PRÉFET
DE LA GIRONDE
Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Service interministériel de défense et de protection civile

Affaire suivie par :
Section opérationnelle et Défense

Bordeaux, le 23 JUIN 2023

Le Préfet

à

Mmes et MM. les Maires des communes de Gironde

Copie : Mmes et MM. les Sous-Préfets d'arrondissement de Gironde

Objet : Adaptation de la posture VIGIPIRATE « été – automne 2023 ».

Je vous informe de l'entrée en vigueur de l'adaptation de posture VIGIPIRATE « été – automne 2023 ». Elle maintient pour l'ensemble du territoire national le niveau :

« sécurité renforcée – risque attentat ».

Dans le contexte d'une menace terroriste qui reste durablement élevée et de l'accueil de la coupe du monde de Rugby, du 8 septembre au 28 octobre 2023 sur le territoire métropolitain, cette posture met l'accent sur :

- la sécurité des sites en lien avec la coupe du monde de rugby ;
- la sécurité des lieux de rassemblement culturels et festifs ;
- la sécurité des transports et des bâtiments publics.

Une vigilance particulière devra être portée en raison de l'affluence attendue pour la coupe du monde de rugby, aussi bien pour les sites concernés par l'événement que les espaces où des manifestations publiques en lien avec celui-ci pourraient être organisées.

L'effort de surveillance et de contrôle doit porter sur les rassemblements liés à cet événement majeur, ainsi qu'aux manifestations religieuses, politiques et culturelles.

La surveillance des lieux de rassemblements festifs et leurs abords, qui connaîtront un afflux de public sera également renforcée, notamment les établissements recevant du public de type N (restaurants et débits de boissons). De même concernant les établissements de santé de première ligne.

Enfin, face aux menaces d'origine cyber, il convient de sensibiliser les utilisateurs aux risques numériques et à l'application de la politique de sécurité des systèmes d'information, en particulier lors de l'utilisation de supports amovibles, de navigation Internet ou d'échanges de courriels.

Tél : 05 56 90 60 60
Mél : pref-defense-securite-civile@gironde.gouv.fr
2, esplanade Charles-de-Gaulle
CS 41397 – 33077 Bordeaux Cedex
www.gironde.gouv.fr

I – Les consignes issues de la nouvelle posture « Été – Automne 2023 » :

1) Sécurité de la coupe du monde de rugby

Bien qu'aucune menace majeure ciblant spécifiquement l'événement n'ait été détectée à ce jour, la coupe du monde de rugby (CMR) demeure une vitrine médiatique internationale et un vecteur de concentration de foules qui en font une cible privilégiée.

La CMR 2023 se déroulera en France du vendredi 8 septembre au samedi 28 octobre 2023. La compétition réunira 20 équipes, représentant des nations issues de cinq continents, qui disputeront 48 matchs pendant cette période de 51 jours organisés dans plusieurs villes-hôtes dont Bordeaux. L'affluence attendue pour ce grand événement sportif international est estimée à 2,6 millions de spectateurs, dont 600 000 visiteurs étrangers présents sur le territoire national pour suivre la compétition. Le nombre de téléspectateurs escomptés est estimé à 900 millions.

Les préfets ont reçu des directives pour organiser la protection de la CMR, aussi bien pour les sites concernés par l'événement que pour les « villages-rugby », où des manifestations publiques en lien avec cet événement pourraient être organisées.

Une vigilance accrue, quant à la détention d'armes blanches ou autre objets suspects ou à l'utilisation de véhicules béliers contre les attroupements, sera portée lors des contrôles mis en place aux différents accès de ces rassemblements.

2) Sécurité des lieux de rassemblement et des lieux de culte

- Contexte général :

La capacité à faire face à une attaque terroriste dans les lieux de rassemblement de personnes demeure une priorité essentielle.

