La protezione dei dati e la sicurezza informatica in uno scenario post-GDPR

#KingstonIsWithYou

La protezione dei dati e la sicurezza informatica in uno scenario post-GDPR

Introduzione

Sono tante le imprese e le organizzazioni che hanno lavorato duramente e assunto nuovo personale per farsi trovare pronte all'arrivo del GDPR. E probabilmente la vostra è tra queste. Tuttavia, l'inarrestabile evoluzione delle minacce informatiche non permette di fermarsi a riprendere fiato. La conformità al GDPR non è questione di caselle da spuntare, ma è piuttosto un protocollo che consente di valutare e misurare l'impegno quotidianamente profuso per la sicurezza informatica e la protezione dei dati. Non c'è spazio per la negligenza.

Questo breve eBook riporta i pareri dei commentatori più autorevoli del Regno Unito in materia di sicurezza informatica, per valutare l'evoluzione avutasi nel panorama della protezione dei dati in seguito all'introduzione del GDPR. Ci si soffermerà inoltre sui metodi adottati dalle imprese per trasmettere ai propri dipendenti la consapevolezza delle esigenze sottese alla conformità, valutando ciò che i reparti IT e i fornitori di tecnologia possono fare per rendere ancora più sicure le infrastrutture IT e preparare gli utenti finali alle sfide sulla sicurezza che ci attendono.

La protezione dei dati e la sicurezza informatica in uno scenario post-GDPR

Contributori

Questo breve eBook è stato realizzato con il contributo di cinque esperti in materia di protezione dei dati e sicurezza informatica.

Rob Allen
@Rob_A_kingston

Rob ricopre il ruolo di Director of Marketing & Technical Services in Kingston Technology e lavora per la società dal 1996. Rob ha il compito di supervisionare PR, Social Media, Channel Marketing e Digital Marketing Media per tutti i prodotti e i marchi di Kingston.

Tara Taubman-Bassirian
@clarinette02

Tara ha numerosi titoli: avvocato, mediatore, ricercatrice, consulente, relatrice e autrice. La sua sconfinata esperienza in aree quali privacy, proprietà intellettuale e protezione dei dati l'ha resa celebre in diverse aree del pianeta, soprattutto nel Regno Unito, Francia e USA.

Rafael Bloom
@rafibloom73

Rafael è Direttore di Salvatore ltd. Il suo ruolo consiste nell'aiutare le società ad affrontare le sfide operative, commerciali e strategiche e ad approfittare delle opportunità offerte dall'evoluzione normativa e tecnologica.

Miriam Brown
@Kingston_MBrown

B2B Strategic Marketing Manager, in Kingston Technology fin dal 1997. Nel suo ruolo attuale Miriam guida strategie, campagne e contenuti marketing relativi a tutti i prodotti Kingston B2B.

Sally Eaves
@sallyeaves

La prof. Sally Eaves viene descritta come un "tedoforo della tecnologia etica". Avendo ricoperto ruoli quali CEO, CTO, Docente di Tecnologie emergenti e Consulente strategico internazionale ha un enorme contributo esperienziale da offrire. Sally è una pluripremiata relatrice, autrice, ricercatrice e influencer, esponente di un'autentica e originale leadership di pensiero.

La protezione dei dati e la sicurezza informatica in uno scenario post-GDPR

Indice

Sezione 1	Come è cambiata la protezione dei dati dopo il GDPR?	5 – 7
Sezione 2	In che modo le organizzazioni stanno formando i propri dipendenti?	8 - 9
Sezione 3	I dipartimenti IT possono rendere più sicuri i dispositivi?	10 - 11
Sezione 4	In che modo i fornitori di tecnologia possono agevolare processi e conoscenza?	12 - 13
	Riepilogo	14
	Informazioni su Kingston	15

Sezione 1 – Come è cambiata la protezione dei dati dopo il GDPR?

Le imprese hanno fatto molti progressi! Negli ultimi due anni, i team legali si sono ampliati, l'assunzione di Data Protection Officer è schizzata alla stelle[1] e sono aumentate anche le consulenze acquisite all'esterno da esperti di privacy. Migliaia di organizzazioni hanno acquisito familiarità con la compilazione delle valutazioni di impatto sulla protezione dei dati (DPIA).

Ma la strada è ancora lunga.

