Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle

Mai 2020

Document rp220068

Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle

Unal Tatar
Université d'Albany – SUNY
Albany (NY), États-Unis

Omer Keskin
Université Old Dominion
Norfolk (VA), États-Unis

Hayretdin Bahsi
Université de technologie de Tallinn
Tallinn, Estonie

C. Ariel Pinto
Université Old Dominion
Norfolk (VA), États-Unis

Projet financé par les organisations suivantes :

Casualty Actuarial Society
Institut canadien des actuaires
Society of Actuaries

TABLE DES MATIÈRES

Quantification du cyberrisque pour les actuaires

Une approche économique fonctionnelle

La gestion des cyberrisques demeure importante pour la viabilité des organisations. Il est encore difficile de quantifier ces risques pour prendre de meilleures décisions en matière de placement. Dans la présente étude, nous avons élaboré un cadre d'analyse des cyberrisques d'une organisation. Le cadre proposé met à profit une méthode qui analyse les dépendances fonctionnelles en intégrant des graphes d'attaque probabiliste pour mesurer les répercussions économiques des cyberattaques sur les activités.

Remerciements

Les auteurs sont très reconnaissants aux membres du Groupe chargé de la surveillance du projet pour leur rétroaction précieuse et constructive. Leurs commentaires judicieux ont permis d'améliorer le rapport final. Ce projet est appuyé par la Society of Actuaries (SOA). Les opinions exprimées et les conclusions tirées sont celles des auteurs et elles ne représentent pas une position ou une opinion officielle de l'ICA, de la SOA ou de leurs membres.

Section 1 : Introduction et aperçu

En raison de sa complexité, la sécurité du cyberespace est l'un des plus grands défis d'aujourd'hui. Le cyberenvironnement devenant davantage intégré au monde réel, l'impact direct des incidents de cybersécurité sur l'entreprise est également accru. L'analyse du cyberrisque représente le principal outil de gestion des conséquences des cyberévénements.

L'analyse des risques repose sur la réponse à trois questions :

1. Qu'est-ce qui pourrait mal tourner?
2. Quelle est la probabilité que cela se produise?
3. Quelle en serait l'incidence? (Kaplan et Garrick, 1981)

La formule générale d'analyse quantitative du risque, qui s'applique également à l'analyse du cyberrisque, est créée à partir de ces questions. Selon cette formule générale, le risque est un ensemble de triplets, $R = \{< S_i, P_i, X_i, >\}, i = 1,2,..,N$ où S_i est une identification de scénario, P_i est la probabilité de ce scénario, X_i est l'incidence de ce scénario, et N est le nombre de scénarios envisagés (Kaplan et Garrick, 1981).

Le National Institute of Standards and Technology (NIST) définit le cyberrisque comme suit : [traduction libre] « Risque de pertes financières, de perturbations opérationnelles, ou de dommages, découlant de la défaillance des technologies numériques utilisées pour les fonctions informationnelles ou opérationnelles introduites dans un système de fabrication par des moyens électroniques par suite de l'accès, de l'utilisation, de la divulgation, de la perturbation, de la modification ou de la destruction non autorisés du système de fabrication » (Stouffer et coll., 2019).

L'évaluation des répercussions, qui fait partie intégrante de l'analyse des risques, tente d'estimer les dommages possibles d'une cybermenace pour une entreprise ou une mission. Elle donne un aperçu du classement des risques par priorité, car elle intègre les exigences opérationnelles à l'analyse des risques afin de mieux équilibrer la sécurité et la convivialité. De plus, cette évaluation constitue le principal flux d'information entre les techniciens et les dirigeants d'entreprise. Il convient donc d'harmoniser efficacement les aspects technologiques et opérationnels de la cybersécurité (Bahsi et coll.,2018).

1.1 Limites des méthodes actuelles d'analyse du cyberrisque

Les méthodes actuelles d'analyse du cyberrisque présentent plusieurs limites. Le cyberrisque est souvent traité comme un problème de technologie de l'information plutôt qu'un élément essentiel de la gestion du risque d'entreprise (Moore, Dynes et Chang, 2015). Les méthodes existantes d'analyse du cyberrisque évaluent le risque principalement au niveau de la couche d'actifs (c.-à-d. l'évaluation des risques liés aux logiciels, au matériel et aux données par l'assurance de la qualité des logiciels, l'analyse des vulnérabilités, la détection des intrusions et l'analyse des logiciels malveillants), dans une certaine mesure à l'échelle de l'organisation (c.-à-d. les processus opérationnels), et rarement sur le plan des écosystèmes (c.-à-d. les chaînes d'approvisionnement) (U.S. Department of Homeland Security, 2018).

Une autre lacune a trait à l'insuffisance des métriques utilisées pour appuyer les décisions de placement, y compris la cyberassurance, la sécurité et les contrôles. Des métriques qualitatives et des termes opérationnels, plutôt que des mesures financières quantifiées, sont souvent utilisés comme indicateurs du cyberrisque qui éclairent les décisions de placement. Les métriques qualitatives ou opérationnelles du cyberrisque entraînent, d'une part, un manque de compréhension des dirigeants d'organisations et, d'autre part, une réticence à apprécier l'importance des cyberrisques. Cette question a été énoncée dans le plan stratégique du Programme fédéral de recherche et développement sur la cybersécurité : [traduction libre] « Il n'existe pas de fondement scientifique pour l'analyse du risque de coût, et les décisions opérationnelles sont souvent fondées sur des données non scientifiques ou des arguments de qualité non quantifiés » (National Science and Technology Council, 2011). En outre, l'absence de quantification de la façon dont les placements dans des contrôles particuliers modifient le niveau de risque (c.-à-d. la mesure de l'efficacité des contrôles prévus ou mis en œuvre) constitue une autre limite des méthodes actuelles d'analyse du cyberrisque.

On note une variation du langage utilisé dans la communication du cyberrisque entre les décideurs en cybersécurité à tous les niveaux de gestion et les unités opérationnelles d'une organisation. À l'instar de nombreux autres domaines, la prise de décisions en matière de cybersécurité comporte trois niveaux : tactique, opérationnel et stratégique. La différence entre les paramètres décisionnels des gestionnaires de niveau tactique (p. ex., le nombre de systèmes vulnérables), opérationnel (p. ex., les contraintes juridiques et organisationnelles) et stratégique (p. ex., l'incidence sur l'ensemble des activités) crée une lacune en matière de communication, ce qui empêche l'évaluation exacte du cyberrisque.

L'incidence et la probabilité d'un scénario de risque peuvent varier au fil du temps. Très peu d'études traitent du changement de la vigueur et de la criticité des dépendances dans le temps et de la valeur des risques qui s'y rattachent.

Cette recherche a pour but d'élaborer un modèle d'analyse quantitative probabiliste du cyberrisque sur la façon dont sont reliés le risque rattaché à l'actif et les objectifs de l'organisation. Dans le cadre de cette méthode, nous tiendrons compte des répercussions en cascade au moyen des dépendances internes d'une organisation.

La méthode d'analyse du cyberrisque mise au point utilise des graphes d'attaque probabiliste, qui reposent sur les vulnérabilités connues des logiciels et des topologies de réseau. Les capacités d'évaluation dynamique du risque sont accrues dans le graphe d'attaque fondé sur des réseaux bayésiens. Le cadre proposé tirera également parti de la dépendance fonctionnelle. La propagation de la cyberincidence est modélisée dans les couches d'une entreprise et entre les différentes entreprises. Parmi les caractéristiques, mentionnons l'expression de l'incidence comme fonction de la perte de confidentialité, d'intégrité et de disponibilité (CID), et de nouvelles relations de dépendance mathématique reflétant la nature des cyberdépendances. Gardons en tête les définitions suivantes :

- La *confidentialité* consiste à [traduction libre] « préserver les restrictions autorisées à l'accès à l'information et à sa divulgation, y compris les moyens de protéger les renseignements confidentiels et exclusifs » (McCallister, Grance et Scarfone, 2010).
- L'*intégrité* représente [traduction libre] « l'objectif de sécurité qui crée l'exigence d'une protection contre les tentatives intentionnelles ou accidentelles de porter atteinte à l'intégrité des données (la propriété selon laquelle les données n'ont pas été modifiées de façon non autorisée) ou l'intégrité des systèmes (la qualité dont dispose un système lorsqu'il remplit sa fonction prévue d'une manière non altérée, sans manipulation non autorisée) » (Stoneburner, 2001).
- La *disponibilité* consiste à [traduction libre] « assurer un accès rapide et fiable à l'information et son utilisation » (Ross, McEvilley et Oren, 2016).

La perte de confidentialité, d'intégrité et de disponibilité est mesurée dans l'étude afin de quantifier les répercussions des cyberattaques sur les systèmes d'entreprise. D'autres analyses quantifient les répercussions économiques au moyen de la perte de CID.

Cette étude vise à élaborer un modèle générique qui peut être appliqué par n'importe quelle organisation. Aux fins de la validation de la méthode d'analyse du cyberrisque élaborée, des simulations et une analyse de sensibilité seront effectuées.

1.2 Gestion du cyberrisque du point de vue de l'actuariat

La gestion du cyberrisque du point de vue de l'actuariat pose problème. Dans le cas de l'assurance traditionnelle, l'utilisation de données historiques sur les sinistres est habituellement privilégiée dans les modèles actuariels. Toutefois, dans le cyberdomaine, les données historiques sont insuffisantes pour deux raisons principales : (1) La cyberassurance est un domaine relativement nouveau et novateur qui ne comporte pas un long historique de plusieurs décennies et (2) les données existantes deviennent vite désuètes, car les menaces, les vulnérabilités et les méthodes d'atténuation évoluent rapidement (Böhme, Laube et Riek, 2017).

Certaines études dans la littérature regroupent les données actuellement disponibles sur les pertes liées à des cyberincidents dans le but d'obtenir une perte totale moyenne (Biener, Eling et Wirfs, 2015; NetDiligence, 2018). Toutefois, les résultats ne sont pas avantageux puisque les méthodes et les contextes des études varient de façon considérable. Même si Biener, Eling et Wirfs (2015) laissent à entendre que le coût moyen par cyberincident est de

40 millions de dollars pour 994 incidents entre 1971 et 2009, l'étude de NetDiligence (2016; 2018) conclut que le coût moyen pour 1 201 sinistres entre 2013 et 2017 s'établit à 0,7 million de dollars. Cette différence s'explique, comme en font foi les deux raisons principales mentionnées précédemment. En raison de ces problèmes, les actuaires craignent d'utiliser ce genre de données dans les analyses. Le contexte éventuellement différent de chaque cyberincident peut s'ajouter aux différences entre les diverses entreprises de différentes industries.

Les problèmes liés à la modélisation du cyberrisque qui dépend des données ont forcé les actuaires à adopter d'autres approches pour estimer la modélisation des pertes et la quantification du cyberrisque. Le modèle élaboré dans l'étude aide les actuaires à évaluer les cyberrisques que pose un réseau de technologies d'information et de communications (TIC) d'entreprise afin de prendre des décisions bien éclairées au sujet de la garantie des polices, des primes et des franchises. Le modèle élaboré peut être appliqué à tout réseau de TIC d'entreprise en personnalisant les intrants en conséquence.

1.3 Contribution

La contribution scientifique de cette recherche est de mieux comprendre et évaluer l'impact dans le contexte de l'analyse du cyberrisque. L'un des résultats les plus novateurs est l'élaboration d'un modèle probabiliste quantitatif du risque fondé sur des graphes, pour déterminer la propagation de l'impact à chaque couche et entre toutes les couches (c.-à-d., les actifs, les services ou les processus opérationnels) d'une organisation.

Cette méthode évalue les étapes des attaques et évalue comment les autres composants sont affectées par la connexion de graphes d'attaques probabilistes alimentés par le système commun de notation des vulnérabilités (CVSS) et les réseaux de dépendance fonctionnelle. La méthode proposée permet de hiérarchiser les vulnérabilités en fonction de leur impact et de promouvoir de meilleures décisions de placement en fonction des risques.

Section 2 : Relation entre l'équation du risque, les graphes d'attaque et les graphes d'impact

Les graphes d'attaque aident à calculer les cyberrisques d'une organisation. Le risque est fonction de la vraisemblance et de l'impact :

$$Risque = f(vraisemblance, impact) \quad \text{(Équation 1)}$$

- La vraisemblance d'une attaque dépend de l'expérience et de la motivation de l'attaquant; par conséquent, elle est liée à l'attaquant.
- L'impact dépend de l'importance des composantes du réseau cible pour l'organisation; l'impact concerne donc la victime.

La facilité et les avantages d'une cyberattaque constituent des facteurs essentiels pour estimer la vraisemblance d'une occurrence. Les graphes d'attaque, qui examinent les réseaux du point de vue de l'attaquant, sont utiles pour calculer la vraisemblance d'un événement de risque (Ingoldsby, 2010). Cependant, l'impact doit être calculé en fonction de la valeur de l'actif pour l'organisation et de son incidence sur des services et des processus opérationnels particuliers.

Dans la présente étude, nous avons utilisé des graphes d'attaque de type bayésien pour calculer les valeurs de vraisemblance (section 5) et des graphes d'impact qui utilisent l'analyse des réseaux de dépendance fonctionnelle (FDNA; section 6) pour calculer l'impact opérationnel en tenant compte de la propagation.

Le calcul de la vraisemblance au moyen de graphes d'attaque nécessite des renseignements détaillés sur la vulnérabilité pour chaque actif du graphe d'attaque. Des renseignements détaillés sont extraits de la Base de données nationale sur les vulnérabilités (BDNV), où toutes les vulnérabilités connues du matériel et des logiciels sont présentées à l'aide du CVSS.

La modélisation et la simulation de la propagation de l'impact représentent un autre volet de la présente étude. La propagation de l'impact dépend de la mesure dans laquelle chaque processus opérationnel dépend fonctionnellement des services et des actifs individuels au sein du réseau des TIC de l'entreprise. L'analyse des réseaux de dépendance fonctionnelle est une méthode déterministe qui sert à calculer les effets d'entraînement de la propagation de l'impact entre les couches d'entreprise.

Section 3 : Graphe d'attaque

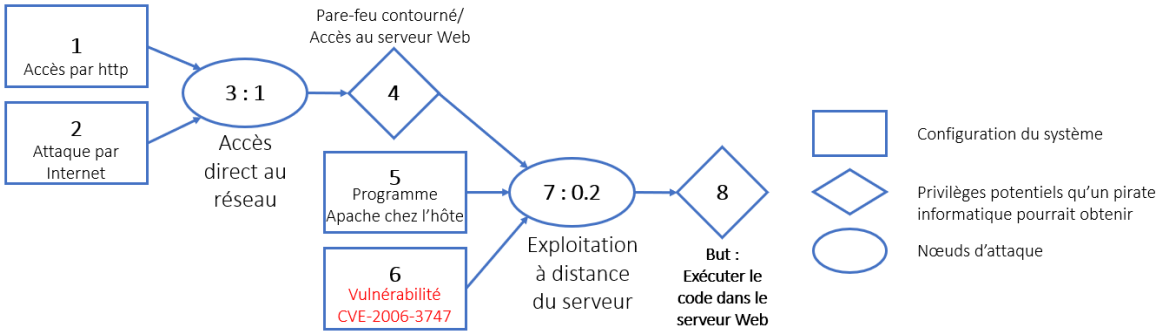
Un réseau type de TIC d'entreprise comporte des centaines de nœuds (p. ex., des ordinateurs, des routeurs, des commutateurs, des dispositifs de stockage). Le dénombrement des vulnérabilités des composantes de ces réseaux ne constitue pas une façon efficace et efficiente de quantifier les cyberrisques. Dans un tel réseau, bon nombre de ces vulnérabilités ne sont pas exploitables au départ, car une défense multicouche empêche l'attaquant d'atteindre directement l'hôte ciblé. De plus, certaines vulnérabilités ne sont pas du tout exploitables. Pour atteindre l'hôte cible, l'attaquant doit examiner la topologie du réseau et exploiter efficacement les vulnérabilités existantes sur chaque nœud du chemin qui l'amène à sa cible.

En ce qui concerne la défense, le personnel chargé de la sécurité de l'information doit tenir compte du réseau du point de vue des attaquants afin de déterminer les composantes essentielles, de révéler les chemins d'attaque possibles et de préciser les liens les plus faibles dans le réseau. L'estimation des chemins d'attaque les plus probables améliore la gestion des risques et appuie les placements dans des produits et services de cybersécurité plus efficaces.

Un *graphe d'attaque* est un formalisme fondé sur la théorie des graphes qui aide à visualiser et à analyser les cyberattaques et qui combine l'exploitation de multiples vulnérabilités (Swiler, Phillips et Gaylor, 1998). Les configurations de sécurité du système sont indiquées avec les vulnérabilités existantes sur un graphe. L'exploitation des vulnérabilités entraîne des changements dans l'état du système (Singhal et Ou 2011). Les significations des nœuds et des limites et ce qu'ils représentent peuvent changer selon les définitions établies par quiconque produit le graphe d'attaque (Haque, Keffeler et Atkison 2017). Les graphes 1 et 2 présentent la même séquence d'attaque avec différentes approches de représentation. Dans la figure 1, les rectangles représentent les configurations du système, les losanges illustrent les privilèges potentiels qu'un attaquant pourrait obtenir, et les ellipses affichent les nœuds d'attaque. Il s'agit d'une forme très détaillée de visualisation d'un graphe d'attaque qui permet de voir facilement toutes les conditions préalables d'une attaque. Chaque nœud possède un numéro d'identification. Les nœuds d'attaque en forme d'ellipse ont une probabilité de réussite. La première étape consiste à accéder au serveur Web à partir d'Internet, ce qui a une probabilité de 1 puisqu'il est ouvert au public. La deuxième étape consiste à exploiter une vulnérabilité sur le serveur Web Apache pour obtenir le privilège d'exécuter un code arbitraire sur le serveur Web.

Figure 1

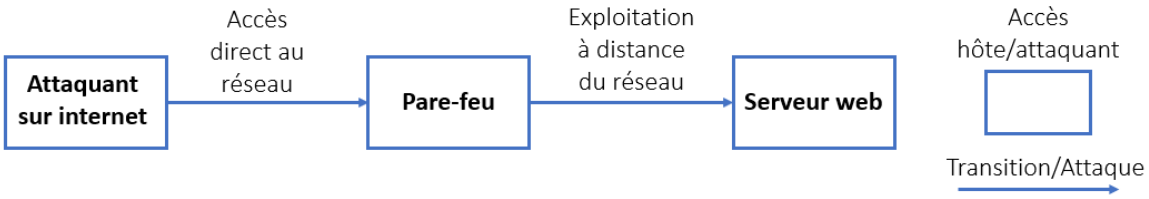
EXEMPLE DE GRAPHE D'ATTAQUE



Source : Adapté de Singhal et Ou (2011)

Dans les graphes d'attaque, les nœuds représentent habituellement les états des composantes du réseau et les limites présentent les transitions entre les différents états. Ce formalisme est moins déroutant que le précédent puisqu'il se concentre sur les étapes de l'attaque avec un plus petit nombre de nœuds. Dans notre étude, nous utilisons cette représentation, car une augmentation du nombre de composantes des TIC engendre des graphes très compliqués.

Figure 2
REPRÉSENTATION DIFFÉRENTE DE L'EXEMPLE DE GRAPHE D'ATTAQUE DE LA FIGURE 1



Les graphes d'attaque représentent une version évoluée des arbres d'attaque et des arbres de défaillance. Les objectifs de l'utilisation de chacune de ces trois approches se chevauchent d'une certaine façon. Toutes trois paraissent semblables et elles sont analysées au moyen de procédures semblables. Des différences émergent au chapitre de leur lecture et de leurs domaines d'application (p. ex., militaire, systèmes énergétiques, cybersécurité). Étant donné que certains concepts utilisés pour la production et l'analyse des arbres d'attaque ont été adoptés à partir des approches relatives aux arbres d'attaque et aux arbres de défaillance, ils ont été inclus dans le présent rapport pour améliorer la compréhension.

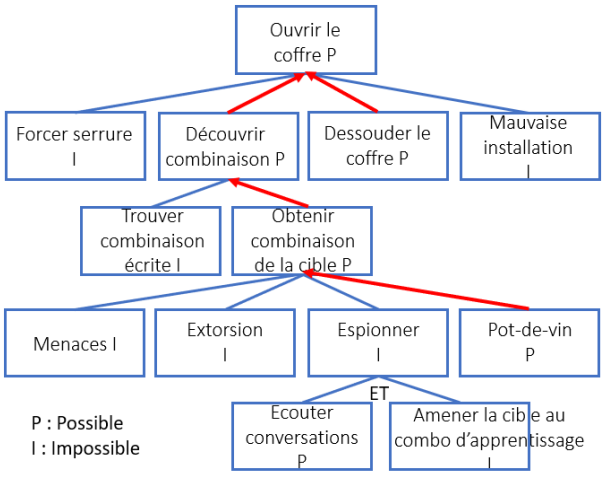
3.1 Similitudes et différences entre les graphes d'attaque et les arbres d'attaque et de défaillance

Les arbres d'attaque servent à évaluer la sécurité des TIC. La différence entre un graphe d'attaque et un arbre d'attaque se situe dans ce que représentent les limites et les nœuds. Un arbre d'attaque complet ressemble à un arbre dont la racine est la cible ultime, et les feuilles sont les attaques élémentaires (Haque, Keffeler et Atkison 2017).

Les arbres d'attaque offrent un point de vue pratique pour comparer différentes stratégies d'attaque visant une cible particulière. Les facteurs de comparaison peuvent être modifiés pour étudier la sécurité du système sous des angles différents. Dans l'exemple d'un arbre d'attaque de base contre un coffre-fort de Schneiner (1999), quatre approches principales permettent d'ouvrir le coffre, et l'une d'elles comporte plusieurs étapes, comme le montre la figure 3.

Ici, la cible se trouve à la cime de l'arbre. Ce graphe peut être vu comme un arbre à l'envers où la racine est la cible et les différentes stratégies sont les branches. Chacune des autres cases représente une phase d'attaque. Il existe quatre approches principales; trois des principales stratégies sont des attaques en une étape, tandis que le « le combo d'apprentissage » comporte des étapes d'attaque préalables.

Figure 3
EXEMPLE D'ARBRE D'ATTAQUE SIMPLE



Source : Adapté de Schneiner (1999)

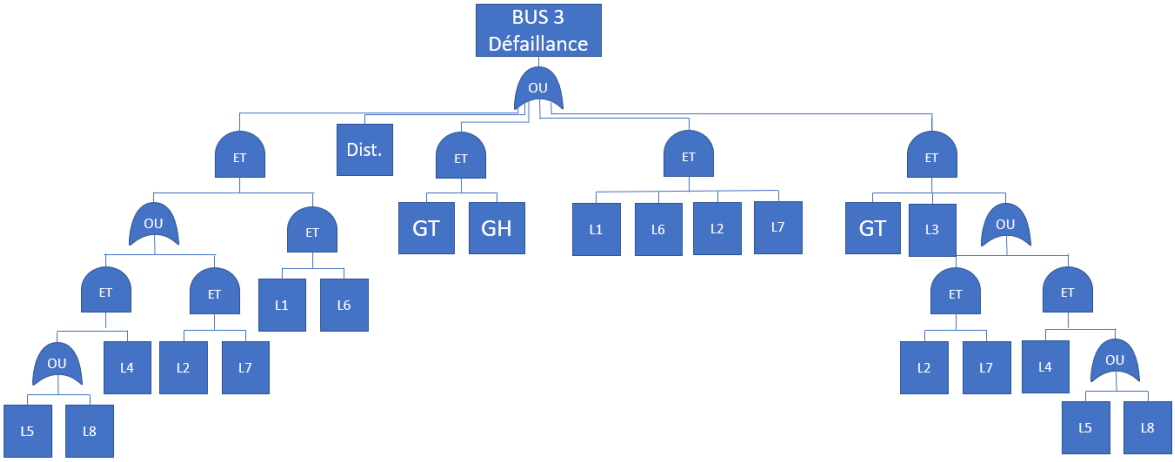
Pour analyser l'attaque du point de vue de l'attaquant, les quatre approches peuvent être envisagées pour déterminer si elles sont possibles ou impossibles compte tenu du niveau de compétence de l'attaquant. Deux des étapes sont combinées à la logique « ET », ce qui signifie que pour obtenir la combinaison du coffre-fort par écoute clandestine, l'attaquant doit être en mesure d'écouter une conversation et de faire en sorte que la personne ciblée énonce la combinaison dans la conversation. Dans ce cas, même si l'écoute est possible, il est impossible d'amener la victime à déclarer la combinaison, ce qui rend impossible l'approche d'écoute clandestine pour atteindre l'objectif d'ouvrir le coffre-fort. Dans cet arbre d'attaque, tous les nœuds sont combinés à la logique « OU », à moins qu'une logique « ET » soit énoncée. Dans cet exemple, seulement deux approches – indiquées par des flèches rouges – sont raisonnablement possibles : faire sauter le coffre-fort et obtenir la combinaison de la personne ciblée par corruption.

Lorsqu'un arbre d'attaque est prêt pour l'analyse, il peut être envisagé sous différents angles, par exemple si l'attaque est possible pour un type particulier d'agent malveillant. En outre, d'autres analyses peuvent être effectuées en fonction, par exemple, du coût estimatif pour l'attaquant, du besoin d'équipement spécial et du temps requis pour exécuter l'attaque. Les responsables de la sécurité devraient évaluer le système à l'aide de l'arbre d'attaque du point de vue de divers adversaires possibles qui disposent de compétences et de ressources différentes.

L'analyse des arbres de défaillances est utilisée depuis des décennies pour calculer les effets des défaillances des composantes et la fiabilité de systèmes comme les systèmes militaires et les réseaux électriques. Ces graphes servent à calculer comment un comportement de défaillance réparti aléatoirement ou fondé sur une distribution de probabilité particulière modifie la fiabilité globale d'un système (Ingoldsby, 2010). La figure 4 présente un exemple d'arbre de défaillance dont la fiabilité du nœud à la cime est analysée en utilisant les probabilités de défaillance des nœuds carrés, qui représentent la défaillance de composantes particulières avec un taux de défaillance à une distribution de probabilité connue.

Figure 4

EXEMPLE D'ARBRE DE DÉFAILLANCE



3.2 Production de graphes d'attaque

Les intrants requis pour générer le graphe d'attaque d'un réseau sont les suivantes :

1. La liste des vulnérabilités du réseau;
2. La topologie réseau et les configurations réseau spécifiques;
3. La base de données des attaques connues (Swiler, Phillips et Gaylor 1998).

Il existe de nombreux progiciels pour analyser un réseau afin de dresser la liste de toutes les vulnérabilités connues des hôtes, des routeurs, des logiciels et des autres composantes du réseau. Nessus (n.d.) est l'un des lecteurs de vulnérabilité réseau les plus utilisés. Le résultat d'une lecture Nessus et de la topologie réseau est utilisé pour produire un graphe d'attaque au moyen de logiciels comme Topological Analysis of Network Attack Vulnerability (TVA) (Jajodia, Noel et O'Berry 2005); Network Security Planning Architecture (NETSPA) (Artz 2002); et Multihost, multistage, Vulnerability Analysis (MULVAL) (Ou, Govindavajhala et Appel 2005).

Il est courant qu'une entreprise possède de nombreux actifs, et chacun de ces actifs peut présenter de multiples vulnérabilités. Avec une grande surface d'attaque, une entreprise peut avoir un graphe d'attaque comportant de nombreux chemins d'attaque. Un attaquant ne dispose pas de tous les détails relatifs à un réseau de TIC. Il ne serait donc pas réaliste de supposer qu'il puisse révéler tous les chemins d'attaque que peut générer un défenseur. La richesse d'un graphe d'attaque peut amener un défenseur à conclure que le risque est élevé. Ce graphe est toutefois un outil qui aide à trouver les nœuds critiques partagés par de multiples chemins d'attaque. La correction des vulnérabilités de ces nœuds aide à atténuer les risques.

Section 4 : Système commun de notation des vulnérabilités (CVSS)

Les graphes d'attaque sont élaborés à partir de l'information sur la vulnérabilité d'un réseau. Dans la présente section, nous expliquerons le Système commun de notation des vulnérabilités, qui est un cadre ouvert d'évaluation des vulnérabilités mis au point par FIRST.Org Inc. (2019b) pour communiquer la gravité des vulnérabilités des logiciels. Il est largement utilisé dans les études de vulnérabilité à titre de norme. Dans la présente étude, nous avons utilisé la plus version la plus récente, CVSS 3.1.

4.1 Spécifications techniques du CVSS

À l'aide du CVSS, il est possible d'attribuer une note à une vulnérabilité particulière en répondant à un jeu de questions. Selon les caractéristiques et la gravité d'une vulnérabilité, une note de 0 à 10 est attribuée. D'après cette note, chaque vulnérabilité est classée dans les catégories Aucune, Faible, Moyenne, Élevée et Critique de l'échelle de notation qualitative.

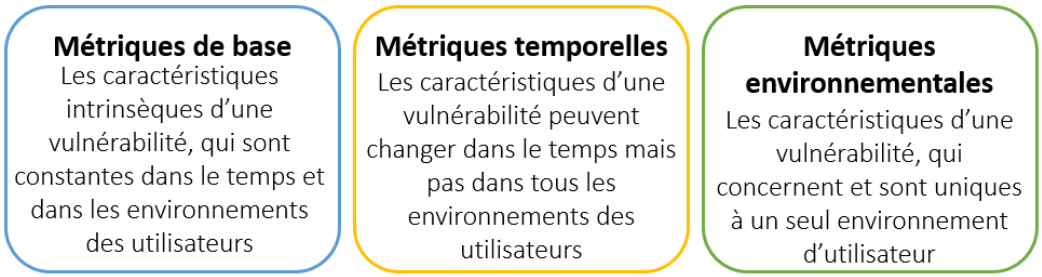
Il existe trois groupes principaux de métriques dans le système CVSS : les métriques de base, les métriques temporelles et les métriques environnementales (figure 5) :

- Les métriques de base sont communes pour une vulnérabilité au sein de toutes les organisations et elles ne changent pas au fil du temps.
- Les métriques temporelles peuvent changer au fil du temps.
- Les métriques environnementales permettent d'adapter la note à chaque organisation. (FIRST.Org Inc., 2019a)

Des métriques de base sont nécessaires pour calculer la note du système CVSS. Les métriques temporelles et environnementales sont facultatives. Les utilisateurs peuvent utiliser toute l'information disponible pour mettre à jour la note en fonction des changements au chapitre de la maturité du code d'exploitation ou des effets sur leur propre organisation (FIRST.Org Inc., 2019a).

Figure 5

GROUPES DE MÉTRIQUE DU SYSTÈME CVSS



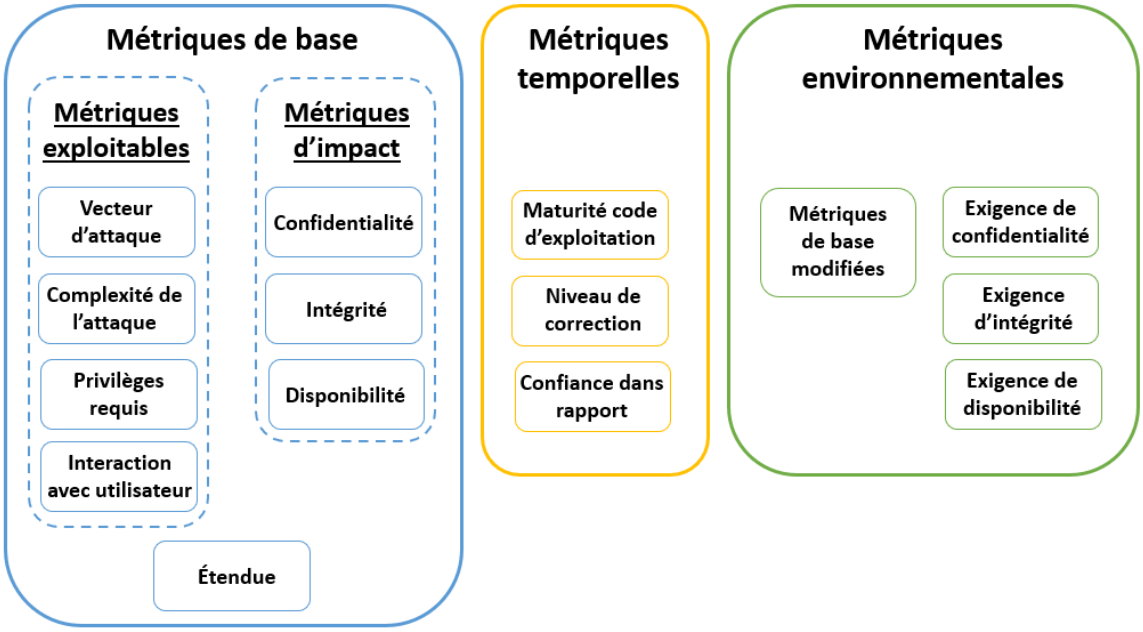
Source : Adapté de FIRST.Org Inc. (2019a)

Chaque groupe de métriques comprend plusieurs métriques (voir la figure 6) :

- Les métriques de base sont le vecteur d'attaque, la complexité de l'attaque, les privilèges requis, l'interaction avec l'utilisateur et les métriques d'impact pour les composantes CID.
- Les métriques temporelles sont la maturité du code d'exploitation, le niveau de correction et la confiance dans le rapport.
- Les métriques environnementales sont des métriques de base modifiées et des exigences de sécurité (exigence de confidentialité, exigence d'intégrité et exigence de disponibilité) (FIRST.Org Inc., 2019a).

