LIVRE BLANC #1

COMMENT EXPOSER DE MANIÈRE FIABLE ET SÉCURISÉE

son application dans le cloud ?

Dcube

INTRODUCTION

Les applications web sont de plus en plus prisées par les sociétés, atteignant le nombre de 1,8 milliard, soit deux fois plus qu'en 2015. Les entreprises se digitalisent massivement avec des solutions web et mobile. L'avènement des objets connectés, et notamment le rapport de force gagné par les smartphones face aux ordinateurs avec 54 % du trafic mondial, les poussent à évoluer.

Les applications web et mobiles deviennent la vitrine des entreprises ; il est donc important de réussir le virage de sa transformation digitale. Des problématiques fortes se posent vis-à-vis du *time to market*, des coûts et bien sûr de la sécurité.

Considérer les enjeux du déploiement d'une solution sur internet aide à prendre les bonnes décisions. Par solution, nous entendons aussi bien un site web classique accessible depuis un navigateur que des interfaces applicatives plus communément appelées API[1]. Au-delà du design ou du choix du langage de programmation, la question de l'infrastructure se pose. Même si conserver ses propres serveurs reste une option crédible, la croissance du cloud offre de belles perspectives. Le cloud soulève beaucoup de questions notamment du point de vue de la sécurité, mais il présente également beaucoup d'avantages.

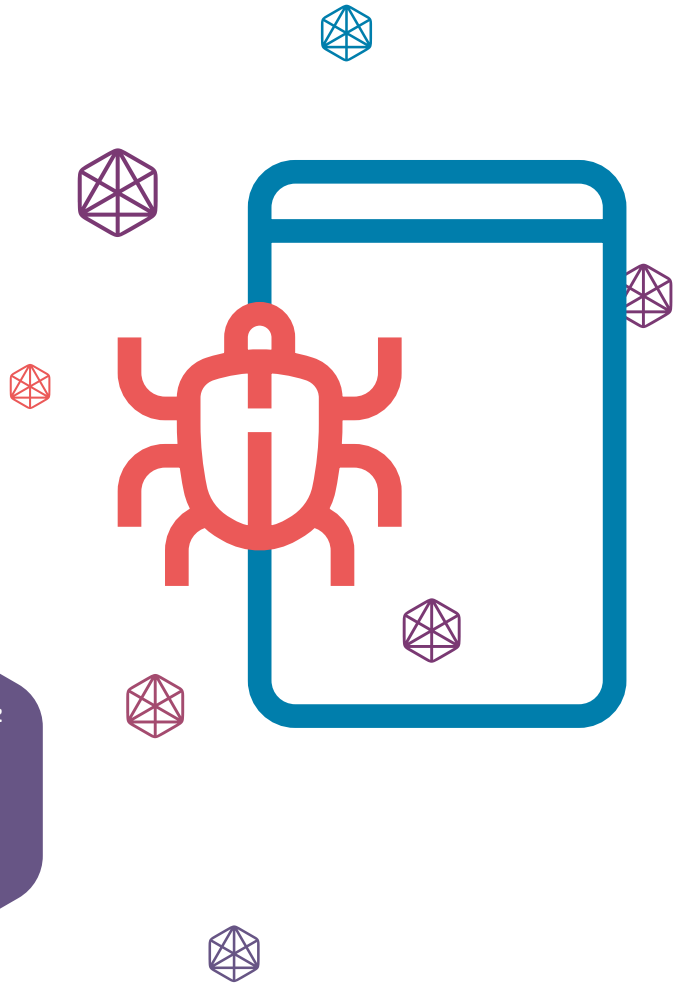
Bonne lecture !

---

[1]Application Programming Interface

QUELS RISQUES LORSQUE VOUS DÉPLOYEZ VOTRE APPLICATION WEB ?

Déployer votre application vous rend vulnérable. Deux grandes familles de risques se dégagent : les attaques malveillantes et l'indisponibilité de votre solution. Les conséquences peuvent être critiques : perte de notoriété, pertes financières, perte de clients.



