DÉCEMBRE 2018
NO. 8

INFORMATION SÉCURITÉ

CYBERSÉCURITÉ : COMMENT PASSER À UN MODÈLE EN PROFONDEUR

TechTarget

La fin de l'innocence

PAR VALÉRY MARCHIVE

L'être humain est par nature enclin à faire confiance à ses semblables. Derrière ce que certains pourraient voir comme de la naïveté, se cache l'une des clés de la capacité de l'espèce à coopérer. Las, c'est bien connu, certains ne manquent pas d'abuser de la confiance des autres. Et pourtant, Internet s'est largement construit, à ses origines, sans considération pour la sécurité et la protection contre d'éventuelles malveillances. La cyber-délinquance ne manque pas de souligner régulièrement, répétitivement, et depuis longtemps déjà, à quel point ce pouvait être une erreur.

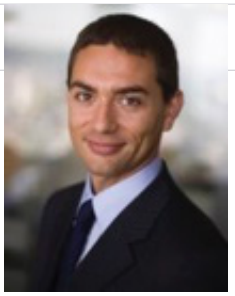
Initialement, la sécurité informatique s'est construite sur la notion de périmètre de confiance, le modèle dit « château-fort » : ce qui est à l'intérieur est sûr ; la menace vient de l'extérieur, de l'autre. Mais cette approche s'est avérée erronée et plus encore, à mesure que se sont ouverts les systèmes d'information, s'interconnectant à ceux de partenaires ou à des services cloud. Une réalité s'est alors imposée : la menace peut être partout ; il n'y a plus d'espace protégé ; il n'y a que des entités (utilisateurs ou systèmes consommateurs/producteurs de données) auxquelles il convient d'accorder prudemment un certain degré de confiance, dosé au plus juste, et de préférence de manière contextuelle, voire dynamique. C'est l'idée de la défense en profondeur, des architectures dites « zero trust », sans confiance. Ou du moins sans confiance absolue et octroyée sans réserve. La fin de l'innocence, en somme, et l'entrée de l'ère d'une défiance rendue nécessaire par l'évolution de la menace, mais également de l'exposition des systèmes d'information à celle-ci.

VALÉRY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

Le modèle de sécurité du futur n'est-il pas celui d'une compagnie aérienne ?

Pour illustrer ses différentes approches, le monde de la sécurité s'est successivement référé à l'image du château-fort, puis de l'aéroport.
Pour la prochaine évolution, l'image de la compagnie aérienne pourrait être utilisée.

Par Gérôme Billois



DEPUIS DES ANNÉES, la filière cybersécurité tente d'expliquer simplement les concepts complexes qu'elle manipule tous les jours.Il s'agit d'un enjeu majeur pour convaincre les dirigeants, les métiers, ou tout simplement pour expliquer aux utilisateurs ce que fait la filière. Aujourd'hui, les systèmes d'information connaissent des évolutions majeures qui nécessitent de repenser la manière dont la sécurité est aujourd'hui déployée. Mais alors quelle image utiliser pour convaincre ?

DU CHÂTEAU FORT À L'AÉROPORT… MAIS APRÈS ?

En 2008, nous avions formalisé une première vision sur l'évolution des modèles de sécurité. Le modèle historique, celui reposant sur la sécurité périmétrique, était alors décrit par l'image d'un château-fort. Un château-fort avec des hauts murs normalement impénétrables (le périmètre), son pont-levis (le pare-feu), mais avec un cœur ouvert à tous (le réseau interne non cloisonné). Et puis, au fil des années, l'ouverture du SI est devenue un élément clé pour réussir la transformation digitale et autoriser certains usages innovants (cloud, BYOD…). Le château-fort c'est donc transformé en aéroport. Un

aéroport ouvert par défaut, avec un hall permettant de récupérer des informations simplement ou de faire des achats. Mais un aéroport avec des zones sécurisées, comme le tarmac et les avions, protégeant alors les périmètres les plus critiques. Ce modèle permet d'ouvrir le SI tout en protégeant les actifs les plus critiques.

DEMAIN, UN SI DE PLUS EN PLUS DÉCENTRALISÉ

En analysant les évolutions actuelles, il est évident que le SI va encore fondamentalement changer. Le SI « interne » va se réduire et regrouper uniquement les périmètres historiques ou très critiques. Les fournisseurs externes et les clouds vont se multiplier et prendre une place prépondérante dans le SI. Ils échangeront directement entre eux des données et interagiront à plusieurs sur des traitements métiers complexes. Les terminaux consommant cette information vont se diversifier, avec les terminaux des clients, les objets connectés ou encore les terminaux personnels des employés. Les données vont donc circuler partout, sur des systèmes et des environnements sur lesquels il n'y a pas de contrôle direct.

La manière d'assurer la cybersécurité dans ce nouveau modèle reposera très certainement sur la création d'une fonction centrale, un service transverse de sécurité. Celui-ci autorisera les différents fournisseurs externes (cloud, partenaires…) et les différents terminaux à accéder aux données en fonction de leur identité (qui, quel rôle) mais aussi de leur niveau de conformité (quelle mise à jour, terminal chiffré, quelle localisation, etc.).