Figure 6

MÉTRIQUES DU SYSTÈME CVSS

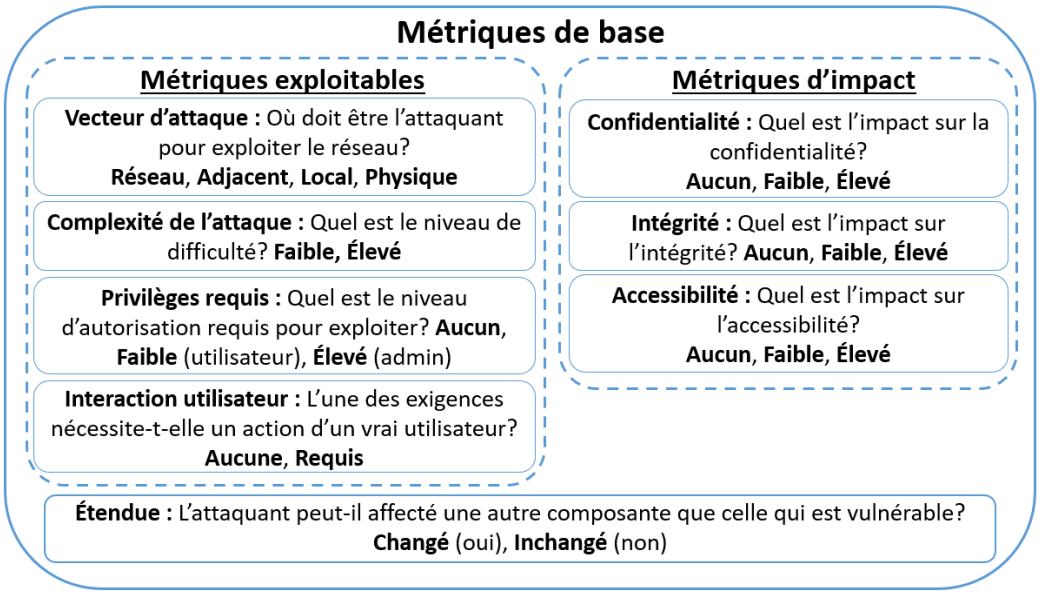


Source : Adapté de FIRST.Org Inc. (2019a)

La valeur de chaque métrique est déterminée en répondant à une question au sujet des caractéristiques de la vulnérabilité. Les questions et les réponses possibles pour les mesures de base sont présentées dans la figure 7. Chaque valeur possible des métriques est également représentée par une valeur numérique. Par exemple, la métrique Vecteur d'attaque indique où l'attaquant doit être pour pouvoir exploiter la vulnérabilité. Dans ce cas, il existe quatre possibilités : Réseau, Adjacent, Local et Physique. Si la valeur est Réseau, cela signifie qu'un attaquant sur l'Internet peut exploiter la vulnérabilité. Toutefois, si la valeur est Physique, seul un attaquant qui peut toucher et contrôler physiquement l'ordinateur avec la vulnérabilité peut l'exploiter, ce qui signifie qu'il est plus difficile de l'exploiter.

Figure 7

QUESTIONS DU GROUPE DES MÉTRIQUES DE BASE DU CVSS ET VALEURS POSSIBLES

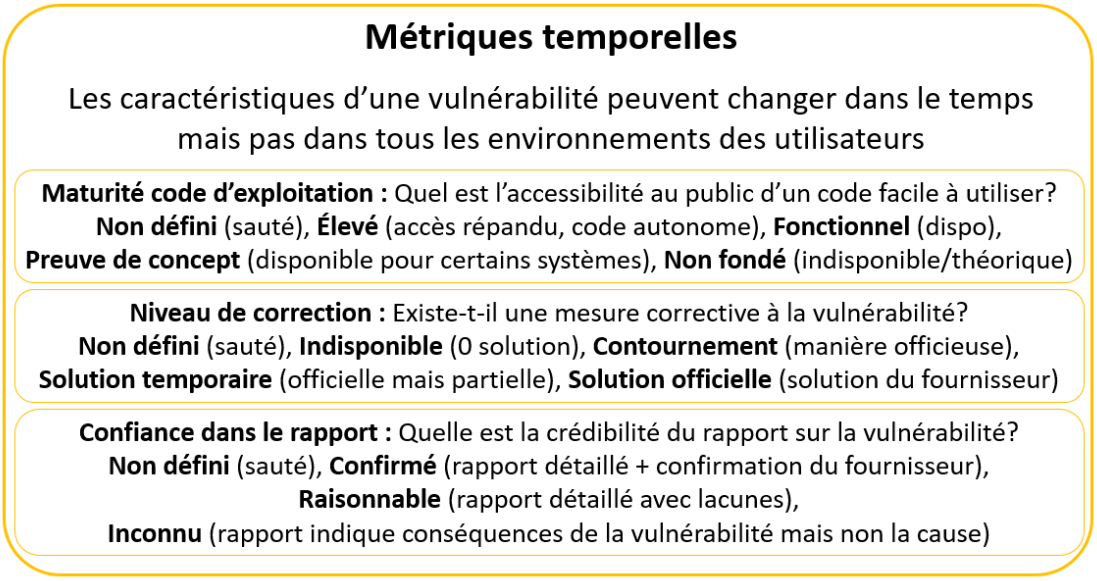


Source : Adapté de FIRST.Org Inc. (2019a)

Les métriques temporelles sont composées de la maturité du code d'exploitation (c.-à-d., le code d'exploitation est-il disponible?), du niveau de correction (c.-à-d., existe-t-il une solution pour cette vulnérabilité?) et de la confiance dans le rapport (c.-à-d., dans quelle mesure la source du rapport est-elle fiable?). L'évaluation de ces facteurs est expliquée dans la figure 8.

Figure 8

QUESTIONS DU GROUPE DES MÉTRIQUES TEMPORELLES DU CVSS ET LES VALEURS POSSIBLES



Source : Adapté de FIRST.Org Inc. (2019a)

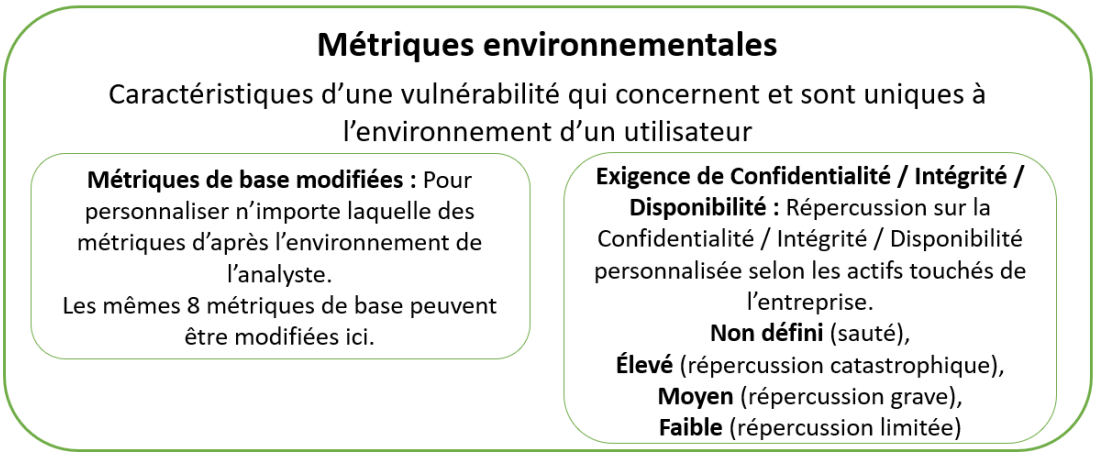
Les métriques environnementales se composent de deux sous-groupes :

- Métriques de base modifiées (pour personnaliser n'importe laquelle des métriques).
- Exigences en matière de confidentialité, d'intégrité et de disponibilité (leur importance pour l'actif).

Les descriptions des métriques environnementales sont fournies dans la figure 9.

Figure 9

QUESTIONS DU GROUPE DES MÉTRIQUES ENVIRONNEMENTALES DU CVSS ET LES VALEURS POSSIBLES



Source : Adapté de FIRST.Org Inc. (2019a)

La valeur d'une vulnérabilité en vertu du CVSS est représentée comme une chaîne vectorielle, constituée de toute l'information sur la vulnérabilité exprimée sous forme abrégée. Les abréviations de chaque métrique et les valeurs possibles sont présentées au tableau 1. Voici un exemple de la chaîne vectorielle d'un exemple de vulnérabilité, CVE-2019-10098 (Base de données nationale sur la vulnérabilité 2019) :

`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N`

L'interprétation de l'exemple de chaîne vectorielle est la suivante :

- Version 3.1 du CVSS
- Vecteur d'attaque : Réseau (`AV:N`)
- Complexité de l'attaque : Faible (`AC:L`)
- Privilèges requis : Aucun (`PR:N`)
- Interaction avec l'utilisateur : Requis (`UI:R`)
- Portée : Modifiée (`S:C`)
- Confidentialité : Faible (`C:L`)
- Intégrité : Faible (`I:L`)
- Disponibilité : Aucune (`A:N`)

Tableau 1

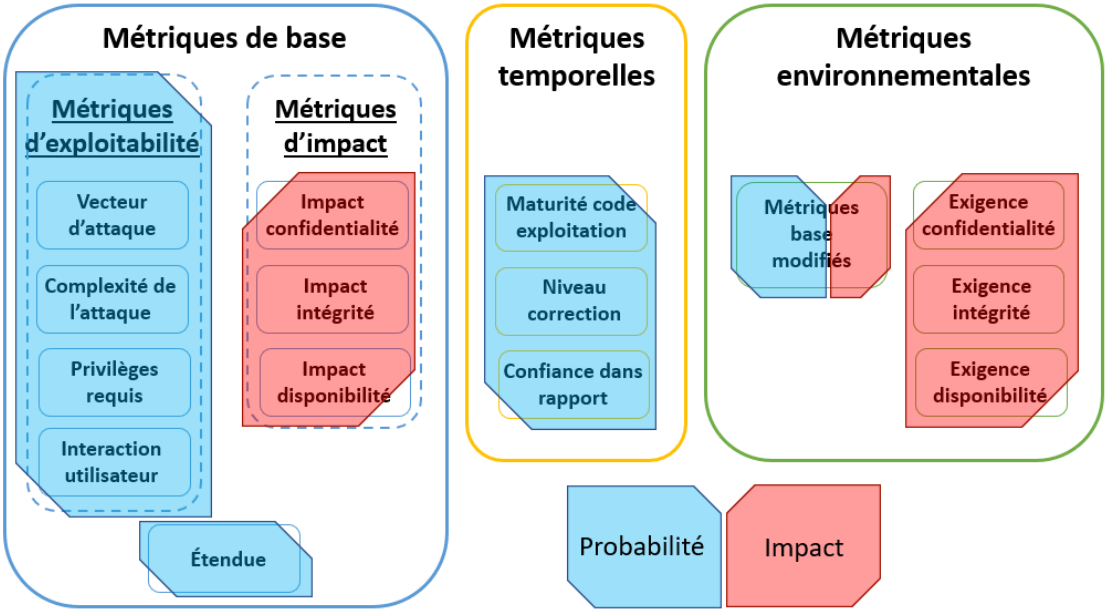
NOMS DES MÉTRIQUES, ABRÉVIATIONS ET VALEURS POSSIBLES AVEC ABRÉVIATIONS

Groupe de métriques	Nom de la métrique (et forme abrégée)	Valeurs possibles
Groupe de métriques de base	Vecteur d'attaque (AV)	Réseau (N), Adjacent (A), Local (L), Physique (P)
	Complexité de l'attaque (AC)	Faible (L), Élevée (H)
	Privilèges requis (RP)	Aucun (N), Faible (L), Élevé (H)
	Interaction utilisateur (UI)	Aucune (N), Requise (R)
	Portée (S)	Inchangée (U), Modifiée (C)
	Confidentialité (C)	Élevée (H), Faible (L), Aucune (N)
	Intégrité (I)	Élevée (H), Faible (L), Aucune (N)
	Disponibilité (A)	Élevée (H), Faible (L), Aucune (N)
Groupe de métriques temporelles	Maturité du code d'exploitation (E)	Non défini (X), Élevé (H), Fonctionnel (F) Validation de principe (P), Non validé (U)
	Niveau de correction (RL)	Non défini (X), Non disponible (U), Solution de rechange (W), Correction temporaire (T), Correction officielle (O)
	Confiance dans le rapport (RC)	Non définie (X), Confirmée (C), Raisonnable (R), Inconnue (U)
Groupe de métriques environnementales	Exigence de confidentialité (CR)	Non définie (X), Élevée (H), Moyenne (M), Faible (L)
	Exigence en matière d'intégrité (IR)	Non définie (X), Élevée (H), Moyenne (M), Faible (L)
	Exigence de disponibilité (AR)	Non définie (X), Élevée (H), Moyenne (M), Faible (L)
	Vecteur d'attaque modifié (MAV)	Non défini (X), Réseau (N), Adjacent (A), Local (L), Physique (P)
	Complexité de l'attaque modifiée (CAM)	Non définie (X), Faible (L), Élevée (H)
	Privilèges requis modifiés (MPR)	Non définis (X), Aucun (N), Faibles (L), Élevés (H)
	Interaction utilisateur modifiée (MUI)	Non définie (X), Aucune (N), Requise (R)
	Portée modifiée (MS)	Non définie (X), Inchangée (U), Modifiée (C)
	Confidentialité modifiée (MC)	Non définie (X), Élevée (H), Faible (L), Aucune (N)
	Intégrité modifiée (MI)	Non définie (X), Élevée (H), Faible (L), Aucune (N)
	Disponibilité modifiée (MA)	Non définie (X), Élevée (H), Faible (L), Aucune (N)

Source : Adapté de FIRST.Org Inc. (2019a)

Dans la figure 10, les métriques du CVSS utilisées pour le calcul de la probabilité et de l'impact sont indiquées par des formes bleues et rouges, respectivement.

Figure 10
MÉTRIQUES UTILISÉES POUR CALCULER LES VALEURS DE LA VRAISEMBLANCE ET DE L'IMPACT



- L'estimation de la vraisemblance repose sur les métriques d'exploitabilité (vecteur d'attaque, complexité de l'attaque, privilèges requis et interaction avec l'utilisateur), la portée, les métriques temporelles (maturité du code d'exploitation, niveau de correction et confiance dans le rapport), les métriques d'exploitabilité modifiées (vecteur d'attaque modifié, complexité de l'attaque modifiée, privilèges requis modifiés et interaction avec l'utilisateur modifiée), et la portée modifiée, comme le montre la figure 10.
- L'estimation de l'impact est fondée sur les métriques d'impact (impact sur la confidentialité, impact sur l'intégrité et impact sur la disponibilité), les métriques d'impact modifiées (impact sur la confidentialité modifiée, impact sur l'intégrité modifiée et impact sur la disponibilité modifiée), et les exigences de sécurité (exigence de confidentialité, exigence d'intégrité et exigence de disponibilité), également indiquées dans la figure 10.

Les métriques temporelles et environnementales peuvent être utilisées dans le cadre élaboré; toutefois, elles sont facultatives et ne sont pas fournies dans la Base nationale de données sur la vulnérabilité (BDNV). Les valeurs doivent être déterminées et appliquées manuellement aux calculs. De plus amples renseignements sur le calcul de la probabilité figurent à la section 5.2, et le calcul de l'impact est abordé à la section 6.5.

4.2 Base de données nationale sur les vulnérabilités et expositions et vulnérabilités communes

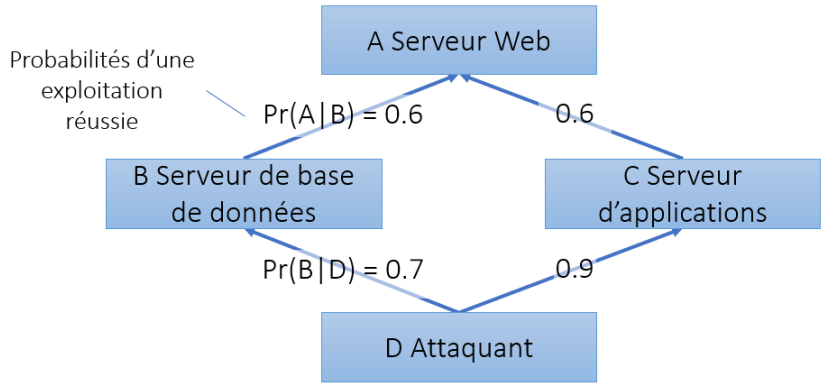
Le National Institute of Standards and Technology fournit toutes les vulnérabilités connues du matériel et des logiciels, ainsi que leurs notes du CVSS dans la BDNV. Les vulnérabilités et les expositions communes (CVE) sont énumérées par la MITRE Corporation et elles sont intégrées à la BDNV. En fonction de la disponibilité, chaque inscription comprend une brève description, le logiciel visé, les notes de base des versions 2.0 et 3.1 du CVSS, ainsi que des renseignements sur les correctifs officiels ou les commentaires du fabricant ou du développeur. Dans la présente étude, les valeurs des métriques spécifiques de la version 3.1 du CVSS pour chaque vulnérabilité sont extraites de la BDNV. Ces données sont utilisées comme intrants pour les analyses des graphes d'attaque et des graphes d'impact.

Section 5 : Graphe d'attaque bayésien pour l'analyse des risques

La probabilité d'attaque peut être calculée en fonction du nombre et des caractéristiques des vulnérabilités d'un actif de TIC. Toutefois, dans les attaques à plusieurs étapes, où l'attaquant exploite un système vulnérable pour l'utiliser comme tremplin pour la cible réelle, l'utilisation des valeurs individuelles de vraisemblance de chaque vulnérabilité serait insuffisante pour calculer le cyberrisque global du réseau. Pour calculer la vraisemblance d'une attaque à plusieurs étapes, il faut combiner les probabilités individuelles. Ces probabilités cumulées sont calculées en utilisant des réseaux bayésiens sur des graphes d'attaque, ce qui introduit le concept de graphe d'attaque bayésien.

Par exemple, la figure 11 représente un graphe d'attaque où les hôtes (composantes du réseau de TIC) sont indiqués comme des nœuds. A, B et C sont des hôtes dans le système et D est l'attaquant sur Internet. L'attaquant peut utiliser le serveur de base de données ou le serveur d'application pour atteindre sa cible, le serveur Web. Les probabilités conditionnelles d'exploitation sont indiquées aux limites, juste avant chaque hôte qui présente la vulnérabilité. La probabilité qu'une vulnérabilité dans le serveur de base de données soit exploitée avec succès, sachant que l'attaquant veut exploiter et est capable d'exploiter, est de 0,7 et notée Pr(B|D). Cette valeur de probabilité est estimée en fonction des caractéristiques intrinsèques de la vulnérabilité qui existent dans le serveur de base de données.

Figure 11
EXEMPLE DE GRAPHE D'ATTAQUE BAYÉSIEN



Source : Adapté de Poolsappasit, Dewri et Ray (2012).

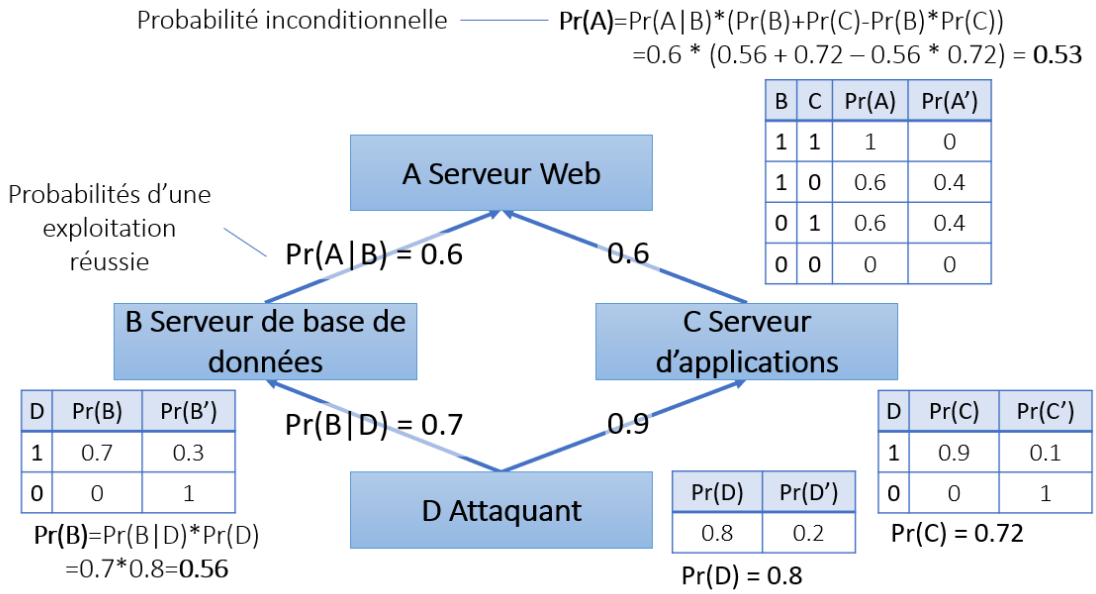
Ce graphe comporte deux chemins d'attaque. Dans les deux cas, l'attaquant pourrait attaquer le serveur Web. Les deux chemins sont reliés au serveur Web au moyen d'une logique OU et elles ne sont pas des préalables l'une de l'autre.

5.1 Calcul des probabilités conditionnelles locales et des probabilités inconditionnelles

La logique bayésienne est utilisée pour analyser le graphe d'attaque dans son ensemble et pour fournir des probabilités inconditionnelles pour chaque nœud en tenant compte de toutes les probabilités précédentes. La figure 12 présente les calculs des probabilités inconditionnelles d'un graphe d'attaque bayésien.

Figure 12

PROBABILITÉS DES NŒUDS D'UN GRAPHE D'ATTAQUE BAYÉSIEN



Source : Adapté de Poolsappasit, Dewri et Ray (2012) et Wang et coll. (2008)

Tout d'abord, une probabilité est attribuée, d'après l'expérience du défenseur, à l'attaquant qui lance une attaque sur le réseau. Dans ce cas, une note de 0,8 est attribuée à Pr(D) = Pr (D = Vrai). Pr(D') = Pr (D = Faux) est la probabilité que l'attaquant n'attaquera pas et elle est calculée en soustrayant Pr(D) de 1. Certains calculs ci-après s'appuient sur la valeur de probabilité Pr(D) sous forme de chaînes. Les tableaux de la figure 12 représentent une distribution de probabilité conditionnelle locale. Ces tableaux ne comprennent que des probabilités locales (c.-à-d. l'hôte avec la vulnérabilité et la condition des nœuds précédents). Les tableaux montrent toutes les possibilités des conditions locales et ils fournissent les probabilités. Par exemple, comme le montre le tableau 2, la probabilité d'exploiter avec succès une vulnérabilité dans le serveur d'applications est de 0,9, étant donné que l'attaquant est disposé et apte à attaquer. Dans ce cas, Pr(C|D) est égal à 0,9, qui peut aussi être exprimé comme Pr(C|D=Vrai) = 0,9. La probabilité de ne pas exploiter la vulnérabilité étant donné que l'attaquant est disposé et apte à attaquer est de Pr(C'|D) = 1 – Pr(C|D) = 0.1. Puisqu'il n'est pas possible que cette exploitation réussisse sans l'intention de l'attaquant, sa probabilité est nulle; donc, Pr(C|D') = 0.

Tableau 2

DISTRIBUTION DE PROBABILITÉS CONDITIONNELLES LOCALES POUR C (SERVEUR D'APPLICATIONS)

D	Pr(C)	Pr(C')
1/Vrai	Pr(C|D) = Pr(C|D = Vrai) = 0,9	Pr(C'|D) = Pr(C'|D = Vrai) = 0,1
0/Faux	Pr(C|D') = Pr(C|D = Faux) = 0	Pr(C'|D') = Pr(C'|D = Faux) = 1

En calculant la distribution de probabilité conditionnelle locale pour les nœuds avec la logique OU, les probabilités de tous les chemins doivent être prises en compte. Les calculs sont les mêmes pour les autres cas, sauf lorsque les valeurs des deux nœuds sont Vrai. Dans le cas où les deux nœuds précédents ont déjà été exploités avec succès, la probabilité présentant la valeur la plus élevée devient la valeur de ce nœud.

Pour comprendre la vraisemblance réelle qu'un hôte soit exploité, les distributions de probabilité conditionnelles locales ne sont pas suffisantes. Les probabilités inconditionnelles doivent être calculées en tenant compte de toutes les probabilités des événements antérieurs (Wang et coll., 2008; Shetty et coll., 2018). Par exemple, la probabilité d'exploitation réussie de la vulnérabilité dans le serveur de base de données est de 0,7, étant donné que l'attaquant est prêt à lancer l'attaque. La probabilité de l'existence de l'action d'un attaquant est de 0,8. Par conséquent, la probabilité inconditionnelle d'exploitation du serveur de base de données est calculée comme suit :

$$Pr(B) = Pr(B|D) * Pr(D) = 0.7 * 0.8 = 0.56$$

De même, la probabilité inconditionnelle d'exploitation réussie de la vulnérabilité dans le serveur d'applications est calculée comme suit :

$$Pr(C) = Pr(C|D) * Pr(D) = 0.9 * 0.8 = 0.72$$

Comme on peut l'observer, même si les valeurs de probabilité conditionnelle sont relativement élevées, les probabilités inconditionnelles sont plus faibles en raison de la nature des attaques à plusieurs étapes. À mesure que la chaîne s'allonge, la vraisemblance d'une attaque diminue dans une large mesure.

Enfin, la probabilité inconditionnelle de l'exploitation réussie de la vulnérabilité du serveur Web, qui est la cible ultime, est calculée en tenant compte des deux chemins d'attaque. Le lien logique OU (Wang et coll., 2008) est établi comme suit :

$$Pr(A) = Pr(A|B) * (Pr(B) + Pr(C) - \Pr(B) * \Pr(C)) = 0.6 * (0.56 + 0.72 - 0.56 * 0.72) = 0.53$$

Les valeurs de probabilité inconditionnelle sont des mesures importantes pour calculer les risques posés par chaque composante du réseau des TIC. Ces calculs sont largement utilisés dans la présente étude.

5.2 Valeurs de probabilité d'exploitation réussie de chaque vulnérabilité (vraisemblance)

Les calculs de la distribution de probabilité conditionnelle locale et des probabilités inconditionnelles ont déjà été expliqués. Ces calculs dépendent des valeurs de probabilité de l'exploitation réussie de chaque vulnérabilité. Nous parlons également de « vraisemblance » dans la présente étude. Les valeurs de vraisemblance sont calculées à l'aide de métriques particulières des groupes de métriques de base et temporelles du CVSS.

Les métriques du CVSS fournissent de l'information sur la vraisemblance et l'impact. Les métriques pertinentes pour la vraisemblance sont les suivantes :

- Vecteur d'attaque (AV)
- Complexité de l'attaque (AC)
- Privilèges requis (RP)
- Interaction utilisateur (UI)
- Portée (S)
- Maturité du code d'exploitation (E)
- Niveau de correction (RL)
- Confiance dans le rapport (RC)

Les cinq premières métriques se trouvent dans le groupe des métriques de base et elles figurent dans la BDNV; toutefois, les trois dernières métriques font partie du groupe des métriques temporelles et elles ne figurent pas dans la BDNV, car leurs valeurs réelles peuvent changer au fil du temps. Dans la présente étude, ces métriques servent à calculer la vraisemblance (probabilité d'exploitation réussie de chaque vulnérabilité). La vraisemblance est une valeur décimale comprise entre zéro et un, et l'équation 2 montre son mode de calcul :

$$\Pr(e_i) = 2.1 * \text{Vecteur d'attaque} * \text{Complexité de l'attaque} * \text{Privilèges requis} * \text{Interaction avec l'utilisateur} * \text{Maturité du code d'exploitation} * \text{Niveau de correction} * \text{Confiance dans le rapport}$$ Équation 2

Nous avons multiplié les valeurs des paramètres du CVSS par 2,1 pour normaliser la vraisemblance d'une valeur de 0 à 1. Il existe dans la littérature des méthodes semblables servant à calculer les probabilités conditionnelles d'exploitation des vulnérabilités à l'aide des métriques du CVSS. Singhal et Ou (2011), Nicol et Mallapura (2014), et Shetty et coll. (2018) ont utilisé la version 2.0 du CVSS pour calculer les probabilités d'exploitation des vulnérabilités. De façon générale, les études antérieures n'utilisaient que les métriques de l'exploitabilité (vecteur d'attaque, complexité de l'attaque et privilèges requis [authentification pour la version 2.0 du système CVSS]). Pour calculer la probabilité, Singhal et Ou (2011) n'ont utilisé que la métrique de la complexité de l'attaque en attribuant une valeur numérique fondée sur des catégories, comme 0,2, 0,6 et 0,9 pour la complexité élevée, moyenne et faible de l'attaque, respectivement. Nicol et Mallapura (2014) ont amélioré l'approche et ont tenu compte de la complexité de l'attaque et des privilèges requis (c.-à-d. l'authentification). Ils ont aussi inversé la note d'exploitabilité afin de fournir de plus petites valeurs pour les attaques plus faciles dans le calcul de la difficulté/des coûts de l'attaque. L'évolution originale de la version 2.0 du CVSS (Mell, Scarfone et Romanosky 2007) précise que le multiplicateur de la note d'exploitabilité est 20. Cependant, Shetty et coll. (2018) ont modifié cette formule en ramenant le multiplicateur à 2 afin de normaliser les valeurs de vraisemblance entre 0 et 1. Dans la présente étude, nous avons utilisé la version 3.1 du CVSS, qui comprend les métriques indiquées au tableau 3. L'équation 2 modifie la note d'exploitabilité en incluant des métriques temporelles pour calculer plus précisément la valeur de la vraisemblance.

Les valeurs numériques requises pour calculer la probabilité d'une exploitation réussie sont fournies dans la BDNV à l'aide du CVSS. Pour chaque métrique de l'équation de vraisemblance, une représentation numérique de la réponse à la question pertinente dans les spécifications du système CVSS doit être utilisée. Les chiffres du tableau 3 sont utilisés dans l'équation 2. À propos du processus de collecte des chiffres et des équations du CVSS, FIRST.Org Inc. (2019a) fournit l'énoncé suivant :

> [traduction libre] « La formule de la version 3.1 du CVSS fournit une approximation mathématique de toutes les combinaisons possibles de métriques classées par ordre de gravité (un tableau de consultation des vulnérabilités). Pour produire la formule de la version 3.1 du CVSS, le Groupe d'intérêts spéciaux (GIS) du CVSS a encadré le tableau de consultation en attribuant des valeurs de métriques aux vulnérabilités réelles, de même qu'un groupe de gravité (faible, moyenne, élevée, critique). Après avoir défini les fourchettes numériques acceptables pour chaque degré de gravité, le GIS a collaboré avec Deloitte & Touche LLP pour rajuster les paramètres de la formule afin d'harmoniser les combinaisons de métriques avec les cotes de gravité proposées par le GIS. »

Les valeurs des métriques et des équations du CVSS ont été testées avec des vulnérabilités réelles afin d'analyser et de communiquer les risques de vulnérabilité avec plus d'exactitude. Le CVSS représente un modèle de normalisation de la notation des vulnérabilités qui s'applique à toutes les vulnérabilités connues. Il permet les évolutions, les prolongations et l'adaptation (p. ex., les métriques environnementales) pour être mieux adapté aux caractéristiques évolutives des vulnérabilités.