Le renforcement des échanges d'information entre les organisateurs et les services de l'État reste capital. Préalablement à l'organisation de tout événement, les responsables et initiateurs doivent impérativement prendre contact avec les forces de sécurité intérieure (FSI) et les services préfectoraux quand bien même l'avis des référents sûreté départementaux de la police ou de la gendarmerie a été sollicité.
Les responsables de sites sont invités à adapter les mesures de sûreté qui leur incombent en fonction des vulnérabilités particulières des lieux, de la fréquentation et des amplitudes horaires d'ouverture (jour/nuit), du contexte local évalué avec les services de l'État. Les personnels de l'équipe d'organisation seront sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

- Mesures propres aux fêtes religieuses :

La sécurité sera renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre ou des militaires de l'opération Sentinelle selon un mode de sécurisation dynamique, assorti de prises de contact avec les responsables de lieux de culte voire statique (avant et pendant les offices et jusqu'à dispersion des fidèles) s'agissant des sites signalés comme sensibles voire très sensibles par les autorités religieuses. En liaison avec les autorités religieuses locales, la mise en œuvre de mesures de contrôle des accès (limitation du nombre d'accès, contrôles visuels des flux entrants à la diligence des équipes communautaires ou paroissiales) est recommandée. De la même façon, une attention particulière devra être portée aux véhicules en stationnement à proximité des lieux de rassemblement ou de culte. **A cet égard, je vous invite à prendre des mesures temporaires d'interdiction de circuler et de stationner si nécessaire.**

- Mesures propres aux périodes de vacances scolaires :

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (stations balnéaires, salles de spectacles, etc.) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure et unités Sentinelle) adapteront leur dispositif en conséquence. Les opérateurs sont incités à solliciter l'appui des référents sûreté départementaux de la police ou de la gendarmerie nationales.

- Guide des bonnes pratiques de sécurisation d'un événement de voie publique :

Le ministère de l'Intérieur a publié et diffusé un **guide des bonnes pratiques de sécurisation d'un événement de voie publique en octobre 2018.**

Ce guide est disponible sur le site Internet :
https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique.

3) Sécurité des grands espaces de commerce, de tourisme et de loisirs

Les lieux de commerce, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées.
La sécurité restera renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (salons d'expositions, foires, etc.), les interconnexions de transports en milieu clos dotées de commerce (gares, etc.) demeurent également un point de vigilance.

Le secteur du tourisme, les stations balnéaires et les parcs de loisirs, particulièrement fréquentés au moment des vacances scolaires pourraient être ciblés. Enfin, la sécurité des grands espaces de commerce lors des soldes d'été, marquées par une forte affluence, demeure un axe d'attention majeur.

Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou qu'un événement révèle une vulnérabilité particulière, ceux-ci sont communiqués par les autorités préfectorales aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif.

Cette démarche s'inscrit dans la volonté de renforcer les liens et la coordination entre acteurs publics et privés.

- La sensibilisation des personnels :

Elle doit être assurée par les gestionnaires de centres et d'enseignes commerciaux.

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

Par ailleurs, les responsables d'enseignes sont incités à former leur personnel aux gestes de premiers secours.

Enfin, la connaissance fine des sites par le personnel qui y travaille et l'organisation d'exercices collectifs constituent des prérequis indispensables.

- Le renforcement des échanges et de la coordination entre acteurs publics et privés :

Ce renforcement se matérialise par la mise en place ou l'adaptation de conventions locales de coopération de sécurité.

Pour rappel, la convention nationale, signée le 19 février 2019, entre le secrétaire d'Etat auprès du ministère de l'Intérieur et les principales organisations professionnelles représentant les grandes surfaces commerciales promeut des conventions locales « *visant au développement d'un plan de sécurisation suivi et pérenne des espaces commerciaux* ». Il est recommandé à ces établissements de mettre en place un plan de sûreté et de désigner un coordonnateur en gestion de crise.

Ces types de coopération animés dans le cadre de la police de sécurité du quotidien (PSQ) instaurent une confiance mutuelle et impulsent une nouvelle dynamique d'échanges d'informations. Le développement de ces conventions locales est recherché.

- Un 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.

Sur la voie publique, la vidéoprotection peut être mise en œuvre par les personnes morales, sur autorisation préfectorale, 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).

