[Introduction] [Résultats] [Analyse] [Conclusion]

Introduction

Pour créer et administrer des machines virtuelles dans un IaaS public, les fournisseurs mettent à disposition de leurs clients des interfaces Web accessibles via le protocole sécurisé https. Ces interfaces sont des éléments particulièrement sensibles car elles sont accessibles publiquement sur Internet et leur compromission permettrait à un attaquant de prendre le contrôle total de nos machines dans le Cloud.

Le problème est que le protocole https utilise des fonctions cryptographiques (SSL/TLS), historiquement développées par Netscape au début des années 90 et que ces fonctions cryptographiques ont subi ces dernières années de nombreuses attaques : attaque sur la renegociation, attaque sur RC4, collision MD5, BEAST, CRIME, POODLE, etc… Il y a également d'autres problèmes non pas liés à la cryptographie SSL elle-même mais plutôt à de mauvaises implémentations logicielles comme par exemple le bug dans OpenSSL (Heartbleed) mais aussi celui dans la librairie open source utilisée par Apple (goto fail). Et les problèmes ne sont pas terminés comme en témoigne l'annonce de 8 nouvelles vulnérabilités dans OpenSSL le 8 janvier 2015 dont l'une d'elles permet de réaliser l'attaque SSL/TLS du moment : FREAK (Factoring attack on RSA-Export Keys).

Nous avons donc décidé de vérifier si les interfaces d'authentification de 4 fournisseurs IaaS français (OVH, Numergy, Cloudwatt et Outscale) étaient correctement paramétrées d'un point de sécurité. En d'autres termes, les fournisseurs nationaux respectent-ils les bonnes pratiques de sécurité concernant les flux chiffrés SSL/TLS.

Nos tests ont porté exclusivement sur la gestion des flux chiffrés. Il ne s'agit en aucun cas d'un audit de sécurité, ni d'un test d'intrusion mais tout simplement d'une vérification de la configuration SSL/TLS. Les vulnérabilités spécifiques aux applications Web (XSS, CSRF, SQL injection, etc…) n'entrent pas dans le périmètre de notre étude.

Pour ce faire, nous avons utilisé sur www.ssllabs.com, un outil gratuit et disponible publiquement sur Internet proposé par Qualys. Il a été développé par Ivan Ristic, le concepteur du pare-feu applicatif mod_security.

Son utilisation est très simple. On soumet le nom du serveur à tester à ssllabs et le service effectue une vérification approfondie de la configuration SSL/TLS de la cible et délivre une note globale de sécurité sous forme d'une lettre de A à F.

Il faut ensuite interpréter les résultats de la façon suivante :

Excellente configuration SSL/TLS
Aucune vulnérabilité connue n'est exploitable

Mauvaise configuration SSL/TLS
Une ou plusieurs vulnérabilités peuvent compromettre la session

Très mauvaise configuration SSL/TLS
Une ou plusieurs vulnérabilités facile à exploiter peuvent compromettre la session