La métrique relative à la portée dans le CVSS permet de déterminer si une vulnérabilité dans une composante peut influer sur une autre composante du réseau des TIC. Cette métrique a un effet distinct sur la façon dont la vraisemblance est calculée. Elle modifie les valeurs numériques des valeurs Faible et Élevée de la métrique Privilèges requis.

L'information fournie au sujet d'une vulnérabilité dans le BDNV pourrait ne pas correspondre à l'environnement propre à la composante du réseau des TIC à l'étude. Dans ce cas, les métriques modifiées du groupe de métriques environnementales du CVSS sont utilisées. Cela permet de modifier les valeurs prédéfinies par la BDNV en fonction des caractéristiques distinctes de la composante à l'étude.

Tableau 3

VALEURS NUMÉRIQUES DES MÉTRIQUES DE LA VRAISEMBLANCE

Groupe de métriques	Métrique	Valeur de la métrique	Valeur numérique
Métriques de base	Vecteur d'attaque (AV)	Réseau	0,85
		Adjacente	0,62
		Locale	0,55
		Physique	0,2
	Complexité de l'attaque (AC)	Faible	0,77
		Élevée	0,44
	Privilèges requis (RP)	Aucune	0,85
		Faible	0,62 (0,68 si la portée est modifiée)
		Élevée	0,27 (0,5 si la portée est modifiée)
	Interaction avec l'utilisateur (UI)	Aucune	0,85
		Requise	0,62
Métriques temporelles	Maturité du code d'exploitation (E)	Non définie	1
		Élevée	1
		Fonctionnelle	0,97
		Validation de principe	0,94
		Non prouvée	0,91
	Niveau de correction (RL)	Non défini	1
		Non disponible	1
		Solution de rechange	0,97
		Correction temporaire	0,96
		Correction officielle	0,95
	Confiance dans le rapport (RC)	Non définie	1
		Confirmée	1
		Raisonnable	0,96
		Inconnue	0,92

Source : Adapté de FIRST.Org Inc. (2019a)

5.3 Le facteur humain dans les cyberrisques

Les personnes – utilisateurs, administrateurs de système ou propriétaires de TIC – jouent un rôle essentiel dans la cybersécurité et elles en assument la responsabilité. Même dans les réseaux bien protégés, un utilisateur négligent peut causer une violation en cliquant sur un lien ou en modifiant involontairement une configuration de sécurité. Ce cadre comprend un facteur humain dans les analyses de la vraisemblance de réussite de l'attaque et de son impact.

Certaines vulnérabilités nécessitent une action de la part de l'utilisateur. Pour ce type de vulnérabilité, un humain est ajouté comme nœud au graphe d'attaque avec une valeur de probabilité permettant l'exploitation. Si l'exploitation d'une vulnérabilité nécessite un accès privilégié, elle influe sur la probabilité puisqu'elle nécessite un hameçonnage ou une attaque d'ingénierie sociale contre les utilisateurs ou les administrateurs de système.

Selon la spécification originale du CVSS, nous avons classé les métriques des facteurs humains en deux groupes : métriques de base et métriques environnementales. Les valeurs de vraisemblance des métriques de base ont été déterminées à partir d'une enquête menée par Alohali et considérées comme identiques pour toutes les organisations, même si les décideurs peuvent les modifier. Les métriques de l'exploitabilité de base comprennent la vulnérabilité des personnes aux infractions relatives aux composantes CID (voir le tableau 4).

Les métriques d'impact de base comprennent les niveaux d'utilisateur suivants : Utilisateur ordinaire, utilisateur de niveau C (comme le dirigeant principal de la sécurité de l'information [DPSI] et le dirigeant principal de l'information [DPI]), et l'administrateur de système. L'impact de l'extraction des justificatifs d'identité des personnes de chacune de ces trois catégories dans le système des TIC serait différent. Par exemple, étant donné qu'un administrateur de système peut avoir un accès élargi aux actifs de TIC de l'entreprise et détenir le pouvoir de modifier les configurations de sécurité, l'impact de la perte des justificatifs de l'identité de l'administrateur est le plus élevé.

Les valeurs des métriques environnementales ont une nature plus subjective et elles évoluent selon l'environnement de l'entreprise. Les métriques environnementales liées aux facteurs humains comprennent deux groupes : la cyberhygiène des employés et la cybersécurité à l'échelle de l'entreprise. Le premier concerne la vraisemblance et le second, l'impact. Les décideurs devraient déterminer les valeurs numériques en fonction des caractéristiques de l'entreprise.

La cyberhygiène des utilisateurs et des administrateurs de système influe sur la vraisemblance d'un événement indésirable. L'exécution d'un test d'hameçonnage auprès des employés donnerait une idée de la façon dont ils réagissent aux courriels contenant des liens suspects. Qu'il s'agisse de dissimuler une cyberinfraction chez les employés de l'entreprise ou de la rendre publique de façon transparente à des fins de responsabilisation est un indicateur essentiel de la fiabilité des employés. La fiabilité se répercuterait sur la sensibilisation à la cybersécurité et elle inciterait les employés à se montrer plus prudents à l'égard des cybermenaces. La tenue d'ateliers ou de séances de formation sur la sensibilisation à la cybersécurité contribue à améliorer la cyberhygiène. De plus, la formation certifiée, surtout pour les administrateurs de système, est une étape cruciale.

La cybersécurité à l'échelle de l'entreprise influe sur l'impact d'un cyberincident. L'existence d'un poste de DPSI ou d'un service de cybersécurité dans une entreprise engendre une meilleure préparation et une meilleure défense contre les cyberincidents. De plus, les gouvernements et les chefs de file de l'industrie ou les organismes de réglementation élaborent et appliquent des normes de conformité ou recommandent leur application.

Tableau 4

MÉTRIQUES LIÉES AUX FACTEURS HUMAINS

Groupe de métriques	Groupe de sous-métriques	Métrique	Valeur de la métrique	Valeur numérique
Métriques de base liées aux facteurs humains	Vraisemblance	Susceptibilité à une violation de la confidentialité	Susceptible	0,32
		Susceptibilité à une violation d'intégrité	Susceptible	0,24
		Susceptibilité à une rupture de disponibilité	Susceptible	0,13
	Impact	Privilèges requis	Utilisateur ordinaire	0,30
			Utilisateur de niveau C	0,45
			Administrateur de système	1,00
Métriques environnementales liées aux facteurs humains	Cyberhygiène des utilisateurs et des administrateurs de système de l'entreprise (vraisemblance)	Résultats des tests d'hameçonnage	Positifs	
			Négatifs	
		Déclaration des cyberincidents	Masquée	
			Déclarée	
		Formation de sensibilisation à la sécurité au cours de la dernière année	Aucune	
			Une fois	
			Plusieurs fois	
		Certification en cybersécurité et formation des administrateurs de système	Aucune formation	
			Formation	
			Certificat	
	Cybersécurité à l'échelle de l'entreprise (impact)	Poste de DPSI ou l'équivalent	Oui	
			Non	
		Service de cybersécurité	Oui	
			Non	
		Conformité aux normes gouvernementales ou industrielles (p. ex., ISO 27001, PCIDSS)	Aucune conformité	
			En attente	
			Conformité	

Section 6 : Graphe d'impact

Le graphe de dépendance d'impact, à la figure 13 propose une vue de dépendance d'une entreprise (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet, 2016). Les entreprises peuvent être considérées comme ayant trois niveaux : une couche d'actifs, une couche de services et une couche de processus opérationnels. Nous avons choisi cette structure comme cadre de référence pour la représentation des couches organisationnelles et leurs dépendances. Les limites du système d'entreprise sont déterminées dans cette section tout en générant le graphe d'impact, qui est un réseau de dépendances fonctionnelles de l'entreprise qui indique tous les actifs, services et processus opérationnels, ainsi que les dépendances fonctionnelles au sein de ces trois couches et entre elles (c.-à-d. les dépendances horizontales et verticales).

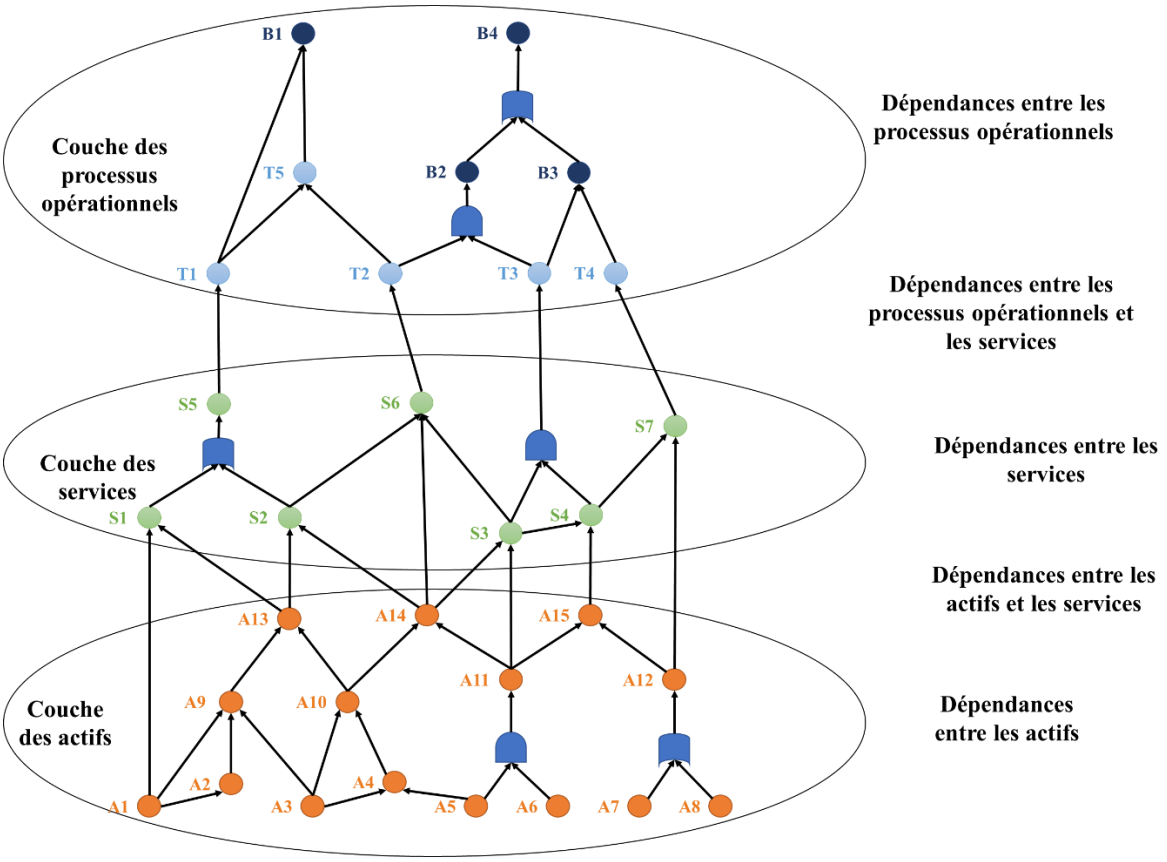
- La *couche d'actifs* se compose de logiciels, de matériel, de données et de personnes. Dans l'approche axée sur les actifs, qui est la plus courante dans l'analyse des risques, des milliers d'actifs dans une organisation de taille moyenne doivent être analysés et mis à jour périodiquement selon divers scénarios de risque (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet, 2016).
- La *couche des services* repose sur les actifs visant à faciliter les tâches et les processus opérationnels. La connexion Internet, la gestion de l'identité, les courriels et la vidéoconférence sont quelques-uns des services qui peuvent être offerts dans une entreprise. Dans la perspective axée sur les services, les risques sont cernés et évalués en fonction de leur incidence sur les services (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet ,2016).
- La *couche des processus opérationnels* est supérieure et elle repose sur les couches des actifs et des services. Un processus opérationnel se compose de tâches reliées pour atteindre un objectif organisationnel (Bititci et Muir, 1997). Bien que la couche des processus opérationnels soit principalement utilisée dans le contexte civil, elle est appelée *couche des missions* dans le domaine militaire. Dans le présent document, ces deux expressions sont utilisées de façon interchangeable. Du point de vue opérationnel, les valeurs ne sont pas attribuées aux actifs, mais plutôt aux processus qui sont directement liés aux objectifs opérationnels (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet, 2016).

Une *dépendance verticale* est une vue ascendante qui tient compte du degré de contribution d'une ressource à un nœud d'une couche supérieure, comme illustré à la figure 13. Bien qu'une vue verticale indique les dépendances entre les ressources de différentes couches, une *dépendance horizontale* renvoie aux dépendances entre les ressources de la même couche (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet, 2016).

Dans un *modèle non propagé*, on suppose que l'impact n'est pas propagé à d'autres ressources à l'intérieur des couches ou entre elles. Dans un *modèle propagé*, l'impact de l'attaque sur la ressource compromise est habituellement propagé à d'autres ressources par des dépendances verticales et horizontales (Bahsi et coll., 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar et Cheriet, 2016).

L'impact des cybermenaces et des cyberincidents sur les actifs des systèmes d'information est évalué en fonction des propriétés de sécurité, de la confidentialité, de l'intégrité et de la disponibilité. Selon la définition donnée précédemment, la *confidentialité* consiste à [traduction libre] « préserver les restrictions autorisées à l'accès à l'information et à sa divulgation, y compris les moyens de protéger les renseignements personnels et exclusifs » (McCallister, Grance et Scarfone, 2010). L'*intégrité* représente [traduction libre] « l'objectif de sécurité qui crée l'exigence d'une protection contre les tentatives intentionnelles ou accidentelles qui portent atteinte à l'intégrité des données (la propriété selon laquelle les données n'ont pas été modifiées de façon non autorisée) ou l'intégrité des systèmes (la qualité d'un système lorsqu'il remplit sa fonction prévue d'une manière non altérée, sans manipulation non autorisée) » (Stoneburner, 2001). La *disponibilité* consiste à [traduction libre] « assurer un accès rapide et fiable à l'information et à son utilisation » (Ross, McEvilley et Oren, 2016).

Figure 8
GRAPHE DE DÉPENDANCE DE L'IMPACT



Remarque : A = actifs; B = processus opérationnels; S = services; T = tâches.

6.1 Contexte et travaux connexes sur l'impact

Nous avons exécuté l'examen systématique de 22 documents choisis sur 773 pertinents. Cet examen avait pour but de consulter, de résumer et de critiquer la documentation qui décrit ce qui est connu au sujet de l'impact des cyberincidents sur les processus opérationnels (Bahsi et coll., 2018). Dans la présente section, nous indiquerons les lacunes en matière de connaissances relevées dans notre recherche (Bahsi et coll., 2018).

D'après l'examen systématique de la documentation sur l'impact opérationnel des cyberincidents, nous avons cerné trois lacunes dans la recherche :

1. L'inexactitude des renseignements sur les dépendances;
2. Le suivi de la propagation de l'attaque, et non de l'impact, sur les dépendances horizontales de la couche d'actifs;
3. L'absence de propagation de l'impact entre toutes les couches verticales et à l'intérieur des couches horizontales.

Toutes les études que nous avons analysées comprenaient la propagation de l'impact au sein des différentes couches d'une entreprise et entre celles-ci. Toutefois, la plupart des relations de dépendance n'étaient pas bien définies. Premièrement, dans les modèles fondés sur des graphes, une dépendance est représentée comme un lien simple entre les nœuds. Nous devons compter sur des modèles de dépendance qui reflètent non seulement un lien simple entre les nœuds, mais aussi *la conjonction logique et la disjonction* dans les dépendances. Les aspects des cyberimpacts, comme l'impact sur les valeurs CID, doivent également être pris en compte dans les définitions de

dépendance de la fonction de propagation. Deuxièmement, les modèles actuels de propagation de l'impact que nous avons analysés étaient déterministes, à l'exception d'un *modèle probabiliste fondé sur un graphe*, pour évaluer les conséquences opérationnelles des cybermenaces (Granadillo et coll., 2016). Les modèles probabilistes représentent mieux les systèmes avec incertitude (p. ex., le choix par les attaquants des vulnérabilités à exploiter et leur impact subséquent) que les modèles déterministes, car ils sont plus rentables et leurs résultats sont plus faciles à communiquer aux décideurs de haut niveau (Kirchsteiger, 1999).

La dépendance horizontale dans la couche d'actifs est un concept important pour analyser la propagation de l'impact d'un cyberincident sur un actif et d'autres actifs. Toutefois, dans les études que nous avons analysées, ces dépendances n'ont été établies que pour l'identification des chemins d'attaque. La modélisation du graphe d'attaque, qui vise à trouver les dépendances entre les vulnérabilités de l'hôte pour déterminer les chemins d'attaque, ne fournit pas d'instrument pour évaluer la propagation de l'impact. Dans un scénario d'attaque type, les auteurs infiltrent le système cible; ils effectuent des mouvements latéraux; atteignent l'actif ou les données du système cible principal; et ils prennent les mesures finales comme l'exfiltration, la suppression ou la modification des données. Les dépendances horizontales existantes dans les études analysées nous permettent de suivre et d'évaluer les mouvements possibles d'un attaquant jusqu'à l'acte final. Par conséquent, ils peuvent contribuer à l'*évaluation* de la menace, mais non à son *impact*. Un cyberincident touche finalement un actif à la fin du chemin, et l'impact ne se propage qu'au service ou au processus opérationnel pour s'étendre davantage dans la même couche. Il est essentiel de déterminer les données et les dépendances fonctionnelles entre les différents actifs pour comprendre la propagation de l'impact au chemin d'attaque.

Pour que la mesure des risques soit plus précise, il convient de tenir compte de la propagation de l'impact à l'intérieur des couches des actifs, des services et des processus opérationnels d'une entreprise et entre celles-ci. Un nombre limité d'études seulement ont porté sur la propagation de l'impact dans toutes les dépendances verticales et horizontales, y compris les trois couches (Granadillo et coll., 2016; Jakobson, 2011; Lei, 2015; Llansó et Klatt, 2014). L'écart entre les évaluations du risque technique et du risque opérationnel persiste. Une analyse globale de l'impact ne peut être effectuée que lorsque tous les chemins possibles de propagation de l'impact sont pris en compte.

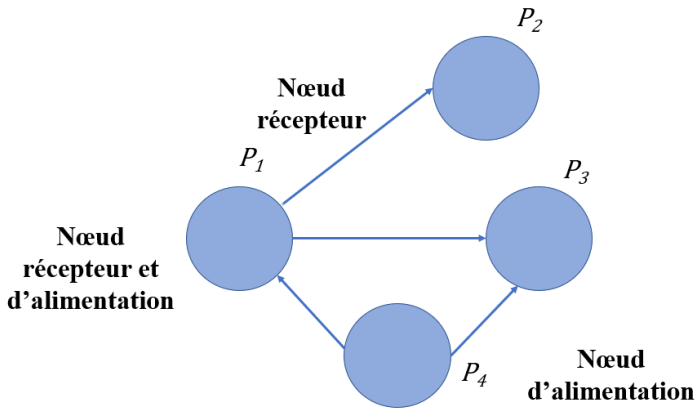
6.2 Aperçu de l'analyse des réseaux de dépendances fonctionnelles

L'analyse des réseaux de dépendances fonctionnelles (FDNA) est une méthode [traduction libre] « élaborée pour modéliser et mesurer les relations de dépendance entre les fournisseurs de technologies et les fournisseurs de services que ces technologies permettent à l'entreprise de fournir » (Garvey et Pinto, 2009).

Il est essentiel de modéliser les relations de dépendance entre les nœuds d'un système pour modéliser et mesurer les effets d'entraînement de la défaillance ou de la perte d'opérabilité de l'un des nœuds par rapport aux autres nœuds dont il dépend. La FDNA utilise la théorie des graphes pour définir les dépendances entre ses nœuds (figure 14).

La FDNA peut servir à modéliser les dépendances de divers systèmes, comme [traduction libre] « les domaines de l'économie des intrants-extrants, l'analyse des risques liés aux infrastructures essentielles et les problèmes non stationnaires, temporels d'analyse des dépendances » (Garvey et Pinto, 2009).

Figure 9
EXEMPLE DE TOPOLOGIE DE GRAPHE FDNA À QUATRE NŒUDS



Les principaux concepts de la FDNA sont définis comme suit (Garvey et Pinto, 2009) :

Performance opérationnelle : Mesure utilisée pour indiquer la réalisation du résultat d'un nœud.

Opérabilité : État dans lequel un nœud fonctionne à un certain niveau de performance.

Niveau d'opérabilité : Niveau de performance atteint par un nœud ou l'utilité qu'il produit.

Niveau d'opérabilité de base (NOB) : Niveau d'opérabilité du nœud récepteur lorsque le nœud d'alimentation est complètement inutilisable.

Nœud d'alimentation : Nœud qui contribue à l'opérabilité d'un ou de plusieurs autres nœuds (les nœuds récepteurs).

Nœud récepteur : Nœud qui reçoit une contribution d'un ou de plusieurs autres nœuds (les nœuds d'alimentation) pour atteindre un certain niveau d'opérabilité.

Solidité de la dépendance (SD) : Mesure dans laquelle le niveau d'opérabilité d'un nœud récepteur dépend du niveau d'opérabilité des nœuds d'alimentation. La SD saisit les effets des relations qui augmentent le rendement comme ajout au NOB.

Criticité de la dépendance (CD) : Caractère essentiel des contributions d'un nœud d'alimentation à un nœud récepteur pour qu'il atteigne ses objectifs de niveau d'opérabilité. La CD détermine la façon dont le rendement du nœud récepteur diminuera en deçà du NOB au fil du temps et pourrait devenir inutilisable.

L'équation algébrique générale de la FDNA pour le graphe de la figure 15 est :

$$P_j = f\left(P_i, \alpha_{ij}, \beta_{ij}\right), 0 \le P_i, P_j \le 100\ , 0 < \alpha_{ij} \le 1\ , 0 \le \beta_{ij} \le 100\ (1 - \alpha_{ij})$$

où P_j est le niveau d'opérabilité du nœud récepteur,

P_i est le niveau d'opérabilité du nœud d'alimentation,

α_{ij} est la contrainte de SD et ($0 < \alpha_{ij} \le 1$), et

β_{ij} est la contrainte de CD et ($0 \le \beta_{ij} \le 100\ (1 - \alpha_{ij}) \le 100$).

Selon la définition originale de Garvey (2009), l'équation fondamentale de la FDNA pour le niveau d'opérabilité du nœud P_y qui dépend des niveaux d'opérabilité de h autres nœuds $P_1, P_2, P_3, \ldots, P_h$ est donnée par

$$0 \le P_y = Min\left(SODP_j, CODP_j\right) \le 100$$

$$SODP_j = Average\left(SODP_{j1}, SODP_{j2}, SODP_{j3}, \ldots, SODP_h\right)$$

$$SODP_{ji} = \alpha_{ij}P_i + 100\left(1 - \alpha_{ij}\right), 0 \le P_i, P_j \le 100, 0 < \alpha_{ij} \le 1, i = 1,2,3, \ldots, h$$

$$CODP_j = Min\left(CODP_{j1}, CODP_{j2}, CODP_{j3}, \ldots CODP_{jh}\right)$$

$$CODP_{ji} = P_i + \beta_{ij}, 0 \le \beta_{ij} \le 100\ (1 - \alpha_{ij})$$

où SODP$_j$ est l'équation SD de P_j sur les nœuds d'alimentation $P_1, P_2, P_3, \ldots, P_h$,

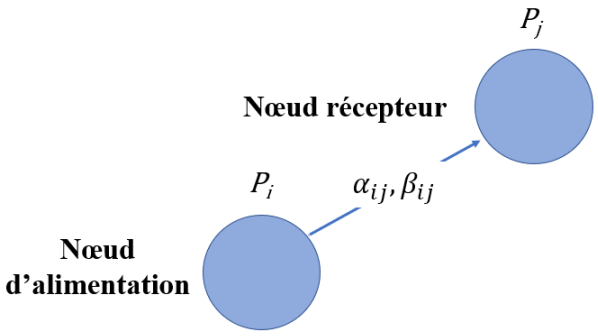
CODP$_j$ est l'équation CD de P_j sur les nœuds d'alimentation $P_1, P_2, P_3, \ldots, P_h$,

α_{ij}: représente la fraction de SD P_j sur les nœuds d'alimentation P_i, et

β_{ij} est le niveau d'opérabilité auquel un nœud récepteur diminue sans sa contribution au nœud d'alimentation.

Figure 10

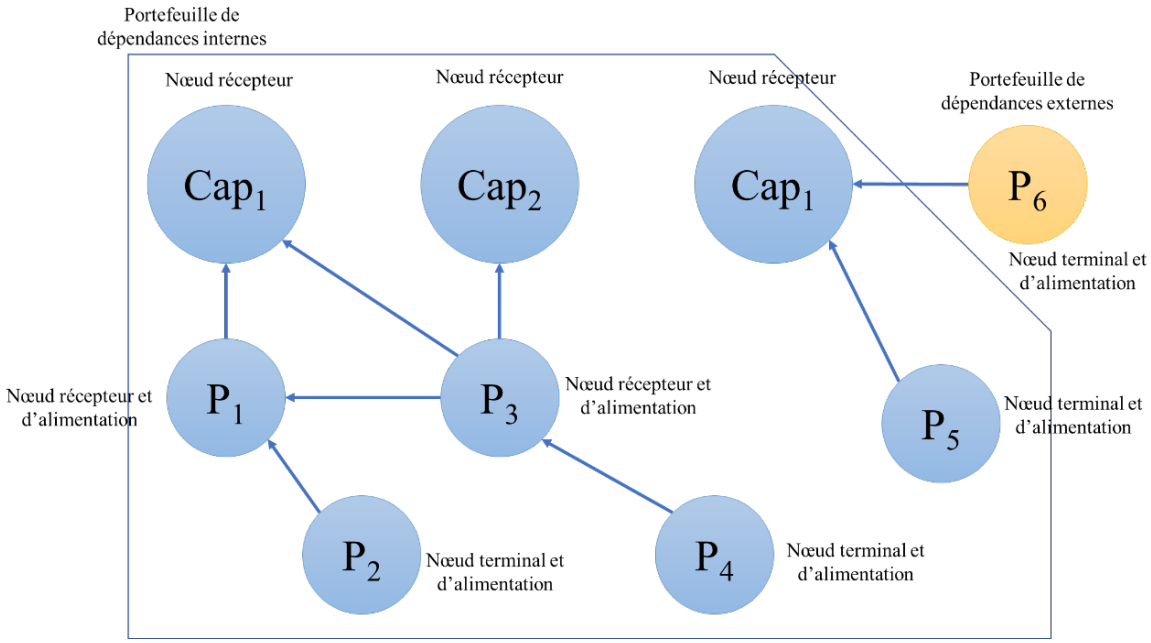
GRAPHE FDNA À DEUX NŒUDS



La FDNA joue un rôle très important dans la modélisation des effets d'entraînement de toute perte d'opérabilité dans le(s) nœud(s) d'alimentation, en analysant non seulement l'opérabilité, mais aussi la continuité des activités d'une entreprise. Comme le montre la figure 16, le portefeuille de capacité d'une entreprise, y compris le(s) nœud(s) de dépendance interne(s) et externe(s) du portefeuille, et les capacités peuvent être représentés par la FDNA pour calculer la perte de capacité de l'entreprise en cas de perte de fonctionnalité dans n'importe quel nœud.

Figure 11

REPRÉSENTATION DU CONTEXTE D'UN PORTEFEUILLE DE CAPACITÉS DANS LE GRAPHE FDNA



Source : Adapté de Garvey et Pinto (2009).

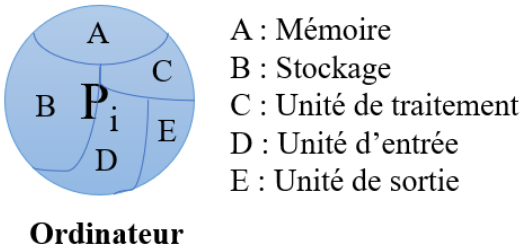
6.3 Nœuds de FDNA à plusieurs composantes

La FDNA est une méthode de la théorie des graphes utile pour répondre aux questions suivantes (Garvey, 2009) :

> Dans quelle mesure les capacités dépendent-elles des risques, de sorte que les menaces qui leur sont faites peuvent être découvertes avant que les programmes contributeurs (p. ex., les fournisseurs) ne se dégradent, échouent ou soient éliminés?
>
> Quel est l'effet de la capacité sur l'opérabilité si, en raison de la concrétisation des risques, un ou plusieurs programmes contributeurs ou chaînes de fournisseurs se dégradent, échouent ou sont éliminés?

La FDNA est également un outil pratique lorsqu'un nœud est constitué de plusieurs composantes. Garvey et Pinto (2009) décrivent un *nœud à composante unique* comme « un nœud défini par une seule composante ». Un nœud à plusieurs composantes, appelé *nœud constitutif*, est « un nœud caractérisé par deux composantes ou plus ». Il est toujours possible de scinder un nœud constitutif en au moins deux composantes distinctes. Par exemple, un ordinateur, composé d'une mémoire, d'une capacité de stockage, d'une unité de traitement, d'une unité d'entrée et d'une unité de sortie, pour un total de cinq composantes, est un exemple de nœud constitutif. La représentation graphique de cet exemple de nœud constitutif est fournie à la figure 17.

Figure 12
REPRÉSENTATION D'UN NŒUD CONSTITUTIF



Source : Tatar (2019).

6.3.1. Théorie qui sous-tend les nœuds constitutifs

Pour comprendre la théorie qui sous-tend l'opérabilité d'un nœud constitutif, il est essentiel de bien saisir les concepts de fonction de valeur, de fonction de valeur unidimensionnelle et de fonction de valeur additive.

Une fonction de valeur est [traduction libre] « une fonction mathématique de valeur réelle définie à partir d'un critère d'évaluation qui représente la mesure de la « qualité » d'une option sur les niveaux du critère » (Garvey, 2009). La *qualité* peut également être désignée sous le nom d'utilité, ou « util. », de rendement, etc., dans différents contextes. La fonction de valeur a habituellement une fourchette de qualité de zéro à un ou 100, où zéro représente le niveau le moins privilégié.

La *fonction de valeur unidimensionnelle* (FVU) est une fonction de valeur définie à partir d'un critère. Un exemple de critère est la couleur d'une voiture (le critère est désigné par X) qui peut avoir des valeurs comme bleu, rouge, noir, jaune (la valeur est désignée par x). On peut supposer que le fait de posséder une voiture bleue, rouge, noire et jaune a une valeur de qualité (la valeur de qualité est désignée par $V_X(x)$) de 0, 1/4, 2/3, et 1, respectivement.

$$V_{CAR\ COLOR}(blue) = 0$$

Le critère d'une fonction de valeur ne doit pas être nécessairement une variable catégorique (discrète). Il peut aussi s'agir d'une variable continue comme le prix en dollars. En outre, une fonction de valeur peut suivre une courbe exponentielle avec des préférences en hausse ou en baisse. Par exemple, une fonction de valeur exponentielle pour le prix d'une voiture peut suivre une préférence décroissante, où des montants moindres sont préférables. Un exemple d'augmentation monotone de la fonction de valeur peut être la consommation d'essence aux 100 kilomètres, où moins de litres d'essence aux 100 kilomètres est préférable (Garvey 2009).

