LES DOSSIERS TECHNIQUES

SHADOW IT À L'ÈRE DU CLOUD

Mars 2023

CLUSIF

L'article L. 122-5 de la propriété intellectuelle n'autorisant pas les représentations ou reproduction intégrale, ou partielle, faites sans le consentement de l'auteur ou de l'ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d'une source licite et strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », analyses et courtes citations dans un but d'exemple et d'illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du code de la propriété intellectuelle.

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Jean-Marc	**JACQUOT**	LEXAURA
Baptiste	**HAMON**	SSI CONSEIL

Les contributeurs :

Xavier	**AIT-YAHIATENE**	SYNETIS
Ludovic	**BARBIER**	UNEO
Linley	**BRASSE**	ITEC SECURITY
Valentin	**JANGWA**	JUMIO CORPORATION
Maxly	**MADLON**	C2S BOUYGUES
Hervé	**SCHAUER**	HS2
Eric	**TETELIN**	MINISTERE DE LA TRANSITION ECOLOGIQUE

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Selon le NIST (*National Institute of Standards and Technology*), le terme « Shadow IT » désigne l'utilisation de matériel, logiciels ou services SaaS (*Software as a Service*) dans le cadre du travail par un ou plusieurs membres du personnel, et ce, à l'insu du service informatique.

Un exemple typique de Shadow IT est l'utilisation, par un département de l'entreprise, d'une solution SaaS pour effectuer une tâche critique, une souscription réalisée sans accord au préalable du service informatique. La direction des systèmes d'information (DSI) ne se rend généralement compte de l'existence de ce système qu'au moment où l'accès au dit service est perdu ou encore s'il fait l'objet d'une violation, mettant ainsi en péril la mission critique.

Dans la même lignée, le « Bring Your Own Cloud » (BYOC) fait son apparition en suivant la même philosophie que le « Bring Your Own Device » (BYOD), mais cette fois en rapport au cloud. Celui-ci s'invite peu à peu dans l'entreprise à l'insu de la DSI, entraînant un problème de maîtrise du système d'information (SI).

De plus, comme le confirme la cartographie des attaques majeures en 2021 éditée par l'ENISA[1], les menaces cyber actuelles visent tout particulièrement les utilisateurs. Or, dans un environnement cloud, garder le contrôle de leur comportement est encore plus difficile. Avec un cloud sans réelle limite entre vie personnelle et professionnelle, la maîtrise de ces comportements devient essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des données de l'entreprise.

Ce document a pour but de faire le point sur le phénomène de Shadow IT dans le cloud en abordant le sujet de façon pragmatique, en commençant par un état des lieux, puis en donnant des éléments de réponse pour gérer cette problématique tant sur les aspects techniques et fonctionnels que de gouvernance.

2 Réalités du Shadow IT à l'ère du cloud

2.1 Quelques exemples

La facilité de souscription, qu'elle soit gratuite ou non, à des services cloud (IaaS, PaaS, SaaS, aaS) favorise le Shadow IT. Voulues ou non, ces souscriptions peuvent remettre en cause la gouvernance ou la cohérence de l'ensemble d'un SI et en augmenter la surface d'attaque.

Avec l'arrivée des services cloud, le Shadow IT trouve un environnement particulièrement propice à son expansion. Les exemples qui suivent témoignent de cette facilité : le cloud est synonyme d'un accès aux services rapide et simple. Il dote l'entreprise d'une grande capacité d'évolution en termes de ressources et d'infrastructure pour s'adapter au besoin du moment (traitement, stockage, etc.), et ce avec une mise en œuvre facile. Des avantages qui poussent à la pratique du Shadow IT.

Les exemples qui suivent témoignent de cette facilité.

Exemple 1

L'utilisation dans le cadre professionnel d'une solution de partage de données dans le cloud, solution qui ne soit pas gérée par l'organisation (par exemple WeTransfer, Dropbox, Microsoft® OneDrive, Google Drive, NAS/messagerie, etc.) est une source potentielle de fuite d'information.

[1] https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_fr.pdf

Exemple 2

L'absence de maîtrise des accès au travers d'un proxy pour les employés en mobilité (télétravail, déplacement, etc.) facilite la souscription à des services cloud à l'insu de la DSI.

Exemple 3

Autre possibilité, le développement d'un programme informatique (destiné au cloud ou « On Premise ») par une personne en interne. Le programme est destiné à améliorer le fonctionnement d'un service ou de toute l'organisation en répondant à des besoins métier. Dans ce cas, la pérennité et la cohérence des données manipulées par le programme seront difficiles à garantir, menant à une perte de maîtrise du SI.

Exemple 4

Un utilisateur connecté sur un outil de partage de fichiers personnels et professionnels sur le même poste de travail se trompe lors d'une copie de données en transférant des données professionnelles sur son outil de partage de fichiers personnels.

2.2 Panorama des menaces

La 5e édition du « Threat Report » de l'éditeur Netskope[2] donne un aperçu de la place prise par le Shadow IT au sein des entreprises. Quelques chiffres clés :

97 % des applis cloud utilisées au sein des entreprises relèvent du Shadow IT :

- Le Shadow IT s'est accentué lors du premier confinement en 2020. Les employés, se sentant à l'abandon, ont cherché de nouvelles façons de travailler ensemble. Dans de nombreux cas, la DSI, dépassée par l'ampleur de l'événement, n'a pu rattraper la situation ou n'a toujours pas connaissance de ces nouveaux usages.

