Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

SECRÉTARIAT GÉNÉRAL

Paris, le 23 FEV. 2018

SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE
TELEDOC 722
120 RUE DE BERCY
75572 PARIS CEDEX 12

N°SHFDS/2018/02/6236

NOTE POUR
MESDAMES ET MESSIEURS LES DIRECTEURS, OFFICIERS,
DELEGUES ET RESPONSABLES DE SECURITE

Objet : Posture VIGIPIRATE « Printemps 2018 »

Annexes : 1. Fiche : Prévention et signalement des cas de radicalisation djihadiste.

2. Fiche : Recommandations pour la sécurisation des lieux de rassemblement ouverts au public.

3. Fiche : Sécurité du numérique – Sensibilisation des dirigeants.

La posture Vigipirate « Printemps 2018 » est active à compter du 1er mars 2018. Elle s'applique, sauf événement particulier, jusqu'au 13 juin 2018, veille du lancement de la coupe du monde de football qui se déroulera en Russie et du début des grandes manifestations estivales.

L'ensemble du territoire national est maintenu au niveau « sécurité renforcée - risque attentat ».

Dans un contexte de menace terroriste qui demeure à un niveau élevé, elle met l'accent sur :

- la sécurité des transports collectifs de personnes, plus particulièrement lors des vacances scolaires et universitaires et des périodes de ponts qui ponctueront le mois de mai 2018 ;
- la sécurité des lieux à forte fréquentation (espaces de commerces, sites touristiques) et des lieux de divertissement (stades, salles de concert, cinémas) ;
- la sécurité des bâtiments publics (services publics, locaux associatifs ou politiques, écoles et universités, etc.) et des établissements de santé, médico-sociaux et sociaux ;
- la vigilance autour des grandes célébrations religieuses de printemps ;
- la protection des systèmes d'information face au risque d'attaques cybernétiques.

Cette posture rappelle les consignes de vigilance destinées aux représentants de l'autorité publique (militaires, policiers, gendarmes, surveillants pénitenciers, etc.), régulièrement visés par des attaques au cours des derniers mois en France.

Après une description du contexte général et une évaluation de la menace, cette note de posture expose les objectifs de sécurité associés à la période couverte qui doivent être déclinés par les ministères. Des fiches de recommandations pratiques sont annexées et une version actualisée du tableau des mesures VIGIPIRATE est jointe à la présente note (cf. Annexe 2).

1. CONTEXTE GENERAL

La posture Vigipirate « Printemps 2018 » s'applique, sauf événement particulier, jusqu'au 13 juin 2018. Cette période est marquée par l'organisation de grands événements ou manifestations à caractère culturel, social, sportif ou religieux. Ces événements requièrent une mobilisation accrue des acteurs de la sécurité, qu'ils soient publics ou privés.

2. ADAPTATION DE LA POSTURE VIGIPIRATE « Printemps 2018 »

La posture Vigipirate « Printemps 2018 » est active à partir du 1er mars 2018 et s'applique, sauf événement particulier, jusqu'au 13 juin 2018. L'ensemble du territoire national est maintenu au niveau « sécurité renforcée - risque attentat ».

2.1. Sécurité des sites touristiques, des espaces culturels et des expositions à thème sensible

A l'approche de l'ouverture des premiers festivals de la saison 2018, les travaux et mesures destinés à rendre plus efficaces les interactions avec les forces de sécurité intérieures conservent toute leur pertinence.

La circulaire INTA1711331J du 20 avril 2017, relative au plan de relance du tourisme, instaure une convention de site permettant à la préfecture d'attribuer un label « sécuri-site » à un lieu touristique concerné, et s'inscrit dans cette logique[1]. Cette convention doit déterminer les mesures de sûreté les plus adaptées au site touristique.

De même, les procédures internes de confinement ou d'évacuation permettent une gestion rapide et efficace du public et des personnels situés dans l'enceinte d'un site ou d'un événement culturel face à une attaque directe, ou lors d'une attaque à proximité. Les sorties de spectacle ou de grand rassemblement public, font l'objet d'une attention particulière et doivent bénéficier d'un dispositif de sécurité jusqu'à la dispersion du public.

