



FACULTÉ DE GÉNIE

Sécurité Cloud - Détournement de services et de compte

<i>Auteur</i>	<i>Email</i>	<i>Id</i>
Diab Khanafer	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED

Présenté à :
REDACTED

12 décembre 2023

1 Abstract

L'infonuagique représente un domaine actuellement en grande expansion qui comprend beaucoup d'enjeux surtout au niveau de la sécurité. En effet, de nombreuses compagnies utilisent l'infonuagique comme outil pour entreposer leur donnée. Or plusieurs de ces données comprennent des informations sensibles ou importantes qui nécessite d'être gardé loin d'utilisateurs malveillant. Or cet environnement reste à risque d'attaques comme des attaques de détournement de services et de comptes. Ainsi dans cet article, nous cherchons à déterminer si les recommandations AWS en matière de sécurité peuvent fournir un certain niveau de protection de base contre des attaques de détournement de services et de comptes commune. Ainsi nous avons réalisé six attaques de détournement de services et de comptes sur deux environnements AWS soit un non conforme et un conforme afin de comparer l'impact de ses attaques sur chacun d'eux. Pour l'environnement non conforme, il a été possible de réaliser les six attaques sans difficulté tandis que pour l'environnement conformes aucune des six attaques n'a fonctionné. Ceci démontre que les recommandations AWS offrent réellement une bonne base pour créer un environnement infonuagique sécuritaire et l'importance de suivre ces recommandations.

2 Introduction

2.1 Arrière-plan

L'infonuagique est un domaine qui est actuellement en grande expansion. En effet, il représente pour plusieurs secteurs une occasion pour de nouvelle opportunité ou bien simplement un moyen d'améliorer leur efficacité. Un des avantages principaux de l'infonuagique est au niveau financier. Cet avantage se traduit par la possibilité d'éliminer les coûts importants reliés à l'acquisition et la maintenance d'un réseau interne ("capital expenditures") en une stratégie de "pay-as-you-go/use" ("operating costs") [21]. Cela permet non seulement de sauver des coûts, mais aussi de diminuer les risques inhérents à l'entretien d'une infrastructure complexe.

Or malgré les nombreux avantages que procure l'infonuagique, il ne faut pas oublier les enjeux et implications au niveau de la sécurité. Un des grands enjeux est au niveau des données [10]. En effet, plusieurs compagnies entreposent et traitent une grande quantité de données sensibles sur le nuage. De ce fait, ils ont l'obligation de protéger l'accès de ses données et de se conformer à différentes législations sur la manière dont celle-ci est entreposée.

Un autre enjeu important est que les compagnies ne doivent pas seulement s'assurer d'éviter des attaquants malveillants d'accéder à ces données, mais ils doivent également s'assurer de protéger l'intégrité de ces données. En effet, pour une compagnie, la modification de leurs données par un individu non autorisé peu engendré des problèmes majeurs. Finalement, le dernier enjeu est qu'il est important pour les compagnies de se protéger contre les attaques qui pourraient nuire à la disponibilité des données. En infonuagique, il est important que les

données qui y sont entreposées soient toujours disponibles pour être capables de répondre à la demande des utilisateurs.

2.2 Énoncé du problème

L'objectif de ce projet est d'étudier et de déterminer l'impact du détournement de services et de comptes sur un environnement infonuagique AWS. Pour ce faire, nous réaliserons différentes attaques communes sur un environnement qui sera basé sur les meilleures pratiques et recommandations de AWS. Ultimement, cette expérimentation nous permettra de déterminer si ces recommandations permettent d'offrir un niveau de protection adéquat à une infrastructure AWS.

2.3 Planification des mesures de sécurité du cloud

Le détournement de services et de comptes est un enjeu de sécurité important dans le domaine de l'infonuagique. Ainsi il est primordial pour les compagnies de mettre en place des mesures de sécurité robustes qui permettront de prévenir ce type d'attaque.

Afin de s'assurer d'un niveau de sécurité optimal, il est important qu'une compagnie ait un plan complet. Ainsi, il faut tout d'abord s'assurer d'une protection minimale de base que ce soit en optant d'ajouter l'authentification multi-facteur, de mettre en place des politiques IAM strictes pour contrôler l'accès aux ressources ou bien en s'assurant de chiffrer les données sensibles. Toutefois, un plan de sécurité ne s'arrête pas simplement à la mise en place de mesure préventive. Il est important de faire une surveillance continue des ressources afin de détecter en temps réel des anomalies et d'analyser ceux-ci afin de pouvoir réagir face aux attaques et corriger les vulnérabilités détectées. Par la suite, il est important de faire des formations pour sensibiliser les employé et utilisateur des risques de sécurité présents sur le nuage. Finalement, il est important de mettre un plan d'intervention clair et détaillé en cas d'incident. En effet, la mise en place de ce plan permettra aux équipes de réagir plus rapidement en cas d'attaques et permettra ainsi d'éviter plus de dommage.

2.4 Porté du projet

Le projet commencera par la mise en place de deux environnements AWS à l'aide de Terraform. Le premier environnement sera non conforme aux recommandations de l'état de l'art, alors que le deuxième suivra les recommandations de AWS en date de décembre 2023. Puis, un recensement des attaques les plus communes liées au détournement de services et de comptes sera effectué afin de simuler ses attaques sur nos deux environnements. Finalement, une évaluation des impacts des attaques sur l'intégrité des deux environnements et de la suffisance des recommandations de l'état de l'art sera effectuée. Dû à l'expérience de l'équipe, les outils fournissent et le temps alloué, seulement des attaques de base commune seront réalisées. Le code source du projet en entié se trouve à l'url disponible dans la référence [2] ou à l'url *ici*.

3 Travaux connexes

3.1 Revue des articles

Le domaine de la cybersécurité dans l'infonuagique est un domaine large sur lequel plusieurs chercheurs se sont déjà penchés. Dans la littérature, il existe des articles tels que celui de Patrick Mosca et al. [17] qui aborde les différents risques communs et les mesures préventives contre de tels types d'attaque. On retrouve aussi d'autre article plus général comme celui de Michael Soltys [19]. Cet article examine le contenu d'un cours de cybersécurité avancé permettant d'aborder les concepts clés de la cybersécurité en fonction des services de AWS.

