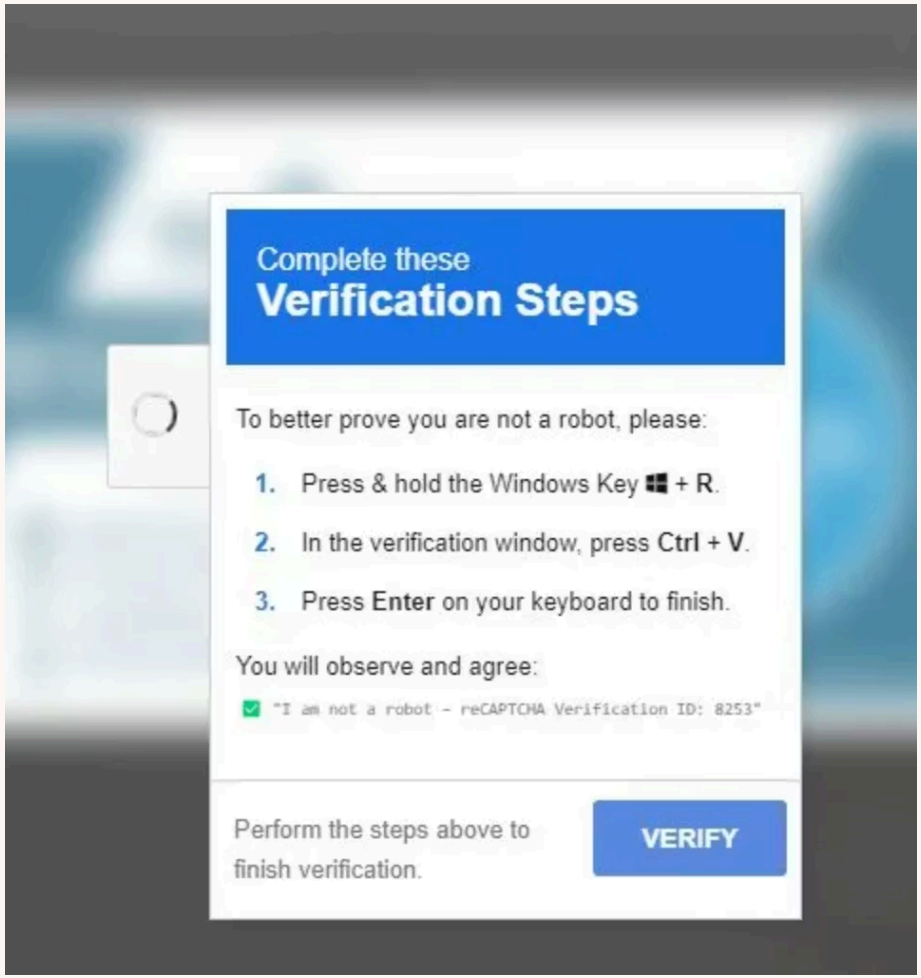
Mentimeter

Scenario iniziale

Un collega riceve una mail apparentemente legittima da un fornitore che chiede di accedere a un portale per manutenzione; durante l'accesso compare un CAPTCHA ma l'accesso non funziona. Il fornitore nega di aver inviato la richiesta.



Mentimeter

Quale dovrebbe essere la prossima azioni?

1. Chiedere ai colleghi se hanno ricevuto email simili e capire se quanto è successo è un caso isolato o un errore del fornitore

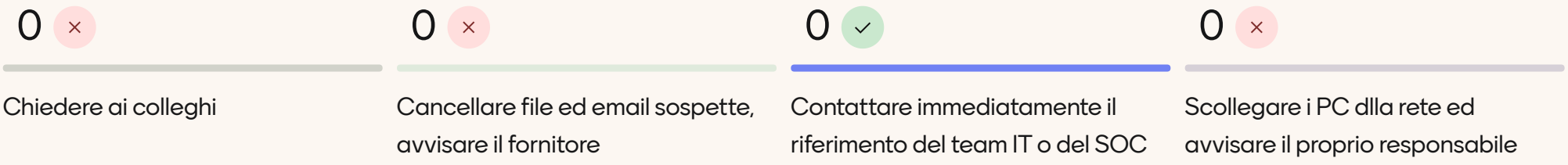
2. Rimuovere tutti i potenziali file sospetti o pericolosi dal PC, cancellare le email e segnalare al fornitore che sono sotto attacco

3. Interrompere le operazioni e contattare immediatamente il riferimento del team IT/SOC tramite i contatti che sono stati forniti dall'azienda

4. Il tempo di risposta ad un incidente è fondamentale per evitare che il problema si propaghi: scollegare immediatamente il PC dalla rete e supportare i colleghi a fare altrettanto, una volta messi al sicuro i sistemi segnalare immediatamente il problema al responsabile che valuterà come agire

Mentimeter

Quale dovrebbe essere la prossima azione?