« La manière d'assurer la cybersécurité dans ce nouveau modèle reposera très certainement sur la création d'une fonction centrale, un service transverse de sécurité. »

— Gérôme Billois

UN MODÈLE INSPIRÉ DE CELUI D'UNE COMPAGNIE AÉRIENNE

Pour expliquer cette évolution, une autre image simple peut être utilisée. C'est celle de la compagnie aérienne. Aujourd'hui, une compagnie aérienne dispose d'avions. Ils sont l'équivalent des données de notre système d'information. Ces avions sont très critiques pour les compagnies, ils transportent les clients et les équipes de la compagnie aérienne.

Mais les compagnies aériennes font confiance à un écosystème complexe pour s'assurer que les avions arrivent à bon port. Les aéroports accueillent les avions et les passagers comme un fournisseur de cloud peut

accueillir des données et les traiter. Les aéroports sont capables d'accueillir des avions de plusieurs compagnies en garantissant la sécurité et la confidentialité, au même titre qu'un fournisseur cloud gère les données de plusieurs clients. Le contrôle aérien s'assure du fonctionnement global du secteur et de la sécurité des différents vols.

Quand une compagnie aérienne décide d'ouvrir une nouvelle ligne, elle évalue la sécurité du pays, de l'aéroport, avant de prendre une décision. Un processus nécessaire aussi avant de souscrire à des offres cloud. Et en fonction du niveau de sécurité du pays et de l'aéroport, la compagnie peut décider d'ajouter des mesures complémentaires de sécurité. Voire parfois de fermer temporairement des lignes en cas de changement brusque de contexte.

Surtout, une compagnie aérienne dispose d'un centre de contrôle opérationnel, qui va suivre et surveiller l'ensemble des vols, l'ensemble des avions, et s'assurer du niveau de sécurité des aéroports en fonction des informations qui lui remontent ou qu'il acquiert via les services de sécurité (threat intelligence). En cas d'incidents ou de crise, c'est le centre opérationnel qui va prendre la main et gérer la crise, imposant des mesures de sécurité nouvelles si besoin.

UN MODÈLE DIFFICILE À IMPLÉMENTER

C'est clairement ce modèle de « confiance dynamique », avec une évaluation des droits accès en fonction de la sécurité de ceux qui accèdent (terminaux, serveurs, personnes, etc.), avec la capacité à surveiller globalement les données où qu'elles soient et avec la capacité à pousser de nouvelles règles de sécurité dynamiquement, qui sera au cœur de la cybersécurité dans les années qui viennent. Ce modèle sera requis pour embrasser toutes les innovations à venir.

Il représente encore un défi, même si de nombreuses initiatives vont dans cette direction. Citons notamment le standard « software defined perimeter » de la Cloud Security Alliance ou l'initative « Beyond Corp » de Google. Une direction à suivre pour les années à venir. Et une image à garder en tête pour l'expliquer simplement. ■

GÉRÔME BILLOIS *est senior manager au sein de la « practice Risk Management et Sécurité de l'information » de Wavestone. Il est également membre du conseil d'administration du CLUSIF et du comité ISO JTC1/SC27 responsable de la standardisation pour la sécurité de l'information, et l'un des membres fondateurs du Club27001, une association dédiée à la promotion du standard ISO 27001. Il est certifié CISA, CISSP et ISO 27001 PA.*

Trust Fabric : Oracle met en musique son offre de sécurité

Avec cette dénomination, l'éditeur positionne son portefeuille comme une pile intégrée complète adaptée aux enjeux soulevés par des environnements IT hybrides où la notion de périmètre n'a plus grande pertinence.

Par Valéry Marchive

UN PORTEFEUILLE DE SÉCURITÉ INTÉGRÉ « *conçu pour l'ensemble de l'écosystème IT, Oracle et tiers, en local comme en mode* SaaS, PaaS *et* IaaS ». C'est ainsi que Troy Kitch, directeur sénior d'Oracle en charge du marketing des produits de sécurité, présente Trust Fabric, le fruit d'une stratégie agressive et menée au pas de charge au cours des dernières années, par l'éditeur.

Dans un billet de blog, il détaille un modèle qui s'articule « *autour de la notion de protection des données critiques sensibles et s'appuie sur sept couches* » : protection des données (avec chiffrement, masquage, et contrôle des accès), gestion des clés de chiffrement, gestion des identités et des accès, visibilité des usages cloud et prévention des fuites de données, sécurité des applications exposées en ligne, sécurité de l'infrastructure cloud, supervision et analytique de sécurité appliquées au cloud. Le tout saupoudré d'une pincée d'apprentissage automatique pour « *détecter et réagir rapidement aux menaces* ».

Comme le souligne Eric Olden, vice-président et directeur général d'Oracle en charge de la sécurité et de l'identité en mode cloud, il s'agit de proposer une approche complète de la sécurité des environnements IT à l'heure du cloud et de l'hybridation, centrée sur la protection des données en lien avec les identités.

