CROWDSTRIKE

LA SICUREZZA INFORMATICA AI TEMPI DEL COVID-19: SUGGERIMENTI PER RENDERE LO SMART WORKING EFFICACE E SICURO

11 marzo 2020 | Michael Sentonas | Rapporto sintetico

La dichiarazione da parte dell'Organizzazione mondiale della sanità che COVID-19 è una pandemia conferma un fatto di cui siamo tutti ormai consapevoli: la malattia provocata da questo coronavirus causerà una serie di sconvolgimenti economici e sociali assolutamente inediti per l'epoca moderna. I nostri clienti ci stanno già comunicando le gravi difficoltà che improvvisamente si trovano a gestire per implementare le direttive aziendali che impongono di sospendere l'attività lavorativa negli uffici e nei campus e di predisporre lo smart working, o lavoro agile, per la forza lavoro. Garantire la sicurezza a fronte di questo scenario emergenziale globale comporta notevoli rischi per la maggior parte delle organizzazioni.

RISCHI ASSOCIATI ALL'ADOZIONE RAPIDA DI UN REGIME DI SMART WORKING

Secondo l'ultimo report di International Workplace Group, in tutto il mondo il 50% della forza lavoro opera all'esterno dell'azienda per almeno 2,5 giorni a settimana. In questo momento, tuttavia, l'emergenza COVID-19 sta obbligando più aziende, se non tutte, ad adottare immediatamente un modello di attività lavorativa in remoto. Oltre alla ovvia pressione che questo esodo dagli uffici esercita sul personale IT, sulle architetture di rete e, non ultimi, sui fornitori di attrezzature, ci sono reali rischi informatici che le aziende devono prendere in considerazione.

Sei fattori chiave che favoriscono la sicurezza dei lavoratori agili:

- **Definire politiche di sicurezza informatica aggiornate che includano lo smart working.** Anche se l'azienda si è già dotata di politiche di sicurezza efficaci, è importante riconsiderarle nell'ottica di verificarne l'adeguatezza per una forza lavoro che lavori prevalentemente da remoto. Le politiche devono includere la regolamentazione della gestione dell'accesso da remoto, dell'utilizzo dei dispositivi personali, prevedere policy aggiornate in materia di privacy dei dati rivolte ai dipendenti che accedono a documenti e altre informazioni aziendali e aggiungere la variabile del maggiore utilizzo di shadow IT e della tecnologia cloud.
- **Predisporre i dispositivi personali dei dipendenti, o BYOD, per la connessione al sistema aziendale.** È probabile che i dipendenti facciano affidamento sui loro dispositivi personali per le attività di lavoro da remoto, e questo è particolarmente vero se la contingenza non permette di accedere a dispositivi forniti dall'azienda in un momento in cui la catena di approvvigionamento risulta rallentata. I dispositivi personali devono però garantire lo stesso livello di protezione dei dispositivi aziendali. Inoltre, è necessario considerare le implicazioni in materia di privacy legate al fatto che un dispositivo personale si collega direttamente alla rete aziendale.
- **Reti Wi-Fi non protette potrebbero accedere a dati sensibili.** I dipendenti che lavorano da casa potrebbero accedere a dati aziendali sensibili collegandosi attraverso reti Wi-Fi domestiche che, diversamente dalle reti dell'ufficio, non sono protette da sistemi di sicurezza adeguati, come i firewall. Dal momento che i punti di ingresso remoti alla rete si moltiplicano, sarà necessario porre in essere maggiori tutele per la privacy dei dati e sorvegliare più potenziali punti di intrusione.

- **Igiene informatica e visibilità sono fondamentali.** Non è raro che i dispositivi personali siano caratterizzati da una scarsa igiene informatica. Un elevato numero di dipendenti che opera da remoto può far perdere all'azienda la visibilità sui dispositivi collegati, la cui configurazione, protezione e livello di sicurezza rimarranno sconosciuti.
- **È fondamentale restare aggiornati, perché le truffe legate al coronavirus sono in aumento.** L'Organizzazione mondiale della sanità e la U.S. Federal Trade Commission (FTC) hanno avvisato che sono in atto numerose attività di phishing legate al coronavirus e campagne di false email. È estremamente importante che gli utenti restino continuamente aggiornati e informati e che i lavoratori remoti abbiano la possibilità di contattare tempestivamente il personale IT in caso di problemi. Le aziende dovrebbero anche prendere in considerazione di adottare misure di protezione email più severe.
- **I piani di gestione delle crisi e di risposta agli incidenti devono essere attuabili dalla forza lavoro remota.** Un incidente informatico in uno scenario di lavoro che esula dalle normali condizioni ha maggiori probabilità di finire vertiginosamente fuori controllo. La presenza di strumenti di collaborazione remoti efficaci, come bridge per videoconferenze fuori banda, piattaforme di messaggistica e applicazioni di produttività, invece, consentono ai membri geograficamente distanti di un team di creare una "sala operativa virtuale" da cui gestire le attività di risposta agli incidenti. Se i piani dell'azienda prevedono la presenza fisica di tecnici per interventi specifici, come la ricreazione dell'imaging o la sostituzione dei sistemi infetti, sarebbe prudente esplorare misure alternative o ricorrere a risorse locali.

