NOTE DU CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Numéro 62 – Octobre 2021

Florence ESSELIN

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

EN OCTOBRE J'AGIS POUR LE CYBER MOIS

#cybermois

EBIOS RISK MANAGER : UNE MÉTHODE ACCESSIBLE POUR SÉCURISER LA TRANSFORMATION NUMÉRIQUE

Sous l'effet conjugué de la loi du marché et des politiques publiques, les organisations et les individus deviennent de plus en plus dépendants du « numérique » – des technologies, systèmes et services qui permettent de « dématérialiser » les biens et les personnes, de traiter et faire circuler en quelques instants des volumes colossaux d'informations dans un espace indépendant des frontières terrestres : le cyberespace.

Dans le cyberespace, la compétition mondiale permanente peut dégénérer en affrontement à tout moment ; la criminalité y est installée.

Ce contexte expose alors chaque individu – *a fortiori* chaque gendarme dans sa vie personnelle comme dans ses missions – à des risques qu'il faut savoir comprendre pour sa sécurité.

Procéder à une analyse de risque préalablement à la mise en œuvre d'un projet de transformation numérique, puis régulièrement pour prendre en compte l'évolution des cybermenaces, est bien plus qu'une recommandation ; dans de nombreux cas, c'est une obligation légale.

Cet article présente une méthode élaborée et recommandée par l'Agence nationale de sécurité des systèmes d'information (ANSSI) : EBIOS Risk Manager[1]. Quoique récente, son usage se répand rapidement ; ses points communs avec la méthode de raisonnement tactique (MRT), enseignée aux cadres des armées et de la gendarmerie, peuvent en faciliter l'adoption par les gendarmes dans leurs missions de prévention des cybermenaces et de protection dans le cyberespace.

I) Analyser les risques liés à la sécurité de l'information : recommandation ou obligation légale ?

Réserver un livre à la bibliothèque municipale sur le site Internet de sa commune, gérer son compte en banque depuis son PC à domicile, faire sa déclaration d'impôts en ligne, consulter un médecin à distance, réserver et payer une place de stationnement depuis son téléphone portable, déposer une pré-plainte en ligne, pouvoir à tout moment prendre rendez-vous auprès de la brigade de gendarmerie la plus proche, etc. Tous ces services assistés par l'informatique (téléservices) ont en commun une obligation d'analyse préalable des risques liés à la sécurité de l'information.

En effet, trois types de démarches rendues obligatoires pour certains secteurs ou du fait de la nature des données s'appuient sur une analyse de risque :

- l'homologation de sécurité : elle vise à « s'assurer, sur la base d'une analyse de risques globale, prenant en compte tous les éléments, y compris environnementaux, indispensables au fonctionnement et à la sécurité du système d'information (SI) considéré, que l'ensemble des risques a été identifié et fait l'objet d'un traitement approprié et que les risques résiduels sont acceptés ». Cette démarche est sanctionnée par une décision d'homologation qui engage la responsabilité de la personne physique désignée autorité d'homologation. Elle est obligatoire pour les systèmes d'information contenant des informations classifiées[2], mais aussi pour les téléservices mis en œuvre par les autorités administratives[3], pour tout système d'information

1 La méthode EBIOS Risk Manager [en ligne]. Disponible sur : https://www.ssi.gouv.fr/ebios.
2 Cf. Instruction générale interministérielle n° 1300.
3 Cf. Le référentiel général de sécurité, pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

de l'État[4], pour les systèmes d'information d'importance vitale[5], ainsi que pour les réseaux et systèmes d'information des opérateurs de services essentiels[6];
- l'analyse d'impact[7]: exigée par le règlement général sur la protection des données ainsi que par la directive européenne 2016/680 relative aux données de la « sphère pénale »[8], elle inclut une analyse de risque focalisée sur les données à caractère personnel ;
- la certification des systèmes d'information des hébergeurs de données de santé[9].