« Il s'agit de proposer une approche complète de la sécurité des environnements IT à l'heure du cloud et de l'hybridation, centrée sur la protection des données en lien avec les identités. »

— Eric Olden VP et DG sécurité et identité Oracle.

En fait, avec Trust Fabric, Oracle offre une marque à sa pile de sécurité construite avec le rachat de Palerra, à l'automne 2016. Avec cette opération, l'éditeur s'offrait une passerelle d'accès cloud sécurisé (CASB) basée sur les API proposées par les fournisseurs de services SaaS, PaaS et IaaS, et offrant un éventail fonctionnel complet : analyse des risques et des comportements des utilisateurs, réponse aux incidents, gestion de cas, intégration de renseignement sur les menaces, ou encore gestion de la remédiation basée sur des approbations. À l'époque, Oracle affichait clairement ses ambitions : rapprocher la plateforme de Palerra de son offre de gestion des identités et accès en mode cloud (IDaaS) – Oracle Identity Cloud Service – pour « *fournir une protection complète des utilisateurs, applications, APIs, données et infrastructures* ».

L'an dernier, l'éditeur a franchi une étape supplémentaire, avec l'annonce d'un nouveau service cloud de supervision et d'analyse de sécurité, combinant les fonctionnalités d'un système de gestion des informations et des événements de sécurité (SIEM) et analyse comportementale (UEBA, User and Entity Behavior Analytics), tant des hôtes que des utilisateurs. Il manquait à l'édifice un nom. C'est aujourd'hui fait.

Et ce nom n'est sûrement pas innocent. Le terme « trust », ou confiance en anglais, renvoie ainsi au concept d'architecture dite zero-trust, ou sans confiance, régulièrement mis en avant comme l'alternative à une approche périmétrique de la sécurité dépassée, à l'heure d'environnement ouverts, massivement interconnectés ou tout au moins de plus en plus hybrides. A la manière de l'approche BeyondCorp que Google applique graduellement, depuis plusieurs années, à l'ensemble de son infrastructure. ■

VALÉRY MARCHIVE, *Rédacteur en chef adjoint LeMagIT.*

Avec ScaleFT, Okta s'apprête à dépoussiérer le contrôle d'accès

Le spécialiste de la gestion des accès vient de s'offrir cette jeune pousse qui met en avant le concept d'architecture sans confiance pour renforcer le contrôle des accès aux ressources des systèmes d'information.

Par Valéry Marchive

CE N'EST PROBABLEMENT PAS UN RACHAT TRÈS ONÉREUX, et annoncé au milieu de la torpeur estivale, il pourrait presque passer inaperçu. Mais sur le fond, l'acquisition de ScaleFT par Okta constitue un tournant important.

Créée en 2015 par quatre anciens de Rackspace, la jeune pousse a levé moins de 3 M$ pour développer une plateforme de gestion des contrôles d'accès inspirée de l'initiative BeyondCorp de Google.

Dévoilée début 2015, cette initiative vise à renoncer au concept de périmètre protégé, et réputé sûr, pour miser sur une approche en profondeur de la

sécurité. Elle repose en particulier sur une gestion du contrôle d'accès extrêmement granulaire et basée sur des niveaux de confiance. Ceux-ci reflètent en fait le niveau croissant de sensibilité des ressources – applications, services et infrastructures sujets au contrôle d'accès. Un niveau de confiance minimum requis est associé à chacune de ces ressources.

« Le niveau de confiance associé à une entité tentant d'accéder à une ressource est déterminé par un système dédié qui analyse et annote l'état de l'appareil en continu. »

Le niveau de confiance associé à une entité tentant d'accéder à une ressource est déterminé par un système dédié qui analyse et annote l'état de l'appareil en continu. C'est lui qui affecte donc à un appareil le niveau de confiance maximal auquel il est susceptible d'accéder en fonction de son état.

Un dispositif de contrôle d'accès se charge alors de faire respecter les règles définies par les administrateurs, en fonction des informations contenues dans le registre d'inventaire des entités. Ce contrôle d'accès s'étend à tous les composants de l'infrastructure susceptibles de jouer un rôle de passerelle vers les ressources : commutateurs réseau, serveurs SSH, proxies Web, etc.

En fait, dans cette approche, toute entité – définie comme « *une collection de composants physiques et virtuels qui agit comme un ordinateur* » – est potentiellement suspecte. Le niveau de confiance qui lui est attribué est ainsi évalué et ajusté en continu.

Depuis plusieurs années maintenant, Google applique graduellement cette approche à l'ensemble de son infrastructure. ScaleFT avait l'ambition de l'ouvrir à n'importe quelle entreprise, pour le contrôle d'accès à ses ressources sensibles, qu'il s'agisse de serveurs ou simplement d'applications Web.

La plateforme développée par la jeune pousse assure donc l'évaluation du niveau de confiance à accorder à un équipement ou un utilisateur en continu. Un reverse-proxy positionné devant chaque ressource couverte se charge de décider, pour chaque requête, si le niveau de confiance présenté est satisfaisant, compte tenu des règles définies par les administrateurs. Les échanges nécessaires pour l'attribution des niveaux de confiance sont assurés par un bus de messages Kafka. Chaque requête acceptée induit la génération d'un certificat ou d'un jeton unique à durée de vie extrêmement limitée.

