AIIC2023
FORTEZZA DA BASSO
Firenze 10-13 maggio 2023
Convegno Nazionale
Associazione Italiana Ingegneri Clinici
Innovazione e accessibilità:
il governo delle tecnologie sanitarie come sfida sociale
30 AIIC 1993 - 2023

CYBERSECURITY E DISPOSITIVI MEDICI: LA SICUREZZA CHE VERRA

Cybersecurity TTE

Andrea Gelmetti-Maurizio Rizzetto-Andrea Assunto-Paolo Piaser

CYBERSECURITY E DISPOSITIVI MEDICI: LA SICUREZZA CHE VERRA

Cybersecurity Tabletop Exercise (TTE)

Obiettivo

- Fornire informazioni sulla gestione degli incidenti di sicurezza informatica e sulla Business Continuity e Disaster Recovery.
- Fornire informazioni sui ruoli, le responsabilità e gli adempimenti normativi che potrebbero seguire un attacco informatico.

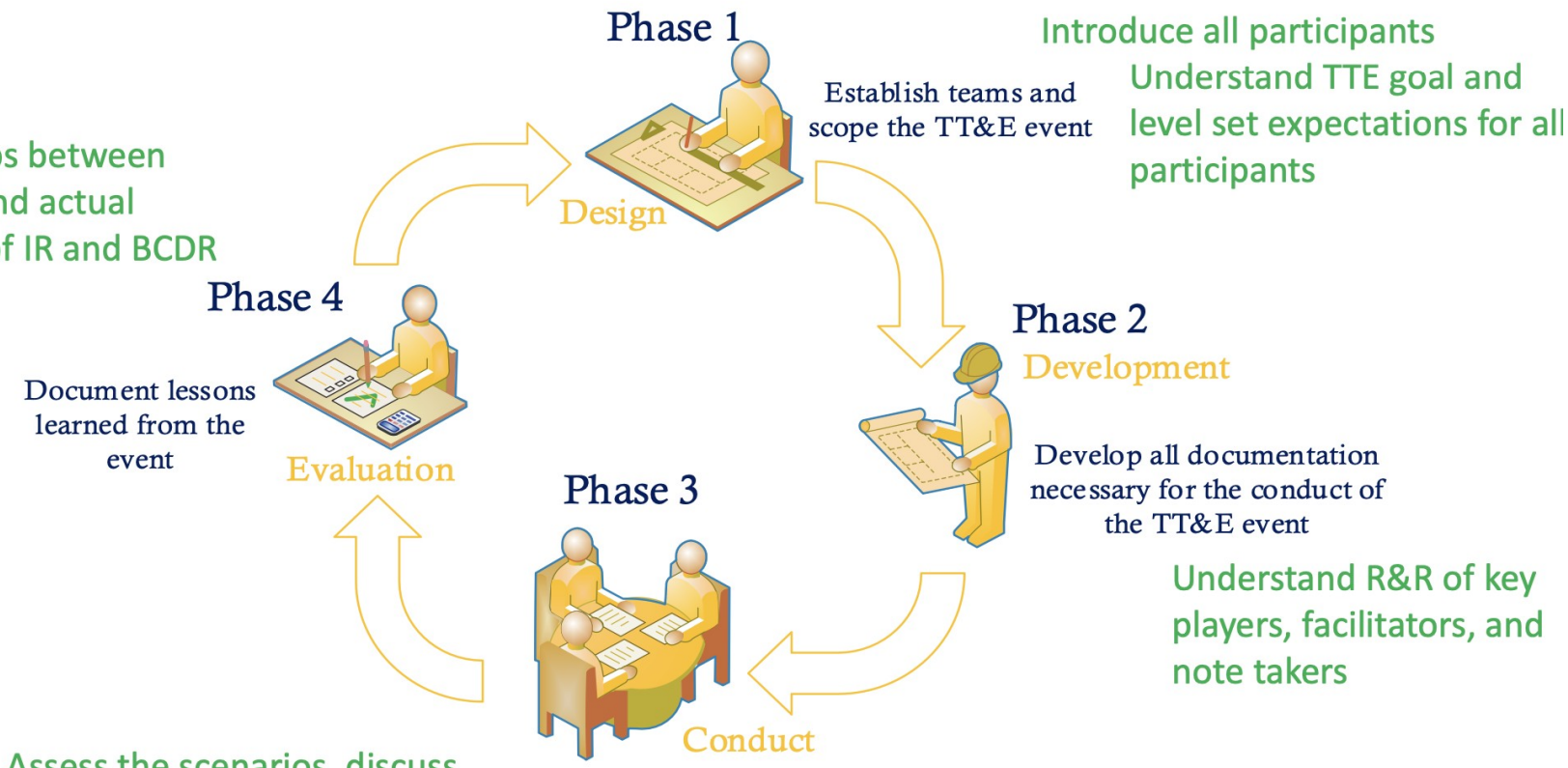
Attività

- Simulare la gestione di un attacco informatico critico e le attività correlate.
- Il gruppo dovrà prendere decisioni al fine di indirizzare le attività per la risoluzione della problematica sotto diversi ambiti
- Come avviene nella realtà non avrete tutte le informazioni rilevanti disponibili nella fase iniziale dell'esercizio.

