DIRITTO DELLE TECNOLOGIE
Prof. Avv. Fabrizio Corona

News – 15 ottobre 2021

ATTACCO HACKER ALLA REGIONE LAZIO: COSA CI INSEGNA?

Il 4 agosto 2021, la Regione Lazio ha subito un attacco hacker al ced regionale. L'attacco è partito dal computer di un dipendente LazioCrea in smart working, contagiato da malware. Ad essere criptati sono stati i dati presenti su virtual machine VM-Ware e documenti regionali. Inoltre, ad aggravare la posizione della Regione Lazio è stata l'assenza di un backup offline e la cancellazione da parte degli hacker di quello online. L'attacco, da un'analisi dell'ultimo rapporto Clusit, era tra i più prevedibili in quanto il settore pubblico è tra gli obiettivi più colpiti dal Cybercrime dal 2020. La maggioranza degli attacchi avviene con malware ed il trend è in evidente crescita.

Ma quali sono le considerazioni di natura legale-normativa in riferimento a questo attacco?

In primo luogo, bisogna analizzare le misure minime di sicurezza dell'AGID (Agenzia per l'Italia Digitale) per la Pubblica Amministrazione, le quali richiedono che i supporti contenenti almeno una delle copie di backup non siano permanentemente accessibili dal sistema, onde evitare che attacchi su questo possano coinvolgere anche tutte le copie di sicurezza.
Occorre poi tenere in considerazione le prescrizioni della Direttiva europea NIS (Network and Information Security), la quale impone agli Stati Membri dell'Unione Europea l'adozione di una serie di misure comuni per la sicurezza informatica, con l'obiettivo di definire un'unica linea strategica tra i vari Stati dell'Unione contro il rischio di incidenti ai danni delle reti e dei sistemi di informazione.
L'infrastruttura critica della Regione Lazio rientra a pieno titolo nella Direttiva europea NIS, la quale prevede espressamente l'obbligo di implementare un piano di risposta agli incidenti che descriva le procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti che comportano una violazione di dati personali, oltre ad un piano di ripristino da eseguire dopo aver subito un incidente di sicurezza.

In secondo luogo, la Regione Lazio è soggetta alla normativa privacy, che prevede specifici obblighi di comunicazione ai soggetti interessati quando la violazione comporta un rischio elevato per i loro diritti e libertà. L'Autorità Garante per la protezione dei dati personali ha da subito seguito con particolare attenzione gli sviluppi dell'attacco informatico subito dalla Regione e ha già analizzato la prima notifica preliminare di violazioni dei dati, che gli è stata trasmessa dalla Regione stessa, al fine di valutare la gravità dell'attacco.

Questo attacco potrebbe portare la Regione Lazio a subire, oltre al danno d'immagine, anche una sanzione privacy che, nei casi più gravi, arriva fino ad € 20.000.000,00.