La *fonction de valeur additive* combine plusieurs FVU (c.-à-d. plusieurs critères). L'équation qui suit est un exemple de fonction additive avec *n* critères où w représente la pondération de chaque critère :

$$V_Y(y) = w_1V_{X_1}(x_1) + w_2V_{X_2}(x_2) + w_3V_{X_3}(x_3) + \cdots + w_nV_{X_n}(x_n)$$

La somme des facteurs de pondération des critères est égale à 1.

$$\sum_{i=1}^{n} w_i = 1$$

Si nous considérons la couleur, le prix et la consommation de la voiture comme des critères de la fonction additive des FVU dans notre exemple, la fonction est désignée comme suit :

$$V_Y(y) = w_1V_{COULEUR}(couleur) + w_2V_{PRIX}(prix) + w_3V_{CONSOMMATION}(consommation),$$

où

$$w_1 + w_2 + w_3 = 1.$$

6.3.2. Détermination des facteurs de pondération

Les facteurs de pondération des différentes valeurs rattachées aux critères d'une fonction de valeur additive peuvent être calculés en utilisant des données historiques ou en faisant appel au jugement d'experts. Pour notre exemple de la voiture, supposons que le prix est deux fois plus important que le nombre de litres aux 100 kilomètres et que le nombre de litres aux 100 kilomètres est deux fois plus important que la couleur du véhicule. Dans ce cas, la relation peut être exprimée comme suit :

$$4 * w_1 = w_2 = 2 * w_3$$

Puisque la somme des facteurs de pondération est égale à 1,

$$w_1 + 4 * w_1 + 2 * w_1 = 1$$

$$w_1 = \frac{1}{7}, w_2 = \frac{4}{7}, w_3 = \frac{2}{7}$$

La fonction de valeur peut être reformulée comme suit :

$$V_Y(y) = \frac{1}{7} * V_{COULEUR}(couleur) + \frac{4}{7} * V_{PRIX}(prix) + \frac{2}{7} * V_{CONSOMMATION}(consommation)$$

Pour le modèle de la cyberFDNA, chaque nœud est un nœud constitutif à trois composantes. Par conséquent, la fonction de valeur additive comporte trois critères – la confidentialité, l'intégrité et la disponibilité – et chacun représente un FVU. Des détails sont fournis à la section 6.4.2.

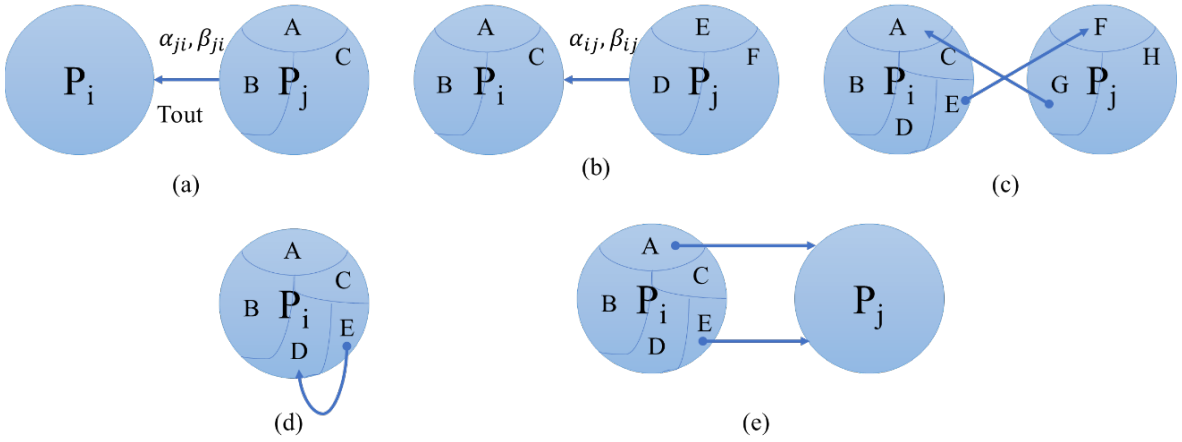
6.3.3. Types de relations de dépendance entre les nœuds constitutifs

Un nœud constitutif peut être un nœud d'alimentation ou un nœud récepteur. Comme le montre la figure 18, un tel nœud ou ses composantes peuvent avoir plusieurs relations de dépendance possibles : a) dépendance d'un nœud constitutif à un nœud unique; b) dépendance d'un nœud constitutif à un autre nœud constitutif; c) dépendance d'une composante d'un nœud constitutif à autre composante dans un autre nœud constitutif; d) dépendance d'une composante d'un nœud constitutif à une composante dans le même nœud constitutif; et e) dépendance d'une composante d'un nœud constitutif à nœud unique dans son ensemble.

Le niveau d'opérabilité d'un nœud constitutif est différent de celui d'un nœud unique, celui-ci pouvant être représenté par un FVU. Le niveau d'opérabilité d'un nœud constitutif est une fonction des niveaux d'opérabilité de ses composantes. Comme pour le nœud unique, le niveau d'opérabilité de chaque composante d'un nœud constitutif est représenté par son FVU. Une forme classique de la fonction de valeur additive de Keeney-Raiffa est utilisée pour calculer l'opérabilité globale d'un nœud constitutif (Keeney et Raiffa, 1976). Cela signifie que [traduction libre] « la fonction d'opérabilité globale du nœud constitutif est une somme additive linéaire de chaque FVU » (Garvey, 2009).

Figure 13

RELATIONS DE DÉPENDANCE ENTRE LES NŒUDS CONSTITUTIFS ET LES NŒUDS UNIQUES



(a) Nœud unique : Dépendance au nœud constitutif
(b) Nœud constitutif : Dépendance au nœud constitutif
(c) Composante d'un nœud constitutif : Dépendance à la composante d'un autre nœud constitutif
(d) Composante d'un nœud constitutif : Dépendance à une autre composante du nœud constitutif
(e) Composante d'un nœud constitutif : Dépendance au nœud unique

Source : Tatar (2019).

Par exemple, (c) dans la figure 18, les fonctions d'opérabilité des éléments A, B, C, D et E sont représentées par des FVU $V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D)$, and $V_E(x_E)$. L'opérabilité de la fonction P_i est la suivante :

$$P_i = w_A V_A(x_A) + w_B V_B(x_B) + w_C V_C(x_C) + w_D V_D(x_D) + w_E V_E(x_E),$$

où

$$w_A + w_b + w_C + w_D + w_E = 1 \; and \; 0 \leq P_i, V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), V_E(x_E) \leq 100.$$

Une représentation générale de la fonction d'opérabilité d'un nœud constitutif P_y comportant k composantes est

$$P_y = \sum_{i=1}^{k} w_i V_{A_i}(x_i),$$

où

$$w_1 + w_2 + w_3 + \cdots + w_k = 1 \; et \; 0 \leq P_i, V_{A_i}(x_i), \leq 100.$$

6.4 Modification de la FDNA pour passer à la cyberFDNA

Nous vous présentons la cyberFDNA, une nouvelle méthode fondée sur la FDNA afin de répondre aux limites de la méthode antérieure dans l'analyse des cyberrisques. La présente section explique la justification des modifications et de la nouvelle algèbre de la cyberFDNA. Trois modifications importantes sont apportées à la FDNA traditionnelle : (1) l'introduction de l'autoefficacité des nœuds; (2) l'intégration des valeurs CID aux nœuds; et (3) de nouvelles relations de dépendance (dépendances ET et OU).

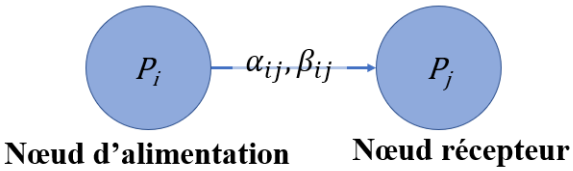
6.4.1 Autoefficacité des nœuds

La FDNA joue un rôle déterminant dans la modélisation des effets d'entraînement entre les nœuds dépendants sur le plan fonctionnel. Elle suppose que la perte d'opérabilité d'un nœud n'est possible que si le niveau d'opérabilité d'au moins un de ses nœuds d'alimentation se détériore. Bien que cette condition soit présente dans le cyberespace, il existe d'autres possibilités qui peuvent causer la dégradation de l'opérabilité d'un nœud récepteur

alors que tous ses nœuds d'alimentation sont entièrement opérationnels. Par exemple, dans le cas d'une relation de dépendance entre un routeur et un ordinateur personnel, l'ordinateur personnel pourrait tomber en panne en raison d'une erreur de système ou d'une cyberattaque, même si le routeur est entièrement opérationnel. Le niveau d'opérabilité de l'ordinateur peut se dégrader en raison de la panne. Par conséquent, un nouveau paramètre doit être ajouté à l'algèbre de la FDNA pour couvrir ce genre de situation.

Un nouveau paramètre, l'*autoefficacité,* a été élaboré pour améliorer la FDNA afin de couvrir les situations où l'opérabilité du nœud récepteur se dégrade pendant que tous les nœuds d'alimentation sont entièrement opérationnels. L'autoefficacité d'un nœud est un multiplicateur de son niveau d'opérabilité fondé sur les dépendances de la SD et de la CD avec ses nœuds d'alimentation. Les nouvelles équations de la FDNA pour un graphe à deux nœuds (figure 19) suivent. Cette formule d'autoefficacité est différente de la formule *d'autoefficacité* élaborée par Guariniello et DeLaurentis (2014).

Figure 14
GRAPHE DE LA FDNA À DEUX NŒUDS



$$P_j = SE_j * \Big(Min\big(SODP_j, CODP_j\big)\Big) = SE_j * \Big(Min\big(\alpha_{ij}P_i + 100\big(1-\alpha_{ij}\big), P_I + \beta_{ij}\big)\Big),$$

où SE_j est l'autoefficacité de P_j et de $0 \leq SE \leq 1$;

α_{ij} est la solidité de la fraction de dépendance entre $P_i$et P_j et $0 \leq \alpha_{ij} \leq 1$; et

β_{ij} est la criticité de la dépendance entre Pi et Pj et $0 \leq \beta_{ij} \leq 100(1-\alpha_{ij})$

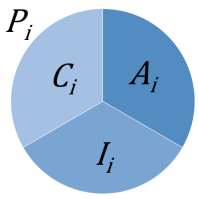
$$0 \leq P_i, P_j \leq 100.$$

6.4.2 Intégration de la confidentialité, de l'intégrité et de la disponibilité

Comme bien d'autres, les normes du NIST exigent une évaluation de l'actif en fonction des valeurs CID. Cette évaluation tridimensionnelle permet de différencier chaque type d'attaque et son impact respectif. Dans le modèle de cyberFDNA, la valeur et l'impact des dépendances sont définis comme un vecteur des valeurs CID.

Chaque nœud (c.-à-d. un actif, un service ou un processus opérationnel) du graphe de cyberFDNA possède ses propres valeurs CID. La représentation constitutionnelle des nœuds de la FDNA est déterminante dans la définition des nœuds (illustrée à la figure 20).

Figure 15
UN NŒUD DE LA CYBERFDNA



À l'instar de la forme classique de la fonction de valeur additive de Keeney-Raiffa, qui est utilisée pour calculer l'opérabilité globale d'un nœud constitutif (Keeney et Raiffa, 1976), le niveau d'opérabilité d'un nœud de cyberFDNA est fonction des niveaux d'opérabilité de ses composantes – les valeurs CID. Cela signifie que la fonction d'opérabilité globale d'un nœud de cyberFDNA est une somme additive linéaire des fonctions de valeur unidimensionnelle de confidentialité, d'intégrité et de disponibilité.

Pour l'exemple de la figure 20, les fonctions d'opérabilité de C_i, I_i et D_i sont représentées par des FVU $V_{C_i}(x_{C_i}), V_{I_i}(x_{I_i}),$ and $V_{A_i}(x_{A_i})$. La fonction d'opérabilité P_i est la suivante :

$$P_i = w_{Ci}V_{Ci} + w_{Ii}V_{Ii} + w_{Ai}V_{Ai}, \qquad \text{Équation 3}$$

où

$$w_{Ci} + w_{Ii} + w_{Ai} = 1$$

$$V_{Ci} = V_{Ci}(X_{Ci}), V_{Ii} = V_{Ii}(X_{Ii}), V_{Ai} = V_{Ai}(X_{Ai})$$

$$0 \leq V_{Ci}, V_{Ii}, V_{Ai} \leq 100.$$

Tout en déterminant les facteurs de pondération relatifs aux fonctions des valeurs CID, les métriques des exigences de confidentialité, d'intégrité et de disponibilité du groupe de métriques environnementales du CVSS peuvent être prises en compte puisqu'elles se chevauchent sur le plan conceptuel.

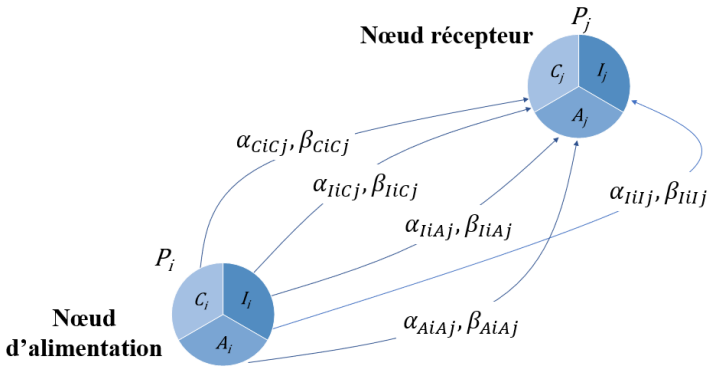
Cet exemple constitue un nœud d'un graphe d'impact tiré de cette étude. La plupart du temps, les trois volets de la triade CID sont essentiels à la sécurité des composantes et des systèmes des TIC. Toutefois, l'un d'eux peut parfois être plus essentiel ou négligeable que les autres, selon les attentes des utilisateurs. Des facteurs de pondération sont attribués en fonction de l'importance particulière des valeurs CID pour chaque nœud. Par exemple, pour un hôte de serveur Web accessible au public, même si l'importance de la disponibilité et de l'intégrité est élevée, la confidentialité n'est pas un aspect important. Par ailleurs, pour un système de point de vente par carte de crédit ou une base de données renfermant des renseignements personnels sur la santé, la confidentialité et l'intégrité sont beaucoup plus importantes que la disponibilité. Les facteurs de pondération doivent être attribués en conséquence. Ces concepts s'appliquent également aux nœuds des couches des services et des processus opérationnels. Les services bancaires en ligne doivent être relativement plus robustes du point de vue de l'intégrité. Pour une entreprise de magasinage en ligne, la disponibilité de son site Web de commerce électronique, qui constitue le principal processus opérationnel, est cruciale.

L'opérabilité d'un nœud de la cyberFDNA est une somme pondérée des valeurs d'opérabilité que sont la confidentialité, l'intégrité et la disponibilité. Dans la FDNA, chaque nœud représente une fonction. Dans la cyberFDNA, chaque nœud représente une fonction comme un actif, un service ou un processus opérationnel. La confidentialité, l'intégrité et la disponibilité d'un nœud ne sont pas des aspects de sécurité entièrement indépendants; toutefois, chacun possède un concept distinct. Il est possible qu'une attaque n'affecte qu'un de ces aspects, ou une combinaison de ceux-ci, en partie ou en totalité. Un attaquant peut n'avoir accès qu'à la lecture des données d'un actif sans pouvoir les modifier ou les désactiver. Par ailleurs, un attaquant peut interrompre le fonctionnement d'un service, mais les données contrôlées par le service pourraient être protégées contre les aspects de confidentialité et d'intégrité. Un autre exemple pourrait être une attaque par rançongiciel qui chiffre toutes les données de l'actif et exécute également un script malveillant qui modifie toutes les configurations du logiciel appliquées à l'actif. Dans ce cas, sa confidentialité ne serait pas affectée, mais les valeurs d'opérabilité des dimensions intégrité et disponibilité diminueraient sensiblement, peut-être même jusqu'à zéro.

Pour définir l'algèbre de la cyberFDNA, plusieurs équations de dépendance de la cyberFDNA ont été élaborées à partir d'exemples.

Exemple : Formuler les équations FDNA pour le graphe de la figure 21.

Figure 16
GRAPHE DE CYBERFDNA À DEUX NŒUDS



Le graphe de cyberFDNA à la figure 21 se compose de deux nœuds, P_i *et* P_j. Les équations pour le niveau d'opérabilité de chaque nœud —P_i et P_j– sans tenir compte des dépendances sont les suivantes :

$$P_i = w_{Ci}V_{Ci} + w_{Ii}V_{Ii} + w_{Ai}V_{Ai}$$

$$P_j = w_{Cj}V_{Cj} + w_{Ij}V_{Ij} + w_{Aj}V_{Aj}$$

$$w_{Ci} + w_{Ii} + w_{Ai} = 1$$

$$w_{Cj} + w_{Ij} + w_{Aj} = 1$$

$$V_{Ci} = V_{Ci}(X_{Ci}), V_{Ii} = V_{Ii}(X_{Ii}), V_{Ai} = V_{Ai}(X_{Ai}), V_{Cj} = V_{Cj}(X_{Cj}), V_{Ij} = V_{Ij}(X_{Ij}), V_{Aj} = V_{Aj}(X_{Aj})$$

$$0 \le V_{Ci}, V_{Ii}, V_{Ai}, V_{Cj}, V_{Ij}, V_{Aj} \le 100$$

$$0 \le P_i, P_j \le 100\,,$$

$$For\ \forall\ X, Y\ \in \{C, I, A\}, 0 < \alpha_{XiYj} \le 1\,, 0 \le \beta_{XiYj} \le 100\ (1 - \alpha_{XiYj})$$

Commençons par un scénario de base. Nous supposerons qu'il n'y a qu'un seul point de dépendance. Si cette dépendance est de C_i à C_j, , l'équation de la cyberFDNA est la suivante :

$$V_{Cj} = SE_{Cj} * \left(Min\left(SODV_{CjCi}, CODV_{CjCi}\right)\right) = SE_{Cj} * \left(Min\left(\alpha_{CiCj}V_{Ci} + 100\left(1 - \alpha_{CiCj}\right), V_{Ci} + \beta_{CiCj}\right)\right),$$

où SE_{Cj} est l'autoefficacité de la composante de confidentialité de P_j et $0 \le SE_{Cj} \le 1$;

α_{CiCj} est la solidité de la fraction de dépendance entre V_{Ci} et V_{Cj} et $0 \le \alpha_{CiCj} \le 1$; and

β_{CiCj} est la criticité de la dépendance entre V_{Ci} et V_{Cj} et $0 \le \beta_{CiCj} \le 100(1 - \alpha_{CiCj})$

$$0 \le V_{Ci}, V_{Cj} \le 100.$$

Si cette dépendance est de I_i à I_j, l'équation de cyberFDNA est la suivante :

$$V_{Ij} = SE_{Ij} * \left(Min\left(SODV_{IjIi}, CODV_{IjIi}\right)\right) = SE_{Ij} * \left(Min\left(\alpha_{IiIj}V_{Ii} + 100\left(1 - \alpha_{IiIj}\right), V_{Ii} + \beta_{IiIj}\right)\right),$$

où SE_{Ij} est l'autoefficacité de la composante d'intégrité de P_j et $0 \le SE_{Ij} \le 1$;

α_{IiIj} est la solidité de la fraction de dépendance entre V_{Ii} et V_{Ij} et $0 \le \alpha_{IiIj} \le 1$; and

β_{IiIj} est la criticité de la dépendance entre V_{Ii} et V_{Ij} et $0 \le \beta_{IiIj} \le 100(1 - \alpha_{IiIj})$

$$0 \le V_{Ii}, V_{Ij} \le 100.$$

Si cette dépendance est de A_i à A_j, , l'équation de cyberFDNA est la suivante :

$$V_{Aj} = SE_{Aj} * \left(Min\left(SODV_{AjAi}, CODV_{AjAi}\right)\right) = SE_{Aj} * \left(Min\left(\alpha_{AiAj}V_{Ai} + 100\left(1-\alpha_{AiAj}\right), V_{Ai} + \beta_{AiAj}\right)\right),$$

où SE_{Aj} est l'autoefficacité de la composante de disponibilité de P_j et $0 \le SE_{Aj} \le 1$;

α_{AiAj} est la solidité de la fraction de dépendance entre V_{Ai} et V_{Aj} et $0 \le \alpha_{AiAj} \le 1$;

β_{AiAj} est la criticité de la dépendance entre V_{Ai} et V_{Aj} et $0 \le \beta_{AiAj} \le 100(1-\alpha_{AiAj})$

$$0 \le V_{Ai}, V_{Aj} \le 100.$$

Lorsque nous examinons les cinq points de dépendance dans la figure 21 (c.-à-d. les dépendances de C_i à C_j, de I_i à I_j, de I_i à C_j, de I_i à A_j et de A_i à A_j), la fonction de dépendance de la cyberFDNA pour ce graphe est donnée par les équations suivantes :

$$V_{Cj} = SE_{Cj} * \left(Min\left(Ave\left(SODV_{CjCi}, SODV_{CjIi}\right), CODV_{CjCi}, CODV_{CjIi}\right)\right)$$

$$V_{Cj} = SE_{Cj} * \left(Min\left(\frac{\alpha_{CiCj}V_{Ci}}{2} + \frac{\alpha_{IiCj}V_{Ii}}{2} + 100\left(1 - \frac{\alpha_{CiCj} + \alpha_{IiCj}}{2}\right), V_{Ci} + \beta_{CiCj}, V_{Ii} + \beta_{IiCj}\right)\right)$$

$$V_{Ij} = SE_{Ij} * \left(Min\left(SODV_{IjIi}, CODV_{IjIi}\right) = SE_{Ij} * Min\left(\alpha_{IiIj}V_{Ii} + 100\left(1-\alpha_{IiIj}\right), V_{Ii} + \beta_{IiIj}\right)\right)$$

$$V_{Aj} = SE_{Aj} * \left(Min\left(Ave\left(SODV_{AjAi}, SODV_{AjIi}\right), CODV_{AjAi}, CODV_{AjIi}\right)\right)$$

$$V_{Aj} = SE_{Aj} * \left(Min\left(\frac{\alpha_{AiAj}V_{Ai}}{2} + \frac{\alpha_{IiAj}V_{Ii}}{2} + 100\left(1 - \frac{\alpha_{AiAj} + \alpha_{IiAj}}{2}\right), V_{Ai} + \beta_{AiAj}, V_{Ii} + \beta_{IiAj}\right)\right)$$

où SE_{Cj} est l'autoefficacité de la composante de confidentialité de P_j et $0 \le SE_{Cj} \le 1$;

α_{CiCj} est la solidité de la fraction de dépendance entre V_{Ci} et V_{Cj} et $0 \le \alpha_{CiCj} \le 1$;

β_{CiCj} est la criticité de la dépendance entre V_{Ci} et $V_{CAnnée}$ et $0 \le \beta_{CiCj} \le 100(1-\alpha_{CiCj})$

$$0 \le V_{Ci}, V_{Cj} \le 100;$$

SE_{Ij} est l'autoefficacité de la composante d'intégrité de P_j et $0 \le SE_{Ij} \le 1$;

α_{IiIj} est la solidité de la fraction de dépendance entre V_{Ii} et V_{Ij} et $0 \le \alpha_{IiIj} \le 1$;

β_{IiIj} est la criticité de la dépendance entre V_{Ii} et V_{Ij} et $0 \le \beta_{IiIj} \le 100(1-\alpha_{IiIj})$

$$0 \le V_{Ii}, V_{Ij} \le 100;$$

SE_{Aj} est l'autoefficacité de la composante de disponibilité de P_j et $0 \le SE_{Aj} \le 1$;

α_{AiAj} est la solidité de la fraction de dépendance entre V_{Ai} et V_{Aj} et $0 \le \alpha_{AiAj} \le 1$;

β_{AiAj} est la criticité de la dépendance entre V_{Ai} et V_{Aj} et $0 \le \beta_{AiAj} \le 100\left(1-\alpha_{AiAj}\right)$;

α_{IiAj} est la solidité de la fraction de dépendance entre V_{Ii} et V_{Aj} et $0 \le \alpha_{IiAj} \le 1$; and

β_{IiAj} est la criticité de la dépendance entre V_{Ii} et V_{Aj} et $0 \le \beta_{IiAj} \le 100(1-\alpha_{IiAj})$

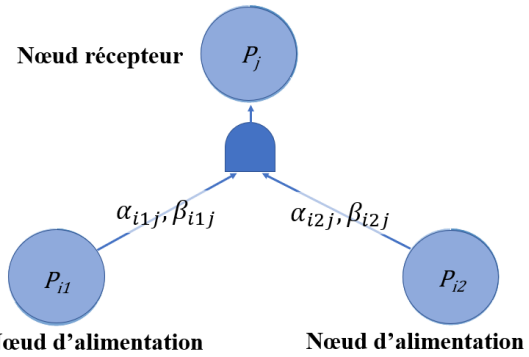
$$0 \le V_{Ai}, V_{Aj} \le 100.$$

6.4.3 Intégration de portes ET

Dans le cyberespace, les relations de dépendance de la FDNA classique ne sont pas suffisantes pour modéliser les types de dépendances de certains nœuds de la cyberFDNA (c.-à-d. actifs, services ou processus opérationnels). Par exemple, s'il y a deux bases de données dans un système et qu'un serveur d'applications doit les interroger simultanément (p. ex., en demandant le numéro de sécurité sociale de l'utilisateur dans une base de données et la

date de naissance dans une autre) pour répondre à une demande provenant d'un serveur Web (c.-à-d., le numéro de sécurité sociale et la date de naissance de l'utilisateur), les dépendances du serveur d'applications aux serveurs de base de données ne peuvent pas être modélisées par une dépendance de nœud à deux alimenteurs et un récepteur de l'algèbre de la FDNA classique. Un nouveau concept – portes ET – a été élaboré pour élargir l'algèbre de la FDNA classique pour couvrir de telles situations, comme le montre la figure 22.

Figure 17
DÉPENDANCE ET D'UN GRAPHE FDNA À TROIS NŒUDS



Ce graphe comprend trois nœuds : P_i, P_{i2} et P_j. Les équations du niveau d'opérabilité du nœud récepteur (P_j) sont les suivantes :

$$P_j = SE_j * \left(Min\left(Min\left(SODP_{ji1}, CODP_{ji1}\right), Min\left(SODP_{ji2}, CODP_{ji2}\right)\right)\right)$$

$$\Rightarrow \quad P_j = SE_j * \left(Min\left(SODP_{ji1}, SODP_{ji2}, CODP_{ji1}, CODP_{ji2}\right)\right)$$

$$\Rightarrow \quad P_j = SE_j * \left(Min\left(\alpha_{P_{i1j}} P_{i1} + 100\left(1 - \alpha_{P_{i1j}}\right), \alpha_{P_{i2j}} P_{i2} + 100\left(1 - \alpha_{P_{i2j}}\right), P_{i1} + \beta_{P_{i1j}}, P_{i2} + \beta_{P_{i2j}}\right)\right)$$

où SEj est l'autoefficacité de Pj et $0 \leq SE_j \leq 1$;

α_{Pi1j} est la solidité de la fraction de dépendance entre P_{i1} et P_j et $0 \leq \alpha_{Pi1j} \leq 1$;

β_{Pi1j} est la criticité de la dépendance entre P_{i1}et P_j et $0 \leq \beta_{Pi1j} \leq 100(1 - \alpha_{Pi1j})$;

α_{Pi2j} est la solidité de la fraction de dépendance entre P_{i2}et P_j et $0 \leq \alpha_{Pi2j} \leq 1$; and

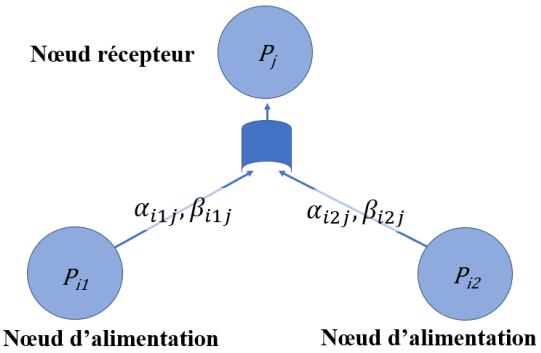
β_{Pi2j} est la criticité de la dépendance entre P_{i2}et $P_j$et $0 \leq \beta_{Pi2j} \leq 100(1 - \alpha_{Pi2j})$.

6.4.4 Intégration de portes OU

Pour accroître la résilience d'un cybersystème essentiel, l'ajout de composantes redondantes au système est une pratique établie. Un serveur redondant est une reproduction du serveur principal ayant la même puissance informatique, la même capacité de stockage et les mêmes applications (ou parfois semblables). Un serveur redondant est inactif jusqu'à ce que le serveur principal tombe en panne. Une fois que le serveur principal cesse de fonctionner, le serveur redondant devient actif et assume les responsabilités du serveur principal pour prévenir la défaillance du système ou les temps d'arrêt.

Les relations de dépendance de la FDNA classique ne sont pas suffisantes pour modéliser les nœuds redondants. Un nouveau concept – portes OU – a été mis au point pour appliquer l'algèbre de la FDNA classique à de telles situations, comme le montre la figure 23.

Figure 18
DÉPENDANCE OU D'UN GRAPHE FDNA À TROIS NŒUDS



Ce graphe se compose de trois nœuds : P_{i1}, P_{i2} et P_j. Les équations du niveau d'opérabilité du nœud récepteur (P_j) sont les suivantes :

$$P_j = SE_j * \left(Max\left(Min\left(SODP_{ji1}, CODP_{ji1}\right), Min\left(SODP_{ji2}, CODP_{ji2}\right)\right)\right)$$

$$\Rightarrow \quad P_j = SE_j * \left(Max\left(Min\left(\alpha_{P_{i1j}} P_{i1} + 100\left(1 - \alpha_{P_{i1j}}\right), P_{i1} + \beta_{P_{i1j}}\right), Min\left(\alpha_{P_{i2j}} P_{i2} + 100\left(1 - \alpha_{P_{i2j}}\right), P_{i2} + \beta_{P_{i2j}}\right)\right)\right)$$

où SE_j est l'autoefficacité de P_j et $0 \leq SE_j \leq 1$;

α_{Pi1j} est la solidité de la fraction de dépendance entre P_{i1}et P_j et $0 \leq \alpha_{Pi1j} \leq 1$;
β_{Pi1j} est la criticité de la dépendance entre P_{i1}et P_j et $0 \leq \beta_{Pi1j} \leq 100(1 - \alpha_{Pi1j})$;
α_{Pi2j} est la solidité de la fraction de dépendance entre P_{i2}et P_j et $0 \leq \alpha_{Pi2j} \leq 1$; and
β_{Pi2j} est la criticité de la dépendance entre P_{i2} et $P_j$et $0 \leq \beta_{Pi2j} \leq 100(1 - \alpha_{Pi2j})$.

6.5 Métriques d'impact

Outre les résultats de la fonction d'intégration, le graphe d'impact a besoin de certaines informations provenant des métriques de base suivantes du CVSS liées à l'impact :

- Impact sur la confidentialité
- Impact sur l'intégrité
- Impact sur la disponibilité

Dans le système CVSS, les métriques de confidentialité et d'intégrité font référence aux impacts qui influent sur les données utilisées par le service. Cependant, la métrique de l'impact sur la disponibilité renvoie au fonctionnement du service lui-même. Par exemple, le vol de numéros de carte de crédit constitue une atteinte à la confidentialité, et le contenu de la page Web qui a été modifié de façon malveillante constitue un problème d'intégrité. Ces deux cas concernent les données. Par ailleurs, la mesure de la disponibilité porte sur le rendement et le fonctionnement du service lui-même, et non sur la disponibilité des données. Même si les données utilisées par un service sont modifiées, cela n'influe pas directement sur la disponibilité du service. Par exemple, une vulnérabilité dans un service Internet comme le courriel pourrait permettre à un attaquant de supprimer tous les courriels antérieurs dans une boîte de réception. Le seul impact est lié à l'intégrité, et non à la disponibilité, car le service de courriel fonctionne toujours – il ne fait que servir en l'absence des données historiques importantes (FIRST.Org Inc., 2019b). En raison de ces différences, dans la présente étude, chaque composante des TIC est un nœud constitutif des composantes de la CID, chacune ayant une pondération en fonction de son importance.

Les valeurs des métriques du tableau 5 ont été déterminées par le CVSS. Les métriques de confidentialité, d'intégrité et de disponibilité du groupe des métriques de base du CVSS et les métriques de base modifiées du groupe de métriques environnementales peuvent se voir attribuer trois valeurs : élevée, faible et aucune.