- **Joint Commission:** Hazzard Vulnerability Analysis (HVA)
- **NIST:** Risk Management Framework (MITRE ATT&CK Framework)
- **ONC:** Security Risk Assessment Toole (SRA)

Scegli visualizzazione barra laterale

Table Top Exercise Methodology



Ref: NIST 800-84

Background

- In una Regione Italiana, vengono accorpate due aziende sanitarie di diverse dimensioni, e diverse esperienze organizzative e competenze diverse.
- La Prima (Azienda 1) fortemente informatizzata, con un alto livello di integrazione e tecnologie mediche evolute che garantiscono un elevata qualità diagnostica e capacità di cura
- La seconda (Azienda 2) meno informatizzata che possiede diverse tecnologie obsolete

La Direzione Strategica chiede che la fusione venga completata nel minor tempo possibile (entro due settimane) come concordato con i vertici della Regione

Lo scenario

- Mentre la definizione dei passaggi amministrativi legati all'accorpamento è in fase avanzata, il personale IT, il personale addetto alla sicurezza e l'ingegneria clinica è in difficoltà.
- Il team IT: il gruppo reti sta cercando di uniformare il livello della rete estendendo i servizi attivi nella LAN di Azienda 1 anche ad Azienda 2, con difficoltà legata alla scarsa documentazione e agli apparati obsoleti installati nei presidi di Azienda 2, causando lentezza al sistema nel suo complesso
- Il team Sistemi: il gruppo dei sistemisti che integra la funzione di IAM ha unificato le modalità di accesso riunendo tutti gli utenti sotto un'unica Active Directory
- Questo fine settimana dalla LAN di Azienda 2 sarà visibile la LAN di Azienda 1 e pertato i fornitori di cartella clinica elettronica potranno migrare i dati nella soluzione scelta dalla Direzione Strategica
- Il team IC: il gruppo derivato dalla fusione dei due servizi precedenti, dopo aver definito i piani di manutenzione e rinnovo del parco macchine.
- Gli ecografi, dopo l'assessment condotto, risultano essere interessati da numerosi richiami e CVE (Common Vulnerabilities Exposures) di criticità legate alla sicurezza.
- Al fine di rientrare dalla situazione di criticità il personale dell'ingegneria clinica ha provveduto in autonomia aggiornando tramite chiavette USB i sistemi ecografici, ad eccezione di quelli obsoleti, dismessi da Azienda 1 da almeno 5 anni.

Primo step 1 – 5 minuti

- È venerdì, alle 15:30, nelle ultime tre settimane, gli ingegneri clinici e i tecnici del servizio in global sono stati impegnati a raccogliere le informazioni sui dispositivi medici in tutte le sedi di Azienda 2, completando l'inventario.
- Il responsabile dell'ingegneria clinica evidenzia il sottodimensionamento del personale in forze presso il servizio per affrontare la messa in sicurezza delle apparecchiature conferite tramite l'accorpamento (mancanza di aggiornamenti, mal gestite/configurate)
- I nuovi firewall e sistemi di sicurezza stanno segnalando che alcuni dei sistemi ecografici obsoleti tentano di raggiungere un sito, www.ecoobsoleti.com, nome simile a quello del produttore dei sistemi. I gestori della parte firewall chiedono all'ingegneria clinica se il traffico rilevato è da considerarsi normale.

Quali strumenti servono per evidenziare il traffico anomalo?

Alla scoperta del traffico anomalo cosa si deve fare?

Chi deve essere informato?

Secondo step– 5 minuti

- Il lunedì, dopo il weekend, gli infermieri e il personale del pronto soccorso stanno segnalando problemi con gli ecografi di marca EcoNEW modello Elite con OS Windows 10.
- I sistemi si avviano correttamente ma non sembrano funzionare opportunamente. Il perosnale segnala che non è possibile consultare i precedenti.
- Il gruppo di rete segnala che altri ecografi, in aggiunta a quelli di venerdì, stanno generando traffico verso www.ecoobsoleti.com. Viene chiesto al responsabile dell'ingegneria clinica se questo comportamento è da considerarsi nella norma.

Quali strumenti servono per evidenziare il traffico anomalo?

Alla scoperta del traffico anomalo cosa si deve fare?

Chi deve essere informato?

Terzo step 3 – 5 minuti

- Lunedì, nella tarda mattinata, i clinici riportano problemi nella consultazione delle mmagini ecografiche tramite la cartella clinica elettronica.
- Gli ecografi interessati dalla problematica sono ancora fuori servizio
- L'ingegneria clinica riferisce che gli ecografi più vecchi, basati su windows 7, non sembrano interesati dalla problematica. I sistemi più aggiornati, equipaggiati con windows 10 risultano inutilizzabili, se non quelli ubicati nelle sedi periferiche.
- Il team di rete riferisce che vedono molto traffico tra le macchine ad ultrasuoni e molti stanno ancora inviando dati tramite protocolli FTP e SCP a www.ecoobsoleti.com.
- Il CISO (responsabile team sicurezza) chiede al responsabile dell'ingegneria clinica la lista dei CVE e la loro criticità relativa all'intera flotta di ecografi aziendali

Quali sistemi dovresti avere a disposizione per valutare l'anomalia nel traffico e acquisire informazioni rilevanti?