La plateforme s'intègre avec n'importe quel système fournisseur d'identités, comme un annuaire Active Directory ou LDAP, et supporte également SAML. Elle supporte également l'intégration avec des systèmes de gestion de journaux d'activité, et d'informations et d'événements de sécurité (SIEM).

Dans un billet de blog, Frederic Kerrest, co-fondateur d'Okta, explique avoir l'ambition d'apporter, avec ScaleFT, « *des capacités d'authentification continue de nouvelle génération pour sécuriser les accès aux serveurs, depuis le cloud jusqu'au sol* ». Ce qui ne manque pas de s'inscrire dans la stratégie de l'éditeur en faveur du contrôle d'accès conditionnel.

Dans un communiqué de presse, le spécialiste du contrôle d'accès en mode cloud (IDaaS) indique que ses clients pourront ainsi profiter d'une plateforme « *qui fournit aux employés une expérience transparente et permet aux équipes IT d'améliorer la posture de sécurité de leur entreprise* ». ■

VALÉRY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

Comment Google joue la carte de la sécurité en profondeur

Depuis 2015, le géant du Web montre la voie. Il a tourné le dos à l'approche périmétrique traditionnelle de la sécurité au profit d'un système de contrôle d'accès adaptatif hautement granulaire. Un exemple, même s'il n'est pas facile à suivre.

Par Valéry Marchive

L'APPROCHE DE GOOGLE, en matière de sécurité, est clairement affichée depuis début 2015 : la sécurité périmétrique a fait son temps. Non pas qu'il faille ouvrir son système d'information à tous les vents, mais une approche en profondeur de la sécurité est devenue indispensable. Le message est connu, répété à l'envi, mais dans la pratique, toutefois, rares sont les entreprises ayant réellement entrepris de refondre ainsi la sécurité de leur SI. Alors l'exemple n'est probablement pas malvenu.

C'est toute la logique autour de laquelle s'articule l'initiative BeyondCorp de Google détaillée début 2016, et qui mise sur une sécurité en profondeur et basée sur la confiance. Et l'infrastructure cloud du géant du Web apparaît traduire cette approche, à tous les niveaux.

UNE CONFIANCE RÉÉVALUÉE EN CONTINU

Cela commence par le contrôle des accès. Là, comme l'expliquent des ingénieurs de chez Google dans un

rapport d'étape « BeyondCorp, design to deployment at Google », tout repose sur des niveaux de confiance « *représentant les niveaux croissants de sensibilité* » des ressources. Celles-ci sont les applications, les services et les infrastructures « *sujettes au contrôle d'accès* » : « cela peut inclure n'importe quoi depuis les bases de connaissance en ligne jusqu'aux bases de données financières. » Un niveau de confiance minimum requis est associé à chacune de ces ressources.

Le niveau de confiance associé à un appareil tentant d'accéder à une ressource est déterminé par un système dédié, le Trust Inferer, qui « *analyse et annote l'état de l'appareil en continu* ». C'est lui qui affecte donc à un appareil le niveau de confiance maximal auquel il est susceptible d'accéder en fonction de son état et, en conséquence, « *le VLAN qu'il pourra utiliser sur le réseau interne* ». Ces informations sont enregistrées dans un registre dédié et actualisées à chaque changement d'état de l'appareil.

Un dispositif de contrôle d'accès se charge alors de faire respecter les règles définies par les administrateurs, en fonction des informations contenues dans le registre d'inventaire des appareils. Ce contrôle d'accès s'étend à tous les composants de l'infrastructure susceptibles de jouer un rôle de passerelle vers les ressources : commutateurs réseau, serveurs SSH, proxies Web, etc.

TOUT EST SUSPECT

L'un des points clés de cette approche est la suspicion généralisée. Le terme appareil recouvre ainsi un ensemble assez vaste : « *un appareil est une collection de composants physiques et virtuels qui agit comme un ordinateur, alors qu'un hôte est une photographie de l'état d'un appareil à un instant donné* ».

« L'un des points clés de cette approche est la suspicion généralisée. »

Ainsi, le service d'inventaire « *contient des informations sur les appareils, leurs hôtes correspondants, et sur les décisions de confiance appliquées aux deux* ». Ce service se nourrit de nombreuses sources, à commencer par l'annuaire Active Directory, ainsi que les outils d'administration Puppet et Simian (développé en interne par Google, sur la base du projet Munki, et reversé à la communauté du libre), mais également par « *des agents sur les appareils, les systèmes de gestion des configurations et les systèmes de gestion des actifs corporate* ». Il s'alimente également auprès de scanners de vulnérabilités, d'autorités de certification et d'éléments d'infrastructure réseau « *comme les tables ARP* ».

