Cyberattaque – que faire?
Aide-mémoire à l'intention des CISO

Mesures techniques

> Assurez-vous que l'horloge de vos sous-réseaux est synchronisée, afin de simplifier l'ajustement des différents journaux sur la même base temporelle et leur analyse.
> En cas d'incident, réaliser des images numériques et copier un grand nombre de journaux, etc. exige très vite un important espace de stockage (p.ex. stockage externe), qui devrait déjà être à disposition.
> Les données sont souvent archivées durant un certain temps. Pour une assistance immédiate, il est souhaitable que les responsables sachent quelles archives existent, comment ils peuvent y accéder et comment les données y sont structurées.

Mesures organisationnelles

> Il faut prévoir à l'avance la manière d'aborder les incidents en définissant clairement une procédure, les responsabilités et des stratégies communicationnelles (élaborées avec le service compétent de l'entreprise).
> La communication interne et externe doit être réglée (avec l'aide du service compétent de l'entreprise). Informez votre équipe technique le plus ouvertement possible afin de réagir aux incidents rapidement et efficacement. Il s'agit en outre d'éviter des dommages collatéraux indésirables.
> Il est recommandé de procéder à l'inventaire complet et à jour de tous les systèmes, logiciels et réseaux. Un tel inventaire doit être directement accessible à toutes les personnes impliquées.
> Établissez un lien direct entre réaction à un incident, gestion des vulnérabilités et gestionnaires des risques, afin de garantir que tous les risques sont connus et traités.
> Il est essentiel de connaître les processus internes les plus importants et d'avoir un plan pour maintenir les affaires opérationnelles en cas de crise.

Côté serveur et côté client

Au niveau des systèmes:
> Il est recommandé d'employer des systèmes dédiés à la gestion des éléments infrastructurels. De plus, les administrateurs devraient utiliser une authentification à deux facteurs.
> Définissez des règles pour détecter si des adjuvants de pirates, tels que psexec ou rexec, sont utilisés.
> Il est recommandé de surveiller soigneusement l'exécution des fichiers binaires (binaries) via l'interface WMI.
> Aidé(e) d'instruments de contrôle d'intégrité, vous pouvez identifier des modifications non autorisées des fichiers système. De plus, ces instruments sont utiles pour évaluer les répercussions d'un incident.
> Prévoyez des moyens de surveiller et d'analyser votre mémoire système. Vous augmentez ainsi vos chances de reconnaître rapidement des menaces complexes et d'y réagir.

Virtualisation:
> Acquérez un certain savoir forensique. Cela vous aidera à constater si un incident aurait pu se produire dans une VM (virtual machine).
> Prévoir des fonctions de reniflage (sniffing) du réseau peut vous aider à surveiller le trafic des données entre VM.

Active Directory:
> Ayez une compréhension claire des relations d'approbation entre les différentes forêts de l'AD (AdForests).
> Procédez à une surveillance précise des protocoles AD pour toute demande – inhabituelle ou d'une grande ampleur – que vous n'attendriez pas.
> Planifiez des mesures pour le pire, soit où Active Directory est complètement compromis.

Réseau:
> Utilisez une interface centrale et bien surveillée, que chaque paquet vers internet doit passer. On peut procéder de la même manière pour les données entrantes, qui seront réparties sur les différentes zones du réseau. Vous pouvez envisager l'aménagement de zones centrales d'accès à l'aide de répartisseurs de charge (load balancer), de logiciels pare-feu pour applications web et de gateways (passerelles) d'authentification, qui vous permettent de surveiller le trafic entrant.
> Examinez soigneusement les voies de routage du réseau interne vers ses domaines exposés, comme une DMZ (demilitarized zone). Ce trafic passe-t-il par l'interface (centrale et bien surveillée) susmentionnée? Dans la négative, placez des capteurs surveillant également ce trafic.
> Chaque accès à internet devrait passer par un proxy consignant toutes les informations d'entête, cookies inclus.
> Rassemblez les données Netflow, non seulement entre les zones du réseau, mais également à l'intérieur de celles-ci.
> Outre des solutions commerciales, utilisez un système classique de détection d'intrusion (IDS) basé sur des signatures, tels que Snort ou Suricata. Il vous donne la possibilité, en cas d'attaque, d'appliquer rapidement des règles de détection manuelles.
> Utilisez un DNS passif, afin que toutes les requêtes DNS passent par internet et soient ainsi rapidement et efficacement repérables.

Fichiers journaux:
> Enregistrez les fichiers journaux le plus longtemps possible. Au moins deux ans, surtout pour des systèmes importants tels que le contrôleur de domaine et les gateways.
> Les fichiers journaux doivent être centralisés. Il est recommandé d'avoir une stratégie pour planifier la gestion des journaux, recouvrant toutes les zones du réseau et rendant possible l'indexation, la recherche et l'archivage de l'ensemble des fichiers journaux.
> Il est en outre indiqué de mettre en place une analyse permanente des journaux, permettant leur ajustement automatique avec les indicateurs de compromission (IOC).
> La gestion des journaux est un processus permanent. Vous devez disposer de suffisamment de ressources pour ajouter régulièrement de nouvelles sources à votre système, car votre paysage informatique ne cesse de changer.
> Adaptez les paramètres de vos journaux à vos besoins. Par exemple, consigner les agents utilisateurs ne fait probablement pas partie de vos paramètres usuels, mais c'est vivement recommandé.
> Un personnel expérimenté devrait non seulement analyser les fichiers journaux prétraités, mais également vérifier d'éventuelles irrégularités dans les journaux bruts. À cet effet, il s'agirait de prévoir suffisamment de temps et de ressources humaines.

En collaboration avec MELANI et Swiss Cyber Experts