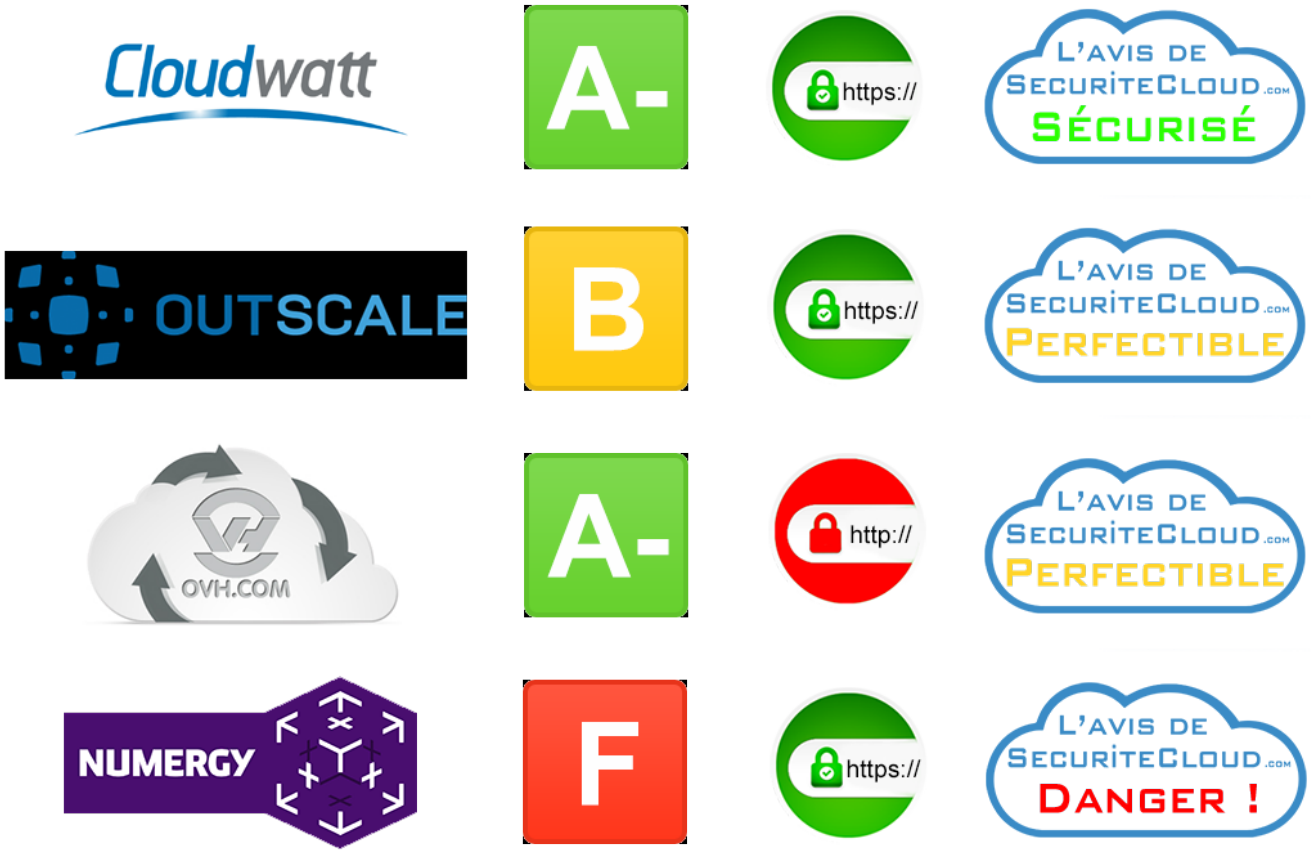
Compte tenu de la criticité de ces interfaces Web dans l'infrastructure Cloud, il va sans dire que pour un fournisseur de IaaS public, on ne s'attend pas à autre chose que la lettre A. Une note A+ serait bien sûr idéale mais un A- sera tout à fait acceptable. Les lettres B, C, D et E indiquent quelques lacunes en matière de sécurité sur lesquelles le fournisseur doit agir assez rapidement. La lettre F traduisant quant à elle de graves lacunes de sécurité sur lesquelles le fournisseur n'a apparemment réalisé aucune évaluation de sécurité et doit maintenant intervenir dans les plus brefs délais. Précisons enfin qu'il n'y a aucun coût financier pour

passer de la lettre F à la lettre A (Pas d'obligation d'acquérir un certificat SSL EV ou un boitier HSM). Il faut simplement effectuer quelques modifications dans les paramètres SSL/TLS des serveurs et l'opération ne prend que quelques minutes.

Nous avons également regardé comment les clients arrivent sur la page d'authentification du service. Si le lien vers la page d'authentification s'effectue via le site Web du fournisseur lui-même accessible uniquement en https alors l'accès à l'interface d'administration est correctement sécurisée. Par contre si l'accès se fait via une page Web en http alors la connexion sera potentiellement vulnérable. Pourquoi ? Parce qu'un site Web accessible via le protocole http signifie qu'aucune authentification du serveur n'est réalisée par le navigateur. L'attaquant peut ainsi très facilement réaliser une attaque de type Man In The Middle (MITM) et substituer ainsi la page d'authentification originale par une page frauduleuse par une simple réécriture d'URL à la volée. Une telle attaque ne pose pas aucune difficulté et plusieurs outils existent pour la réaliser comme par exemple sslsnif et sslstrip de Moxie Marlinspike.

D'autre part, tout site Web accessible via http est beaucoup plus vulnérable aux opérations de phishing toujours en raison de l'absence d'authentification du serveur. En conclusion, même si son contenu n'est pas confidentiel (chiffrement des flux non nécessaire) l'intégralité du site Web du fournisseur doit être uniquement accessible via le protocole https.

Résultat des tests



Les copies d'écran du test ssllabs.com sont disponibles sur cette page.