- Métriques de confidentialité
    - Une valeur élevée est attribuée à la métrique de confidentialité d'une vulnérabilité si elle devait entraîner la perte totale de confidentialité et si tout le contenu de l'actif devenait accessible aux attaquants s'il était exploité. Elle est également considérée comme ayant un impact élevé si les données ne sont pas toutes divulguées, mais les données volées sont très sensibles et ont un impact important, comme les mots de passe des administrateurs ou les clés de chiffrement d'un serveur.
    - Une faible valeur est attribuée à la métrique de confidentialité si l'exploitation n'expose que certaines données restreintes aux attaquants et si ceux-ci n'ont pas de contrôle sur les données obtenues. L'impact n'est pas grave en l'espèce.
    - Aucune valeur n'est attribuée à la confidentialité s'il n'y a pas de perte de confidentialité lorsque la vulnérabilité est exploitée.
- Métrique d'intégrité
    - Une valeur élevée est attribuée à la métrique d'intégrité si une exploitation entraîne une perte complète de protection de l'intégrité des données. Par conséquent, un attaquant peut modifier et supprimer tout ou partie des fichiers. Cette mesure est également considérée comme ayant un impact élevé si seulement une partie des données perd de son intégrité, mais une modification des données peut avoir un impact grave sur la composante des TIC touchée.
    - Une faible valeur est attribuée à la métrique d'intégrité si les attaquants exercent un contrôle limité sur la modification des données ou si les données à modifier n'ont pas d'impact grave.
    - Aucune valeur n'est attribuée à la métrique d'intégrité s'il n'y a pas de perte d'intégrité lorsque la vulnérabilité est exploitée.
- Métriques de disponibilité
    - Une valeur élevée est attribuée à la métrique de disponibilité si l'exploitation désactive toutes les fonctions de la composante. Le refus de service peut se produire pendant l'attaque ou se poursuivre après celle-ci. Une valeur élevée est attribuée parce que les attaquants ne peuvent perturber qu'une partie de la fonction, mais que la perte a un impact grave.
    - Une faible valeur est attribuée à la métrique de disponibilité si l'attaque perturbe partiellement la fonction de la composante et que celui-ci ne refuse pas complètement le service aux utilisateurs légitimes. Dans l'ensemble, il n'y a aucun impact important sur la disponibilité de la composante.
    - Aucune valeur n'est attribuée à la disponibilité s'il n'y a aucun impact sur la disponibilité de la composante lorsque la vulnérabilité est exploitée.

Les valeurs élevées, faibles et nulles des métriques CID du CVSS ont des cotes numériques désignées, respectivement de 0,56, 0,22 et 0. Ces valeurs sont normalisées pour correspondre à la fourchette de 0 à 1 en utilisant le multiplicateur 1,786 et inversées en soustrayant de 1, comme le montre l'équation suivante. Ces valeurs d'impact normalisées sont utilisées pour calculer la dégradation de l'opérabilité par une diminution de l'autoefficacité dans un nœud constitutif (C, I ou D) d'un actif des TIC lorsque la probabilité inconditionnelle est égale à 1. Pour les valeurs de probabilité moindres, la dégradation est interpolée pour calculer le risque de perte d'opérabilité de la composante individuelle des TIC.

Les valeurs d'opérabilité pour la confidentialité, l'intégrité et la disponibilité des actifs sont calculées en normalisant comme suit les métriques d'impact de la base du CVSS :

$$Dégradation\ normalisée\ du\ niveau\ d'autoefficacité\ des\ impacts\ sur\ CIA = 1 - 1.786 * [C, I, D]$$

Après la normalisation, les valeurs de dégradation de l'autoefficacité pour les valeurs élevé, faible et aucun des composantes CID deviennent respectivement 1, 0,39 et 0, comme le montre le tableau 5. Par exemple, si l'exploitation de la vulnérabilité n'a pas d'impact sur la confidentialité, le niveau d'autoefficacité de la confidentialité du nœud demeure à 1. Si l'impact sur la confidentialité est faible, il diminue de 0,39, passant de 1 à 0,61. Si l'impact est élevé, l'autoefficacité est réduite à zéro. Les valeurs numériques du tableau 5 ont été recueillies selon le même processus que celui utilisé dans le tableau 3.

Tableau 5

VALEURS D'OPÉRABILITÉ POUR LES MÉTRIQUES D'IMPACT

Groupe de métriques	Métrique	Valeur de la métrique	Dégradation normalisée de l'autoefficacité
Métriques de base	Impact sur la confidentialité (C)	Élevé	1
		Faible	0.39
		Aucun	0
	Impact sur l'intégrité (I)	Élevé	1
		Faible	0.39
		Aucun	0
	Impact sur la disponibilité (A)	Élevé	1
		Faible	0.39
		Aucun	0

Source : FIRST.Org Inc. 2019a.

La BDNV fournit les métriques d'impact de base CID. Les métriques d'impact modifiées pour les composantes CID du groupe des métriques environnementales peuvent être utilisées par les décideurs pour modifier les données extraites de la BDNV.

Le risque est calculé en multipliant la vraisemblance et la valeur de l'impact. Les chiffres du tableau 5 représentent l'effet de l'attaque si la vraisemblance est de 1. Le risque d'attaque est déterminé en calculant la valeur de dégradation maximale du tableau 5 par la probabilité inconditionnelle de réalisation de l'attaque. Par la suite, la propagation du risque est calculée à l'intérieur du réseau.

En résumé, l'impact est quantifié par l'autoefficacité d'un nœud valant 1 (100 %) pour un nœud entièrement opérationnel. L'autoefficacité du nœud est décomposée en autoefficacité de la confidentialité, de l'intégrité et de la disponibilité en déterminant leurs poids en fonction de l'équation 3. Après une exploitation réussie, le niveau d'autoefficacité des mesures CID diminue une valeur selon le tableau 5 et sa vraisemblance. Par la suite, le risque se propage vers les processus opérationnels selon la topologie du réseau de dépendance fonctionnelle et l'algèbre de la cyberFDNA.

Section 7 : Lien entre le graphe d'attaque et le graphe d'impact

Nous devons intégrer les graphes d'attaque et d'impact. Ces deux types de graphes fonctionnent sur les mêmes actifs; toutefois, les relations de dépendance dans ces graphes sont différentes : les dépendances du graphe d'attaque représentent la voie à suivre pour exploiter efficacement un système cible, tandis que les dépendances du graphe d'impact représentent les dépendances fonctionnelles entre les actifs. Les résultats du graphe d'attaque alimentent l'analyse du graphe d'impact.

Pour intégrer les deux graphes, nous identifions d'abord chaque chemin d'attaque dans le graphe d'attaque. Un graphe d'attaque bayésien fondé sur le CVSS nous donne (1) la liste des actifs qui pourraient être exploités et les vulnérabilités qui leur sont associées; (2) la probabilité d'exploitation pour chaque vulnérabilité et actif; et (3) l'impact (c.-à-d. la perte de confidentialité, d'intégrité ou de disponibilité) sur l'actif si cette vulnérabilité est exploitée. Ensuite, nous utilisons la probabilité d'exploitation et les données sur l'impact provenant du graphe d'attaque pour chaque actif afin de simuler la propagation du risque au moyen des dépendances fonctionnelles entre les actifs. Plus tard, le risque se propagera dans les couches de service et de processus opérationnels de l'organisation et entre elles.

Voici les extrants sortis d'un graphe d'attaque :

1. Chemins d'attaque possibles pour une composante spécifique du réseau cible ($P_{i,j}$)
2. Nœuds (actifs) sur ces voies d'attaque ($A_{i,j,k}$)
3. Vulnérabilités exploitées sur ces nœuds ($v_{i,j,k}$)
4. Valeurs de vraisemblance d'exploitation de ces vulnérabilités, $l_{i,j,k}$

La fonction d'intégration devrait être considérée comme une fonction dans le contexte de la programmation informatique plutôt que des mathématiques. Il s'agit d'un ensemble d'instructions pour exécuter une tâche particulière, dans ce cas, en intégrant le graphe d'attaque au graphe d'impact en préparant les résultats du graphe d'attaque pour alimenter l'analyse du graphe d'impact. La fonction d'intégration peut être représentée comme suit :

$$IF(AG) = \left(AG_i, P_{i,j}, A_{i,j,k}, v_{i,j,k}, l_{i,j,k}\right),$$

où IF est la fonction d'intégration;

AG est le graphe d'attaque complet du réseau des TIC (résultat);
AG_i est le graphe d'attaque où l'actif i est le nœud cible, i: $1,2,3, \dots, n$ (résultat);
$P_{i,j}$ est la chemin d'attaque j, j: $1,2,3, \dots, n$ (résultat);
$A_{i,j,k}$ est l'actif k, k: $1,2,3, \dots, n$ (résultat);
$v_{i,j,k}$ est la vulnérabilité à exploiter sur l'actif k (résultat); et
$l_{i,j,k}$ est la vraisemblance que la vulnérabilité de l'actif k sera exploitée avec succès (résultat).

Le pseudo-code pour la fonction d'intégration graphe d'impact - graphe d'attaque est le suivant :

```
Pour chaque actif
Dresser la liste des vulnérabilités
      Générer le graphe d'attaque en reliant les actifs par événement
d'exploitation des vulnérabilités
      Pour chaque graphe d'attaque
            Déterminer les chemins d'attaque
            Pour chaque chemin d'attaque
                  Identifier les nœuds du chemin d'attaque
                        Pour chaque nœud
                        Déterminer la vulnérabilité à exploiter
                         Calculer la vraisemblance d'exploitation à partir des
                         métriques du CVSS
                        Calculer la probabilité inconditionnelle
                  Générer des extrants (nœuds, vulnérabilités, vraisemblances)
Extrants fournis (numéro de l'actif cible, numéro du chemin d'attaque, numéro de
l'actifs, identificateur de la vulnérabilité, probabilité d'exploitation)
```

L'intrant de la fonction d'intégration est le graphe d'attaque complet des cibles possibles du réseau des TIC. Le résultat de la fonction d'intégration est une liste de listes; en d'autres termes, il s'agit d'un tableau de données. Les colonnes du tableau de sont les suivantes :

1. i Numéro de l'actif cible or AG_i
2. j Numéro du chemin d'attaque or $P_{i,j}$
3. k Numéro de l'actif ou $A_{i,j,k}$
4. v_{ijk} Identificateur de la vulnérabilité à exploiter (p. ex., CVE-20xx-xxxxx)
5. l_{ijk} Valeur de vraisemblance (probabilité inconditionnelle) de l'exploitation de la vulnérabilité v_{ijk} sur l'actif k

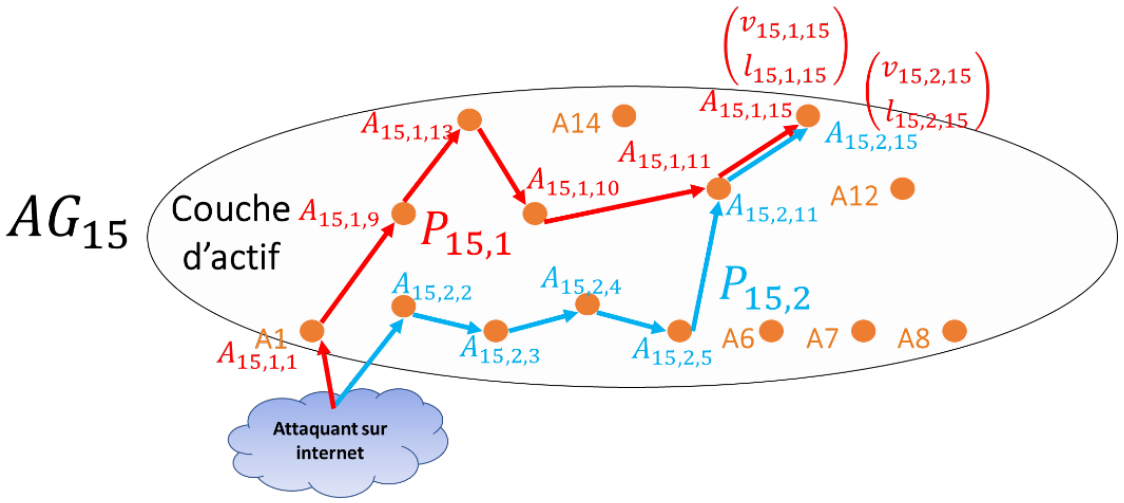
Chaque ligne du tableau représente une autre vulnérabilité et sa valeur de vraisemblance sur chaque actif de chaque chemin d'attaque de chaque graphe d'attaque. Le tableau 11 de la section 10 est un exemple de ce type de tableau.

Ces résultats de la fonction d'intégration deviennent les intrants du graphe d'impact au niveau de la couche d'actifs, ainsi que d'autres informations comme les exigences CID des métriques environnementales du CVSS et la topologie et les paramètres de dépendance fonctionnelle.

Dans le figure 24, un exemple de graphe d'attaque montre les 15 actifs d'une entreprise. Ce graphe est élaboré pour l'actif cible, ou l'actif 15, A_{15}. Par conséquent, le graphe d'attaque est nommé AG_{15}. Il comprend deux chemins d'attaque : $P_{15,1}$ et $P_{15,2}$. D'autres chemins d'attaque doivent être générés pour chaque actif cible possible aux fins d'une analyse complète.

Figure 19

ANALYSE DU GRAPHE D'ATTAQUE



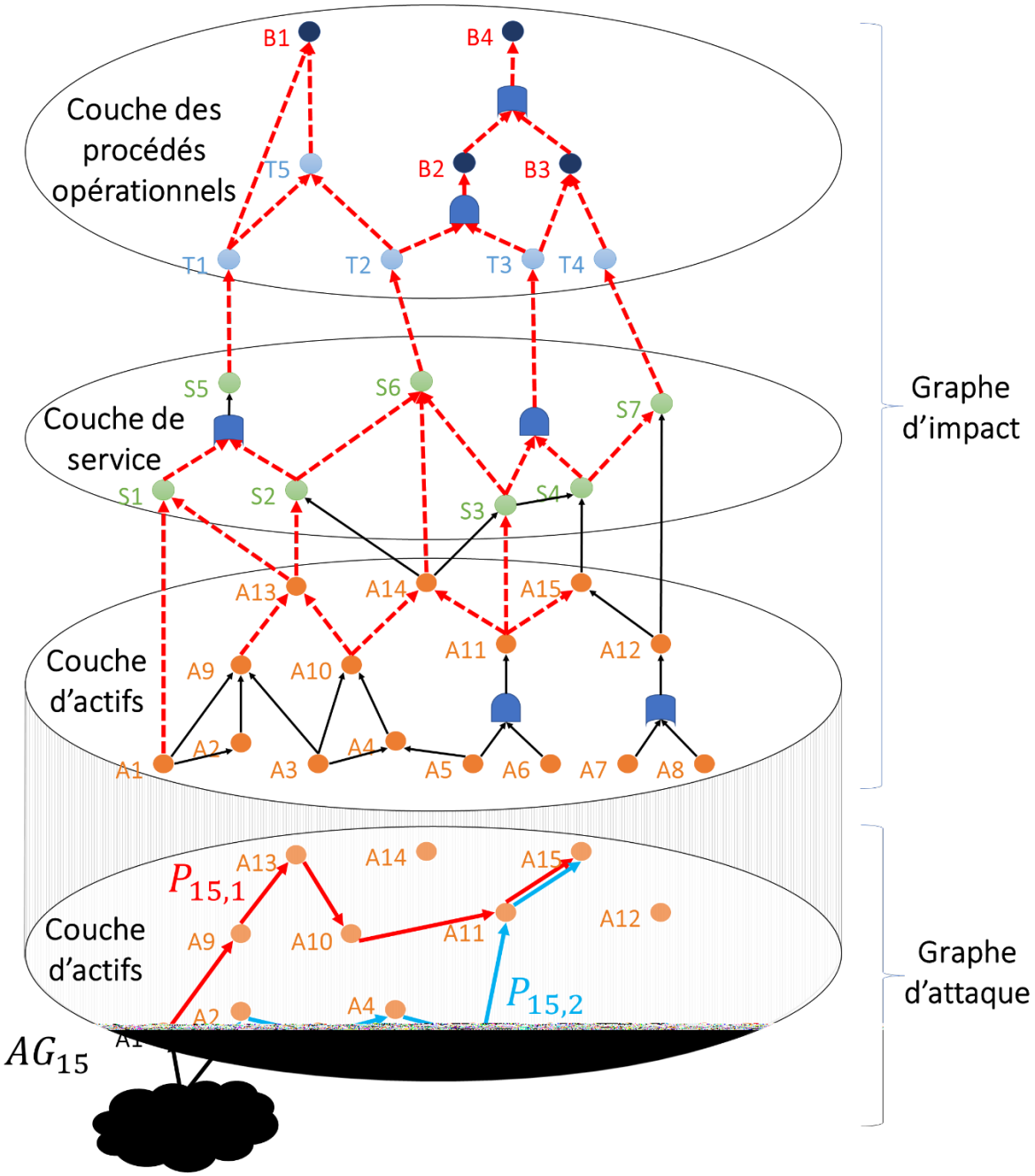
La fonction d'intégration graphe d'attaque-graphe d'impact fournit toute l'information nécessaire à partir de ces deux chemins vers le graphe d'impact, y compris la liste des actifs sur le chemin, les vulnérabilités exploitées et leurs valeurs de vraisemblance. L'intégration de $P_{15,1}$ au graphe d'impact est illustrée à la figure 25. Ce chemin d'attaque est établi pour six actifs :

$$A_{15,1,1}, A_{15,1,9}, A_{15,1,13}, A_{15,1,10}, A_{15,1,11}, A_{15,1,15}$$

La figure 25 représente la propagation de l'impact causée par ce chemin d'attaque avec des flèches rouges, à partir des six actifs indiqués et qui finissent par toucher les quatre processus opérationnels.

Figure 20

QUANTIFICATION DU RISQUE EN INTÉGRANT LE GRAPHE D'ATTAQUE ET LE GRAPHE D'IMPACT



Section 8 : Formule de calcul de la perte d'impact

L'impact économique d'un cyberincident est calculé en fonction de la perte de confidentialité, d'intégrité et de disponibilité sur le plan des processus opérationnels. Selon le Council of Economic Advisors (2018) – d'après des études antérieures menées par le Federal Bureau of Investigation (2017), Verizon (2017) et le l'Open Web Application Security Project – il existe 13 facteurs de coût dans un cyberévénement défavorable : (1) la perte de PI, (2) la perte d'information stratégique, (3) l'atteinte à la réputation, (4) l'augmentation du coût du capital, (5) l'amélioration de la cybersécurité, (6) la perte de données et de matériel, (7) la perte de revenus, (8) les relations publiques, (9) les pénalités réglementaires, (10) la protection des clients, (11) la notification d'infraction, (12) les frais de règlement judiciaire et (13) l'investigation judiciaire (tableau 6).

Une cyberattaque peut entraîner une partie ou la totalité de ces coûts. Par exemple, une attaque par déni de service distribué ciblant une entreprise de vente au détail en ligne perturbe le fonctionnement de la plupart des systèmes de TI et des principaux processus opérationnels. À court terme, l'entreprise perd des ventes pendant l'interruption. À moyen terme, l'entreprise perd ses revenus futurs lorsque certains de ses clients passent à une autre entreprise en raison de la non-disponibilité du service. Selon l'ampleur de l'attaque, des dommages peuvent porter atteinte à la réputation et [traduction libre]« ternir la marque de l'entreprise, réduire ses revenus futurs et ses occasions d'affaires » (Council of Economic Advisors, 2018). Pour réduire l'impact de l'atteinte à la réputation, l'entreprise doit assumer les frais des services de relations publiques pour atténuer ces dommages.

Un autre scénario porte sur les frais encourus en raison d'une attaque de menace persistante avancée (MPA) visant la propriété intellectuelle et l'information stratégique d'une entreprise. L'entreprise perd ainsi son avantage concurrentiel. La propriété intellectuelle volée peut être achetée et utilisée par les rivaux de l'entreprise. La société perd ses revenus futurs. L'entreprise dépense de l'argent pour des services d'investigation judiciaire afin d'identifier l'auteur de l'infraction et elle assume des frais de règlement judiciaire pour obtenir des dommages-intérêts. Le coût du capital – qui [traduction libre] « représente le rendement requis pour exécuter un projet de budgétisation d'immobilisations […] et est utilisé par les entreprises à l'interne pour déterminer si un projet d'immobilisations vaut la mobilisation de ressources, et par les investisseurs qui l'utilisent pour déterminer si un placement vaut le risque par rapport au rendement » (Kenton, 2018) – augmente également puisque les investisseurs estiment que l'entreprise n'a pas suffisamment protégé sa propriété intellectuelle (Council of Economic Advisors, 2018).

Tableau 6

RELATION ENTRE LES CONSÉQUENCES POTENTIELLES ET LES FACTEURS DE COÛT (CONFIDENTIALITÉ, INTÉGRITÉ ET DISPONIBILITÉ)

		Facteurs de coût		
Paramètre de coût	Élément de coût/perte	C	I	D
Ct_1	Perte de PI	X		
Ct_2	Perte d'information stratégique	X	X	X
Ct_3	Atteinte à la réputation	X	X	X
Ct_4	Augmentation du coût du capital	X		
Ct_5	Amélioration de la cybersécurité	X	X	X
Ct_6	Perte de données et de matériel	X	X	X
Ct_7	Perte de revenus	X	X	X
Ct_8	PR	X	X	X
Ct_9	Pénalités réglementaires	X	X	X
Ct_{10}	Protection des consommateurs	X		
Ct_{11}	Avis d'infraction	X		
Ct_{12}	Frais de règlement judiciaire	X	X	X
Ct_{13}	Investigation judiciaire	X	X	X

Le temps et la durée sont également utilisés comme paramètres dans le calcul des coûts.

Les formules de calcul du coût économique sont les suivantes :

$$Coût\ (B_1) = f((C_{BP_1}, t, d), (I_{BP_1}, t, d), (A_{BP_1}, t, d))$$
$$C_{B_1} = g(Ct_1, Ct_2, Ct_3, Ct_4, Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{10}, Ct_{11}, Ct_{12}, Ct_{13})$$
$$I_{B_1} = g(Ct_2, Ct_3, Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{12}, Ct_{13})$$
$$A_{B_1} = g(Ct_2, Ct_3, Ct_5, Ct_6, Ct_7, Ct_8, Ct_9, Ct_{12}, Ct_{13})$$
$$COÛT\ TOTAL = \sum_{k=1}^{n} Coût(B_k)$$

où B_1 représente un processus opérationnel;

C_{B_1} représente le coût de la perte de confidentialité pour B_1;

I_{B_1} représente le coût de la perte d'intégrité pour B_1;

A_{B_1} représente le coût de la perte de disponibilité pour B_1;

t représente le moment où l'impact de la cyberaction est observé;

d représente la durée de la cyberaction.

Les valeurs monétaires indiquées par C_B, I_B, A_B peuvent être déterminées par les réponses d'experts ou à partir des dossiers financiers de l'organisation. Les éléments de coût indiqués au tableau 6 doivent être déterminés en supposant que la vraisemblance d'une attaque réussie est égale à 1. En d'autres termes, l'impact doit être déterminé comme étant indépendant de la vraisemblance. La vraisemblance est censée être intégrée à la mise en œuvre du modèle, et non à l'estimation des éléments de coût.

Il est difficile d'estimer avec exactitude les valeurs des éléments de coût d'une entreprise, et des recherches approfondies sur différentes méthodes se poursuivent. Plus particulièrement, il est relativement difficile d'estimer la perte de PI, la perte d'information stratégique, l'atteinte à la réputation et l'augmentation du coût du capital en ce qui concerne les autres éléments de coût (Council of Economic Advisors, 2018). Par exemple, des études d'événements ont été menées pour analyser les effets des cyberincidents sur les fluctuations du cours des actions qui peuvent servir à estimer la perte de réputation. Pour les entreprises axées sur la recherche et le développement, la perte de PI a tendance à être plus importante, tandis que pour l'armée, la perte d'information stratégique peut être plus importante. Pour les entreprises axées sur la vente au détail en ligne, la perte de revenus est l'élément de coût le plus important. Le calcul de la perte de revenus peut être relativement plus simple si l'on effectue une analyse des ventes en ligne.

Section 9 : Adaptation du modèle à une entreprise

Les chiffres fournis avec ce modèle ne doivent pas être considérés comme les seules intrants pour résoudre le problème de quantification des cyberrisques d'une entreprise. Il existe plusieurs façons de personnaliser le modèle d'après les caractéristiques du profil d'une entreprise. Le modèle élaboré comprend une approche en plusieurs étapes pour modifier les intrants des calculs qui doivent être effectués pour le réseau d'entreprise particulier. En d'autres termes, les chiffres fournis dans le modèle élaboré ne sont pas les seuls intrants des analyses à effectuer sur le réseau de TIC d'une entreprise. Les caractéristiques suivantes du modèle aident à personnaliser les intrants :

1. Groupe des métriques environnementales du CVSS
    a. Métriques de base modifiées
    b. Exigences en matière de confidentialité, d'intégrité et de disponibilité
2. Caractéristiques d'un réseau de dépendances fonctionnelles
    a. Nœuds
    b. Relations de dépendance
    c. Type de relations de dépendance
    d. Paramètres de dépendance
3. Facteurs de pondération des nœuds constitutifs CID

Ces intrants sont expliqués en détail dans les sous-sections suivantes.

9.1 Groupe de métriques environnementales du CVSS

9.1.1 Métriques de base modifiées

Le groupe des métriques environnementales est inclus pour tenir compte des différences entre les caractéristiques des vulnérabilités rattachées aux composantes du réseau des TIC d'entreprises individuelles appartenant à divers secteurs et industries de tailles différentes. Les métriques de base modifiées comprennent toutes les métriques du groupe des métriques de base comme moyen de personnaliser les intrants en fonction des caractéristiques intrinsèques de l'actif de l'entreprise.

Par exemple, il est possible d'exploiter une vulnérabilité particulière si l'ordinateur est branché à un réseau. Par conséquent, la métrique Vecteur d'attaque pour ce logiciel est Réseau. Supposons que l'entreprise dispose d'un réseau intranet isolé qui n'est pas branché à Internet et que l'actif ciblé présente cette vulnérabilité. Comme l'actif n'est pas branché à Internet, un attaquant doit avoir accès à au moins un des ordinateurs branchés à l'intranet. Cette situation peut être gérée en ajustant la métrique Vecteur d'attaque modifié à Local.

Si l'actif cible n'est branché à aucun réseau et ne comporte pas de dispositif de branchement réseau intégré, la seule façon d'exploiter cette vulnérabilité sur cet actif consiste à avoir un accès physique à l'actif proprement dit. Dans ce cas, la métrique Vecteur d'attaque modifié devient Physique.

Des modifications semblables à celles énoncées dans les exemples peuvent être apportées à d'autres métriques de base modifiées pour tenir compte des caractéristiques des vulnérabilités pour les composantes des TIC de l'entreprise.

9.1.2 Exigences en matière de confidentialité, d'intégrité et de disponibilité

Le groupe des métriques environnementales compte trois autres métriques qui aident à évaluer la vulnérabilité à une composante des TIC : Exigences en matière de confidentialité, d'intégrité et de disponibilité. La même vulnérabilité sur une composante des TIC branchée au réseau peut avoir un impact significatif sur la confidentialité, l'intégrité ou la disponibilité. Toutefois, elle peut avoir un effet nul ou moindre si elle est exploitée sur une autre composante. Ces métriques sont utilisées pour tenir compte de ces différences. Par exemple, dans le cas d'une vulnérabilité sur un serveur Web qui rend tout son contenu accessible au public, une exploitation qui n'affecte que sa confidentialité n'est pas importante, puisqu'il n'y a pas de données confidentielles sur le serveur. Dans ce cas, l'exigence de confidentialité pour les vulnérabilités de cette composante des TIC est fixée à Faible.

9.2 Caractéristiques d'un réseau de dépendances fonctionnelles

Certaines caractéristiques de la FDNA permettent de mieux intégrer aux analyses les caractéristiques du réseau des TIC d'une entreprise. Ces caractéristiques sont ses nœuds, les relations de dépendance, le type de relations de dépendance et les paramètres de dépendance. Même de petits changements dans ces caractéristiques peuvent influer sur le comportement du modèle. L'établissement d'un réseau de dépendances fonctionnelles est une étape essentielle du modèle élaboré pour mettre en œuvre les caractéristiques du réseau des TIC de l'entreprise.

9.2.1 Nœuds

Les nœuds de la FDNA ne sont pas nécessairement des composantes individuelles d'un réseau. Chaque actif peut être représenté par plusieurs nœuds si ceux-ci comportent plus d'une fonction dans le réseau des dépendances fonctionnelles.

Les nœuds permettent également de simplifier les actifs aux caractéristiques complexes. Bien qu'il soit possible de représenter un poste de travail rarement utilisé comme un nœud, on peut aussi attribuer comme autre nœud un système de contrôle industriel qui gère le débit d'eau de refroidissement d'un réacteur. Peu importe la complexité de la conception d'un actif ou l'importance de son fonctionnement, sa fonctionnalité devient un nœud dans le réseau des dépendances fonctionnelles. Une personne n'a pas besoin de connaître tous les détails du fonctionnement d'un actif des TIC; il lui suffit de connaître la fonctionnalité fournie par l'actif pour cerner le nœud du réseau de dépendances fonctionnelles.

9.2.2 Relations de dépendance

Tous les processus d'une entreprise peuvent être modélisés dans le cadre du réseau de dépendances fonctionnelles. La relation de dépendance fonctionnelle ne suit pas nécessairement les relations entrées-sorties entre les nœuds. En d'autres termes, les produits ou l'information peuvent passer d'un actif à l'autre, mais la dépendance fonctionnelle peut suivre le flux inverse entre les fonctions de ces nœuds. Par exemple, une boucle de rétroaction dans un processus peut être modélisée comme une fonction permettant de vérifier et d'améliorer la qualité du produit. La boucle peut également être modélisée comme une relation de dépendance fonctionnelle entre le nœud du mécanisme de rétroaction et le processus de production.

9.2.3 Type de relations de dépendance

Dans la cyberFDNA, outre la relation de dépendance de la FDNA, il existe des dépendances logiques ET et OU. Ces types de dépendance aident à mettre en œuvre les caractéristiques des dépendances fonctionnelles des TIC dans les analyses. Par exemple, si la redondance a été intégrée à un système particulier au cas où celui-ci ne fonctionnerait pas, il existe une dépendance OU entre les nœuds redondants et le nœud qui en dépend.

9.2.4 Paramètres de dépendance

La solidité et la criticité de la dépendance définissent le niveau de dépendance entre deux nœuds. Leurs paramètres sont alpha et bêta, respectivement. Ces deux paramètres existent pour chaque relation de dépendance et ils constituent d'autres façons de mettre en œuvre les caractéristiques d'une entreprise dans les analyses.

9.3 Facteurs de pondération des nœuds constitutifs de confidentialité, d'intégrité et de disponibilité

Chaque nœud de la cyberFDNA est un nœud constitutif comportant des composantes CID. Il s'agit d'une caractéristique fondamentale de ce modèle. Les valeurs d'opérabilité de chaque composante d'un nœud représentent la mesure dans laquelle le nœud est protégé du point de vue des composantes CID. Chaque nœud a une valeur d'opérabilité pour chacune de ces composantes. Toutefois, les différences entre les divers types de nœuds sont représentées par les facteurs de pondération de ces composantes pour chaque nœud constitutif. Une pondération plus élevée est attribuée si l'une des composantes CID a une grande importance pour la fonction de l'actif. Par exemple, si la disponibilité d'un actif est plus importante que la confidentialité et l'intégrité, un facteur de pondération plus élevé est attribué à la disponibilité. Les facteurs de pondération peuvent être déterminés en consultant l'opinion d'experts. En attribuant des pondérations en fonction des caractéristiques d'un actif particulier, le modèle est adapté à l'entreprise.

Section 10 : Exemple

Cette section présente une séquence pour l'utilisation efficiente du cadre élaboré. Elle est appliquée à un scénario hypothétique de formation en ligne pour aider le lecteur à comprendre les détails du cadre. La séquence est la suivante :

1. Produire le graphe d'impact
    a. Dresser la liste de tous les processus opérationnels de l'entreprise
    b. Dresser la liste de tous les services qui facilitent le fonctionnement des processus opérationnels
    c. Dresser la liste de tous les actifs de l'organisation
    d. Désigner les dépendances fonctionnelles entre les actifs, les services et les processus opérationnels, y compris les interdépendances et les intradépendances
    e. Déterminer les paramètres de dépendance fonctionnelle pour chaque dépendance
2. Produire le graphe d'attaque
    a. Analyser tous les actifs pour dresser la liste de toutes les vulnérabilités
    b. Produire des graphes d'attaque pour tous les actifs cibles possibles
3. Analyser chaque chemin d'attaque de chaque graphe d'attaque
    a. Calculer les probabilités conditionnelles pour chaque nœud
    b. Calculer la vraisemblance (probabilité inconditionnelle) pour chaque nœud
    c. Utiliser la fonction d'interconnexion graphe d'attaque-graphe d'impact pour chaque chemin d'attaque
4. Analyser le graphe d'impact pour chaque chemin d'attaque
    a. Récupérer le résultat du chemin d'attaque
    b. Calculer les métriques modifiées pour les analyses
    c. Analyser la propagation de l'impact entre les couches
    d. Calculer la perte d'impact pour le chemin d'attaque.
5. Grouper et comparer les résultats

10.1 Produire le graphe d'impact

Une approche descendante peut être utilisée pour produire le graphe d'impact d'une entreprise. Ce graphe comprend des nœuds et des connexions, les nœuds étant des composantes fonctionnelles de l'entreprise, et les connexions représentant les dépendances entre les fonctions.

