Ransomware Attack Response Checklist

PUNTO 1: Disconnetti Tutto

- [ ] **a. Scollega il computer dalla rete**
- [ ] **b. Spegni tutte le opzioni wireless: Wi-Fi, Bluetooth, NFC**

PUNTO 2: Determina la Portata dell'Infezione, e verifica i seguenti Segni di Cifratura

- [ ] **a. Drive associati o condivisi**
- [ ] **b. Folder associati o condivisi da altri computer**
- [ ] **c. Dispositivi d'archiviazione in rete di qualunque tipo**
- [ ] **d. Dischi rigidi esterni**
- [ ] **e. Dispositivi d'archiviazione USB di qualunque tipo (chiavi USB, memory stick, cellular/fotocamere collegati)**
- [ ] **f. Dati archiviati in Cloud: DropBox, Google Drive, OneDrive ecc.**

PUNTO 3: Determina la potenza del Ransomware

- [ ] **a. Che potenza o tipo di ransomware? Per esempio: CryptoWall, Teslacrypt ecc.**

PUNTO 4: Decidi la Risposta

Ora che sai quali e quanti file sono stati criptati e conosci il tipo di ransomware con cui hai a che fare, puoi prendere delle decisioni più informate su quale deve essere la tua prossima mossa.

Risposta 1: Ripristina i tuoi Dati dal Backup

- [ ] 1. **Individua i backup**
  - **a. Assicurati che ci siano tutti i file di cui hai bisogno**
  - **b. Verificane l'integrità (es. file corrotti)**
  - **c. Controlla l'esistenza di Copie Ombra (potrebbero non essere un'opzione in caso di ransoware più recenti)**
  - **d. Controlla la presenza di versioni precedenti dei file che possano trovarsi in Cloud es. DropBox, Google Drive, OneDrive**
- [ ] 2. **Rimuovi il ransomware dal tuo sistema infetto (esegui più di uno scan AV)**
- [ ] 3. **Ripristina i file dal backup**
- [ ] 4. **Determina il vettore d'infezione ed affrontalo**

Risposta 2: Cerca di decriptare

- [ ] 1. **Determina la potenza e la versione del ransomware se possibile**
- [ ] 2. **Individua un decifratore, potrebbero non essercene per i ransomware più recenti. Ma se lo trovi, allora prosegui…**
- [ ] 3. **Collega ogni dispositivo di archiviazione che contenga file criptati (dischi rigidi, chiavi USB, ecc.)**
- [ ] 4. **Decripta i file**
- [ ] 5. **Determina il vettore d'infezione ed affrontalo**

Risposta 3: Non fare nulla (e perdi i file)

- [ ] 1. **Rimuovi il ransomware**
- [ ] 2. **Esegui il backup dei file criptati perché in un futuro più o meno prossimo potrebbe essere trovato un decifratore (opzionale, ma consigliato)**

Risposta 4: Negozia e/o paga il Riscatto

- [ ] 1. **Se possibile, cerca di negoziare per ottenere un riscatto minore da pagare e/o un più lungo periodo di pagamento**
- [ ] 2. **Stabilisci i metodi di pagamento accettabili per il riscatto: Bitcoin, Carta di Credito, ecc.**
- [ ] 3. **Ottieni la possibilità di pagare, probabilmente tramite Bitcoin:**
    - a. **Individua un cambio da cui acquistare Bitcoin (il tempo è essenziale**
    - b. **Setta un account/portafoglio ed acquista il Bitcoin**
- [ ] 4. **Riconnetti il computer criptato a Internet**
- [ ] 5. **Installa il browser TOR (optional)**
- [ ] 6. **Determina l'indirizzo di pagamento del Bitcoin. Può trovarsi sullo screen del ransomware o su un sito TOR appositamente creato**
- [ ] 7. **Paga il riscatto: trasferisci il Bitcoin nel portafoglio del ransomware**
- [ ] 8. **Assicurati che tutti i dispositive con file criptati siano connessi al computer**
- [ ] 9. **Le decifratura dovrebbe iniziare entro le 24 ore, ma spesso anche in meno tempo**
- [ ] 10. **Determina il vettore d'infezione ed affrontalo**

PUNTO 5: Proteggiti per il Futuro

- [ ] a. **Implementa una Checklist per la Prevenzione del Ransomware per evitare attacchi futuri**

Ransomware Prevention Checklist

Prima Linea di Difesa: gli Utenti

- [ ] 1. **Implementa un programma di security awareness efficace per istruire gli utenti sugli elementi da individuare per impedire che applicazioni criminali vengano scaricate/eseguite.**
- [ ] 2. **Esegui attacchi simulati di phishing per vaccinare gli utenti contro le presenti minacce.**

Seconda Linea di Difesa: il Software

- [ ] 1. **Assicurati di avere e di stare utilizzando un firewall.**
- [ ] 2. **Implementa filtri antispam e/o antiphishing. Puoi farlo con un apposito software o tramite un hardware dedicato come SonicWALL o Barracuda.**
- [ ] 3. **Assicurati che tutti in azienda utilizzino un software antivirus robusto e aggiornato, o i più avanzati prodotti di endpoint protection per il whitelisting e/o il blocco in tempo reale dei file eseguibili.**
- [ ] 4. **Stabilisci delle policy per la restrizione dell'uso di software sulla rete per impedire l'esecuzione di applicazioni non autorizzate (opzionale)**
- [ ] 5. **Definisci una procedura di patch molto metodica che aggiorni tutte le applicazioni che possano avere qualche vulnerabilità.**

Terza Linea di Difesa: i Backup

- [ ] 1. **Implementa una soluzione di backup: software, hardware, o entrambe.**
- [ ] 2. **Assicurati che per tutti i dati che hai necessità di salvare o accedere sia effettuato il backup, inclusi quelli su dispositivi mobili/USB.**
- [ ] 3. **Assicurati che i tuoi dati siano protetti, ridondanti e facilmente accessibili dopo il backup.**
- [ ] 4. **Testa con regolarità le funzioni di ripristino della tua procedura di backup/restore. Verifica l'integrità dei dati sui backup fisici e la facilità di ripristino dei backup online o software.**