Analyse des résultats

Cloudwatt propose un accès correctement sécurisé pour ses services. Toutes les erreurs classiques de paramétrage d'un serveur https ont été évitées. On regrettera cependant l'absence de certificat à validation étendue (Certificat SSL EV) permettant d'accroître la confiance dans le site. En effet avec un certificat SSL, identifiable par le cadenas en vert dans la barre d'adresse, l'utilisateur connaît immédiatement quelle société se trouve derrière le site par l'affichage de son nom et du pays dans lequel elle réside. D'autre part, la délivrance d'un certificat SSL EV par une autorité de certification fait l'objet de contrôles bien plus rigoureux sur l'organisme demandeur (existence juridique de 3 ans minimum, inscription au RCS, etc…) que pour un certificat SSL classique ou seule la possession du nom de domaine peut s'avérer suffisante.

4 recommandations pour améliorer la sécurité de Cloudwatt :

- Remplacer les certificats X509 standards par des certificats SSL EV
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)

Outscale n'utilise pas non plus de certificat SSL EV. D'autre part, la configuration laisse apparaître la disponibilité du protocole SSL v3 qui est obsolète et surtout extrêmement vulnérable depuis la découverte en octobre 2014 d'une vulnérabilité dénommée POODLE.

5 recommandations pour améliorer la sécurité de Outscale :

- Corriger immédiatement les problèmes de configuration SSL/TLS sur toutes les interfaces Web en particulier désactiver le protocole SSLv3
- Remplacer les certificats X509 standards par des certificats SSL EV
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)

OVH dispose d'une configuration SSL correcte et utilise de plus des certificats SSL EV. Dommage que le site www.ovh.com soit toujours accessible via http.

5 recommandations pour améliorer la sécurité du Cloud OVH :

- Mettre l'intégralité du site accessible uniquement via https
- Pour les accès en http sur la page d'accueil, faire une redirection (HTTP redirect) vers https

- Positionner le flag HSTS (RFC 6797) pour forcer le navigateur à utiliser exclusivement https
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur

Pour Numergy, tout commence bien avec l'apparition d'un certificat SSL EV sur la page d'accueil du site (www.numergy.com). On passe ensuite sur la page d'authentification (login.numergy.com) qui elle n'utilise pas de certificat EV. Les choses se compliquent ensuite puisque l'analyse détaillée de la configuration révèle de graves lacunes de sécurité.

Pour la page d'authentification du service (login.numergy.com – 87.255.157.62), on dénombre pas moins de 7 problèmes de sécurité dont 3 très graves :

- Utilisation d'algorithme asymétrique (DH) vulnérable pour l'échange des clés
- Support d'anciens algorithmes vulnérables et exploitables via l'attaque FREAK publiée le 3 mars 2015 et découverte par Antoine Delignat Lavaud chercheur à l'INRIA.
- Le protocole SSL v3 est activé et le site est vulnérable à l'attaque POODLE sans aucune contre-mesure permettant d'en limiter l'impact (TLS_FALLBACK_SCSV)

Devant une telle situation, nous avons souhaité voir ce qui se passait derrière la page d'authentification. Nous avons donc crée un compte utilisateur avec nos informations carte bancaire pour la facturation. Pour la petite histoire, on notera que la saisie des informations carte bancaire s'effectue sur un site de paiement de la société générale (paiement.socgenactif.com) qui n'est pas non plus un modèle de sécurité puisqu'il obtient la même note (F) dans le test ssllabs.

Après le paiement, le service nous indique que notre compte a été créé et que notre mot de passe nous sera envoyé par SMS. Le mot de passe arrive et surprise, il ne tient que sur 8 caractères (6 caractères alphabétiques, un caractère numérique et un seul caractère spécial). Nous essayons alors d'utiliser ce même mot de passe pour la création d'un compte chez le concurrent (Cloudwatt), pour voir ce que ça donne :