Una delle maggiori sfide poste dal GDPR consiste nel fatto che non è consentito un minimo calo di attenzione. In quasi tutte le organizzazioni, un qualunque membro del personale, in qualsiasi momento, potrebbe dar vita a una violazione delle regole. Il problema diviene macroscopico nei settori in cui il personale è sottopressione o gode di un elevato grado di autonomia - come nei settori della sanità, dell'educazione o della giustizia. In quest'ultimo ad esempio, sono tanti gli avvocati che considerano normale scambiarsi i dati sensibili di un caso attraverso un allegato email. Per non parlare dei professionisti del settore sanitario, che inviano dati dei pazienti o risultati di una risonanza magnetica da indirizzi email non sicuri. In organizzazioni caratterizzate da un elevato grado di pressione, basta una piccola aggiunta all'elenco delle cose da fare, per veder andare in fumo tutti gli sforzi fatti per raggiungere la conformità. La produttività – a quanto sembra – vince sui protocolli.

Anche se ciò è destinato a cambiare.

E poi c'è il problema della consapevolezza nel settore del volontariato. Troppo spesso i volontari credono di essere esenti dal GDPR. E anche quando sono consapevoli che il GDPR si applica a qualsiasi organizzazione dei settori pubblico, privato e del volontariato, restano comunque riluttanti all'idea di dover investire sulla protezione dei dati, dal momento che ciò significa destinare soldi a una causa diversa rispetto a quella per cui vengono raccolti – cosa per certi versi comprensibile. Un atteggiamento nobile, ma anche improprio. L'investimento IT sarebbe microscopico rispetto alle sanzioni che potrebbero derivare da una violazione del GDPR.

Dal 2016 la domanda di Data Protection Officer (DPO) è schizzata alla stelle con un incremento del 700%.

Tara Taubman-Bassirian
@clarinette02

GDPR, Data Protection & IP Consultant

"Molte organizzazioni del terzo settore dicono: "Il GDPR non si applica a noi, visto che ci occupiamo di gestire la beneficenza." Volendosi limitare anche solo alla conformità del sito web, cerco sempre di far capire loro che il problema non riguarda i dati che si intende raccogliere, quanto le terze parti a cui si permette di accedere ai dati dei propri visitatori."

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [visualizzato il 26.11.19]

Come è cambiata la protezione dei dati dopo il GDPR?

La minimizzazione dei dati è un trend incoraggiante

Viviamo in un'epoca caratterizzata da una sconfinata raccolta dei dati. I "Big Four" (Google, Apple, Facebook e Amazon) conservano gigantesche quantità di dati dei clienti. Si potrebbe presumere che le altre organizzazioni possano imitare i Big Four, raccogliendo quanti più dati possibile. Tuttavia, più sono i dati raccolti, maggiore è il rischio a cui ci si espone. Una delle tendenze più positive a cui si assiste dall'introduzione del GDPR è la ribellione a un'eccessiva raccolta dei dati. Le cd. "smart company" adottano un'etica di minimizzazione dei dati: "se non ne hai bisogno, non raccoglierlo".

Tara Taubman-Bassirian
@clarinette02

GDPR, Data Protection & IP Consultant

"La minimizzazione dei dati è probabilmente uno dei migliori principi del GDPR. Ogni volta che si crea un database si crea anche un rischio."

Rob Allen
@Rob_A_kingston

Director of Marketing & Technical Services, Kingston Technology

"Abbiamo adottato regole di cancellazione dei dati molto stringenti. Ovviamente, i dati business-critical vanno conservati in modo corretto. Ma tutto il resto? Trascorso un anno, deve essere eliminato. Per quale motivo conservarlo oltre?"

I benefici non si limitano alla riduzione del rischio. Prendiamo il marketing, ad esempio. Se il database del marketing non viene ripulito costantemente, è probabile che contenga dati obsoleti. E se parliamo di un database che ospita decine di migliaia di persone, a cui sono collegate campagne di marketing frequenti, i costi lievitano enormemente. Anche le statistiche delle prestazioni delle campagne vengono completamente alterate.

La minimizzazione dei dati riguarda anche i dati cartacei. Fate attenzione a ciò che stampate (è il caso delle scansioni dei passaporti dei clienti); fate attenzione a ciò che annotate (è il caso della password degli account). E quando è proprio necessario conservare una copia cartacea di qualcosa, fatelo in modo del tutto sicuro. La montagna di fogli che sovrastano le scrivanie possono sembrare imponenti. Ma di certo non sono sicure.

