CAMPUS RISQUE

NOTES TECHNIQUES

N°1 - Octobre 2015

Intrusions malveillantes

Directeur Hubert SEILLAN

Michel Ledoux & Associés
10, rue Portalis 75008 PARIS
Tél. : 01 44 90 98 98 - Fax : 01 42 93 97 28
ml@michel-ledoux.fr - www.michel-ledoux.fr

LES NOTES TECHNIQUES

N°1 - Octobre 2015

Les avocats et juristes du cabinet sont souvent questionnés sur des sujets de sécurité variés. Grâce à notre nouvelle organisation de Campus Risque nous allons publier, en tant que de besoin, des fiches techniques, allant à l'essentiel et aidant à avoir une vision panoramique de la question traitée. Il s'agit de fiches, et non d'études approfondies. Leur présentation sommaire et fortement structurée s'explique par notre souci de faciliter une appréhension globale rapide de chaque question.

Les lecteurs de ces Notes sont invités à nous faire part :

- De leurs commentaires et réflexions, que nous pourrons publier s'ils nous accordent leur autorisation ;
- De leurs besoins d'information et de formation sur des sujets particuliers.

Le cabinet est en mesure de leur apporter un appui actif et pluridisciplinaire si nécessaire.

INTRUSIONS MALVEILLANTES

Le sujet de cette 1ère Note Technique s'imposait en raison de la crainte que les intrusions criminelles suscitent chez les pouvoirs publics, les exploitants de sites à risques et plus généralement chez les dirigeants des entreprises et des collectivités. Les exercices qui se multiplient ajoutent à l'inquiétude.

L'attaque spectaculaire et très meurtrière en janvier 2013 de la base gazière de Tiguentourine dans le sud-est de l'Algérie un groupe terroriste multinational avait donné la mesure du risque.

Au début de cette année, nous apprenions que les comptes Twitter et YouTube du commandement militaire des Etats-Unis au Moyen-Orient, basé en Floride, ont été piratés par des hackers se réclamant du groupe Etat islamique.

Pour la France, mentionnons brièvement les cas suivants :

- Fin juin, en Isère un chef d'entreprise a été décapité avant que le terroriste ne tente de faire exploser des citernes de gaz.
- En juillet, 180 détonateurs - électroniques et pyrotechniques - ainsi qu'au moins une dizaine de pains de plastic et une quarantaine de grenades» dépôt militaire à Miramas dans les Bouches-du-Rhône.
- Ce même mois, une vingtaine de militants de Greenpeace ont pénétré dans la centrale nucléaire du Tricastin, dans la Drôme, dans l'intention de pointer des failles de sécurité.

La sûreté des sites Seveso et des sites nucléaires fait l'objet de l'attention la plus soutenue des pouvoirs publics.

Hubert SEILLAN et Laurent JACOB

Michel Ledoux & Associés
10, rue Portalis 75008 PARIS
Tél. : 01 44 90 98 98 - Fax : 01 42 93 97 28
ml@michel-ledoux.fr - www.michel-ledoux.fr

I- DE QUOI S'AGIT-IL ?

- D'un phénomène doublement illicite. L'intrusion est le fait de pénétrer dans un espace donné sans en avoir le droit. La malveillance correspond à l'intention de nuire.
- D'un phénomène en profonde et rapide mutation. Du fait du développement des terrorismes, des insatisfactions sociales, de la concurrence mondialisée et de l'inadaptation et donc de la vulnérabilité de nos systèmes de gestion des risques - centrales nucléaires, usines chimiques, réseaux etc.
- D'un phénomène qui peut être prévenu car il peut être envisagé, imaginé. Mais c'est un phénomène particulier, car mené par des intelligences et non des lois physiques répétitifs connues, ou des actions de force en masse. Il doit donc être traité différemment de tous les autres risques du fait de cette nature.
- D'un phénomène caractérisé : intrusions dans les systèmes numériques, dans les cerveaux des dirigeants par l'installation de puces et aussi la mise en confiance, physiques sur un site sensible, attaques physiques externes -sans intrusion directe, attaques venant de personnes travaillant sur le site -sans intrusion directe.

II- LA DÉMARCHE

- Créer une organisation adaptée au phénomène : une cellule spécialisée, autonome, isolée pour des raisons de discrétion dont la mission est d'élaborer une stratégie, d'analyser et de mobilisation de l'ensemble des moyens humains autour de ses objectifs, de proposer un plan d'action et d'en évaluer en continu la qualité.
- Adopter une stratégie bâtie sur des scenarii. Ceux-ci prennent en compte les cibles -personnes, équipements, biens matériels et immatériels, image etc., les sources - internes, externes, numériques etc., les intentionS -terroriste, économique, sociale, personnelle etc..
- Analyser ses points faibles et de ses points forts – Techniques, Humains, Organisationnels.
- Elaborer plan d'action global visant deux types principaux d'objectifs : réduction des points faibles et renforcement des points forts ; développement d'une capacité collective, en particulier de remontée des signaux faibles.
- Retenir le principe du doute méthodique comme support de la démarche. Sous-évaluer ses capacités, analyser le fonctionnement réel et tous les événements même vus comme signaux très faibles, avoir un regard froid sur sa vulnérabilité et sa résilience.externes -sans intrusion directe, attaques venant de personnes travaillant sur le site -sans intrusion directe.
- Avoir une capacité de réaction rapide face à la détection de signaux faibles.

III- SUGGESTIONS PRATIQUES

- Enseignements des retours d'expérience : Avoir à l'esprit que l'impossible est possible et qu'un point jugé fort peut être un point faible, que la mobilisation collective selon un mode participatif à sens unique est une valeur ajoutée, que les capacités d'imagination et d'intuition doivent être activées régulièrement
- Priorité à l'intuition : il y a toujours quelques failles dans les règles et l'auteur des intrusions va essayer de les détecter et chercher à s'y engouffrer
- La discrétion, condition première du plan d'action : l'auteur des attaques est toujours invisible et bien implanté ; annoncer le plan, c'est lui donner les clés.

Michel Ledoux & Associés
10, rue Portalis 75008 PARIS
Tél. : 01 44 90 98 98 - Fax : 01 42 93 97 28
ml@michel-ledoux.fr - www.michel-ledoux.fr