97 % des utilisateurs de Google Workspace ont autorisé au moins une application tierce à accéder à leur compte Google professionnel :

- L'utilisation de certains « plug-ins » permet une nouvelle forme de Shadow IT. Cet usage d'extensions permet potentiellement l'accès aux données sensibles des utilisateurs sans qu'ils en soient forcément conscients.
- La plupart des applications modernes telles que Google Workspace, Microsoft 365® ou Salesforce permettent l'utilisation des extensions. Ce sujet, non ou mal maîtrisé, peut rapidement devenir le cauchemar d'un DSI. L'exemple le plus connu est celui de CamScanner, un outil de reconnaissance optique de caractères (OCR) utilisé plus de 100 millions de fois. Ce dernier contenait du code malveillant et servait de « cheval de Troie ».

68 % des malwares proviennent d'applis cloud :

- Au second trimestre 2021, 68 % de tous les téléchargements de malwares se faisaient à partir d'applications cloud. Et 66,4 % de ces téléchargements étaient initiés à partir d'applications de stockage dans le cloud.

Trois fois plus de données transférées vers un compte personnel, 30 jours avant un départ :

- Les employés sur le départ téléchargent trois fois plus de données vers des applis personnelles au cours des 30 derniers jours de leurs contrats, notamment par le biais de Google Drive et Microsoft® OneDrive.
- Avec la vague de départs volontaires provoquée par la crise sanitaire, le risque de voir les données d'entreprise être exfiltrées de cette façon prend une toute nouvelle.

Dans le rapport de NinjaOne sur le secteur public en 2022[3], 49 % des employés utilisent pour leur travail des logiciels ou des outils cloud non approuvés par l'organisation.

---

[2] https://www.netskope.com/resources/cloud-reports/cloud-and-threat-report-july-2021

[3] https://www.ninjaone.com/public-sector-shadow-it/

3 Enjeux du Shadow IT à l'ère du cloud

3.1 Causes

Afin de pouvoir gérer correctement le Shadow IT, il apparaît comme primordial de comprendre et d'identifier les causes qui amènent certaines personnes à contourner la DSI en utilisant des outils ou technologies sans signalement ni validation. Il n'y a pas vraiment de profil particulier pour les responsables de ces contournements : un utilisateur comme un membre de la DSI ou encore du comité exécutif peut en être à l'origine.

3.1.1 Côté utilisateur

Individuellement, de nombreuses raisons peuvent pousser une personne à faire, consciemment ou non, du Shadow IT.

Par exemple, on remarque que certains utilisateurs doués en informatique et/ou spécialisés dans un domaine métier particulier auront une tendance naturelle à se créer ou à acquérir, voire à détourner, des outils afin d'améliorer la productivité. Le développement logiciel est une formidable opportunité pour exprimer son désir d'innover.

Il existe également un phénomène générationnel, la nouvelle génération ayant pris l'habitude d'utiliser des outils cloud (SaaS) dans leurs études, dans leur quotidien. Arrivés en entreprise, ils continuent cet usage (BYOC). La frontière est floue pour cette génération concernant le SI d'entreprise et les risques associés. Des actions de sensibilisation et de rappel des règles sont donc souvent nécessaires.

Également à l'origine de cette pratique du Shadow IT, l'utilisation au quotidien d'outils validés, mais qui ne sont pas réellement adaptés pour le travail demandé. Une situation qui poussera certains à se lancer dans le développement de leur propre solution.

Une richesse de l'offre de services bien documentée et une profusion de solutions de formation incitent également tout un chacun à souscrire à des services cloud.

Un service métier peut faire le choix du Shadow IT, notamment lorsqu'il lui est difficile de formaliser son besoin (problème de rédaction du cahier des charges, par exemple). Il arrive par ailleurs qu'une personne n'arrive pas à faire remonter à ses supérieurs hiérarchiques le besoin ressenti et pourrait dans ce cas préférer prendre le raccourci offert par le Shadow IT. Il pourra alors se passer des processus d'arbitrage, de réalisation ou de déploiement… si son service dispose du budget adéquat.

Lorsque le BYOD est autorisé dans l'organisme, ce dernier constitue une porte d'entrée supplémentaire au Shadow IT. En effet, les utilisateurs disposent nativement d'applications installées sur leurs périphériques ne faisant pas partie des programmes autorisés par l'organisme au sein duquel ils évoluent.

3.1.2 Côté direction du système d'information (DSI)

C'est un exercice difficile que de répondre aux nouveaux besoins des utilisateurs du fait de la cadence d'arrivée de nouveaux usages à une fréquence soutenue, tout en maintenant le patrimoine informatique existant. Les exigences du métier, notamment en termes de délai de livraison ou de performance, sont souvent difficiles à atteindre sauf à avoir des équipes surdimensionnées et un budget illimité. La DSI ne peut parfois pas répondre aux requêtes des utilisateurs du fait de l'existence d'un certain nombre de dysfonctionnements. Par exemple, une difficulté de maîtrise de l'urbanisation du SI, l'absence d'un catalogue détaillant les fonctionnalités des applications par manque de moyens ou encore une trop grande complexité des procédures de validation interne sont autant de bonnes raisons pour la DSI de repousser les demandes des utilisateurs faute de pouvoir les satisfaire.

Certaines DSI peuvent, par exemple, se cantonner à un choix restreint d'outils pour simplement rester dans une situation maîtrisée (ou par manque de temps et de ressources pour assurer la veille). D'autres fois, c'est le choix de la méthode projet qui peut poser problème en n'étant tout simplement pas adapté à la situation (Cycle V vs mode Agile).

Les DSI n'offrant pas de référentiel permettant d'accéder facilement aux services proposés ou ayant mis en œuvre des processus trop compliqués pour lancer de nouveaux projets inciteront tout autant les utilisateurs à se tourner vers le Shadow IT.