Une entreprise peut avoir un ou plusieurs processus opérationnels dont les principaux objectifs consistent à générer de la valeur ou des bénéfices. Dans le cas d'un établissement d'enseignement supérieur qui offre des programmes en ligne, les processus opérationnels peuvent comprendre l'« exécution de programmes en ligne », l'« exécution de programmes sur place » et l'« exécution d'activités de recherche ». L'exécution de programmes en ligne représente le processus opérationnel sur lequel porte cet exemple et qui est désigné par B1 dans la figure 26 et au tableau 7.

Les services sont les capacités qui facilitent l'application des processus opérationnels. « L'hébergement d'un site Web pour les cours archivés », « la facilitation de cours synchrones », « l'existence d'un système de gestion de l'apprentissage » et « la prestation de services de courriel » sont quelques-uns des services possibles qui aident l'établissement à offrir des programmes en ligne. L'hébergement d'un site Web pour les cours archivés est désigné par S1 dans la figure 26 et le tableau 7.

Le nombre d'actifs ne correspond pas nécessairement à la quantité de matériel dont dispose l'entreprise. Les actifs doivent être considérés d'un point de vue fonctionnel, car une composante réseau particulière peut servir de multiples façons avec les logiciels installés ou les processus à exécuter. Les actifs qui rendent S1 possible sont le « pare-feu externe », le « serveur Web », le « pare-feu interne » et le « serveur de base de données »; ils sont représentés respectivement par A1, A2, A3 et A4.

La préparation de la liste de tous les processus opérationnels, services et actifs constitue la première étape de la production d'un graphe d'impact. L'étape suivante consiste à établir les liens de dépendance entre ces processus, services et actifs. La même approche descendante ou ascendante peut être utilisée. Les dépendances fonctionnelles dans les couches et entre elles doivent être prises en compte, y compris les dépendances ET et OU. La figure 26 présente une partie du graphe d'impact pour notre établissement théorique. S1 n'est qu'un des services qui appuient B1; toutefois, cet exemple demeure simple pour montrer comment fonctionne le graphe d'impact.

Figure 21

GRAPHE D'IMPACT POUR UN ÉTABLISSEMENT D'ENSEIGNEMENT SUPÉRIEUR

Tous les nœuds de ce graphe d'impact sont des nœuds constitutifs qui comprennent des aspects CID, et chaque aspect est pondéré en fonction de son importance pour chaque nœud. Les facteurs de pondération peuvent être déterminés selon l'opinion d'experts. Les descriptions et les facteurs de pondération de chaque nœud sont présentés dans le tableau 7.

Tableau 7

FACTEURS DE PONDÉRATION ET DESCRIPTIONS DES ASPECTS CID DES NŒUDS DU GRAPHE D'IMPACT

	Nom	Type	w_{Ci}	w_{Ii}	w_{Ai}	Description
A1	Pare-feu externe	Actif	0.10	0.45	0.45	Filtre le trafic vers le serveur Web
A2	Serveur Web	Actif	0.10	0.20	0.70	

La dernière étape de la production du graphe d'impact consiste à déterminer la solidité et la criticité des valeurs de dépendance (paramètres alpha et bêta) des connexions de dépendance. Voici les définitions à retenir :

Solidité de la dépendance (SD) : « La solidité avec laquelle le niveau d'opérabilité d'un nœud récepteur dépend du niveau d'opérabilité des nœuds d'alimentation. La SD saisit les effets des relations qui augmentent le NOB » (Garvey et Pinto, 2009). Le paramètre pour SD est α et sa plage est $0 < \alpha_{ij} \leq 1$.

Criticité de la dépendance (CD) : « La criticité des contributions du nœud d'alimentation à un nœud de récepteur pour qu'il atteigne ses objectifs de niveau d'opérabilité. La CD régit la façon dont la performance du nœud récepteur diminuera sous le NOB dans le temps et pourrait devenir inutilisable à terme » (Garvey et Pinto, 2009). Le paramètre pour la CD est β et sa plage est $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$.

Les tableaux 8 et 9 fournissent les valeurs alpha et bêta entre les dépendances des aspects de CID des nœuds constitutifs; chaque ligne représente un nœud d'alimentation, tandis que chaque colonne représente un nœud récepteur. Par exemple, $\alpha_{A1I,A2I}$ est 0,5, tandis que $\beta_{A1I,A2I}$ est 50. Ces valeurs sont attribuées au moyen d'une évaluation d'expert. Les colonnes A1 et A3 sont toutes vides, car elles ne sont que des nœuds d'alimentation (c.-à-d. pas des nœuds récepteurs). De même, les lignes B1 sont toutes vides parce que B1 n'est qu'un nœud récepteur et non un nœud d'alimentation.

Tableau 8

SOLIDITÉ DE LA DÉPENDANCE ENTRE LES PAIRES DE NŒUDS D'ALIMENTATION (LIGNES) ET DE NŒUDS RÉCEPTEURS (COLONNES)

	A1C	A1I	A1A	A2C	A2I	A2A	A3C	A3I	A3A	A4C	A4I	A4A	S1C	S1I	S1A	B1C	B1I	B1A
A1C				0.3														
A1I				0.3	0.5	0.9												
A1A						0.8												
A2C													1					
A2I													1	1	1			
A2A															1			
A3C				0.8						0.8								
A3I				0.9	0.8	0.5				1	0.9	0.5						
A3A						0.3						0.5						
A4C				0.5														
A4I				0.1	1	0.1												
A4A						0.1												
S1C																0.4		
S1I																0.4	0.4	0.4
S1A																		0.4
B1C																		
B1I																		
B1A																		

Tableau 9

CRITICITÉ DE LA DÉPENDANCE ENTRE LES PAIRES DE NŒUDS D'ALIMENTATION (LIGNES) ET DE NŒUDS RÉCEPTEURS (COLONNES)

	A1C	A1I	A1A	A2C	A2I	A2A	A3C	A3I	A3A	A4C	A4I	A4A	S1C	S1I	S1A	B1C	B1I	B1A
A1C				50														
A1I				50	50	10												
A1A						10												
A2C													0					
A2I													0	0	0			
A2A															0			
A3C				20						20								
A3I				10	20	30				0	10	50						
A3A						30						50						
A4C				25														
A4I				50	0	80												
A4A						85												
S1C																60		
S1I																55	60	55
S1A																		60
B1C																		
B1I																		
B1A																		

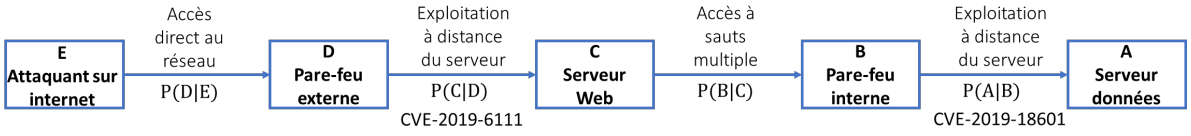
À ce stade, la production du graphe d'impact est terminée. Les intrants du graphe d'attaque sont nécessaires pour l'analyse.

10.2 Produire le graphe d'attaque

Pour générer le graphe d'attaque, tous les actifs doivent être analysés pour déceler les vulnérabilités. Après avoir analysé les quatre actifs, le logiciel de production de graphes d'attaque crée des chemins d'attaque possibles pour des cibles précises. Cet exemple suppose qu'un seul chemin d'attaque cible la disponibilité du serveur de base de données. Le graphe d'attaque d'une telle intrusion par un attaquant qui se trouve sur Internet est illustré à la figure 27.

Figure 22

GRAPHE D'ATTAQUE POUR LE CHEMIN QUI CIBLE LA DISPONIBILITÉ DU SERVEUR DE BASE DE DONNÉES



Comme il est indiqué, l'exploitation de deux vulnérabilités est nécessaire pour perturber le fonctionnement du serveur de base de données.

La première vulnérabilité se trouve sur le serveur Web (C) et son identificateur de la BDVN est CVE-2019-6111. Cette vulnérabilité existe sur OpenSSH, un ensemble de logiciels qui aident à sécuriser le réseautage au moyen du protocole Secure Shell. L'exploitation de cette vulnérabilité permet aux attaquants d'écraser tous les fichiers du répertoire cible et elle est donc considérée comme une attaque contre l'intégrité du serveur. La confidentialité et la disponibilité du serveur ne sont pas touchées par cette attaque. Voici les détails des vulnérabilités, selon la base de données nationale sur les vulnérabilités :

Valeurs CVSS de CVE-2019-6111 sur le serveur Web

Chaîne vectorielle : AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Note de base du CVSS : 5,9 (MOYENNE)

- Vecteur d'attaque (AV :N) : Réseau
- Complexité de l'attaque (AC :H) : Élevé
- Privilèges requis (RP :N) : Aucun
- Interaction utilisateur (UI :N) : Aucun
- Portée (S :U) : Inchangée
- Confidentialité (C :N) : Aucun
- Intégrité (I :H) : Élevé
- Disponibilité (A :N) : Aucun

La deuxième vulnérabilité existe sur le serveur de base de données (A) et son identificateur est CVE-2019-18601. Cette vulnérabilité existe dans un système de fichiers distribué appelé OpenAFS. Les attaquants peuvent exploiter cette vulnérabilité et envoyer à répétition des appels malveillants au serveur de la base de données, ce qui peut provoquer une panne et annuler le service. Une telle attaque est réputée complexe, mais elle ne nécessite aucune interaction avec l'utilisateur ni aucun justificatif d'identité particulier. De plus, il est possible de mener cette attaque à distance à partir d'Internet. Le seul impact est la disponibilité du serveur, ce qui signifie que la confidentialité et l'intégrité du serveur ne sont pas touchées. Voici les détails concernant les vulnérabilités, selon la base de données nationale sur les vulnérabilités :

Valeurs CVSS de CVE-2019-18601 sur le serveur de base de données

Chaîne vectorielle : AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N:A:H

Note de base du CVSS : 7,5 ÉLEVÉE

- Vecteur d'attaque (AV :N) : Réseau
- Complexité de l'attaque (AC :L) : Faible
- Privilèges requis (RP :N) : Aucun
- Interaction utilisateur (UI :N) : Aucun
- Portée (S :U) : Inchangée
- Confidentialité (C :N) : Aucun
- Intégrité (I :N) : Aucun
- Disponibilité (A :H) : Élevé

10.3 Analyser chaque chemin d'attaque de chaque graphe d'attaque

Dans cet exemple, nous avons supposé un seul graphe d'attaque (AG_4) et un seul chemin d'attaque ($P_{4,1}$) pour ce graphe d'attaque. Toutes les probabilités conditionnelles et inconditionnelles sont calculées à cette étape.

Les données numériques du tableau 10 sont déterminées selon l'information sur la BDNV et le tableau 3. Certaines de ces valeurs seront utilisées dans l'analyse des répercussions et expliquées plus loin à la section 10.4. À cette étape, les probabilités inconditionnelles sont calculées au moyen de l'équation 2. On suppose que la probabilité du désir d'attaque d'un attaquant est de 0,5, soit Pr(E).

Tableau 10

VALEURS NUMÉRIQUES DES MÉTRIQUES DE VULNÉRABILITÉ

	CVE-2019-6111		CVE-2019-18601	
Métrique	Valeur	Valeur numérique	Valeur	Valeur numérique
Vecteur d'attaque (AV)	Réseau	0,85	Réseau	0,85
Complexité de l'attaque (AC)	Élevé	0,44	Faible	0,77
Privilèges requis (RP)	Aucun	0,85	Aucun	0,85
Interaction avec l'utilisateur (UI)	Aucun	0,85	Aucun	0,85
Portée (S)	Inchangée		Inchangée	
Confidentialité (C)	Aucun	100	Aucun	100
Intégrité (I)	Élevé	0	Aucun	100
Disponibilité (A)	Aucun	100	Élevé	0
Niveau de correction	Réparation temporaire	0,97		
Probabilité conditionnelle	P(C|D)	0,550428	P(A|B)	0,99304

Le serveur Web est situé dans la topologie du réseau dans une zone démilitarisée (ZD). Le pare-feu externe protège la zone démilitarisée en ne permettant que le trafic pertinent d'Internet au réseau. Pr($D|E$) est la probabilité conditionnelle d'accès direct à partir de la navigation sur Internet dans le contenu publié sur le serveur Web. Puisque ce trafic est autorisé, la probabilité, Pr($D|E$), est égale à 1.

$$\Pr(D) = \Pr(D|E) * \Pr(E) = 1 * 0.5 = 0.5$$

Selon l'équation 2, la probabilité conditionnelle d'exploiter la vulnérabilité du logiciel exécuté sur le serveur Web, qui est Pr($C|D$), est calculée en introduisant les valeurs du tableau 10 comme suit :

$$\begin{aligned}\Pr(C|D) = 2.1 * &Vecteur\ d'attaque * \text{Complexité de l'attaque} * \text{Privilèges requis} \\ &* \text{Interaction avec l'utilisateur} * \text{Maturité du code d'exploitation} * \text{Niveau de correction} \\ &* \text{Confiance du rapport} = 2.1 * 0.85 * 0.44 * 0.85 * 0.85 * 1 * 0.97 * 1 = 0.55\end{aligned}$$

La probabilité inconditionnelle d'exploitation du serveur Web est calculée comme suit :

$$\Pr(C) = \Pr(C|D) * \Pr(D) = 0.55 * 0.5 = 0.28$$

L'impact sur l'intégrité à la suite de l'exploitation de cette vulnérabilité sur le serveur Web est élevé et il permet à un attaquant d'exécuter un code arbitraire sur le serveur. Selon les configurations du pare-feu interne, seul le serveur Web peut accéder au serveur de base de données. Le serveur Web est nécessaire comme tremplin dans ce chemin d'attaque. En utilisant cette escalade de privilège, l'attaquant peut passer outre le serveur interne afin d'exploiter la vulnérabilité du serveur de base de données. La probabilité conditionnelle d'un accès multibond au pare-feu interne est de 1, donc de Pr($B|C$) = 1. Cela donne la probabilité inconditionnelle du pare-feu interne, la valeur Pr(B) = 0.28 * 1 = 0.28.

La probabilité conditionnelle d'exploiter la vulnérabilité sur le serveur de base de données est également calculée en utilisant l'équation 2 et les valeurs du tableau 10, comme suit :

$$\begin{aligned}\Pr(A|B) = 2.1 * &Vecteur\ d'attaque * \text{Complexité de l'attaque} * \text{Privilèges requis} \\ &* \text{Interaction avec l'utilisateur} * \text{Maturité du Code d'exploitation} * \text{Niveau de correction} \\ &* \text{Confiance du rapport} = 2.1 * 0.85 * 0.77 * 0.85 * 0.85 * 1 * 1 * 1 = 0.99\end{aligned}$$

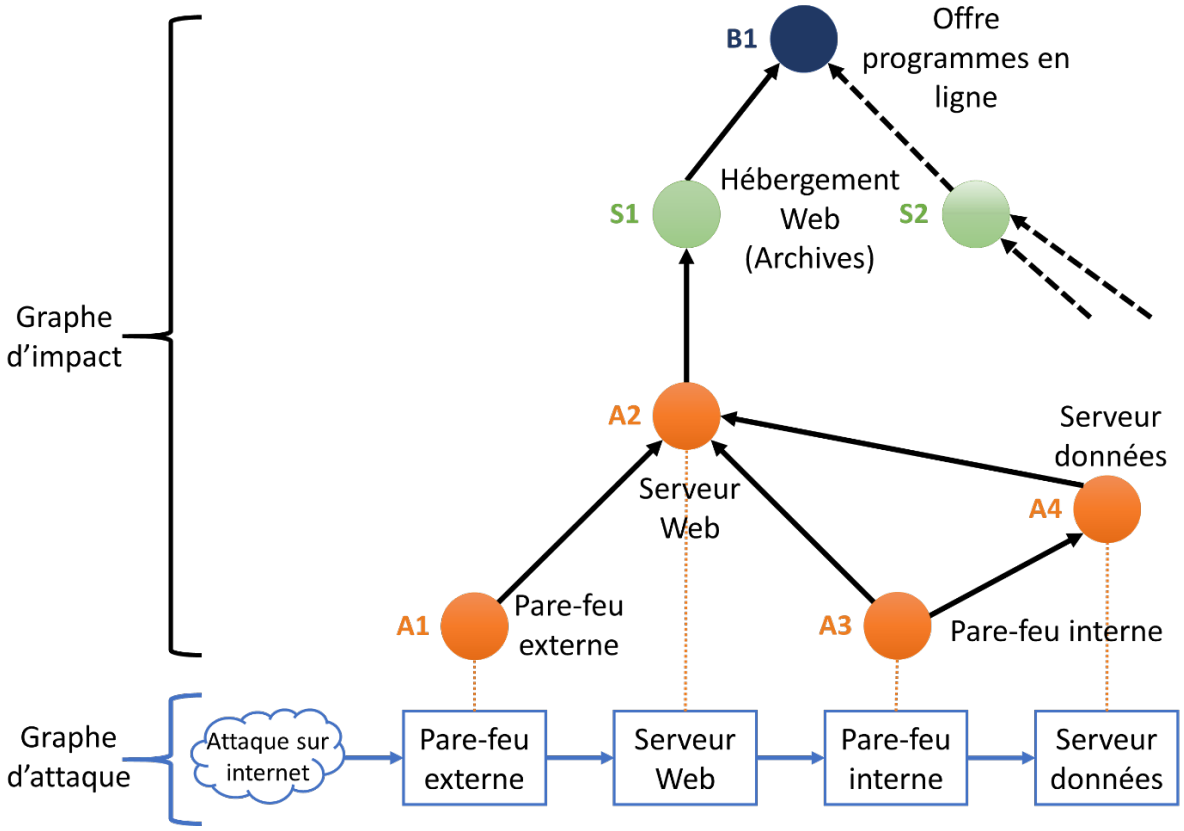
Même si la probabilité conditionnelle est élevée, la probabilité inconditionnelle est beaucoup plus faible puisque le serveur de la base de données est situé dans un réseau mieux protégé.

$$\Pr(A) = \Pr(A|B) * \Pr(B) = 0.99 * 0.28 = 0.27$$

Étant donné que toutes les valeurs de probabilité inconditionnelle ont été calculées, les graphes d'attaque-graphe d'impact peuvent être intégrés. La figure 28 montre cette intégration. Les nœuds connexes des deux graphes sont reliés à des lignes pointillées orange.

Figure 23

EXEMPLE D'INTÉGRATION GRAPHE D'ATTAQUE-GRAPHE D'IMPACT



Il convient de noter que les chemins de propagation d'attaque et de propagation d'impact ne sont pas les mêmes. Bien qu'il y existe un chemin d'attaque (A1-A2-A3-A4), il y a trois chemins de propagation de l'impact (A1-A2; A3-A2; A3-A4-A2) dans la couche d'actifs, parce que la dépendance fonctionnelle entre les actifs n'est pas parfaitement corrélée avec la topologie du réseau des TIC et les attaques en plusieurs étapes possibles.

Les résultats de la fonction d'intégration du graphe d'attaque et du graphe d'impact sont résumés au tableau 11. Dans cet exemple, seul A4 a été choisi comme nœud cible; il n'y a donc qu'un graphe d'attaque (AG_4). Selon les vulnérabilités des actifs, il n'y a qu'un seul chemin d'attaque ($P_{4,1}$). Pour chaque actif le long de ce chemin d'attaque, les vulnérabilités connexes et les valeurs de vraisemblance (probabilité inconditionnelle) sont également présentées dans le tableau.

Tableau 11

TABLEAU DES RÉSULTATS DE LA FONCTION D'INTÉGRATION

AG_i	$P_{i,j}$	$A_{i,j,k}$	$v_{i,j,k}$	$l_{i,j,k}$
AG_4	$P_{4,1}$	$A_{4,1,1}$	—	—
AG_4	$P_{4,1}$	$A_{4,1,2}$	CVE-2019-6111	0.28
AG_4	$P_{4,1}$	$A_{4,1,3}$	—	—
AG_4	$P_{4,1}$	$A_{4,1,4}$	CVE-2019-18601	0.27

10.4 Analyser le graphe d'impact pour chaque chemin d'attaque

Cette étape porte plus précisément sur la façon dont les impacts des cyberattaques se propagent au sein d'une entreprise et entre les couches d'une entreprise, depuis les actifs jusqu'aux processus opérationnels. Dans notre exemple, A2 et A4 sont des actifs touchés par une exploitation de vulnérabilité qui réduit leur rendement.

Selon le tableau 10, l'exploitation de l'A4 a un impact important sur la disponibilité. La confidentialité et l'intégrité de A4 ne sont pas directement touchées par l'exploitation de la vulnérabilité. L'incidence élevée sur la disponibilité réduit la valeur d'opérabilité du nœud constitutif de la confidentialité de 100 à 0, soit une diminution de 100 utils. L'utilité prévue est calculée en multipliant les valeurs de probabilité et d'impact. Puisque la probabilité de cette exploitation, P(A), est de 0,27, la perte d'*utilité prévue* (V_{IA4}) devient $100 * 0{,}27 = 27$ utils (diminution). Pour les nœuds d'alimentation seulement, la valeur d'opérabilité est réduite de 27 utils pour appliquer l'impact de la cyberattaque. Pour les nœuds qui sont à la fois des récepteurs et des alimentateurs, ce changement peut être appliqué en diminuant l'autoefficacité des nœuds. Comme A4 est à la fois un nœud d'alimentation et un nœud récepteur, son autoefficacité est réduite de 0,27, passant de 1 à 0,73, tandis que les valeurs d'opérabilité demeurent constantes. Cela signifie que la disponibilité de A4 ne peut fonctionner qu'avec 73 % de son rendement.

$$SE_{AA4} = 0.73$$

où SE_{IA4} est l'autoefficacité de la composante intégrité de l'actif 4.

De même, selon le tableau 10, l'exploitation de A2 a un grand impact sur l'intégrité. La confidentialité et la disponibilité de A2 ne sont pas directement touchées par cette exploitation de vulnérabilité. La probabilité de l'exploitation, P(C), est de 0,27. L'utilité prévue diminue de $100 * 0.28 = 28$ utils. Comme A2 est à la fois un nœud d'alimentation et un nœud récepteur, son autoefficacité est réduite de 0,28, passant de 1 à 0,72, tandis que les valeurs d'opérabilité demeurent constantes.

$$SE_{IA2} = 0.72$$

où SE_{IA3} est l'autoefficacité de la composante intégrité de l'actif 2.

Compte tenu de ces valeurs d'autoefficacité, la propagation de l'impact peut être calculée. Ce processus commence par les nœuds d'alimentation seulement, qui sont A1 et A3. Toutes les composantes CID de ces nœuds ont une valeur d'opérabilité de 100.

$$P_i = w_{Ci}V_{Ci} + w_{Ii}V_{Ii} + w_{Ai}V_{Ai} \qquad \text{Équation 4}$$

$$P_{A1} = w_{CA1}V_{CA1} + w_{IA1}V_{IA1} + w_{AA1}V_{AA1}$$

$$P_{A1} = 0.10 * 100 + 0.45 * 100 + 0.45 * 100 = 100$$

$$P_{A3} = w_{CA3}V_{CA3} + w_{IA3}V_{IA3} + w_{AA3}V_{AA3}$$

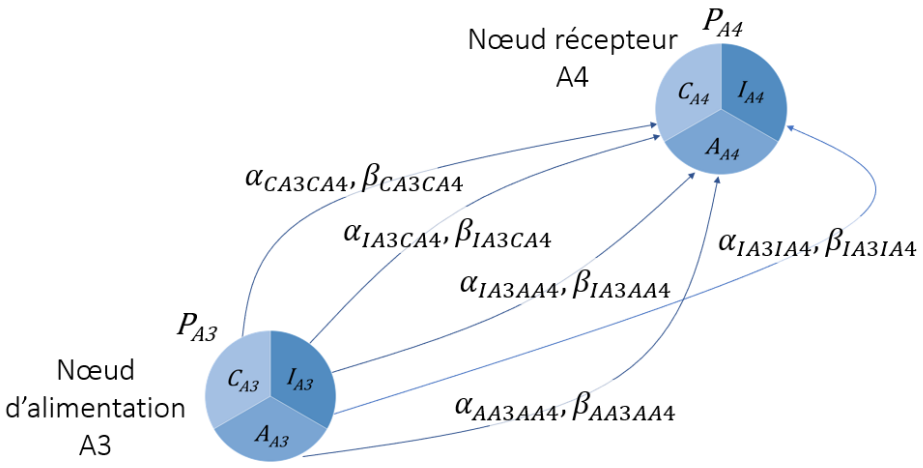
$$P_{A3} = 0.10 * 100 + 0.45 * 100 + 0.45 * 100 = 100$$

Les calculs de propagation de l'impact sont effectués en fonction du réseau de dépendance. A1 et A3 alimentent A2 et A4. Puisque A2 dépend de A4, l'opérabilité de A4 est calculée avant celle de A2.

$$P_{A4} = w_{CA4}V_{CA4} + w_{IA4}V_{IA4} + w_{AA4}V_{AA4}$$

A4 ne dépend que d'un seul nœud, A3. Les relations de dépendance entre les nœuds constitutifs sont illustrées à la figure 29.

Figure 24
RELATION DE DÉPENDANCE ENTRE A3 ET A4



Rappelons les équations suivantes pour la dépendance à un nœud :

$$V_{Cj} = SE_{Cj} * \left(Min\left(Ave\left(SODV_{CjCi}, SODV_{CjIi}\right), CODV_{CjCi}, CODV_{CjIi}\right)\right)$$

$$V_{Cj} = SE_{Cj} * \left(Min\left(\frac{\alpha_{CiCj}V_{Ci}}{2} + \frac{\alpha_{IiCj}V_{Ii}}{2} + 100\left(1 - \frac{\alpha_{CiCj}+\alpha_{IiCj}}{2}\right), V_{Ci} + \beta_{CiCj}, V_{Ii} + \beta_{IiCj}\right)\right)$$

$$V_{Ij} = SE_{Ij} * \left(Min\left(SODV_{IjIi}, CODV_{IjIi}\right) = SE_{Ij} * Min(\alpha_{IiIj}V_{Ii} + 100(1 - \alpha_{IiIj}), V_{Ii} + \beta_{IiIj})\right)$$

$$V_{Aj} = SE_{Aj} * \left(Min\left(Ave\left(SODV_{AjAi}, SODV_{AjIi}\right), CODV_{AjAi}, CODV_{AjIi}\right)\right)$$

$$V_{Aj} = SE_{Aj} * \left(Min\left(\frac{\alpha_{AiAj}V_{Ai}}{2} + \frac{\alpha_{IiAj}V_{Ii}}{2} + 100\left(1 - \frac{\alpha_{AiAj}+\alpha_{IiAj}}{2}\right), V_{Ai} + \beta_{AiAj}, V_{Ii} + \beta_{IiAj}\right)\right)$$

À l'aide de ces équations, l'opérabilité des composantes CID de A4 et A4 peut être calculée comme suit :

$$V_{CA4} = SE_{CA4} * \left(Min(Ave(SODV_{CA4CA3}, SODV_{CA4IA3}), CODV_{CA4CA3}, CODV_{CA4IA3})\right)$$

$$V_{CA4} = SE_{CA4} * \left(Min\left(\frac{\alpha_{CA3CA4}V_{CA3}}{2} + \frac{\alpha_{IA3CA4}V_{IA3}}{2} + 100\left(1 - \frac{\alpha_{CA3CA4}+\alpha_{IA3CA4}}{2}\right), V_{CA3} + \beta_{CA3CA4}, V_{IA3} + \beta_{IA3CA4}\right)\right)$$

$$V_{CA4} = 1\left(Min\left(\frac{0.8 * 100}{2} + \frac{1 * 100}{2} + 100\left(1 - \frac{0.8 + 1}{2}\right), 100 + 20, 100 + 0\right)\right)$$

$$V_{CA4} = 1\left(Min(40 + 50 + 100(1 - 0.9), 120, 100)\right)$$

$$V_{CA4} = 1\left(Min(100, 120, 100)\right)$$

$$V_{CA4} = 100\ utils$$

$$V_{IA4} = SE_{IA4} * (Min(SODV_{IA4IA3}, CODV_{IA4IA3}) = SE_{IA4} * Min(\alpha_{IA3IA4}V_{IA3} + 100(1 - \alpha_{IA3IA4}), V_{IA3} + \beta_{IA3IA4}))$$

$$V_{IA4} = 1 * \ (Min(0.9 * 100 + 100(1 - 0.9), 100 + 10))$$

$$V_{IA4} = Min(90 + 10, 110)$$

$$V_{IA4} = 100\ utils$$

$$V_{AA4} = SE_{AA4} * \left(Min(Ave(SODV_{AA4AA3}, SODV_{AA4IA3}), CODV_{AA4AA3}, CODV_{AA4IA3})\right)$$

$$V_{AA4} = SE_{AA4} * \left(Min\left(\frac{\alpha_{AA3AA4} V_{AA3}}{2} + \frac{\alpha_{IA3AA4} V_{IA3}}{2} + 100\left(1 - \frac{\alpha_{AA3AA4} + \alpha_{IA3AA4}}{2}\right), V_{AA3} + \beta_{AA3AA4}, V_{IA3} + \beta_{IA3AA4} \right) \right)$$

$$V_{AA4} = 0.73\left(Min\left(\frac{0.5 * 100}{2} + \frac{0.5 * 100}{2} + 100\left(1 - \frac{0.5 + 0.5}{2}\right), 100 + 50, 100 + 50 \right) \right)$$

$$V_{AA4} = 0.73\big(Min(25 + 25 + 50, 150, 150)\big)$$

$$V_{AA4} = 0.73 * 100$$

$$V_{AA4} = 73\ utils$$

$$P_{A4} = w_{CA4} V_{CA4} + w_{IA4} V_{IA4} + w_{AA4} V_{AA4}$$

$$P_{A4} = 0.35 * 100 + 0.35 * 100 + 0.30 * 73 = 35 + 35 + 21.9$$

$$P_{A4} = 91.9$$

Puisque l'opérabilité de A1, A3 et A4 est maintenant connue, l'opérabilité de A2 peut être calculée. Étant donné que A2 dépend de trois nœuds, ses calculs sont plus compliqués; toutefois, le même concept s'applique.

