G7 – ÉLÉMENTS FONDAMENTAUX POUR LES TESTS DE PÉNÉTRATION FONDÉS SUR LES MENACES

Résumé

Face à des risques cybernétiques de plus en plus sophistiqués et persistants, qui menacent de perturber nos systèmes financiers mondiaux interconnectés, et après la publication en 2016 du document *Groupe des sept – Éléments fondamentaux pour la cybersécurité du secteur financier*, le G7 continue de promouvoir le développement de cadres pour améliorer les approches retenues par les secteurs public et privé afin de renforcer la cyberrésilience des entités critiques du système financier.

Ces efforts comprennent un ensemble de pratiques ayant pour objectif de garantir la mise en place et l'évaluation de mesures fortes de cyberrésilience, comme souligné dans le document *Groupe des sept – Éléments fondamentaux pour l'évaluation efficace de la cybersécurité dans le secteur financier*, publié en 2017. Ce document contient des éléments qu'il convient d'examiner et de prendre en compte dans l'élaboration de cadres d'évaluation de la cyberrésilience.

Le présent document, *Groupe des sept – Éléments fondamentaux pour les tests de pénétration fondés sur les menaces*, constitue pour les entités un guide d'évaluation de leur résilience face à des cyberincidents malveillants simulés. Il fournit également une orientation à l'attention des autorités publiques qui envisagent de recourir, dans leur juridiction, à des tests de pénétration fondés sur les menaces (*Threat-Led Penetration Testing* en anglais, TPFM ci-après). Ces éléments fondamentaux visent à compléter un ensemble plus large d'outils et de techniques d'évaluation de la cyberrésilience, et n'ont pas vocation à être considérés comme une approche unique.

Les principaux objectifs des *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* sont de renforcer et d'évaluer la cyberrésilience des entités et, plus généralement, du secteur financier, en :

- définissant les éléments fondamentaux et les approches pour la réalisation des TPFM dans les différentes juridictions du G7. Les *Éléments* ont pour objet de favoriser une plus grande compatibilité des approches relatives aux TPFM, tout en encourageant la flexibilité et l'adaptation au niveau local en fonction des spécificités des marchés et des règlementations au sein de chaque juridiction;
- fournissant des orientations aux autorités qui envisagent de recourir aux TPFM dans leur juridiction;
- fournissant aux entités des orientations pour la réalisation de leurs propres évaluations des TPFM; et en
- favorisant l'interaction entre autorités ainsi que la conduite de TPMF impliquant plusieurs juridictions pour les entités multinationales, facilitant ainsi l'acceptation mutuelle des résultats des tests.

Les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* visent à favoriser une plus grande compatibilité des approches relatives aux TPFM sans remettre en question les cadres existants ni empêcher leur adaptation continue au paysage des cybermenaces.

En quoi consistent les TPFM ?

Les TPFM[1] consistent en ***une tentative maîtrisée de compromettre la cyberrésilience d'une entité en simulant les tactiques, les techniques et les procédures utilisées par de vrais pirates informatiques. Ces tests se fondent sur des renseignements ciblés concernant les menaces à l'encontre d'une entité, des personnes qu'elle emploie, des processus qu'elle met en œuvre et des technologies qu'elle utilise, avec une connaissance préalable et un impact sur les opérations limités.***

Quel est l'objet d'un TPFM?

Le TPFM a pour objet d'évaluer et d'apporter un éclairage sur les capacités de résilience des entités face à une simulation de cyberincident dans le monde réel. Le test devrait être mené dans un cadre bien déterminé et inclure un processus de gestion des risques afin de garantir un test maîtrisé qui réduise au minimum le risque pour les entités.

À qui s'adressent les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* ?

Les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* ont pour objet de fournir des orientations : (a) aux autorités publiques qui envisagent de recourir aux TPFM, pour l'élaboration, la mise en œuvre et la gestion des TPFM dans leurs juridictions respectives; (b) aux entités qui réalisent les TPFM; (c) aux organisations qui offrent des services de renseignements sur les cybermenaces (« prestataires de renseignements sur les menaces »); (d) aux organisations qui offrent des services de réalisation des tests de pénétration (« prestataires de tests de pénétration »); et (e) aux organismes d'accréditation et de certification [2].

