

affaritaliani.it

Il primo quotidiano digitale, dal 1996



Sondaggi Spread Borse Coronavirus

ATTIVA LE NOTIFICHE

FONDATORE E DIRETTORE: ANGELO MARIA PERRINO

Home > Mediatech > Smart working e cybersecurity: ecco come prevenire i rischi per le aziende

MEDIATECH

A+ A+

Domenica, 12 aprile 2020 - 11:11:00

Smart working e cybersecurity: ecco come prevenire i rischi per le aziende

Quanto lo smartworking mette a rischio in termini di sicurezza i dati per le aziende? Ecco come prevenire i rischi



L'attuale emergenza ha imposto alle aziende il ricorso allo smart-working, ma allo stesso tempo ha portato alla luce una scarsa predisposizione di imprese, di qualsiasi dimensione, a dotarsi di adeguate infrastrutture. Secondo gli ultimi dati di marzo del Politecnico di Milano emerge, infatti, che tra le grandi aziende il 42% non possiede processi strutturati, il 30% non ne ha ancora previsto l'attivazione, mentre tra le Piccole e medie aziende oltre il 65% non sta nemmeno considerando la questione. E se prima del Covid-19 gli smart-worker erano 570mila in tutta Italia, solo nelle due settimane successive al 21 febbraio, ulteriori 554mila lavoratori hanno iniziato a lavorare da casa (dati Ministero del Lavoro di metà marzo), con un incremento del traffico dati dalle abitazioni dal 20% al 50% in più. La conseguenza diretta è che molti lavoratori accedono a dati aziendali dai propri pc personali, facendo così aumentare i rischi di sicurezza informatica, mettendo a repentaglio anche le infrastrutture informatiche delle imprese, spesso non sufficientemente accorte in tema di cybersecurity.

Ecco che viene da chiedersi quali i rischi principali di sicurezza informatica che lo smart-working porta con sé, quando ci si può accorgere che siamo sotto attacco e

come porre rimedio. Ma soprattutto, si può prevenire il rischio di essere attaccati? Lo abbiamo chiesto a [Davide Capozzi](#), Innovation Director di [WIIT Spa](#), uno dei principali operatori italiani di servizi cloud e hybrid cloud specializzato nelle applicazioni critiche, che in questo periodo è molto attivo nel fornire soluzioni per la cybersecurity, garantendo la continuità alle applicazioni e alle infrastrutture aziendali.

Quanto lo smartworking mette a rischio in termini di sicurezza i dati per le aziende?

SMART WORKING E CYBERSECURITY: ECCO COME PREVENIRE I RISCHI PER LE AZIENDE

E' necessario fare un passo indietro e non generalizzare: non è corretto affermare che lo smartworking mette a rischio i dati delle Aziende, invece è vero che una scorretta implementazione tecnologica (ad es. del telelavoro) ed una debole consapevolezza degli utenti in materia di security si che possono mettere a rischio – e molto – i dati e le infrastrutture Aziendali.

Lo smartworking è una pratica organizzativa, in Italia anche definita “lavoro agile”, che mette in condizione i dipendenti delle aziende di portare a termine le proprie attività “dovunque” essi si trovino. Le aziende che abbracciano questa strategia sono aziende che intervengono profondamente sull'organizzazione, sui processi e sulle tecnologie con la finalità di porre i propri dipendenti in su un percorso di responsabilizzazione e di libertà di auto-organizzarsi rompendo i vincoli dettati dagli “orari d'ufficio” e permettendo di riprendere il controllo del proprio “work-life balance”.

In Italia (pre COVID) iniziative di smartworking erano appannaggio soprattutto di grandi aziende che nel 58% dei casi aveva già iniziative strutturate avviate e che solo nel 3% dei casi apparivano disinteressate. In misura molto minore la PA dichiara solo un 7% di disinteresse ma solo nel 16% dei casi aveva già avviato iniziative avviate per arrivare al 30% includendo quelle già in piano. Il dato interessante è quello che riguarda la PMI – che costituiscono il tessuto produttivo del Paese – che si dichiaravano disinteressate ad iniziative di smartworking per più del 50%, una percentuale decisamente elevata se si pensa ai vantaggi in termini di produttività, minor assenteismo, rispetto delle scadenze e soddisfazione dei dipendenti che queste pratiche portano.

Poi il 23 Febbraio lo scenario italiano e mondiale è cambiato con uno shock improvviso dovuto all'emergenza sanitaria COVID che, dal punto di vista Aziendale, ha repentinamente posizionato in telelavoro praticamente il 100% dei dipendenti se le aziende volevano continuare a produrre.

Come sempre accade quando si è in emergenza, se non si è preparati ad accendere scenari alternativi, il rischio è quello di effettuare scelte ed implementare soluzioni sub-ottimali che trascurano determinati aspetti all'apparenza superflui, ma che possono creare effetti dirompenti. E' il caso appunto di molte Aziende che per far fronte alla necessità di “remotizzare” i propri dipendenti molto velocemente hanno trascurate nelle soluzioni adottate degli aspetti fondamentali di security.

Rischi che si corrono

I rischi che si corrono sono i medesimi che si correvano prima dell'emergenza. E' la probabilità che questi si realizzino che è aumentata almeno per un paio di fattori: la riduzione della capacità dei dipartimenti di security aziendali di governare “perimetri liquidi” e l'aumento delle minacce mirate.