Au total, Google indiquait (toujours dans ce même document BeyondCorp), en 2016, avoir ingéré un total de plus de 80 To de données sur les appareils connectés à

son infrastructure. Et pas question, là, de droit à l'oubli : « *conserver les données historiques est essentiel pour nous permettre de comprendre le cycle de vie de bout en bout d'un appareil donné, suivre et analyser les tendances à l'échelle de la flotte complète, et réaliser des audits de sécurité ainsi que des enquêtes* ». Mais cela ne s'arrête pas là.

UNE NOTION D'ENTITÉ ÉTENDUE

Début 2017, dans un document (« Présentation de la sécurité sur l'infrastructure de Google » en français), les équipes de la Google Cloud Platform décrivaient ainsi une architecture où les serveurs « *utilisent diverses technologies pour s'assurer qu'ils exécutent la bonne pile logicielle* ». Ce sont là des signatures cryptographiques qui sont à l'œuvre « *pour les composants de bas niveau tels que le BIOS, le bootloader, le noyau et l'image de base du système d'exploitation* », afin de les valider à chaque démarrage ou mise à jour. Qui plus est, « *ces composants sont tous durcis, contrôlés et construits par Google* ». Chaque machine dispose en outre de son identité unique « *utilisée pour identifier les appels aux API depuis et vers les services d'administration de bas niveau de la machine* ».

La même approche s'applique au niveau de chaque service déployé sur l'infrastructure, authentification et autorisation « *au niveau applicatif, pour les communications inter-services* ». Les services disposent ainsi de leur propre identité et sont contrôlés dans une logique d'IAM comme peuvent l'être des utilisateurs : « *le propriétaire d'un service peut utiliser les capacités de gestion des accès fournies par l'infrastructure pour spécifier exactement quels autres services peuvent communiquer avec lui* ». Et l'infrastructure met également à disposition des services une liste de contrôle d'accès centralisée et des bases de données de groupes pour permettre aux services « d'implémenter leurs propres contrôles d'accès granulaires personnalisés lorsque c'est nécessaire ».

« Le propriétaire d'un service peut utiliser les capacités de gestion des accès fournies par l'infrastructure pour spécifier exactement quels autres services peuvent communiquer avec lui. »

— Équipe Google Cloud Platform.

UN CHIFFREMENT GÉNÉRALISÉ

Sans surprise après ces premiers éléments, les communications entre services sont elles-mêmes chiffrées, chaque service pouvant déterminer son propre niveau d'exigence en la manière. Et les communications sortant des centres de calcul et passant sur un WAN sont

chiffrées de manière indépendante. Des accélérateurs cryptographiques matériels doivent à terme permettre d'étendre cette approche à l'intérieur des centres de calcul.

La gestion des autorisations est en outre assurée en tenant compte du contexte de l'utilisateur final : l'appel d'un premier service à un second demandant l'accès aux données d'un utilisateur est ainsi assorti d'un ticket temporaire de permission utilisateur.

Les services de stockage de données peuvent être configurés pour tirer profit du service de gestion de clés récemment présenté par Google pour assurer le chiffrement des données au niveau applicatif et ainsi les protéger d'éventuels codes malveillants au niveau du firmware des équipements de stockage. Mais les capacités natives de chiffrement des disques sont également activées. Les disques devant partir au rebus sont effacés « *en utilisant un processus à plusieurs étapes qui inclut deux vérifications indépendantes* ». Les appareils qui échouent à ce processus sont physiquement détruits, sur site.

UN DÉPLOIEMENT PROGRESSIF

Sans surprise, Google s'est donc engagé dans une mise en œuvre graduelle de son initiative BeyondCorp, en commençant par un « *sous-ensemble de passerelles avec un service de méta-inventaire intérimaire* », et « *une petite poignée de sources contenant majoritairement des données prescrites* » - des données gérées manuellement, comme la propriété d'un appareil, par opposition aux données observées et remontées par l'infrastructure.

Parallèlement, le géant du Web a travaillé au développement d'une solution de méta-inventaire capable de fonctionner à plus grande échelle sans introduire de latence susceptible de pénaliser les utilisateurs : « *le service d'inventaire d'appareils agrège des données de plus de 15 sources, ingérant 30 à 100 changements par seconde en fonction du nombre d'appareils générant activement des données* ».

La corrélation de ces données, nécessaire à l'établissement des niveaux de confiance, s'est avérée particulièrement « complexe », poussant les ingénieurs de Google à « *utiliser un certificat X.509 comme identifiant persistant d'appareil* ». De quoi leur permettre de disposer de deux fonctionnalités clés : « *si le certificat change, l'appareil est considéré comme un nouvel appareil, même si tous les autres éléments d'identification restent les mêmes* ». Et s'il est installé sur un autre appareil, les algorithmes de corrélation détectent une anomalie et « *dégradent le niveau de confiance en réponse* ». ■

VALÉRY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

Le passage au cloud hybride, l'occasion d'adopter une approche «zero-trust» ?

Une table ronde organisée par Rohde & Schwarz Cybersécurité, fin mai 2018, autour du thème du cloud hybride, a naturellement été l'occasion d'aborder la question de la sécurité de tels déploiements et de l'opportunité qu'ils peuvent représenter pour adopter graduellement une approche sans confiance de la sécurité.