Plusieurs documents ont été élaborés pour soutenir les responsables de sites ou d'événements dans le domaine de la sûreté. Quatre guides peuvent être utilement consultés sur le site Internet du ministère de la culture http://www.culturecommunication.gouv.fr :

- « guide à destination des organisateurs de rassemblements et festivals culturels » ;
- « guide à destination des dirigeants de salles de spectacle, de cinémas ou de cirques » ;
- « guide à destination des dirigeants d'établissements culturels patrimoniaux (musées, monuments historiques, archives et bibliothèques) » ;
- « gérer la sûreté et la sécurité des événements et sites culturels ».

[1] En date du 9 janvier 2018, 559 labels « sécuri-site » ont d'ores et déjà été attribués et 148 sont en voie de l'être.

Une fiche de recommandations pour la sécurisation des lieux de rassemblement ouverts au public est annexée à cette note (cf. Annexe 2).

2.2. Sécurité des grands espaces de commerce, des lieux de loisirs et des sites touristiques

Les centres et enseignes commerciaux, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées. Les interconnexions en milieu clos dotées de commerces (métros, gares, etc.) constituent également un point de vigilance.

2.2.1. Mesures propres à la période concernée

Cette période de ponts appelle une vigilance accrue sur le secteur du tourisme et des parcs de loisirs. La sécurité est renforcée notamment autour des grands espaces de rassemblements ayant pour objet des activités commerciales ou artisanales ambulantes (salons, foires, etc.).

L'effort est porté sur la présence visible des forces de l'ordre ainsi que sur le déploiement, par les organisateurs de rassemblements et les responsables d'établissements recevant du public, de mesures de sécurité appropriées.

2.2.2. Mesures permanentes

La capacité à faire face à une attaque terroriste dans les espaces de commerce, culturels et de loisirs passe par le renforcement des échanges d'informations entre les services de l'Etat et les responsables de la sûreté des opérateurs privés et publics. Ce renforcement se traduit notamment par la mise en place ou l'adaptation de conventions locales de coopération de sécurité.

De façon plus générale, il revient aux autorités préfectorales d'évaluer le niveau de sécurité à atteindre pour les différentes activités qui ont lieu dans leur département. Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou dès lors qu'une manifestation ou un événement révèle une vulnérabilité particulière, ceux-ci sont communiqués aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif et de mettre en œuvre, le cas échéant, les moyens qu'ils jugent nécessaires.

Cette démarche s'inscrit dans la volonté de renforcer les liens et la coordination entre acteurs publics et privés, réaffirmée lors du dialogue national de sécurité sur les centres commerciaux du mois de décembre 2017.

2.2.3. Sensibilisation des personnels

La sensibilisation des personnels doit être assurée par les gestionnaires des centres et d'enseignes commerciaux, entre autres par la mise à disposition des guides pratiques réalisés conjointement par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et les ministères économiques et financiers, ainsi que par la diffusion de l'affiche et de la vidéo « Réagir en cas d'attaque terroriste ». Ces éléments peuvent être utilement consultés sur le site Internet des ministères économiques et financiers:

https://www.economie.gouv.fr/hfds/vigilance-attentat-bons-comportements

Les salariés doivent être informés sur la procédure de signalement des comportements suspects en vigueur dans leur établissement. Ils doivent être sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

Enfin, la connaissance du site par le personnel qui y travaille, l'organisation d'exercices collectifs et la formation aux gestes de premiers secours constituent des prérequis indispensables afin de réagir de manière efficace et coordonnée en cas d'attaque.

2.2.4. Dispositif de détection du passage à l'acte dans et aux abords des établissements ou des sites disposant d'agents privés de sécurité ou d'un système de vidéoprotection.

Les responsables de la sécurité du secteur marchand privilégient la surveillance dynamique des espaces, la détection des comportements suspects et le recours à la vidéoprotection.

La vidéoprotection de la voie publique peut être mise en œuvre, sur autorisation préfectorale, par les personnes morales pour la protection des abords immédiats de leurs bâtiments et installations, dans les lieux susceptibles d'être exposés à des actes de terrorisme (Cf. art. L. 223-1 du code de la sécurité intérieure).

2.3. Personnel en tenue

Les représentants de l'autorité publique, civils ou militaires, sont particulièrement visés. Il convient de sensibiliser ces agents en éveillant chez eux les bons réflexes en cas de situations inappropriées ou face à un individu au comportement menaçant.