L'ergonomie de ces solutions cloud, souvent plus modernes et mieux pensées que les solutions informatiques traditionnelles, fait également beaucoup d'ombre aux services historiques proposés par la DSI.

Une DSI à l'écoute des attentes utilisateur aura plus de chance de limiter la tendance générale à se tourner vers le Shadow IT plutôt que d'imposer des outils sans laisser d'autres possibilités.

3.1.3 Comité exécutif

Sensibiliser le comité exécutif aux enjeux du Shadow IT est un pan important de la stratégie à adopter. En effet, le comité exécutif a malheureusement parfois tendance à sous-estimer l'importance des problématiques cyber et des impacts potentiels du fait certainement, d'un manque d'information sur le sujet.

Concernant l'aspect budgétaire, les services cloud sont associés à une dépense de fonctionnement généralement perçue comme moins chère que les traditionnelles dépenses d'investissement habituellement proposées par la DSI. Le faible niveau de dépenses peut permettre aux responsables de service d'y souscrire sans validation de la DSI.

3.2 Impacts

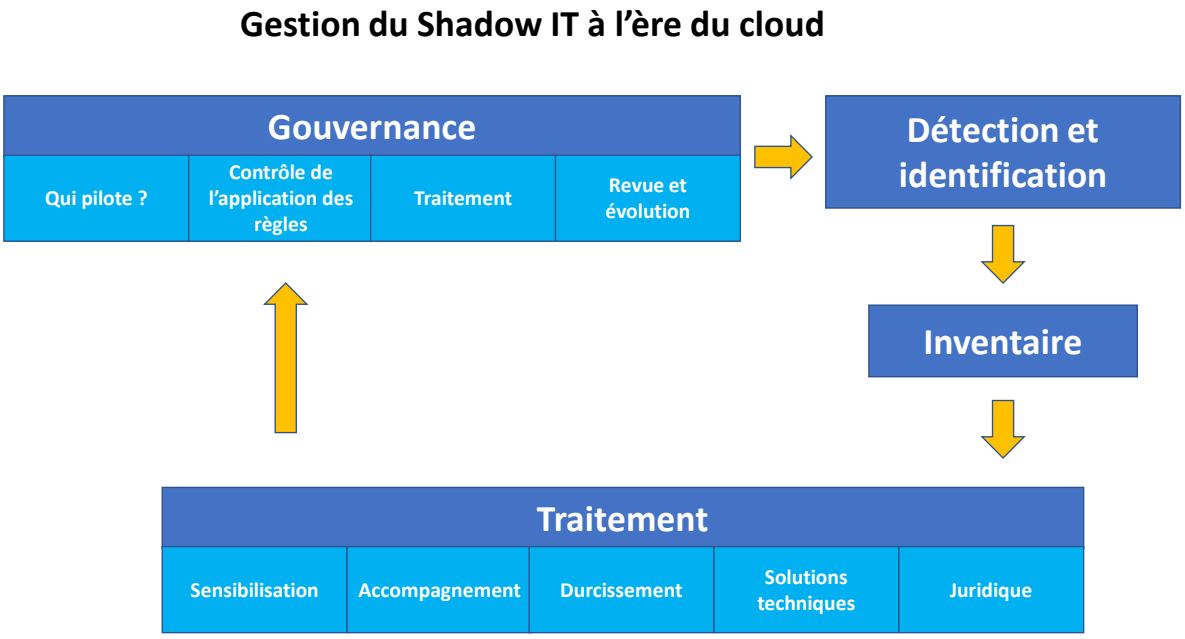
Les impacts liés au Shadow IT sont de différents types. Ils peuvent être multiples et ne pas toujours être liés à une problématique de sécurité :

- Augmentation de la surface d'attaque, l'utilisation d'un service ou exposé sur Internet et ne bénéficiant pas des mesures de surveillance et de sécurité pourrait conduire, par exemple, à une exfiltration de données non détectée car non surveillée.
- Dégradation de l'efficacité du plan de continuité/reprise d'activité : en cas d'application du plan, les éléments déployés en Shadow IT n'y seraient pas inclus, entraînant son échec.
- Dégradation du fonctionnement du SI due à l'ajout d'éléments hors gouvernance :
    - faille de sécurité,
    - performance (réseau, système...).
- Altération/fragilisation du patrimoine informationnel de l'entreprise.
- Perte de maîtrise d'une solution inconnue de la DSI du fait du départ de son exploitant.
- Augmentation de la complexité du SI (problème de synchronisation de base de données) et évolution non ou mal maîtrisée.
- Coûts non maîtrisés (souscription par un utilisateur sans validation de la DSI en utilisant, par exemple, sa carte bancaire professionnelle ou en faisant une note de frais)
- Sécurité/risques non maîtrisés (*i.e.* utilisation d'une solution d'échange de fichiers externalisée sans application des règles de la politique de sécurité des systèmes d'information [PSSI], notamment sur la gestion de l'authentification et du cycle de vie de la donnée).
- Perte de la couverture par l'assurance si une clause exclut le Shadow IT.

- Perte financière et atteinte de la réputation liée à une attaque réussie à cause du Shadow IT à comparer avec le coût d'une solution cloud validée par la DSI.
- Amende CNIL concernant une fuite de données personnelles due à leur insertion dans une solution de Shadow IT. Plus largement, le non-respect des lois et réglementations (RGPD, NIS, LPM, DORA, etc.) entraîne des sanctions pénales et/ou financières.
- Une gestion des droits d'accès aux ressources informatiques en fonction des arrivées et départs de collaborateurs biaisée.