Par Valéry Marchive

QUI DIT CLOUD HYBRIDE, dit cloud public. Alors d'emblée, Laurent Seror, Pdg d'Outscale, veut remettre les choses à leur place : « *on part souvent du principe que le cloud privé est plus sécurisé que le cloud public. Mais une salle des coffres de banque, comparable à un cloud public, est plus sécurisée qu'un coffre-fort chez soi. De mon point de vue, ce que vous mettez en cloud privé, c'est ce que vous n'avez pas sécurisé. Et ce que vous mettez en public, c'est ce que vous voulez sécuriser. Là, il y a des experts qui investissent – parce que c'est leur image, c'est leur business – dans des niveaux de sécurité qui sont les meilleurs du marché, pour pouvoir ne jamais perdre de données clients* », au moins du fait de leur responsabilité. Et de prendre l'agence américaine du renseignement, la NSA, en exemple : « *elle met ses données dans un cloud opéré par Amazon, parce que c'est plus sûr que ce qu'elle sait faire en interne* ».

Pas question cependant, pour Laurent Seror, de se lancer les yeux fermés, ou de se reposer entièrement sur ses partenaires : « *oui, il faut avoir une approche globale et considérer qu'il y a des vulnérabilités inconnues. On peut prendre en exemple Heartbleed, ou encore Spectre et Meltdown. On ne peut pas faire confiance. D'où l'importance, notamment du chiffrement* ». Mais n'importe comment, là non plus : « *avec un système D-Wave, le chiffrement RSA avec une clé sur 2048 bits est cassable en quelques secondes. Il faut changer ses systèmes de chiffrement. Qui a des systèmes quantiques dans la salle ? Personne. Mais les gros fournisseurs cloud, comme Google ou IBM, en ont un ou deux. Car le commun des mortels ne peut pas faire les investissements* ».

Regis Karakozian, responsable des offres cloud de Telehouse, souligne pour sa part que « *les certifications que l'on affiche nous amènent* » à adopter des approches zero trust. Mais attention : « *ce qu'il faut bien mesurer, c'est jusqu'où l'on va* ». Et de s'interroger sur la stratégie développée par Google : « *je voudrais savoir ce que ce sera devenu dans 10 ans, et si c'est encore exploitable. Cela paraît compliqué. Je pense qu'il faut des niveaux [d'exigence] différenciés* ».

De son côté, Grégory Mauguin, directeur de la sécurité chez Linkbynet, rappelle que « *la sécurité a tout de même un coût* ». Et dès lors, certaines approches très complètes, très strictes, du sol au plafond, « *ce n'est pas forcément possible ni nécessaire. Il faut aligner la sécurité sur les besoins, sur la criticité des données. Il n'est pas pertinent de faire des investissements démesurés lorsque les données ne le nécessitent pas* ». *Et concrètement, « nous personnalisons généralement les cloud privés avec des mesures de sécurité dont la valeur médiane généralement acceptée est de 8 % du coût du projet* », indique Grégory Mauguin.

« Il faut aligner la sécurité sur les besoins, sur la criticité des données. Il n'est pas pertinent de faire des investissements démesurés lorsque les données ne le nécessitent pas. »

— Grégory Mauguin, directeur de la sécurité chez Linkbynet.

Dans un contexte règlementaire de plus en plus contraignant, entre directive NIS et règlement général de protection des données (RGPD), notamment, selon Laurent Seror, « la seule solution, pour ceux qui ne veulent pas investir, c'est d'aller vers le cloud public ».

Las, comme le rappelle Maître Iteanou, dans le cloud public, il y a obligation d'adhérer au contrat, tandis que dans le privé, la possibilité de personnalisation s'étend au

contrat : « *il faut choisir en fonction de ses risques et d'un ensemble d'éléments très relatifs et pas absolus* ». Car le cadre réglementaire présente des exigences mais intègre une dose de flexibilité pour tenir de l'état de l'art. Et de la proportionnalité. Quoi qu'il en soit, pour Maître Iteanou, il est important de conserver à l'esprit deux tendances de l'évolution du cadre réglementaire : d'une part, elle traduit une volonté de responsabilisation de l'ensemble de la chaîne et, d'autre part, mais conséquence de ce premier point, « *demain, on peut être victime et responsable* ».

Chez Rohde & Schwarz Cybersécurité, Stéphane de Saint Albin trouve le concept développé par Google « *très intéressant* » car il « *consiste à partir du principe que le périmètre a disparu et que c'est la relation entre utilisateur et donnée qui compte et qu'il faut envisager dans sa globalité. Cela peut créer des défis d'administration, mais le concept correspond à une réalité : les utilisateurs ont des droits qui sont définitifs ou temporaires, mais que l'on peut décider d'ajuster selon des éléments de contexte. Et si l'on n'envisage pas la sécurisation du SI de cette façon, en tenant compte de la flexibilité offerte par les usages modernes, on rate quelque chose. D'autant plus que le cloud permet de supporter cela, pour peu que l'on ait le minimum d'intelligence dans le système pour automatiser ce qui peut l'être* ». ■

VALÉRY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

Quand le contrôle de l'identité s'étend à de multiples entités

Assurer en profondeur la sécurité des données et des applications, c'est contrôler qui y accède, et avec quel appareil, en affichant quelle posture. Le marché l'a compris et joue la carte de l'intégration des technologies.

