Smart Working: ecco gli strumenti per lavorare in sicurezza

Assicurarsi che lo strumento informatico che si utilizza per il lavoro da remoto sia sicuro; avere la certezza che il Pc che si connette al sistema aziendale non abbia problemi di sicurezza; bloccare e disattivare tutti i protocolli non utili; controllare periodicamente il livello di sicurezza. Sono le quattro principali misure che le aziende devono adottare per avere la certezza di operare con un sistema informatico sicuro nello **smart working**. Misure che, Atlante Informatica ha messo a punto e, da circa due mesi, sta illustrando alle principali imprese italiane che hanno deciso di dotarsi di questo nuovo strumento di lavoro.

Sono passati infatti più di due mesi dagli inizi del lockdown e la maggior parte delle aziende che potevano usufruire dei vantaggi dello smart working si sono adeguate. Ma, tra la fretta di adeguarsi per continuare a lavorare e, la novità dello strumento informatico, a che punto siamo con la sicurezza informatica aziendale? "Sono tante le aziende – spiega il Ceo di Atlante Informatica, **Alessandro Musso** – che si chiedono: adesso che adottiamo lo smart working, quali sono i rischi per la sicurezza informatica? Come posso verificare la sicurezza IT dell'azienda? A cosa devo prestare attenzione? A tutte queste domande stiamo dando risposte e, per questo, abbiamo definito un percorso che garantisca la piena sicurezza per le aziende nello smart working".

Indice

Un protocollo che garantisce un'adeguata sicurezza

Atlante Informatica ha così messo a punto un protocollo che definisce e garantisce un'adeguata sicurezza informatica alle imprese. Un protocollo che prevede, prima di tutto, quatto misure indispensabili. "Prima di tutto – sottolinea Musso – ci si deve assicurare che lo strumento informatico che stiamo utilizzando per connettere i nostri utenti remoti al sistema aziendale sia sicuro. Strumenti come le VPN sono considerati tendenzialmente sicuri in quanto utilizzano la crittografia dei dati tra dispositivo remoto e azienda. Esistono poi alcuni protocolli che

permettono il **lavoro da remoto** che possono funzionare anche senza VPN, come il protocollo RDP di Microsoft. Ma questa modalità utilizzata senza il supporto di una VPN che rende il tutto sicuro, causa spesso enormi falle di sicurezza nelle aziende ed è quindi fortemente sconsigliata".

Il secondo passo – aggiunge il Ceo di Atlante Informatica – è quello di assicurarsi che il PC o il dispositivo remoto che si connette al **sistema aziendale sia sicuro**. "Non dobbiamo cadere nella trappola di non preoccuparci di questo aspetto. Se questo dispositivo dovesse essere infettato da un virus o, ancora peggio, sotto il controllo di un hacker, mediante la VPN – spiega – l'attaccante potrebbe raggiungere il sistema azienda e causare danni ingenti. Come si risolve questo problema? La cosa migliore è dotare ogni smartworkers di un dispositivo fornito dall'azienda e dotarlo di sistemi di protezione come antivirus e antimalware. Qualora non fosse possibile occorra assicurarsi che il Computer remoto sia dotato almeno di un antivirus".

Altra misura da tener presente è il blocco e la disattivazione di tutti i protocolli e servizi che non sono utili. "Quando attiviamo un utente remoto – aggiunge Musso -, nella stragrande maggioranza dei casi, i sistemi aziendali abilitano tutte le funzionalità. Spesso però, la maggior parte non verranno mai utilizzate e costituiranno una **vulnerabilità per la nostra rete**. Con l'aiuto di un professionista, sarà necessario identificarle e disabilitarle. Un esempio su tutti è il protocollo di condivisione file che andrebbe disabilitato per evitare che il dispositivo remoto possa accedere direttamente ai server aziendali. Altro esempio è limitare l'accesso degli utenti remoti ai soli dispositivi che devono essere raggiunti da remoto".

Disponibile un ambiente virtuale di test completamente gratuito

La quarta misura riguarda il **controllo periodico della sicurezza**. "Dopo aver predisposto le misure illustrate – spiega ancora Musso -, tutto dovrà essere testato e verificato con strumenti appositi ed automatici ovvero con uno Vulnerability Assessment System. Un Vulnerability Assessment System è uno strumento che è in grado di trovare le vulnerabilità conosciute che affliggono il sistema, e consigliarci un metodo per risolvere il problema. Noi di Atlante Informatica abbiamo realizzato un ambiente di test liberamente scaricabile, gratuito e pronto all'uso. Si tratta di un ambiente virtuale che una volta scaricato, permetterà di eseguire automaticamente delle scansioni di tutti i dispositivi presenti sulla rete aziendale. Dopo aver eseguito questa scansione, il sistema fornisce un report delle vulnerabilità trovate e spesso suggerisce anche come risolvere il problema ed aumentare così il livello di sicurezza. Questo permetterà di individuare e risolvere le falle di sicurezza che potrebbero essersi venute a creare nella fretta di collegare tutti gli utenti al 'sistema azienda'".

Ma non è tutto. Musso sottolinea infatti che "il nostro **ambiente virtuale** è in grado di produrre dei report dettagliati della rete aziendale e dei dispositivi che la popolano. Questi report possono essere facilmente trasformati in Audit ed allagati al fascicolo sulla normativa GDPR. Infatti, non dobbiamo dimenticare gli sforzi fatti per adeguare l'azienda alla normativa GDPR. Per agevolare l'uso di questo ambiente, abbiamo messo a punto una guida che, seguendola passo passo, permetterà di sfruttare al meglio lo strumento. Per riassumere, quindi, il protocollo da seguire prevede: leggere la guida, scaricare lo strumento, effettuare la scansione della rete, analizzare i risultati ottenuti, applicare le correzioni laddove necessarie, rieseguire la scansione. Infine, qualora volessimo, potremmo allegare i report e creare degli Audit per la normativa GDPR".

La guida e l'ambiente di test sono disponibili a questo link:

https://www.firewallhardware.it/vulnerability-assessment

Atlante Informatica Srl è nata nel 2007 con l'aiuto dell'I3P (incubatore del Politecnico di Torino) con l'obiettivo di progettare soluzioni integrate e personalizzate che permettano alle aziende di ottimizzare i loro processi informatici rendendoli automatici ed efficienti. L'azienda è composta da 2 Business Units: Atlante e Miniserver. Atlante fornisce soluzioni e servizi ICT per le PMI Italiane. Miniserver è attiva nella produzione di firewall e router venduti in tutto il

mondo e dotati principalmente di sistemi operativi gratuiti

TAGS Sicurezza Informatica Smart Working

Mi piace 0

Facebook Linkedin Twitter

Potrebbe interessarti anche:

Sulla piattaforma Celiachia Facile parte il ciclo di webinar dedicato alle intolleranze al glutine

Agricoltura: assistenza legale alle imprese con JSL

Sanità: dall'esperienza del Gruppo Dimensione nasce Aywyn

Articoli più letti

Bollonet: come pagare il bollo online

Bollonet è il servizio proposto appositamente dall'ACI - Automobile Club d'Italia - per dare la possibilità di pagare il bollo dell'auto direttamente online, velocizzando la...

Comprare Casa da Privato: cosa devi sapere

Inps Pin: come attivarlo e come usarlo