Diffusion : DRAAF/CMDSZ le 23 novembre 2015 actu N°10

Protection des établissements d'enseignement agricole sur l'ensemble du territoire

Renforcement des mesures de vigilance et de protection en fonction de la sensibilité des lieux, dans toutes leurs composantes (ALR, BAT, RSB, missions EXT, CYBER)

Suspension des déplacements scolaires à l'exception des voyages scolaires hors Ile-de-France

Maintien de mesures de vigilance renforcée

L'interdiction de rassemblements de grande ampleur quelle qu'en soit la nature pourra être prononcée par les autorités préfectorales en fonction de leur appréciation.

ALR alerte ; bat protection bâtiments ; RSB rassemblements ; EXT déplacements étranger ; CYBER sécurité informatique

1- Rappel du cadre général applicable dans les établissements d'enseignement

Sécurisation générale de base des établissements et dispositif de permanences.

Objectifs : surveiller, contrôler et filtrer les entrées et la circulation dans les bâtiments et enceintes des établissements de manière à identifier toute personne ou objet suspect et être en mesure soit d'empêcher l'accès, soit de donner l'alerte et mettre la population à l'abri en cas d'intrusion ou de flagrant délit.

.Mesures :

- *adapter la sûreté des accès en surveillant les accès des personnes, des véhicules et objets entrant dans l'établissement) ;*
- *adapter la sûreté interne en réglementant l'accès aux zones internes sensibles, en surveillant la circulation interne;*
- *dans les sites les plus sensibles, ou dans l'ensemble des établissements en cas de situation correspondant à un niveau d'alerte renforcée, contrôler les entrées des personnes, des véhicules ou des objets entrants (dont le courrier) par des inspections visuelles ou fouilles avec le consentement des intéressés*
- *En cas de péril imminent, dans un contexte d'alerte attentat mettre en sûreté les élèves, les étudiants ou si cela s'avère nécessaire, fermer préventivement l'établissement en liaison avec l'autorité académique et préfectorale.*

Recommandations permanentes de sécurité :

- *Contrôler les clôtures et systèmes d'alarme ou de surveillance, vérifier les dispositifs d'évacuation rapide ;*

- *Signaler aux autorités ou aux responsables de site tout élément suspect (bagage abandonné, véhicule ou comportement suspect, lettre ou colis suspect) y compris aux abords de l'établissement ;*
- *Se conformer aux consignes permanentes ou ponctuelles de sécurité émanant de l'autorité académique ou du préfet.*

2- Analyse de la menace

Instructions du Premier Ministre suite aux attentats du 13 novembre.

3. Mise en œuvre territoriale

Les mesures de protection, surveillance et contrôle sont renforcées dans l'ensemble des composantes du plan *ALR, BAT, RSB, missions EXT, CYBER* :

En particulier :

- la vérification et test des chaînes d'alerte locales et ministérielles
- **la vérification des dispositifs de protection des produits sensibles et dangereux qui doivent faire l'objet d'une supervision**
- **le contrôle des flux entrants et internes qui doit être assuré selon des procédures ad hoc, y compris pour les différentes opérations de livraison (dont le courrier) ; il est notamment rappelé que les agents de surveillance pourront refuser l'accès aux bâtiments qu'ils surveillent à une personne qui refuse de se soumettre à l'inspection visuelle de son bagage à main ou à la fouille de ce bagage avec consentement de la personne ; cette interdiction repose sur le règlement intérieur du lieu.**
- la tenue à jour d'un système d'enregistrement des effectifs présents – jours ouvrés ou non- , des missions et voyages programmés ainsi que des événements programmés dans l'enceinte des établissements qui doit pouvoir être mis à disposition des autorités en cas d'urgence de sécurité
- compte tenu de la dégradation de la situation sécuritaire dans différents pays un pilotage des missions d'apprenants à l'étranger qui doit être renforcé (cf circulaire DGER).

Les responsables d'établissements veillent à anticiper une application durable des mesures VGPRT.

4- Posture de sécurité dans les établissements d'enseignement sur l'ensemble du territoire national :

Il est demandé aux sites et établissements sous tutelle du MAAF de :

- *Renforcer la surveillance des abords des établissements avec la plus grande attention (augmentation des rondes), le cas échéant restreindre voire interdire les activités aux abords de bâtiments ou installations désignés (BAT 12-01)*
- *Contrôler les systèmes de protection des fermetures des bâtiments*
- De renforcer les mesures de contrôle des accès (mesure BAT 23-01): la vigilance sera toute particulière en Ile-de-France

Il s'agira notamment de

Renforcer la surveillance des entrées piétons et des véhicules, bâtiments et résidences ;

Contrôler l'accès de tous les véhicules n'ayant pas autorisation permanente d'accès

Détecter tout élément suspect notamment dans les parkings (risque d'engins improvisés)

L'attention est également rappelée sur la surveillance interne (mesure BAT 31-01) et à toute situation anormale.

