TABLEAU DES MESURES DE VIGILANCE, DE SURVEILLANCE ET DE CONTRÔLE

Nota : les mesures nouvelles figurent en gras dans le tableau

N° mesure	Mesure	Commentaires
ALR 11-02	Diffuser l'alerte au grand public	**Le logogramme reflétant le niveau actuel du plan VIGIPIRATE « Sécurité renforcée – risque attentat » est représenté ci-dessous.**  **Les logogrammes VIGIPIRATE peuvent être téléchargés sur le site du SGDSN : http://www.sgdsn.gouv.fr/vigipirate .**
ALR 11-04	Rappeler les conduites à tenir en réponse à la menace d'actions terroristes (fusillade, colis abandonné, alerte à la bombe)	**Quatre fiches de posture sont diffusées en complément de ce tableau :** - **Fiche « Conduite à tenir lors d'un événement biologique ou chimique », destinée aux seuls responsables sûreté-sécurité des établissements recevant du public (sur demande auprès du SHFDS) ;** - **Fiche « Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ? »** - **Fiche « Comment préparer ses déplacements et voyages à l'étranger ? »** - **Fiche « Sécurité du numérique. Rançongiciel : vos données prises en otage »**
RSB 11-01 RSB 12-01 RSB 13-01	Renforcer la Surveillance et le contrôle	RSB 12-01 : L'effort de vigilance porte sur les rassemblements liés aux manifestations religieuses, politiques, sportives et culturelles propres à la période couverte par la présente posture. Une vigilance accrue, quant à la détention d'armes blanches ou autres objets suspects, sera portée lors des contrôles mis en place aux différents accès de ces rassemblements. Les sorties de spectacles ou de grands rassemblements publics doivent bénéficier d'un dispositif de sécurité, jusqu'à dispersion complète du public. **Une attention particulière sera portée aux événements majeurs affectant cette période : scrutin européen, championnat du monde de football féminin, anniversaires des débarquements de Normandie et de Provence, sommet du G7 à Biarritz, Journées européennes du patrimoine.**
RSB 12-05	Mettre en œuvre des Dispositifs de Protection pour faire	Au regard de la menace associée aux attaques par véhicules-béliers, les préfets encourageront les collectivités territoriales et opérateurs privés à renforcer les dispositifs de protection passive (plots, barrière, blocs en béton, etc.) sur les

	face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier)	lieux et artères les plus fréquentés. **Ils pourront s'appuyer sur le guide réalisé par le ministère de l'intérieur : "Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique".** **Ce guide est téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique.**
RSB 23-02	En appui des forces sécurité intérieures, appel aux armées po la protection des populations dans les zones publiques identifiées.	A l'appréciation des préfets de zone de défense et de sécurité selon les nouvelles modalités du dispositif Sentinelle. Les patrouilles des armées pourront être réorientées pour prendre en compte les principaux événements propres à la période couverte par la posture **« Été-rentrée 2019 »**.
BAT 21-01 BAT 22-01 BAT 23-01	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	BAT 21-01 Les contrôles de l'accès des personnes à l'entrée des établissements, notamment d'enseignement, est maintenu. Les dispositifs de sécurité des espaces privilégient la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance. L'effort de contrôle systématique aux accès des espaces touristiques, culturels et de loisirs est maintenu.
BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	**Renforcement de la surveillance interne dans les organes de presse, les sites touristiques culturels et de loisir, les écoles - en particulier les écoles confessionnelles - les bâtiments officiels. Les dispositifs de sécurité des espaces de commerce privilégient la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance.**
IMD 10-01	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités	Signaler tous vols, disparitions ou transactions suspects de précurseurs d'explosifs (articles L. 2351-1 et R. 2351-1 et suivant la défense) et/ou d'agents chimiques dangereux (articles R. 5132-58 et 59 du code de la santé publique) au point de contact national : pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tel (H/24): 01.78.47.34.29 Références code de la santé publique : Articles R5132-58 et R5132-59
NUM 31-09	Rappeler l'importance d'une mesure d'hygiène ou sectorielle existante	**Il s'agit ici d'appliquer une politique de mot de passe suffisamment robuste et de ne pas utiliser les mots de passe par défaut ou facilement devinable afin d'éviter d'être la cible de password spraying.** **Le password spraying est une technique d'attaque consistant à tester quelques mots de passe faibles sur un nombre très large de comptes utilisateurs. L'intérêt de cette attaque réside dans le fait qu'elle rend les mesures de sécurité habituelles (captcha, blocage des comptes, temporisation entre des essais successifs) inefficaces. Par ailleurs, cette**