Chi informi?

Cosa fai? Quali passi pensi di intraprendere?

Quarto step 4 – 5 minuti

- Lunedì, 14:30, è diventato abbastanza evidente che le vostre strutture sanitarie sono sotto attacco. La CE è operativa ma estremamente lenta, la consultazione della maggioranza dell'imaging diagnostico, non solo gli ultrasuoni, non è più possibile, molti files vengono segnalati come danneggiati.
- Il parco ecografico è operativo solo al 15%, il PS ha iniziato a trasferire pazienti e ambulanze in una situazione di totale congestione delel strutture sanitarie.
- Gli interventi chirurgici che interessano l'utilizzo della diagnostica ecografica vengono riprogrammati.
- Ci si domanda se i ritardi della presa in carico dei pazienti possano portare a conseguenze negative per i pazienti.
- Il tema ingegneria clinica ha chiesto il permesso trasferire i vecchi sistemi ad ultrasuoni dalle sedi periferiche ai reparti dei presidi hub in difficoltà.
- Il team di sicurezza ha rilevato che il sito www.ecoobsoleti.com è un sito malevolo e lo stesso è stato segnalato tre settimane fa con avviso dal produttore.

Quali sistemi dovresti avere a disposizione per valutare la situazione e acquisire informazioni rilevanti?

Chi informi?

Cosa fai? Quali passi pensi di intraprendere?

Quinto step 5 – 5 minuti

- Lunedì, 16:00, info@Azienda1.it riceve un'e-mail che afferma che il gruppo Hacker-Pinko ha lanciato una serie di attacchi alla struttura e sta chiedendo il pagamento di 600.000 euro in Bit Coin per fermare il loro attacco e rilasciare i record di imaging dei pazienti. In caso contrario, continueranno con gli attacchi, corromperanno tutti i record dei pazienti e pubblicando i record dei pazienti rubati sul Dark Web.

Quali sistemi dovresti avere a disposizione per valutare la situazione e acquisire informazioni rilevanti?

Chi informi?

Cosa fai? Quali passi pensi di intraprendere?

Sesto step 6 – 5 minuti

- Lunedì, 16:15, vari canali di notizie locali hanno contattato Azienda 1 chiedendo commenti sulle voci provenienti da più fonti secondo cui sono stati "hackerati". Le fonti sembrano provenire dalle vecchie sedi di Azienda 2, che evidenziano tempi di attesa lunghissimi per le visite al PS.

Quali sistemi dovresti avere a disposizione per valutare la situazione e acquisire informazioni rilevanti?

Chi informi?

Cosa fai? Quali passi pensi di intraprendere?

Settimo step 7 – 5 minuti

- Martedì alle 6:15 mattina è stata indetta una riunione generale dalla Direzione Strategica per valutare la situazione alle 6:30, coinvolgendo tutti gli attori interessati.
- Nella zona si aggirano furgoni delle trupe televisive e mezzi delle autorità competenti.
- Il focus della riunione è come ripristinare la piena operatività, garantendo il corretto trattamento dei dati dei pazienti e le corrette aioni intraprese dall'Azienda 1-2.

Azienda 1-2deve pagare il riscatto sperando di recuperare i dati persi e riportare gli ecografi al normale funzionamento?

Com'era valutato il rischio per i dispositivi interessati prima dell'attacco?

Quali attività di vulnerability assessment e monitoring delle anomalie erano in atto prima dell'attacco?

Quali dati (forensi) hai recuperato tramite i sistemi per definire le metodiche e le tattiche utilizzate nell'attacco?

Hai informato nei modi e tempi appropriati le autorità competenti?

Conclusioni del TTE: Debrief 10 minuti

- Esisteva un piano condiviso tra IT security e ingegneria clinica per ridurre il rischio in Azienda 1-2?
- Sono state seguite best-practices nella valutazione dei beni inventariati da Azienda 2?
- Quale tipo di strumento avrebbe potuto evidenziare i CVE con impatto rilevante tra quelli pertinenti per i MD di Azienda 2?
- Che tipo di strumento si sarebbe potuto utilizzare per rilevare il traffico anomalo che segnava l'inizio dell'attacco?
- Perché il personale di rete non ha isolato le apparecchiature che stavano generano il traffico anomalo?
- I ruoli di responsabilità e decisione erano ben definiti e chiari?
- Chi avrebbe dovuto evidenziare i problemi di sicurezza legati all'unificazione delle due Aziende?
- L'incidente ha evidenziato problemi sistemici nell'organizzazione sanitaria?
- Chi avrebbe dovuto riconoscere tempestivamente l'attacco ed intervenire?
- Chi nell'organizzazione di Azienda 1-2 sarebbe dovuto intervenire per adeguare le attività e le tempistiche del processo di unificazione?
- Secondo voi è stata adeguata la comunicazione per descrivere l'evoluzione della situazione?

Grazie per l’attenzione