$$P_{A2} = w_{CA2} V_{CA2} + w_{IA2} V_{IA2} + w_{AA2} V_{AA2}$$

Les équations sont adaptées pour la dépendance à trois nœuds :

$$V_{CA2} = SE_{CA2} * \left(Min\left(\begin{matrix} Ave(SODV_{CA2CA1}, SODV_{CA2IA1}, SODV_{CA2CA3}, SODV_{CA2IA3}, SODV_{CA2CA4}, SODV_{CA2IA4}), \\ CODV_{CA2CA1}, CODV_{CA2IA1}, CODV_{CA2CA3}, CODV_{CA2IA3}, CODV_{CA2CA4}, CODV_{CA2IA4} \end{matrix} \right) \right)$$

$$V_{CA2} = SE_{CA2} * \left(Min\left(\begin{matrix} \frac{\alpha_{CA1CA2} V_{CA1}}{6} + \frac{\alpha_{IA1CA2} V_{IA1}}{6} + \frac{\alpha_{CA3CA2} V_{CA3}}{6} + \frac{\alpha_{IA3CA2} V_{IA3}}{6} + \frac{\alpha_{CA4CA2} V_{CA4}}{6} + \frac{\alpha_{IA4CA2} V_{IA4}}{6} + \\ 100\left(1 - \frac{\alpha_{CA1CA2} + \alpha_{IA1CA2} + \alpha_{CA3CA2} + \alpha_{IA3CA2} + \alpha_{CA4CA2} + \alpha_{IA4CA2}}{6}\right), \\ V_{CA1} + \beta_{CA1CA2}, V_{IA1} + \beta_{IA1CA2}, V_{CA3} + \beta_{CA3CA2}, V_{IA3} + \beta_{IA3CA2}, V_{CA4} + \beta_{CA4CA2}, V_{IA4} + \beta_{IA4CA2} \end{matrix} \right) \right)$$

$$V_{CA2} = 1 * \left(Min\left(\begin{matrix} \frac{0.3 * 100}{6} + \frac{0.3 * 100}{6} + \frac{0.8 * 100}{6} + \frac{0.9 * 100}{6} + \frac{0.5 * 100}{6} + \frac{0.1 * 100}{6} + \\ 100\left(1 - \frac{0.3 + 0.3 + 0.8 + 0.9 + 0.5 + 0.1}{6}\right), \\ 100 + 50, 100 + 50, 100 + 20, 100 + 10, 100 + 25, 100 + 50 \end{matrix} \right) \right)$$

$$V_{CA2} = 1 * \left(Min\left(\begin{matrix} \frac{30}{6} + \frac{30}{6} + \frac{80}{6} + \frac{90}{6} + \frac{50}{6} + \frac{10}{6} + \\ 100\left(1 - \frac{2.9}{6}\right), \\ 150, 150, 120, 110, 125, 150 \end{matrix} \right) \right)$$

$$V_{CA2} = \left(Min\left(\frac{290}{6} + 100\left(1 - \frac{2.9}{6}\right), 150, 150, 120, 110, 125, 150 \right) \right)$$

$$V_{CA2} = \left(Min\left(\frac{290}{6} + 100 - \frac{290}{6}, 150, 150, 120, 110, 125, 150 \right) \right)$$

$$V_{CA2} = \big(Min(100, 150, 150, 120, 110, 125, 150) \big)$$

$$V_{CA2} = 100\ utils$$

$$V_{IA2} = SE_{IA2} * \left(Min(Ave(SODV_{IA2IA1}, SODV_{IA2IA3}, SODV_{IA2I4}), CODV_{IA2IA1}, CODV_{IA2IA3}, CODV_{IA2IA4})\right)$$

$$V_{IA2} = SE_{IA2} * Min\left(\begin{matrix}\frac{\alpha_{IA1IA2}V_{IA1}}{3} + \frac{\alpha_{IA3IA2}V_{IA3}}{3} + \frac{\alpha_{IA4IA2}V_{IA4}}{3} + 100\left(1 - \frac{\alpha_{IA1IA2} + \alpha_{IA3IA2} + \alpha_{IA4IA2}}{3}\right), \\ V_{IA1} + \beta_{IA1IA2}, V_{IA3} + \beta_{IA3IA2}, V_{IA4} + \beta_{IA4IA2}\end{matrix}\right)$$

$$V_{IA2} = 0.72 * Min\left(\begin{matrix}\frac{0.5 * 100}{3} + \frac{0.8 * 100}{3} + \frac{1 * 100}{3} + 100\left(1 - \frac{0.5 + 0.8 + 1}{3}\right), \\ 100 + 50, 100 + 20, 100 + 0\end{matrix}\right)$$

$$V_{IA2} = 0.72 * Min\left(\frac{230}{3} + 100\left(1 - \frac{2.3}{3}\right), 150, 120, 100\right)$$

$$V_{IA2} = 0.72 * 100$$

$$V_{IA2} = 72\ utils$$

$$V_{AA2} = SE_{AA2} * \left(Min\left(\begin{matrix}Ave(SODV_{AA2AA1}, SODV_{AA2IA1}, SODV_{AA2AA3}, SODV_{AA2IA3}, SODV_{AA2AA4}, SODV_{AA2IA4}), \\ CODV_{AA2AA1}, CODV_{AA2IA1}, CODV_{AA2AA3}, CODV_{AA2IA3}, CODV_{AA2AA4}, CODV_{AA2IA4}\end{matrix}\right)\right)$$

$$V_{AA2} = SE_{Aj} * \left(Min\left(\begin{matrix}\frac{\alpha_{AA1AA2}V_{AA1}}{6} + \frac{\alpha_{IA1AA2}V_{IA1}}{6} + \frac{\alpha_{AA3AA2}V_{AA3}}{6} + \frac{\alpha_{IA3AA2}V_{IA3}}{6} + \frac{\alpha_{AA4AA2}V_{AA4}}{6} + \frac{\alpha_{IA4AA2}V_{IA4}}{6} + \\ 100\left(1 - \frac{\alpha_{AA1AA2} + \alpha_{IA1AA2} + \alpha_{AA3AA2} + \alpha_{IA3AA2} + \alpha_{AA4AA2} + \alpha_{IA4AA2}}{6}\right), \\ V_{AA1} + \beta_{AA1AA2}, V_{IA1} + \beta_{IA1AA2}, V_{AA3} + \beta_{AAAA2}, V_{IA3} + \beta_{IA3AA2}, V_{AA4} + \beta_{AA4AA2}, V_{IA4} + \beta_{IA4AA2}\end{matrix}\right)\right)$$

$$V_{AA2} = 1 * \left(Min\left(\begin{matrix}\frac{0.8 * 100}{6} + \frac{0.9 * 100}{6} + \frac{0.3 * 100}{6} + \frac{0.5 * 100}{6} + \frac{0.8 * 73}{6} + \frac{0.1 * 100}{6} + \\ 100\left(1 - \frac{0.8 + 0.9 + 0.3 + 0.5 + 0.8 + 0.1}{6}\right), \\ 100 + 10, 100 + 10, 100 + 30, 100 + 30, 73 + 20, 100 + 80\end{matrix}\right)\right)$$

$$V_{AA2} = Min\left(\frac{80}{6} + \frac{90}{6} + \frac{30}{6} + \frac{50}{6} + \frac{58.4}{6} + \frac{10}{6} + 100\left(1 - \frac{3.4}{6}\right), 110, 110, 130, 130, 153, 120\right)$$

$$V_{AA2} = Min\left(\frac{318.4}{6} + 100 - \frac{340}{6}, 110, 110, 130, 130, 93, 180\right)$$

$$V_{AA2} = Min\left(100 - \frac{21.6}{6}, 110, 110, 130, 130, 93, 180\right)$$

$$V_{AA2} = Min(96.4, 110, 110, 130, 130, 93, 180)$$

$$V_{AA2} = 93\ utils$$

$$P_{A2} = w_{CA2}V_{CA2} + w_{IA2}V_{IA2} + w_{AA2}V_{AA2}$$

$$P_{A2} = 0.10 * 100 + 0.20 * 72 + 0.70 * 93$$

$$P_{A2} = 89.5\ utils$$

Le niveau d'opérabilité global du serveur Web (A2) est de 89,5. Avec toute l'information sur A2, l'opérabilité de S1 – Hébergement Web pour les cours d'archivage – peut être calculée.

$$P_{S1} = w_{CS1}V_{CS1} + w_{IS1}V_{IS1} + w_{AS1}V_{AS1}$$

S1 dépend d'un seul nœud, A2. Les valeurs d'opérabilité de ses nœuds constitutifs sont calculées comme suit :

$$V_{CS1} = SE_{CS1} * \left(Min(Ave(SODV_{CS1CA2}, SODV_{CS1IA2}), CODV_{CS1CA2}, CODV_{CS1IA2})\right)$$

$$V_{CS1} = SE_{CS1} * \left(Min\left(\frac{\alpha_{CA2CS1}V_{CA2}}{2} + \frac{\alpha_{IA2CS1}V_{IA2}}{2} + 100\left(1 - \frac{\alpha_{CA2CS1}+\alpha_{IA2CS1}}{2}\right), V_{CA2} + \beta_{CA2CS1}, V_{IA2} + \beta_{IA2CS1}\right)\right)$$

$$V_{CS1} = 1 * \left(Min\left(\frac{1 * 100}{2} + \frac{1 * 72}{2} + 100\left(1 - \frac{1+1}{2}\right), 100 + 0{,}72 + 0\right)\right)$$

$$V_{CS1} = Min(50 + 36{,}100{,}72)$$

$$V_{CS1} = 72\ utils$$

$$V_{IS1} = SE_{IS1} * (Min(SODV_{IS1IA2}, CODV_{IS1IA2}) = SE_{IS1} * Min(\alpha_{IA2IS1}V_{IA2} + 100(1 - \alpha_{IA2IS1}), V_{IA2} + \beta_{IA2IS1}))$$

$$V_{IS1} = 1 * Min(1 * 72 + 100(1 - 1), 72 + 0)$$

$$V_{IS1} = 72\ utils$$

$$V_{AS1} = SE_{AS1} * \left(Min\left(\frac{\alpha_{AA2AS1}V_{AA2}}{2} + \frac{\alpha_{IA2AS1}V_{IA2}}{2} + 100\left(1 - \frac{\alpha_{AA2AS1}+\alpha_{IA2AS1}}{2}\right), V_{AA2} + \beta_{AA2AS1}, V_{IA2} + \beta_{IA2AS1}\right)\right)$$

$$V_{AS1} = 1 * \left(Min\left(\frac{1 * 93}{2} + \frac{1 * 72}{2} + 100\left(1 - \frac{1+1}{2}\right), 93 + 0{,}72 + 0\right)\right)$$

$$V_{AS1} = Min(46.5 + 36{,}93{,}72)$$

$$V_{AS1} = Min(82.5{,}93{,}72)$$

$$V_{AS1} = 72\ utils$$

$$P_{S1} = w_{CS1}V_{CS1} + w_{IS1}V_{IS1} + w_{AS1}V_{AS1}$$

$$P_{S1} = 0.20 * 72 + 0.30 * 72 + 0.50 * 72$$

$$P_{S1} = 72\ utils$$

S1 fonctionne avec un rendement de 72 %. Pour cet exemple, on suppose que tous les autres services dont B1 dépend sont entièrement opérationnels. Dans ce cas, la dégradation de S1 peut affecter B1. B1 est un nœud constitutif avec des composantes CID :

$$P_{B1} = w_{CB1}V_{CB1} + w_{IB1}V_{IB1} + w_{AB1}V_{AB1}$$

Les calculs sont effectués comme suit :

$$V_{CB1} = SE_{CB1} * \left(Min(Ave(SODV_{CB1CS1}, SODV_{CB1IS1}), CODV_{CB1CS1}, CODV_{CB1IS1})\right)$$

$$V_{CB1} = SE_{CB1} * \left(Min\left(\frac{\alpha_{CS1CB1}V_{CS1}}{2} + \frac{\alpha_{IS1CB1}V_{IS1}}{2} + 100\left(1 - \frac{\alpha_{CS1CB1}+\alpha_{IS1CB1}}{2}\right), V_{CS1} + \beta_{CS1CB1}, V_{IS1} + \beta_{IS1CB1}\right)\right)$$

$$V_{CB1} = 1 * \left(Min\left(\frac{0.4 * 72}{2} + \frac{0.4 * 72}{2} + 100\left(1 - \frac{0.4 + 0.4}{2}\right), 72 + 60{,}72 + 55\right)\right)$$

$$V_{CB1} = Min(28.8 + 60{,}132{,}127)$$

$$V_{CB1} = 88.8\ utils$$

$$V_{IB1} = SE_{IB1} * (Min(SODV_{IB1IS1}, CODV_{IB1IS1}) = SE_{IB1} * Min(\alpha_{IS1IB1}V_{IS1} + 100(1 - \alpha_{IS1IB1}), V_{IS1} + \beta_{IS1IB1}))$$

$$V_{IB1} = 1 * Min(0.4 * 72 + 100(1 - 0.4), 72 + 60)$$

$$V_{IB1} = Min(88.8{,}132)$$

$$V_{IB1} = 88.8\ utils$$

$$V_{AB1} = SE_{AB1} * \left(Min\left(\frac{\alpha_{AS1AB1}V_{AS1}}{2} + \frac{\alpha_{IS1AB1}V_{IS1}}{2} + 100\left(1 - \frac{\alpha_{AS1AB1}+\alpha_{IS1AB1}}{2}\right), \right.\right.$$
$$\left.\left. V_{AS1} + \beta_{AS1AB1}, V_{IS1} + \beta_{IS1AB1}\right)\right)$$

$$V_{AB1} = 1 * \left(Min\left(\frac{0.4 * 72}{2} + \frac{0.4 * 72}{2} + 100\left(1 - \frac{0.4 + 0.4}{2}\right), 72 + 60{,}72 + 55\right)\right)$$

$$V_{AB1} = Min(28.8 + 60{,}132{,}127)$$

$$V_{AB1} = 88.8\ utils$$

$$P_{B1} = w_{CB1}V_{CB1} + w_{IB1}V_{IB1} + w_{AB1}V_{AB1}$$

$$P_{B1} = 0.1 * 88.8 + 0.45 * 88.8 + 0.45 * 88.8$$

$$P_{B1} = 88.8\ utils$$

Les résultats de l'analyse de propagation de l'impact sont résumés au tableau 12. Selon les calculs, l'attaque a touché initialement A4 et A2. La dégradation de la composante de disponibilité de A4 a également affecté A2. S1 dépend directement de A2; par conséquent, son opérabilité a diminué à 72 utils. Enfin, comme S1 est un service de B1, les valeurs d'opérabilité du processus opérationnel 1 sont réduites à 88,8 utils.

Tableau 12

RÉSUMÉ DE L'ANALYSE DU GRAPHE D'IMPACT

i	V_{Ci}	V_{Ii}	V_{Ai}	w_{Ci}	w_{Ii}	w_{Ai}	P
A1	100	100	100	0.10	0.45	0.45	100
A2	100	72	93	0.10	0.20	0.70	89.5
A3	100	100	100	0.10	0.45	0.45	100
A4	100	100	73	0.35	0.35	0.30	91.9
S1	72	72	72	0.20	0.30	0.50	72
B1	88.8	88.8	88.8	0.10	0.45	0.45	88.8

L'étape suivante consiste à calculer le risque économique. Le tableau des coûts prévus est préparé d'après les renseignements de la section 8. La première colonne indique les éléments de perte. Les colonnes C, I et D sont des pertes estimées pour des processus opérationnels complètement non opérationnels. Ces valeurs peuvent être attribuées en fonction des données historiques ou de l'opinion d'experts. Certaines valeurs sont nulles puisqu'elles ne s'appliquent pas au processus opérationnel d'exécution des programmes en ligne, comme la protection des clients, les pénalités réglementaires et la perte d'information stratégique. Les cellules diagonales du tableau 13 sont des éléments de perte qui ne sont liés qu'à la perte de confidentialité. Certaines valeurs de cet exemple ont été générées de façon aléatoire dans une fourchette raisonnable pour une université. La colonne Jour de la semaine indique que l'attaque a débuté le dimanche et t_i est une valeur attribuée en fonction du premier jour de l'attaque : La valeur 3 est attribuée à la période comprise entre le lundi et le mercredi, la valeur 2 est affectée à la période allant du jeudi au samedi, et la valeur 1 est appliquée au dimanche. La durée indique le nombre de jours pendant lesquels l'attaque s'est poursuivie et d_i est attribuée en fonction de la durée.

Tableau 13

COÛT DE L'ATTAQUE

	C	I	A	Jour de la semaine	t_i	Durée (en jours)	d_i	Coût C	Coût I	Coût D	Coût total
Perte de PI	—			—	—	—	—	—	—	—	—
Perte d'info. strat.	—	—	—	—	—	—	—	—	—	—	—
Atteinte à la réputation	3 622 $	4 251 $	4 648 $	7	1	9,74	1,1	445 $	522 $	571 $	1 539 $
Augment. coût cap.	—			7	1	9,74	1,1	—	—	—	—
Amélioration de. la cybersécurité	20 000 $	30 000 $	30 000 $	7	1	9,74	1,1	2 458 $	3 687 $	3 687 $	9 832 $
Perte de données et de mat.	7 182 $	7 807 $	6 270 $	7	1	9,74	1,1	883 $	960 $	771 $	2 613 $
Perte de rev.	—	—	86 029 $	7	1	9,74	1,1	—	—	10 573 $	10 573 $
RP	2 681 $	2 923 $	3 812 $	7	1	9,74	1,1	330 $	359 $	469 $	1 157 $
Pén. régl.	—	—	—	7	1	9,74	1,1	—	—	—	—
Prot. des clients	—			7	1	9,74	1,1	—	—	—	—
Avis infract. séc.	—			7	1	9,74	1,1	—	—	—	—
Frais de règl. judiciaire	5 000 $	5 812 $	5 000 $	7	1	9,74	1,1	615 $	714 $	615 $	1 943 $
Investigation judiciaire	4 162 $	3 363 $	5 503 $	7	1	9,74	1,1	512 $	413 $	676 $	1 601 $
Total								5 241 $	6 656 $	17 362 $	**29 259 $**

Les colonnes Coût C, Coût I et Coût D indiquent la perte totale pour chaque élément de perte spécifique. Ces valeurs sont calculées en multipliant la valeur des pertes, t_i, et d_i par la dégradation de la valeur d'opérabilité de la composante CID pertinente du processus opérationnel. Les dommages d'atteinte à la réputation seront de 3 622 $ si V_{CB1} est zéro. Puisque V_{CB1} est 88,8, la valeur de l'élément de coût est 445 $. La colonne Coût total correspond à l'addition des colonnes Coût C, Coût I et Coût D pour indiquer combien chaque élément de perte spécifique coûte à l'organisation. La perte totale attendue de ce scénario d'attaque est indiquée dans la cellule inférieure droite du tableau : 29 259 $.

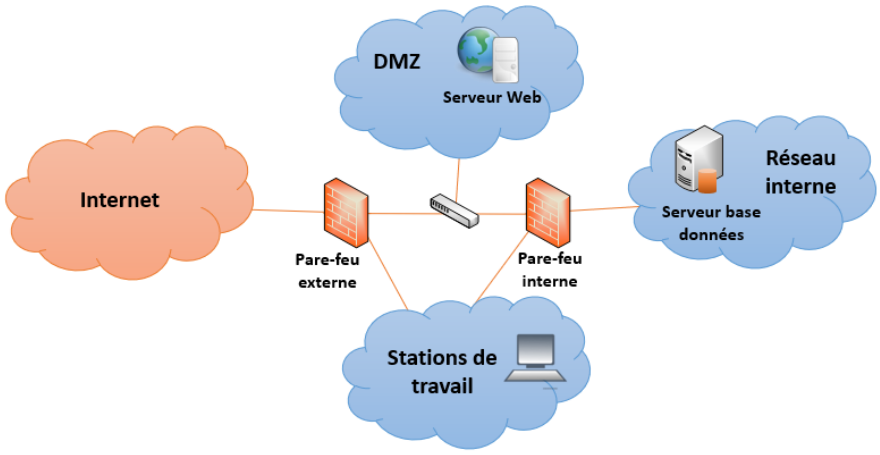
10.5 Grouper et comparer les résultats

Cet exemple montre comment le risque d'une organisation est calculé à l'aide de graphes d'attaque pour établir la vraisemblance et d'un graphe d'impact pour déterminer la propagation de l'impact. Pour simplifier l'exemple, nous analysons un graphe d'attaque ne comportant qu'un chemin d'attaque. De façon générale, compte tenu du nombre de vulnérabilités dans les composantes des TIC du réseau, il existe de multiples chemins d'attaque pour plusieurs cibles possibles. Pour comparer les effets des différentes stratégies d'attaque, les analystes des risques doivent répéter les étapes pertinentes du cadre pour calculer le risque. Même si les calculs semblent compliqués, avec des outils comme Excel, Python et MATLAB, certaines étapes peuvent être automatisées, ce qui facilite grandement le calcul de toutes les valeurs.

Section 11 : Simulation

Des simulations ont été effectuées afin de valider le cadre élaboré pour analyser les cyberrisques. Un exemple de topologie de réseau, présenté à la figure 30, a été mis à l'essai dans plusieurs scénarios de cyberattaque. Cette topologie comprend trois réseaux : la zone démilitarisée (ZD), le réseau interne et les postes de travail des utilisateurs. L'accès à la ZD est contrôlé par des pare-feu externes et internes. La ZD est utilisée pour les opérations des serveurs Web. Le serveur de base de données se trouve dans le réseau interne, derrière le pare-feu interne, il comporte des règles de pare-feu plus strictes pour le contrôle de l'accès. Le réseau des postes de travail des utilisateurs est mis à la disposition des utilisateurs réguliers.

Figure 30
TOPOLOGIE DE RÉSEAU

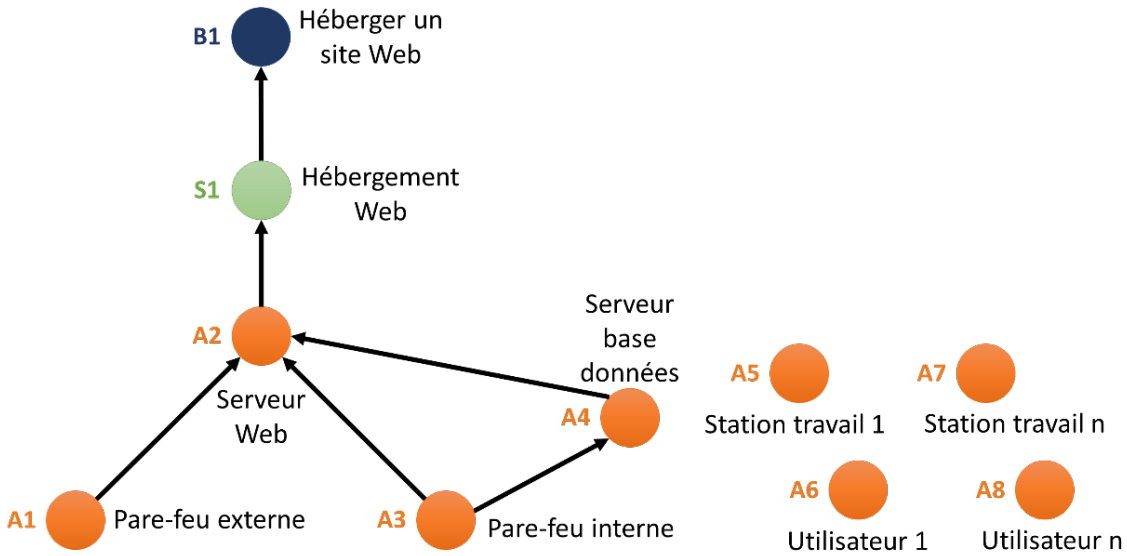


Adapté de Singhal et Ou (2011).

11.1 Produire le graphe d'impact

Par souci de simplicité et de clarté, un réseau comportant un graphe d'impact semblable à celui de la section 10 a été sélectionné pour la simulation. Les facteurs de pondération de la confidentialité, de l'intégrité et de la disponibilité, la solidité de la dépendance et la criticité des valeurs de dépendance sont les mêmes que ceux définis aux tableaux 7, 8 et 9, respectivement. Les équations de propagation de l'impact fournies à la section 10 s'appliquent également au réseau de simulation. Toutefois, certains intrants (perte d'opérabilité liée aux actifs) et extrants (valeur des pertes économiques) du graphe d'impact sont différentes, car le graphe d'attaque pour la simulation est plus complexe. Les postes de travail et les utilisateurs (A5–A8) sont également inclus dans le graphe d'impact comme des nœuds différents; toutefois, ces nœuds n'ont pas de relation de dépendance avec les autres nœuds (figure 31). Les effets de ces actifs ne sont observés que dans le graphe d'attaque.

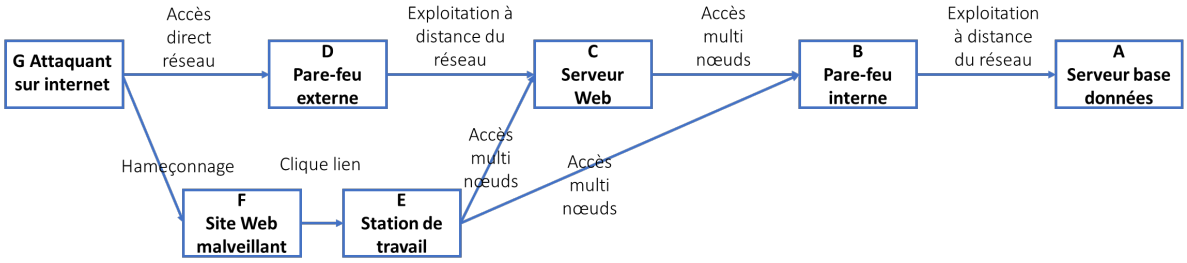
Figure 31
GRAPHE D'IMPACT POUR LA SIMULATION



11.2 Produire le graphe d'attaque

Le graphe d'attaque de ce réseau est présenté à la figure 32. Sous l'influence des postes de travail et des utilisateurs dans la topologie, le graphe d'attaque grandit et de nouveaux scénarios d'attaque (chemins d'attaque) émergent. Dans le navigateur Web d'un poste de travail, il existe une vulnérabilité qui permet à un attaquant d'utiliser un courriel d'hameçonnage; un utilisateur clique sur un lien menant à un site Web malveillant préparé par l'attaquant.

Figure 32
GRAPHE D'ATTAQUE POUR LA SIMULATION



Adapté de Singhal et Ou (2011).

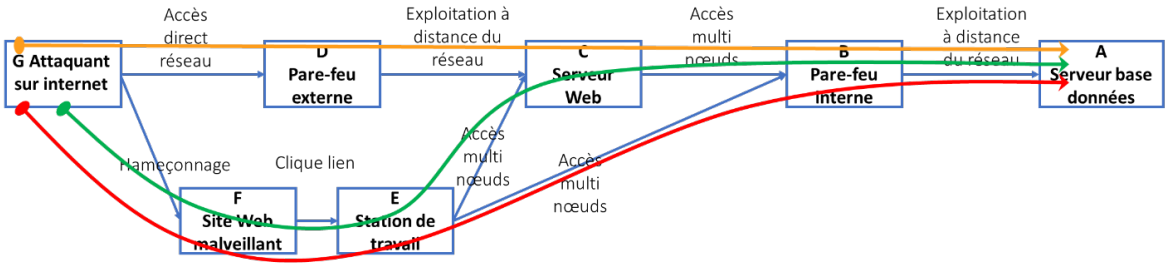
Le graphe d'attaque du réseau de simulation comprend trois chemins d'attaque, qui sont présentés à la figure 33. Voici les détails de ces trois chemins :

1. G→D→C→B→A (chemin d'attaque orange) : Ce chemin d'attaque est abordé dans l'exemple de la section 10.
2. G→F→E→C→B→A (chemin d'attaque vert) : Dans ce chemin d'attaque, l'attaquant d'Internet prépare un courriel d'hameçonnage avec un lien qui mène à du contenu malveillant si l'utilisateur du poste de travail clique sur ce lien. Une attaque d'hameçonnage comporte deux étapes : la préparation du contenu de l'hameçonnage et l'invitation menant l'utilisateur à cliquer sur le lien. Une fois le poste de travail compromis, l'attaquant utilise l'accès multibond pour atteindre le serveur Web, puis il passe par le pare-feu interne pour atteindre le serveur de base de données.

3. G→F→E→B→A (chemin d'attaque rouge) : Ce chemin d'attaque comprend également l'hameçonnage. La seule différence par rapport au deuxième chemin est que l'attaquant atteint le serveur de base de données directement à partir du poste de travail sans passer par le serveur Web.

Figure 33

GRAPHE D'ATTAQUE AVEC TROIS CHEMINS SURLIGNÉS



Ce graphe d'attaque présente trois vulnérabilités. CVE-2019-6111 et CVE-2019-18601 sont présentés à la section 10.2. La troisième vulnérabilité, CVE-2009-1918, existe sur les postes de travail. Le navigateur Internet Explorer installé sur les postes de travail qui présentent cette vulnérabilité peut permettre aux attaquants d'exécuter un code arbitraire au moyen d'un document HTML conçu pour corrompre la mémoire. Les valeurs détaillées du CVSS pour CVE-2009-1918 dans la Base de données nationale sur les vulnérabilités sont les suivantes :

Valeurs CVSS de CVE-2009-1918 sur le poste de travail

Chaîne vectorielle : AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- Vecteur d'attaque (AV:N) : Réseau
- Complexité de l'attaque (AC:L) : Faible
- Privilèges requis (RP:N) : Aucun
- Interaction utilisateur (UI:R) : Requise
- Portée (S:U) : Inchangée
- Confidentialité (C:H) : Élevée
- Intégrité (I:H) : Élevée
- Disponibilité (A:H) : Élevée

Les données numériques du tableau 14 sont déterminées d'après l'information de la BDNV et du tableau 3. La probabilité inconditionnelle est calculée comme étant 0,72 au moyen de l'équation 2.

Tableau 14

VALEURS NUMÉRIQUES DES MÉTRIQUES DE VULNÉRABILITÉ POUR CVE-2009-1918

	CVE-2009-1918	
Métrique	Valeur	Valeur numérique
Vecteur d'attaque (AV)	Réseau	0,85
Complexité de l'attaque (AC)	Faible	0,77
Privilèges requis (RP)	Aucune	0,85
Interaction avec l'utilisateur (UI)	Requise	0,62
Portée (S)	Inchangée	
Confidentialité (C)	Élevée	0
Intégrité (I)	Élevée	0
Disponibilité (A)	Élevée	0
Probabilité conditionnelle	P(F|H)	0,7243

Les chemins d'attaque multiples sont analysés pour calculer les valeurs de probabilité inconditionnelle pour chaque nœud en fonction des équations fournies par Wang et coll. (2008) et Shetty et coll. (2018). Le graphe d'attaque comporte trois chemins d'attaque, et le calcul des valeurs de probabilité inconditionnelle tient compte des trois. Les calculs des variables inconditionnelles sont les suivants :

$$P(G) = 0.5$$

$$P(F) = P(F|G) * P(G) = 0.724 * 0.50 = 0.362$$

où $P(F|G)$ est la probabilité conditionnelle liée à l'hameçonnage.

$$P(E) = P(E|F) * P(F) = 0.243 * 0.362 = 0.088$$

où $P(E|F)$ est la susceptibilité de l'utilisateur à une attaque d'intégrité (c.-à-d. la probabilité de cliquer sur le lien d'hameçonnage).

$$P(D) = P(D|G) * P(G) = 1 * 0.50 = 0.50$$

P(C) et *P(B)* sont calculés selon la logique de la OU (Wang et coll., 2008) :

$$P(C) = P(C|D) * \Big(1 - \big((1 - P(E)) * (1 - P(D))\big)\Big) = 0.55 * \Big(1 - \big((1 - 0.09) * (1 - 0.50)\big)\Big) = 0.299$$

$$P(B) = P(B|E) * \Big(1 - \big((1 - P(E)) * (1 - P(C))\big)\Big) = 1 * \Big(1 - \big((1 - 0.088) * (1 - 0.299)\big)\Big) = 0.361$$

$$P(A) = P(A|B) * P(B) = 0.993 * 0.361 = 0.358$$

Le sommaire des valeurs de probabilité inconditionnelles est présenté au tableau 15.

Tableau 15

RÉSULTATS SOMMAIRES DE L'ANALYSE DU GRAPHE D'ATTAQUE AVEC PROBABILITÉS INCONDITIONNELLES

Actif	Description	Probabilité inconditionnelle	Valeur
A5	Poste de travail	*P(E)*	0,09
A1	Pare-feu externe	*P(D)*	0,50
A2	Serveur Web	*P(C)*	0,30
A3	Pare-feu interne	*P(B)*	0,36
A4	Serveur de base de données	*P(A)*	0,36

11.3 Analyser le graphe d'impact

Cette étape porte plus précisément sur la façon dont les répercussions des cyberattaques se propagent au sein d'une entreprise et entre les couches d'une entreprise, depuis les actifs jusqu'aux processus opérationnels. A2, A4 et A5 sont des actifs touchés par une exploitation de vulnérabilité qui réduit leur rendement avec les valeurs suivantes :

$$SE_{CA5} = SE_{IA5} = SE_{AA5} = 0.91$$
$$SE_{CA2} = SE_{IA2} = SE_{AA2} = 0.70$$
$$SE_{AA4} = 0.64$$

L'analyse de propagation de l'impact est effectuée à l'aide de ces valeurs d'autoefficacité, compte tenu du réseau de dépendance fonctionnelle et de tous les paramètres fournis dans les tableaux 7, 8 et 9. Les calculs sont semblables à ceux des étapes présentées à la section 10. Les résultats de l'analyse du graphe d'impact sont présentés au tableau 16.