4) Sécurité des bâtiments publics

Il convient d'actualiser les annuaires de crise au sortir et les procédures d'alerte afférentes.
Les plans de protection et les procédures internes d'évacuation ou de confinement seront portés à la connaissance des nouveaux arrivants.

5) Sécurité des établissements d'enseignement et de recherche, des structures d'accueil collectif de mineurs (ACM), des séjours de cohésion du service national universel (SNU) et des établissements publics relevant du ministère des sports et des jeux olympiques et paralympiques

L'adaptation de cette posture maintient les mesures antérieures et met l'accent sur :

- l'organisation ministérielle et les liens entre les services de l'État dans le cadre de la coupe du monde de rugby ;

- le travail partenarial avec les acteurs concourant à la préparation des jeux olympiques et paralympiques 2024 ;

- les mesures de sécurisation nécessaires à prendre avec les préfectures, les collectivités territoriales et les opérateurs le cas échéant, face aux risques d'intrusion ou de toute atteinte à la sûreté d'un établissement ;

- La mise à jour des plans particuliers de mise en sûreté (PPMS) et des plans de continuité d'activité (PCA) à adapter en conséquence et la réalisation des exercices associés. En cas d'événement perturbant le fonctionnement de l'établissement concerné (violences, intrusion, risque de débordement, etc.), le responsable du site doit prendre toute mesure nécessaire (activation du PPMS, du PCA, de son dispositif de crise) et en informer les autorités compétentes ;

- le signalement aux forces de sécurité intérieure de toute menace proférée à l'encontre de personnels exerçant une mission de service public ou lors de diffusion d'informations relatives à sa vie privée, familiale ou professionnelle, conformément aux consignes adressées aux recteurs dans la circulaire du 9 novembre 2022 relative au plan pour la laïcité dans les écoles et établissements scolaires ;

- les séjours de cohésion dans le cadre du service national universel ;

- Le maintien d'une attention particulière à la sécurisation des systèmes d'information.

Contexte général

Les établissements d'enseignement et de recherche sont des cibles privilégiées, quelle que soit l'origine de la menace, en raison notamment de leur charge symbolique.

Les mesures des directives ministérielles et interministérielles doivent être mises en œuvre au sein des établissements et organismes relevant des ministères de l'Éducation nationale et de la jeunesse et de l'enseignement supérieur et de la recherche (MENJ/MESR), du ministère de l'Agriculture et de la souveraineté alimentaire (MASA), au titre des activités d'enseignement, et du ministère des Sports et des jeux olympiques et paralympiques (MSJOP), avec les préfectures, les forces de sécurité intérieure, les collectivités territoriales et les responsables de structures privées accueillant le public des MENJ/MESR/MSJOP.

Objectifs de sécurité recherchés durant la période

■ **Coupe du monde de rugby 2023**

L'enjeu sécuritaire et médiatique de la coupe du monde de rugby appelle également une organisation adaptée du MSJOP. Une haute vigilance des impacts des grands événements sportifs sur le périmètre MSJOP devra être assurée. Les régions académiques et établissements du MSJOP mettront en œuvre les mesures des directives interministérielles.

Il importe également que des liens renforcés soient déployés entre les services de l'État et les collectivités territoriales hôtes, dans un souci de partage d'informations et de gestion d'incidents ou d'événements graves le cas échéant.

■ **Sécurisation des personnes et des biens**

Les établissements et organismes des MENJ/MESR et du MASA doivent maintenir leurs efforts habituels, et toujours indispensables, de sécurisation des personnes (personnels et usagers) et des biens.

Dans les établissements et les sites des opérateurs sous tutelle des MENJ/MESR et du MASA, une attention particulière sera portée à la protection et aux contrôles des laboratoires sensibles soumis à une réglementation spécifique, ainsi qu'aux lieux de stockage de matières dangereuses (sources radioactives, produits toxiques ou agents pathogènes, précurseurs d'explosifs, matières biologiques, etc.) et lieux abritant des animaleries.

Les zones considérées sensibles (zones à régime restrictif, zones sécurisées, zones d'accès restreint) doivent faire l'objet d'une vigilance maximale, de procédures de contrôle renforcées et de signalements systématiques.