LES ATTAQUES

Vous vous exposez aux attaques de hackers dès lors que votre solution est disponible sur Internet. Le OWASP[2], organisme à but non lucratif, produit un certain nombre de projets open source autour de la sécurité. Ils ont pour objectif d'améliorer les standards du web et de sensibiliser les développeurs.

« Vous vous exposez aux attaques de hackers dès lors que votre solution est disponible sur Internet. »

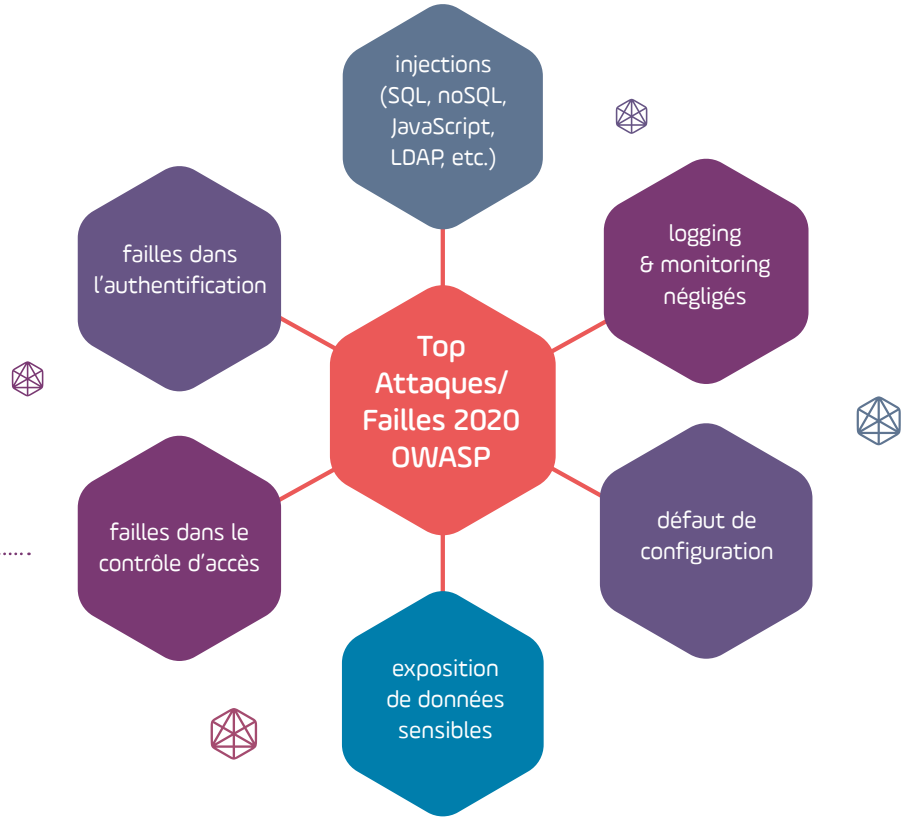
Parmi eux, le *Cheat Sheet Series Project* regroupe sous forme de fiches, rédigées par des professionnels du domaine, des informations sur des sujets précis touchant à la sécurité des applications web. Il constitue une ressource efficace d'informations et d'apprentissages pour mieux protéger vos applications.

[2] Open Web Application Security Project

QUELS RISQUES LORSQUE VOUS DÉPLOYEZ VOTRE APPLICATION WEB ? (suite)

Le OWASP tient également un classement des attaques et/ou failles les plus courantes utilisées pour attaquer des applications web.

En voici quelques-unes identifiées par cet organisme pour 2020 :



Les failles d'injections, connues de tous les développeurs, sont toujours parmi les plus exploitées en 2020. Elles permettent aux hackers d'insérer du code malveillant non prévu par l'application et ainsi de compromettre sa sécurité.