L'application des *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* est non contraignante. Cependant, les autorités pourraient intégrer des TPFM dans leurs évaluations de la cyberrésilience de certaines entités en tenant compte notamment :

- du niveau de priorité de la cyberrésilience du point de vue de la stabilité financière et de l'intégrité des marchés;
- de l'importance de certaines entités qui exercent des fonctions et fournissent des services critiques au sein du secteur financier; et
- de la (non-)disponibilité d'autres outils et techniques d'évaluation des risques pour tester la cyberrésilience.

Les autorités peuvent également envisager la proportionnalité afin de prendre en compte le type, la taille, la complexité, le degré de perfectionnement et le profil de risque des entités ciblées.

[1] Dans certaines juridictions, on emploie le terme de cyberpiratage éthique (*Ethical Red Teaming*).

[2] L'organisme d'accréditation et de certification valide le niveau de compétence de base que doivent atteindre les prestataires de renseignements sur la menace et de tests de pénétration.

Dans le cas d'entités multinationales, les autorités de différentes juridictions devraient collaborer pour planifier et coordonner ces tests afin de parvenir à un résultat optimal quant au calendrier, au champ d'application et à la mise en œuvre des tests.

L'efficacité des TPFM repose sur l'engagement fort de l'ensemble des parties prenantes tout au long du processus d'évaluation. S'agissant des entités participant aux évaluations transfrontières, avant de s'engager à participer aux TPFM, elles devraient définir la liste des autorités participantes. L'objectif est d'encourager les évaluations transfrontières, de favoriser les discussions sur l'acceptation mutuelle, par les différentes juridictions, des résultats des TPFM portant sur des entités multinationales, et de développer des protocoles pour partager les livrables résultant de l'évaluation des TPFM.

Partage de renseignements et protection des données

L'entité est chargée de mener une évaluation des TPFM et de partager les livrables conformément aux exigences de l'ensemble des autorités compétentes. Ces autorités peuvent souhaiter collaborer sur le partage de renseignements, le cas échéant et en conformité avec les normes de protection des données et de partage de renseignements entre juridictions.

Des mesures efficaces devraient être en place afin de protéger l'ensemble des informations liées aux activités des TPFM. Celles-ci devraient tenir compte de la sensibilité des informations. Les informations devraient être diffusées selon le principe du besoin de connaître.

Éléments fondamentaux pour les TPFM

Afin de tenir compte des objectifs généraux des TPFM, les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* définissent six éléments fondamentaux dont les autorités publiques et les entités doivent tenir compte pour l'élaboration et la réalisation des TPFM. Ces éléments clarifient les responsabilités des différentes parties prenantes à chaque phase. En général, les TPFM comportent les phases suivantes : définition du champ d'application du test et gestion des risques, renseignements sur la menace, tests de pénétration et clôture.

Élément 1 : Définition du champ d'application du test et gestion des risques

Il existe des risques potentiels inhérents aux TPFM pour l'ensemble des parties prenantes. C'est pourquoi les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* accordent une nette priorité à la définition claire du champ d'application des tests et à la mise en œuvre de processus efficaces de gestion des risques tout au long du processus d'évaluation.

Rôles et responsabilités

L'équipe blanche (« *White Team* ») [3] est chargée de garantir l'existence de contrôles appropriés en matière de gestion des risques et de parvenir à un accord avec les parties prenantes concernées sur le champ d'application du test. Le test étant réalisé sans que l'équipe bleue (« *Blue Team* ») [4]

[3] L'équipe blanche est le groupe chargé de coordonner un engagement entre une équipe rouge d'acteurs simulant une menace et une équipe bleue chargée de défendre les systèmes d'information au sein de l'entité. Durant le test, l'équipe blanche applique les règles de l'exercice, observe l'exercice, résout tout problème susceptible d'apparaître, recueille toutes les demandes d'informations ou questions, et garantit l'exécution du test conformément à ce qui était prévu.

[4] L'équipe bleue est le groupe chargé de défendre les systèmes d'information de l'entité face à un groupe d'acteurs simulant une menace (c'est-à-dire l'équipe rouge).

en ait connaissance préalablement, afin de permettre à l'équipe rouge (« *Red Team* ») [5] d'évaluer de manière efficace les capacités de résilience de l'entité, l'équipe blanche est incitée à jouer le rôle de gestionnaire de projet tout au long du processus d'évaluation, y compris durant la phase de définition du champ d'application et de gestion des risques.

