**الجــمـهـوريـة الـجــزائـرية الـديمـقـراطـية الشــعـبـيـة**

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE LA NUMERISATION ET DES STATISTIQUES



**Annexe 1 :**

**Fiche technique sur la Matrice des Risques et Attaques Informatiques**

**Introduction :**

De nos jours, les attaques informatiques ont devenu de plus en plus sophistiquées. On parle souvent de nouveaux concepts sur des attaques tels que les ransomware, attaques contre les algorithmes d’apprentissage…etc. les attaquants ne cessent de développer de nouvelles techniques ce qui a conduit le monde a une guerre purement électronique dans le monde virtuel dont l’information est considérée comme le nouveau pétrole. Plusieurs pays dans le monde ont déjà commencé à élaborer des matrice d’attaques permettant de localiser et énumérer les possibles risques pouvant toucher surtout l’économie, la sécurité et la politique du pays.

Parlant de nouvelles attaques, l’Algérie n’est pas une exception. En effet, ces derniers temps, l’Algérie connaît une transformation digitale de ses services gouvernementaux et administratifs. Cette transformation qui rend l’information personnelle du citoyen algérien précieuse et rend l’Algérie une cible de plus en plus des nouvelles attaques. Ce document résume les concepts liés au risque et attaque informatique.

**Concepts et définitions :**

1. **Risque informatique :**

Le risque en informatique représente la possibilité d’exploitation des menaces et vulnérabilités existantes dans un système d’information afin de produire un impact inattendu. Le risque informatique peut être désigné comme le risque métier associé à l'utilisation, la possession, l'exploitation, l'implication, l'influence et l'adoption de l'informatique dans une organisation.

1. **Attaque informatique :**

Une attaque (dite aussi intrusion) peut être définie comme tout ensemble d'actions qui essayent d’exploiter une ou plusieurs failles du système d’information à travers une ou plusieurs menaces détectées afin de compromettre sa sécurité.

1. **Matrice des risques :**

Une matrice des risques est essentiellement un moyen permettant de comprendre les risques auxquels un système d’information est confronté ; dans notre cas, on parle des plateformes numériques et leurs infrastructures. Chaque ligne de la matrice indique un scénario possible d’une attaque. L’analyse des matrices des risques permet d’éviter ces scénarios en considérant des actions préventives.

La matrice des risques peut être local correspondante à un système d’information particulier à l’image d’une plateforme numérique ou un Datacenter d’une organisation ; comme elle peut être plus générale décrivant des scénarios plus ou moins communs à l’image des ressources mutualisées et transversales.

**Des exemples des matrices :**

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est en grande base de connaissances de techniques accusatoires - une ventilation et une classification des actions à caractère offensif qui peuvent être utilisées contre des plates-formes particulières, telles que Windows. Contrairement aux travaux antérieurs dans ce domaine, l'accent n'est pas mis sur les outils et les logiciels malveillants utilisés par les adversaires, mais sur la façon dont ils interagissent avec les systèmes au cours d'une opération. Ces actions sont divisées en deux grandes parties : techniques et tactiques

**Les tactiques** représentent le « pourquoi » d'une technique ATT&CK. La tactique est l'objectif tactique de l'adversaire pour effectuer une action. Les tactiques servent de catégories contextuelles utiles pour les techniques individuelles et couvrent les notations standard de niveau supérieur pour les choses que les adversaires font pendant une opération, telles que persister, découvrir des informations, se déplacer latéralement, exécuter des fichiers et exfiltrer des données.

**Les techniques** représentent « comment » un adversaire atteint un objectif tactique en effectuant une action. Par exemple, un adversaire peut vider des informations d'identification pour accéder à des informations d'identification utiles au sein d'un réseau qui peuvent être utilisées ultérieurement pour un mouvement latéral. Les techniques peuvent également représenter « ce que » un adversaire gagne en effectuant une action. Il s'agit d'une distinction utile pour la tactique de découverte, car les techniques mettent en évidence le type d'informations qu'un adversaire recherche pour une action particulière. Il peut y avoir plusieurs façons, ou techniques, d'atteindre des objectifs tactiques, il y a donc plusieurs techniques dans chaque catégorie tactique.

La relation entre les tactiques et les techniques est visualisée dans la matrice ATT&CK publiée en 2013 est mise à jour régulièrement selon l’avancement de la technologie de l’information. La figure suivante montre la matrice ATT&CK



**Figure 1 :** matrice ATT&CK

Parmi les projets récents dans ce sens, un projet qui a été lancé par l’agence Américaine MITRE – responsable de la matrice ATT&CK – en collaboration avec Microsoft, IBM, NVIDIA et BOSCH dont l’objectif est de créer une matrice contre les attaques visant les vulnérabilités des algorithmes d’apprentissage du domaine de l’intelligence artificielle occupant lui-même une place importante ces dernières années dans digitalisation des procédures[[1]](#footnote-1). La figure suivante présente une partie de ladite matrice.



**Figure 2 :** Matrice des menaces accusatoires des algorithmes d’apprentissage

**Une matrice en Algérie ?**

En Algérie, il est remarqué, malheureusement, une absence d’une matrice générale décrivant les risques et attaques communs. C’est pour cela que dans le cadre des actions du MNS inscrites dans le plan d’action gouvernemental notamment le renforcement de la sécurité de l’information, il est nécessaire de définir un tel projet qui rentre dans le cadre des missions de la sous-direction de cybersécurité définies dans le décret n° 20-364 notamment la mission concernant l’élaboration et maintient à jour la cartographie des risques et menaces informatiques.

Ce projet consiste principalement de réunir les parties prenantes afin de créer une cellule permanente. Cette dernière aura le rôle d’élaborer, de publier et de tenir à jour une matrice nationale des risques et attaques informatiques en Algérie. Les objectifs principaux de ce projet sont :

* Etablir une matrice unique informationnelle des différents risques informatiques pouvant toucher la sureté du citoyen numérique.
* Construire une base de connaissance aux chercheurs Algériens permettant de bénéficier des avantages de la recherche scientifique.
* Garantir le maintient à l’actualité des risques et attaques informatiques vis-à-vis le développement numérique en Algérie

1. <https://thehackernews.com/2020/10/adversarial-ml-threat-matrix.html> [↑](#footnote-ref-1)