2.4. Sensibilisation à la menace des attaques par véhicules-béliers

Les attaques par véhicules-béliers demeurent un mode d'action fréquemment utilisé par les organisations terroristes.

La vigilance pour faire face à cette menace concerne l'ensemble des acteurs, publics et privés, notamment ceux qui gèrent des parcs de véhicules (sociétés de location, sociétés de transports de voyageurs ou de marchandises, etc.). Les gestionnaires de parcs de véhicules sont ainsi appelés à signaler, sans délai, aux autorités, tout vol de véhicule ou comportement suspect.

Une fiche de recommandations sur ce sujet est disponible sur le site Internet du SGDSN :

http://www.sgdsn.gouv.fr/uploads/2017/07/fiche-recommandations-vehicules-beliers.pdf

Les préfets sensibilisent les collectivités territoriales et les opérateurs privés à renforcer les dispositifs de protection passive (plots, barrières, etc.) sur les lieux (terrasses de restaurant à proximité de la voie publique par exemple) et les artères les plus fréquentées, en s'appuyant notamment sur l'expertise des référents sûreté des directions départementales de sécurité publique et des groupements de gendarmerie départementale.

Dans le cadre de l'organisation d'événements festifs en plein air, il convient de choisir un lieu d'implantation qui présente le moins de vulnérabilités possibles. Les zones de stationnement des véhicules doivent être géographiquement isolées des zones d'évolution du public. Cette mesure de cloisonnement des espaces dédiés aux véhicules, d'une part, et aux piétons, d'autre part, contribue directement à la sécurisation du site.

2.5. Vigilance et mesures de prévention face au risque NRBC-E (nucléaire, radiologique, biologique, chimique, explosif).

Les derniers attentats, ou actes de malveillance, commis en Europe, ont démontré la capacité des criminels et terroristes à fabriquer des explosifs artisanaux ou des substances toxiques à partir de

produits chimiques d'usage courant. Les professionnels qui vendent ce type de produits ont l'obligation de signaler tout vol, disparition ou transaction suspecte au plateau d'investigation explosif et armes à feu (PIXAF) de la Gendarmerie nationale, point de contact national. Le PIXAF est joignable aux coordonnées ci-dessous :

pixaf@gendarmerie.interieur.gouv.fr – 01 78 47 34 29 (24h/24h)

En cas d'attaque NRBC-E, il est déterminant que les services intervenants puissent mettre en œuvre, sans délai, les moyens, procédures et protocoles afin de minimiser et atténuer les effets sur les personnes, les biens et l'environnement. Pour cela, il se révèle indispensable de :

- contrôler la diffusion et la connaissance des consignes NRBC-E auprès des agents qui auraient à les mettre en œuvre (fiches réflexes, instructions et circulaires) ;

- rappeler les consignes de protection et les conduites à tenir individuelles et collectives à mettre en œuvre en cas d'événement de nature NRBC-E.

2.6. Vigilance en cas de voyages à l'étranger ou d'expatriation

Il est recommandé aux Français souhaitant voyager ou séjourner à l'étranger de se connecter, avant leur départ, au site https://www.diplomatie.gouv.fr, afin de :

- consulter les fiches conseils aux voyageurs, y recueillir les numéros utiles et les conserver pendant toute la durée de leur séjour ;

- s'inscrire parallèlement sur l'application Ariane, quelle que soit leur destination, y compris à l'intérieur de l'Union européenne. Cette précaution permet :

    - de recevoir des recommandations de sécurité par courriels si la situation dans le pays le justifie ;

    - d'être contacté en cas de crise dans le pays de destination ;

    - de prévenir, en cas de besoin, la personne contact désignée.

Par ailleurs, les Français séjournant à l'étranger doivent s'enregistrer auprès des autorités consulaires afin d'être joignables en cas de crise et d'obtenir ainsi toutes les informations pratiques et instructions émanant de l'Ambassade de France.

3. SENSIBILISATION DU GRAND PUBLIC

3.1. Efforts de communication

Vous veillerez tout particulièrement à l'effectivité de la mise en place des logogrammes « Sécurité renforcée - risque attentat ». En effet, d'anciens logogrammes « Alerte attentat » sont encore affichés dans certains lieux publics et peuvent être source de confusion pour la population.