Or le sujet de ce projet se concentre sur un sous-domaine de la cybersécurité dans l'infonuagique, soit le détournement de services et de comptes. Il existe plusieurs articles qui abordent le sujet de la gestion d'identité. On retrouve un article par Eghbal Ghazizadeh et Brian Cusack [9] qui aborde l'efficacité de la méthode Delphi pour identifier des risques de sécurité et de confidentialité potentiels. Les mêmes auteurs ont également publié un article analysant les forces et la faiblesse des méthodes actuelles de gestion d'identité [12]. On retrouve également des articles identifiant les différentes vulnérabilités existant dans les processus d'authentification tel que l'article de Oleksandr Oksiuk et Vladyslava Chaikovska [18].

Toutefois, la gestion d'identité reste un domaine avec beaucoup d'ampleur. Il est ainsi possible de trouver de nombreux articles sur un sous-domaine tel que l'authentification multi-facteur. En effet, on retrouve des articles comme celui de Das, Wand et Camp [11] sur la perception des gens face à l'authentification multi-facteur et l'impact que ceci a sur ce type de solution. Aussi on retrouve des papiers sur des alternatives à l'authentification multi-facteur tel que celui par AnaKath, Rajakumar et Ambika [7].

3.2 Informations obtenues

Grâce aux articles identifiés ci-dessus, il a été possible d'identifier les vulnérabilités et les attaques les plus communes et les stratégies de l'état de l'art pour les contrer. Ses informations nous permettront d'informer le "setup" de notre infrastructure et de notre expérimentation. En termes des vulnérabilités les plus communes, celle-ci est donnée ci-dessous :

- Mauvaise configuration
- Pas d'application du "Least-Privilege"
- Manque de "training" et d'expertise
- Pas de surveillance
- Pas de MFA
- Audit inadéquat

La vulnérabilité principale semble être une mauvaise configuration des ressources. Une mauvaise configuration en termes de la gestion d'identités ou de services ne serait pas de "multi-factor authentication" (identification par plusieurs facteurs, ex. : mot de passe sur

l'ordinateur et validation sur le cellulaire), pas d'application du "Least-Privilege" (utilisateur/rôles ont plus d'accès que nécessaire) ou pas de surveillance de l'infrastructure avec CloudTrail, CloudWatch, etc. Au-delà de la configuration des ressources, une des vulnérabilités principales reste l'ingénierie sociale et l'utilisateur humain. En effet, il est important de toujours avoir des utilisateurs entraînés, prudent et averti afin de diminuer les risques de mauvaise configuration ou de "phishing". Finalement, une analyse non existante ou non régulière des ressources et de leur configuration à l'interne ou par un tiers parti autorisé vient aussi contribuer à l'apparition de différente vulnérabilité.

Pour ce qui est des attaques les plus communes, celles-ci sont données ci-dessous :

- Brute-force
- Phishing
- Elevation of Privilege
- Man-in-the-middle
- Data Tampering

Plusieurs techniques peuvent être utilisées pour obtenir les informations d'identifications d'un utilisateur. Le brute-force revient à essayer de pénétrer un environnement en essayant de deviner le bon mot de passe ou équivalents (attaque de dictionnaire, etc.). L'hameçonnage est une stratégie d'ingénierie sociale ou un utilisateur est redirigé vers un environnement "fake" à l'aide d'un courriel ou autre. Man in the middle est lorsqu'un pirate informatique est capable de s'insérer et de voler des informations dans la communication entre deux parties. Finalement, le "data tampering" revient à essayer de manipuler l'information sur l'identité d'un utilisateur dans la base de données du fournisseur d'identité pour le service infonuagique. Une fois qu'un attaquant a obtenu l'accès à un compte, celui-ci peut utiliser l'élévation du privilège afin d'essayer d'escalader le privilège d'un utilisateur pour avoir le plus d'accès et faire le plus de dommage ou de vols possible.

Comme il est possible de voir, la littérature sur le domaine de la cybersécurité et du détournement de services et de compte est très abondante. Toutefois, il reste encore de l'espace pour d'autres projets dans le domaine. En ce qui a attrait à notre projet aucun papier que nous avons pu trouver exécute la même expérimentation que nous.

4 Méthodologie

4.1 Services et composants AWS

Voici la liste et une explication rapides de chacun des services AWS que nous utiliserons dans notre méthodologie :

- AWS EC2 : un service web qui fournit une capacité de calcul redimensionnable dans le nuage. Il permet de créer des serveurs virtuels, appelés "instances", avec une variété de caractéristiques différentes et systèmes d'exploitation. Les instances peuvent être customisées pour répondre à des besoins spécifiques en matière de calcul, de mémoire, de stockage, et de fonctions.
- AWS S3 : un service de stockage qui permet de stocker et de récupérer des objets et des données, que ce soit des documents, des images, des vidéos ou voir des sauvegardes. Il est conçu pour l'évolutivité, la durabilité et un accès aux données à faible latence.
- AWS VPC : un service de création et mise en réseau qui vous permet de créer des réseaux virtuels isolés dans le nuage AWS. Il permet de définir des plages d'adresses IP, créer des sous-réseaux et configurer les paramètres de routage et de sécurité du réseau privé entier.
- AWS Cloudwatch : un service de surveillance qui collecte et suit les métriques, les journaux et les événements des ressources. Il fournit des informations sur les performances, la santé et l'état opérationnels de vos applications et de votre infrastructure. Le service permet aussi la création d'alarmes et des actions basées sur le lancement de ces alarmes pour de l'automatisation.
- AWS CloudTrail : un service qui enregistre les appels et événements d'API pour les comptes AWS. Il fournit un historique des modifications et des interactions avec les services et ressources AWS, contribuant ainsi à la sécurité, à la conformité et au dépannage.
- AWS IAM : un service qui vous permet de gérer l'accès aux services et ressources AWS en toute sécurité. Il vous permet la création et la gestion des utilisateurs, des groupes et des rôles pour accorder ou refuser des autorisations sur les ressources AWS.
- AWS Lambda : un service de calcul sans serveur qui vous permet d'exécuter du code en réponse à des événements sans provisionner ni gérer de serveurs. Il s'agit d'une excellente solution pour créer des applications évolutives et basées sur des événements.

