AUDIT GLOBAL DE SITUATION

Risques sécuritaires du dirigeant

PRÉSENTATION

DESCRIPTION DE L'OFFRE

Cet audit global, véritable « due diligence » de sûreté, a pour finalité de permettre aux dirigeants de l'entreprise, et au premier chef à son Président, de mesurer la nature et l'ampleur des risques, en termes de sûreté, pesant sur eux-mêmes à raison de leur activité professionnelle, à tous les moments de leur existence (y compris dans leur vie privée), ainsi que les conséquences en découlant pour l'entreprise.

PRINCIPAUX OBJECTIFS

L'audit doit vous permettre de disposer des éléments suivants :

- Une analyse de la sûreté de votre environnement direct (locaux professionnels et résidences, véhicules, communications) ;
- Une analyse de votre « e-réputation » et de celle de votre entreprise (y compris au regard d'éventuelles menaces du type « terrorisme » ou « crime organisé ») ;
- Une analyse du profil d'agressivité de vos concurrents et votre environnement social ;
- Une analyse des empreintes numériques à risques.

PRINCIPAUX MOYENS MIS EN ŒUVRE

- Audit bâtimentaire ;
- OSE (opérations de sécurité électronique dites de « dépoussiérage »), incluant les véhicules utilisés ;
- Test d'intrusion de cyber-sécurité ;
- Fiche « people analytics » du dirigeant ;
- Empreinte numérique positive et négative ;
- Analyse de la concurrence ;
- Analyse des facteurs sociaux de risque (type d'action syndicale, personnes licenciées…).

LES SOCIÉTÉS PRESTATAIRES

Diomède Groupe (deux sociétés, l'une notamment dédiée aux différents audits de sûreté, l'autre à la protection rapprochée).

PERSONNE-CLEF ET PERSONNES REFERENTES

Gilles Marchandon, ENS Ulm, ENA (promotion Voltaire), contrôleur général économique et financier honoraire, Président du Groupe Diomède.

Jacques Poinas, Sciences Po Paris, Ecole Nationale Supérieure de Police, inspecteur général honoraire, Consultant expert en sécurité en France et à l'international ;

Jacky Le Pemp, Ecole des Officiers de la Gendarmerie Nationale, Université de Nice Sophia-Antipolis, lieutenant-colonel de Gendarmerie (ER), chef de projet sûreté à l'international (CIVIPOL).

PROCÉDURES ET GARANTIES

En raison de la « sensibilité » particulière du service proposé, la « personne-clef » mentionnée ci-dessus s'engage à superviser et contrôler de bout en bout le déroulement de l'audit global de situation, et à établir elle-même le rapport final (ou à en contrôler entièrement la rédaction) issu dudit audit.

CONTENU DU RAPPORT FINAL

Le rapport final, conclusion de « l'audit global de situation – risque sécuritaire du dirigeant », est un rapport d'évaluation des risques encourus, en termes de sûreté, par le ou les dirigeants concernés, sa ou leur famille, et conséquemment par l'entreprise concernée. Sa composition, dépendant des situations particulières, ne peut évidemment être établie ne varietur.

Toutefois, nous nous engageons à ce qu'il comporte, au minimum :

- Le classement de la situation analysée sur une échelle des risques comportant cinq degrés ;
- Une cartographie des risques établie sous forme d'un tableau « heuristique » ;
- De premières préconisations ;
- Une mise en forme des conclusions, « opposable » aux autorités fiscales et aux actionnaires minoritaires, dans l'hypothèse de dépenses significatives exposées par la société pour la protection de son dirigeant, voire de la famille de ce dernier.

AUDIT BÂTIMENTAIRE

▶ Objectif :

Identification des menaces périphériques ;
Identification des vulnérabilités (menaces technologiques, menaces naturelles) ;
Identifications des particularismes locaux (économiques, sociaux et culturels);
Mise en évidence des « porosités » de sûreté.

▶ Méthode :

* Analyse de l'environnement immédiat ;
* Analyse périphérique ;
* Analyse périmétrique ;
* Evaluation du contrôle d'accès ;
* Evaluation du poste central de sécurité ;
* Analyse de l'autonomie du site ; Revue des procédures existantes (consignes générales de sécurité) ;
* Analyse des systèmes de communication ;
* Intrusion (le cas échéant).

OPÉRATIONS DE SÉCURITÉ ÉLECTRONIQUE (OSE)

▶ Objectifs :

Sécurisation de l'environnement électronique ;
Sécurisation des communications ;
Inhibition de tout système d'écoute ou de surveillance clandestin.

▶ Méthode :

* Détection électronique de capteurs d'ambiance ;
* Recherche électronique des sources infrarouges, wifi et bluetooth par capteurs spécialisés ;
* Recherche électronique de micros émetteurs, d'enregistreurs dissimulés, d'écoutes filaires à distance ;
* Recherche de micros GSM et d'enregistreurs/émetteurs GSM ;
* Protection électronique par des dispositifs de brouillage (le cas échéant).

EMPREINTES NUMÉRIQUES

▶ Objectif :

Permettre au décideur d'avoir tous les éléments d'aide à la compréhension de son écosystème et des risques, menaces s'y rattachant.

Analyse e-réputation : recherche et analyse de la e-réputation du dirigeant dans le Big Data :

* fiche *People analytics* du dirigeant : vision des informations qu'une personne malveillante pourrait avoir sur le dirigeant par les sources ouvertes ;
* empreinte numérique, positive et négative du dirigeant, de sa (ses) société (s), de ses proches collaborateurs et de son cercle familial ;
* niveau de risque lié à l'information disponible sur le dirigeant et ses proches collaborateurs pouvant mener à des actions néfastes (arnaque au président, chantage médiatique ...).

Stratégie d'influence

* Recherche des influenceurs qui s'expriment sur le dirigeant et son entreprise ;
* Mise en veille des influenceurs (3 mois).

Cartographie des risques

* La cartographie de l'activité, de l'environnement, des réseaux d'une entité ou d'une personne est indispensable à la bonne visualisation et à la compréhension de l'ensemble des risques qui y sont associés.

▶ Méthode :

Nos analystes, en toute confidentialité, vont capter les empreintes numériques issues du Big Data grâce à notre logiciel de cyber-investigation e-Perion®. Ce logiciel « propriétaire » nous permet de réaliser nos études en toute autonomie sans possibilité pour des tiers de connaître nos sujets d'investigation. Une fois les empreintes numériques captées, elles sont analysées une par une, afin de comprendre le niveau d'intérêt ou de risque. Dans son rapport , l'analyste rend intelligible les données et propose après un travail en commun avec nos designers, un unique exemplaire en format « papier » (pour des raisons de sécurité) d'une carte heuristique qui permet une compréhension rapide et visuelle des résultats.

TEST D'INTRUSION CYBER-SÉCURITÉ

▶ Objectifs :

Simuler des attaques externes afin d'identifier et d'évaluer les vulnérabilités présentes dans vos systèmes d'information personnel et professionnel.

▶ Méthode :

* Nos ingénieurs vont pratiquer des tests d'intrusion de vos systèmes d'information ainsi que des tentatives de pénétrer dans vos systèmes (de la méthode whitebox à blackbox) comme les pratiquent les hackers (bien sûr avec votre autorisation). Chaque audit est accompagné d'un rapport complet et d'une proposition d'un ensemble de mesures correctives.

Diomède SAS
36 rue Ernest Renan 92190 Meudon
Tél : 06 63 27 70 37
marchandon@diomede.eu