Le minacce del lavoro da remoto alla sicurezza – e come risolverle

#KingstonIsWithYou

Le minacce del lavoro da remoto alla sicurezza – e come risolverle

Introduzione

È arrivato il momento che il personale prenda davvero sul serio la sicurezza dei dati. È oramai noto che il lavoro da remoto è un fattore di crescita per il business. Ma le minacce poste da tale fattore alla sicurezza della rete e alla conformità al GDPR sono troppo grandi per essere ignorate. Molte aziende ritengono che sia impossibile riuscire a mantenere un controllo dimostrabile sull'ecosistema IT senza affrontare investimenti significativi. Ma le cose non stanno necessariamente così. I costi non possono essere una causa esimente.

I sistemi, i servizi e i prodotti ci sono - e costano meno di quanto si possa generalmente pensare. La verità è che la sfida in materia di sicurezza non riguarda solo l'ambito finanziario o tecnico, ma anche culturale. La creazione di un corretto ambiente IT adatto al lavoro da remoto non richiede particolari complessità.
Ma se il personale non adotta un approccio e un comportamento altrettanto corretti verso la sicurezza e la conformità alla normativa sui dati, l'azienda ne risentirà sempre e comunque. E il costo di un episodio di violazione dei dati può arrivare ad essere incredibilmente alto.

I prodotti ci sono.
Ma è la formazione a fare la differenza.

Contenuti

Questo breve ebook è stato redatto da tre esperti sulla sicurezza dei dati e sul lavoro da remoto.

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.

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.

Sarah Janes
@SarahkJanes

Sarah ricopre il ruolo di Managing Director in Layer 8 Ltd dal 2014. La loro mission li porta a sostenere i responsabili della sicurezza nello sforzo di favorire una svolta culturale efficace nell'ambito della sicurezza informatica delle organizzazioni - sia nelle piccole realtà che nelle sconfinate corporation.

Le minacce del lavoro da remoto alla sicurezza – e come risolverle

Indice

Sezione 1 – Il problema

L'accesso remoto è fonte di criticità

I giorni in cui il lavoro veniva svolto interamente all'interno di un'unica sede centrale sono andati da tempo. Il personale accede alle email di lavoro direttamente dal proprio smartphone. I Direttori operativi passano intere giornate lavorando da casa o nei loro cafè preferiti. Gli agenti di vendita accedono a dati interni critici per l'azienda quando si trovano presso un cliente. Il lavoro da remoto è divenuto la nuova regola.

Aumenta la produttività e il tasso di fidelizzazione del personale.[1] Riduce i costi aziendali.[2] Aiuta l'ambiente.[3] Una ricerca ha rivelato che il **70% dei professionisti lavora da remoto almeno una volta alla settimana**.[4]

Tuttavia, una sola persona può compromettere l'integrità della sicurezza di un'intera organizzazione se non rispetta i necessari protocolli di sicurezza.

La conformità al GDPR è un must

La necessità di conseguire un adeguato livello di sicurezza non può essere messa in discussione, sia per la sicurezza dell'azienda che per la conformità al GDPR. Anche perché il GDPR sa essere molto severo. L'ICO (Information Commissioner's Office) ha di recente sanzionato la British Airways e la catena di hotel Marriott per un importo complessivo di circa 300 milioni di sterline a seguito di episodi di violazione dei dati.[5]

70% dei professionisti lavora da remoto almeno una volta alla settimana.[4]

Quali sono le aziende a rischio?

Se il vostro personale lavora da remoto o usa dispositivi personali per accedere ai sistemi aziendali, allora la vostra azienda è a rischio. Il problema è tutto qui.

[1] **Inc.com: "A 2-Year Stanford Study Shows the Astonishing Productivity Boost of Working From Home" -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: "What are the cost savings of telecommuting?" -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 statistiche sull'impatto ambientale delle telecomunicazioni -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: lo studio rivela testualmente "70% of people globally work remotely at least once a week" -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **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

Sezione 2 – Le sfide dell'accesso remoto

Il lavoro da remoto è fonte di numerose minacce per la sicurezza.

