ATTACCO HACKER ALLA REGIONE
COSÌ È STATO SVENTATO

È accaduto ad agosto: per quattro giorni e quattro notti il team campano e gli esperti di Digital Value hanno lavorato insieme. Preservati i dati grazie agli investimenti in sicurezza

di **Paola Cacace**

Immaginate dei cybercriminali che cercano di entrare nell'infrastruttura di una Regione per cercare di distribuire software malevolo, rubare i dati e, magari chiedere un riscatto. Immaginate però che questi cybercriminali abbiano trovato «ad attenderli» i «buoni». Ossia un team in grado di contrastare il loro attacco hacker. E, ancora, immaginate che questa battaglia a colpi di cybersecurity si sia protratta per 4 giorni e 4 notti. Ininterrotte.

Ebbene questa non è la trama di una spy story ma quanto è successo quando a fine dell'agosto scorso la Regione Campania è riuscita a sventare un attacco hacker che mirava all'esfiltrazione di dati grazie al lavoro combinato del proprio team di esperti di cyber security aiutato da quello di Digital Value, operatore di riferimento in Italian le settore delle Infrastrutture ICT. «Ci siamo trovati a dover agire in pochissimo tempo per scongiurare una situazione che poteva avere conseguenze devastanti per la riservatezza delle informazioni, con milioni di dati di utenti e cittadini che rischiavano di essere compromessi e utilizzati in modo illecito - spiega Massimo Bisogno, Direttore Ufficio Speciale per la crescita e la transizione digitale della Regione Campania - Una vicenda che abbiamo sventato prontamente grazie agli investimenti in sicurezza, formazione e tecnologia messi a disposizione della Regione, che, oltre a risorse proprie, si avvale anche di partner specializzati di alto livello come Digital Value Cyber Security. Ma il lavoro che ci ha permesso di sventare l'attacco è iniziato molto prima di agosto. Anzi direi che la prima regola quando si parla di cybersicurezza è la prevenzione. Fondamentale per tutti, sia che si sia pubblica amministrazione che un'azienda privata. C'è chi penserà che io sia pessimista ma sono solo realista: quando si parla di cyberattacchi non è una questione di "se attaccano" ma di "quando". Per questo l'amministrazione aveva fatto in-

Bisogno (Regione): la prima regola della cybersicurezza è la prevenzione, fondamentale per gli enti pubblici

vestimenti a riguardo creando un gruppo di lavoro dedicato e attivando tutti i possibili allarmi. E proprio per questo il 28 agosto abbiamo ricevuto delle notifiche su dei comportamenti anomali. A questo punto è entrato in campo il nostro Fabio De Paolis che ha visto la mail in tempo reale, tra l'altro in giorni feriali, è intervenuto subito».

«I tempi di reazione sono stati molto rapidi e quindi abbiamo bloccato qualsiasi esfiltrazione di dati. Ovviamente poi c'è voluto qualche giorno per fare tutte le verifiche del caso - spiega De Paolis della Regione Campania - affiancati dagli esperti di Digital Value Cyber Security. E così individuata subito la compromissione di una postazione server, e una volta isolata e controllata, ci siamo subito mossi per comunicare l'evento all'Agenzia per la Cybersicurezza Nazionale così tutte le fasi di analisi ed approfondimento a seguire sono state svolte in costante collaborazione tra il gruppo di sicurezza regionale e CSIRT. Inutile dire che la primissima azione è stata il blocco della rete regionale. Un'azione precauzionale che però ci ha permesso di contrastare l'attacco in sicurezza. La verifica dei backup poi ci ha confermato che eravamo riusciti a farlo». Un lavoro che il team della Regione ha portato avanti senza alcuna interruzione h24 per 4 giorni e 4 notti grazie alla guida di Antonio Montillo, responsabile offensive security e incident response leader di Digital Value che spiega: «Il processo di verifica delle postazioni di lavoro e dei sistemi server è stato lungo e intensivo, ma è stato eseguito diligentemente dal personale della Regione per consentire la riapertura progressiva e sicura della rete, che era stata chiusa a scopo precauzionale. In questi casi un partner tecnologico come Digital Value Cyber Security è fondamentale per attivare immediatamente le incident procedures, per risalire alla fonte da cui origina l'intrusione nel sistema, isolare le postazioni colpite e monitorare il perimetro dell'infrastruttura in coerenza con la tipologia d'attacco subito. Un intervento tempestivo fa la differenza per questo è essenziale che si sia la massima collaborazione tra enti e società private. Il gioco di squadra è la migliore difesa».

Società come Digital Value S.p.A. realtà quotata sul mercato Euronext Milan da maggio 2023, che è uno degli operatori di riferimento in Italia del settore, infatti, giusto per tirare un po' le somme, ha registrato ricavi consolidati di 708,5 milioni di euro (secondo bilancio consolidato al 31 dicembre 2022) e conta oltre 400 dipendenti. «La cybersicurezza è un'emergenza che non va mai sottovalutata - commenta Irene Sorani, Ceo di Digital Value Cybersecurity – specialmente in uno scenario geopolitico come quello attuale il panorama futuro è quello di possibili attacchi che non limitano il proprio scopo all'estorsione ma anche al furto di informazioni e al mettere in difficoltà le infrastrutture. Ciò permette di immaginare che gli attacchi saranno sempre più complicati e complessi ed è qui che investimenti e know-how possono fare la differenza».