4.2 Configuration de l'infrastructure

Pour notre analyse, nous utilisons deux infrastructures assez similaires pour effectuer nos expérimentations. Les deux sont appliqués en utilisant les configurations Terraform construites à cet effet, et contiennent les services suivants représentés sur la figure 1 :

- deux "buckets" AWS S3, un étant publique et hébergeant un site web static, et l'autre privé contenant de l'information sensible.
- un seul utilisateur AWS IAM
- une instance AWS EC2

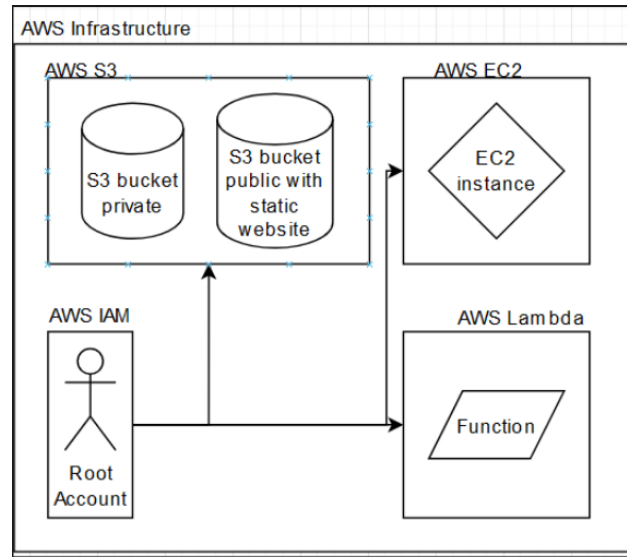


FIGURE 1 – Schéma d'infrastructure

— une fonction AWS Lambda

Cependant, les deux infrastructures contiennent certaines différences concernant leurs configurations. La première est celle que l'on considérera "faible" et n'applique aucun des "best practices" de AWS. La deuxième, quant à elle, les applique. C'est pour cela que, au courant de l'article, nous ferons référence à la première infrastructure comme étant l'infrastructure faible, et la deuxième comme étant l'infrastructure forte.

4.3 Surveillance et journalisation

En termes de surveillance et journalisation, le service CloudWatch offre des capacités de surveillance robustes pour divers services tels que EC2, S3, IAM et Lambda, qui sont les services que nous utilisons pour ce projet. Ce service permet de suivre des métriques telles que l'utilisation du processeur, l'utilisation du stockage et les exécutions de fonctions. La configuration d'alertes CloudWatch basées sur ces métriques permet des réponses proactives aux violations potentielles, aux anomalies ou problèmes de performance. Cette surveillance proactive permet d'identifier et d'atténuer rapidement des risques de sécurité sur différents services AWS. Dans notre infrastructure, il n'y a pas de surveillance et de journalisation dans la version d'infrastructure faible, mais la version d'infrastructure forte oui.

De plus, nous avons l'option d'utiliser AWS CloudTrail conjointement avec CloudWatch logs pour la centralisation des journaux permettant l'agrégation des journaux et la recherche. CloudWatch logs collecte les journaux générés par les services AWS et CloudTrail collecte les journaux de requêtes API effectués sur les comptes AWS. Cette centralisation permet et simplifie l'analyse de sécurité des logs pour une meilleure détection, réponse aux incidents et gestion de conformité. Dans notre cas, la centralisation de logs est activée dans l'infrastructure

forte avec tous les journaux dirigés vers CloudWatch, ainsi que le versionnage de buckets S3 actif.

4.4 Détection d'anomalie

La détection d'anomalie est une étape importante pour garder une infrastructure AWS sécuritaire. Pour se faire, il faut mettre en place des manières de détection telle que basée sur des seuils, des services autogérés, ou même avec détection par l'apprentissage automatique.

La une détection basée sur des seuils implique de définir des seuils prédéfinis pour diverses métriques associées à des ressources telles que les instances EC2, les buckets S3, les activités IAM et les fonctions Lambda. Les écarts au-delà de ces seuils déclenchent des alertes, indiquant des anomalies potentielles. Nous avons différentes détections basées sur des seuils d'implémentées dans la configuration forte pour lever des alarmes CloudWatch lorsque les seuils sont franchis.

Comme service autogéré, il y a le service AWS GuardDuty, qui est un service de détection de menaces géré qui surveille en continu les activités malveillantes et les comportements non autorisés dans les comptes AWS. En continu, il analyse les journaux de flux VPC, les journaux d'événements CloudTrail et les journaux DNS pour identifier les comportements suspects à l'aide de flux de renseignements sur les menaces et d'algorithmes d'apprentissage automatique ("machine learning"). Dans nos infrastructures, nous ne faisons malheureusement pas usage de telle détection.

La détection par apprentissage automatique ("machine learning") permet une meilleure détection d'anomalies dans certains scénarios. La détection se base sur l'analyse de modèles d'historique de données et identifie des écarts de différences pouvant indiquer des risques. Un tel service serait Amazon Macie, ou même les fonctionnalités de détections de CloudWatch. Dans notre cas, nos infrastructures n'utilisent pas Amazon Macie, mais seulement CloudWatch dans le cas de l'infrastructure forte.