Les logogrammes peuvent être téléchargés sur le site du Gouvernement http://www.gouvernement.fr/vigipirate et du SGDSN http://www.sgdsn.gouv.fr/vigipirate.

Vous êtes par ailleurs invités à relayer le plus largement possible les outils de sensibilisation à la menace terroriste téléchargeables sur les deux sites cités supra.

3.2. *Sensibilisation des professionnels et du grand public aux bonnes pratiques*

Dans un souci de pédagogie et de large diffusion des bonnes pratiques face à la menace terroriste, cette posture comporte, en annexe, des fiches de sensibilisation à destination tant du grand public que des professionnels.

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public doit être renouvelée et renforcée. Cette communication peut se faire par le biais de l'affiche dédiée « Réagir en cas d'attaque terroriste », qui doit être imprimée sur un format adapté au lieu où elle est placée et visible du public (privilégier les entrées et sorties des établissements, les halls, ou salles d'attente, etc.).

L'ensemble de ces éléments, ainsi que d'autres documents utiles, sont consultables en ligne et téléchargeables depuis les sites suivants :

- http://www.sgdsn.gouv.fr/plan-vigipirate/
- http://www.gouvernement.fr/reagir-attaque-terroriste
- http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate

Enfin, la version publique du plan VIGIPIRATE « Faire face ensemble », également disponible en langue anglaise, peut y être téléchargée.

3.3. *Sensibilisation à la cybersécurité*

La protection du cyber espace doit également faire l'objet d'une information auprès des particuliers et des professionnels afin de les sensibiliser aux menaces dont il est l'objet.

Si la période considérée n'est pas marquée par des évènements pouvant générer un risque d'attaque informatique majeure, la cybermenace doit pourtant être considérée en tout temps avec le plus grand sérieux (ex : exploitations de vulnérabilités critiques de processeurs, attaques par rançongiciel et en déni de service, attaques ciblant des systèmes industriels, utilisations illégitime de ressources à des fins de minage de monnaies virtuelles, etc).

A des fins de pédagogie et de sensibilisation, une fiche « Sécurité du numérique – Sensibilisation des dirigeants » est anexée à la présente note (cf. Annexe 3).

Il vous est demandé de diffuser cette posture « Printemps – 2018 » à l'ensemble de vos services ou adhérents.

Le Haut fonctionnaire de défense et de sécurité adjoint

Christian DUFOUR

ANNEXES

Annexe 1 : « *Prévention et signalement des cas de radicalisation djihadiste* »

Diffusion sans restriction

Annexe 2 : « *Recommandations pour la sécurisation des lieux de rassemblement ouverts au public* »

Diffusion sans restriction

Annexe 3 : « *Sécurité du numérique – Sensibilisation des dirigeants* »

Diffusion sans restriction

Annexe 1 à la note SHFDS/2018/02/6236

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION DJIHADISTE

VIGIPIRATE

La radicalisation djihadiste se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. L'objectif du signalement au *centre national d'assistance et de prévention de la radicalisation* (CNAPR) est de protéger, non seulement ces personnes contre elles-mêmes en s'assurant qu'elles ne sont pas sur une voie qui conduit à commettre un acte criminel, mais également la population contre de possibles comportements violents.

1 Pourquoi signaler un cas de radicalisation ?

La radicalisation djihadiste conduit à participer à des actes terroristes dans le but revendiqué de tuer de nombreux citoyens français sans distinction, en raison uniquement de leurs valeurs et de leurs modes de vie.

On parle de **processus de radicalisation** progressif avec adhésion à une idéologie avec des composantes de violence et de rupture avec l'environnement habituel. Il peut être dangereux de sous-estimer la rapidité du passage aux paliers ultimes. **La radicalisation apparaît comme un phénomène profondément lié à l'exploitation de conflits d'identité, de frustrations ou de fragilités.** Certains groupes terroristes djihadistes cherchent notamment à enrôler des individus en perte de repères et vulnérables.

La force d'une idéologie et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leurs frustrations ou à un sentiment d'humiliation, à leurs difficultés et apporte des solutions.

