in particolare, delle banche e delle società di telecomunicazioni, già soggette a regole stringenti imposte sia dall'attuale legge italiana sulla privacy sia da normative internazionali. Aziende che avevano poco o nulla da aggiungere per essere conformi al GDPR.
Molti degli esperti con cui abbiamo parlato sono convinti che la corsa alla compliance partirà veramente solo dopo che fioccheranno le prime multe.
Ricordiamo, infatti, che mentre banche e operatori di telecomunicazioni, da tempo erano tenuti a informare di eventuali violazioni, dal 25 maggio toccherà farlo a tutti e sono

I Privacy Filter3M contro i visual hacker

Filtri Privacy 3M mette a disposizione un'articolata gamma di filtri da applicare ai monitor di qualsiasi dispositivo, dai grandi formati per le workstation fino a tablet e smartphone. Realizzati grazie a una tecnologia ottica avanzata che garantisce privacy visiva e protezione degli schermi, questi filtri costituiscono una difesa dal visual hacking, fornendo protezione contro i danni fisici e l'abbagliamento dello schermo. Grazie alla tecnologia Microlouver i filtri privacy di 3M oscurano completamente la visione laterale, mentre l'utilizzatore godrà la massima nitidezza dell'immagine dall'angolo di visualizzazione centrale.

Il vicino sul treno o il collega indiscreto vedranno solo uno schermo nero o color oro.

Diversi i modelli disponibili per soddisfare le multiple esigenze del mercato.

Ci sono i filtri 3M Privacy Nero con e senza cornice, compatibili con un'ampia gamma di portatili e di monitor esterni, hanno un lato lucido e uno satinato che aiuta a ridurre i riflessi. Seguono i filtri3M Privacy Oro senza cornice (che mantengono tutte le caratteristiche del filtro Nero, fornendo in media il 25% di nitidezza in più rispetto quest'ultimo). A ciò si aggiunge una speciale superficie lucida che proietta uno schermo di un vivido color oro per una privacy superiore. Sono considerati l'ideale, da 3M, per gli schermi ad alta risoluzione.

Per i computer portatili dotati di funzione touch sono stati progettati i filtri 3M Privacy Nero, che forniscono una maggiore risposta tattile, anche grazie al filtro più sottile prodotto dal costruttore, a effetto vellutato e rappresentano la soluzione migliore, a detta dei tecnici 3M per gli schermi ad alta risoluzione con maggiore densità di pixel. Tutti i filtri 3M Privacy possono essere applicati, per garantire la riservatezza e facilmente rimossi ogniqualvolta si vogliano

in tanti a non accorgersi di un attacco andato a buon fine se non dopo settimane o mesi.

Un aspetto importante è la possibilità di "scaricare" parte della responsabilità a una società esterna. Un vantaggio per chi già utilizza servizi di terze parti per la sicurezza, cioè il 38% dei rispondenti al nostro sondaggio, che hanno dichiarato di esternalizzare almeno in parte la gestione della sicurezza.

Secondo quanto emerge dalla nostra inchiesta, la maggior parte di chi usa il cloud lo fa con attenzione: il punteggio più alto per le priorità viene, infatti, assegnato alla sicurezza, con un 2,9 rispetto al massimo di 3, o, quantomeno alla sensazione di sicurezza che il cloud provider scelto è riuscito a trasmettere.

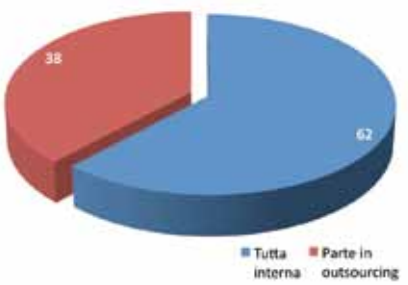
I managed security service, però, supportano bene la protezione logica del dato, mentre per quanto riguarda quella fisica occorre garantire le condizioni previste dal regolamento europeo nell'ambiente aziendale, quindi senza possibilità di trasferimento della responsabilità.

Al secondo posto, ma quasi a pari merito c'è il costo, che arriva a 1,92, appena sopra all'1,85 assegnato alle prestazioni.

Non abbiamo approfondito le ragioni di questo voto, anche se la sensazione è che il cloud oggi viva principalmente di servizi storage ed è ovvia la preoccupazione per la sicurezza dei dati, mentre le prestazioni vengono fatidicamente accettate in funzione della banda a disposizione.

condividere i contenuti.
Le pellicole protettive 3M Privacy per i telefoni, invece, sono progettate per essere usate all'occorrenza: nell'orientamento verticale garantiscono la privacy e in quello orizzontale consentono di condividere lo schermo. L'applicazione è semplice e con tecnologia stay-clean si evita l'accumulo di polvere e sporco sui bordi.
Va segnalato che sono possibili personalizzazioni per dispositivi di marche e dimensioni diverse: sul sito di 3M è presente un selettore di prodotto che, in base al dispositivo, individua i filtri compatibili.

La gestione della cyber security nella tua azienda è tutta interna o in parte in outsourcing?



Nella scelta del cloud provider in quale ordine hai considerato la sicurezza, le prestazioni e il costo (mettili in ordine da 1 a 3 dove 1 è quello considerato il più importante).