CAMERA
DI COMMERCIO
INDUSTRIA
ARTIGIANATO
E AGRICOLTURA
DI TRENTO

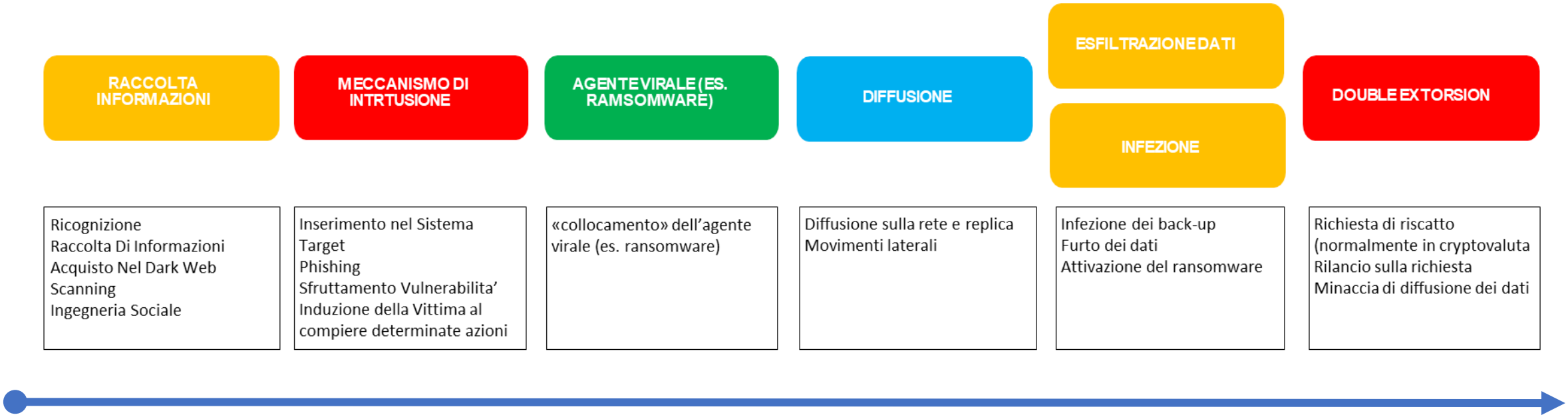
Pronti all'impresa

CYBERSECURITY: MEGLIO PENSARCI PRIMA

Un caso reale di attacco, ripristino e successiva messa in sicurezza

BEINNOVA

Come avviene un attacco?



L’incidente

Grande azienda italiana – i numeri:

- 1,2 Miliardi di € di fatturato
- 8.000 dipendenti
- attiva in oltre 25 Paesi

Da una prima raccolta di informazioni, il problema era attribuibile ad un attacco che aveva disattivato il server e diffuso tramite il domain controller aziendale il malware «Sodinokibi», che criptava dati contenuti nei client e nei server, rendendo inutilizzabili pressoché tutti gli strumenti aziendali (posta elettronica, file server, server gare, applicativi amministrativi, ecc. ecc...).

La timeline dell'attacco

1 — Vulnerabilità umana
Il DG si registra su un APP lecita utilizzando le credenziali aziendali (mail e password)

2 — Vulnerabilità esterna
L'APP subisce un data breach e le credenziali degli utenti vengono esfiltrate

3 — Raccolta Informazioni Darkweb
Il dataset contenente le credenziali del DG vengono vendute in un dataset nel Dark Web

4 — Meccanismo di intrusione
Phishing-social engineering
Viene inviata una mail di phishing a diversi collaboratori dall'indirizzo email del DG

5 — Agente Virale
Phishing-social engineering
La mail contiene del testo credibile, un allegato attendibile ed un ransomware occultato

6 — Vulnerabilità umana
Un dipendente che opera in Mozambico, riceve la mail e ne scarica il contenuto

7 — Vulnerabilità Tecnica
Il PC utilizzato ha un antivirus «free» e viene infettato

8 — Vulnerabilità Tecnica
Tramite collegamento alla rete (RDP) il ransomware si introduce nella rete aziendale

9 — Vulnerabilità Tecnica
Il sistema antivirus aziendale non rileva il malware

10 — Vulnerabilità Tecnica
La rete aziendale è «piatta» e non tutti i server sono dotati di AV

11 — Diffusione
Tramite «movimenti laterali» il malware prende possesso del Domain Controller

12 — Diffusione
Vulnerabilità tecnica
Tramite DC il ransomware si diffonde a tutti i server, ai NAS, ai backup ed al server Antivirus!

