*Voir aussi la page 47*
*du document VIGIPIRATE «Faire face ensemble»*
*SGDSN - 01/12/2016*

# SÉCURITÉ DES INFORMATIONS

**Les recommandations figurant dans cette fiche sont à adapter en fonction du lieu, de la nature, de l'importance et de la durée de l'événement auquel elles peuvent s'appliquer.**

La perte de confidentialité, d'intégrité et, de disponibilité des informations en version papier ou sous format électronique peut représenter un problème critique pour les organisations. Nombre d'entre elles s'appuient sur leurs systèmes d'information pour exercer leur activité, ainsi que pour gérer la sécurité et les systèmes d'ingénierie.

Vos informations confidentielles peuvent intéresser des entreprises concurrentes, des criminels, des services de renseignement étrangers, ou des terroristes. Ceux-ci peuvent essayer d'y accéder en s'introduisant dans vos systèmes informatiques, en s'emparant des données que vous avez jetées, ou en infiltrant votre organisation. Une telle attaque pourrait perturber votre activité et nuire à votre réputation.

Lorsque vous considérez ce type d'attaques, il vous faut examiner les installations et les processus du site de votre manifestation et de tout autre lieu à partir duquel vous opérez. De nombreux organisateurs de grandes manifestations souscrivent à des systèmes de sécurité et de contrôle d'accès. Assurez-vous d'établir clairement qui est responsable de la gestion et de la sécurité des données.

**Avant de prendre des mesures de protection spécifiques, vous devez :**

- **évaluer la menace et vos vulnérabilités ;**
- vous demander dans quelle mesure vos informations courent un risque, qui pourrait s'y intéresser, comment ces personnes pourraient les obtenir, et en quoi leur perte ou leur vol vous seraient préjudiciables ;
- prendre en considération les bonnes pratiques actuelles de sécurité des informations visant à contrer les cyberattaques et à protéger les documents.

**Les cyberattaques** menées contre les systèmes peuvent :

- permettre à l'assaillant de dérober, de modifier ou de supprimer des informations sensibles ;
- permettre à l'assaillant d'accéder à votre système informatique et de faire tout ce que le propriétaire du système est capable de faire ; notamment, modifier vos données, éventuellement de façon subtile pour que cela ne soit pas immédiatement visible, installer un logiciel malveillant (virus ou ver) susceptible d'endommager votre système, ou encore installer des dispositifs matériels ou logiciels conçus pour transmettre les informations à l'assaillant ; ce genre d'attaques contre des systèmes connectés à Internet est extrêmement fréquent ;
- rendre vos systèmes inutilisables grâce à des attaques « par déni de service » ; ces dernières, de plus en plus courantes, sont relativement simples à lancer et il est difficile de s'en protéger.

**Les cyberattaques sont beaucoup plus aisées lorsque les systèmes informatiques sont directement ou indirectement connectés à des réseaux publics, tels qu'Internet.**

Les méthodes traditionnellement utilisées pour une cyberattaque sont les suivantes :

### LOGICIELS MALVEILLANTS

Les techniques et les effets des logiciels malveillants (virus, vers, chevaux de Troie, etc.) sont aussi variables que bien connus. Les principaux moyens de propagation d'un virus sont :

1. l'ouverture ou l'exécution d'une pièce jointe reçue dans un e-mail ;
2. les clics sur un lien obtenu sur un site Internet ;
3. une navigation inappropriée sur Internet, qui conduit souvent à un site distribuant des logiciels malveillants ;
4. l'autorisation accordée au personnel de connecter des périphériques de stockage amovibles (clés USB, disques, CD, DVD) aux machines de l'entreprise ;
5. l'autorisation accordée à votre personnel de connecter des lecteurs multimédias et des téléphones portables aux machines de l'entreprise.

### DÉNI DE SERVICE (DOS)

Ces attaques visent à submerger un système en l'inondant de données indésirables. Certaines attaques DoS sont distribuées, ce qui signifie que de grandes quantités de machines « innocentes » non sécurisées (appelées « zombies ») sont enrôlées de force pour organiser des attaques.

### PIRATAGE INFORMATIQUE

Il s'agit d'une tentative d'accès non autorisé, presque toujours motivée par des intentions malveillantes ou criminelles.

### MODIFICATION MALVEILLANTE DU MATÉRIEL

Le matériel informatique peut être modifié de manière à organiser ou à autoriser une attaque électronique. Cela se produit généralement au stade de la fabrication ou de la livraison préalablement à l'installation, même si cela peut également être réalisé au cours d'interventions de maintenance ou par des personnes de l'intérieur. Le but de ces modifications est de permettre le lancement d'une attaque ultérieure, éventuellement déclenchée à distance.

## Mesures à prendre

- Achetez vos systèmes informatiques auprès de fabricants et de fournisseurs réputés.
- Assurez-vous que vos logiciels sont régulièrement mis à jour. Les éditeurs corrigent continuellement les failles de sécurité de leurs logiciels. Ces correctifs sont disponibles sur leur site Internet ; envisagez de vérifier quotidiennement les correctifs et les mises à jour.

- Assurez-vous que tous les ordinateurs connectés à Internet sont équipés d'un logiciel antivirus et protégés par un pare-feu.

- Sauvegardez vos informations, en conservant de préférence une copie sécurisée dans un autre endroit.