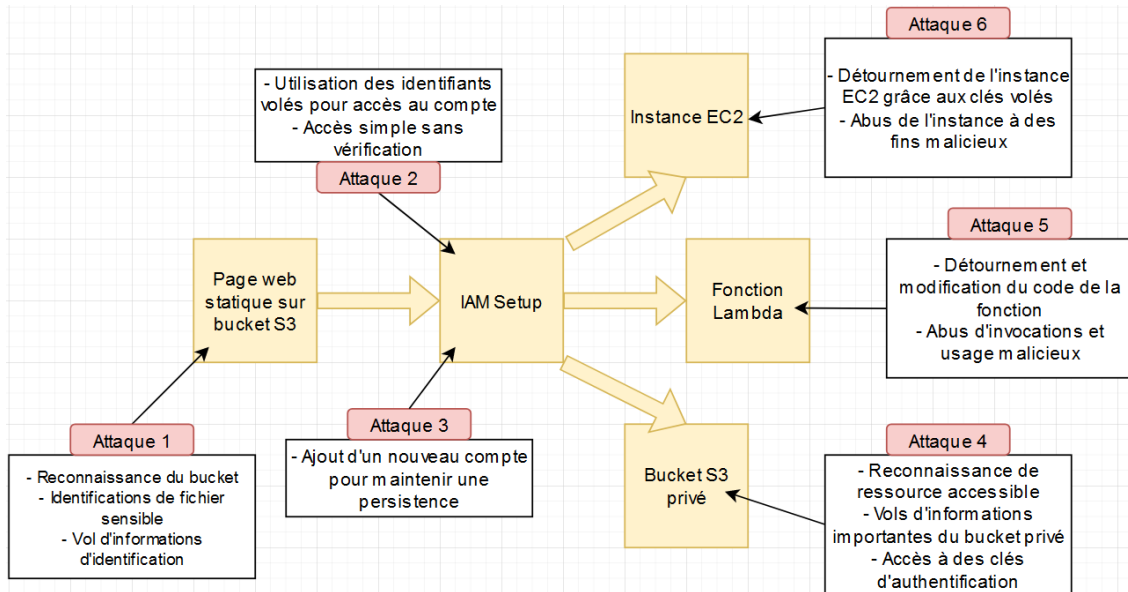


FIGURE 2 – Schéma d'attaques

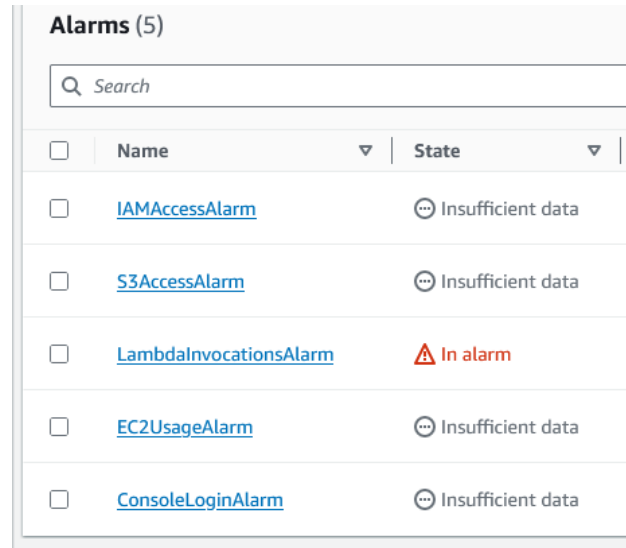
5 Expériences

5.1 Simulations de violations de données

L'objectif de simulation de violations de données est d'imaginer des scénarios d'attaques concernant le vol de données dans l'infrastructure, généralement provenant de "snooping" des buckets ou sur le data en transition. Dans nos simulations, nous exploitons spécifiquement ces vulnérabilités pour nous permettre d'acquérir un accès à l'intérieur de l'infrastructure faible, tel que l'attaque 1 sur la figure 2. L'attaque initiale était constituée d'effectuer une reconnaissance du site web étant hébergé sur un bucket S3. Ceci permet de découvrir les fichiers sensibles qui permettront la suite de la chaîne d'attaque. Cette attaque est possible puisque le bucket est public, mais aussi parce qu'il est mal configuré et permet l'accès à des fichiers sensibles à la racine du bucket. Ceci est une vulnérabilité très récurrente que l'on retrouve à plusieurs endroits dans des buckets S3 publics.

5.2 Tests de pénétration des infrastructures

L'objectif de tests de pénétration de l'infrastructure est de faire ressortir les vulnérabilités d'une infrastructure quelles soient causés par des attaques sur le VPC ("virtual private cloud"), la violation d'instance ou l'utilisation de mauvaise configuration pour arriver à un but. Selon notre configuration de l'infrastructure, les seuls tests que nous avons appliqués sont les tests de pénétration sur l'abus de mauvaise configuration que ce soit sur IAM ou sur les services tels quels. Très généralement, la plupart des successions de la chaîne d'attaques se basent sur de la mauvaise configuration de rôle et de permissions. Lorsque la base de l'infrastructure d'une organisation est mal configurée, les brèches deviennent très dures à contenir et éviter. Ceci est le cas dans notre première infrastructure qui n'a pas de défense pour le compte initial qui est utilisant par l'attaque. Les attaques 2, 3 et 4 sont possibles, car



Alarms (5)		
Search		
<input type="checkbox"/>	Name	State
<input type="checkbox"/>	IAMAccessAlarm	Insufficient data
<input type="checkbox"/>	S3AccessAlarm	Insufficient data
<input type="checkbox"/>	LambdaInvocationsAlarm	In alarm
<input type="checkbox"/>	EC2UsageAlarm	Insufficient data
<input type="checkbox"/>	ConsoleLoginAlarm	Insufficient data

FIGURE 3 – Alarmes créées dans l'infrastructure forte

le compte n'était pas protégé, et le modèle de "least privilege" n'était pas appliqué pour permettre une répartition des tâches dans l'infrastructure. Ainsi, le compte était facile d'accès et il avait un accès total à l'infrastructure. Les résultats des attaques et leurs analyses sont présentés dans la section 7 du rapport.

5.3 Tests de détection d'anomalies

L'objectif de tests de détection d'anomalies est de s'assurer de pouvoir être capable de détecter des anomalies dans les services lorsqu'elles occurrent. Très généralement, des métriques sont surveillées en utilisant des services telles qu'AWS CloudWatch avec l'ajout d'alarmes pour alerter sur des anomalies détectées. Des exemples d'anomalies sont l'augmentation de l'usage réseau, des appels suspects sur l'API d'AWS, ou des services tel que GuardDuty qui lève des alarmes. Dans notre infrastructure forte, nous avons en place différentes alarmes en place pour détecter et tester la détection d'anomalies, figure 3, inattendu lorsque nous effectuons nos attaques. Dans l'infrastructure faible, ceci n'est pas testé du tout.