Dans le périmètre du MESR et du MASA, dans tous les cas, y compris hors cas prévus par les dispositions réglementaires encadrant le dispositif de protection du potentiel scientifique et technique, le fonctionnaire de sécurité de défense/ officier de sécurité (OS) de l'établissement doit être informé de toute problématique sécuritaire et en faire part au haut-fonctionnaire de défense et de sécurité (HFDS) du périmètre ministériel dont relève son établissement.

■ **La sécurisation des systèmes d'information (données et infrastructures numériques)**

Il est demandé aux services et établissements des MENJ/MESR/MSJOP de veiller aux consignes relayées par le fonctionnaire de sécurité des systèmes d'information.

6) Sécurisation des sites touristiques, culturels et des expositions à thème sensible

Compte tenu de la situation internationale et de la persistance d'un niveau élevé de menace terroriste, les exploitants de sites touristiques sont invités à renforcer leurs mesures de vigilance et à prendre l'attache des forces de sécurité intérieure (police nationale et gendarmerie nationale).

L'attention des propriétaires de monuments qui désire participer aux 40èmes Journées européennes du patrimoine est tout particulièrement attirée sur les mesures de précautions élémentaires et la nécessité de se manifester auprès du commissariat de police ou de la brigade de gendarmerie locale. Concernant cet événement particulier, les recommandations de vigilance accrue concernant les sites à forte valeur symbolique du point de vue historique régulièrement formulées dans le cadre de l'exploitation normale de ces monuments restent valables.

Pour ce qui concerne les événements se déroulant sur la voie publique, plus nombreux durant l'été, les organisateurs sont invités à se référer au guide des bonnes pratiques de sécurisation d'un événement de voie publique disponible sur le site Internet du ministère de l'Intérieur à l'adresse suivante : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique

Ce document détaille les procédures de déclaration à respecter et donne des exemples illustrés de mesures de protection, contre les véhicules béliers notamment. Une série d'autres guides de recommandations est également disponible sur le site internet du SGDSN (cf. paragraphe II 6°).

La période est également marquée par l'Olympiade culturelle dans le cadre de laquelle sont labellisés des événements permettant de rappeler les liens qui existent entre le sport et la culture. Compte tenu de la couverture médiatique et de la puissance évocatrice des Jeux Olympiques et Paralympiques de Paris 2024, les organisateurs d'événements labellisés sont invités à observer scrupuleusement les consignes formulées dans la présente note de posture.

Enfin, les sinistres récents au sein de bâtiments classés ou inscrits au titre de monuments historiques invitent les établissements culturels à compléter ou à mettre à jour leur plan de sauvegarde des biens culturels (PSBC). La protection du patrimoine culturel compte parmi les objectifs du dispositif ORSEC, le PSBC doit donc être réalisé en relation étroite avec les services de secours et être mis à leur disposition en cas d'intervention.

7) Sécurité du numérique

- Contexte général
Les menaces visant les administrations et les entreprises privées restent élevées et variées (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques entre autres).

Afin de se tenir à jour du niveau de la menace et des mesures cyber préventives cyber prioritaires, il est préconisé de consulter régulièrement les sites suivants :
- https://www.ssi.gouv.fr (site de l'Agence nationale de la sécurité des systèmes d'information) ;
- https://www.cert.ssi.gouv.fr (site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

- Objectifs de sécurité recherchés sur la période
Au regard de l'évaluation de la menace pour la sécurité du numérique présentée aux paragraphes supra nécessite, il apparaît nécessaire d'appliquer les objectifs et mesures de sécurité suivants :

- Rechercher sur le SI des marqueurs particuliers correspondant à une attaque :
Compte tenu de l'évolution de la menace cyber, il est recommandé de mettre en place un processus pour consulter régulièrement les rapports de la menace (https://www.cert.ssi.gouv.fr/cti/) et récupérer les marqueurs de compromissions associés (https://www.cert.ssi.gouv.fr/ioc/). Un feed MISP public relayant ces marqueurs est également mis à disposition par l'ANSSI (https://misp.cert.ssi.gouv.fr/feed-misp/). Ces marqueurs peuvent être complétés par d'autres sources de marqueurs provenant de partenaires de confiance.
Ces marqueurs peuvent être intégrés, dès publication, aux systèmes de détection disponibles (antivirus, EDR, NIDS, HIDS...). Par ailleurs, il est recommandé de chercher la présence de ces marqueurs sur l'historique des journaux disponibles afin d'identifier d'éventuelles tentatives de compromission.

- Consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR) :
Afin de se prémunir d'éventuelles attaques suite à la découverte de vulnérabilités, il convient de mettre en place un processus de veille concernant la publication de vulnérabilités relatives aux éléments du SI. Il est notamment possible de s'appuyer sur les bulletins du CERT-FR (https://www.cert.ssi.gouv.fr/avis/ et https://www.cert.ssi.gouv.fr/alerte/).
Cette veille sur les vulnérabilités doit être réalisée de manière quotidienne, idéalement via un processus automatisé à partir de sources complémentaires pour couvrir l'ensemble des briques du système d'information.

- Absorber le trafic illégitime au niveau du réseau :
Compte tenu des attaques menées par DDoS et du risque de défiguration de sites web, il est important de s'assurer que les opérateurs de services numériques, d'une part, disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement de leurs systèmes d'information et des sites web hébergés.

Sur la base des informations transmises par l'ANSSI, il est nécessaire d'identifier les moyens de filtrage les plus efficaces (par exemple avec un équipement en entrée de réseau ou avec l'appui d'un opérateur de communication électronique ou un fournisseur de solution spécialisé). Il est recommandé de prendre en compte les différentes typologies d'attaques par déni de service (au niveau applicatif, spécifique à protocole ou basé sur la volumétrie) et la couverture offerte par les moyens de filtrage. Les organisations doivent ensuite mettre en place ces mécanismes de protection anti-déni de service sur les services qu'ils hébergent ou demander la mise en place auprès des prestataires d'hébergement ou de communication le cas échéant.

- Sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter :
Dans le contexte d'importance des menaces d'origine cyber, il convient de sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application de la politique de sécurité des systèmes d'information, en particulier vis-à-vis de l'utilisation de support amovibles, de navigation Internet ou d'échanges de courriels.
L'attention à la sensibilité de l'information et à sa protection est également à intégrer au sein de cette sensibilisation. La non-séparation des usages et matériaux personnels et professionnels, échanges professionnels dans des lieux publics, présence de matériaux protégés ou classifiés sur des systèmes inadéquats sont à proscrire.
Dans le cadre de cette sensibilisation, il est possible de s'appuyer sur SecNumacadémie (https://secnumacademie.gouv.fr/), la formation en ligne de l'ANSSI, qui détaille les bonnes pratiques pour une utilisation sécurisée des outils numériques.

- Valider et appliquer un correctif de sécurité :
Face aux vulnérabilités critiques et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est nécessaire et pour des raisons d'urgence et de criticité, être appliqués en dehors des processus de maintien en condition de sécurité des systèmes d'information. De même, les correctifs mentionnés dans les avis de sécurité et qui correspondent à la veille sur plus d'une centaine de produits, doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des systèmes d'information. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site www.cert.ssi.gouv.fr.
Les correctifs de sécurité correspondant aux bulletins d'alerte du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :

*CERTFR-2022-ALE-009 (https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-009/) – Multiples vulnérabilités dans Zimbra Collaboration
Ces vulnérabilités sont simples à exploiter et peuvent être combinées pour prendre le contrôle total de la machine vulnérable. Un correctif est disponible depuis octobre 2022. Le CERT-FR a connaissance de cas d'exploitation de cette vulnérabilité et de codes d'exploitation publiquement disponibles. Zimbra reste la cible d'exploitations en 2023 et la mise à jour des serveurs Zimbra reste d'actualité – au même titre que la mise à jour des serveurs Microsoft Exchange.