13 — Esfiltrazione
Viene esfiltrata una copia dei dati aziendali

14 — Infezione
Ha luogo l'infezione, tutti i dati vengono cryptati

15 — Estorsione
Vengono richiesti 750.000 $ di riscatto per avere i codici di decriptazione dei dati

recoinnassance — exploitation — extorsion

t0 — t0 + 180 gg — t0 + 210 gg — t0 + 240 gg

Gli effetti DIRETTI dell'attacco

1. Impossibilità di accesso ai dati ed agli applicativi
2. Ricezione richiesta di riscatto (**750.000 €**)
3. Blocco del 65% della produzione (impossibilità invio ordini materiali)
4. Personale impossibilitato a lavorare: richiesta di cassa integrazione/ferie forzate per centinaia di dipendenti
5. Bloccati processi di gara (progettazione-offerta) e di esecuzione commesse
6. 4 settimane per il ripristino dell'85% della produttività ordinaria
7. Attivate denunce alle autorità di Polizia Giudiziaria e Garante Privacy
8. 2 CDA straordinari per gestione dell'incidente: denunce, comunicazioni al Garante, ferie e cassa integrazione del personale
9. Costo dell'Emergency Response Team BE INNOVA – Delta Informatica

Gli effetti INDIRETTI dell’attacco

1. Danni di immagine e reputazionali
2. Penali per ritardi su consegne
3. Perdita opportunità (abortite 2 offerte)
4. Rischio diffusione dei dati personali nel DarkWeb

Il flusso di lavoro nella gestione di cyber incident e data breach

BEINNOVA

STEP 1

Identify & Contain Threat

- Confirm incident internally
- Identify threat
- Contain threat

STEP 2

Regulatory Assessment

- Determine jurisdictional coverage
- Assess wider regolatory risk

STEP 3

Communicate to Stakeholders

- Alert effected [and tangetial] departments

STEP 4

Investigate the Breach

- Investigate affected endpoints to determine how breach occurred
- Collect compromised data
- Analyse compromised data

STEP 5

Notification Process

- Notify regulators of breach
- Communicate the breach to the company

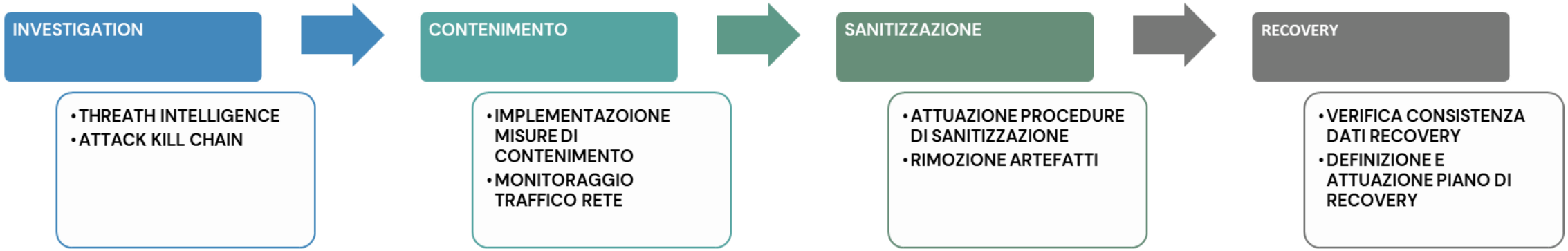
STEP 5

Remediate the Breach

- Third-party remedation setup
- Third-party remedation communication
- Engage law enforcement if needed

L’intervento di Be Innova e Delta Informatica

1. T1 (03/2021): telefonata con richiesta di supporto per un generico: «abbiamo perso i dati aziendali»
2. T1 + 30’: organizzata squadra di primo intervento (ERT) e organizzata riunione con personale del Cliente, pre-allertando Corporate Legal di gruppo
3. T1 + 90’: attivato Data Breach Management



Action plan – fase 1: azioni immediate di identificazione e contenimento del contagio

1. Identificazione causa (Sodinokibi) e studio funzionamento dell'attacco
2. Identificazione e Isolamento asset impattati
3. Disabilitazione di tutte le utenze con privilegio di amministrazione
4. Isolamento zone/asset non impattati (distacco cablaggio fisico/disattivazione schede di rete)
5. Disabilitazione RDP e collegamenti da/verso azienda
6. Analisi e isolamento copie di back-up
7. Informazione a tutti i referenti aziendali
8. Attivazione contatti con vendor tecnologici per supporto
9. Denuncia a Polizia Postale
10. Attivazione per valutazione necessità di informativa verso garante Privacy (GDPR)
11. Copia dei log (FW, DC etc.)