5.4 Évaluation de l'efficacité du suivi

L'objectif ici est de faire une évaluation de l'efficacité du suivi des journaux, de la latence de génération des journaux, de la granularité des métriques recueillies par les services et de la rétention de journaux ainsi que la facilité de récupérer ces journaux la. Dans nos infrastructures, nous faisons usage de cette évaluation seulement dans l'infrastructure forte, qui incorpore les "best practices" d'AWS. La rétention de log se fait sur une durée d'une semaine (7 jours) dans les groupes de journaux de CloudWatch. La période recommandée allant de 1 semaine à 2 semaines selon la taille de l'entreprise, avec un mode très verbeux, donc pas de spécification, tous les journaux sont gardés. Ceci est considéré du "hot storage", qui veut dire qu'il est accessible très facilement et sans délai, tandis que les systèmes de "cold storage" sont faits pour garder de plus longues périodes de journaux allant jusqu'à des mois,

voir des années. Dans notre cas, nous n'avons pas cette deuxième option d'implémenter pour nos expériences. Le service CloudWatch s'occupe de faire la rotation de ces logs lorsque leur temps de vie est écoulé.

La granularité des métriques est ajustée à des évaluations par groupe de 5 minutes, et avec des seuils prédéfinis. Par exemple, la métrique qui déclenche l'alarme de lambda est configurée à 5 invocations sur une période de 5 minutes, tandis que les autres sont placés à 1 pour le threshold par période 5 minutes.

Pour ce qui est de la latence, l'agent CloudWatch qui se charge de l'envoi des journaux est configuré par défaut à 5 secondes par envois, mais reste tout de même configurable par l'utilisateur. Pour notre infrastructure, nous gardons la valeur par défaut. Ceci signifie que l'envoi des logs vers les groupes de journaux se fait à chaque 5 secondes pour chaque service utilisé dans l'infrastructure.

6 Réponse aux incidents

6.1 Planification de la réponse aux incidents

Avoir un plan d'intervention en cas d'incident est important afin d'être capable de contrer efficacement tout type d'attaque, dont les attaques de détournement de services et de comptes. Les bénéfices qu'apporte cette mesure préventive sont majeurs, puisqu'il permet d'organiser efficacement une réponse aux attaques de sécurité. Tout d'abord, avoir un plan d'intervention clair et précis permet de diminuer le temps de détection d'incident et le temps nécessaire pour effectuer des contre-mesures. En effet, on remarque que les compagnies possédant un plan d'intervention bien définie ont tendance à détecter plus tôt les attaques. Ceci a pour impact que les compagnies sont capable d'intervenir plus rapidement et ainsi minimiser les dommages potentiels d'une attaque ou de prévenir davantage de dommage que déjà réalisé. Un bon plan d'intervention permet aussi comme mentionné de diminuer les répercussions d'une attaque. En effet, avec un plan bien détaillé, il est souvent possible pour les organisations d'isoler plus facilement et rapidement de différents éléments compromis et ainsi contenir l'attaque et minimiser l'impact global.

Un bon plan d'intervention inclut également un plan pour la communication où les différentes chaînes de communication à utiliser en cas d'incident sont bien définies. Ceci permet d'efficacement coordonner les individus nécessaires pour implémenter la solution. De plus, un bon plan inclue une analyse post-incident afin d'analyser les failles du système ayant permis l'attaque, pour ensuite les corriger. Aussi, l'analyse post-incidente devrait inclure une analyse de processus d'intervention afin de prendre note des bon et mauvais coups afin de continuer d'améliorer le plan d'intervention.

6.2 Détection et reporting des incidents

AWS fournit plusieurs outils permettant de faciliter la sécurité de l'infrastructure infonuagique de leur client. Voici quelque outil disponible dans AWS pour aider avec la détection d'incident :

- AWS CloudTrail : C'est un service AWS qui permet de conserver les activités API. Ceci inclut les événements tels que ce qui a fait l'action, quand l'action a été faite, quelle action a été exécutée et quelle ressource a été affecté par l'action. Ainsi cette ressource permet de conserver et surveiller les actions réalisées sur les différentes ressources AWS.
- AWS CloudWatch : C'est un service AWS qui permet de recueillir et surveiller des données ou fichiers. Ce service permet aussi d'établir des alarmes lorsque les activités sortent des seuils préétablis.
- AWS Config : C'est un service AWS qui permet aux utilisateurs d'évaluer et d'analyser leur configuration de leurs ressources AWS. En effet, cet outil fournit des informations sur les différentes ressources d'un compte et un historique des modifications des configurations des différentes ressources.

Il est important de noter qu'il est aussi possible pour les compagnies d'utiliser d'autres outils que ceux fournis par AWS. AWS permet aux individus d'intégrer des outils externes à leur

infrastructure infonuagique pour augmenter la sécurité de leur environnement.

Tous ces outils sont pratiques pour aider à détecter les anomalies. Toutefois, afin qu'il soit réellement efficace, il faut que les compagnies les utilisant définissent premièrement des points de référence par rapport à quel type d'activité sont considérés normaux. En effet, sans la définition de ces points de références, il est impossible de détecter la présence d'anomalie même avec l'utilisation des outils mentionnée plus haut. Aussi, dans le processus de détection d'anomalie, il est important de détailler le processus utilisé pour classer les anomalies. EN effet, il est important d'avoir des processus clairs pour déterminer si une anomalie est un réel incident ou simplement un faux positif. Ceci inclut le processus à suivre pour investiguer et confirmer s'il s'agit réellement d'une anomalie ou d'un simple faux positif.

6.3 Analyse des incidents

Une fois qu'un incident a été détecté, grâce aux ressources et méthode misent de l'avant dans la section précédente, il est nécessaire de bien caractériser l'incident afin de s'assurer que les bonnes mesures sont mises en place pour la résolution, la remédiation et la prévention de futur incident.