4 Gestion du Shadow IT à l'ère du cloud

4.1 Schéma récapitulatif



4.2 Gouvernance

La définition d'une stratégie au niveau de l'organisation permet de choisir des règles communes et la direction adoptée en termes d'usage. Suivant la sensibilité des données, l'usage de services cloud peut être restreint ou interdit. Ces règles doivent être édictées dans la charte d'utilisation du SI et/ou dans la PSSI. Un catalogue de services peut y être référencé et ce dernier devra être revu régulièrement afin d'intégrer des offres adaptées aux nouveaux usages.

Au-delà des règles établies par l'organisme que les utilisateurs doivent respecter, il est important de comprendre pourquoi ces services non référencés ont été adoptés par les utilisateurs. Pour rappel, cela pourrait être :

- l'arrivée de nouveaux besoins nécessitant une mise en place rapide ;
- l'btention de meilleures performances qu'avec un outil existant ;

- la méconnaissance du catalogue de services (si l'entreprise en a déjà établi un) ;
- une démarche lourde et complexe pour bénéficier d'un service du catalogue ;
- des services tiers existants adaptés au besoin des utilisateurs.

4.2.1 Qui pilote ?

Selon le contexte, il s'agit généralement d'un service de type gestion des risques, conformité ou sécurité opérationnelle, voire une personne qui aurait la charge de contrôler la bonne application des règles et également d'établir une « comitologie » appropriée avec tous les acteurs concernés.

Cette approche est nécessaire pour avoir une vision à jour et partagée par tous des nouveaux usages, des outils déjà utilisés et non référencés et des plans de remédiation nécessaires pour les intégrer si besoin.

Doivent figurer dans cette comitologie tous les acteurs de l'entreprise, les responsables métier, la DSI, les responsables juridiques, les responsables des ressources humaines (RH).

In fine, le but est d'intégrer un plan de remédiation à la stratégie du SI de l'organisme et de le partager avec tous les utilisateurs afin qu'ils adhèrent au processus de décision.

Une priorisation peut être établie en fonction de la sensibilité des données (médicales, personnelles, stratégiques, etc.).

4.2.2 Contrôle de l'application des règles

Afin que les services non supportés et cependant utilisés puissent être détectés ou référencés, il est conseillé de pratiquer des audits et/ou contrôles périodiques :

- Une enquête réalisée auprès des utilisateurs permettant à la fois de consigner leurs besoins et qui aura aussi pour but de les sensibiliser et de les responsabiliser sur le risque de certains usages.
- Une détection effectuée par un outillage spécifique (plusieurs éditeurs du marché ont développé ce type de solution) appliqué au SI afin d'obtenir une cartographie exhaustive des services utilisés.

4.2.3 Revue et évolution

Il est important de ne pas négliger l'incidence de la mise à jour en mode continu de la politique de gouvernance afin de prendre en compte au fur et à mesure les modifications de stratégie de l'organisme, souvent réalisées en fonction de l'arrivée de nouveaux usages et/ou besoins.

4.3 Détection et identification

La découverte des applications Shadow IT utilisées au sein d'une organisation est complexe : les équipes informatiques n'ont généralement à disposition que peu d'outils pour résoudre ce problème.

Habituellement, la détection du Shadow IT est basée sur les quatre axes suivants :

- le réseau ;
- les serveurs et postes de travail ;
- les utilisateurs ;
- l'analyse financière (budgets, bilan/compte de résultat, notes de frais, flux de trésorerie, dépenses cartes bancaires, etc.).

Néanmoins, un des meilleurs moyens pour « découvrir » l'utilisation de ces applications reste la communication orale (machine à café, réunion formelle ou informelle, etc.).

L'une des façons d'initier cette communication est d'engager la discussion régulièrement avec

les utilisateurs et de les associer à la mise à jour du schéma directeur informatique afin de prévoir de potentielles évolutions du SI. Une manœuvre qui facilite l'intégration des besoins actuels et futurs de l'organisation. Cela peut se traduire par :

- Entretiens service par service pour connaître leur satisfaction en matière de temps de réponse du service informatique par rapport aux besoins exprimés par les directions opérationnelles. Cette démarche, qui est en réalité un sondage et un recensement (identification *a posteriori*), doit être présentée comme une démarche avec deux objectifs :
  - identifier les évolutions à prévoir dans les applications métiers ;
  - identifier des besoins non couverts par une application proposée par la DSI et qui ont été partiellement, voire totalement couverts par la direction opérationnelle.
- Audit organisationnel révélant l'usage de solutions non approuvées par la DSI ou ne respectant pas la politique de sécurité officielle.
- Mise à jour du registre des traitements RGPD (**règlement général sur la protection des données**) cette mise à jour est généralement l'occasion de découvrir d'éventuelles applications Shadow IT traitant des données personnelles.

Cependant, la communication orale ne peut pas être la seule source de détection du Shadow IT, il faut également s'équiper d'outils permettant de mettre en place une sorte de radar à 360°.

D'un point de vue technique, les éléments suivants peuvent être utilisés pour cette détection :

- Analyse des logs (ou utilisation d'un SIEM) / détection en temps réel :
  - firewall ;
  - DNS ;
  - SWG/Proxy ;
  - EDR, XDR ;
  - outil d'inventaire ;
  - CASB, SASE.
- Scan réseau/tests d'intrusions.
- EASM (*External Attack Surface Management*) : surveillance des noms de domaines, bases whois et marques, liés à l'organisation (création d'un nom de domaine par un utilisateur ou un service)

En ce qui concerne les serveurs et les postes de travail, il faut également chercher à identifier les applications qui ne sont pas répertoriées dans le portefeuille d'applications de la DSI. Ce travail d'identification reste difficile, car il nécessite d'étudier l'ensemble des applications installées, par exemple, à l'aide d'un agent réalisant l'inventaire. Par ailleurs, en étudiant les connexions sortantes d'un équipement, il est possible de déterminer si une application cloud non répertoriée est utilisée professionnellement.