Action plan – fase 2: analisi dell’impatto e valutazione dei danni

- Identificazione dei vettori d’attacco, dei punti d’ingresso, dei target colpiti e delle tecniche usate per portare a fondo l’assalto attraverso l’attività di analisi dei log, tracking dell’attacco (kill chain), target analysis e data compromise discovery.

- Forensic investigation: cristallizzazione delle evidenze e delle prove raccolte al fine di indentificare, preservare, recuperare e analizzare i dati raccolti

Action plan – fase 2: analisi dell’impatto e valutazione dei danni

1. Analisi dei log per individuare fonte e modalità dell’infezione
2. Coinvolgimento e richiesta di analisi dei log da parte dei vendor (AV etc.)
3. Individuazione e analisi degli assett infetti
4. Individuazione e analisi dei servizi impattati
5. Predisposizione comunicazione verso utenti
6. Acquisizione di copie forensi
7. Analisi della sussistenza dei presupposti art. 33 GDPR
8. Predisposizione comunicazione verso utenti, clienti, fornitori, Garante
9. Attivazione monitoraggio sui server «apparentemente» non infetti

Action plan – fase 3: Integrity & Vulnerability checkup

L'Integrity check consiste nella fase di verifica dell'integrità della struttura colpita.

L'azione consiste nel controllare e verificare se all'interno dell'infrastruttura non siano ancora presenti elementi malevoli installati dagli attaccanti. L'intero step viene portato a termine attraverso l'asset inventory, (malware assessment, log analysis etc.)

Il Vulnerability checkup ha lo scopo di preservare l'integrità dell'infrastruttura informatica.

L'analisi delle criticità ha l'obiettivo di identificare e determinare le eventuali vulnerabilità sfruttate da terze parti per l'attacco.

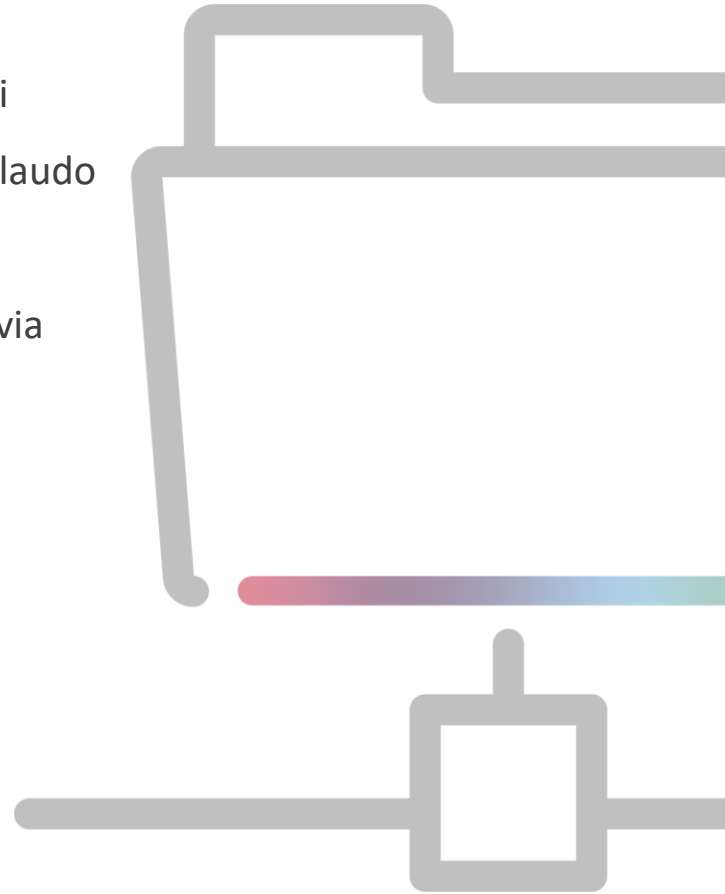
Tutto ciò avviene mediante penetration test, vulnerability test e network scan.

