**RISCHIO CYBER: NON BASTA L’IT A PROTEGGERCI  
Il commento di ANRA, Associazione Nazionale dei Risk Manager**

*Analisi di Alessandro De Felice, Presidente ANRA – Associazione Nazionale Risk Manager e Responsabili Assicurazioni Aziendali*

La transizione repentina di molte aziende al *remote working* e l’esigenza improvvisa di gestire gran parte delle attività a distanza, a seguito dell’emergenza Covid, ha spostato di fatto in modo massiccio operazioni e processi in ambito digitale e fatto emergere nuove vulnerabilità in un brevissimo lasso di tempo. Si tratta di cambiamenti che avrebbero richiesto anni per essere implementati correttamente all’interno delle aziende, ma che hanno fatto irruzione senza possibilità di scelta e molto spesso senza un adeguato piano operativo, aprendo di conseguenza nuovi scenari di rischio.

I rischi connessi con la digitalizzazione dei processi sono noti da tempo e non possono più essere definiti una minaccia emergente. Una recente survey presentata da The Innovation Group in un evento patrocinato da ANRA ha confermato che **solo l’8% delle aziende italiane negli ultimi mesi non ha registrato alcun episodio di attacco cyber** (solo tentato, per fortuna, nella maggior parte dei casi). La percentuale si fermava all’11% nel 2018. In questo contesto già vulnerabile, si è inserito l’improvviso massivo ricorso ad un telelavoro che dal punto di vista della sicurezza informatica ha avuto ben poco di “smart”: spesso adottato in carenza di infrastrutture e dotazioni tecniche adeguate (molti lavoratori sono stati obbligati a rendere noti recapiti personali e a utilizzare dispositivi privati pur di garantire la continuità operativa), con poco tempo per formare i dipendenti sul tema, e ancora meno per strutturare un risk assessment che tenesse conto della mutata situazione.

Per fare un bilancio preciso sarà necessario aspettare ancora qualche mese – considerando il ritardo con cui molti attacchi vengono rilevati –, ma è significativo che **solo nel primo semestre 2020 in Italia gli attacchi di phishing sono cresciuti del 28%, i ransomware del 23%, i trojan del 27%, le minacce/chatbot via social media del 19%** (dati Bitdefender). Considerando che la modalità da remoto resterà ancora per lungo tempo, se non definitivamente, la modalità prevalente di lavoro in molti settori, è necessario che ciascuna azienda svolga un assessment ad hoc dei nuovi rischi connessi all’uso della rete e dei dispositivi, per poi predisporre un programma di gestione al fine di pianificare e governare le azioni volte a ridurre gli impatti con contromisure efficienti a breve e lungo termine.

I driver principali di queste azioni sono:

* i rischi di non compliance
* rischi di danno reputazionale
* rischi di interruzioni all’operatività
* costi correlati al ripristino dei sistemi
* rischio di controversie legali, ove fossero coinvolti dati sensibili

Cosa possono fare le aziende?

1. **Formare e sensibilizzare dipendenti e utenti**: prima di autorizzare connessioni remote alla rete aziendale, i dipendenti devono ricevere adeguate informazioni sulle campagne di phishing e sulle direttive in materia di sicurezza. Inoltre, devono conoscere tutti i processi e le procedure aziendali per denunciare un eventuale incidente.
2. **Connessioni sicure**: per accedere alle reti aziendali, utilizzare unicamente un accesso remoto sicuro. Ove possibile, utilizzare una rete privata virtuale (VPN) o un altro meccanismo di connessione criptata.
3. **Autenticazione multifattore**: le VPN devono essere configurate con un’autenticazione multifattore per aggiungere un ulteriore livello di protezione e garantire che soltanto le persone autorizzate accedano alla rete aziendale.
4. **Protezione perimetrale**: gli uffici IT devono assicurare che i firewall siano opportunamente configurati e monitorare il logging dei firewall per individuare tentativi di connessione o connessioni non riuscite da parte di indirizzi Internet Protocol (IP) non autorizzati o sospetti.
5. **Sicurezza e conformità del cloud**: le aziende che utilizzano servizi di cloud devono garantire che le configurazioni di sicurezza siano opportunamente rafforzate e monitorate.
6. **Più monitoraggio e diligence**: se vi sono regioni geografiche o paesi a cui i dipendenti non hanno motivo di collegarsi in remoto dalla rete aziendale, l’ufficio IT deve proattivamente mettere in ‘black list’ le rispettive gamme IP, onde impedire la connessione da remoto alle reti aziendali.

Le conseguenze della pandemia hanno imposto un’accelerazione allo sviluppo digitale del nostro Paese, forzando anche le aziende più restie ad adottare le nuove tecnologie, ed è un’opportunità che non va sprecata. I rischi, anche quelli cyber, si individuano, si gestiscono. Il rischio più grande resta quello di non saper cogliere l’opportunità.

**CHI È ANRA**

*ANRA è l'associazione che dal 1972 raggruppa i risk manager e i responsabili delle assicurazioni aziendali. L'associazione opera attraverso la sede di Milano e vari corrispondenti regionali. ANRA è il punto di riferimento in Italia per diffondere la cultura d'impresa attraverso la gestione del rischio e delle assicurazioni in azienda. Si relaziona con le altre associazioni nazionali di risk manager in Ferma, a livello europeo, e in Ifrima a livello internazionale. ANRA è costituita da Risk Officer, Risk Manager ed Insurance Manager che operano quotidianamente nella professione e che trovano vantaggio nello scambio continuo delle proprie esperienze e nella condivisione di progetti a beneficio dello sviluppo del settore. Complessivamente, le aziende pubbliche e private di cui fanno parte i soci rappresentano un fatturato complessivo di oltre 430 miliardi (pari a circa il 25% del PIL).*

*Nella piena convinzione che l'esperienza sia il miglior argomento per diffondere la cultura del risk management, ANRA organizza incontri aperti a professionisti ed aziende su tematiche inerenti al rischio aziendale, corsi di formazione per nuove figure e scambi di esperienze con colleghi stranieri. Nella sua attività di supporto a manager ed imprese, ANRA si appoggia a molti partner, come enti universitari, società di consulenza, compagnie assicurative, broker, società di servizio nell'ambito del rischio d'impresa: con le loro competenze specifiche, tutti questi attori portano valore aggiunto ai membri dell'associazione e alle loro imprese. Dal giugno 2016 ANRA promuove "alp" - ANRA Learning Path - la nuova Accademia ANRA per la formazione dei professionisti della gestione del rischio, riconosciuta e certificata RIMAP a livello europeo.* [www.anra.it](http://www.anra.it)

**Per informazioni**

Noesis - ufficio stampa ANRA

Elena Cerutti, Eleonora Carminati

T. 348.3175490 – 02.8310511

[anra@noesis.net](mailto:anra@noesis.net)