Grâce aux EDR (*Endpoint Detection & Response*), il est possible d'identifier les applications installées. L'EDR remonte également des informations sur les connexions réalisées par un équipement donné et donc identifie les applications utilisées par les employés d'une entreprise. Il est à noter qu'il est possible pour l'EDR de bloquer depuis sa console centrale n'importe quelle application si nécessaire.

Le CASB (*Cloud Access Security Broker*), protège quant à lui l'accès aux services cloud. Il offre également une fonction de découverte de ces applications grâce aux informations en provenance des pare-feux et serveurs mandataires (proxy) à travers l'analyse des données de connexion.

4.4 Inventaire

Un inventaire des actifs préalablement classés reste un élément essentiel. Il est donc primordial de pouvoir dresser régulièrement un inventaire exhaustif afin de détecter le plus rapidement possible des écarts de type Shadow IT. Différentes possibilités s'offrent à la personne en charge pour effectuer ces inventaires :

- L'intégration de la sécurité dans les projets permet d'identifier les besoins et de circonscrire les usages en fonction des règles de sécurité.
- Une analyse des traces d'une Secure Web Gateway, d'un proxy, du DNS du pare-feu peut s'avérer nécessaire sous certaines conditions. En effet, les logs d'un proxy ou d'une SWG seront pertinents à la condition :
  - qu'un agent logiciel soit installé sur le poste de travail,
  - de passer par une connexion à travers un VPN en limitant les accès à Internet sans ce VPN.
- Mise en place d'un CASB, qui permettra d'établir une cartographie des usages et de détecter les outils considérés comme du Shadow IT.
- Mise en œuvre d'un service de CTI (Cyber Threat Intelligence) avec un inventaire externe régulier.
- Mise à niveau des analyses de risques intégrant les nouveaux usages (risques en matière de sécurité des données, de conformité réglementaire, de pérennité des fournisseurs, etc.).
- Classification des services de Shadow IT.
- Consultation de l'urbanisation du SI pour dresser une cartographie afin de constater les écarts avec le référentiel.

Il pourrait être intéressant de confronter l'inventaire effectué avec une cartographie des usages des utilisateurs pour pouvoir alerter ceux-ci et leur proposer une alternative. Dans ce cas, une comitologie pourra être mise en place pour passer en revue les points les plus sensibles ou les comportements à risque.

4.5 Traitement

La question du traitement du Shadow IT est intrinsèquement liée à la capacité de souplesse et d'agilité de la DSI. D'autres services de l'organisation, tels que les services achats (relations fournisseurs) et juridiques (élaboration des contrats) peuvent collaborer avec la DSI et l'avertir si celle-ci n'avait pas été impliquée.

Il convient également de trouver le bon équilibre entre l'accompagnement – via le fait d'étoffer le catalogue de services et/ou d'applications de la DSI, par exemple – et les blocages techniques qu'il est possible d'implémenter au sein du SI.

4.5.1 Sensibilisation

Les employés auront moins tendance à avoir recours au Shadow IT s'ils sont informés des risques que cette pratique fait courir à l'entreprise. Quelles que soient les mesures techniques de protection mises en œuvre, la sensibilisation reste primordiale, idéalement sous forme de formation continue.

4.5.2 Accompagnement

Les utilisateurs doivent pouvoir accéder facilement à un catalogue des services autorisés et pris en charge officiellement dans l'organisation, ou à défaut obtenir une assistance rapide de la DSI pour trouver le service répondant à leurs besoins.

S'ils ont déjà identifié une solution en dehors du catalogue de services, ils doivent pouvoir

demander l'autorisation de l'utiliser au travers d'un processus formalisé. Cette demande doit faire l'objet d'une validation par la hiérarchie ainsi qu'une étude au niveau de la DSI afin de vérifier qu'un service existant ne réalise pas déjà la même fonction. Si ce n'est pas le cas, la DSI étudie alors la mise en place du nouveau service (contrat, vérification de la sécurité, etc.). Il est important que ce processus soit rapide –ou à défaut, que son état d'avancement soit régulièrement communiqué aux utilisateurs potentiels – afin d'éviter que ces derniers contournent les politiques en attendant la réponse de la DSI.

Par ailleurs, ce processus obligera les personnes demandeuses à bien formuler leur besoin avec l'aide de la DSI.

Ce processus devra non seulement faire l'objet d'un traitement rapide, mais devra également adresser les problématiques suivantes :

- analyse du besoin et identification d'éventuelles solutions déjà présentes et/ou validées par la DSI permettant d'y répondre ;
- évaluation de la pertinence de l'outil vis-à-vis des orientations stratégiques de l'organisation, en particulier, étude et validation de la compatibilité de la solution demandée avec les objectifs de sécurité et de protection des données ;
- analyse d'impact sur les processus métier et, le cas échéant, adaptation des procédures dégradées et autres éléments relatifs à la continuité d'activité ;
- analyse des risques.

