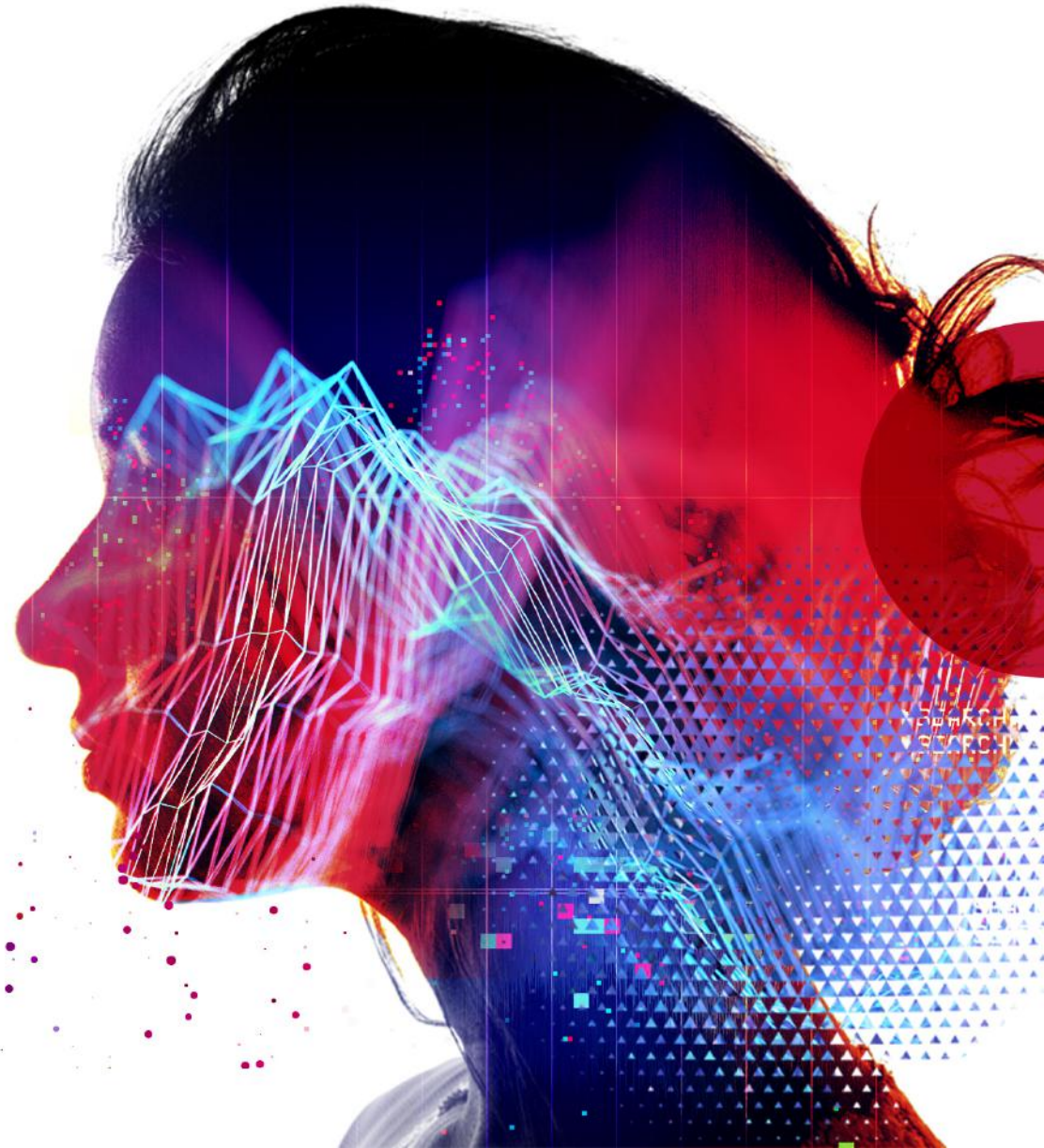
LUTECH
your digital Ξvolution partner.