1. Analisi approfondita dei log con i vendor
2. Network Scan
3. Vulnerability Assessment
4. Ricerca sul deep/dark web di eventuali dati esposti (utenze e password, credenziali, dati personali)
5. Valutazione dell'impatto sui dati personali di dipendenti, clienti, fornitori etc. in ottica GDPR

Action plan – fase 4: ripristino e riavvio dei servizi

Ripristino della rete e degli asset aziendali tramite:

- La creazione di una VLAN di test, sicura e monitorata, nella quale testare i vari asset ripristinati
- Ripristino progressivo degli asset, aggiornamento, installazione tool di sicurezza aggiuntivi, collaudo degli asset, revisione privilegi di accesso
- La creazione di varie reti segmentate (client, server, backup etc.) da popolare con gli asset via via ripristinati e messi in sicurezza
- Monitoraggio continuo degli asset progressivamente immessi in rete
- Revisione generale rete, riconfigurazione privilegi di accesso
- Re-installazione sistemi, server, riavvio applicazioni
- Recupero dati da backup e ripopolamento, verifica integrità
- Riavvio applicazioni, connessioni di rete
- Riattribuzione credenziali
- Supporto costante al personale IT del Cliente



Action plan – fase 5: reporting & remediation

Redazione del «verbale delle operazioni» contenente la descrizione delle attività svolte, delle evidenze emerse, delle criticità rilevate e delle scelte adottate (remediation-mitigation).

Produzione di un documento contenente la descrizione delle azioni future: necessarie, opportune, consigliate corredate dalle argomentazioni tecniche.

Redazione della documentazione relativa alle informazioni necessarie per la completa e corretta compilazione della notifica al Garante oltre a fornire indicazioni di dettaglio per la corretta security governance aziendale.

Produzione di una relazione descrittiva della tipologia dei dati compromessi, la metodologia e la modalità dell'attacco, i target, le misure di sicurezza/contenimento adottate e da adottare, nonché, un piano di mitigazione dei rischi che individui le azioni da mettere in atto per evitare il ripetersi del problema.

Le buone pratiche: meglio pensarci prima!

1. Formazione/sensibilizzazione del personale: l'errore umano è dietro l'angolo
2. Evitare ove possibile l'uso di account aziendali per la registrazione su servizi esterni, in ogni caso utilizzo di password diverse, anche dove vi è MFA
3. Utilizzo di sistemi di posta / antispam evoluti per prevenire più possibile il phishing (ad es. con banner di avviso ricezione mail esterne all'organizzazione)
4. Utilizzo di soluzioni antivirus / threath detection evolute
5. Aggiornamento puntuale di sistemi e applicazioni aziendali anche attraverso sistemi automatizzati di patch management.

Le buone pratiche: meglio pensarci prima!

6. Evitare l'esposizione diretta su internet di sistemi di accesso remoto (rdp) e/o applicazioni se non tramite gateway sicuri e DMZ isolate.
7. Segmentazione delle reti interne tramite l'uso di vlan e regole di firewall volte a consentire solo il traffico di rete necessario per il funzionamento e l'interoperabilità dei vari sistemi
8. Least privilege: evitare quanto più possibile l'assegnazione di «diritti amministrativi» agli utenti, utilizzo di account amministrativi nominali dedicati.
9. Backup: sistemi di backup su apposita vlan dedicata, copie secondarie su supporti offline, remoti, immutabili e pianificazione periodica di test di restore.
10. Non sottovalutare l'importanza del mantenimento dei sistemi infrastrutturali (ad es Active Directory) in favore delle applicazioni LOB.

BEINNOVA

Sede Operativa: Via E. Maccani 195, 38121 Trento (TN)
Sede Milano: Viale Achille Papa, 30 20149 – Milano (MI)

+39 0461 405800
https://www.be-innova.eu | info@be-innova.eu

Delta Informatica

Sede di trento: Via Kufstein, 5 38121 Trento (TN)
Filiale di Vicenza: Viale dell'industria, 42 | 36100 Vicenza (VI)

+39 0461 042200
www.deltainformatica.eu | info@deltainformatica.eu