Afin d'effectuer une analyse de l'incident, il est nécessaire d'avoir accès et de collecter des informations qui permettront de caractériser l'incident. Dans l'environnement infonuagique, cela prend majoritairement la forme de "logs" qui sont produits par les différents services. Ceux-ci contiennent des informations tels que l'activité des utilisateurs, les appels API, les changements de ressources, etc. Tels que mentionnés dans la section précédente, ses logs peuvent être collectés et entreposer par des services Amazon tels que CloudTrail, CloudWatch et Config. Ci-dessous, une liste qui met de l'avant différents types de logs et de ressources qui pourraient être utilisées dans l'analyse d'incident [15] :

- All EC2 instance metadata
- Amazon EBS disk snapshots
- EBS disks streamed to S3
- Memory dumps
- CloudTrail logs
- AWS Config rule findings
- Amazon Route 53 DNS resolver query logs
- VPC Flow Logs
- Elastic Load Balancing access logs
- System logs

Au-delà de la collection de logs et d'évidence, deux stratégies sont de mises lors de l'analyse d'un incident, soit l'analyse de la cause originelle (root-cause-analysis) et l'analyse criminalistique (forensic analysis). Tels que son nom le mentionne, l'analyse de la cause originelle chercher avant tout à identifier la cause du problème (IAM avec trop de permission, mauvaise configuration de ressources, etc.), alors que l'analyse criminalistique est beaucoup plus holistique et cherche non seulement à identifier la source du problème, mais chercher à analyser

et identifier tout les aspects de l'incident, incluant l'identification des acteurs dans le but de potentiellement bâtir un cas légal.

Plusieurs outils existe dans l'environnement AWS et à l'extérieur qui permettent de compléter et d'aider dans l'analyse d'incident. Le premier est Amazon Detective, cet outil permet d'identifier la cause principale d'un incident en amassant les logs vus plus tôt et en utilisant des outils d'apprentissage machine, d'analyse statistique et des graphes et réseaux afin de construire un ensemble de données facile à analyser et investiguer [3].

6.4 Correction et récupération

Une fois que la source de l'incident a été identifiée et analysée, il est nécessaire de passer à la phase de remédiation et de récupération des ressources. Le but de celle-ci est essentiellement de revenir le plus rapidement à un environnement non compromis qui permettra de fournir les fonctionnalités nécessaires aux opérations de l'entreprise. Afin de faire ceci, plusieurs outils et techniques peuvent être mis en place.

Premièrement, l'utilisation d'un outil de IaC, tels que Terraform ou Cloud Formation permet de facilement redéployer l'infrastructure de façon uniforme et sans erreur. Deuxièmement, l'utilisation de AWS Backup, un service permettant de gérer et configurer tout ce qui touche aux sauvegardes des ressources AWS de bases (EC2, EFS, etc.) permet de s'assurer que les sauvegardes des différentes ressources est le plus proche possible du début de l'incident afin de limiter la perte de données ou autre. Finalement, il est important de toujours d'avoir une sauvegarde à jour du format AMI qui a été utilisé pour créer les instances EC2 [5].

6.5 Leçons apprises et examen des incidents

Enfin, une fois que l'incident où l'attaque a été détecté, analyse et que l'infrastructure a été rétablie avec un minimum de temps d'interruptions, il est nécessaire d'examiner l'incident. En utilisant l'analyse de cause initiale ou le rapport criminalistique, il est nécessaire d'essayer de trouver une solution à la faille qui a causé l'incident et de faire une revue de la performance du plan de réponse aux incidents. Un format tel que celui donné par AWS peut permettre de structurer les démarches [6].

Finalement, il est important de toujours prendre en compte la responsabilité des différents partis lors d'attaque ou d'incident. En effet, l'utilisation des ressources infonuagique de AWS implique un modèle de responsabilité partagé. En fonction de l'infrastructure choisie et des ressources mise en œuvre, il est important de bien comprendre ce qui est la responsabilité de AWS et ce qui est la responsabilité du consommateur ou de l'entreprise. À noter que AWS offre un service de consultation "AWS Incident Detection and Response" qui permet d'aider des entreprises avec peu ou pas de ressources ou d'expertise en infonuagique à établir, réviser et prendre en charge leur plan de réponse aux incidents [4].

7 Discussion

7.1 Key Findings

Comme décrit dans les sections précédentes, l'expérimentation était basée sur deux scénarios, soit un avec une infrastructure respectant les recommandations de l'état de l'art et une autre ne les respectant pas. Les résultats de ses deux expérimentations sont donnés par le tableau 1 et 2.

Attaque	Résultats non-SOTA	Analyse
Site statique	Données volés des buckets	Dépôt d'informations sensibles sur un bucket mal configuré et public
Compte AWS	Accès au compte avec les informations sensibles du bucket	Pas de double vérification sur les comptes sensibles sensibles
Ajout compte	Ajout d'un nouvel utilisateur	Compte initial ont beaucoup trop de permissions et permettent la création de nouveaux comptes
Vol .key files	Accès à des clés privées de ssh	Compte initial a beaucoup trop de permissions et permet l'accès à d'autres informations
EC2 Hijack	Capable de se connecter à l'instance	Instance EC2 mal configurée et permet la connexion de n'importe quel emplacement
Lambda Hijack	Capable de modifier le code et d'abuser la fonction	Compte initiaux a beaucoup trop de permissions et permet la modification et l'abus de fonction lambda

TABLEAU 1: Résultats du scénario non-SOTA

Des six attaques qui ont été simulées, on voit que dans le scénario non sécurisé, l'entièreté de celle-ci ont réussi à faire le dommage souhaité, alors que dans le scénario avec les recommandations de l'état de l'art, aucune attaque n'a réussi à pénétrer. Dans le tableau 2, certaines étapes ont des étoiles (*) dans la colonne "résultats". La raison est que puisque les attaques s'enchaînent une après l'autre, donc il faut que l'attaque 1 réussisse pour que l'attaque 2 soit possible, nous assumons que pour chaque attaque subséquente à réussis. Par exemple, le résultat de l'attaque contre le compte AWS (donc l'attaque 2 de la figure 2) n'existerait pas si l'attaque 1 sur le site statique n'est pas réussie puisque l'attaquant n'aura tout simplement pas accès aux données sensibles initialement. Il est de même pour les attaques 3, 4, 5 et 6 de la figure 2 qui dépendent des attaques 1 et 2 successivement pour être fait.

Dans le cas d'une telle infrastructure et en ayant un scénario tel que l'infrastructure faible, un attaquant qui obtient les accès pourrait massivement impacter plusieurs aspects de cette

organisation. Il pourrait infliger des coûts énormes avec l'abus de services sans surveillance et suivi. Autres que les coûts, l'attaquant ayant maintenant accès aux services, il pourrait procéder à de futures attaques en utilisant les services compromis tels que la machine EC2 pour commettre des actes plus ou moins légales, ou des attaques de déni de service avec l'instance EC2 ou la fonction lambda. Encore plus poussé, il pourrait prendre le contrôle de l'infrastructure de l'organisation qu'il a été capable d'infiltrer et d'extraire toutes informations sensibles déposées aux fils du temps.

