DDoS: attaque par déni de service (distribuée) – que faire?
Aide-mémoire à l'intention des techniciens

Processus généraux complémentaires

Pour toutes les mesures techniques décrites ci-après, vous devriez, en tant qu'entreprise attaquée, ne pas perdre de vue que les responsables commerciaux et de la clientèle doivent le cas échéant être informés de manière à pouvoir eux-mêmes informer. Afin de vous décharger, il est recommandé d'intégrer le service de communication de l'entreprise – il peut également identifier des intervenants proches et proposer un ordre de priorité.

1. Prendre des mesures correctives

> Contactez votre fournisseur d'accès internet pour stopper l'attaque.
> Vous pouvez éventuellement prendre vous-mêmes des mesures correctives en bloquant les adresses IP à l'aide du pare-feu (GEO-blocking) ou en adaptant le routage.

2. Informer la police cantonale ainsi que MELANI et définir avec eux la suite de la procédure

> Nommez votre fournisseur d'accès internet ainsi que les adresses expéditrices et destinataires de l'attaque, ce qui permet aux autorités de poursuite pénale de mener les premières investigations.

3. Sauvegarder les données utiles

> L'attaque terminée, sauvegardez les journaux utiles, notamment celui du pare-feu, et transmettez-les aux autorités de poursuite pénale comme annexe à un courriel.
> Si les pirates ont envoyé une lettre de chantage par courriel, celle-ci peut être comprimée en fichier ZIP que vous pouvez transmettre aux autorités de poursuite pénale par courriel.

4. Contrôler si votre réseau présente des anomalies

Les attaques DDoS sont souvent utilisées pour camoufler d'autres attaques telles qu'incorporer des logiciels malveillants ou voler des données. C'est pourquoi après une attaque DDoS vous devriez contrôler que votre réseau ne présente pas d'anomalies.

En collaboration avec MELANI et Swiss Cyber Experts