		famille d'attaque est encore assez peu souvent détectée, ce qui lui permet de réussir tout en restant sous le radar de la détection.
NUM 41-01	Valider et appliquer un correctif de sécurité	**Les correctifs de sécurité correspondant aux bulletins du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :** **- CERTFR-2019-ALE-002 (www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-002) – Vulnérabilités affectant l'écosystème MICROSOFT Exchange et Active Directory** **- CERTFR-2018-ALE-013 (www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-013) – Vulnérabilité dans MICROSOFT Internet Explorer** **- CERTFR-2019-AVI-090 (www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-090) – Multiples vulnérabilités dans GOOGLE Chrome**
NUM 41-02	Vérifier la correction effective d'une vulnérabilité	**Face aux récentes vulnérabilités affectant Microsoft Exchange et aux nouveaux scénarios d'attaque touchant l'Active Directory, l'ANSSI souhaite contrôler le niveau de sécurité des annuaires de chaque Opérateur d'Importance Vitale et de chaque ministère afin d'y déceler les défauts de configuration les plus habituels qui affaiblissent le niveau de sécurité et de vérifier, quand c'est possible, que les composants Microsoft Exchange sont bien à jour. A cette fin, l'ANSSI a publié en source ouverte un outil de collecte (Outil de récupération automatique de données de l'Active Directory - ORADAD). L'ANSSI s'engage à fournir un rapport, sous forme électronique, sous quinze jours, avec des recommandations à mettre en place pour améliorer significativement le niveau de sécurité et faire face à cette tendance de prise de contrôle du SI par le contrôle de l'annuaire Active Directory.** **La procédure à suivre est la suivante :** **• Télécharger la dernière version de l'outil de collecte ORADAD disponible sur GitHub [https://github.com/ANSSI-FR/ORADAD/releases]** **• Extraire les fichiers (exécutable ORADAD.exe et fichier de configuration)** **• Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à exécuter : ORADAD.exe <outputDirectory>]** **• Envoyer le fichier contenant les résultats de la collecte (et présent dans le répertoire <outputDirectory>) par email à l'adresse club@ssi.gouv.fr . Si la taille du fichier de collecte est supérieure à 10 Mo, l'ANSSI met à disposition du bénéficiaire un serveur d'upload sur lequel le bénéficiaire peut déposer le fichier contenant les résultats de la collecte. L'URL et les comptes permettant d'accéder au serveur seront fournis à la demande (adresser la demande par email à club@ssi.gouv.fr)**
NUM 51-02 NUM 52-02	Adapter les dispositifs de	**Compte tenu de la menace persistante liée aux programmes malveillants portant atteinte en intégrité se propageant sur les systèmes d'exploitation**

	réponse à incidents aux caractéristiques de la menace	**(rançongiciels), il est nécessaire de s'assurer que le plan de continuité d'activité (PCA) est opérationnel et que le personnel chargé de le mettre en œuvre est familiarisé avec celui-ci. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA si le dernier exercice a été effectué il y a plus d'un an.**
NUM 51-06	**Procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques**	**Compte tenu de la menace persistante liée aux programmes malveillants portant atteinte à l'intégrité et se propageant sur les systèmes d'information (rançongiciels), il est nécessaire d'être en capacité de restaurer le bon fonctionnement des systèmes les plus critiques en cas de destruction ou d'altération des données par un programme automatisé en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration.**