Par Valéry Marchive

C'ÉTAIT EN 2016. Gartner entrevoyait une convergence entre IDaaS, la gestion des accès en mode cloud, les passerelles de sécurisation des accès cloud (CASB), et la gestion de la mobilité d'entreprise (EMM) – au moins, car celle-ci s'étend de plus en plus à la gestion unifiée des postes de travail (UEM). Frédéric Kerrest, co-fondateur d'Okta, entrevoyait la même perspective : « *une grande intégration est en cours, parce qu'accéder à des services cloud depuis le Web ou un terminal mobile, c'est pareil* ».

VMware a tenté de construire une offre combinant IDaaS - avec Identity Manager - et UEM - avec Airwatch. Mais il s'est depuis rapproché d'Okta. Et pour le directeur des

activités françaises de ce dernier, Nicolas Petroussenko, c'est bien simple : « *eu égard à la complexité du sujet de l'IDaaS, [VMware] a décidé de s'appuyer sur un acteur spécialisé, en l'occurrence nous. Cela signifie une sorte d'abandon à terme de leur solution, au profit de la nôtre* ».

« Eu égard à la complexité du sujet de l'IDaaS, [VMware] a décidé de s'appuyer sur un acteur spécialisé, en l'occurrence, nous [Okta]. »

— Nicolas Petroussenko directeur activités françaises, Okta.

Pour autant, il est difficile de distinguer là une tendance de fond venant nier la complémentarité de ces domaines. Car avec ces trois briques que constituent IDaaS, EMM et CASB, il s'agit de faire une chose : contrôler l'accès aux données et aux applications par les utilisateurs, en tenant compte des terminaux qu'ils utilisent.

Le fait est qu'Okta mise sur l'intégration avec des produits tiers, plutôt que de chercher à construire à une pile complète. Une direction dans laquelle beaucoup se sont toutefois engagés de manière déterminée.

IBM ne regarde pas dans une autre direction. Le rachat de Lighthouse Security Group en 2014 lui a permis d'acquérir une brique d'IDaaS. Mais c'est en septembre 2016 que le groupe a présenté Cloud Security Enforcer, une offre intégrant justement CASB, IDaaS et prévention des menaces. La brique d'EMM ? IBM en dispose depuis la fin 2013, avec la solution cloud MaaS360 de FiberLink.

Mais il faut aussi compter avec Forcepoint qui a, début 2017, complété son offre avec le rachat de Skyfence, le CSAB d'Imperva, ou encore Symantec, qui s'est offert Blue Coat, après que ce dernier eut consolidé CASB et passerelle de sécurité Web (SWG). En parallèle, l'éditeur n'a censé de renforcer son offre de protection des terminaux, notamment dans le domaine de la mobilité, avec le rachat d'Appthority, mais aussi, en 2017, de Skycure, ou encore celui de Fireglass, pour le déport du rendu Web et de l'e-mail. Le tout a d'ailleurs été récemment consolidé dans le service Web Security Service.

Et que dire de Cisco, qui s'est offert son CASB avec CloudLock et dispose, dans son portefeuille, d'une solution d'EMM, avec Meraki, et d'une autre de gestion des accès avec ISE (Identity Services Engine). Sans compter Oracle, avec Palerra, et MobileIron qui a également mis un pied sur le marché des CASB début 2016. Plus récemment, c'était Fortinet.

Et bien sûr, il y a Microsoft, qui ne semble pas voir les choses autrement. Son patron, Satya Nadella, voit l'IDaaS comme un composant clé à l'heure du cloud et de la mobilité, un véritable pivot encourageant les entreprises à consommer plus de services cloud signés Microsoft.

Ainsi, le patron de l'éditeur expliquait fin janvier 2016 aux investisseurs que « *si vous déployez Exchange online, vous avez Azure AD, et de là, l'extension naturelle est la suite EMS avec administration de terminaux pour tous vos terminaux mobiles, et aussi Advance Threat Protection* ». Des « synergies », donc, et une complémentarité naturelle que Microsoft prévoit encore de pousser en avril, avec Microsoft Cloud App Security, une offre de passerelle d'accès Cloud sécurisé (CASB) basée sur la technologie d'Adallom.

Longtemps, Centrify c'est construit autour d'une double offre d'EMM et d'IDaaS. Aujourd'hui, il doit se recentrer sur la gestion des comptes à privilèges et déporter le reste de ses activités dans une entité distincte, Idaptive. Mais pas question pour celle-ci d'abandonner l'EMM pour autant. ■

VALÉRY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

Thales adopte une architecture sans confiance pour l'administration de son SI

Le groupe ne badine pas avec la cybersécurité. Et comme en témoigne son intégration des outils de Centrify dans son environnement d'administration, ce n'est pas qu'un vœu pieu, loin s'en faut.