Ce processus devra idéalement s'appuyer sur une équipe dédiée pour un gain d'agilité : chef de projet DSI, RSSI, DPO, architecte/urbaniste. Cela permettra l'arbitrage sur les aspects suivants dont l'alignement stratégique :

- Intégration de la solution dans le catalogue DSI avec une étude d'opportunité pour proposer cette solution à d'autres directions métiers ou d'autres utilisateurs :
    - intégration à l'inventaire des services de la DSI,
    - intégration dans les processus de mise à jour et suivi de vulnérabilités/veille,
    - autres.
- Étude d'urbanisation afin de s'assurer d'une intégration optimale (non-redondance de données, cohérence des données, etc.).
- Refus éclairé d'utiliser la solution, mais avec une proposition alternative permettant de répondre au besoin (soit solution déjà existante, soit recherche d'une autre solution).

Ci-après, quelques exemples concrets d'accompagnement des utilisateurs :

- Plateformes SaaS ou décorrélées du SI (Trello, WhatsApp, etc.) : discuter avec les utilisateurs afin de comprendre leurs besoins, puis évaluer la possibilité d'offrir un service identique, ou s'en approchant, mais qui serait intégré au SI.
- Macro Excel : malheureusement très difficiles à détecter, dans ce cas les phases de sensibilisation, d'échange et d'accompagnement des utilisateurs deviennent toutes primordiales.

4.5.3 Durcissement

Une partie du traitement du Shadow IT peut être envisagé en utilisant des techniques ou des outils permettant le durcissement (refus d'installation de clients locaux sur les postes, blocage firewall/proxy, etc.) qui seront détaillés dans le prochain chapitre.

Une autre façon de renforcer le respect des règles relatives au Shadow IT peut passer par la mise en place d'éventuelles sanctions à l'encontre de ceux qui enfreindraient ces règles comme explicité dans le chapitre Juridique.

4.5.4 Solutions techniques

Il existe plusieurs types de services permettant de faciliter le traitement de la sécurité dans le

cloud et de lutter contre le Shadow IT dans le cloud.

Les solutions d'inventaire de type :

- **Portail d'applications de l'organisation (SSO)** : permet notamment aux utilisateurs d'accéder facilement à l'ensemble des applications validées par l'organisation tout en garantissant un bon niveau de sécurité (identification, authentification multifacteur, gestion des droits, etc.)
- **Solution d'inventaire** : permet d'identifier les différents services/solutions « as a Service ».
- **Solution de surveillance externe (CTI)** : service réalisant des scans en continu des noms de domaines ressemblant à ceux de l'organisation.

Solutions de blocage fondées sur le concept **SASE** :

Ce concept permet le paramétrage, l'application et le contrôle des règles de sécurité définies par la gouvernance au travers d'une console centralisée qui pilote tout un ensemble de sous-services réseaux et sécurité **(**CASB, FWaaS, SWG, ZTNA, EDR, etc.). Ces briques peuvent être utilisées pour la lutte contre le Shadow IT dans le cloud :

- **ZTNA** : permet de réaliser un contrôle d'accès depuis les équipements de l'organisation (client lourd) et donc force l'utilisation du SWG ;
- **SWG** : permet d'identifier les utilisateurs et de filtrer l'accès aux services (URL) et transmet les logs au CASB ;
- **CASB** : permet d'identifier un service en Shadow IT et de lui attribuer une stratégie de cybersécurité (blocage total ou partiel, réorientation vers une application du catalogue, intégration au catalogue, etc.) ;
- **FWaaS** : permet de réaliser des blocages d'URL, adresses IP et services (par exemple, autorisation de télécharger mais pas de téléverser) identifiés comme source de Shadow IT ;
- **EDR** : permet de détecter et bloquer toutes solutions installées sur le poste de travail de l'utilisateur et d'analyser les connexions réseau vers d'éventuels services Shadow IT.

4.5.5 Juridique

Afin de limiter au maximum l'utilisation de services ou ressources non déclarés, un chapitre spécifique peut être ajouté à la charte d'utilisation du SI et/ou à la PSSI afin d'essayer de responsabiliser juridiquement les utilisateurs tout en dégageant la responsabilité de l'organisation. Des sanctions peuvent être prévues en cas de non-respect de cette règle.

Il est important de noter que l'absence de contrôle du Shadow IT dans le cloud peut engendrer des sanctions juridiques sur l'entité ou son responsable (par exemple, stockage de données personnelles à l'étranger sans informations de l'utilisateur ou divulgation de données médicales/sensibles sanctionnées par le RGPD, etc.).

5 Pour aller plus loin

5.1 Comment convaincre le comex ?

Il parait pertinent d'impliquer le comité exécutif (comex) dans la gestion de la sécurité de l'information, et notamment dans la gestion du Shadow IT. Il s'agit d'expliquer les enjeux et risques que son utilisation peut avoir sur l'organisme, en insistant sur :

- les enjeux : utilisation de nouvelles applications, télétravail, bénéfices, opportunités, flexibilité, agilité ;
- les risques : pertes opérationnelles et financières, dégradation de l'image, perte de réputation.

De manière plus concrète, cette démarche peut être confortée par un état des lieux de la capacité de résilience de l'organisme, complété d'actions de sensibilisation et de démonstrations. Plus généralement, il s'agit d'assurer la promotion du plan d'action de l'équipe cybersécurité.

Par ailleurs, le Shadow IT ne pouvant pas être pris en compte dans le cadre d'un PCA/PRA, la survenance d'un incident sur ce périmètre peut mener à une perte de données et/ou un arrêt de service. Ce fait peut conduire à une crise ou venir amplifier un incident en cours.

5.2 Shadow IT au sein de la DSI

Le fait que la plupart des membres de la DSI aient des droits d'administration sur leurs postes, les serveurs et/ou sur des applications cloud font qu'il est important de ne pas oublier ni négliger la DSI dans le traitement du Shadow IT.