II) Le risque est la combinaison d'une menace et des pertes qu'elle peut engendrer

La notion de risque nous est familière depuis l'enfance : en effet, quel enfant n'a jamais tenté de braver une interdiction parentale en s'exposant à ses conséquences, dont une potentielle sanction, dans l'espoir d'un gain incertain ? Les normes NF, ISO 31000 relative au management du risque et ISO/IEC 27000 relative aux systèmes de management de la sécurité de l'information, en donnent une définition générale et des indications pour la préciser. Ainsi, un risque peut être présenté comme la combinaison d'une menace et des pertes qu'elle peut engendrer, occultant la potentialité d'une conséquence positive qui motive généralement une prise de risque. Définir plus précisément un risque lié à la sécurité des systèmes d'information (risque « cyber ») permet d'envisager son traitement en agissant sur un ou plusieurs de ses éléments. Ainsi, le risque « cyber » peut être défini comme l'opportunité que les vulnérabilités de « biens supports » (matériel informatique, logiciel, etc.) soient exploitées par une source de risque[10] visant un objectif et causant *in fine* un impact sur des « valeurs métier » (informations et processus ayant de forts besoins de protection) de l'entité atteinte. Un chemin d'attaque peut se bâtir sur les vulnérabilités intrinsèques au système d'information (SI) de l'entité et sur celles introduites par son interconnexion avec les SI de multiples parties prenantes (partenaire, hébergeur, etc.).

En quoi une méthode peut-elle être utile pour lutter contre la cybercriminalité ?
Tout comme la méthode de raisonnement tactique invite à analyser la situation avant de concevoir une manœuvre soumise à la décision du chef, la méthode EBIOS (expression des besoins et identification des objectifs de sécurité) permet d'apprécier les risques qui pèsent sur un projet numérique pour être en capacité de les traiter, c'est-à-dire de déterminer et de faire valider les actions à entreprendre et les moyens à mettre en œuvre pour renforcer sa sécurité et se préparer à faire face aux conséquences des risques résiduels.
C'est un outil de réflexion, de prévention et de protection, qui peut servir tant à la préparation de l'homologation de sécurité d'un projet informatique qu'à la mise en œuvre d'un processus interne de management du risque cyber pour l'ensemble du SI ; c'est aussi un outil de communication entre les parties prenantes de la transformation numérique. Enfin, maîtriser EBIOS Risk Manager peut aussi être un atout dans l'anticipation des scénarios d'évolution du volet cyber d'une crise, car cette version de la méthode EBIOS permet de définir rapidement des scénarios de risques de niveaux stratégique et opérationnel.

L'évolution d'EBIOS en 25 ans
La méthode EBIOS a été créée en 1995 au sein du service central de la sécurité des systèmes d'information du secrétariat général de la défense nationale, dont les héritiers sont respectivement l'ANSSI et le secrétariat général de la défense et la sécurité nationale. Cette méthode a été adoptée par les armées et la gendarmerie comme outil d'homologation de sécurité des systèmes d'informations classifiées et sensibles. Elle a évolué en tenant compte à la fois de la normalisation dans le domaine de la gestion des risques cyber (norme ISO 27005) et du retour d'expérience de l'ANSSI ainsi que du club EBIOS accueillant experts de la méthode, formateurs et éditeurs d'assistants logiciels pour la version EBIOS Risk Manager (RM).
Les premières versions d'EBIOS s'attachaient à identifier de façon exhaustive les différents éléments constitutifs d'un risque pour, d'une part, éliminer toutes les combinaisons invraisemblables ou d'impact négligeable et, d'autre part, déterminer sur quel(s) élément(s) agir pour réduire chaque risque.
Avec la version EBIOS RM présentée en octobre 2018, l'ANSSI a fait le pari d'une méthode orientée davantage vers l'étude des capacités de nuisance des acteurs de « l'écosystème » – amis et ennemis – et l'identification des scénarios d'attaque les plus significatifs. EBIOS RM abandonne l'inventaire exhaustif et souvent laborieux des vulnérabilités propres au SI à protéger et celui des menaces courantes peu sophistiquées, considérant qu'elles peuvent être compensées par l'application de mesures « d'hygiène informatique » constituant le « socle de sécurité ».
Cette approche est confortée par deux phénomènes :

