POSTURE « TRANSITION 2017-2018 »

MESURES PUBLIQUES (1/5)

Action	Libellé mesure	Commentaires	N° mesure
Informer Sensibiliser Informer Alerter	Diffuser l'alerte au grand public	**Activation des cellules de veille et de crise laissée à 'appréciation des autorités académiques ou des établissement d'enseignement supérieur et de recherche** **RAPPEL** - Afficher le logo du niveau ***« sécurité renforcée-risque attentat »*** à l'entrée des sites accueillant du public.  Ces logos doivent être affichés à l'entrée et dans les espaces d'attentes des sites accueillant du public et peuvent être complétés d'une fiche synthétique récapitulant les conditions particulières de sécurité au sein de la structure. L'utilisation du logo ***« urgence attentat »*** fera l'objet d'instructions particulières en cas d'activation de ce niveau.  - Encourager et organiser la remontée des signes pouvant précéder une crise ou un attentat : comportements anormaux de personnes ou de véhicules, repérages, bagages ou colis abandonnés, etc. - Recommander le téléchargement de l'application pour Smartphone "Système d'alerte et d'information des populations" (SAIP) : http://www.gouvernement.fr/appli-alerte-saip	ALR 11-02 ALR 11-04

Sensibiliser Informer Alerter	Sensibiliser le personnel aux mesures de cybersécurité, demeurer vigilant sur les courriels reçus, ne pas ouvrir les pièces jointes suspectes, limiter les navigations internet aux seuls rapports professionnels	-Responsabiliser le personnel. 1) En rappelant aux utilisateurs les points suivants : - mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux - demeurer vigilants sur les courriels reçus dont l'origine n'est pas certaine. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant. Vérification de l'origine, analyse antivirus, ou ouverture dans un environnement dédié - minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ; - Signaler toute suspicion d'attaque,rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail. 2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. B) Protéger logiquement ses systèmes d'information en conduisant dans les meilleurs délais les actions suivantes : - Appliquer en priorité les mises à jour des postes utilisateur, en particulier antivirus, le système d'exploitation et le navigateur internet et les greffons (flash, java, etc). - Appliquer le filtrage des pièces jointes aux messages en fonction de leur extension. - Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires. Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR 1. guide d'hygiène : http://.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique. 2. Guide de bonnes pratiques : http://ssi.gouv.fr/entreptrie/guide/guide-des-bonnes-pratiques-de-informatique/ Dénis de service-Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001 3. Sécurisation des sites web : http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/ 4. Comprendre et anticiper les attaques en DDos : http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les- attaques-ddos/ 5. Défiguration dénis de services : www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateus.pdf, 6. Cyberattaques, prévention, réaction :	CYB

		www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf 7. Conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002 8. Défiguration de sites : www.cert.ssi.gouv.fr/site/CERTA-INF-002 9. Mesures de prévention relatives à la messagerie : www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002 10. Politique de restrictions logicielles sous Windows : www.ssi.gouv.fr/entreprise/guide:recommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows **Notifications d'incidents :** **www.ssi.gouv.fr/agence/contacts/cossicert-fr**	

Action	Libellé mesure	Commentaires	N° mesure
Surveiller Protéger	Renforcer la surveillance et le contrôle	***Manifestations en extérieur :*** Effort particulier de vigilance à porter : -aux activités culturelles, conférences, congrés, - aux activités sportives ; - aux activités et aux déplacements de groupes de mineurs. - Ces dispositions ne font pas obstacle à la liberté de l'organisateur de renoncer à la tenue d'une manifestation dès lors qu'il le juge nécessaire, soit parce qu'il estime ne pas être en mesure de satisfaire pleinement à ces obligations de sécurité du public ou des participants, soit en fonction de circonstances liées notamment à la thématique de la manifestation. Un contact avec les services de sécurité intérieure locaux est recommandé afin d'aider les organisateurs dans leur appréciation du risque.	RSB 11-01 RSB 12-01 RSB 13-01 **RSB 20-03** **(nouvelle mesure)**
	Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés	En lien avec les préfectures, renforcement de la vigilance	BAT 11-02 BAT 12-02 BAT 13-02
	Renforcer la surveillance aux abords des installations et	La sensibilisation à la détection et au signalement de comportements suspects doit être réalisée.	BAT 11-03 BAT 12-03 **BAT 20-02** **(nouvelle mesure)**