*CERTFR-2023-ALE-001 (https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-001/) - Vulnérabilité dans Fortinet FortiOS
Cette vulnérabilité permet à un attaquant de prendre le contrôle à distance de plateformes de pare-feu FortiGate utilisant le système FortiOs. L'éditeur Fortinet a indiqué avoir observé des cas d'exploitation de cette vulnérabilité dans le cadre d'attaques ciblées.
Les équipements de sécurité tels que les points de terminaison VPN sont fréquemment ciblés par les attaquants et le CERT-FR a connaissance de cas d'exploitation des vulnérabilités affectant les solutions Fortinet et en particulier les produits de la marque Fortinet.
Dans son guide pour le nomadisme, le CERT-FR recommande de mettre en place une infrastructure sécurisée pour l'administration des équipements et des services. Le maintien en condition de sécurité de ces infrastructures est essentiel, et le déploiement des correctifs de sécurité fait partie des mesures qu'il convient d'appliquer systématiquement.

*CERTFR-2023-ACT-004 (https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-004/) - Fin de support de Windows 8.1, Windows Server 2012 et Windows Server 2012 R2
Le support de Microsoft Windows 8.1 s'est arrêté le 10 janvier 2023, tandis que le support de Microsoft Windows Server 2012 / 2012 R2 s'arrêtera le 10 octobre 2023.
Le CERT-FR a pu constater que de nombreux systèmes utilisant Microsoft Windows 7, Windows Server 2012 ou Windows Server 2012 R2 sont aujourd'hui encore en service. L'ANSSI attire l'attention sur la nécessité d'anticiper dès à présent une migration : Microsoft Windows 11 (ou Windows 10 si le processeur n'est pas compatible) et Windows Server 2022.
En cas d'impossibilité de migrer un système obsolète vers une version supportée, l'isolation de celui-ci vis-à-vis du système d'information constitue une mesure compensatoire visant à limiter les impacts en cas de compromission. Cette isolation devra être réalisée dans les plus brefs délais.

*CERTFR-2023-ALE-015 (https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/) - Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi
Le CERT-FR a pris connaissance de campagnes d'attaque ciblant les hyperviseurs VMware ESXi dans le but d'y déployer un rançongiciel. Ces campagnes d'attaque semblent avoir tiré parti de l'exposition d'hyperviseurs ESXi qui n'auraient pas été mis à jour des correctifs de sécurité suffisamment rapidement. Ces vulnérabilités permettent à un attaquant de réaliser une exploitation de code arbitraire à distance. Des codes d'exploitation sont disponibles en source ouverte depuis au moins mai 2021.
Le CERT-FR a édité un guide pour la sécurisation de l'administration des systèmes d'information.

- Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace :
Compte tenu des menaces cyber persistantes, il est essentiel de s'assurer que les outils et dispositifs de réponse à incident sont opérationnels et adaptés à la menace numérique et que le personnel chargé de le mettre en œuvre soit familiarisé avec celui-ci. Le guide de l'ANSSI sur la thématique de la gestion de crise cyber aide les organisations à organiser leur dispositif : https://www.ssi.gouv.fr/uploads/2021/12/anssi-guide-gestion_crise_cyber.pdf.

Il est également important que la baisse des effectifs liés aux congés estivaux n'impacte pas l'organisation de ce dispositif. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA ou de gestion de crise cyber si le dernier exercice a été effectué il y a plus d'un an. Le guide de l'ANSSI sur les exercices de gestion de crise cyber aide les entités à organiser ces exercices : https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/.
Enfin, au regard des tensions géopolitiques actuelles, certaines consignes spécifiques proposées par l'ANSSI peuvent être mises en place au sein de l'organisation : https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/.

- Vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés :
Face aux menaces cyber, il convient de s'assurer que la capacité de communication entre le personnel en charge de répondre à la crise sera maintenue. Il est donc essentiel de vérifier que les annuaires de crise, contenant les contacts du personnel pertinent en cas de crise, en interne comme en externe, sont bien à jour et correctement diffusés à tous les acteurs. Par ailleurs, certaines menaces (notamment de type rançongiciel) peuvent aboutir à la perte des outils de communication usuels. Il est nécessaire de tester régulièrement les moyens de communication alternatifs et sécurisés, qui pourront être utilisés dans le cas d'une attaque impactant les outils de communication nominaux.
Des tests de vérification des communications peuvent être menés pour vérifier la bonne réception des alertes par les contacts d'urgence, ainsi que la capacité de chacun à utiliser les outils de connexion sécurisés.

- Procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques :
En cas d'attaque par rançongiciel, de destruction ou d'altération des données, il est important de pouvoir restaurer le bon fonctionnement des systèmes les plus critiques en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration. Le guide de l'ANSSI « Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ? » aide les entités à réduire le risque d'attaque et réagir lorsque celle-ci réussie : https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/.

II – Les consignes particulières de vigilance, prévention et protection

1) Sensibilisation des personnels en tenue

Toutes les personnes, civiles ou militaires, portant un uniforme ou une tenue avec des signes distinctifs, et représentant une autorité, constituent des cibles privilégiées. Elles seront sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

2) 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. Les organisateurs d'événements de voie publique doivent prendre en compte cette menace et mettre en œuvre des dispositifs adaptés afin de s'en prémunir. Ils peuvent pour cela solliciter l'avis des référents sûreté locaux et/ou consulter :

- la fiche de recommandations Vigipirate « *Se protéger contre les attaques au véhicule-bélier* », disponible sur le site Internet du SGDSN : http://www.sgdsn.gouv.fr/vigipirate ;
- le guide du ministère de l'Intérieur évoqué ci-dessus (paragraphe I.2).

3) Signalement des cas suspects de radicalisation, des troubles comportementaux ou psychiatriques/psychologiques.

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. Des troubles psychologiques peuvent offrir un terreau favorable à la radicalisation.

L'objectif du signalement au centre national d'assistance et de prévention de la radicalisation (CNAPR) est de protéger ces personnes contre elles-mêmes et la population contre de possibles comportements violents. Les combinaisons de comportements suivants doivent éveiller la vigilance et méritent de faire l'objet d'un signalement : changements physiques, vestimentaires et alimentaires, propos asociaux, passage à une pratique religieuse hyper ritualisée, rejet de l'autorité, repli sur soi, rejet brutal des habitudes quotidiennes, refus du débat, rejet de la société et des institutions, modification soudaine des centres d'intérêt, discours complotiste ou apocalyptique, tentative d'imposition agressive d'un ordre religieux.

Le signalement des cas suspects de radicalisation, quel que soit le type de radicalisation (religieuse, politique...) se réalise de la manière suivante :

- Appel au numéro vert : 0 800 005 696

En cas de suspicion d'une action violente ou de toute autre cas d'urgence, appelez immédiatement le 17 ou le 112 pour alerter les forces de sécurité intérieure.

Il existe un référent radicalisation en préfecture qui a vocation à servir d'interlocuteur local pour cette problématique : pref-coraso@gironde.gouv.fr

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

Les récents attentats, ou actes de malveillance, commis ou déjoués en Europe, ont démontré une capacité à fabriquer des explosifs artisanaux ou des substances toxiques à partir de produits chimiques d'usage courant. La recrudescence d'envois de lettres ou de colis piégés a justifié l'envoi d'un bulletin d'alerte le 21 décembre 2022. Au moindre doute sur le contenu d'un colis ou d'une enveloppe, ce dernier ne doit pas être manipulé. Il doit être contrôlé au moyen d'un détecteur à rayon X. En cas d'impossibilité à mettre en œuvre ce type de technologie, il convient d'alerter les forces de sécurité intérieure (appel au 17 ou 112) et d'établir un périmètre de sécurité en faisant évacuer et en balisant la zone.

Les professionnels qui vendent des explosifs artisanaux ou des substances NRBC 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 : *pixaf@gendarmerie.interieur.gouv.fr ou 01.78.47.34.29 (24/7)*

En cas d'attaque NRBC, il est déterminant que les services intervenants mettent en œuvre, sans délai, les moyens, procédures et protocoles afin d'en minimiser les effets.

Pour cela, il se révèle indispensable de :

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

- rappeler les consignes de protection et les conduites à tenir individuelles et collectives.