Cette radicalisation est un phénomène complexe, protéiforme, amplifié par le développement d'internet et des réseaux sociaux. La propagande véhiculée touche des profils variés : délinquants, personnes vulnérables en quête d'identité, personnes ayant des troubles du comportement adaptatif, etc. La complexité du phénomène actuel porte sur l'identification du niveau de radicalisation et de ses conséquences : l'ensemble des pratiquants rigoristes d'une religion ne sont pas djihadistes mais tous les djihadistes sont radicalisés.

Difficile à repérer et à traiter, la radicalisation est donc un enjeu majeur de sécurité nationale et de survie pour notre société.

2 Identifier une situation de radicalisation

Appliquer strictement les préceptes d'une religion ne constitue pas un élément alarmant en soi. La pratique religieuse doit alerter l'entourage quand elle s'accompagne pour l'intéressé, d'une volonté de rupture avec sa propre personnalité antérieure et donc, avec son entourage proche et tout ce qui peut le ramener à sa vie d'avant.

Aussi, identifier un processus de radicalisation ne se fait pas sur la base d'un seul indice. Pris isolément, un des comportements listés ci-dessous ne signifie pas qu'il y a radicalisation. **C'est la combinaison de plusieurs signes qui donne une forme de cohérence et qui doit provoquer vigilance et alerte.**

Certaines combinaisons de comportements ou de traits de caractère sont des signaux tangibles de radicalisation et doivent attirer votre attention, que ce soit dans votre environnement quotidien ou sur votre lieu de travail.

COHÉRENCE → VIGILANCE → SIGNALEMENT

- Changements physiques, vestimentaires et alimentaires ;
- Propos asociaux ;
- Passage soudain à une pratique religieuse hyper ritualisée ;
- Rejet de l'autorité et de la vie en collectivité ;
- Rejet brutal des habitudes quotidiennes ;
- Repli sur soi ;
- Haine de soi, rejet de sa propre personne, déplacement de la haine de soi sur autrui ;
- Rejet de la société et de ses institutions (école, etc.) ;
- Éloignement de la famille et des proches ;
- Modification soudaine des centres d'intérêt ;
- Appréhension complotiste, antisémite, apocalyptique de la société.

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION DJIHADISTE

3 Initier une démarche de signalement

Il s'agit de prévenir, voire d'éviter, le basculement vers un comportement violent, en accompagnant les radicalisés et leurs familles par des professionnels, sous la supervision des cellules adaptées au sein des préfectures de leur département de résidence.

En signalant, on protège non seulement l'intéressé en lui évitant de participer à un acte criminel (pour le sortir au plus tôt du chemin mortifère sur lequel il s'est engagé peut-être sans en avoir conscience) **mais également la société contre de possibles préméditations de meurtres.** Prévenir c'est protéger. **Appeler ne représente pas une mesure punitive, il s'agit d'une mesure préventive.** Après un appel, les services de l'État s'appuient sur des spécialistes pour en évaluer le bien-fondé et le danger potentiel. Ils mettront en place un accompagnement adapté pour éviter que la situation ne se détériore.

Dans quels cas appeler ?

- Pour signaler une situation inquiétante, qui paraît menacer un proche ;
- Si vous avez un doute ou des questions sur une situation ;
- Pour obtenir des renseignements sur la conduite à tenir ;
- Pour être écouté(e), conseillé(e) dans vos démarches.

Appeler le numéro vert : 0 800 005 696
Les appels sont strictement confidentiels, votre identité ne sera pas dévoilée.
Remplir le formulaire en ligne : http://www.stop-djihadisme.gouv.fr

4 Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'État, la personne faisant l'objet du signalement ainsi que sa famille **bénéficieront d'un accompagnement spécialisé et adapté à leur situation.**

Votre identité ne sera pas dévoilée, les signalements sont strictement confidentiels. Même si vous n'êtes pas sûr d'avoir reconnu des combinaisons de signes de comportement suspect, **vous pouvez sauver des vies.** Il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de qualifier la situation de préoccupante ou non.

Signaler une situation ne vous sera jamais reproché. Faites le avant qu'il ne soit trop tard.

5 Signaler un contenu appelant à la haine ou faisant l'apologie du terrorisme sur Internet

Internet et les média sociaux favorisent la diffusion d'appels à la haine et de messages faisant l'apologie du terrorisme.