	bâtiments désignés		
	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	Renforcement de la surveillance interne dans : - les bâtiments officiels. En s'appuyant sur les guides de bonnes pratiques. Pour les points d'importance vitale relevant du secteur.	BAT 31-01
	Renforcer le niveau de sécurité des systèmes d'information	*www.ssi.gouv.fr:en-cas-d'incident*	CYB

Action	Libellé mesure	Commentaires	N° mesure
Surveiller Protéger	Renforcer la protection contre les intrusions dans les systèmes d'information Renforcer la protection contre les attaques en déni de service	Appliquer en priorité les mises à jour des postes utilisateur et les systèmes d'information utilisés ; Appliquer des règles de filtrage entre les réseaux (interne et externe) ; Limiter les impacts d'une attaque en déni de service, Mettre en place des sauvegardes régulières de toutes les données critiques. Élever la fréquence de sauvegarde à un niveau permettant la reprise des activités en cas d'altération des données.	CYB 42-01 CYB 42-02 CYB 43-01 CYB 43-02
Contrôler	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	Contrôles renforcés aux accès des : Maintien et renforcement supplémentaire du contrôle des accès dans les bâtiments universitaires et de recherche, les écoles, les bâtiments officiels. Le ciblage, les modalités et l'intensité de ce contrôle sont à définir par les chefs d'établissement, les présidents d'universités, les directeurs d'organismes, en lien avec les préfectures et les autorités administratives ou académiques. Dans la mesure du possible, les contrôles doivent être au moins aléatoires sinon systématiques. Les contrôles peuvent se traduire par des inspections visuelles des sacs, des filtrages des entrées, une présence renforcée des services de sécurité. Sur l'ensemble du territoire, renforcement supplémentaire dans les lieux de culte, écoles confessionnelles, établissements culturels et symboliques sensibles des diverses confessions religieuses. Une attention particulière au contrôle des accès sera portée lors des manifestations pouvant se dérouler dans l'enceinte des établissements (journées portes ouvertes, congrés, conférences , inscriptions universitaires…). Ces manifestations doivent être signalées à la préfecture et	BAT 21-01 BAT 22-01 BAT 23-01 BAT 31-01 RSB 23-02

		au rectorat. *Les mesures de contrôle peuvent notamment consister en des dispositifs de filtrage et d'inspection visuelle des sacs.*	
Alerter ontrôler Alerter	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 suspectes de précurseurs d'explosifs et agents NRBC au point de contact national : - pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tél H/24 : 01.78.47.34.29. et au service spécialisé du HFDS : Etablir et mettre à jour les plans particuliers de protections (PPP), les Plans d'Opérations Internes (POI) les Plans d'Urgences Interne (PUI) les Plans de Protections Externes (PPE)relatifs au transport de marchandises dangereuses à hauts risques. Tenir à jour les	IMD 10-06 IMD 10-02
Protéger les structures OIV	Protéger les établissements Site SEVESO	Les directeurs des établissements 'enseignement supérieur et de recherche doivent poursuivent les efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE), le renforcement des relations avec les préfectures et les forces de sécurité intérieure et la mise en œuvre d'actions de formations à l'intention de l'ensemble de leur personnel.	

NB : Les mesures sont numérotées avec les critères suivants :

- trigramme de domaine :

ALR : Alerte	BAT : Installations et bâtiments
CYB : CYBER	IMD : Installations et matières dangereuses
RSB : Rassemblements et zones ouvertes au public	

- numéro d'ordre (dans le tableau du plan Vigipirate) de la mesure de 01 à 0x pour les mesures du socle et de 01 à 0x pour les mesures additionnelles.

Exemple : la mesure BAT 13-04 : est une mesure du secteur installations et bâtiments (BAT), s'inscrit dans le 1er objectif du secteur (adapter la sûreté externe).