5) Sensibilisation à la lutte anti-drone

L'utilisation des drones est un mode d'action régulièrement mis en œuvre pour capter des images ou diffuser des messages mais elle permet également de perpétrer des actes de malveillance ou à caractère terroriste.
Les responsables d'activités sensibles et de grands rassemblements doivent prendre en compte cette menace en menant une analyse de risque avec l'appui des référents sûreté locaux de la police ou de la gendarmerie nationales. Ils ont la possibilité de mettre en œuvre les moyens de détection des drones aux abords de leur site.
Les technologies de détection actuelles présentent des ambitions, performances et coûts variés, offrant des solutions adaptées aux besoins identifiés lors de l'analyse de risque, qui vont de l'exploitation à moindre coût de l'exigence de signalement électronique des drones de masse supérieure à 800 grammes (250 grammes pour les drones commercialisés avec une mention de classe européenne), à des moyens plus onéreux permettant de détecter des drones ne se signalant pas.
Ces moyens permettent la mise en œuvre des mesures de sauvegarde immédiate en cas de menace imminente, l'orientation des forces de sécurité vers le télé-pilote pour mettre fin au survol, et le relevé des éléments de preuve des infractions. Selon l'analyse de la sensibilité d'un événement et du niveau de menace, les forces de sécurité intérieures peuvent déployer des moyens de détection additionnels et des moyens de neutralisation des drones (brouillage, filets, destruction, etc.), capacité qui reste exclusivement du ressort des services de l'État.

6) Sensibilisation du grand public

- Efforts de communication :

Vous veillerez à **mettre en place l'affichage** du **logogramme VIGIPIRATE** à l'entrée de chaque établissement public et des lieux privés recevant du public (centres commerciaux, etc...).

Il peut être téléchargé sur : https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble.

- Sensibilisation des professionnels et du grand public aux bonnes pratiques :

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, des fiches de sensibilisation sont accessibles en ligne sur : https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation.

Elles traitent des sujets suivants :
- que faire en cas d'exposition à un gaz toxique ?
- réagir en cas d'attaque terroriste.

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public est fondamentale. Aussi ces affiches peuvent téléchargées et imprimées sur un format adapté au lieu où elles sont placées afin de les rendre visibles du public (privilégier les entrées et sorties des établissements, les halls, ou salles d'attente, etc.).

Par ailleurs, un ensemble de fiches de recommandations et de bonnes pratiques à l'attention du grand public est également téléchargeable sur :
https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques
Par exemple :
- recommandations à l'attention des gestionnaires de parcs et loueurs de voitures (prévention des attaques au véhicule bélier) ;
- signalement des situations suspectes ;
- organisation d'un confinement face à une menace terroriste ;
- se protéger contre les attaques au véhicule bélier ;
- prévention et signalement des cas suspects de radicalisation ;
- règles d'utilisation des drones et mesures de prévention face à un usage malveillant ;
- chaîne d'alerte en cas de menace.

En complément, plusieurs guides de bonnes pratiques à destination des élus et des professionnels sont également téléchargeables sur : https://www.sgdsn.gouv.fr/vigipirate/les-guides

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

Enfin, deux modules de formation en ligne, développés en liaison avec de nombreux partenaires sont accessibles sur : https://vigipirate.gouv.fr.
- Un module long, dédié essentiellement aux professionnels de la sécurité ;
- Un module court, disponible en plusieurs langues, dédié au public.
Ces modules intègrent des témoignages vidéo, de citoyens ou de professionnels, ayant été confrontés à des attaques ou à des prises d'otages, ou dont les services contribuent au quotidien à lutter contre le terrorisme. Ils permettent, en quelques heures, d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter afin de prévenir un acte terroriste ou de réagir en cas d'attaque.

***

Je vous demande de bien vouloir appliquer les mesures relatives à la mise en œuvre de cette adaptation de posture VIGIPIRATE et d'en informer les services placés sous votre autorité, ainsi que les responsables de sites publics ou privés situés sur votre commune.

Je vous remercie de m'informer de toutes difficultés que vous pourriez rencontrer dans la mise en œuvre de ces consignes nationales.

Le Préfet,

Étienne GUYOT