La liberté d'expression est un élément fondamental de notre société. Elle ne constitue toutefois pas un « passe-droit » pour tout rédiger et publier n'importe quoi sur Internet. En 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation, également appelée PHAROS, a été mise en place par l'Etat pour signaler les comportements illicites sur internet.

Lorsque vous constatez des contenus appelant à la haine ou faisant l'apologie du terrorisme sur Internet, ne les partagez pas, ne les likez pas, ne les retweetez pas. Ayez le bon réflexe, signalez les sur :

https://www.internet-signalement.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, réglementaire, images – DSCOM/DPI – Février 2018.

Annexe 2 à la note SHFDS/2018/02/6236

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

VIGIPIRATE

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 février 2018)

Cette fiche traite de la protection des lieux de rassemblement ouverts au public (événements sportifs, festivals, marchés de Noël, braderies, etc.) et doit pouvoir servir de guide pratique aux organisateurs de ce genre de manifestations. Elle doit être largement diffusée. Certains des conseils délivrés ci-dessous peuvent ne pas être applicables à tous les sites. Ils doivent donc être adaptés en fonction de la configuration des lieux et du bon sens de circonstance.

1 Identifier les menaces et les vulnérabilités

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités locales (préfet, maire, Police Nationale, Gendarmerie Nationale) :

- pourquoi ce rassemblement pourrait-il être ciblé par des terroristes ?
- en quoi est-il un symbole du mode de vie occidental et des valeurs de la République ?
- ce rassemblement a-t-il une couverture médiatique qui donnerait une forte visibilité à une action terroriste ?

Les différentes attaques possibles doivent être envisagées :

- jet ou dépôt d'un engin explosif à l'intérieur ou en périmétrie du site ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule-bélier ;
- fusillade ou attaque suicide ;
- prise d'otage ;
- attaque à l'arme blanche.

2 Organiser la sécurité de l'événement

Il est primordial que les organisateurs de rassemblements se coordonnent avec le maire et le préfet, ainsi qu'avec les forces de police, de gendarmerie, les services de police municipale et d'incendie et de secours.

Par ailleurs, il peut être nécessaire de faire appel aux compétences de sociétés privées de sécurité pour renforcer la sécurité d'un tel événement.

2.1 - En périphérie du rassemblement

- **choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités.** Il est préférable de choisir le lieu du rassemblement de manière à limiter l'accès de véhicules (ne pas s'installer au débouché d'un axe important) ;
- **limiter ou interdire le stationnement** des véhicules aux abords immédiats du lieu du rassemblement ;
- **mettre en place une signalétique** afin d'orienter les piétons sur le lieu de l'événement et de détourner les flux de véhicules ;
- **cloisonner le flux des véhicules de l'espace de déambulation des piétons ;**
- **identifier le mobilier urbain** qui pourrait servir à dissimuler de l'explosif, le faire retirer par les autorités habilitées, en réduire l'utilisation ou mettre en place des rondes de vérification ;
- **solliciter les forces de l'ordre** ou la police municipale pour la réalisation de patrouilles, voire la mise en place de points de contrôle et de filtrage. Des agents des sociétés privées de sécurité peuvent concourir à cette mission ;
- **identifier les points de vulnérabilité hauts** (immeubles surplombant) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéoprotection donnant, en priorité, sur les accès au site, en prenant en compte les dispositions du Code de la sécurité intérieure.

2.2 - Sur la périmétrie du rassemblement

- **aménager des points de contrôle ou de filtrage en nombre suffisant** aux entrées du site afin de fluidifier l'entrée du public. Leur efficacité repose sur la présence d'un superviseur, de moyens de communication et de procédures claires afin de diffuser l'alerte et de faciliter l'intervention des forces de sécurité intérieure en cas d'incident ;
- **maintenir le niveau de vigilance tout au long de l'événement mais également lors du moment sensible de sa dispersion** (le 22 mai 2017 à Manchester, au Royaume-Uni, un homme a fait détoner une charge explosive qu'il portait sur lui à la sortie de la salle de spectacle *Manchester Arena*), en rappelant régulièrement des messages de sensibilisation à destination du public (*via* la sonorisation de l'événement par exemple – « TOUS acteurs de la sécurité) » ;
- **installer une délimitation physique du périmètre extérieur** de l'événement au moyen de barrières reliées entre elles, de blocs en béton, de véhicules du comité d'organisation comme élément de barrage, etc. ;
- organiser un ou plusieurs cheminements jusqu'au point de contrôle en installant des barrières. Séparer, dans la mesure du possible, les flux entrants et les flux sortants ;
- **aménager les issues de secours en nombre suffisant** au regard de l'importance de l'événement afin de permettre une évacuation rapide du public en cas de danger à l'intérieur de la zone ;
- **organiser et contrôler les livraisons.** Prévoir des équipements mobiles permettant de bloquer physiquement les véhicules appelés à pénétrer dans le périmètre le temps de ce contrôle ;
- apposer les affiches de sensibilisation à destination du public aux points d'entrées notamment « Réagir en cas d'attaque terroriste ».

