Cosa fare in caso di ciberattacchi?
Lista di controllo per i CISO

Misure tecniche

> Assicuratevi che l'ora dei segmenti di rete impostata dal sistema sia sincronizzata in modo da poter comparare e analizzare vari protocolli in base agli stessi orari.
> In caso di incidente, misure quali la creazione di immagini digitali o la copia di molti protocolli richiedono rapidamente una grande quantità di spazio di archiviazione che deve già essere disponibile (ad es. su dispositivi di archiviazione esterni).
> Spesso i dati vengono archiviati per un lasso di tempo definito. È opportuno che i responsabili che devono intervenire per primi sappiano quali archivi esistono, come sono strutturati e come accedervi.

Misure organizzative

> La gestione degli incidenti deve essere preparata in anticipo definendo procedure, responsabilità e strategie di comunicazione sulla base della comunicazione aziendale.
> La comunicazione interna ed esterna deve essere regolata in base alla comunicazione aziendale. Informate il team tecnico in modo chiaro affinché possa reagire in modo puntuale ed efficace in caso di incidente. Cercate inoltre di evitare danni collaterali indesiderati.
> Utilizzate una versione aggiornata e completa di tutti i sistemi, i programmi e le reti. Tale inventario deve essere direttamente accessibile da tutte le parti interessate.
> Stabilite un collegamento diretto tra reazione agli incidenti, gestione dei punti deboli e gestori del rischio al fine di garantire che tutti i rischi siano noti e vengano gestiti.
> È essenziale conoscere i principali processi interni e avere un piano per proseguire l'attività operativa in caso di crisi.

Lato server e lato client

A livello di sistema

> Usate sistemi dedicati per l'amministrazione degli elementi dell'infrastruttura. Inoltre, per gli amministratori si dovrebbe utilizzare un'autenticazione a due fattori.
> Definite regole per riconoscere precocemente gli strumenti di cui si servono gli hacker (ad es. psexec o rexec).
> Monitorate attentamente l'esecuzione di file binari sull'interfaccia WMI.
> Adoperate strumenti di verifica dell'integrità che consentono di riconoscere modifiche non autorizzate nei documenti di sistema e possono essere utili per stimare gli effetti di un incidente.
> Abbiate già pronte le risorse per monitorare e analizzare la memoria di sistema. In questo modo aumentate le possibilità di riconoscere rapidamente minacce complesse e diminuite i tempi di reazione.

Virtualizzazione

- Acquisire buone conoscenze forensi vi aiuterà a capire se può essersi verificata una sospensione della macchina virtuale. La preparazione di funzioni per lo sniffing di rete può aiutarvi a sorvegliare il traffico dati tra macchine virtuali.

Active Directory (AD)

- Abbiate un'idea chiara delle relazioni di trust tra le varie foreste dell'AD.
- Monitorate attentamente i protocolli dell'AD in caso di richieste ("queries") insolite e voluminose inattese.
- Preparate dei piani di misure da attuare in caso di emergenza che contemplino anche la totale compromissione dell'architettura dell'AD.

Rete

- Utilizzate un'interfaccia centrale e ben sorvegliata attraverso cui filtrare ogni pacchetto in direzione Internet. Può essere applicato lo stesso principio per il traffico di dati in entrata distribuito su varie zone della rete. Per sorvegliare in modo centralizzato il traffico di dati in entrata, potete creare zone d'accesso centrali con bilanciatori di carico, firewall per applicazioni web e gateway di autenticazione.
- Esaminate attentamente i percorsi di routing dalla rete interna ai settori di rete esposti (ad es. una DMZ "demilitarized zone"). Anche questo traffico passa sull'interfaccia centrale e ben sorvegliata citata? In caso negativo, impostate dei sensori che monitorino anche questo traffico dati.
- Ogni accesso a Internet deve avvenire tramite un proxy che protocolla tutte le informazioni contenute nell'header, inclusi i cookie.
- Raccogliete i dati NetFlow non solo tra le varie reti, ma anche all'interno di esse.
- Oltre a soluzioni commerciali, utilizzate un IDS classico come Snort o Suricata. In caso di intrusioni, questo vi consente di mettere in atto regole di riconoscimento personalizzate velocemente.
- Impiegate un DNS passivo affinché tutte le query di dominio passino tramite Internet e possano essere trovate in modo veloce ed efficiente.

File di log

- Tenete i log il più a lungo possibile. Si consiglia di conservarli per almeno due anni in particolare per sistemi importanti quali domain controller e gateway.
- I file di log devono essere raccolti in modo centralizzato. Raccomandiamo un piano di gestione del protocollo che comprenda tutti i tipi di rete e consenta l'indicizzazione, la ricerca e l'archiviazione di tutti i file di log.
- Inoltre, consigliamo di implementare una continua analisi del protocollo che consenta un confronto automatizzato di questi file di log con IOC conosciuti.
- La gestione del log è un processo costante. Dovete disporre di abbastanza risorse per aggiungere sempre nuove fonti al vostro sistema in quanto anche il vostro ambiente informatico cambia costantemente.
- Adattate le impostazioni di log alle vostre necessità. Ad esempio, la registrazione dell'agente utente probabilmente non è predefinita ma fortemente consigliata.
- I collaboratori più esperti dovrebbero analizzare i file di log pre-processati e verificare la presenza di irregolarità in protlogocolli abbozzati. A tal fine, devono essere pianificate abbastanza risorse in termini di tempo e personale.