Covid-19, quali sono i rischi informatici che le imprese devono affrontare?



Oramai è la normalità, con l'arrivo della pandemia di **Covid-19** (o **Coronavirus**), molte organizzazioni si sono spostate verso un ambiente di lavoro virtuale.

Chi ha già compiuto questo passo o chi ancora sta compiendo la trasformazione, obbligatoriamente ha dovuto iniziare a lavorare con fornitori terzi per mantenere la propria *business continuity.*

Covid-19 e cybersecurity: quali rischi?

Ma se da un lato i fornitori possono aiutare a mantenere l'attività "in piedi", dall'altro comportano anche un Cyber rischio aggiuntivo, che spesso può essere trascurato o addirittura ignorato mentre le operazioni quotidiane cambiano

così rapidamente.

Quali sono allora i Cyber rischi che le organizzazioni devono affrontare e risolvere per potersi affidare a terzi durante l'epidemia di COVID-19?

Lo scenario della Cyber Security al tempo del Covid-19

Per capire quanto il virus sia diventato pervasivo anche nel mondo del Cyber Crime basta dare uno sguardo a quanto sta succedendo al momento.

Il rischio Cyber quando ci si affida a terze parti, d'altronde, non è nulla di nuovo. I Criminal Hacker operano sul concetto di "*path of least resistance*" per portare a termine i loro attacchi e spesso i fornitori sono una delle porte d'ingresso preferite. Prenderli di mira significa spesso per loro riuscire a non essere scoperti ed eventualmente prendere di mira più organizzazioni contemporaneamente.

Naturalmente il passaggio a un luogo di lavoro virtuale aumenta l'uso dei canali online, tra cui le riunioni, le comunicazioni e le operazioni quotidiane. La maggiore presenza online presenta rischi crescenti per la sicurezza informatica, poiché la superficie di attacco si espande oltre la rete tradizionale dell'organizzazione.

Il problema non può essere ignorato, secondo un recente studio a campione quasi il 60% delle aziende intervistate ha subito una violazione dei dati attraverso un fornitore terzo e solo il 30% ha un inventario completo di tutti i fornitori terzi con cui lavora.

Ora, soprattutto per le aziende che di solito non hanno lavoratori in Smart working è emersa ancora di più la necessità di affidarsi a servizi come VPN e software di video-conferencing.

Le categorie di rischio

Operativo

Il rischio operativo è la prospettiva di perdite derivanti da procedure, sistemi o policy inadeguate o non funzionanti. Questo tipo di rischio può includere errori dei dipendenti, errori di sistema, frodi o altre attività criminali; insomma qualsiasi evento che interrompa i processi aziendali.

È imperativo che i fornitori siano controllati per garantire che le esigenze dell'organizzazione possano essere soddisfatte. Ciò dovrebbe includere la garanzia che il partner abbia un piano di business continuity e di disaster recovery. Ça va sans dire che è imperativo sincerarsi anche che il fornitore abbia un piano per superare la pandemia COVID-19, poiché il loro stesso fallimento potrebbe causare una perdita anche alla vostra organizzazione.

Transazione

Il rischio di transazione è il rischio di perdita a causa di problemi con il servizio o la delivery dello stesso. Questi tipi di rischio includono capacità inadeguate, guasti tecnici ed errori umani.

Durante la pandemia COVID-19 è fondamentale che le organizzazioni siano in grado di continuare ad operare a un livello il più possibile vicino all'As-is. I fornitori che non sono in grado di gestire la capacità delle esigenze di un'organizzazione rappresentano un rischio.

I piani di continuità operativa dei propri partner dovrebbero includere anche piani per fornire un servizio ininterrotto alle organizzazioni durante la pandemia.

Compliance

Questo tipo di rischio potrebbe estendere la responsabilità all'organizzazione se la terza parte subisce violazioni della sicurezza che coinvolgono le informazioni del cliente in violazione degli standard di tutela delle informazioni del cliente.

Mentre i cambiamenti nel flusso di lavoro stanno cambiando rapidamente, è imperativo che le organizzazioni si assicurino che tutti i fornitori terzi seguano le leggi e i regolamenti applicabili.

Come mitigare il rischio

Sebbene molte aziende stiano lavorando rapidamente per far migrare in maniera efficiente i propri dipendenti verso il lavoro a distanza, è più importante che mai garantire che i rischi sopra elencati siano presi in considerazione e valutati. Ecco alcuni modi in cui la vostra organizzazione può mitigare la situazione e intervenire:

- Prendetevi il tempo necessario per analizzare il vostro partner/fornitore. Potrebbe salvare la vostra organizzazione dall'assumere rischi non necessari;
- Mantenere o creare un team di risposta. Questo team può aiutare a valutare il rischio e a formulare raccomandazioni in base alle necessità. Questo team dovrebbe anche tenere un inventario completo di tutti i fornitori terzi e includere copie dei piani di continuità operativa;
- Tenere traccia dei Cyber Incident che potrebbero interessare i vostri fornitori. I servizi di Cyber Threat Intelligence, nascono e servono anche per questo. La biblioteca di intelligence contiene una moltitudine di aggiornamenti sugli incidenti che potrebbero interessare i fornitori terzi di un'organizzazione;

https://www.key4biz.it/covid-19-quali-sono-i-rischi-informatici-che-le-imprese-devono-affrontare/298220/