Tableau 16

RÉSUMÉ DE L'ANALYSE DU GRAPHE D'IMPACT DE LA SIMULATION

	VC	VI	VA	wC	wI	wA	P
A1	100	100	100	0.10	0.45	0.45	100
A2	70	70	58.8	0.10	0.20	0.70	62.2
A3	100	100	100	0.10	0.45	0.45	100
A4	100	100	64	0.35	0.35	0.30	89.2
S1	70	70	58.8	0.20	0.30	0.50	64.4
B1	88	88	85.8	0.10	0.45	0.45	87

11.4 Résultats de la simulation[1]

L'étape suivante consiste à calculer la valeur monétaire du cyberrisque. Le tableau des coûts prévus (tableau 17) est préparé conformément à l'information présentée à la section 8. La première colonne indique les éléments de perte. Les colonnes C, I et D sont des pertes estimatives pour les processus opérationnels qui ne sont absolument pas opérationnels. Ces valeurs peuvent être attribuées en fonction des données historiques C, I et D ou de l'opinion d'experts. La simulation utilise les mêmes valeurs que celles de la section 10 pour les colonnes CID, Jour de la semaine, t_i et Durée.

[1] L'ensemble de données et le modèle utilisés dans la simulation peuvent être obtenus par courriel auprès du chercheur principal du projet, le docteur Unal Tatar (utatar@albany.edu).

Les colonnes Coût C, Coût I et Coût D indiquent la perte totale pour chaque élément de perte spécifique. Ces valeurs sont calculées en multipliant la valeur des pertes, t_i, par d_i, compte tenu de la dégradation de la valeur d'opérabilité de la composante CID pertinente du processus opérationnel. Les coûts d'atteinte à la réputation s'élèveraient à 3 622 $ si V_{CB1} est zéro. Puisque V_{CB1} est 88, la valeur de l'élément de coût est de 477 $. La colonne Coût total représente la somme des colonnes Coût C, Coût I et Coût D pour indiquer le coût de chacun de ces éléments pour l'organisation. La perte totale attendue de ce scénario d'attaque est indiquée dans la cellule inférieure droite du tableau : 34 821 $.

Tableau 17

TABLEAU DU COÛT DE L'ATTAQUE POUR LA SIMULATION

	C	I	A	Jour de la semaine	t_i	Durée (en jours)	d_i	Coût C	Coût I	Coût D	Coût total
Perte de PI	—							—	—	—	—
Perte d'info. strat.	—	—	—					—	—	—	—
Atteinte à la réputation	3 622 $	4 251 $	4 648 $	7	1	9,74	1,1	477 $	560 $	726 $	1 763 $
Augment. coût cap.	—			7	1	9,74	1,1	—	—	—	—
Amélioration de la cybersécurité	20 000 $	30 000 $	30 000 $	7	1	9,74	1,1	2 634 $	3 950 $	4 688 $	11 272 $
Perte de données et de mat.	7 182 $	7 807 $	6 270 $	7	1	9,74	1,1	946 $	1 028 $	980 $	2 954 $
Perte de rev.	—	—	86 029 $	7	1	9,74	1,1	—	—	13 443 $	13 443 $
RP	2 681 $	2 923 $	3 812 $	7	1	9,74	1,1	353 $	385 $	596 $	1 334 $
Pén. régl.	—	—	—	7	1	9,74	1,1	—	—	—	—
Prot. des clients	—			7	1	9,74	1,1	—	—	—	—
Avis infract. séc.	—			7	1	9,74	1,1	—	—	—	—
Frais de règl. judiciaire	5 000 $	5 812 $	5 000 $	7	1	9,74	1,1	658 $	765 $	781 $	2 205 $
Investigation judiciaire	4 162 $	3 363 $	5 503 $	7	1	9,74	1,1	548 $	443 $	860 $	1 851 $
Total								5 616 $	7 131 $	22 074 $	34 821 $

Lorsque nous examinons les résultats de la simulation (figure 34), nous constatons que la majeure partie du coût est attribuable à la perte de revenus (13 443 $) puisque les revenus de l'organisation dépendent fortement de la disponibilité de ses données pour ses clients. Les autres éléments de coût sont liés aux composantes CID. Les coûts liés à l'amélioration de la cybersécurité suivent la perte de revenus à 11 272 $. Les coûts liés à la perte de données et de matériel, les frais de règlement judiciaire, l'investigation judiciaire, les dommages pour atteinte à la réputation et la RP sont les autres éléments qui posent un risque pour l'organisation.

Lorsque nous examinons les résultats relatifs à la perte de confidentialité, d'intégrité et de disponibilité (figure 35), nous constatons que 63 % du risque est causé par la disponibilité des services fournis par le réseau (22 074 $). Les pertes liées à la confidentialité et à l'intégrité représentent respectivement 16 % et 20 % du total des coûts. Nous pouvons également constater que la perte de revenus entraîne le plus grand risque. Elle est suivie des améliorations en matière de cybersécurité.

Figure 34

RÉSULTATS DE SIMULATIONS COMPARANT LES ÉLÉMENTS DE PERTE

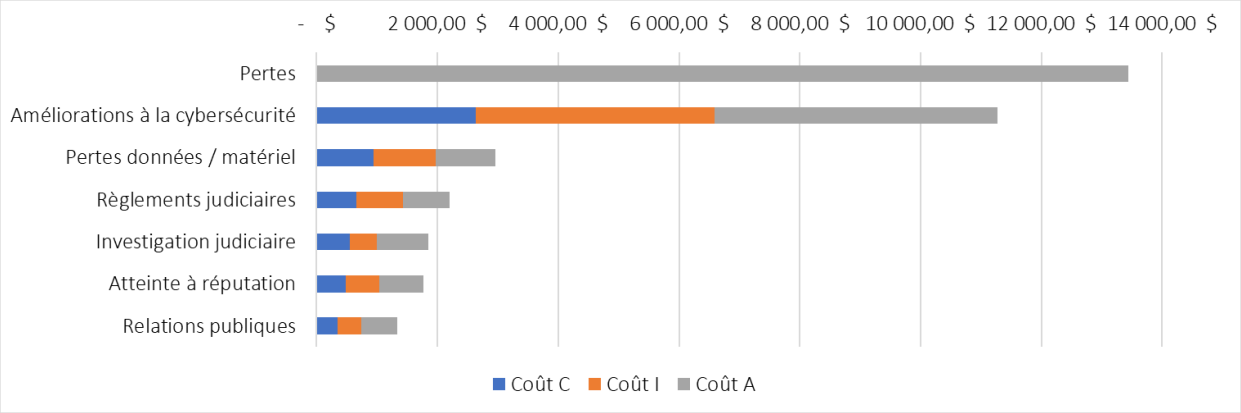
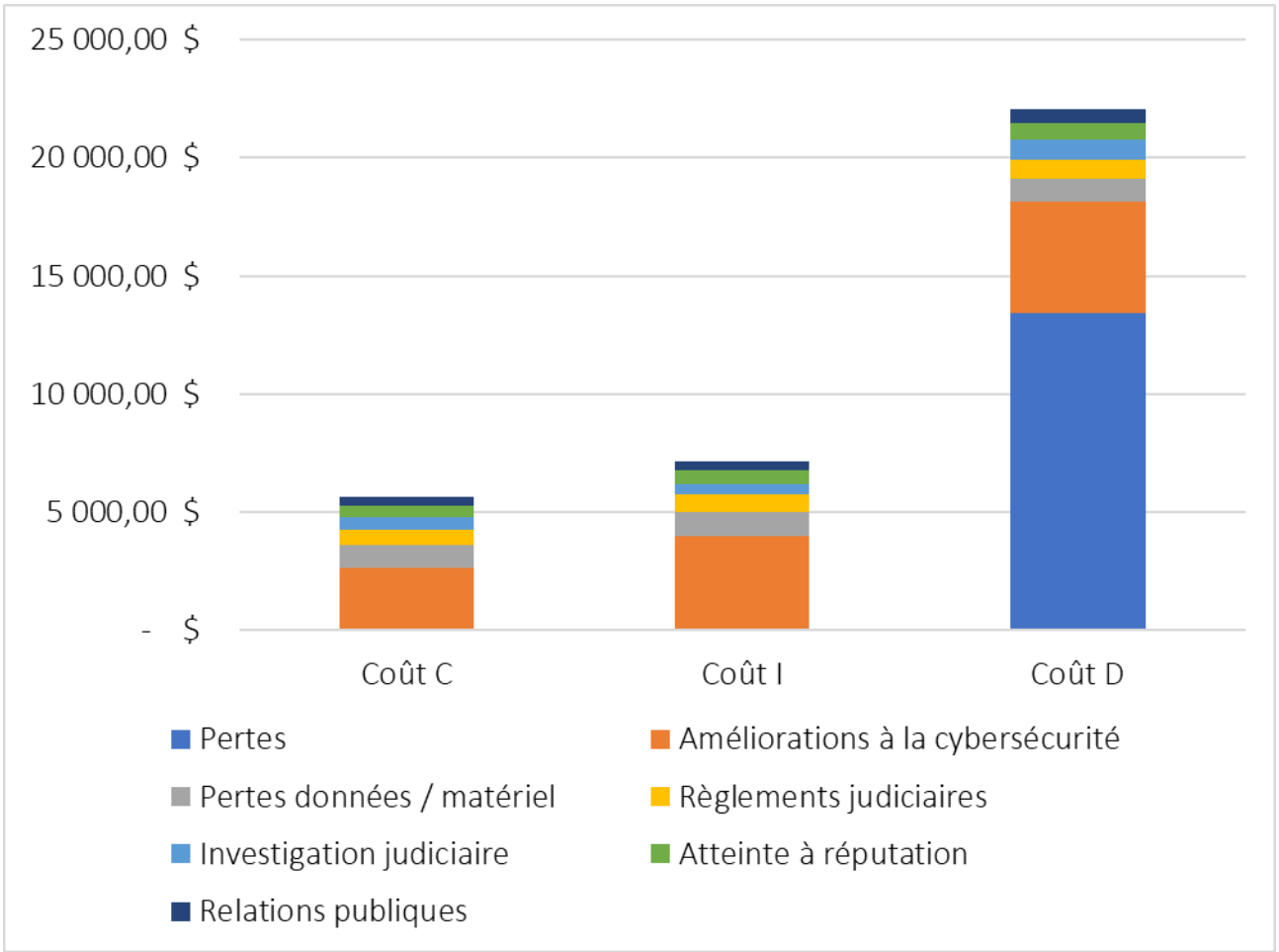


Figure 35

RÉSULTATS RELATIFS AUX IMULATIONS DE PERTE DE CONFIDENTIALITÉ, D'INTÉGRITÉ ET DE DISPONIBILITÉ



11.5 Implications des résultats relatifs aux simulations

Selon le graphe d'attaque, l'actif le plus essentiel à première vue est le serveur de base de données, puisqu'il se trouve sur tous les chemins d'attaque et que sa valeur de probabilité inconditionnelle est la plus élevée. Nous pouvons en déduire que si la vulnérabilité du serveur de base de données était éliminée en corrigeant le système, le problème serait résolu. Toutefois, compte tenu du graphe d'impact, nous constatons que les mesures de contrôle appliquées au serveur de base de données ne réduisent que légèrement le risque. De telles mesures réduiraient *P(A)* à zéro et l'efficacité de la base de données augmenterait à 1. Mais en ce qui concerne le graphe d'impact, seulement V_{CB3} augmenterait, passant de 85,8 utils à 88 utils. Cet impact est négligeable.

Toutefois, si la vulnérabilité du serveur Web était éliminée par la correction du système, *P(C)* serait ramené à zéro, tandis que *P(A)* passerait de 0,36 à 0,09. Dans ce cas, l'autoefficacité des composantes CID de A2 (serveur Web) passerait à 1, et l'autoefficacité de la disponibilité de A4 (serveur de base de données) augmenterait à 0,91. Ainsi, toutes les composantes CID de B1 augmenteraient jusqu'à 100, ce qui éliminerait tous les risques.

Un autre scénario d'atténuation consisterait à supprimer deux chemins d'attaque (deuxième et troisième) en réparant les postes de travail des utilisateurs ou en offrant au personnel de la formation sur l'hameçonnage. Ces mesures consomment probablement davantage de ressources que la simple correction du serveur de base de données; elles ne sont donc pas efficientes. Elles peuvent supprimer deux des trois chemins d'attaque; toutefois, il existe encore un autre chemin d'attaque qui cause en soi un risque important, comme le montre l'exemple de la section 10.

Lorsque l'on examine les répercussions de ces trois scénarios d'atténuation, la correction du serveur Web représente la meilleure option, car elle est la plus efficace et la plus efficiente. La troisième option, la correction des postes de travail et la formation du personnel, est efficace, mais non efficiente. La première option, la correction de la base de données, n'est ni efficace ni efficiente. Pour un petit réseau comme celui-ci, la meilleure option consiste à prendre toutes ces mesures d'atténuation. Toutefois, il convient de noter que le cadre élaboré permet de déterminer les mesures qui sont plus efficaces et les plus justifiées sur le plan du placement; dans un réseau plus vaste, il ne serait peut-être pas possible de fournir toutes les mesures de sécurité, de sorte que la priorisation deviendrait cruciale.

Section 12 : Principaux constats

Le principal objectif de toutes les organisations consiste à continuer de fonctionner. La simulation présentée à la section 11 montre que les résultats de l'analyse des risques sont très différents selon que l'on adopte le point de vue des actifs ou celui des entreprises. Les actuaires doivent évaluer le cyberrisque en tenant compte de l'impact d'une perte d'actif sur les processus opérationnels. Pour ce faire, le cyberrisque doit être intégré à la gestion du risque d'entreprise, et l'analyse des risques doit reposer sur les commentaires des experts techniques (c.-à-d. le personnel des TI) et des dirigeants d'entreprise.

La simulation présentée à la section 11 montre également que même pour un réseau à petite échelle, l'analyse portant sur le graphe d'attaque sans tenir compte du graphe d'impact ne constitue pas un moyen efficace ou efficient de réduire les cyberrisques. Pour un réseau de cette taille, la correction de tous les systèmes en fonction de toutes les vulnérabilités exploitables connues pourrait constituer une option, mais les réseaux à grande échelle, qui comprennent des centaines d'actifs, ont besoin de techniques d'atténuation des risques priorisées, efficaces et efficientes pour tenir à jour la cybersécurité du réseau. Puisque des stratégies efficaces pour prioriser les activités d'atténuation des cyberrisques sont essentielles pour les grands réseaux, les organisations peuvent utiliser le cadre élaboré à cette fin. Les actuaires peuvent aussi se servir du cadre élaboré pour évaluer la cybersécurité des organisations afin de mieux quantifier les risques.

Il est difficile d'appliquer le cadre élaboré à un réseau réel, compte tenu de la complexité de tous les détails nécessaires. Les actuaires doivent collaborer avec les gestionnaires de réseaux de TI ou les gestionnaires des risques de cybersécurité pour mener à bien toutes les étapes du cadre.

Le cadre élaboré est utile même lorsqu'il est appliqué en partie plutôt qu'en toute rigueur. Il est également possible pour les gestionnaires du cyberrisque et les actuaires de retirer certains concepts clés sans quantifier intégralement tous les éléments. Ces concepts clés sont les suivants :

- La prise en compte des composantes CID est essentielle pour les évaluations et les décisions en matière de cybersécurité. L'utilisation de ces concepts, dont il est question aux sections 6.4.2, 6.5 et 9.3, permet de prioriser plus efficacement les activités de cybersécurité en fonction du contexte opérationnel et des attentes de l'organisation. Si une entreprise se fie beaucoup plus à la confidentialité et à l'intégrité qu'à la disponibilité (p. ex., une banque par rapport à une centrale électrique), elle peut se concentrer davantage sur les systèmes qui assurent l'intégrité et la confidentialité que sur ceux qui assurent la disponibilité.
- L'évaluation des risques dans la topologie du réseau du point de vue des attaquants comporte plusieurs avantages :
    - Elle permet de démontrer qu'il existe de multiples vecteurs d'attaque et vulnérabilités cibles, et que certaines des vulnérabilités sont plus susceptibles d'être exploitées (sections 5.1, 5,2, 10.3 et 11.2).
    - Elle met en évidence des actifs spécifiques où se chevauchent la plupart des vecteurs d'attaque. La mise en évidence des principaux entonnoirs dont tous les systèmes dépendent peut aider à identifier des systèmes particuliers qui sont beaucoup plus au cœur de la cyberinfrastructure que d'autres. L'identification des composantes essentielles du réseau aide à prioriser les placements dans les mesures d'atténuation des risques de cybersécurité (sections 11.4 et 12.1).
    - La mise en évidence des principaux entonnoirs aide également à déterminer où des actifs supplémentaires pourraient être placés (p. ex., le fait que tout le trafic passe par un pare-feu dans l'exemple de simulation pourrait limiter la probabilité d'une attaque par les vecteurs rouge/vert de la section 11.2).
- La mise en correspondance de la topologie du réseau avec la perspective de l'impact sur les activités comporte également plusieurs avantages :
    - L'objectif principal des activités de cybersécurité consiste à maintenir l'organisation active sans divulguer de renseignements confidentiels ni faire l'objet de manipulations. Il est très important de connaître les actifs les plus essentiels à l'exploitation de l'entreprise afin de prioriser l'affectation des ressources (sections 6 et 8).

    - L'actif le plus essentiel pour le graphe d'attaque n'est pas toujours le plus essentiel pour la viabilité des activités de l'organisation. Pour cette raison, la propagation de l'impact doit être considérée qualitativement, même si elle n'est pas effectuée de façon quantitative (section 11.2).
- La participation des utilisateurs et l'importance de la gestion des privilèges dans la pratique de la cybersécurité sont essentielles, car la susceptibilité humaine est un facteur habilitant de la plupart des cyberattaques (sections 5.3 et 11.2).
- L'estimation des pertes à l'aide de la méthode décrite à la section 8 peut être effectuée pour déterminer laquelle parmi les composantes CID est particulièrement prioritaire pour chaque processus opérationnel. Toutefois, le cadre élaboré peut également n'être appliqué que pour quantifier le risque sans calculer les valeurs monétaires décrites à la section 8.
- L'intégration d'analyses de la propagation de l'attaque dans le cyberréseau et de la propagation de l'impact au moyen du réseau de dépendance fonctionnelle de l'entreprise permet de quantifier les cyberrisques dans une perspective globale (comme le montre la section 10).
- Il peut être difficile d'appliquer le cadre élaboré à un réseau complexe. Toutefois, même si l'application du cadre global n'est pas possible en raison d'un manque de ressources, le fait de mettre l'accent sur les deux ou trois processus opérationnels les plus importants de l'organisation et de ne tenir compte que de l'infrastructure pertinente des TI donnera une vision plus favorable du risque pour l'organisation.

Section 13 : Limites

Le cadre que nous avons élaboré suppose qu'une organisation dispose déjà d'un graphe de dépendance fonctionnelle (c.-à-d. les dépendances à l'intérieur des couches d'actifs, de services et de processus opérationnels et entre celles-ci). Il existe des méthodes automatiques ou semi-automatiques pour déterminer ces relations de dépendance, comme l'exploration des processus opérationnels et l'extraction des connaissances sur les processus des registres d'événements (Bahsi et coll., 2018), mais cela dépasse la portée de la présente recherche.

Bibliographie

Alohali, M., Clarke, N., Li, F. et S. Furnell. « Identifying and Predicting the Factors Affecting End-users' Risk-taking Behavior », *Information & Computer Security*, vol. 26, nº 3, 2018, pp. 306-226.

Artz, M. L. Netspa : *A Network Security Planning Architecture*, Thèse de maîtrise, Massachusetts Institute of Technology, 2002.

Bahşi, H., Udokwu, C.J., Tatar. U. et A. Norta. « Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review ». *ICCWS 2018 13th International Conference on Cyber Warfare and Security,* vol. 11. Sonning Common, UK : Academic Conferences and Publishing International, 2018.

Biener, C., Eling, M. et J. H. Wirfs. « Insurability of Cyber Risk: An Empirical Analysis », *The Geneva Papers on Risk and Insurance-Issues and Practice* , vol. 40, nº 1, 2015, pp. 131-158.

Bititci, U.S. et D. Muir. « Business Process Definition: A Bottom-up Approach ». *International Journal of Operations & Production Management,* vol. 17, nº 4, 1997, pp. 365-374.

Böhme, R., Laube, S. et M. Riek. « A Fundamental Approach to Cyber Risk Analysis ». *Variance* , vol 1, nº 2, 2017, pp. 161-185.

Council of Economic Advisors. *The Cost of Malicious Cyber Activity to the US Economy*. 2018.https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Federal Bureau of Investigation. *Intellectual Property Theft/Piracy*, 2017, extrait de : https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft.

FIRST.Org Inc. Common Vulnerability Scoring System Version 3.1 Specification Document Revision 1, 2019a. https://www.first.org/cvss/specification-document.

FIRST.Org Inc. Common Vulnerability Scoring System Version 3.1 User Guide Revision 1, 2019b. https://www.first.org/cvss/user-guide.

Garvey, P. R. *An Analytical Framework and Model Formulation for Measuring Risk in Engineering Enterprise Systems: A Capability Portfolio Perspective*. [thèse de doctorat, Old Dominion University] ProQuest Dissertations and Theses Global, 2009.

Garvey, P. R. et C. A. Pinto. « Introduction to Functional Dependency Network Analysis (FDNA) », volume 5 du *Second International Symposium on Engineering Systems*. MIT, Cambridge, Massachusetts, 2009.

Granadillo, G. G., Motzek, A., Garcia-Alfaro, J. et H. Debar. « Selection of Mitigation Actions Based on Financial and Operational Impact Assessments », dans le cadre de la *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 137-146. New York: IEEE.

Guariniello, C. et D. DeLaurentis. « Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks Through Interdependency Analysis ». *Procedia Computer Science* , vol. 28, 2014, pp. 720-727.

Haque, S., Keffeler, M. et T. Atkison. « An Evolutionary Approach of Attack Graphs and Attack Trees: A Survey of Attack Modeling », *Proceedings of the International Conference on Security and Management (SAM'17)*, pp. 224-229. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2017.

Ingoldsby, T. R. « Basic Attack Tree Concepts », *Attack Tree-Based Threat Risk Analysis*, Calgary (Alberta), Aastra Technologies Limited, 2010, pp. 3-9.

Jajodia, S., Noel, S. et B. O'Berry. « Topological Analysis of Network Attack Vulnerability », *Managing Cyber Threats*, Boston (MA), Springer, 2005, pp. 247-266.

Jakobson, G. « Mission Cyber Security Situation Assessment Using Impact Dependency Graphs », *14th International Conference on Information Fusion*, New York. IEEE, 2011, pp. 1-8.

Kaplan, S. et B. J. Garrick. « On the Quantitative Definition of Risk », *Risk Analysis*, vol. 1, nº 1, 1981, pp 11-27.

Keeney, R. L. et H. Raiffa. *Decisions with Multiple Objectives Preferences and Value Tradeoffs*, New York, John Wiley & Sons, 1976.

Kenton, W. « Cost of Capital Definition », *Investopedia*, 2018 https://www.investopedia.com/terms/c/costofcapital.asp.

Kirchsteiger, C. « On the Use of Probabilistic and Deterministic Methods in Risk Analysis », *Journal of Loss Prevention in the Process Industries*, vol 12, nº 5, 1999, pp. 399-419.

Lei, J. « Cyber Situational Awareness and Mission-centric Resilient Cyber Defense », *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, vol. 1, New York, IEEE, 2015, pp 1218-1225.

Llansó, T. et E. Klatt. « CyMRisk: An Approach for Computing Mission Risk Due to Cyber Attacks », *2014 IEEE International Systems Conference Proceedings*, New York, IEEE, 2014, pp 1-7.

Mell, P., K. Scarfone, K. et S. Romanosky. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*, 2007. https://www.first.org/cvss/v2/cvss-v2-guide.pdf.

McCallister, E., Grance, T. et K.A. Scarfone. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. NIST SP 800-122. Gaithersburg, MD: National Institute of Standards and Technology, 2010. https://csrc.nist.gov/publications/detail/sp/800-122/final.

Moore, T., Dynes, S. et F. R. Chang. *Identifying How Firms Manage Cybersecurity Investment*, 2015, p. 32. https://cpb-us-w2.wpmucdn.com/blog.smu.edu/dist/e/97/files/2015/10/SMU-IBM.pdf.

National Science and Technology Council. « Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program », 2011. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

National Vulnerability Database. « CVE-2009-1918 Detail. » https://nvd.nist.gov/vuln/detail/CVE-2009-1918, 2019a.

National Vulnerability Database. « CVE-2019-6111 Détail » https://nvd.nist.gov/vuln/detail/CVE-2019-6111, 2019b.

National Vulnerability Database. « CVE-2019-10098 Detail » https://nvd.nist.gov/vuln/detail/CVE-2019-10098, 2019c.

National Vulnerability Database. « CVE-2019-18601 Detail. » https://nvd.nist.gov/vuln/detail/CVE-2019-18601, 2019d.

Nessus. n.d. [logiciel] Tenable Inc. https://www.tenable.com/products/nessus.

NetDiligence. « Cyber Claims Study. », 2016 https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf.

NetDiligence. « Cyber Claims Study. », 2018 https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf.

Nicol, D. M. et V. Mallapura. « Modeling and Analysis of Stepping Stone Attacks », *Proceedings of the 2014 Winter Simulation Conference*, New York, IEEE, 2014, pp. 3036-3047. http://publish.illinois.edu/science-of-security-lablet/files/2014/06/Modeling-and-Anaylysis-of-Stepping-Stone-Attacks.pdf.

Ou, X., Govindavajhala, S. et A. W. Appel. « MulVAL: A Logic-based Network Security Analyzer », *USENIX Security Symposium* nº 8, 2005, pp. 113-128.

Poolsappasit, N., Dewri, R. et I. Ray. « Dynamic Security Risk Management Using Bayesian Attack Graphs », *IEEE Transactions on Dependable and Secure Computing*, vol. 9, nº 1, 2012, pp 61-74.

Ross, R., McEvilley, M. et J. C. Oren. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* NIST SP, 800-160. Gaithersburg, MD: National Institute of Standards and Technology, 2016 .https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

Schneier, B. « Attack Trees. » *Schneier on Security*. Arbres d'attaque, 1999. https://www.schneier.com/academic/archives/1999/12/attack_trees.html,.

Shameli-Sendi, A., Aghababaei-Barzegar, R. et M. Cheriet. « Taxonomy of Information Security Risk Assessment (ISRA) », *Computers & Security*, 2016, n° 57, pp. 14-30.

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K. et L. L. Njilla. « Reducing Informational Disadvantages to Improve Cyber Risk Management », *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 43, n° 2, 2018, pp. 224-238.

Singhal, A. et X. Ou. *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs*. NIST Interagency Report 7788. Gaithersburg, MD: National Institute of Standards and Technology, 2011.

Stoneburner, G. *Underlying Technical Models for Information Technology Security-Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-33. Gaithersburg, MD: National Institute of Standards and Technology, 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-33.pdf.

Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J. et J. McCarthy. *Cybersecurity Framework Manufacturing Profile*. NIST Internal or Interagency Report (NISTIR) 8183. Gaithersburg, MD: National Institute of Standards and Technology, 2019.

Swiler, L. P., Phillips, C. et T. Gaylor. *A Graph-based Network-Vulnerability Analysis System*. No. SAND-97-3010/1. Albuquerque, NM: Sandia National Labs, 1998.

Tatar, U. A Multilayer Propagative Approach. [thèse de doctorat, Old Dominion University] ProQuest Dissertations and Theses Global, 2019.

Département américain de la sécurité intérieure. « U.S. Department of Homeland Security Cybersecurity Strategy » https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, 2018.

Verizon. *2017 Data Breach Investigations Report.* 10th ed., 2017 https://enterprise.verizon.com/resources/reports/2017_dbir.pdf,

Wang, L., Islam, T., Long, T., Singhal, A. et S. Jajodia. « An Attack Graph-based Probabilistic Security Metric, dans *IFIP Annual Conference on Data and Applications Security and Privacy*, 2008, pp. 283 296. Berlin: Springer

À propos de la Society of Actuaries

Constituée en 1949, la Society of Actuaries (SOA) est l'un des plus importants organismes professionnels au monde voué au service de 31 000 actuaires membres et du public aux États-Unis, au Canada et ailleurs dans le monde. Conformément à l'énoncé de vision de la SOA, les actuaires sont des chefs de file auprès des entreprises dans l'élaboration et l'utilisation des modèles mathématiques pour mesurer et gérer le risque à l'appui de la sécurité financière des particuliers, des organisations et du grand public.

La SOA appuie les actuaires et fait progresser la connaissance au moyen de la recherche et de l'éducation. Dans le cadre de ses travaux, elle cherche à éclairer l'élaboration de la politique publique et à faciliter sa compréhension par le grand public par le biais de la recherche. Elle aspire à devenir une source de confiance en recherche et en analyse objective fondée sur des données, dans une perspective actuarielle pour ses membres, l'industrie, les décideurs et le public. Ce point de vue distinct provient de la SOA à titre d'association d'actuaires qui possèdent une formation formelle rigoureuse et une expérience directe de praticiens en recherche appliquée. La SOA est également fière de la possibilité de s'associer à d'autres organisations dans le cadre de ses travaux, le cas échéant.

La SOA collabore depuis longtemps avec les décideurs du secteur public et les organismes de réglementation pour la préparation d'études d'expérience historiques et l'élaboration de techniques de projection, de même que des rapports individuels sur les soins de santé, la retraite et d'autres sujets. Les travaux de recherche de la SOA ont pour but de faciliter les travaux des décideurs et des organismes de réglementation, et de suivre certains principes fondamentaux :

Objectivité : Les travaux de recherche de la SOA fournissent un éclairage et une analyse auxquels peuvent se fier d'autres personnes et organisations prenant part aux débats sur la politique publique. La SOA ne prend pas position ou n'appuie pas des projets de politique particuliers.

Qualité : Dans tous ses travaux et toutes ses analyses, la SOA vise les plus hautes normes de qualité et d'éthique. Notre processus de recherche est supervisé par des actuaires et des non-actuaires expérimentés représentant de nombreux secteurs et organismes professionnels. Un examen rigoureux par les pairs garantit la qualité et l'intégrité de nos travaux.

Pertinence : La SOA fournit des travaux de recherche opportuns sur des sujets relevant de la politique publique. Ces travaux font progresser la connaissance actuarielle tout en présentant une perspective critique sur des questions stratégiques fondamentales, ajoutant ainsi à la valeur des travaux des intervenants et des décideurs.

Quantification : La SOA met à profit les compétences diverses des actuaires afin de produire des travaux de recherche et des constatations fondés sur les meilleures données et les meilleures méthodes. Les actuaires utilisent des modèles détaillés pour analyser le risque financier et fournir une perspective et une quantification distinctes. En outre, les normes actuarielles exigent de la transparence, et la divulgation des hypothèses et de la démarche d'analyse qui sous-tendent les travaux.

Society of Actuaries
475 N. Martingale Road, bureau 600
Schaumburg
Illinois 60173
www.SOA.org

À propos de l'Institut canadien des actuaires

L'Institut canadien des actuaires (ICA) est l'organisme bilingue national et le porte-parole de la profession actuarielle au Canada. Ses membres rendent des services et des conseils actuariels de la plus haute qualité. L'Institut fait passer l'intérêt public avant les besoins de la profession et ceux de ses membres.

Vision

La sécurité financière des Canadiens.

Mission

À titre de porte-parole bilingues de la profession actuarielle au Canada, nous assurons le progrès de la science actuarielle et de ses applications au profit du bien-être de la société.

Valeurs

Les valeurs façonnent notre attitude et influencent notre éthique professionnelle. Nos valeurs sont :

Intégrité

Nous sommes des professionnels honnêtes et responsables; nous veillons au respect de principes éthiques stricts. Nous recourons à notre expertise, à nos normes rigoureuses et à notre objectivité pour assurer la prestation de conseils et de services actuariels de la plus haute qualité.

Communauté

Nous faisons passer l'intérêt public avant nos propres intérêts. Nos processus sont transparents et le bénévolat se situe au cœur de nos activités.

Avancement

Nous sommes engagés à prouver la valeur de la gestion efficace du risque. Nous recourons à l'innovation pour assurer le progrès de la science actuarielle et de ses applications.

Institut canadien des actuaires
360, rue Albert, bureau 1740
Ottawa (Ontario) KIR 7X7
www.cia-ica.ca