Logiciels malveillants – 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. Contacter la police cantonale ainsi que MELANI pour définir avec eux la suite de la procédure

> Informez votre corps de police cantonal et MELANI, et discutez avec eux pour savoir s'il faut d'abord observer le logiciel malveillant ou prendre des mesures correctives. La suite de la procédure dépend essentiellement (mais pas seulement) de la situation: la victime est-elle en contact avec les pirates? Ceux-ci attendent-ils une réponse de la victime? La police vous conseille, notamment sur la manière de communiquer avec les pirates et sur le comportement à adopter face à eux.
> Discutez avec la police pour savoir s'il serait judicieux qu'elle intervienne immédiatement pour vous seconder.

2. Prendre des mesures correctives sur le réseau de l'entreprise

> Détectez l'URL et les adresses IP pirates ainsi que l'étendue de la contamination.
  > Les liens pirates (URL et adresses IP) doivent être détectés et immédiatement bloqués sur le serveur proxy interne, ou sur le pare-feu, afin d'empêcher une communication involontaire avec le serveur pirate.
  > Lors d'une contamination par courriel, certains liens pirates (URL et adresses IP) sont parfois relativement faciles à extraire, soit directement du courriel (hyperlien), soit d'une annexe spécifique.
  > L'étendue de la contamination peut être déterminée à l'aide des journaux des serveurs courriel et proxy et du pare-feu et, le cas échéant, d'autres logiciels de sécurité du réseau de l'entreprise attaquée. L'URL et les adresses IP pirates peuvent ainsi être détectées.
> Bloquez l'URL et les adresses IP pirates sur le serveur proxy ou sur le pare-feu.
> Séparez si possible immédiatement les appareils et ordinateurs infectés du réseau. Cependant: les appareils et ordinateurs infectés ne devraient pas être désactivés par l'entreprise victime, mais au contraire gardés enclenchés, tant que le maliciel n'a pas été analysé par les autorités cantonales de poursuite pénale et MELANI ou par l'entreprise victime.

3. Sauvegarder les données utiles

> Sauvegardez les fichiers journaux ainsi que les données utiles énumérées ci-après, et transmettez-les aux autorités de poursuite pénale pour leur enquête sur les pirates:
  > Les journaux du serveur proxy ou du pare-feu: l'URL et les adresses IP pirates peuvent être transmises aux autorités de poursuite pénale sous forme d'annexe à un courriel.
  > Si le maliciel est parvenu à l'entreprise infectée par courriel, celui-ci et son annexe peuvent être comprimés en fichier ZIP que vous transmettez ensuite aux autorités de poursuite pénale par courriel.
  > Si la contamination a eu lieu par téléchargement furtif (drive-by download), le logiciel malveillant doit être si possible isolé par l'entreprise infectée, comprimé en fichier ZIP et transmis ensuite aux autorités de poursuite pénale par courriel.
  > Si la contamination a eu lieu par une clé USB, celle-ci doit être mise à disposition des autorités de poursuite pénale (par lettre recommandée ou directement de main à main).
  > Si l'entreprise attaquée a procédé à des analyses du maliciel, celles-ci peuvent être transmises aux autorités de poursuite pénale comme annexe à un courriel.

En collaboration avec MELANI et Swiss Cyber Experts