Les failles dans l'authentification sont du pain béni pour des hackers qui les exploitent afin de générer des jetons de session, se connecter à votre application et accéder à vos données.

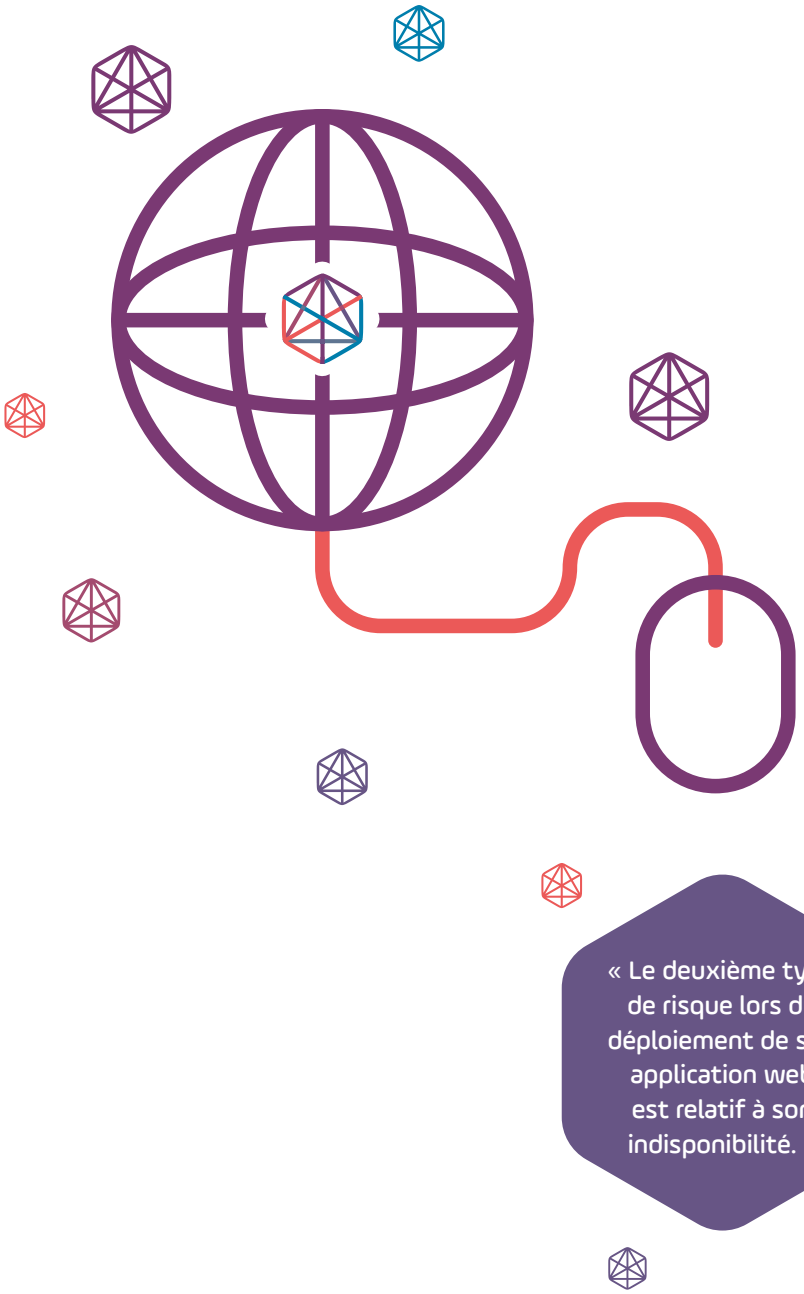
Les failles dans le contrôle d'accès reposent sur un défaut dans la stratégie de la gestion des droits des utilisateurs. Il est important de contrôler rigoureusement les droits d'accès aux ressources.

L'exposition de données sensibles concerne à la fois les données stockées et celles transitant entre différents serveurs ou entre un serveur et un navigateur. Le problème survient lorsque les données sont transmises ou stockées, en clair ou de manière cryptée, avec un algorithme dépassé.