- Évaluez la fiabilité des personnes chargées de l'entretien, de l'exploitation et de la surveillance de vos systèmes.

- Envisagez d'utiliser des programmes de chiffrement pour les documents que vous souhaitez protéger, en particulier s'ils sont transportés hors du site ; sollicitez toutefois au préalable l'avis d'un spécialiste.

- Prenez des précautions élémentaires pour empêcher vos logiciels ou autres informations sensibles de tomber entre de mauvaises mains. Sensibilisez vos employés à la sécurité, en les formant à ne pas laisser traîner de documents sensibles et à appliquer la politique du bureau bien rangé (c.-à-d. que les bureaux doivent être dégagés de tout matériel de travail à l'issue de chaque séance de travail).

- Assurez-vous que vos employés savent que les utilisateurs peuvent être incités à révéler des informations susceptibles de servir à accéder à un système, telles que des identifiants ou des mots de passe.

- Investissez dans des classeurs sécurisés, installez des portes verrouillables, et veillez à détruire les documents sensibles de façon appropriée.

- Dans la mesure du possible, verrouillez ou désactivez les lecteurs de disques, les ports USB et les connexions sans fil.

- Assurez-vous que l'accès aux ordinateurs est protégé par des mots de passe individuels contrôlés de manière sécurisée, ou par la biométrie et des mots de passe.

- Mettez en œuvre à l'intention du personnel une politique d'utilisation acceptable concernant la navigation sur Internet, la messagerie électronique, les salons de discussion, les sites de réseaux sociaux, les sites marchands et les sites de téléchargement de jeux et de musique.

## Exemples de cyberattaques

- Un ancien administrateur systèmes a pu intercepter des e-mails échangés entre des dirigeants de l'entreprise parce que le prestataire de services de sécurité externalisés avait omis de sécuriser le système.

- Un ancien employé a pu se connecter à distance à un système et a apporté des modifications à un magazine numérique spécialisé, entraînant une perte de confiance des clients et des actionnaires.

## Élimination des informations sensibles

Les sociétés et les particuliers doivent parfois éliminer des informations sensibles. Certains des documents couramment jetés par les entreprises peuvent servir à des groupes très divers : concurrents, usurpateurs d'identité, criminels, terroristes, etc.

Plusieurs types d'informations sont concernés : noms et adresses des employés, numéros de téléphone, informations sur les produits, données client, informations relevant de la loi sur la protection des données, spécifications techniques, ou encore données chimiques et biologiques. On sait que les groupes terroristes ont manifesté de l'intérêt dans les deux derniers domaines.

## Les principaux moyens de destruction des déchets sensibles sont les suivants :

### LE DÉCHIQUETAGE

Il n'existe actuellement aucune norme industrielle pour le déchiquetage des documents au Royaume-Uni, mais l'Allemagne en a établies depuis quelque temps déjà (normes DIN). La plupart des pays de l'UE ont adopté la norme allemande.
Les déchiqueteurs spécifiés dans la norme DIN 32757 - 1 de niveau 4 produisent une taille de bandes de 15 mm x 1,9 mm. Ils conviennent aux exigences d'un niveau de sécurité moyen à élevé.

## L'INCINÉRATION

L'incinération est probablement le moyen le plus efficace pour détruire les déchets sensibles, y compris les disques et autres types de supports magnétiques et optiques, à condition d'utiliser un incinérateur adéquat (renseignez-vous auprès des autorités locales). Les feux en plein air ne sont pas fiables, dans la mesure où les matériaux ne sont pas systématiquement détruits et où des papiers lisibles risquent d'être emportés par le courant d'air ascendant.

## LE DÉFIBRAGE

Cette opération, qui consiste à réduire les déchets à l'état fibreux, n'est efficace que pour le papier et le carton. Toutefois, certaines défibreuses se contentent de déchirer le papier en grands morceaux et de le transformer en papier mâché, duquel il est toujours possible d'extraire des informations. Cela représente un risque plus élevé qu'auparavant, les encres utilisées par les photocopieuses et les imprimantes laser modernes ne coulant pas lorsqu'elles sont mouillées.

D'autres méthodes existent pour l'effacement des supports numériques, telles que l'écrasement ou la démagnétisation.

**Avant d'investir dans du matériel de destruction des déchets, vous devez :**

- si vous avez recours à des contractants, vous assurer que leur matériel et leurs procédures sont conformes aux normes en vigueur ; déterminez qui supervise le processus, le type de matériel dont ces personnes disposent, et s'il y a deux conducteurs à bord des véhicules de collecte, de façon à ce que l'un d'eux reste auprès du véhicule pendant que l'autre procède à la collecte ; il est également souhaitable que le véhicule et sa base puissent communiquer ;

- vous assurer que le matériel est adapté à la tâche ; cela dépend des matériaux que vous désirez détruire, de leur niveau de confidentialité, et des quantités concernées ;

- vous assurer que vos procédures et votre personnel sont sûrs ; il ne sert pas à grand-chose d'investir dans du matériel coûteux si les personnes employées pour l'utiliser constituent elles-mêmes un risque pour la sécurité ;

- confier la responsabilité de la destruction des déchets sensibles à votre service de sécurité plutôt que d'en faire une tâche de gestion des installations.