Champ d'application du test

Le champ d'application du test devrait être principalement défini sur la base d'une évaluation des fonctions et services critiques de l'entité, laquelle guidera les décisions concernant la durée du test et confirmera l'inclusion ou l'exclusion de paramètres. L'entité devrait identifier les personnes, les processus et la technologie qui soutiennent ces fonctions et services critiques, y compris les prestataires tiers (tels que les prestataires de services informatiques et ceux liés à la chaîne d'approvisionnement). Si la portée du test nécessite d'inclure des prestataires de services tiers, il appartient à l'entité de faire la liaison avec ces prestataires et de garantir leur participation.

L'entité devrait comprendre les exigences des autorités des juridictions concernées en matière de définition champ d'application du test; en outre, elle est incitée à analyser leurs exigences respectives. Cela est particulièrement important si l'entité souhaite utiliser les résultats des TPFM afin de satisfaire aux exigences des autorités de ces juridictions. Dans ce cas, l'entité devrait consulter, dès le stade initial de la définition du champ d'application, l'ensemble des autorités compétentes qui sont susceptibles de lui fournir des orientations en la matière.

Au cours du cycle de vie du test, son champ d'application et sa durée peuvent varier en fonction des interactions entre les prestataires de renseignements sur les menaces et les prestataires de tests de pénétration, sur la base des résultats de leurs travaux. Les parties prenantes concernées (l'entité, les prestataires précités, les autorités publiques, etc.) devraient s'entendre sur ces modifications au regard des exigences des autorités.

La gestion des risques

Les entités, en concertation avec les parties prenantes concernées, devraient appliquer des processus de gestion du risque afin de réduire le risque d'impact potentiel sur les données de l'entité, d'atteinte aux actifs de l'entité et de perturbation des services et/ou opérations critiques au sein de l'entité ou du secteur financier. Dans le cadre de la gestion des risques, l'équipe blanche peut interrompre le test à tout moment si elle considère que la poursuite du test présente un risque inacceptable pour l'entité.

La communication au sein de l'entité devrait être réduite au minimum afin de préserver l'intégrité du test, mais l'entité devrait néanmoins veiller à ce que des processus appropriés de gestion des risques soient communiqués et compris par l'ensemble des parties concernées.

Classification des résultats

Durant la phase de définition du champ d'application du test, les parties prenantes, y compris les prestataires de tests de pénétration, devraient s'accorder sur un schéma de classification des

[5] L'équipe rouge est un groupe de testeurs, autorisé et organisé pour imiter les actions potentielles d'un pirate informatique ou exploiter des failles potentielles d'une entité.

vulnérabilités détectées au cours des tests, ainsi que sur les éléments probants à même de démontrer leur réussite. Le schéma de classification vise à montrer le caractère critique et le niveau de priorité des vulnérabilités détectées, conformément au dispositif de gestion des risques de l'entité.

Le livrable relatif à la définition du champ d'application du test devrait être remis au fournisseur de renseignements sur les menaces, afin de faciliter l'élaboration de scénarios fondés sur ces renseignements pour tester les services critiques.

Élément 2 : Ressources
Il incombe à l'entité d'engager des prestataires de renseignements sur les menaces et de tests d'intrusion. En raison de la nature sensible des TPFM, les entités devraient soigneusement sélectionner ces prestataires, sur la base de facteurs tels que le niveau d'expertise, le code de conduite éthique et des niveaux d'assurance suffisants (assurance responsabilité civile, par exemple). L'accréditation et la certification peuvent constituer une méthode de validation de l'expertise de ces prestataires.

Si les prestataires externes de renseignements sur les menaces et de tests d'intrusion offrent généralement un point de vue indépendant, le recours à leurs services peut être soumis à des exigences différentes selon les juridictions. Les entités devraient confirmer que leur approche satisfait aux exigences des juridictions ciblées lors de la phase de définition du champ d'application de l'exercice. Par exemple, certaines juridictions peuvent exiger le recours aux services de prestataires externes et la validation de leur expertise par des organismes d'accréditation et de certification.

Élément 3 : Renseignements relatifs aux menaces
Les renseignements relatifs aux menaces constituent une phase clé du processus TPFM global. Les prestataires de renseignements sur les menaces utilisent des renseignements et l'identification des menaces adaptés à l'entité afin de créer des profils de menace crédibles qui, en imitant de vrais pirates informatiques, revêtent une importance critique pour la définition du champ d'application des tests. Les profils de menace contiennent des scénarios de cybermenace qui contribuent au développement, par l'équipe rouge, de plans de tests qui seront utilisés durant la phase de tests de pénétration.