Può essere difficile da accettare, ma si tratta di una verità da prendere molto sul serio se si vuole preservare l'integrità dell'organizzazione.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Uno dei principali problemi che la normativa GDPR pone a un'azienda consiste nel riuscire ad avere il controllo sui dati personali raccolti. Cosa evidentemente impossibile se l'azienda non sa dove sono archiviati quei dati."

Le aziende faticano ad aggiornare i sistemi e i dispositivi interni al ritmo con cui si evolve la moderna tecnologia.

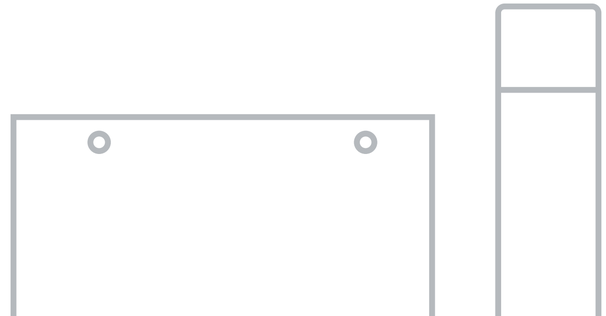
In effetti, il 38% delle persone che lavorano da remoto nell'area EMS ritengono di non avere le conoscenze o il supporto tecnologico necessari quando lavorano da casa o in uno spazio pubblico.

Ciò può portare i dipendenti a improvvisare soluzioni in grado di annullare le misure predisposte a protezione dei dati, lasciando l'azienda esposta al rischio di minacce alla sicurezza. Se i protocolli di sicurezza non sono stati studiati in modo da favorire la produttività del personale, è inevitabile che i dipendenti inventino espedienti - finendo ad esempio per salvare dati sensibili in posti come Slack, Dropbox, email personali o USB private. Peggio ancora se si instaura una cultura del "Loro / Noi", che pone un muro tra il team addetto alla sicurezza IT e il resto del personale. Il rischio diviene sensibile per la vostra azienda.

Rob Allen
@Rob_A_kingston

Director of Marketing & Technical Services, Kingston Technology

"Nella mia esperienza ho potuto notare che più sono grandi le organizzazioni, più diventa complesso per i dipendenti lavorare da remoto - con tempi di accesso lunghissimi e numerosi step di sicurezza da superare".



Sezione 2 – Le sfide dell'accesso remoto

Lavorare con il proprio dispositivo

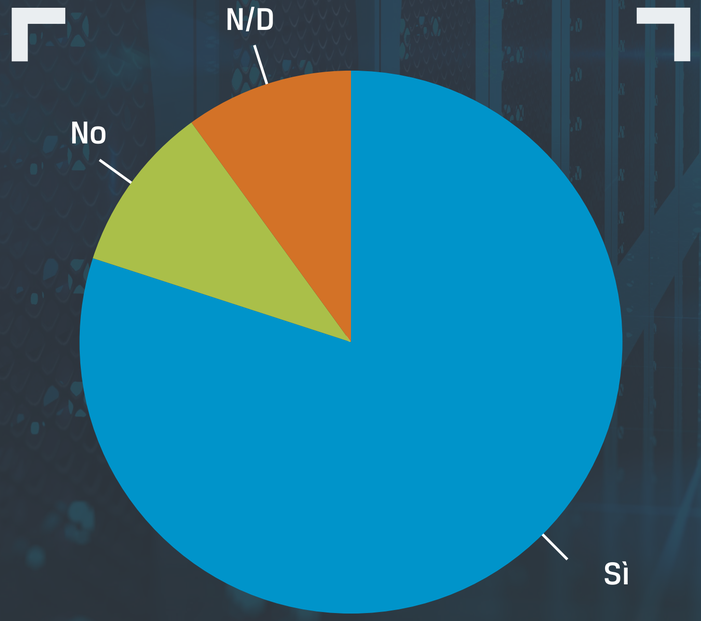
È divenuta oramai una consuetudine per i professionisti usare il proprio smartphone per leggere le email di lavoro o accedere ai dati dell'organizzazione tramite il proprio laptop o tablet. Ovviamente, ciò crea dei pericoli. Il personale porta i dati all'esterno dell'organizzazione? I loro dispositivi sono sicuri e il loro software è protetto? Si tratta di domande che non possono retare senza risposta.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Le aziende sono fortemente minacciate dal rischio di non sapere dove si trovano i dati che raccolgono."