Les véhicules-béliers constituent un mode d'action terroriste de plus en plus utilisé : attentats de Nice et de Berlin en 2016, attaque contre une patrouille de militaires à Levallois-Perret, attentats en Catalogne et attaque au camion-bélier à New-York en 2017. Pour faire face à ce mode opératoire, il est recommandé de mettre en place des moyens de circonstance permettant d'interdire l'accès au site ou de réduire la vitesse des véhicules à proximité des lieux de rassemblement. La mise en place de chicanes avec des obstacles successifs est également conseillée : plots en béton, bacs de fleurs de dimensions importantes, herses mobiles, barrières d'arrêt ou véhicules lourds (camions). Il est indispensable de tenir compte de la distance de pénétration potentielle d'un véhicule-bélier lors de la définition du périmètre extérieur d'un rassemblement (distance de sécurité entre les dispositifs de sécurité et la foule).

2.3 - Au niveau des volumes intérieurs

- **désigner un responsable sûreté** qui sera l'interlocuteur unique des forces de l'ordre et des services d'incendie et de secours en cas d'intervention sur le site. Véritable coordinateur de la sûreté de l'événement, il doit connaître les bons réflexes à adopter. Il peut se rapprocher préalablement des forces de sécurité intérieure pour recueillir leurs conseils ;
- prévoir l'aménagement d'un **poste central de sûreté** au sein du site. Ce dernier doit être équipé 24H/24 par au moins un opérateur en mesure de visualiser les images du système de vidéo-protection mis en place ;
- **sécuriser la zone en période de fermeture du public** par la mise en œuvre d'un gardiennage humain ;
- **sensibiliser l'ensemble des collaborateurs au niveau de menace,** aux modes opératoires terroristes et à la détection de situations suspectes. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque.

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Annexe 3 à la note SHFDS/2018/02/6236

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

SÉCURITÉ DU NUMÉRIQUE
SENSIBILISATION DES DIRIGEANTS

VIGIPIRATE

Cette fiche s'adresse aux dirigeants d'entreprises privées ou de collectivités territoriales et vise à les aider à appréhender la question de la sécurité du numérique à travers quelques exemples et recommandations pratiques.

1 Cela pourrait vous arriver...

Les scénarios proposés ci-dessous illustrent quelques exemples (parmi d'autres) de menaces de nature cyber pesant sur les organisations et relevant de la responsabilité de leurs dirigeants.

Usurpation d'identité / hameçonnage

Le hameçonnage consiste à usurper l'identité de l'expéditeur dans le but de duper le destinataire qui est invité à ouvrir une pièce-jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette 1ère machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation.

Arnaud reçoit une demande d'ajout de contact sur LinkedIn de la part de son supérieur hiérarchique pendant la période des fêtes de fin d'année. Ce dernier est en congés et souhaite lui transmettre des documents car il n'a pas accès à sa boite mail momentanément. Mais ce qu'Arnaud ne sait pas, c'est que la personne qui s'adresse à lui n'est pas son supérieur mais un groupe d'attaquants ayant usurpé son identité. En transmettant à ce collaborateur un simple document contenant une charge malveillante, ils ont pu compromettre les équipements de l'entreprise connectés à Internet et exfiltrer des données sensibles en relation avec une importante négociation commerciale de nature confidentielle. Dès le lendemain, les informations fuitent dans la presse, conduisant ainsi à la rupture de la négociation au profit d'une entreprise concurrente.

Rançongiciel

Le rançongiciel est un programme malveillant chiffrant tout ou partie des données stockées sur un ordinateur ou accessibles par un réseau. L'objectif est de proposer à la victime de récupérer ses données en échange du paiement d'une rançon.