Pensate ad un'azienda con persone che vivono e lavorano all'interno di un castello medioevale e pensate che la maggior parte dei dipartimenti di security aziendali costruiscono i propri sistemi di difesa per presidiare le mura di questo castello dagli attacchi esterni attraverso sofisticati strumenti di prevenzione delle intrusioni, identificazione di eventuali infezioni tra le persone, verifica delle informazioni in ingresso ed in uscita dagli unici canali ben noti. Ora pensate che l'emergenza COVID e le relative misure che le aziende hanno attuato per effettuare telelavoro, è stato come far uscire tutti e pretendere di controllare le attività continuando a presidiare le mura del castello, le porte e le infezioni all'interno.

Le IT aziendali hanno vissuto l'incubo di vedere letteralmente “sciogliersi” i propri perimetri (che sono divenuti “liquidi” per l'appunto) in poche ore e a pretendere di governare, con strumenti tradizionali, utenti che si collegavano alle applicazioni aziendali usando PC personali (ben lontani dagli standard e policy aziendali) e attraverso reti pubbliche.

Il secondo effetto è dovuto invece allo sfruttamento da parte di male intenzionati della situazione congiunturale di emergenza per sfruttare sia implementazioni deboli di sicurezza, che un fisiologico abbassamento dell'attenzione degli utenti che stavano vivendo un cambiamento inatteso.

E' presto per avere dati affidabili, ma sono noti casi di malware inseriti nei pdf di autocertificazione del Ministero dell'Interno o l'attacco portato al sito del INPS in occasione dell'apertura delle domande di sussidio.

Come accorgersi che siamo sotto attacco?

Gli attacchi informatici hanno molte analogie con le epidemie, sia come dinamiche di diffusione che come modalità per proteggersi, che come strategie per eliminarle che come strumenti per combatterle. Allo stesso modo di un virus nella popolazione, un attacco informatico si continua a diffondere in azienda indisturbato se non presenta “sintomi” o se non si possiede un “test” per identificarlo.

SMART WORKING E CYBERSECURITY: ECCO COME PREVENIRE I RISCHI PER LE AZIENDE

E' noto che il tempo medio a livello globale che intercorre tra l'inizio di un attacco informatico e l'identificazione è di 99 giorni, con picchi oltre i 1000 giorni in area Asia Pacifico. Fanno meglio gli Stati Uniti con 42,5 giorni, ma comunque sono tempi infinitamente lunghi e più che sufficienti ad un attaccante per infettare "senza sintomi" l'intera infrastruttura ed al momento opportuno sferrare un attacco micidiale.

E' per questo motivo che sono diventati sempre più efficaci e richiesti strumenti di "early detection", degli antivirus avanzati basati su algoritmi di AI che analizzano il comportamento e si costruiscono dei modelli statistici di riferimento in cui, anche la minima anomalia, viene identificata. Si tratta di strumenti sofisticati appannaggio di strutture specialistiche come i Security Operating Center che, oltre a schierare ed utilizzare lo strumento, identificano ed analizzano le anomalie classificandole come veri o falsi positivi.

Come correre ai ripari

Nel momento in cui un'azienda si rende conto di essere bersaglio di un attacco informatico, probabilmente gran parte dei suoi sistemi potrebbe essere già stata compromessa ed è molto complicato se non sconsigliato intervenire autonomamente, ma il consiglio è quello di rivolgersi ad aziende esperte in grado di intervenire in emergenza con strumenti e persone di alto livello.

Se un'azienda si riconosce nell'ultimo periodo nell'aver attuato soluzioni di telelavoro senza badare a questi aspetti e non ha rilevato "sintomi" di una possibile infezione, probabilmente è ancora in tempo per accendere un servizio di SOC esterno che prenda il controllo dell'infrastruttura e pratichi dei "sanity check" per verificare l'integrità del perimetro.

Si può prevenire il rischio?

Sì, ma bisogna prima misurarlo, poi identificare una strategia per ridurlo e successivamente gestire il rischio residuo. Nel caso di soluzioni di smartworking è possibile accedere ad una offerta completamente a servizio, come ad esempio quella offerta da ["Wiit Smartworking as a Service"](#) o da altri seri operatori del mercato, a servizi pre-confezionati che permettono alle aziende di acquisire soluzioni, modulari e scalabili, che hanno già all'interno gli strumenti per gestire in sicurezza gli utenti, le connessioni ed i dati, l'accesso a tutte le piattaforme aziendali, anche quelle più critiche grazie alle tecnologie di remotizzazione applicativa, anche se gli utenti sono collocati su reti pubbliche e con dispositivi propri.

Commenti: 0

Ordina per [Meno recenti](#) ↕



Aggiungi un commento...

 Plug-in Commenti di Facebook

PROMOTED CONTENT

 Mgid



Prince Harry & Meghan's Marriage May Be On The Rocks



This Kind Of Behavior On A Plane Is Unacceptable!



Matilda Actress Is 32 Now & Gorgeous



A Giant Bird That Looks Totally Out Of This World

Commenti

[Accedi o crea un profilo per commentare](#)

[Articolo successivo >](#)

SMART WORKING E CYBERSECURITY: ECCO COME PREVENIRE I RISCHI PER LE AZIENDE