Le défaut de configuration prennent appui sur des défaillances d'une ou plusieurs couches (réseau, système d'exploitation, serveur web, l'application elle-même, etc.). Chacune de ces couches possède ses propres mécanismes de configuration et donc ses propres vulnérabilités.

Le Logging & Monitoring négligé part du principe que toute application est vulnérable. Il est primordial de réunir tous les éléments pour qu'une attaque soit traitée rapidement. Des traces applicatives insuffisantes ou non pertinentes et surtout un manque de surveillance de ces traces permettent aux hackers de commettre plus de dégâts et de s'immiscer plus en profondeur dans vos systèmes.

QUELLES OPTIONS POUR VOTRE DÉPLOIEMENT ?



L'INDISPONIBILITÉ

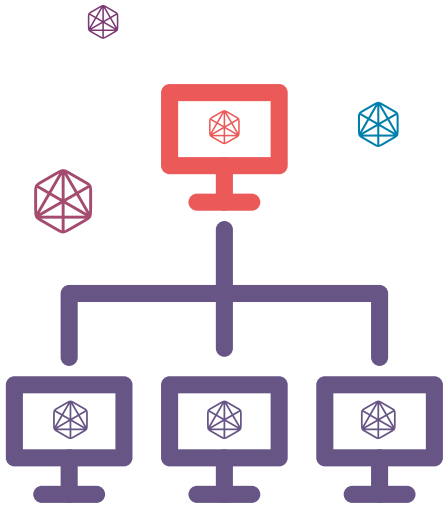
Le deuxième type de risque lors du déploiement de son application web est relatif à son indisponibilité. Cela concerne non seulement l'impossibilité d'atteindre votre application, mais aussi une baisse des performances ou la non-réalisation d'une fonctionnalité.

Plusieurs raisons sont susceptibles de générer ces problèmes. Ce peut être un souci technique chez l'hébergeur de votre application comme une panne matérielle, une coupure d'alimentation ou simplement une maintenance programmée. Le code applicatif lui-même peut être mis en cause. Une mauvaise implémentation ou une faute de frappe peuvent rendre tout ou partie de votre application inutilisable. Un pic d'affluence peut conduire à une qualité de service dégradée. La configuration matérielle du serveur, son partage avec d'autres applications ou une attaque malveillante peuvent augmenter considérablement les problèmes de performances de votre site.

Vos efforts, pour déployer votre application, doivent se porter à la fois sur le code applicatif de votre solution et sur l'infrastructure qui l'hébergera. Il faut également veiller aux moyens humains ou techniques mis à disposition pour suivre son évolution afin de trouver les causes de défaillances le plus rapidement possible.

« Le deuxième type de risque lors du déploiement de son application web est relatif à son indisponibilité. »

QUELLES OPTIONS POUR VOTRE DÉPLOIEMENT ? (suite)



Deux stratégies de déploiement s'offrent à vous : l'hébergement sur vos propres serveurs ou sur le cloud.

DES SERVEURS *ON-PREMISE*

C'est la solution historique pour votre hébergement utilisée avant l'arrivée des fournisseurs de cloud. L'hébergement *on-premise* est toujours très prisé dans les sociétés, notamment pour des raisons de confidentialité et de proximité avec les données. Ainsi, l'entreprise est seule responsable de la sécurité de ses informations. Les données sont plus facilement isolables, à condition bien sûr que l'infrastructure soit sécurisée correctement.
Les serveurs sont installés dans l'entreprise, généralement dans une salle dédiée. Cette salle, souvent bruyante et climatisée, a un coût. Il se fait ressentir sur le plan matériel, puisque la maintenance des serveurs à la suite d'une panne ou d'un désir de monter en gamme doit être réalisée soit par un remplacement de composant, soit par l'achat de nouveaux serveurs. La dépense électrique est non négligeable pour subvenir à la fois à l'alimentation des serveurs et à leur refroidissement. L'acquisition et le renouvellement de licences impliquent également un coût logiciel. Enfin, il faut considérer le coût humain pour financer cette maintenance.