Guillaume est dirigeant d'entreprise. Nous sommes vendredi après-midi avant le début des congés de fin d'année et Guillaume avait déjà autorisé ses employés à partir exceptionnellement à 15h00. Son responsable sécurité lui indique qu'une mise à jour de l'ensemble des postes de travail doit être réalisée mais ne pourra pas être effective avant 15h00. Guillaume décide de fermer l'entreprise comme prévu et de reporter l'opération de mise à jour.

Le 2 janvier, les ordinateurs de tous les employés affichent un écran noir porteur d'un message exigeant d'eux le paiement d'une rançon en échange de la récupération de leurs données. Les employés ne pouvant plus travailler, l'activité de l'ensemble de l'entreprise et de ses sous-traitants est à l'arrêt et mise en péril.

Les conséquences pour votre entreprise peuvent être graves :
perte financière importante, atteinte à l'image de l'organisation, etc.

2 S'emparer de la question de la sécurité numérique

5 questions pour faire le point

- Depuis quand n'ai-je pas entendu parler de cybersécurité ?
- Mon entreprise est-elle une cible d'intérêt pour des attaquants ?
- Ai-je pris toutes les précautions pour protéger mes informations et les échanges avec mes partenaires et mes collaborateurs ?
- Quel est la part du budget consacrée à la sécurité informatique ?
- Ai-je déjà parlé de cybersécurité à mes collaborateurs ?

5 questions à poser à mon RSSI

- Quelles sont nos principales vulnérabilités ?
- Quels sont les moyens de protection actuellement en place pour lutter contre les attaques et codes malveillants ?
- A-t-on déjà fait un audit de sécurité des SI ?
  A-t-on déjà fait une analyse de risques ?
  Dispose-t-on d'une cartographie des SI ?
- Sommes-nous préparés si une crise d'origine cyber survenait ?
- Disposons-nous d'une couverture juridique et nos contrats d'assurance intègrent-ils le risque cyber ?

Vous êtes au coeur de la stratégie de gestion des informations clés de l'entreprise. Vos données personnelles sont autant d'informations potentiellement convoitées par des individus aux intentions malveillantes. Soyez notamment vigilant à l'égard de possibles usurpations de votre identité sur les réseaux sociaux et maîtrisez les informations sur votre entreprise qui circulent sur Internet.

Sensibiliser vos employés aux bonnes pratiques

Vos employés doivent être sensibilisés voire formés aux bonnes pratiques de l'informatique et devenir acteur de la sécurité numérique de leur entreprise.

Analyser les risques et protéger les systèmes d'information sensibles

Il est essentiel de savoir quels sont les systèmes d'information les plus cruciaux pour le bon fonctionnement de votre entreprise afin de pouvoir traiter les risques susceptibles de les fragiliser.

Préparer votre entreprise à une attaque informatique

Assurez-vous de disposer d'un plan de réaction aux incidents de sécurité (notamment un processus de sauvegarde régulier des données critiques) et testez-le. En particulier, établissez une chaine de remontée d'incidents connue des employés afin de reconnaitre au plus tôt une tentative d'attaque.

Organiser un exercice simulant une attaque

Un exercice de gestion de crise permet de vérifier la solidité des procédures mises en place dans votre organisme et de les corriger si nécessaire.

3 Vous pensez avoir été victime d'une attaque

Qui prévenir ?

Dirigeant d'une entreprise (TPE, PME) ou d'une collectivité territoriale, il est recommandé de vous rendre sur la plateforme numérique **www.cybermalveillance.gouv.fr** afin d'être mis en relation avec des prestataires de proximité susceptibles de vous assister techniquement. Vous pouvez également déposer plainte auprès d'un service de la Police nationale ou de la Gendarmerie nationale ou adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
https://www.ssi.gouv.fr/uploads/2017/01/guide_cgpme_bonnes_pratiques.pdf.pdf
Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
MOOC (Massive Open Online Course) SecNumacadémie de l'ANSSI
https://www.secnumacademie.gouv.fr
En cas d'incident
https://www.ssi.gouv.fr/en-cas-dincident/

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrications, réalisations, images © SGDSN/DCPP, © Février 2018.