Rafael Bloom
@rafibloom73

Director,
Salvatore Ltd

"Stiamo assistendo a un nuovo modo di concepire l'interfaccia tra la tecnologia e l'attività effettiva di un'azienda. Il livello di maturità digitale raggiunto dalla leadership aziendale era assolutamente necessario."

L'effetto delle sanzioni: dal management all'utente finale

Il concetto di imporre per legge la protezione dei dati esiste da decenni. Ma le multe salate imposte a numerose società, incluse Google[1], British Airways e la catena di hotel Marriott[2] – insieme alla copertura mediatica che è stata data loro – hanno portato il GDPR all'attenzione dei manager. Con ricadute molto positive.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [visualizzato il 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [visualizzato il 26.11.19]

Come è cambiata la protezione dei dati dopo il GDPR?

Continua...

Un'altra forza trainante verso l'adozione di un'efficace protezione dei dati consiste nella collaborazione tra aziende Le grandi imprese oggi eseguono controlli estesi di due diligence sull'integrità della sicurezza dei dati dei potenziali fornitori, non volendo rischiare di essere ritenute responsabili in concorso di eventuali episodi di data breach.

Ma la maggiore consapevolezza a livello commerciale del GDPR ha anche un altro lato della medaglia da considerare: gli utenti finali sono molto più consapevoli dei diritti che hanno sui propri dati. E sanno che se una società perde il controllo sui loro dati – il che non implica necessariamente una violazione – hanno diritto a richiedere un risarcimento. Le aziende devono essere attente.

Sally Eaves
@sallyeaves

CEO & Director,
Sally Eaves Consultancy

"La protezione dei dati è divenuto un imperativo da cui dipende la conquista o la perdita della fiducia dei propri clienti."

Sezione 2 – In che modo le organizzazioni stanno formando i propri dipendenti?

Formazione del personale: due parole che in genere provocano occhiatacce da parte dei dipendenti.

Motivo di più per far sì che la formazione risulti coinvolgente. Una forza lavoro formata contravviene con meno probabilità alle buone pratiche sulla protezione dei dati. Inoltre, se si verificasse una violazione dei dati, l'ICO (Information Commissioner's Office) dovrebbe in ogni caso tenere in considerazione la prova fornita circa l'avvenuta formazione del personale sulla sicurezza dei dati.

Rafael Bloom
@rafibloom73

Director,
Salvatore

"Mi piace pensare ai dati come a un elemento di una catena di fornitura, in cui la provenienza e l'intero ciclo di vita sono soggetti a un'appropriata governance. Non c'è niente di male nel tenere il personale in una stanza per un'ora e mezza, per dare loro regole e raccomandazioni, quali adottare una password adeguata, non lasciare dati in giro, ecc. Di certo si ridurrà il rischio per l'organizzazione. Ma, trascorso qualche giorno, ci sarà davvero una differenza apprezzabile a parte quel piccolo impatto iniziale che si è ottenuto forzando le persone a un dato comportamento? No."

In ogni caso, ad aprile 2019, il Ministro alla digitalizzazione Margot James ha dichiarato che solo tre aziende inglesi su dieci hanno provveduto a formare il proprio personale sulle minacce informatiche[1]. È arrivato il momento di prendere la formazione sul serio.

Bisogna far cambiare mentalità, non somministrare quiz formativi

La formazione deve provocare un reale mutamento culturale e comportamentale, senza limitarsi ai soliti quiz a risposta multipla. È facile acquistare un pacchetto di formazione online con alcune semplici domande sulla protezione dei dati a cui tutti sarebbero in grado di rispondere correttamente. Ma questo consentirebbe davvero di incrementare la protezione dell'organizzazione?

I comportamenti davvero in grado di proteggere i dati hanno due comuni denominatori. Primo, una formazione intelligente, coinvolgente e indirizzata alle difficoltà che interessano da vicino l'organizzazione in cui si lavora. Secondo, comprendere che il GDPR richiede una profonda cultura dell'ambiente di lavoro che riguarda tutto il personale, ogni giorno. Parlando di dati, è imperativo adottare il comportamento corretto, qualunque sia la posizione ricoperta all'interno dell'organizzazione. Prendiamo ad esempio le risorse umane. Pensiamo ai dati personali di tutti i candidati che risiedono nei server di email.
La protezione dei dati è responsabilità di tutti.

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [visualizzato il 26.11.19]

In che modo le organizzazioni stanno formando i propri dipendenti?

C'è sempre una persona dietro i dati

Nella prima sezione si è fatto accenno alla maggiore consapevolezza che gli utenti stanno assumendo circa i diritti relativi ai propri dati. Un buon punto di partenza per una formazione efficace consiste nell'aiutare il personale a realizzare che dietro i dati c'è sempre una persona. Chiedete ai vostri dipendenti di pensare a tutte le organizzazioni a cui hanno trasmesso i propri dati e vedrete che realizzeranno che proteggere i dati significa tutelare la privacy delle persone.

Preparate un piano contingente

Sally Eaves
@sallyeaves

"La formazione continua dei dipendenti sulla protezione e la sicurezza dei dati è imprescindibile per un'azienda. Non bisogna pensare a una banale sessione formativa da svolgersi una volta l'anno; al contrario, deve trattarsi di un'esperienza proattiva, interattiva e coinvolgente che entri nel quotidiano della vita lavorativa. I dipendenti devono essere coinvolti nelle dinamiche di ciò che intendiamo mitigare, gestire e difendere."

Miriam Brown
@Kingston_MBrown

"È interessante chiedere alle persone durante la formazione: "E se si fosse trattato dei tuoi dati?" Se il mio consulente finanziario dovesse lavorare da casa sul proprio laptop, ospitando dati sensibili sul quel laptop, vorrei che i miei dati fossero custoditi all'interno di un drive protetto da crittografia."

Rob Allen
@Rob_A_kingston

"Trattate i dati come se fossero vostri."

Sezione 3 –
I dipartimenti IT possono rendere più sicuri i dispositivi?

Il lavoro da remoto è divenuto la nuova regola

È probabile che il personale acceda al proprio ambiente di lavoro da più dispositivi - inclusi quelli personali, che possono essere dimenticati su un treno o smarriti in un taxi. La sfida consiste nel consentire ai dipendenti di essere produttivi senza tuttavia esporre l'azienda al rischio di data breach o di minacce alla sicurezza. Basta il comportamento di una sola persona per vanificare l'impegno a protezione dei dati profuso da un'intera impresa.

Sally Eaves
@sallyeaves

CEO & Director,
Sally Eaves Consultancy

"I dati devono essere protetti sempre - che siano in uso, in transito o in attesa. È essenziale aver disposto un piano di eliminazione, ripristino e protezione a 360 gradi dei dati, capace di garantire la loro sicurezza in ogni contesto. In particolare, bisogna prestare attenzione alle aree a rischio che vengono spesso sottovalutate, come ad esempio i drive USB privi di crittografia, le email con cui vengono spediti allegati non crittografati e le funzioni dei browser Web che condividono dati sensibili degli utenti. Visto il gran numero di dispositivi interconnessi e di modelli di collaborazione in continua evoluzione, è vitale garantire ai dati che si trovano in uno smartphone lo stesso livello di protezione dei dati che si trovano in un server aziendale."

Autenticazione a doppio fattore

In media, la cosa più semplice e più immediata da fare per un'impresa consiste nel proteggere il proprio perimetro di rete – cosa che si può fare in modo davvero semplice, con l'utilizzo di password manager e l'autenticazione a doppio fattore. Un buon esempio di autenticazione a doppio fattore si ha quando a un utente è richiesto di immettere un codice che gli viene inviato sul proprio smartphone dopo aver immesso la password sul proprio laptop.

VPN e SSD/USB dotati di crittografia

L'uso di reti VPN si sta diffondendo tra le PMI. Le reti VPN sono irrinunciabili nel caso di personale che deve accedere ai dati aziendali attraverso reti WiFi pubbliche. Ma le imprese devono fare attenzione a non sovrastimare le possibilità delle reti VPN. Non sono la soluzione, ma solo parte di essa. Accade molto spesso che le imprese adottino una rete VPN, lasciando poi che i laptop o i notebook che vi si collegano da remoto non siano dotati di drive con crittografia hardware. Tutti archiviano dati sui propri laptop. Cosa accade se quel dispositivo viene hackerato, rubato o smarrito? Un drive USB e SSD dotato di crittografia costa davvero poco di più della versione standard. Distribuire dispositivi USB con crittografia e dotare i notebook di SSD crittografati protegge quasi del tutto dalle minacce alla sicurezza create dal lavoro in remoto. E se un dispositivo dovesse essere smarrito o sottratto, potete star certi che nessuno riuscirà mai ad accedere ai file crittografati. Potete addirittura distruggere da remoto i dispositivi USB smarriti.

"Una volta parlai con un esperto di sicurezza informatica che, tentando di convincere il CEO di una società ad adottare l'autenticazione a doppio fattore, si sentì rispondere con fermezza: "No, non lo faremo: è complicato ed implica un passaggio in più. La mia risposta è no." Dopo poco, l'azienda fu vittima di una frode da £40.000."

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd

"In fin dei conti, il modo migliore per accrescere la cultura sulla sicurezza consiste nell'aprire un dialogo costruttivo con i dipendenti, volto alla ricerca di soluzioni che garantiscano insieme sicurezza e produttività."

Rob Allen
@Rob_A_kingston

Director of Marketing & Technical Services, Kingston Technology

I dipartimenti IT possono rendere più sicuri i dispositivi?

MSP e server privati

Sono sempre più numerose le grandi aziende che stanno tornando ad avere i propri server on-site. Questo consegna loro il pieno controllo sul patrimonio server, senza avere più nulla memorizzato nel cloud accessibile pubblicamente. Poi ci sono le soluzioni server ibride, che prevedono l'archiviazione dei dati sensibili on-site e tutto il resto nel cloud. Per le PMI e le organizzazioni del terzo settore potrebbe risultare troppo costoso avere un proprio server on-site. Ed è proprio qui che fornitori di servizi gestiti e i server privati virtuali entrano in gioco, consentendo di concentrarsi sulla sicurezza, ma senza richiedere costi operativi che sarebbero proibitivi.

Segnalazione automatica dei dati in scadenza

Un principio fondante del GDPR è l'obbligo di cancellare i dati vecchi. Alcuni tipi di dati personali, ad esempio, non devono essere conservati per più di 7 anni. E se l'imminente scadenza di un dato venisse comunicata automaticamente? Con il giusto database, sarebbe facile per il team IT creare un'azione che informi automaticamente il DPO quando si avvicina la scadenza di un dato che non può essere conservato oltre.

Scegliete i fornitori giusti

Nel settore della sicurezza IT, esistono infiniti produttori e rivenditori. Fate un'attenta selezione. È essenziale poter contare su un sistema offerto da un produttore affidabile, in grado di vantare un'esperienza specifica nelle soluzioni dedicate alle organizzazioni del vostro specifico settore. Assicuratevi che i fornitori scelti, oltre a disporre della tecnologia necessaria, siano anche in grado di comprendere le difficoltà da superare per riuscire a garantire la sicurezza dei dati.

Sezione 4 – In che modo i fornitori di tecnologia possono agevolare processi e conoscenza?

TLC per il DPO

Dal 2016 la domanda di Data Protection Officer è schizzata alla stelle, con un incremento del 700%.[1] Ad oggi si contano più di 500.000 DPO impiegati in Europa – il che vuol dire 6 volte più di quel che era stato previsto nel 2017.[2] Eppure, l'importanza del ruolo del DPO è spesso sottovalutata e banalizzata.

Un DPO deve poter avere una visione completa su tutto ciò che afferisce alla sicurezza aziendale e tutela dei dati. È un lavoro a tempo pieno. Ma sono ancora tante le organizzazioni in cui "DPO" è semplicemente un'etichetta assegnata al membro del team che ha una maggiore conoscenza della tecnologia. E invece si tratta di persone su cui ricade la responsabilità della protezione dei dati di tutta l'azienda, mentre sono impegnate a svolgere le mansioni quotidianamente richieste dal proprio ruolo.

In realtà, servirebbe una gamma di servizi e strumenti professionali da mettere a disposizione di questa nuova figura di professionisti. Ed anche per chi ha assunto un DPO a tempo pieno, la sicurezza dei dati si muove a una velocità tale da porre sfide per cui è richiesta una seconda opinione. Collaborare con un consulente esterno o un esperto in materia di scurezza dei dati può rivelarsi molto utile, ma è comunque necessario aver fatto prima ordine nella gestione interna dei dati.

Chiarezza, contingenza e coesione

L'infrastruttura IT è forte quanto il suo elemento più debole. Ecco perché, in occasione di qualsiasi nuovo innesto nell'ecosistema IT, il relativo fornitore dovrebbe fare piena chiarezza sulle minacce che potrebbe apportare alla sicurezza e offrire consigli chiari cu some usare il nuovo prodotto in modo sicuro.

Tara Taubman-Bassirian
@clarinette02

GDPR, Data Protection & IP Consultant

"Provo spesso a spiegare alle persone che installando videocamere a circuito chiuso dappertutto non si esaurisce il compito sulla sicurezza, visto che spesso vengono installate senza una password. Così, chiunque può collegarsi all'indirizzo web, accomodarsi e godersi lo spettacolo. È come dire al ladro: 'vieni a vedere quando sono fuori!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [visualizzato il 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [visualizzato il 26.11.19]

In che modo i fornitori di tecnologia possono agevolare processi e conoscenza?

C'è un problema di contingenza. Cosa accade quando un prodotto raggiunge la fine della sua vita operativa o necessita di essere aggiornato? I fornitori di tecnologia dovrebbero offrire consulenza sulle contingenze che potrebbero inavvertitamente compromettere i dati ospitati nei prodotti o danneggiare in altro modo la sicurezza del più ampio ecosistema IT. Prendiamo ad esempio un'apparecchiatura per la risonanza magnetica. In genere sono dotate di un drive SSD da quattro terabyte in cui vengono archiviate le immagini dei pazienti. Ma che succede quando si raggiunge il limite di quella memoria?

I fornitori di tecnologia e le stesse organizzazioni dovrebbero inoltre agevolare un ambiente di coesione tra dati e tecnologia digitale - sia dentro che fuori l'organizzazione, quando si collabora con fornitori e partner esterni. Un'esigenza, questa, cruciale per organizzazioni come il SSN che si caratterizzano per un'attività distribuita su più territori, dipartimenti e ambiti operativi.

Miriam Brown
@Kingston_MBrown

B2B Strategic Marketing Manager, Kingston Technology

"Abbiamo venduto numerosi prodotti al SSN - ma ogni volta rileviamo differenze nette tra i vari responsabili quando chiediamo quali sono i protocolli o le policy in materia di protezione dei dati adottati."

Uno sguardo all'orizzonte

La tecnologia avanza rapidamente, lasciando spesso indietro la sicurezza. Con le tecnologie emergenti – come il caso dei pagamenti con riconoscimento facciale in Cina – capita spesso che le organizzazioni corrano a dotarsi della tecnologia ancora prima di essersi fermate a considerare le possibili implicazioni sulla sicurezza e sulla protezione dei dati. Tra uno o al massimo due anni è previsto che vi sarà accesso diffuso alle reti 5G, con il conseguente diffondersi dell'edge computing e dei silos di dati distribuiti. I fornitori tecnologici devono essere in grado di aiutare le organizzazioni a sfruttare in modo sicuro le tecnologie emergenti, senza compromettere l'integrità dei loro dati o la sicurezza IT.

Sally Eaves
@sallyeaves

CEO & Director, Sally Eaves Consultancy

"Sono convinto che inizieremo a vedere cambiamenti nel GDPR: oltre a ridursi le difficoltà connesse alla sua implementazione, ci si inizierà a focalizzare sull'ottimizzazione dei possibili vantaggi - come ad esempio l'evoluzione dei processi IT, il backup e il ripristino o l'incremento della sicurezza - sfruttando questi aspetti come elementi di differenziazione rispetto agli altri player del settore."

Riepilogo

Il GDPR ha determinato un'evoluzione nel mondo aziendale, portando la tutela dei dati e la sicurezza della rete all'attenzione del management e degli utenti finali. La conformità tuttavia impone un'attenzione alla sicurezza dei dati costante – giorno dopo giorno – da parte di tutto il personale. La continua evoluzione della tecnologia e delle minacce informatiche rendono vitali per un'azienda la disponibilità di una solida infrastruttura della sicurezza e di una valida formazione - accompagnati da un buon servizio di consulenza sulla tecnologia e sulla tutela dei dati. Ricordare che c'è sempre una persona dietro i dati è molto importante, perché aiuta i dipendenti ad adottare una cultura di protezione dei dati. E un cambiamento culturale è molto più efficace di un esercizio formativo con quiz a risposta multipla.

Informazioni su Kingston

Grazie ai suoi 32 anni di esperienza, Kingston è in grado di individuare e risolvere efficacemente le problematiche che il lavoro remoto crea nella vostra organizzazione – consentendo al personale di lavorare con facilità e in sicurezza ovunque, senza impatti sulla produttività aziendale.

©2021 Kingston Technology Europe Co LLP e Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Regno Unito.
Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. Tutti i diritti riservati. Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari.

#KingstonIsWithYou