Incident Analyse du rapport

Résumé	Notre réseau interne a été pertubé pendant deux heures suite à une attaque par déni de service distribué (DDoS) .cette attaque a été rendue possible à cause d'un pare-feu mal configuré . L'équipe de gestion des incidents a réagi en bloquant les paquets ICMP entrants, en arrêtant tous les services réseau non critiques hors ligne et en rétablissant les services réseau critiques. Une enquête interne a permit de retracer l'origine de l'attaque et de mettre en oeuvre de nouvelles mesures de sécurité
Identifier	Notre équipe a audité les systèmes, les appareils et les politiques d'accès impliqués dans l'attaque afin d'identifier les failles de sécurité.Nous avons découvert qu'un acteur malveillant avait envoyé un flot de pings ICMP dans le réseau de l'entreprise par l'intermédiaire d'un pare-feu non configuré. Cette vulnérabilité a permis à l'attaquant malveillant de submerger le réseau de l'entreprise par le biais d'une attaque par déni de service distribué (DDoS) rendant indisponible le service réseau . Il est à noter également une absence de service de surveillance , de limitation du nombre de paquets ICMP.
Protéger	L'équipe a mis en place de nouvelles politiques afin de protéger le réseau de l'organisation. Il s'agit de la filtration des ports qui consiste à bloquer les ports non utilisés et autoriser le trafic nécessaire . De plus nous allons mettre une politique en vue de configurer convenablement le pare-feu en vue de filtrer le trafic entrant et sortant en vue de protéger les serveurs de l'organisation et mettre à jour régulièrement les règles en fonction des expériences (bloqué un ip spécifique , bloquer un trafic entrant provenant d'un ip qui est déjà dans le

	réseau interne pour bloquer les usurpations d'identité), pour filtrer une partie du trafic ICMP en fonction de caractéristiques suspectes, mettre en place un reverse proxy pour protéger les serveurs .
Détecter	Pour protéger l'organisation contre les attaques par DoS ou DDoS des systèmes de détection d' intrusion (IDS) et des systèmes de protection des intrusions (IPS) seront installés pour surveiller tout le trafic pour détecter un trafic inhabituel , malveillant , alerter et bloquer ce trafic . Aussi des systèmes de gestion des événements (SIEM) seront installé qui utilisent des algorithmes pour centraliser les données sur un tableau de bord afin de permettre à l'équipe de vite détecter les menaces et de réagir efficacement .
Répondre	L'équipe a bloqué les paquets ICMP entrants, arrêté tous les services réseau non critiques hors ligne et rétablit les services réseau critiques..Nous avons dispensé une formation aux analyste afin sur la manière d'utiliser les SIEM et de configurer les pare-feu pour prévenir un tel incident..Nous avons informé la direction de cet événement, qui contactera nos clients par courrier pour les informer du rétablissement des services .. La direction devra également informer les forces de l'ordre et autres organismes, conformément à la législation locale. Nous avons documenté l'incident et avons initiés des test d'intrusions pour déterminer de potentielles failles de sécurités
Récupérer	L'équipe a remis le réseau en marche et restaurer les données compromises par l'incident grâce aux sauvegardes pour permettre aux utilisateurs de pouvoir profiter de nos services . Aussi nous avons mis à jour les playbook pour mieux se préparer . À l'avenir, les attaques par saturation ICMP externes pourront être bloquées au niveau du pare-feu. Ensuite, tous les services réseau non critiques devront être arrêtés afin de réduire le trafic réseau interne. Les services réseau critiques devront ensuite être restaurés en premier. Enfin, une fois le délai d'expiration du flot de paquets ICMP écoulé, tous les systèmes et services réseau non critiques pourront être remis en ligne.

Réflexions/Notes :