Par Valéry Marchive

DRASTIQUE. C'est le qualificatif qu'a employé Nicolas Alamome, responsable des annuaires techniques chez Thales, lors d'un atelier organisé aux Assises de la Sécurité, pour décrire le « *corpus d'exigences* » qui entoure le contrôle de l'administration des hôtes du système d'information. Et à écouter la description de l'architecture retenue, le terme retenu n'apparaît pas trop fort.

L'objectif affiché a de quoi paraître simple : « *centraliser la gestion des machines, Windows et* Unix », tout en homogénéisant les règles applicables aux différentes entités du groupe, en suivant les pratiques de référence préconisées par l'Agence nationale pour la sécurité des systèmes d'information (Anssi) et Microsoft, et bien sûr en traçant toutes les activités d'administration pour

réussir à savoir « *qui a fait quoi sur quoi* ». La traduction pratique apparaît en revanche bien moins triviale que l'énoncé. Et cela d'autant plus qu'il n'est pas question d'affecter l'expérience des administrateurs, ne serait-ce que pour ménager leur productivité.

Tout d'abord, l'administration de l'ensemble du parc doit se faire « *à partir d'un cœur de confiance, une solution d'administration conçue spécifiquement* ». Mais tous les administrateurs doivent pouvoir travailler de la même manière, et cela malgré le recours à des comptes dédiés – pas question, chez Thales, de laisser trainer des comptes administratifs génériques. Les habilitations sont

« Qui aura le droit de faire quoi sur quoi, et pour combien de temps. »

— Nicolas Alamome, responsable des annuaires techniques Thales.

également gérées étroitement, sans chèque en blanc, en somme – « *qui aura le droit de faire quoi sur quoi, et pour combien de temps* ».

Qui plus est, il faut compter avec une ségrégation forte des populations d'administrateurs : « *nous n'avons*

« Nous n'avons pas envie qu'un administrateur d'annuaire puisse aller administrer un serveur ou un poste de travail. »

— Nicolas Alamome

pas envie qu'un administrateur d'annuaire puisse aller administrer un serveur ou un poste de travail ». Découlent de cette segmentation rigoureuse « *plusieurs dizaines de profils et de sous-profils d'administration afin de gérer les droits de manière très fine* ».

Pour ne rien gâcher, les administrateurs n'ont pas de droits d'administration sur leurs systèmes… « *afin d'empêcher la primo-infection des postes d'administration* ». Et la connexion à la production avec des comptes dédiés à l'administration est interdite, tant via la gestion des habilitations que par le biais de règles réseau.

Un réseau physique dédié à l'administration est déployé sur chacun des sites du groupe, avec des services d'infrastructure qui lui sont spécifiques et indépendants de ceux du SI de production « *qui ne servent qu'à administrer nos forêts d'administration* », explique Nicolas Alamome. Et d'ajouter que « *deux types de postes d'administration dédiés et durcis sont rattachés à des forêts*

d'administration – une pour les annuaires et les privilèges, et une autre pour les ressources ».

C'est dans cet environnement que Thales a déployé la solution de Centrify, pour notamment gérer les délégations de privilèges et assurer une expérience homogène de l'administration sur l'ensemble des ressources administrées, quelles qu'elles soient et quel que soit le système d'exploitation concerné. « *Avec Windows et Centrify, nous avons réussi à positionner des droits fins* ». Mais cela vaut aussi pour le monde Unix où « *des zones Centrify assurent le lien entre identifiant Windows et Unix. Le serveur génère des attributs Unix pour gérer la correspondance entre identité et objet Active Directory* ».

Nicolas Alamome reconnaît de bon cœur que « *tout cela ne s'est pas fait en un mois. Le modèle est tel, que l'intégration a demandé beaucoup de travail conjoint entre équipes d'annuaire et Centrify* ». Mais les administrateurs ont été impliqués dès le départ pour accélérer l'adoption et l'éditeur « *nous a accompagnés dans la conception et la mise en œuvre, notamment pour l'expérience des administrateurs* ». Des difficultés ont été rencontrées et ont nécessité l'intervention de l'ingénierie de Centrify, par exemple « *pour le SSO avec Kerberos* », les développements nécessaires ont été réalisés : « *au final, l'intégration est parfaite, et nous n'avons pas eu à transformer notre modèle d'intégration* ». ■

VALERY MARCHIVE *Rédacteur en chef adjoint LeMagIT.*

TechTarget Security Media Group

INFORMATION SÉCURITÉ

RÉDACTEUR EN CHEF Cyrille Chausson

RÉDACTEUR EN CHEF ADJOINT Valéry Marchive

COORDINATRICE ÉDITORIAL Pascale Roncin

ÉDITEURS Bill Crowley et Byrony Seifert

ABONNEMENT

www.lemagit.fr

TechTarget - LeMagIT, 22 rue Léon Jouhaux, 75010 Paris