Decision Point: contenimento dell’attacco

Il team IT da inizio alle operazioni di gestione tecnica dell'incidente.

In questi concitati momenti le figure decisionali sono spesso coinvolte quanto meno a livello informativo e come riferimenti di escalation, è quindi fondamentale essere allineati sul corretto modo di agire.

In questo caso il team IT suggerisce di avviare le operazioni di contenimento che prevedono l'isolamento dei sistemi coinvolti e bloccare tutte le comunicazioni verso l'esterno.

Mentimeter

Quale linea di condotta è la più opportuna?

1. Isolare tutti i sistemi aziendali a prescindere dall'impatto operativo al fine di arginare la minaccia e consentire l'analisi della situazione
2. Isolare i sistemi coinvolti dall'anomalia segnalata ed avviare l'analisi per comprendere l'eventuale livello di compromissione
3. Analizzare immediatamente la situazione per chiarire gli effettivi impatti della minaccia e riportare al responsabile/dirigente gli esiti delle verifiche. Solo in caso le verifiche confermino un effettivo problema di sicurezza si procedere con isolamento dei sistemi accettando i conseguenti impatti sull'operatività dell'organizzazione
4. Dare disposizione al team IT di spegnere ogni cosa, ogni sistema, ogni server fino nuove disposizioni da parte della direzione

Mentimeter

Quale linea di condotta è la più opportuna?

0	0	0	0
Isolare tutti i sistemi dell'azienda, avviare analisi	Isolare i sistemi coinvolti, definire livello compromissione	Analizzare situazione, se incidente confermato si procede al blocco	Imporre lo spegnimento di ogni servizio/sistema fino a nuovo ordine

Decision Point: gestione delle prime ore

I sistemi sono quindi in parte isolati e l'operatività dell'azienda è compromessa. Alcune funzioni principali come la posta elettronica ed i telefoni funzionano ma la produzione è al momento bloccata.

Clienti e fornitori, ignari dell'accaduto, continuano a contattarci per le normali attività del day-by-day.

Come ci comportiamo con clienti e fornitori?

1. Fino a quando la situazione è sotto controllo e nessuno sa cosa è successo, non diamo nessuna informazione e comunichiamo giustificazioni plausibili a chi chiede informazioni.
2. Segnaliamo che al momento abbiamo delle difficoltà tecniche ed i nostri team IT sono già all'opera per ripristinare i servizi. Facciamo seguire degli aggiornamento sulla situazione con informazioni certe.
3. La trasparenza prima di tutto: avvisiamo tutti che siamo sotto attacco, tutto e bloccato e non sappiamo quando la situazione sarà ripristinata.
4. In base a chi ci contatta decidiamo, caso per caso, cosa dire in virtù dei rapporti o dell'importanza dell'interlocutore.

Mentimeter

Come ci comportiamo con clienti e fornitori?

0	0	0	0
Mantendo il silenzio finché posso.	Segnaliamo difficoltà tecniche in gestione, seguono aggiornamenti.	Massima trasparenza e "vuoto il sacco": tutto bloccato e non si sa per quanto.	Valuto caso per caso in base all'interlocutore.

Mentimeter

Decision Point: il team di gestione della crisi.

Il team IT ci comunica che stiamo effettivamente subendo un attacco e si tratta di un ransomware.

Sono passate meno di 24 ore dall'inizio delle attività tecniche, parte dell'operatività è già impattata e si sta cercando di capire quanto in profondità sono stati compromessi i sistemi.

C'è il sospetto che l'attacco sia arrivato a sistemi interni ed a credenziali privilegiate.

Mentimeter

In che momento è il caso di attivare il team per la gestione della crisi?

1. Al termine delle analisi tecniche, se l'esito è di un effettivo impatto sui sistemi o di una effettiva compromissione di dati, sarà necessario attivare il team per informarli della situazione e valutare le attività da eseguire.
2. Solo se si tratta di un ransomware che ha effettivamente cifrato i sistemi e la situazione è di blocco completo.
3. Solo se l'impatto sulla produzione ha iniziato a recare disturbo al clienti.
4. Una volta accertato il perimetro e la tipologia (ransomware), anche se non vi è un immediato impatto, il team deve essere informato.

Mentimeter

In che momento è il caso di attivare il team di gestione della crisi?

0	0	0	0
Solo al termine delle analisi se impatto e gravità accertati	Solo se il ransomware cifra i dati/sistemi	Solo se gli impatti operativi creano disagi ai clienti	Appena definito il perimetro ed il potenziale impatto grave

Decision Point: pagare o non pagare.

Mentre le attività tecniche sono ancora in corso il threat-actor prende contatto e ci comunica che oltre al blocco dei sistemi sono anche state trafugate delle informazioni che verranno pubblicate salvo pagamento di un riscatto in cripto-valuta.

Ci viene inoltre fornito l'indirizzo di una chat (via onion site) per mettersi in contatto con l'attaccante.

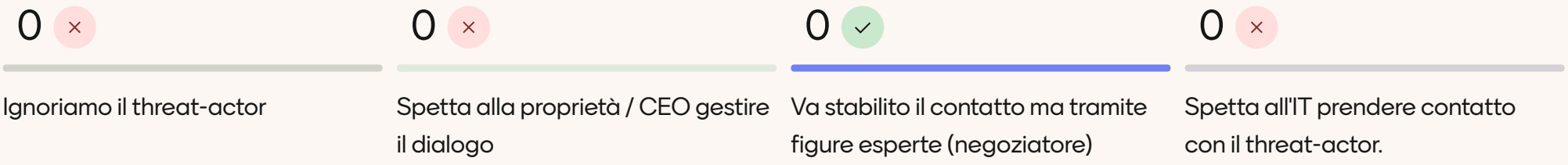
Mentimeter

Come ci comportiamo con il dialogo verso l'attaccante?

1. Nessuna comunicazione, meglio ignorare completamente l'attaccante
2. La responsabilità in merito alle scelte economiche sono sempre a discrezione della proprietà, è quindi la proprietà che devo avviare il dialogo
3. Il contatto va stabilito ed è necessario farlo tramite un esperto negoziatore
4. L'IT (interno o esterno) è l'unica figura di riferimento tecnico che può prendere contatto con l'attaccante

Mentimeter

Come ci comportiamo con il dialogo verso l'attaccante?



Decision Point: comunicazione e notifica dell’incidente

Durante le operazioni il team IT riesce a contenere con successo il ransomware, nessun dato viene cifrato e l'infezione contenuta ed eradicata in meno di 20 ore.

L'attaccante è riuscito a trafugare alcuni documenti dal fileserver contenenti dati personali dei dipendenti. Apparentemente nessun dato dei clienti è stato manomesso.

L'impatto sui servizi è stato gestito ed i rallentamenti operativi non hanno generato sospetti nei clienti.

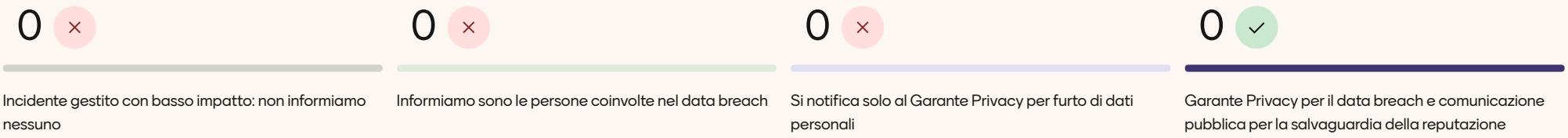
Mentimeter

Che tipo di comunicazione dobbiamo prevedere?

1. Se l'incidente è stato effettivamente gestito e gli impatti sono stati "assorbiti" non è necessario comunicare ai clienti l'accaduto.
2. È necessario informare solo le persone e/o le aziende interessate dal data breach.
3. L'incidente è stato gestito entro le 24h e l'operatività ha avuto poco impatto, ma alcuni dati personali sono stati sottratti. È necessario avvisare solo il Garante Privacy.
4. L'impatto sui dati personali impone la notifica al Garante Privacy. È comunque opportuna una comunicazione pubblica o ai clienti per informarli su come è stato gestito l'incidente.

Mentimeter

Che tipo di notifiche e/o comunicazioni dobbiamo prevedere?



Incidente gestito con basso impatto: non informiamo nessuno

Informiamo sono le persone coinvolte nel data breach

Si notifica solo al Garante Privacy per furto di dati personali

Garante Privacy per il data breach e comunicazione pubblica per la salvaguardia della reputazione