4 Cf. la politique de sécurité des systèmes d'information de l'État, portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014.
5 Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du Code de la défense.
6 Cf. Art. 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, transposant la directive européenne *Network and Information System Security* (NIS) du 6 juillet 2016.
7 CNIL. *Analyse d'impact relative à la protection des données. Privacy Impact Assessment (*PIA) [en ligne]. Février 2018. Disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf.
8 EVANS, Mark. Les fichiers de sécurité : une exigence d'efficacité et une obligation de conformité [en ligne]. *Revue de la gendarmerie nationale*, décembre 2018, n° 263, p. 93-97. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-263.
9 Code de la santé publique, art. L.1111-8 modifié par la loi n° 2016-41 du 26 janvier 2016.
10 La source d'un risque peut être naturelle, animale, humaine involontaire ou malveillante avec des profils variés tels un fraudeur opportuniste, un concurrent déloyal, un proche vindicatif, un cyberdélinquant récidiviste, un cybermercenaire travaillant pour une officine, un groupe de cyberterroristes, etc. EBIOS RM étudie essentiellement les sources de risque humaines malveillantes.

- de nombreuses organisations ont généralement établi un socle de mesures de sécurité par nécessité de conformité à divers lois et règlements ; ces mesures doivent être prises en compte dans les nouveaux SI, sans les justifier par une analyse de risque ;
- corriger toutes les failles connues d'un SI est une tâche très ardue et d'efficacité limitée, car aux vulnérabilités et à leurs correctifs éventuels publiés chaque jour par les éditeurs et les centres d'alerte et de réaction aux attaques informatiques[11] s'ajoutent les failles qui ne sont pas encore rendues publiques mais peuvent être connues de cybercriminels (dites failles « jour zéro » ou « zero day »). Il faut corriger prioritairement les vulnérabilités qui peuvent être exploitées dans les scénarios d'attaque crédibles qui auraient le plus d'impact.

III) La méthode EBIOS Risk Manager : une démarche itérative articulée en cinq ateliers

EBIOS RM vise l'efficacité et non l'exhaustivité ; employée avec bon sens et agilité, en fonction de l'objectif de l'étude et de ses contraintes calendaires, elle nécessite d'impliquer dans ses divers « ateliers » un panel représentatif des parties intéressées par le SI à sécuriser.
La méthode, illustrée par l'étude du cas fictif d'une société de biotechnologie fabricant des vaccins, est exposée en détails dans un guide et son supplément disponibles sur le site de l'ANSSI (www.ssi.gouv.fr/ebios).

Atelier 1 – Cadrage et socle de sécurité
Dans le premier atelier, EBIOS RM invite à poser le cadre de l'étude, son périmètre, les métiers et entités concernés et tout autre élément de contexte utile. Dès cette étape, il est important d'exprimer les « événements redoutés », c'est-à-dire les situations que l'on veut éviter parce qu'elles auraient un impact négatif important.
Cet atelier est aussi l'occasion de recenser tout ce qui constitue le socle de sécurité (par exemple la politique de sécurité des systèmes d'information ou les règles de sécurité imposées au secteur d'activité considéré).
Les principales questions à se poser sont :
- quelles sont les missions de l'organisme ?
- quels sont les processus et informations essentiels à protéger (« valeurs métier ») ?
- quelles sont les parties prenantes du SI ?
- quels situations et dommages veut-on éviter prioritairement ?
- quelles sont les diverses contraintes (opérationnelles, légales, etc.) ?
- quelles sont les mesures de sécurité existantes ?

