Cybercrime, come difendersi da attacchi ransomware

Chi non ha mai sentito parlare di **ransomware**? Son gli attacchi informatici perpetrati a danno soprattutto di aziende e professionisti con cui i cyber-criminali bloccano l'accesso ai dati e ne promettono la restituzione solo in cambio di un riscatto.

Ma quante sono le vittime? Quanto si paga di riscatto? Il fenomeno è in crescita? Quali sistemi operativi colpisce maggiormente? A rispondere a queste domande ci ha pensato **Achab** che insieme a **Datto** (di cui qui abbiamo raccontato del suo **fondatore Austin McChord**) ha realizzato una **ricerca intitolata 'Lo stato del ransomware in Italia'** dalla quale emergono spunti utili a comprendere meglio il fenomeno.

La ricerca stima che **il 5% delle PMI a livello mondiale abbia subito attacchi ransomware**. In Italia quasi li 90% degli MSP (i fornitori di servizi informativi, ndr) intervistati da Achab e Datto ha eseguito interventi in seguito ad attacchi ransomware negli ultimi 2 anni. E oltre il 30% ha dovuto eseguire 5 o più interventi nel solo 2017. Oltre l'80% degli MSP dichiara che il ransomware è destinato ad aumentare dei prossimi 12 mesi e il 19% di questi pensano che aumenterà in modo significativo.

Il 40% de partecipanti al sondaggio ha denunciato almeno una volta alle autorità l'attacco, un balzo in avanti rispetto alla precedente edizione del sondaggio relativa all'anno precedente da cui emergeva che solo il 25% aveva fatto denuncia. Inoltre la percentuale di chi è stato disponibile a pagare almeno una volta il ricatto è calata dal 37% al 24%. E di questi il 9% non è comunque riuscito a recuperare i dati.

Non è però **il riscatto chiesto dal ransomware a creare i maggiori problemi alle aziende quanto lo sono invece downtime e la perdita di dati.** Quasi il 90% degli MSP dichiara che i propri clienti hanno subito downtime e quasi il 50% ha subito delle perdite di dati. **Il valore del riscatto è mediamente compreso tra i 500 e i duemila euro in oltre la metà dei casi**, nel 34% dei casi è inferiore a 500 euro e solo nel restante 14% dei casi è superiore a duemila euro.

La ricerca ha anche rilevato un ulteriore aspetto che appare decisamente preoccupante e cioè che le versioni più avanzate e recenti di attacchi **ransomware non risparmiano nessun sistema e nessuna azienda.** Tutte le aziende vengono infatti attaccate, indipendentemente dai sistemi di sicurezza messi

in atto e una volta entrato il ransomware cifra tutto quello che trova: il 38% degli intervistati dichiara di aver visto cifrare anche i backup.

Insomma il pericolo è concreto e serio e i sistemi di protezione più classici come gli antivirus sono spesso inefficaci così come non sono immuni nemmeno i sistemi operativi considerati tradizionalmente più sicuro come OsX o come quelli dei dispositivi mobili anche se, rileva l'analisi, il più colpito resta il sistema operativo Windows. E nemmeno il cloud è immune a questo tipo di attacchi.

Come ci si difende? Bisogna agire in modo coordinato e su più livelli, essere pronti a reagire in modo efficace e a ricostruire i dati in caso tutte le altre difese siano state penetrate. Secondo gli esperti di Achab e Datto **la prima linea di difesa non è tecnologica ma culturale**, serve infatti rendere tutte le persone dell'azienda consapevoli verso i rischi potenziali, e la consapevolezza è uno degli elementi chiave dal quale partire per costruire una difesa, e mettere loro in condizione di saperli riconoscere e quindi bloccarli all'origine per quanto possibile. Poi è naturalmente fondamentale dotarsi di una infrastruttura tecnologica resiliente che abbia funzioni di backup sia locali sia in cloud e sia in grado di garantire la cosiddetta **business continuity.**

La ricerca di Achab e Datto non cita esplicitamente le **startup**, ma è lampante che **il rischio riguarda ogni tipo di impresa,** comprese quelle che muovono i primi passi e per le quali un attacco del genere potrebbe significare anche la morte immediata. D'altra parte è anche vero che le startup, soprattutto se in fase early stage, è dotata di poche risorse finanziarie da investire per dotarsi di sistemi informativi completi di tutte le funzionalità necessarie a ottenere un livello di sicurezza sufficiente. Perciò è ancora più determinante in questi casi la consapevolezza e la formazione delle persone che lavorano con i sistemi informativi, che sia una rete complessa o semplicemente uno smartphone.