UNE OFFRE DANS LE CLOUD

En premier lieu, un hébergement chez un fournisseur de cloud permet de s'assurer une solution évolutive en termes de capacité et de performance.

L'exemple le plus parlant est une entreprise vendant des produits en ligne. Elle réalise une grosse part de son chiffre d'affaires sur de courtes périodes, comme les fêtes de fin d'années ou les soldes. Une solution cloud offre très simplement la possibilité de mettre à disposition une force de frappe importante pour quelques semaines uniquement.

En second lieu, une solution cloud offre l'avantage de réduire les coûts. En effet, l'achat et la maintenance de serveur sont du ressort de votre fournisseur cloud. Exit aussi la salle serveur et les charges de consommation y ayant trait.

Votre application sera également davantage préservée des pannes. Les fournisseurs de cloud garantissent généralement un niveau de service élevé, appelé SLA[3], très proche des 100 %. Leur performance s'explique par une alimentation continue, l'utilisation de générateurs de secours, la présence du personnel de sécurité sur les datacenters 24h/24 ainsi qu'un réseau redondant. De plus, les prestataires de cloud proposent souvent un service de la réplication des données sur plusieurs serveurs voire même sur plusieurs régions du monde.

[3] Service Level Agreement

QUELLES OPTIONS POUR VOTRE DÉPLOIEMENT ?

PAAS vs IAAS

Les fournisseurs de service cloud proposent plusieurs solutions pour déployer votre application web, dont les offres IaaS[4] et PaaS[5].

	sur site	IaaS	PaaS
applications	●	●	●
données	●	●	●
runtimes	●	●	●
intégration SOA	●	●	●
base de données	●	●	●
système d'exploitation	●	●	●
virtualisation	●	●	●
serveurs	●	●	●
stockage	●	●	●
réseaux	●	●	●

● à votre charge ● dans le cloud

La solution IaaS

La solution IaaS met à votre disposition toute l'infrastructure informatique, c'est-à-dire le serveur, le stockage des données et le réseau. Ainsi, vous avez la responsabilité du système d'exploitation, des applications et de toute la couche intermédiaire entre les deux. Cette couche, appelée middleware, comprend entre autres l'environnement d'exécution des applications (framework, runtime, etc.) et les bases de données.

La solution PaaS

Avec PaaS, vous pourrez vous focaliser sur l'application elle-même. En effet, l'infrastructure informatique, le système d'exploitation et le middleware sont gérés pour vous par le fournisseur cloud. Plus flexible et moins coûteuse, c'est la solution la plus rapide pour aller dans le cloud.

Comment cela se passe-t-il en pratique ?

Une fois votre abonnement en poche, vous créerez, pour une offre IaaS, une machine virtuelle en configurant notamment les capacités du serveur, l'image à installer ou encore les propriétés du réseau. C'est donc à vous de choisir les aspects CPU, mémoire, type de disque, système d'exploitation, ouverture de port. Vous installerez ensuite, grâce une API, la base de données sélectionnée, l'environnement d'exécution pour votre application (runtime .NET Core ou Java par exemple), puis votre application elle-même. Les fournisseurs de cloud proposent généralement des surcouches aux APIs de déploiement de ressources comme un portail web et/ou une application CLI[6].
En revanche, pour une offre PaaS, vous déciderez du type de ressource à installer en fonction de votre be-

[4] Infrastructure as a Service
[5] Platform as a Service
[6] Command-Line Interface

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ

soin : une application web, une base de données, un compte de stockage et bien d'autres. Vous définirez aussi votre environnement d'exécution. Pour une application web par exemple, cela comprend les capacités du serveur, le système d'exploitation, le choix et la version du Framework. Vous n'aurez ensuite plus qu'à déployer votre application sur cette ressource grâce à l'API.