Temete che i dipendenti possano adottare soluzioni incompatibili con le misure di sicurezza adottate in azienda?



Fonte: Sondaggio Kingston 2019

Reti WiFi pubblica

I problemi non riguardano solo il lavoro da casa. Non bisogna dimenticare la parte dello staff che accede ai sistemi aziendali mentre sorseggia un cappuccino al bar. Le reti WiFi pubbliche sono il paradiso degli hacker. Dovete assolutamente dotare i dipendenti degli strumenti necessari a difendersi dal rischio dei loro attacchi.

Cyber attacchi e phishing evoluto

Le email di phishing indirizzate ai dipendenti stanno diventando sempre più sofisticate e persuasive. Avete insegnato al vostro personale come fare a riconoscerle? Per non parlare delle minacce sempre più pressanti di malware e ransomware. I vostri dispositivi – tutti, nessuno escluso – devono essere protetti.

Sezione 3 – L'infrastruttura dell'accesso remoto (e una nota sul corretto approccio mentale)

La tecnologia che semplifica la protezione dalle minacce poste alla sicurezza dal lavoro in remoto esiste. E non deve necessariamente costare una fortuna.

Come creare la giusta infrastruttura

Le aziende devono assicurarsi che i dipendenti che lavorano da remoto possano accedere con semplicità ed efficienza agli strumenti e ai dati necessari allo svolgimento delle loro mansioni quotidiane, senza alcun pregiudizio per la produttività. Non occorre introdurre nuovi prodotti: basta partire da un'attenta scelta delle dotazioni di base. Ad esempio, la maggior parte delle aziende usa computer or laptop. Ecco, basta scegliere dischi rigidi (HD) o a stato solido (SSD) crittografati. In questo modo, se il dispositivo venisse perso o sottratto, i dati dell'azienda non potrebbero in ogni caso finire nelle mani sbagliate. Inoltre, se si verificasse una violazione dei dati, l'ICO dovrebbe in ogni caso tenere in considerazione l'attenuante dell'aver adottato misure di protezione dei dati dimostrabili.

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 una produttore affidabile, in grado di vantare un'esperienza specifica nelle soluzioni dedicate al lavoro da remoto.

VPN

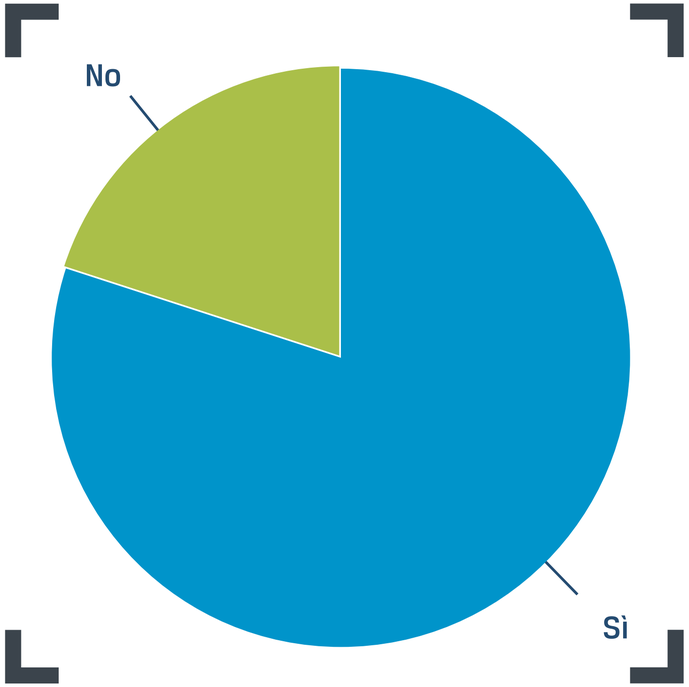
Se la protezione dell'azienda passa dall'uso di una VPN (Virtual Private Network), allora per ridurre i rischi è necessario dotare le persone giuste di strumenti adeguati. Le reti VPN sono irrinunciabili nel caso di personale che deve accedere ai dati aziendali attraverso reti WiFi pubbliche.