Les membres de la DSI ayant bien souvent les compétences nécessaires pour installer et/ou mettre en fonction rapidement un service, il est d'autant plus critique de bien les sensibiliser. Il est important de différencier une expérimentation d'un logiciel dans le cadre d'un test vis-à-vis d'une utilisation plus régulière le faisant basculer dans le Shadow IT.

Ceci est particulièrement dangereux dans le cas des développeurs ou des personnes en charge de l'exploitation qui pourraient déployer des équipements ou des applications utilisés en production sans qu'ils soient référencés.

Cela peut également concerner des outils utilisés au sein de la DSI en elle-même, par exemple pour gérer des schémas d'architecture. Si la personne utilise un outil cloud pour générer ces schémas et qu'elle ne met à disposition qu'un export dans un format non modifiable, alors il sera nécessaire de refaire tous les schémas en partant des exports non modifiables après son départ si cela n'a pas été correctement géré en amont. Par ailleurs, la confidentialité de ces schémas d'architecture est compromise par le stockage dans le cloud.

On pourrait aussi s'interroger sur le risque de Shadow IT porté par la sous-traitance (utilisation d'outils de la société de sous-traitance au lieu de ceux du client final).

6 Conclusion

Le Shadow IT est un sujet qui mériterait d'être correctement traité par les organisations. La méconnaissance des outils de la DSI et les préférences des utilisateurs ne correspondant pas forcément au catalogue conduisent souvent à une situation complexe à gérer d'un point de vue sécurité.

La mise sur le marché d'une offre pléthorique de services cloud, facilement accessibles – sur le plan du coût et de la technique, un navigateur suffit – a été sans aucun doute le catalyseur

du développement du Shadow IT. Une tendance déjà présente, mais largement amplifiée avec l'arrivée des services cloud. Cette tendance était déjà présente avant l'arrivée des services cloud mais l'accroissement des risques cyber, complété par l'expansion du nomadisme et le développement des activités professionnelles sur smartphone amplifie ce phénomène.

Le moteur principal du Shadow IT est souvent l'absence de réponse considérée comme adéquate aux besoins utilisateurs dans un contexte toujours plus exigeant en termes de productivité et d'objectifs à atteindre, qu'ils soient au niveau individuel ou métier.

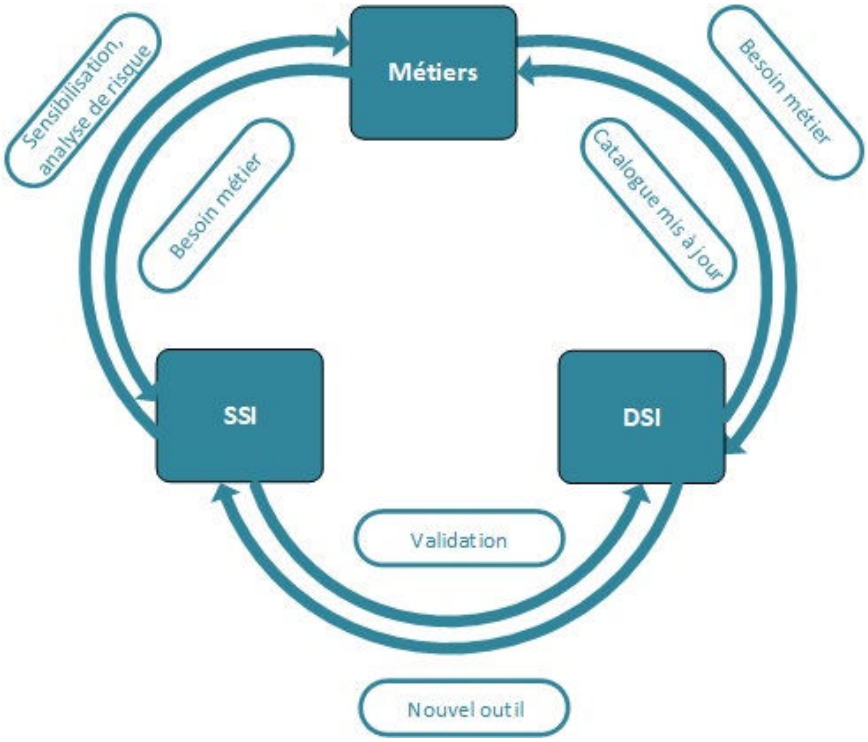
Les conséquences sont nombreuses et pas nécessairement à effet immédiat. On pourrait citer, entre autres, un risque d'accroissement de la surface d'attaque cyber, une non-optimisation des coûts humains par défaut de mutualisation des développements métiers, des fuites d'informations synonymes de fuites de savoir-faire pouvant mettre en péril un organisme.

Au-delà d'une seule posture de gendarme qui conduirait à rendre encore plus obscur le Shadow IT dans le cloud, la DSI pourrait instaurer une stratégie qui commencerait par une gouvernance du SI axée sur la satisfaction du besoin utilisateur. En complément, la mise en place d'une comitologie permettrait d'échanger sur ces besoins, les prioriser en tenant compte de la stratégie globale de l'organisme, répartir équitablement les ressources entre les différentes entités métier et surtout conduire à la planification d'une réponse qui soit acceptée par toutes les parties prenantes.

Ces règles à fixer collectivement ne doivent pas être uniquement l'apanage des fonctions supports traditionnelles (DRH, DAJ, DAF, etc.), les acteurs de la SSI assurent également un rôle important de veille et d'offreurs de solutions en réponse aux besoins émis.

Pour cela, la SSI dispose d'une palette d'outils étendue comme les solutions intégrées à une architecture de type SASE par exemple, encore en voie de développement mais dont la mise en œuvre est de mieux en mieux appréhendée.