Rôles et responsabilités
Les prestataires de renseignements sur les menaces sont habituellement en charge de : (1) la production de livrables en matière de renseignements sur les menaces, alignés sur le champ d'application du test et conformes aux instructions données par l'entité; (2) la justification de la pertinence des livrables en matière de renseignements sur les menaces; (3) la diffusion à l'équipe blanche de ces livrables; et (4) l'apport d'un soutien, le cas échéant, à l'équipe rouge. Cela comprend l'aide apportée pour l'élaboration de scénarios de cybermenace, ainsi que la satisfaction des nouveaux besoins en matière de renseignements qui pourraient survenir au cours du test de pénétration.

L'entité devrait fournir : (1) des instructions au fournisseur de renseignements sur les menaces concernant les fonctions ou les systèmes inclus dans le champ d'application du test; (2) des

informations générales afin d'assister ce fournisseur dans l'élaboration rapide et efficace des profils de menace; et (3) des livrables en matière de renseignements sur les menaces au fournisseur de tests de pénétration, aux parties prenantes appropriées et aux autorités, le cas échéant.

Compétences relatives aux renseignements sur les menaces
Au minimum, les prestataires de renseignements sur les menaces sont dotés de :

- la capacité à établir le profil des pirates informatiques pertinents à l'échelle de l'entité, du secteur et de la zone géographique;
- la capacité à élaborer des scénarios de cybermenace, en reproduisant la méthodologie des pirates informatiques sélectionnés;
- la capacité à utiliser différentes méthodologies ainsi que des sources et des types de renseignements multiples, tels que le renseignement de sources ouvertes (*Open Source Intelligence* - OSINT) et les indicateurs de compromission relatifs au secteur concerné afin d'établir une image précise et actualisée des zones d'attaque vulnérables d'une entité, en se concentrant sur les personnes, les processus et la technologie; et
- la capacité à collecter l'information en plusieurs langues.

Livrables en matière de renseignements sur les menaces
Pour chaque exercice de TPFM, le fournisseur de renseignements sur les menaces devrait produire les livrables suivants :

- un rapport traitant des renseignements sur les menaces - Le rapport devrait contenir des profils de cyberattaquants qui représentent une menace crédible pour l'entité. Lorsqu'aucun rapport spécifique concernant l'entité n'est disponible, ces acteurs peuvent être sélectionnés sur la base d'activités antérieures connues au sein de secteurs ou de zones géographiques pertinentes. Chacun des profils devrait contenir un scénario de cyberattaque mettant l'accent sur la méthodologie et les outils utilisés par le cyberattaquant. Les scénarios de cybermenace devraient être suffisamment détaillés pour donner aux prestataires de tests d'intrusion l'ensemble des approches et des informations pertinentes nécessaires à la formulation de plans de tests efficaces.
- un rapport de ciblage - Le rapport de ciblage devrait fournir un profil de l'entité mettant en lumière les zones d'attaque vulnérables ou exposées en rapport avec les personnes, les processus et la technologie, conformément au champ d'application identifié. Le rapport devrait chercher à fournir aux prestataires de tests d'intrusion les vecteurs potentiels de menace au sein de l'entité cible.

Une approche coordonnée devrait être développée pour inclusion dans le plan de test de pénétration, afin que les parties prenantes puissent mettre à l'épreuve les livrables en matière de renseignements sur les menaces et établir les scénarios de cybermenace convenus pour les systèmes inclus dans le périmètre du test. Cette coordination, généralement facilitée par l'entité, permet à l'équipe rouge d'élaborer un plan de test de pénétration plus ciblé, conformément aux objectifs principaux du test.

Tout au long de ce processus et durant la phase de tests de pénétration, le fournisseur de renseignements sur les menaces devrait continuer de proposer son expertise, au moment requis et selon les modalités requises. Dans le cas d'entités proposant leurs services dans plusieurs

juridictions, les différentes parties prenantes devraient accorder une attention particulière au partage des livrables entre les juridictions, compte tenu de la sensibilité et de la confidentialité de l'information.