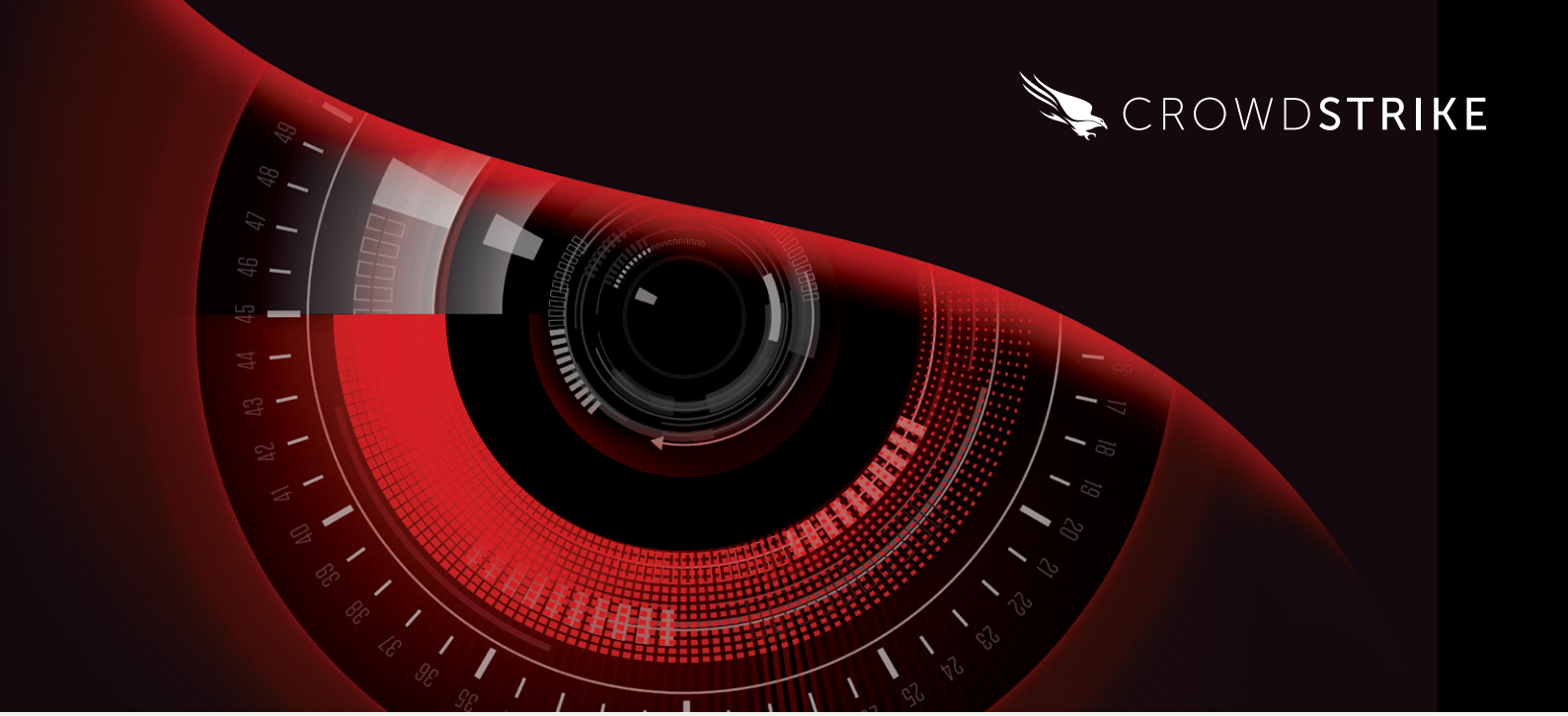
GARANTIRE LA SICUREZZA DELLA FORZA LAVORO REMOTA

CrowdStrike si è guadagnata una posizione unica per aiutare le aziende a gestire questa improvvisa urgenza di predisporre una forza di lavoro remota per due i motivi: il primo è che la nostra piattaforma cloud e la nostra architettura basata su agent a basso impatto sono particolarmente indicate per garantire l'operatività e la messa in sicurezza di una forza di lavoro remota; il secondo è che CrowdStrike stessa, come azienda, utilizza una forza lavoro composta da moltissime persone geograficamente lontane, e questo aspetto le ha permesso di ricavare le competenze necessarie per operare in modo sicuro ed efficace.