Attaque	Résultats SOTA	Analyse
Site statique	Pas d'information sensible sur le bucket S3	Élimination de la source d'entrée, car le bucket est mieux sécurisé et ne contient pas d'information sensible
Compte AWS	Pas d'accès au compte, car bloqué par MFA, utilisateur alerté de l'accès*	L'attaquant n'est pas capable de continuer, car la double vérification l'en empêche
Ajout de compte	Pas capable d'ajouter un nouvel utilisateur, car pas de permissions	Le compte initial n'ayant pas de permissions trop élevées, l'attaquant n'est pas capable de créer un nouvel utilisateur
Vol des .key files	Pas d'accès au bucket S3 super important*	Le compte initial n'ayant pas de permissions trop élevées, l'attaquant n'est pas capable d'aller sur d'autres ressources
EC2 Hijack	Incapable de se connecter à la machine EC2 même avec la bonne clé*	L'attaquant n'est pas capable de se connecter à l'instance, car elle ne lui permet pas de son emplacement/adresse
Lambda Hijack	Incapable de modifier et prendre contrôle de la fonction lambda*	L'attaquant n'est pas capable de se modifier la fonction, car il n'a pas accès

TABLEAU 2: Résultats du scénario SOTA

7.2 Limitations

Une des limitations de ce projet est au niveau des contraintes de l'environnement universitaire. C'est-à-dire que l'environnement ou non faisons nos simulation, soit AWS Academy, ne permettait pas certains types d'attaques et de manipulation (ceux sur les rôles dans IAM). Notre projet étant sur l'exploitation des comptes et services, les attaques sur les rôles d'IAM (qui font partie de ce domaine) n'ont pas pu être testées. De plus, n'étant pas des experts dans le domaine, le Terraform permettant l'automatisation de l'expérience a grandement augmenté la complexité du projet et à cause du temps alloué cela a aussi limité le temps que nous avons pu passer sur l'expérimentation. Celle-ci est donc moins complexe et complète qu'originellement souhaiter.

Finalement, un pan complet et très commun du détournement de compte et de services sont les attaques liées à l'ingénierie sociale, d'hameçonnage et, etc. Ce type d'attaque n'a pas été simulé dans ce projet par souci de temps, du fait qu'il n'était pas possible de créer ce type d'attaques avec les ressources utilisées et que dans la plupart du temps, les solutions sont autant au niveau du logiciel "filtering des courriels et, etc." qu'au niveau des individus (entraînement et, etc.). Ce qui aurait rendu l'expérimentation et l'évaluation des recommandations de l'état de l'art difficile à faire dans le contexte du projet.

7.3 Implications

Les résultats obtenus dans cette étude sont très intéressants pour les compagnies utilisant AWS. En effet, à partir des résultats, il a été possible de conclure que les recommandations AWS procurent une certaine protection de base aux environnements infonuagique qui les applique contre les attaques de détournement de services et de comptes de base. Ceci est très positif pour les compagnies, puisqu'ils peuvent utiliser ces recommandations comme base pour leur infrastructure de sécurité de leur environnement infonuagique tout en aillant la tranquillité d'esprit que cette infrastructure de sécurité leur procure une réellement protection contre les attaques de détournement de services et de comptes.

Il est important de noter que cette protection qu'offrent ces recommandations n'est probablement pas parfaite. Toutefois il constitue un bon point de départ pour débuté la mise en place une infrastructure et des protocoles de sécurité.

8 Conclusion and Future Work

8.1 Recap

Dans ce projet notre équipe cherchait à déterminer si les recommandations AWS au niveau de la sécurité permettent d'offrir un niveau de protection adéquat à une infrastructure infonuagique AWS. Pour y parvenir, une expérimentation a été réalisée. Lors de cette expérimentation, deux environnements, un non conforme et un conforme aux recommandations de l'état de l'art, ont été testés contre des attaques de détournement de services et de comptes de base. Six attaques ont été réalisées au total soit une sur le site statique, une sur le compte AWS, une sur l'ajout de compte, une sur le vole de fichier de clés privées, une sur EC2 hijacking et une sur lambda hijacking.

Dans ce projet notre équipe cherchait à déterminer si les recommandations AWS au niveau de la sécurité permettent d'offrir un niveau de protection adéquat à une infrastructure infonuagique AWS. Pour y parvenir, une expérimentation a été réalisée. Lors de cette expérimentation, deux environnements, un non conforme et un conforme aux recommandations de l'état de l'art, ont été testés contre des attaques de détournement de services et de comptes de base. Six attaques ont été réalisées au total soit une sur le site statique, une sur le compte AWS, une sur l'ajout de compte, une sur le vole de fichier de clés privées, une sur EC2 hijacking et une sur lambda hijacking.

Les résultats obtenus suite à cette expérience démontrent que les recommandations AWS de sécurité permettent d'offrir un niveau de protection adéquat à une infrastructure infonuagique AWS contre les attaques de détournement de services et de comptes de base. En effet, dans l'environnement non conforme il était possible pour un attaquant fictif de réaliser les six attaques testées sans beaucoup de difficulté. Toutefois, dans l'environnement conforme, l'attaquant n'a pas pu réaliser aucune des six attaques.

8.2 Recommendations

Suite à ce projet, nous conseillons de mettre en place les recommandations AWS dans vos différentes infrastructures infonuagiques. En effet, ces mesures permettent d'offrir un certain niveau de protection de base contre les attaques de détournement de services et de comptes de base. Il est fort possible qu'uniquement l'utilisation de ces recommandations n'offre pas une protection complète contre tous les niveaux d'attaques. Toutefois, en combinant ces différentes recommandations avec d'autres mécanismes de cybersécurité en infonuagique il sera possible de protéger ces différentes infrastructures infonuagiques d'une bonne majorité d'attaques et, en cas d'attaques, être capable de répondre rapidement.