Une bonne gestion du Shadow IT dans le cloud entraînera une collaboration plus étroite entre la DSI, la SSI et les directions métiers. Cette relation tripartite pourrait aboutir à une nouvelle chaîne de valeurs *(voir schéma ci-dessous)* au sein de l'organisme.



7 Glossaire

ADSL (*Asymmetric Digital Subscriber Line*) : Technologie permettant d'accéder à Internet en utilisant le réseau (et particulièrement le câble) de la téléphonie fixe.

BIA (*Business Impact Analysis*) : Analyse en partant d'un sinistre (par exemple, perte d'un immeuble) pour définir la stratégie de continuité d'activité.

CASB (*Cloud Access Security Broker*) : Point d'application de la stratégie de sécurité (sur site ou dans le cloud) qui intervient entre les utilisateurs et les fournisseurs de services cloud. Il combine et associe les stratégies de sécurité d'entreprise lorsque des utilisateurs accèdent à des ressources dans le cloud.

Cloud ou **cloud computing** (Informatique en nuage) : correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels) via Internet.

CTI (*Cyber Threat Intelligence*) : Discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberespace.

DAJ : Direction des affaires juridiques.

DORA (*Digital Operational Resilience Act*) : Règlement européen qui a pour objectif d'améliorer la résilience opérationnelle informatique des acteurs des services financiers en mettant en place un cadre de gouvernance et de contrôle interne spécifique (ICT *Risk Management Framework*)

DLP (*Data Leak/Loss Prevention*) : Fait référence à un ensemble de techniques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies.

DPO (*Data Protection Officer*) : Délégué à la protection des données. C'est le chef d'orchestre chargé de la mise en conformité et du maintien du RGPD au sein de l'organisation.

DNS (*Domain Name Server*) **:** Serveur de nom de domaine qui fait la relation entre un nom, une adresse réseau et un service.

DSI : Directeur des systèmes d'information ou direction des systèmes d'information.

EASM (*External Attack Surface Management*) : Pilotage de tous les actifs informationnels de l'organisation accessibles directement sur Internet et, dès lors, susceptibles de faire l'objet de tentatives de compromission par des entités malveillantes.

EDR (*Endpoint Detection and Response*) : Désigne une catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information. Initialement dénommée « *Endpoint Threat Detection & Response* » (ETDR), en 2015 Gartner a réduit l'expression en « *Endpoint Detection and Response* » (EDR).

ENISA : Agence européenne en charge de la sécurité des réseaux et de l'information

FWaaS (*Firewall as a Service*) : Pare-feu hébergé sur le cloud par un fournisseur tiers. « Pare-feu dans le cloud » est un autre terme pour ce type de service. Un FwaaS n'est pas un appareil physique, et il n'est pas hébergé dans les locaux d'une organisation**.**

FinOps : Approche, méthodologie, contraction des termes finance et opération, qui vise à monitorer et optimiser les coûts en matière de cloud computing.

IaaS (*Infrastructure as a Service* – infrastructure en tant que service) : Un fournisseur délivre à ses clients un accès à l'utilisation au stockage, au réseau, aux serveurs et à d'autres ressources informatiques dans le cloud.

LPM (Loi de programmation militaire) : Texte destiné à établir le programme des dépenses militaires sur une période de quatre, cinq ou six ans. La loi de programmation militaire 2014-2019 impose aux opérateurs d'importance vitale le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent.

NIS (*Network Information Security*) : Adoptée par les institutions européennes en juillet 2016, la directive NIS a pour objectif d'assurer un certain niveau de sécurité pour les réseaux et systèmes d'information des infrastructures critiques et sensibles des pays membres de l'Union européenne.

NIST (*National Institute of Standards and Technology*) : Agence du département du commerce des États-Unis dont le but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.

On-Premise (littéralement « dans les locaux » ou « sur site ») : Modèle d'utilisation ou de licence s'appliquant à tout ou partie d'un SI et/ou d'une infrastructure lorsque cette dernière est physiquement située dans les locaux de l'entreprise.

PaaS (*Platform as a Service* – plateforme en tant que service) : Un fournisseur de services fournit un environnement cloud dans lequel les utilisateurs peuvent construire et mettre à disposition des applications. Le fournisseur fournit l'infrastructure sous-jacente.

RGPD (règlement général sur la protection des données) : Règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

SaaS (*Software as a Service* – logiciel en tant que service) : Un fournisseur de services offre des logiciels et des applications via internet. Les utilisateurs s'abonnent à un logiciel et y accèdent par le web ou par les API du fournisseur.

SASE (*Secure Access Service Edge*) : Concept basé sur le cloud qui fournit des services réseau et de sécurité destinés à protéger les utilisateurs, les applications et les données.

SIEM (Security Information & Event Management) : Outil de gestion et de corrélation d'événements informatiques permettant de détecter et d'analyser les menaces afin de répondre rapidement aux incidents de sécurité.

SSO (*Single Sign On*) : Méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.

SWG (*Secure Web Gateway* – passerelle web sécurisée) : Solution de cybersécurité généralement mise en œuvre sous la forme d'un service cloud entre les utilisateurs et le Web.

VPN (*Virtual Private Network*) : Système permettant de créer un lien direct entre des points distants, qui isole leurs échanges en chiffrant le flux du reste du trafic se déroulant sur des réseaux de télécommunication publics

XDR (*eXtended Detect and Response*) : Collecte et met automatiquement en corrélation des données sur plusieurs couches de sécurité : email, end point, serveur, charge de travail sur le cloud et réseau.

Tour Eria
5 rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr