# Cyberattacco – che fare?
# Lista di controllo per CISO nel caso di un cyberattacco

## Misure tecniche

> Si accerti che gli orari di sistema dei Suoi segmenti di rete siano sincronizzati per permettere delle facili comparazioni e analisi di protocolli variegati su una base temporale che sia la medesima per tutti i segmenti della rete utilizzati.
> Se si verifica un evento, la realizzazione di immagini digitali, la copiatura di un gran numero di protocolli ecc. richiedono subito una grande capacità di memoria (esempio: memoria esterna) che dovrebbe già essere a disposizione.
> Spesso si archiviano dati secondo determinati periodi di tempo. È raccomandabile che i responsabili per il primo intervento sappiano quali archivi esistano, come possano essere utilizzati e in quali strutture vengano archiviati i dati.

## Misure organizzative

> La gestione di possibili eventi ha da essere preparata preventivamente in base a procedure, responsabilità e strategie comunicative (realizzate in collaborazione con l'ufficio comunicazione aziendale).
> La comunicazione interna ed esterna deve essere regolata (assistita dall'ufficio comunicazione). Informi la Sua squadra tecnica quanto apertamente possibile in modo da reagire agli eventi tempestivamente ed efficacemente. Vanno inoltre evitati danni collaterali indesiderati.
> È raccomandabile tenere un inventario attualizzato e completo di tutti i sistemi, software e reti. Questo inventario deve essere accessibile a tutti gli interessati.
> Stabilisca un collegamento diretto fra reazione a eventi, trattamento dei lati deboli e risk manager in modo che tutti i rischi siano noti e gestibili.
> È importante conoscere i processi interni principali e possedere un piano di continuazione dell'attività operativa in caso di crisi.

## Lato server e client

Livello sistema:

> È raccomandabile usare sistemi dedicati per la gestione di elementi infrastrutturali. Per amministratori inoltre va utilizzata un'autentificazione bifattoriale.
> Definisca delle regole di riconoscimento per i tool ausiliari degli aggressori come psexec o rexec.
> È consigliabile sorvegliare l'esecuzione di file binari (binaries) attraverso l'interfaccia WMI.
> Tool di controllo dell'integrità Le permettono di riconoscere mutazioni non autorizzate dei file di sistema. Essi danno pure una mano per valutare le conseguenze dopo un evento.
> Prepari le possibilità di controllo e analisi della Sua memoria di sistema. Ciò accresce la Sua possibilità di riconoscere rapidamente le minacce complesse e di reagirvi di conseguenza.

Virtualizzazione:

> Acquisisca di una certa conoscenza di elementi forensi. Ciò L'aiuterebbe a riconoscere se mai fosse avvenuta una fuga di VM.
> L'allestimento di funzioni sniffing in rete La può assistere nella sorveglianza dello scambio dati fra VM.

Active Directory:
> Abbia una comprensione ben chiara per i rapporti di fiducia fra diversi AdForests.
> Esegua un controllo preciso sui protocolli AD in merito a grossi e insoliti rilevamenti di dati che non si aspetterebbe di trovare.
> Tenga pronti piani d'intervento comprensivi di un Active Directory completamente compromesso per il caso di emergenza.

Rete:
> Utilizzi un'interfaccia centrale e ben sorvegliata da cui ogni pacchetto dati diretto a internet debba per forza passare. La stessa misura si può prendere per lo scambio dati in arrivo che si divide in diverse zone di rete. Può valutare eventualmente anche l'allestimento di settori centrali di prelievo dati con Load Balancer, Web Application Firewall e portali di autentificazione, tramite i quali si lascia sorvegliare in modo centralizzato lo scambio dati in entrata.
> Osservi attentamente l'inoltro tramite router dalla rete interna verso settori di rete esposti come ad esempio una DMZ. Questo scambio passa anch'esso l'interfaccia centrale e ben sorvegliata di cui sopra? Se non fosse il caso, piazzi dei sensori che controllino pure questo flusso.
> Ogni accesso a internet dovrebbe passare per un proxy che protocolli tutte le informazioni della testata inclusi i cookie.
> Raccolga i dati netflow non soltanto fra le zone di rete ma anche all'interno di esse.
> Oltre alle soluzioni in commercio utilizzi anche un classico sistema IDS basato su segnature quale Snort o Suricata. Questo Le dà la possibilità, in caso di un'aggressione, di applicare rapidamente regole di riconoscimento fatte in casa.
> Utilizzi Passive DNS per far passare tutti i rilevamenti di domain attraverso internet e trovarli rapidamente ed efficacemente.

Log file:
> Salvi i file protocollo per quanto possibile a lunga scadenza. Si raccomandano almeno due anni, particolarmente per sistemi importanti come domain controller e gateway.
> I file protocollo sono da salvare centralmente. È raccomandabile avere un concetto di gestione dei protocolli che copra tutte le zone rete e permetta indicizzazione, ricerca e archiviazione di tutti i file protocollo.
> È inoltre indicata l'implementazione di un'analisi protocolli continuata che permetta un confronto automatico dei detti file protocollo con IOC noti.
> La gestione dei protocolli è un processo continuato. Lei deve disporre di risorse sufficienti per aggiungere continuamente nuove fonti al Suo sistema poiché cambia costantemente anche il Suo paesaggio IT.
> Adatti le impostazioni log alle Sue necessità. La verbalizzazione dell'agente utenza, ad esempio, non è possibilmente l'impostazione standard. Si raccomanda in questo caso di cambiarla urgentemente.
> Collaboratori esperti non dovrebbero limitarsi ad analizzare i file protocollo prelaborati, ma esaminare anche i protocolli grezzi in merito a irregolarità. A questo scopo occorre preventivare sufficienti risorse temporali e personali.

In collaborazione con MELANI e Swiss Cyber Experts