Atelier 2 – Sources de risques
EBIOS RM invite ensuite à identifier les « sources de menaces » et les « objectifs visés » par celles-ci. Les sources considérées dans EBIOS RM sont exclusivement humaines et malveillantes. Le postulat est que les autres sources (animales, naturelles, humaines involontaires) sont à l'origine de risques déjà couverts par le socle de sécurité ou portés par les parties prenantes étudiées à l'atelier 3.
Dans cet atelier, la connaissance qu'ont les gendarmes de la cybercriminalité est particulièrement précieuse. L'échelle BEPA-Cyber[12] [13]élaborée par des réservistes cyber de la gendarmerie peut aussi aider à diagnostiquer rapidement les sources de menaces et leurs capacités.

Atelier 3 – Scénarios stratégiques
EBIOS RM s'attache également à identifier tous les partenaires qui interagissent avec le SI à protéger mais qui sont hors de contrôle de l'organisme responsable du SI, ceci afin d'estimer le niveau de menace qu'ils apportent, puis les contre-mesures à prendre. Cette analyse est devenue une nécessité avec l'évolution des cybermenaces contre les grandes entreprises ou l'État ; en effet, ceux-ci ayant généralement mis en place des mesures de sécurité conséquentes ne laissant pénétrer dans leurs SI que des partenaires identifiés, la tactique des cybercriminels est souvent d'attaquer les partenaires plus petits et plus accessibles, pour atteindre finalement les entités visées.
Avec les résultats des ateliers précédents, il est alors possible de dresser une liste de scénarios d'attaques vraisemblables, pouvant causer des dommages importants s'ils atteignaient des « valeurs métier ».

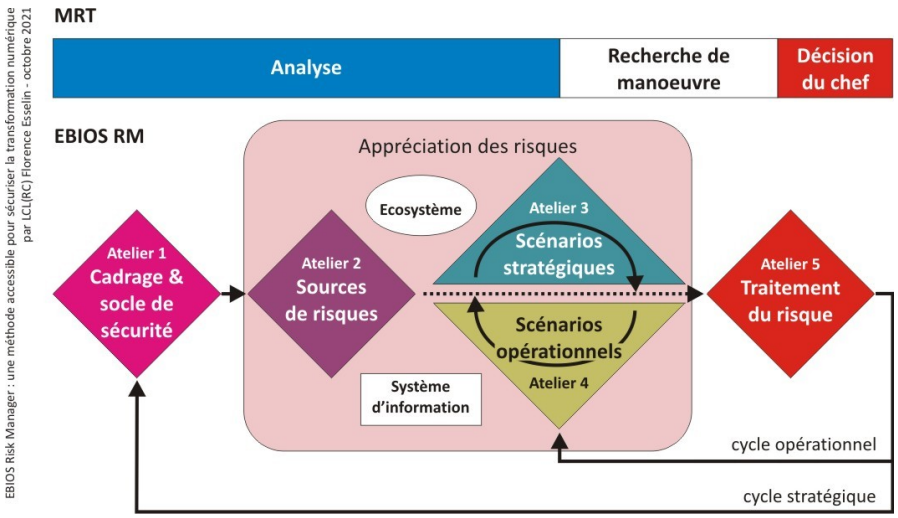
Atelier 4 – Scénarios opérationnels
Il reste à affiner chaque scénario stratégique en scénarios opérationnels, par la connaissance des modes opératoires des cybercriminels. Elle permet d'anticiper le cheminement d'un attaquant dans le SI selon ses capacités à exploiter les failles de diverses natures (techniques, procédurales, humaines). Les vulnérabilités des composants techniques du SI considéré (appelés « biens supports ») confèrent une vraisemblance à chacun des scénarios opérationnels.