Le funzionalità che mette a disposizione la piattaforma cloud CrowdStrike Falcon® per aiutare i clienti ad adottare rapidamente un regime di smart working sono:

Sfruttare la scalabilità e la convenienza del cloud. La sua architettura creata appositamente per il cloud è modulabile in base alle esigenze del cliente e offre capacità di archiviazione e potenza di elaborazione tali da assicurare una protezione in tempo reale, a prescindere dall'ampiezza geografica dell'infrastruttura di rete. Con un'architettura di sicurezza basata sul cloud l'implementazione di risorse aggiuntive non presenta alcuna difficoltà. E se l'assetto remoto richiede l'aggiunta di ulteriori nuovi dipendenti, non è necessario pianificare, preparare e fornire nuovo hardware e software.

Mantenere il massimo livello di sicurezza a prescindere dalla dislocazione dei dipendenti. Un'architettura di sicurezza basata al 100% sul cloud consente di proteggere ogni carico di lavoro in qualsiasi punto della rete, compresi quelli al di fuori del perimetro del firewall e quelli offline, e di garantire misure di sicurezza in tempo reale, il massimo livello di efficacia e rispetto della conformità. La ricerca delle minacce su ogni dispositivo, e specialmente quelli che non sono in rete, è un'attività imprescindibile. Per riuscirci con facilità, pur mantenendo i dati istantaneamente accessibili a chiunque sia autorizzato, è necessario fare ricorso a una soluzione basata sul cloud.



Affidarsi a un'architettura di sicurezza semplice che assicura completa visibilità. Sapere quali utenti e dispositivi si collegano alla rete è indispensabile per attuare un sistema di gestione della sicurezza proattivo. Ogni singolo dispositivo che si collega alla rete deve essere visibile, indipendentemente da dove si trovi. L'agent unico a basso impatto della piattaforma CrowdStrike® Falcon viene installato senza richiedere un riavvio, ha un impatto minimo sulle prestazioni, non infastidisce gli utenti con lunghe operazioni di scansione né con aggiornamenti invasivi delle firme e mette in sicurezza gli utenti nel giro di qualche secondo. Le attività di ricerca e monitoraggio dei carichi di lavoro che la piattaforma Falcon esegue su base continua assicurano ai responsabili della sicurezza una visibilità completa su tutti i dispositivi, siano essi dispositivi locali, aziendali remoti o personali e carichi di lavoro del cloud. Questa visibilità estende la protezione anche ai container e ai dispositivi mobili.

Sicurezza senza preoccupazioni con una soluzione di protezione degli endpoint fornita come servizio. Con CrowdStrike Falcon Complete™, i clienti possono affidare l'implementazione, la gestione e la risposta agli incidenti relativi alla sicurezza dei loro endpoint al collaudato team di esperti della sicurezza di CrowdStrike. Il risultato? Ottimizzazione istantanea della condizione di sicurezza senza sostenere il peso, il carico di lavoro e i costi legati alla gestione di un programma di protezione degli endpoint completo, e con la libertà di impiegare le risorse interne su altri progetti. Falcon Complete è una soluzione di protezione degli endpoint sicura che non richiede alcun intervento. Adottandola, i clienti avranno il personale, i processi e la tecnologia necessari per gestire tutti gli aspetti della protezione degli endpoint, dall'integrazione e la configurazione dei dispositivi fino alla manutenzione, al monitoraggio, alla gestione e al ripristino degli incidenti, a prescindere che riguardino un sistema locale o un collaboratore remoto.

CONCLUSIONI

La crisi causata dal COVID-19 non si risolverà nel breve periodo. Le aziende saranno obbligate a prendere rapidamente decisioni difficili, come adottare un regime di smart working per la forza lavoro. Un passo di questo tipo fatto in emergenza comporta dei rischi, ma la sicurezza delle reti, dei dispositivi e dei dati non devono risentirne.

Chiama un rappresentante di CrowdStrike per ottenere informazioni sui programmi speciali riservati ai clienti CrowdStrike che si trovano ad affrontare un'impennata del numero di collaboratori che operano da remoto. CrowdStrike si prodiga per eliminare quegli attriti che intralciano gli interventi decisivi e per assicurare a tutti gli utenti, a prescindere da dove si trovino, l'accesso alla tecnologia e alle competenze necessarie per operare in un contesto sicuro.

NON PERDERE IL NOSTRO WEBCAST

Ascolta gli esperti di CrowdStrike mercoledì 18 marzo in un webcast che spiega come rendere lo smart working efficace e sicuro. **Iscriviti ora.**

Risorse aggiuntive

- Scopri maggiori informazioni sulla **piattaforma CrowdStrike Falcon.**
- Iscriviti al webcast: **La sicurezza informatica ai tempi del COVID-19: Suggerimenti per rendere lo smart working efficace e sicuro.**
- Visita la pagina **Falcon Complete** per maggiori informazioni sulla protezione degli endpoint senza intervento manuale.
- **Prova una versione completa e gratuita di CrowdStrike Falcon Prevent™** e scopri come il nostro antivirus di ultima generazione gestisce le minacce più sofisticate di oggi.