8.3 Future Directions

Dans le futur, il serait intéressant d'étendre le scope du projet réalisé ici. En effet, dû à de nombreuses contraintes comme le temps ou l'environnement choisis il n'était que possible de réaliser lors de l'expérimentation des attaques de détournement de services et de comptes

de base. Or, pour un futur projet, il serait intéressant d'augmenté la liste d'attaque de détournement de services pour inclure des attaques plus avancées comme "Olympic Destroyer, "Operation Parliament ou "Energitic Bear" pour en nommer que quelque une. En effet, en utilisant des attaques plus avancées il sera d'avantages possibles de trouver des failles dans les recommandations de AWS.

Également pour un futur projet de recherche, il serait intéressant de tester différentes propositions d'améliorations pour les recommandations AWS pour voir quelle est la protection additionnelle qu'ils ajoutent. Bien que les recommandations AWS actuelles permettent de protéger les environnements infonuagiques contre des attaques de détournement de services et de comptes, il existe de nombreuse faille qui permette encore à des acteurs malveillants de réaliser de tel type d'attaques. Ainsi, il y a de la place à étudier ces attaques plus poussées et trouver des moyens ou technique qui pourront être ajoutées aux recommandations AWS pour permettre de les bloquer.

9 Acknowledgement

Tous les membres de l'équipe confirment que tous les membres de l'équipe ont participé activement à la réalisation de projet de manière équitable.

- Diab Khanafer, 1952548
- Zachary Allaire, 1945146
- Zoé Paradis, 2008732

Références

- [1] Temidayo ABAYOMI-ZANNU et Isaac ODUN-AYO. « Cloud Identity Management – A Critical Analysis ». en. In : *Hong Kong* (2019).
- [2] Zachary ALLAIRE, Diab KHANAFER et Zoé PARADIS. *Projet final INF8102*. 2023. URL : <https://github.com/diab2013/inf8102finalproject.git> (visité le 10/12/2023).
- [3] AMAZON. *Amazon Detective*. 2023. URL : <https://aws.amazon.com/detective/> (visité le 09/12/2023).
- [4] AMAZON. *AWS Incident Detection and Response*. 2023. URL : <https://aws.amazon.com/premiumsupport/aws-incident-detection-response/> (visité le 09/12/2023).
- [5] AMAZON. *Disaster recovery options in the cloud*. 2023. URL : <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore> (visité le 09/12/2023).
- [6] AMAZON. *Establish a framework for learning from incidents*. 2023. URL : <https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/establish-framework-for-learning.html> (visité le 09/12/2023).
- [7] A. S. ANAKATH, S. RAJAKUMAR et S. AMBIKA. « Privacy preserving multi factor authentication using trust management ». In : *Cluster Computing* (2019).
- [8] Indranil BOSE et Alvin Chung Man LEUNG. « The impact of adoption of identity theft countermeasures on firm value ». en. In : *Decision Support Systems* 55.3 (juin 2013), p. 753-763. ISSN : 01679236. DOI : 10.1016/j.dss.2013.03.001. URL : <https://linkinghub.elsevier.com/retrieve/pii/S016792361300081X> (visité le 12/10/2023).
- [9] Brian CUSACK et Eghbal GHAZIZADEH. « Defining cloud identity security and privacy issues : A Delphi method ». In : *AMCIS 2019 Proceedings* (2019).
- [10] Marwan DARWISH. « Privacy and Security of Cloud Computing : A Comprehensive Review of Techniques and Challenges ». In : (nov. 2018).
- [11] S. DAS, B. WANG et L. J. CAMP. « Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content ». In : *arXiv* (2019).
- [12] Eghbal GHAZIZADEH et al. « A survey on security issues of federated identity in the cloud computing ». en. In : *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*. Taipei, Taiwan : IEEE, déc. 2012, p. 532-565. ISBN : 978-1-4673-4510-1 978-1-4673-4511-8 978-1-4673-4509-5. DOI : 10.1109/CloudCom.2012.6427513. URL : <http://ieeexplore.ieee.org/document/6427513/> (visité le 12/10/2023).
- [13] Eghbal GHAZIZADEH et al. « A Trust Based Model for Federated Identity Architecture to Mitigate Identity Theft ». en. In : *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*. London, UK : IEEE, 2014. ISBN : 978-1-908320-39-1.

- [14] Ibrahim GOMAA et al. « Automated Security Assessment for IDaaS Framework ». en. In : *Wireless Personal Communications* 116.4 (fév. 2021), p. 3465-3490. ISSN : 0929-6212, 1572-834X. DOI : 10.1007/s11277-020-07860-8. URL : <http://link.springer.com/10.1007/s11277-020-07860-8> (visité le 12/10/2023).
- [15] Anna MCABEE, Ciarán CARRAGHER et Pratima SINGH. *Logging strategies for security incident response*. 2023. URL : <https://aws.amazon.com/blogs/security/logging-strategies-for-security-incident-response/> (visité le 09/12/2023).
- [16] A. MIRIAN et al. « Hack for hire : Exploring the emerging market for account hijacking ». In : *In The World Wide Web Conference* (2019).
- [17] Patrick MOSCA et al. « Cloud Security : Services, Risks, and a Case Study on Amazon Cloud Services ». en. In : *International Journal of Communications, Network and System Sciences* 07.12 (2014), p. 529-535. ISSN : 1913-3715, 1913-3723. DOI : 10.4236/ijcns.2014.712053. URL : <http://www.scirp.org/journal/doi.aspx?DOI=10.4236/ijcns.2014.712053> (visité le 12/10/2023).
- [18] Oleksandr OKSHUK et Vladyslava CHAIKOVSKA. « Authentication Process Threats in the Cloud Technologies ». en. In : (2018).
- [19] Michael SOLTYS. *Cybersecurity in the AWS Cloud*. en. arXiv :2003.12905 [cs]. Mars 2020. URL : <http://arxiv.org/abs/2003.12905> (visité le 12/10/2023).
- [20] Tri Hoang VO et al. « Identity-as-a-Service : An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment ». en. In : *Future Internet* 11.5 (mai 2019), p. 116. ISSN : 1999-5903. DOI : 10.3390/fi11050116. URL : <https://www.mdpi.com/1999-5903/11/5/116> (visité le 12/10/2023).
- [21] G. YEE. *Privacy and Security for Cloud Computing*. Springer London, 2013.