Tiens, il semblerait que les deux fournisseurs n'aient pas la même approche sur la robustesse des mots de passe. On se dit que tout ceci n'est pas bien grave et que Numergy va évidemment nous imposer dès la première connexion de changer ce mot de passe. Et bien pas du tout ! Le mot de passe envoyé par mail est utilisable en permanence sur la console d'administration du service IaaS. Nous avons essayé l'option « j'ai oublié mon mot de passe » et une fenêtre nous demande notre e-mail et nous renvoi un nouveau mot de passe par SMS. Ce mot de passe est toujours aussi faible avec 8 caractères (dont un numérique et un spécial) et toujours permanent. Ce choix technique n'est évidemment pas judicieux quand on sait que de nombreuses vulnérabilités (sous iOS et Androïd en particulier) permettent de récupérer les SMS des smartphones. On peut par exemple récupérer en quelques secondes l'intégralité des SMS dans un iPhone lorsque celui-ci est jailbreaké. D'autre part, sur de nombreux téléphones, tout SMS reçu s'affiche en clair sur l'écran même si le téléphone est verrouillé. Pour prendre le contrôle d'un compte administrateur sur Numergy, il suffit donc de saisir l'adresse email de la victime et d'avoir l'écran de son téléphone en visuel. Scénario, on ne peut plus simple à réaliser. Ensuite, on constate que le mot de passe a été créé par Numergy et une règle de base en sécurité est qu'il ne faut jamais conserver un mot de passe généré par un algorithme inconnu. D'autre part, ce mot de passe est potentiellement connu de l'opérateur Télécom puisqu'il est envoyé par SMS et éventuellement d'un autre fournisseur Cloud si l'administrateur a synchronisé son smartphone dans le nuage. Ca fait quand même beaucoup de monde qui peuvent potentiellement avoir accès à nos données dans le Cloud Numergy sans pour autant avoir besoin de faire appel aux services du GCHQ ou de la NSA…

Tant qu'à être connecté, nous avons également testé la gestion de session. Nous ouvrons donc une session dans un navigateur que nous laissons ensuite en totale inactivité pendant plus de 4 heures. Nous revenons ensuite sur le navigateur et nous constatons que la session d'administration est toujours active.

Nous vérifions maintenant les mécanismes anti « brute force ». On tente de se connecter avec notre identifiant valide en injectant une trentaine de mots de passe erronés. L'interface réagit à chaque fois immédiatement en nous indiquant l'échec d'authentification et en nous invitant à recommencer. Aucun délai entre les mires de login et aucun CAPTCHA ne viennent perturber notre test. Nous essayons maintenant de nous connecter pour voir si notre compte n'est pas verrouillé et là encore pas de problème, ça passe. Une fois connecté, aucun message d'alerte ne vient nous informer des tentatives infructueuses que vient de subir le compte.

Pour terminer cette très rapide évaluation de sécurité, nous avons lancé deux autres tests ssllabs :

Site d'administration des machines virtuelles
mon2.numergy.com – Adresse IP : 87.255.151.7

API Rest du service Numergy
api2.numergy.com – Adresse IP 87.255.151.6

6 recommandations pour améliorer la sécurité SSL/TLS chez Numergy :

- Corriger immédiatement les problèmes de configuration SSL/TLS sur toutes les interfaces Web du Cloud Numergy et en particulier celles accessibles publiquement via Internet (login.numergy.com, mon2.numergy.com)
- Même chose avec les API Rest du service (api2.numergy.com)
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur les serveurs
- Généraliser l'usage des certificats SSL EV sur l'ensemble des serveurs

+ 7 recommandations complémentaires pour Numergy :

- Ne pas générer de mot de passe permanent pour les clients
- Imposer au strict minimum 10 caractères avec minuscules, majuscules, chiffres et caractères spéciaux
- Ne jamais envoyer un mot de passe permanent par SMS
- Gérer un timeout d'inactivité sur la session
- Intégrer un mécanisme anti brute force et en cas d'attaque verrouiller le compte et informer le client
- Proposer une option d'authentification à deux facteurs (comme le font tous les leaders mondiaux du Cloud)
- Prendre en compte plus rapidement les alertes de sécurité en provenance des clients (suivi d'incident détaillé en fin d'article)

Conclusion

Premier constat et ce n'est pas pour nous une véritable surprise : La seule société à ne pas être certifiée ISO 27001, Cloudwatt, est celle qui obtient la meilleure note de sécurité. Rappelons encore une fois qu'une certification ISO 27001 ne garantit pas un niveau de sécurité. Elle ne garantit pas non plus que les solutions de sécurité ont été déployées conformément aux bonnes pratiques et à l'état de l'art. La norme ISO 27001 atteste simplement que le fournisseur a mis en œuvre un processus de gestion de la sécurité de son système d'information (SMSI) conforme à la politique de sécurité qu'il a lui-même défini. Elle ne certifie donc en aucun cas que les données du fournisseur ou celles de ses clients seront correctement sécurisées et notre étude en est une parfaite illustration.

Second constat, de nombreux clients font une confiance aveugle aux fournisseurs de services Cloud. Les labels de sécurité, les discours marketing et l'opacité des infrastructures de Cloud public rendant les audits indépendants impossibles sont d'autant de moyens pour convaincre les clients de la sécurité du service. Nous recommandons donc naturellement à tous les clients d'aller plus loin dans l'évaluation de la sécurité de leur fournisseur avant de leur confier leurs données.

Et pour finir, que faut-il penser de la sécurité des Clouds souverains ? En effet, Numergy est une société française créée en 2012 par SFR, Bull et l'état français dans le cadre du projet de Cloud souverain français (Andromède).
Pour beaucoup de fournisseurs et de médias français, la souveraineté se réduit trop souvent à deux choses. Une menace clairement identifiée : l'USA PATRIOT Act et une réponse imparable : la localisation des datacenters en France. Les fournisseurs français ont-ils bien intégré que le Patriot Act n'était pas la seule menace qui

pèse sur les entreprises françaises et qu'il fallait agir en conséquence pour démontrer leur capacité à contrer toutes les menaces potentielles dans le Cloud ?

Et si l'on en revient un instant au Patriot Act et plus généralement à la menace en provenance des USA, posons-nous les bonnes questions :

- Peut-on véritablement être souverain lorsque l'infrastructure de sécurité réseau s'appuie sur les technologies israélo-américaines de Cisco, F5, Fortinet et Checkpoint ? Qui pourrait imaginer un seul instant un pare-feu Airbus Defense & Space dans un GovCloud AWS ?
- Peut-on assurer la sécurité de nos données face à une puissance étrangère si les flux de communication chiffrés sont affectés par de multiples vulnérabilités ?
- Peut-on assurer la sécurité de nos données, si l'on envoie les mots de passe d'administration par SMS que la NSA peut intercepter facilement tant sur le réseau de l'opérateur que sur les terminaux mobiles ?

Note importante

Vendredi 13 mars 2015 à 20h30 : Ouverture Ticket d'incident Numergy
Plus de 3 jours avant la publication de cet article, nous avons ouvert un ticket incident (Priorité 1 : Very high) au support Numergy pour les informer des vulnérabilités sur leurs interfaces Web. Nous réactualiserons ci-dessous cet article dès que Numergy nous fera un retour.

Message dans le ticket d'incident :
En tant que nouvel utilisateur du Cloud Numergy (compte crée ce jour – 13/03/2015), je me suis permis de vérifier si vos interfaces Web étaient correctement paramétrées d'un point de vue sécurité.
A l'aide du service sslabs.com, j'ai testé :
login.numergy.com, mon2.numergy.com et api2.numergy.com.
Il apparait que ces 3 systèmes sont extrêmement mals configurés avec pour conséquence la possible compromission de toutes nos machines virtuelles dans le Cloud Numergy.
Je vous invite à remédier à ces problèmes dans les plus brefs délais et de me tenir au courant dès que cela sera fait.
Je vous remercie de votre compréhension.

Samedi 14 mars 2015 à 12h33 : 1ère réponse de Numergy
Bonjour,
Dans un premier temps nous vous remercions de votre vigilance .
Sachez que Numergy porte une attention particulière à la sécurité .
Tout nos systèmes sont régulièrement scanné pour en vérifier la sécurité .

Dans ce sens , votre remarque a été remontée a notre équipe de supervision et sécurité qui vous recontactera dans les plus brefs délais.
Cordialement,
L'Equipe Numergy

Mercredi 23 mars 2015 à 15h33 : 2eme message de Numergy
Monsieur, je vous remercie de votre retour.

Nous mettons tout en œuvre au quotidien pour assurer la sécurité de la plateforme et des environnements clients.
Certains des points remontés ont été jugés pertinents et les actions associées ont été menées.

Nous vous souhaitons une excellente journée.

Cordialement,
Service Support

Suite à la prise en compte de notre message au support Numergy, deux interfaces (mon2.numergy.com et api2.numergy.com) ont été corrigées le 18 mars et sont maintenant classées « A » par ssllabs. La troisième interface (login.numergy.com) a été corrigée le 23 mars et obtient également la même note pour la configuration SSL/TLS. Nous ne pouvons que féliciter le support Numergy qui a pris en compte notre alerte.
Si le comparatif avait lieu aujourd'hui, Numergy obtiendrait désormais la meilleure note avec la lettre A pour configuration SSL/TLS et https pour l'intégralité du site Web.