Software DLP

Quasi tutte le suite di software DLP offrono la possibilità di limitare l'accesso alla propria rete, creando white-list per specifici dispositivi, come nel caso degli USB crittografati, appositamente progettati per essere identificati in modo univoco. In questo caso, parliamo di costi trascurabili (date uno sguardo alla gamma di prodotti USB di Kingston, offerti con le opzioni di personalizzazione per la vostra azienda).

La conformità al GDPR ha richiesto modifiche significative alla vostra organizzazione?

Fonte: Sondaggio Kingston 2019



Sezione 3 – L'infrastruttura dell'accesso remoto (e una nota sul corretto approccio mentale)

USB e SSD

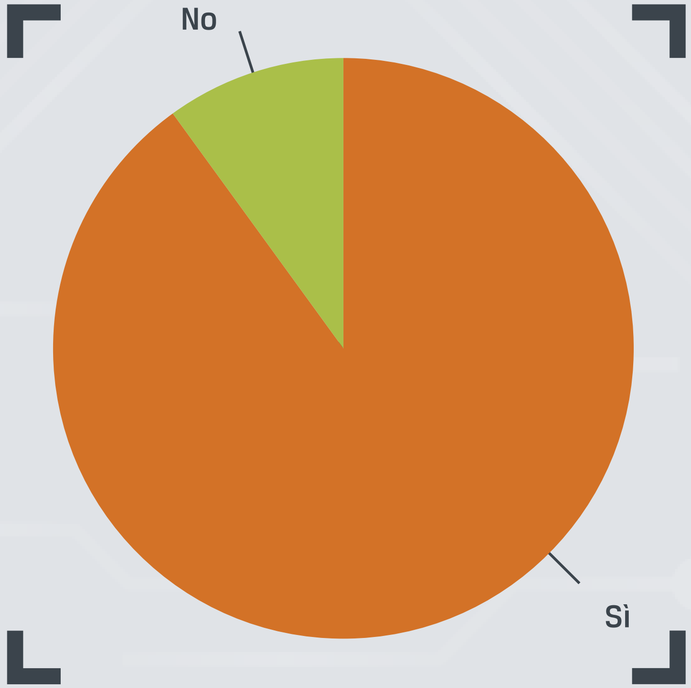
Distribuire dispositivi USB con crittografia e dotare i notebook di SSD crittografati protegge quasi del tutto dalle minacce alla sicurezza create dal lavoro in remoto. Adottando soluzioni USB e hardware SSD crittografati (con o senza WiFi) i dati sono protetti e disponibili - sempre e ovunque. E se 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.

Siate sempre pronti al peggio

Talvolta, un atteggiamento ottimistico nasconde una cieca fiducia. E per un team responsabile della sicurezza è sempre meglio - in realtà, necessario - pensare al peggio. È giusto fidarsi dei dipendenti e delle misure di sicurezza adottate. Ma bisogna comunque prepararsi a gestire gli scenari peggiori. Pensando che la vostra rete potrà – e sarà – violata, non farete altro che migliorare l'integrità della sicurezza.

Avete aggiunto al software di sicurezza per endpoint anche dispositivi mobili aziendali - quali USB, notebook o altro?

Fonte: Sondaggio Kingston 2019



Sezione 4 – La formazione del personale è una strada obbligata

L'adozione della tecnologia adeguata porta a metà strada. Il vero problema sta in quello che fa il vostro personale quando è da solo. Ecco perché si ritiene che il rischio per la sicurezza dei dati sia più un problema culturale che tecnologico. Senza un'adeguata formazione, i dipendenti percepiranno sempre come un fastidio i comportamenti necessari alla conformità con normative quali GDPR, PECR e altre.

Ecco alcuni consigli utili.

Mai dare regole senza motivarle

"Non andare dietro quell'albero."
"Non andare dietro quell'albero, perché ci troverai un leone."

Quale delle due verrà memorizzata? Le persone non sono molto recettive nei confronti delle regole prive di motivazioni. È quindi essenziale aiutare i dipendenti a capire le motivazioni che sorreggono ciascuna regola.

Coinvolgeteli personalmente

Se vengono visualizzate nella propria sfera privata, le minacce alla sicurezza risultano sicuramente più facili da percepire. Prendiamo ad esempio il GDPR. Per aiutare il vostro team a comprendere meglio che dietro un set di dati c'è sempre una persona, fate in modo che pensino a come potrebbero sentirsi se un'azienda a cui hanno trasmesso i loro dati non si prodigasse per proteggerli. Come si sentirebbero se i loro dati personali finissero nelle mani sbagliate?

"Se spiegate a un dipendente l'importanza che il GDPR e le politiche sulla sicurezza hanno per la protezione dei suoi interessi, al di fuori della sfera lavorativa, inizierà a comprendere meglio i motivi che obbligano le organizzazioni a proteggere i dati."

Rafael Bloom
@rafibloom73
Direttore di 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."

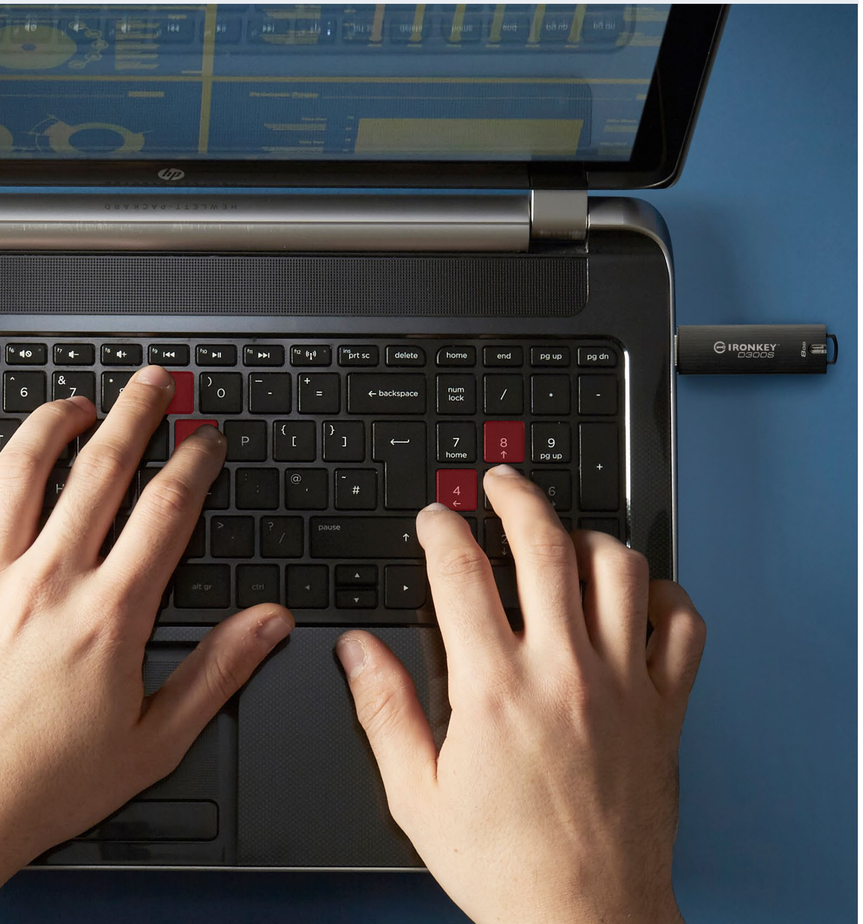
Sarah Janes
@SarahkJanes
Managing Director
Layer 8 Ltd

Fonte: Sondaggio Kingston 2019

Controllate con regolarità l'utilizzo dei dispositivi esterni dei dipendenti?