Allerta ransomware: sei pronto a ripartire?

I fondamentali per la prevenzione, la risposta agli attacchi e il data recovery



Fabio Bucciarelli - 27 Maggio 2020

Come affrontare la prevenzione e la risposta agli attacchi cyber in azienda?

Le misure di sicurezza organizzative, procedurali e tecnologiche in azienda

Devono essere contestualizzati sul livello di integrazione dei processi di gestione del rischio cyber all'interno dell'organizzazione.

Può essere opportuno partire da una gap analysis fra le misure di sicurezza applicate dall'azienda rispetto a best practices, linee guida, framework

Best practices, linee guida, framework

Perché?

- Si tratta di strumenti per aiutare le organizzazioni a definire un percorso strategico volto alla cybersecurity e alla protezione dei dati coerente con i regolamenti, riducendo i costi necessari e aumentando l'efficacia delle misure realizzate
- Una possibilità è quella di utilizzare il Cybersecurity Framework del NIST, contestualizzato in Italia con il Framework nazionale per la cybersecurity e la data protection. Fornisce uno strumento operativo per organizzare i processi di cybersecurity e di data protection adatto alle organizzazioni pubbliche e private, di qualunque dimensione
- Vediamo ora ad altissimo livello cosa prevede il framework e come ci può essere d'aiuto nell'individuare le misure che ci permettano di prevenire e rispondere agli attacchi di ransomware

NIST Cybersecurity Framework

Core

Attività abilitanti alla cybersecurity quali controlli di sicurezza, best practices, ecc. Sono categorizzate in modo da indicare specifici obiettivi di sicurezza

Profiles

Rappresentano la “postura” attuale / desiderata di un’organizzazione attraverso le attività abilitanti del core

Implementation Tiers

Indicano il livello di integrazione della cybersecurity nei processi di risk management

Framework Core

- Function
- Category
- Subcategories

Identify

Obiettivo: identificare per prevenire e proteggersi dagli attacchi ransomware

- Identificare i requisiti di business (dati critici, requisiti di accesso, requisiti di sicurezza, ecc.)
- Assegnazione dei valori di impatto RID dei dati
- Gestione degli asset hardware e software
- Identificazione degli utenti anche in base ai loro ruoli e identificazione dei rischi loro associati

Protect

Obiettivo: evitare che il ransomware attecchisca

- Programmi di awareness mirati alle varie categorie di utenti e campagne di phishing simulato
- Limitare al massimo visibilità e accesso ai dati (segmentazione della rete, controllo degli accessi)
- Mantenere aggiornati i sistemi
- Strumenti anti malware avanzati
- URL / web filtering
- Strumenti di protezione delle mail
- Strumenti di cyber threat intelligence

Detect

Obiettivo: rilevare l’infezione il prima possible

- Strumenti di rilevamento delle anomalie (livello rete, postazione di lavoro, comportamento utente, ecc.)
- Sistemi di sandboxing
- Comunicazione tra i sistemi di detection e quelli di prevention
- Security continuous monitoring
- Struttura dedicata al monitoraggio della sicurezza (SOC interno o esterno)

Respond

Obiettivo: essere preparati a fronteggiare l'emergenza, avendo chiari ruoli e procedure

- Formalizzazione di un processo per la gestione degli incidenti che preveda:
  - pianificazione e preparazione alla risposta;
  - individuazione e analisi dell'incidente;
  - contenimento, eliminazione e ripristino;
  - analisi post-incidente
- Forensics "readiness"
- Istituzione di un team dedicato alla gestione degli incidenti, con possibilità di utilizzare un team interno e/o SOC esterni con know-how di alto livello.

Recover

Obiettivo: recuperare i dati persi

- Una prima importante misura di recovery dei dati è il ripristino dai backup
- In caso di ransomware questo potrebbe non essere sufficiente in quanto anche i dati di backup potrebbero essere stati cifrati dal ransomware
- Potrebbe quindi essere necessaria una soluzione specifica per il recovery dei dati