11 CSIRT (*Computer Security Incident Response Team*).
12 ESSELIN, Florence, AUTRET, Thierry. BEPA-CYBER, la base d'estimation des potentiels d'attaques cyber [en ligne]. *Revue de la gendarmerie nationale*, décembre 2013, n° 248, p. 112-125. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/notre-communication/publications-documentations/la-revue/revue-248.
13 ESSELIN, Florence. De la résilience humaine à la résilience collective face aux cybercrises avec la BEPA-Cyber [en ligne]. *Revue de la gendarmerie nationale*, décembre 2019, n° 266, p. 65-74. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-266.

Atelier 5 – Traitement du risque
Grâce à cette analyse, on est en capacité de définir des mesures aptes à rendre impossible, sinon retarder, la progression de l'attaquant et le décourager.
On peut également enregistrer et surveiller spécifiquement des « points de passage » obligés, pour détecter des comportements anormaux. Le raisonnement dans cet espace dématérialisé emprunte alors beaucoup à la protection des biens et des personnes dans le monde réel.

Traiter les risques identifiés relève de décisions stratégiques :
- accepter un risque et ses conséquences ;
- réduire chaque risque en agissant sur une ou plusieurs de ses composantes pour en diminuer la vraisemblance ;
- transférer à un tiers de confiance une partie du risque ;
- abandonner tout ou partie d'un projet de transformation numérique pour éviter des risques inacceptables qu'on ne peut traiter autrement.

IV) Similitudes avec la méthode de raisonnement tactique (MRT)



EBIOS RM et la MRT présentent de nombreuses similitudes. En effet, l'atelier 1 s'inscrit dans l'étape d'analyse de la MRT, par l'étude du cadre général de l'action et la définition des rôles et missions. Les ateliers 2 et 3 (par l'identification des partie prenantes critiques) concourent aux bilans quantitatifs et qualitatifs des ennemis et amis de l'analyse MRT.
L'effet majeur recherché est alors défini par la connaissance des besoins de sécurité des « valeurs métier », des événements redoutés et des objectifs visés par les sources de risques.
La recherche de manœuvre s'appuie, quant à elle, sur les scénarios stratégiques et opérationnels déterminés aux ateliers 3 et 4.
Enfin, la décision du chef intervient dans le traitement du risque, à l'atelier 5 ; il nécessite la validation de la stratégie de traitement du risque et éclaire le chef sur les risques résiduels, en proposant un plan d'amélioration de la sécurité dans un cadre formalisé de suivi des risques.

V) Une méthode qui gagne

L'usage d'EBIOS RM s'étend en France au sein d'entités publiques et privées grâce au dispositif de labellisation porté par le Club EBIOS. La méthode est également promue au niveau européen ; l'évolution de la règlementation en matière de protection des intérêts économiques dans le cyberespace des pays membres de l'Union Européenne devrait développer l'analyse de risque dans la transformation numérique.
Si la méthode EBIOS RM est principalement employée pour prévenir les cyberattaques élaborées, son approche par scénarios et les similitudes qu'elle présente avec la MRT, employée pour structurer l'action opérationnelle dans un délai contraint, permettent d'envisager un développement de son usage pour l'anticipation dans les situations de crise.
Gageons alors qu'EBIOS Risk Manager intéressera, outre les officiers de sécurité des SI, les élèves officiers captivés par le numérique, les commandants d'unité promoteurs d'une innovation ayant une composante informatique, les référents conseillant les entreprises et les collectivités, les chefs de projets de transformation numérique et même tout gendarme soucieux de savoir quels risques il prend avec sa famille dans l'usage courant d'Internet et des réseaux sociaux.

Florence ESSELIN *est ingénieur diplômé, inspecteur à l'ANSSI, ancien conseiller expert en numérique et cybersécurité au cabinet du directeur général de la gendarmerie nationale (juillet 2018 - juin 2021), lieutenant-colonel de la réserve citoyenne de la gendarmerie nationale.*