Sì	No	Non so	N/D
71%	11%	9%	9%

Sezione 4 – La formazione del personale è una strada obbligata



La formazione è il primo passo, non l'ultimo

Dal momento che molte organizzazioni non riescono a fornire formazione interna sulla sicurezza, diverse aziende sono entrate in azione per colmare il vuoto. Ma fate attenzione ai falsi profeti. La formazione fornita da consulenti esterni spesso riflette i requisiti di conformità propri dell'azienda che eroga la formazione (perché evidentemente è per questo che vengono pagati), il che significa che il vostro personale non acquisirà una visione e una comprensione complete sulla sicurezza informatica. I comportamenti pericolosi non cesseranno.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Le organizzazioni che vogliono conseguire modifiche comportamentali, devono spingersi oltre la solita formazione sulla sicurezza fatta di schede preconfezionate. Devono riuscire a fornire una formazione di base che permetta di comprendere il senso generale della sicurezza informatica."

È chiaro che la formazione non deve essere una foglia di fico. È troppo semplicistico pensare che la formazione ricevuta porterà direttamente il personale ad adottare comportamenti sicuri, che garantiscano la conformità. Si tratta di un'ingenuità pericolosa. Il successo in questo campo richiede un continuo sostegno, di natura sia culturale che comportamentale.

Rafael Bloom
@rafibloom73

Direttore di Salvatore Ltd

"Ho visto società "certificate" che continuano a conservare le password in un file o appuntate su fogli volanti, e altre che probabilmente neanche sanno di avere copie non crittografate dei propri hard disk lasciate incustodite di notte nelle auto dei dipendenti. A che serve essere certificati quando le persone non conoscono le basi della sicurezza?"

La soluzione sta tutta nella responsabilità

Una strategia valida ad attuare la necessaria svolta culturale consiste nell'istituire in azienda la figura del Security Champion, incaricato di spiegare al personale le minacce alla sicurezza e stabilire le norme di comportamento elementari, previste dai protocolli sulla sicurezza.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Il miglior modo per essere certi che vengano adottati i comportamenti giusti consiste nell'istituzione dei "Champion" che dialogano con i dipendenti per aiutarli a comprendere l'impatto che la sicurezza ha nella loro vita lavorativa – con l'ausilio di materiali formativi online che facilitano il compito."

Riepilogo

Garantire la protezione dei dati e la sicurezza informatica può sembrare una responsabilità gravosa. Tuttavia, il lavoro da remoto può diventare semplice e sicuro se si adottano gli strumenti adatti - che non sono affatto necessariamente costosi. Tuttavia, bisogna aver chiaro che per arrivare all'adozione di comportamenti sicuri da parte del personale è necessario passare per una svolta culturale e per la configurazione di una corretta infrastruttura IT.

Ecco un breve riepilogo.

- Il lavoro da remoto non è un fenomeno passeggero e produce molti benefici – tra cui un incremento della produttività e della fedeltà del personale a fronte di una riduzione dei costi aziendali. Tuttavia, il lavoro da remoto comporta anche notevoli rischi per la sicurezza.
- La violazione dei dati rappresenta un problema serio, considerate anche le sanzioni emesse dall'ICO in caso di non conformità al GDPR.
- L'uso di dispositivi privati, l'hardware insicuro, l'uso inappropriato del software e le reti WiFi pubbliche sono minacce molto comuni per la sicurezza.
- Una valida infrastruttura di sicurezza deve agevolare – non ostacolare – l'efficienta del personale. In caso contrario, i dipendenti inizieranno a inventare soluzioni incompatibili con le misure di sicurezza.
- Cercate produttori e distributori di soluzioni IT che possano vantare una specifica conoscenza di settore.
- I dispositivi crittografati come SSD e USB, le VPN e il software DLP sono soluzioni facili da implementare e non hanno necessariamente costi proibitivi.
- Il successo nel campo della sicurezza e della protezione dei dati richiede una svolta culturale e comportamentale interna all'organizzazione. Il personale deve comprendere le motivazioni che sono dietro le singole regole, piuttosto che essere spinto a seguire ciecamente i protocolli.
- I consulenti esterni possono risultare utili per la formazione del personale – ma occorre accertarsi che il materiale somministrato sia adeguato e in ogni caso non bisogna mai illudersi che le informazioni trasmesse durante la formazione basteranno da sole a produrre automaticamente il cambiamento comportamentale atteso.
- È consigliabile istituire la figura del "Security Champion", incaricato di spiegare al personale le minacce alla sicurezza e favorire l'adozione dei corretti comportamenti alla base.

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.

#KingstonIsWithYou