Ces mesures de renforcement s'appliquent jusqu'à nouvel ordre sur l'ensemble du territoire national.

Les renforcements des dispositions liées à la sécurisation des établissements ne doivent en aucun cas contrarier l'éventuel besoin d'évacuation. Il est donc demandé aux responsables d'établissements :

- **de s'assurer que les dispositifs d'évacuation (signalétique, alarmes, portes…) sont opérants (fonctionnement et dégagements des cheminements d'évacuation) ;**
- **De rappeler les procédures liées à l'incendie et plus particulièrement celles spécifiques à l'évacuation à leur personnel.**

5- Consignes *en matière de déplacements d'apprenants :*

5.1 Voyages scolaires

Sont suspendus les déplacements et sorties scolaires jusqu'au 29 novembre 2015 inclus, à l'exception des voyages scolaires hors Ile-de-France : les établissements scolaires ont alors pour obligation de signaler en amont ces voyages à leur autorité académique. En lien avec les préfets, celle-ci peut interdire un déplacement ou une sortie scolaire ne remplissant pas les conditions de sécurité.

Les déplacements et sorties scolaires à destination de l'Ile-de-France sont interdits jusqu'au 29 novembre 2015.

Les déplacements et sorties scolaires nécessitant un transit en Ile de France peuvent toutefois être autorisés, après validation de l'autorité académique, au vu des conditions de sécurité.

Pour les déplacements et sorties scolaires à l'étranger, les consignes de la note de service DGER/SDRICI/2015-524 du 16 juin 2015 doivent être strictement observées.

Enfin, les déplacements et sorties scolaires liés à la COP 21 en région Île-de-France sont annulés.

5.2 Sessions publiques d'accueil dans des établissements

Des mesures spécifiques devront être envisagées pour toute opération « journée porte ouverte » scientifique, sociale ou culturelle éventuellement organisée par les établissements sous tutelle du MAAF.

***Po*ur ce type d'événement, le dispositif de contrôle des flux doit être suffisamment dimensionné de manière à assurer la meilleure fluidité possible et d'éviter également d'éventuelles sources de vulnérabilité supplémentaires liées à des groupes de personnes en attente.**

Le contrôle des accès comporte un filtrage avec individualisation des entrées (contrôle visuel des sacs des visiteurs).Les zones d'accès au public seront clairement canalisées et placées sous surveillance permanente afin de repérer tout comportement ou objet suspect. Les moyens affectés à la surveillance doivent par conséquent être correctement adaptés au contrôle des flux internes.

Les Préfets seront systématiquement informés des projets d'organisation de manifestations ouvertes ou public (colloques, journées portes ouvertes..), pour évaluation des risques potentiels.

6- Autres mesures :

La chaîne SSI a été également mobilisée afin de procéder à la remontée des problèmes divers de disponibilité/intégrité de sites informatiques dont pourraient être victimes les établissements sous tutelle du MAAF ; les RSSI des établissements rendront compte le cas échéant aux ASSI/DRAAF lesquels restent en liaison régulière avec la SDSI et le FSSI de la Mission défense.

Enfin, il est demandé aux responsables d'établissements d'assurer la plus large diffusion des bonnes pratiques de cyber sécurité qui impliquent l'ensemble de la collectivité de travail voir lien guide : http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf

Recommandations de SSI de base :

Responsabiliser le personnel.

1. En rappelant aux utilisateurs les points suivants :

   - demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ;

   - minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;
   - 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.

Protéger logiquement ses systèmes d'information

En conduisant dans les meilleurs délais les actions suivantes :
- assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision
- contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ;

- vérifier ou mettre en place les mesures de prévention en matière de déni de service.

Protéger logiquement ses systèmes d'information - Base documentaire :

Notes d'information du site www.cert.ssi.gouv.fr, notamment :
- [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ;
- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;
- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;
- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.
- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet
- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion
Guide du site de l'ANSSI, notamment :
- [f] www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.
- [g] www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques.
[a] sécurisation des sites Internet : www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web
[b] attaques par défiguration : www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration
[c] comprendre et anticiper les attaques en déni de service : www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos
[d] conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002