RANSOMWARE

@FEDERPRIVACY

CHE COS'E'?

I **RANSOMWARE** sono virus informatici che rendono inaccessibili i file dei computer o dei dispositivi infettati e chiedono il pagamento di un riscatto per ripristinarli

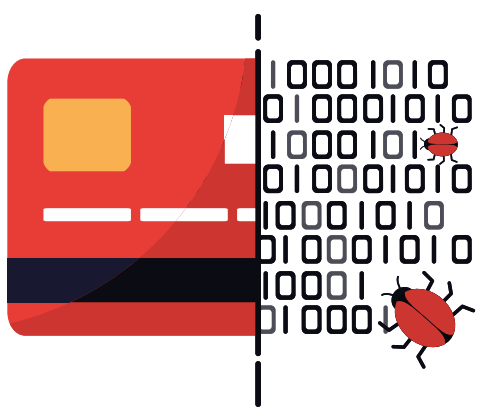
COME SI PRENDE?

- L'utente che pone scarsa attenzione o non ha consapevolezza può innescare il ramsoware attraverso l'**apertura di una e-mail** (email di phishing)
- Il ransmoware può propagarsi in rete usando le vulnerabilità dei software e/o dei sistemi operativi

COME TE NE ACCORGI?

Tutti i file non sono più utilizzabili e/o accessibili. Al posto dello sfondo del desktop compare un avviso con la **richiesta di un riscatto.** Generalmente in CRIPTOVALUTA (Bitcoin ma non solo)

COSA FARE? PAGO?



NO! Pagare il riscatto può esporre a **responsabilità penale**. Il pagamento può essere perseguito in quanto "***favorisce***" **il reato commesso da chi effettua l'attacco (favoreggiamento); inoltre, potrebbe costituire uno dei reati presupposto ai sensi del D.Lgs. 231/2001.** Infine, si potrebbe porre in contrasto con i valori, i principi e gli ideali di comportamento di cui al ***Codice Etico dell'azienda.***

Nel caso di PA si deve anche rispondere per **Danno Erariale.**

Per tali motivi si raccomanda sempre di NON PAGARE

RANSOMWARE

FEDERPRIVACY

COME SI PREVIENE?

Per prevenire gli effetti di un attacco ransomware dobbiamo ricordarci di applicare alcune accortezze.

0 Eseguire **Backup** periodici secondo la **Regola 3-2-1**

Utilizzare **Password** sicure ricorrendo al riconoscimento multifattoriale 1

2 **Proteggere** la rete locale da attacchi esterni mediante **firewall**

Usare sempre **mail istituzionali** con crittografia abilitata 3

4 Evitare il **click compulsivo:** prima di aprire un messaggio di posta con allegato, **verificare** sempre il mittente, andando a controllare che il nome che compare corrisponda all'indirizzo mail, e che questo non sia un **fake**

Proteggere ogni **postazione di lavoro** (PC o notebook) con **AntiVirus** 5

6 **Aggiornare** i Software ed i Sistemi Operativi quando viene richiesto

Attivare autonomamente oppure con il supporto del fornitore un **piano di protezione dei dati**, meglio se basato su un'analisi dei rischi (**Security by Design**) 7

8 Effettuare **formazione** periodica a tutti i dipendenti

Seguire uno o più canali che divulgano informazioni appartenenti al settore sicurezza informatica (social, siti web, notifiche sms, ecc.) per essere tempestivamente al corrente delle nuove minacce 9

RANSOMWARE

@FEDERPRIVACY

COME SI INTERVIENE?

0 Creare un **TAVOLO TECNICO DI LAVORO** per la Sicurezza delle Informazioni. Il tavolo si deve riunire periodicamente e deve essere composto almeno da:
- Rappresentante del Titolare;
- Responsabile IT;
- DPO o Referente Privacy

1 Riunire l'Unità di Crisi che comprende il Titolare, il Tavolo Tecnico e l'avvocato (eventualmente in un secondo momento)

2 Fare l'**analisi** delle infrastrutture e dei dati impattati e valutare i danni (se necessario coinvolgendo anche esperti esterni)

3 Valutare se occorre inviare la **notifica** di Data Breach a Garante Privacy entro **72** ore da quando se ne è venuti a conoscenza

4 Se si rientra negli **OPERATORI dei SERVIZI ESSENZIALI (OSE)** notificare entro **6** ore l'incidente al CSIRT (Computer Security Incident Response Team - Italia)

5 Valutare se occorre **comunicare** la violazione agli interessati

6 Contattare lo **studio legale** e valutare le attività difensive :
- **denuncia** all'Autorità di Polizia Postale;
- **costituzione di parte civile** per la richiesta di risarcimento dei danni in sede penale

7 Valutare con il legale di avviare le **indagini difensive forensi**

8 Documentare tutte le azioni intraprese (**quando** e **cosa**)

9 Predisporre un **piano di miglioramento della Cybersecurity** per non ricadere nuovamente nel riscatto