Élément 4 : Tests de pénétration
Après l'achèvement de la phase de renseignements sur les menaces, l'équipe rouge devrait organiser et exécuter un test des systèmes et services cibles, comme définis dans le champ d'application. Il est recommandé, sur la base de celui-ci, d'accorder suffisamment de temps à la phase de tests de pénétration afin de permettre à l'équipe rouge de mener des tests réalistes dans lesquels les scénarios de cyberattaque seront déroulés.

Rôles et responsabilités
L'équipe rouge est généralement chargée de : (1) produire un plan de tests de pénétration, aligné sur le champ d'application et les processus de gestion des risques, qui présente clairement les scénarios à suivre durant les tests; (2) conduire les tests conformément aux scénarios de cyberattaque conçus à partir des données des prestataires de renseignements sur les menaces; et (3) rédiger et transmettre à l'entité le rapport final sur les tests de pénétration.

L'équipe blanche est chargée de : (1) coordonner et faciliter les activités de tests; (2) maintenir un dialogue continu avec l'équipe rouge et fournir un soutien supplémentaire lorsque nécessaire; (3) superviser et contrôler l'équipe bleue; et (4) mettre en œuvre des processus de gestion des risques efficaces (y compris l'arrêt des tests à tout moment si cela est jugé nécessaire).

Les autorités concernées peuvent suivre le déroulement des tests en même temps que l'équipe blanche.

Méthodologie, approche et livrables en matière de tests
L'entité devrait conduire une évaluation du TPFM conforme aux exigences des autorités concernées auprès desquelles elle cherche à recueillir l'acceptation du test.

L'équipe rouge devrait utiliser les livrables en matière de renseignements sur les menaces pour développer un plan de tests de pénétration ciblé. L'entité devrait s'assurer que l'équipe rouge dispose de suffisamment de temps pour conduire les tests de façon appropriée.

Conformément aux processus de gestion du risque, l'équipe blanche devrait surveiller de bout en bout l'exécution des tests, afin de s'assurer que les risques pesant sur les systèmes cibles sont minimisés.

L'entité devrait connaître les exigences en matière de tests dans les environnements de production et de non-production, car ces environnements peuvent être sujets à des exigences dans certaines juridictions.

Une fois le test terminé, l'équipe rouge devrait produire un rapport de test de pénétration. Ce rapport devrait détailler l'approche adoptée pour les tests, ainsi que les conclusions et les observations tirées de ces tests. Il devrait évaluer les risques et les contremesures existantes et, le cas échéant, donner un avis concernant les pistes d'amélioration.

Élément 5 : Clôture et actions correctrices
Après l'achèvement de la phase de tests de pénétration, le TPFM passe à la phase de clôture, qui vise à permettre à toutes les parties prenantes concernées d'analyser et de réagir aux résultats du test et d'apporter des modifications visant à renforcer la cyberrésilience de l'entité testée.

Il incombe habituellement au fournisseur de tests d'intrusion d'appuyer les éventuels groupes de travail post-tests, notamment pour la présentation des résultats à l'entité.

Il incombe à l'entité : (1) de communiquer les résultats aux parties prenantes pertinentes à l'aide de moyens sûrs préalablement convenus; (2) d'organiser des groupes de travail post-tests avec les parties prenantes concernées afin d'examiner les résultats et d'identifier les solutions potentielles d'atténuation du risque; et (3) de concevoir et de mettre en œuvre un programme complet de mesures correctrices.

L'autorité concernée est chargée de prendre contact avec l'entité et de convenir avec elle d'un programme de mesures correctrices; et de suivre la mise en œuvre de ce programme dans le cadre de ses activités courantes vis-à-vis de l'entité.

Élément 6 : Données thématiques
Un des objectifs principaux des *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* est de contribuer à l'amélioration de la cyberrésilience des entités et, de façon plus générale, du secteur financier. Un moyen important d'atteindre cet objectif est la production et le partage de données thématiques entre les autorités et les entités.

Les données thématiques devraient identifier les résultats et les vulnérabilités sectoriels communs. Les résultats thématiques doivent empêcher l'identification des entités individuelles. Les juridictions peuvent utiliser leurs propres cadres comme base pour la création de thématiques post-TPFM et la production de données thématiques relatives aux TPFM relève de la responsabilité des autorités concernées. Les autorités peuvent partager les informations selon différentes modalités, si elles sont appropriées et conformes aux normes de protection des données et de partage de renseignements entre juridictions.