Comment sélectionner son offre ?

Si vous partez d'une page blanche, et à condition que votre application n'ait pas besoin d'une puissance de calcul phénoménale, une offre PaaS est à privilégier. Dans le cas contraire, le choix dépend grandement de votre application et des moyens humains, financiers et temporels à votre disposition.
Trois scénarios s'offrent à vous. Le *Lift&Shift* se réalise en faisant une image du serveur sur lequel s'exécute votre application et en l'exécutant sur une machine virtuelle du cloud. Le *Replatforming* consiste en une réinstallation de vos applications sur des offres cloud, en modifiant uniquement la configuration pour monter la version d'un serveur par exemple. Le *Refactoring* correspond à une réécriture complète du programme afin de profiter de tous les avantages et performances du cloud.
D'autres solutions existent pour votre déploiement, comme les technologies de conteneur type Docker ou les applications *serverless* pour lesquelles le fournisseur de cloud alloue dynamiquement des ressources serveur en fonction de la demande. L'option pour une de ces solutions se pose en amont du développement de votre application.

Une multitude de fournisseurs de cloud existe. Il convient de bien se renseigner avant de choisir. En effet, la décision aura des impacts sur le code de votre application, sur l'infrastructure, qu'elle soit créée à la main ou codée, et sur votre stratégie DevOps. Beaucoup d'éléments sont à prendre en compte, comme la flexibilité, la sécurité, le niveau de service, le coût ou encore l'intégration avec vos systèmes en place. Les fournisseurs les plus connus sont Amazon avec Amazon Web Services ou AWS, Google avec Google Cloud Platforme et Microsoft avec Microsoft Azure.
Azure permet de déployer très rapidement une plate-

existence d'une application	framework pris en charge en PaasS	équipe infra disponible	scénario	coût	durée
✓	✗	—	IaaS | lift & shift	€	⏱
✓	✗	—	PaaS | refactoring	€ € €	⏱ ⏱ ⏱
✓	✓	✗	PaaS | replatforming	€ €	⏱ ⏱
✓	✓	●	IaaS | lift & shift	€	⏱
✗	—	—	PaaS | création	€ € €	⏱ ⏱ ⏱

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

forme hautement disponible partout dans le monde. Cette accessibilité induit cependant des risques forts en termes de sécurité. Les usagers exposant des services à l'extérieur d'Azure doivent les connaître, tout comme les ressources mobilisables pour la protection d'une plateforme web. Azure propose un large panel de services pour fiabiliser, monitorer et sécuriser ses ressources. Tout est mis en œuvre pour réduire les risques et agir rapidement en cas de défaillances.

SÉCURISER VOTRE RÉSEAU

Azure est un cloud public impliquant une accessibilité pour tous. Par exemple, tout le monde peut atteindre la page de connexion de votre site web, même si vous recourez à Azure Active Directory pour authentifier vos utilisateurs et exploiter leur identité pour leur limiter l'accès.

Azure dispose de plusieurs moyens pour sécuriser votre solution. Le premier est la mise en place d'une brique type firewall en amont de votre portail.

Azure Front Door pour un accès unique

Le service Azure Front Door agit comme un point d'entrée sécurisé pour vos applications. Il intègre de multiples services, notamment une protection DDoS et un firewall, permettant d'identifier le trafic suspicieux et de réagir adéquatement. Ensuite, vous autorisez uniquement les requêtes provenant de votre instance Azure Front Door dans votre application. Cette partie WAF[7] rend possible la gestion des flux entrants en redirigeant uniquement ceux acceptés par les règles que vous aurez configurées. Azure Front Door s'installe sur des points de présence : le service est déployé globalement, vous ne choisissez pas une région. Le trafic vers vos applications est optimisé puisque le service est au plus proche de vos utilisateurs, quelle que soit leur zone géographique. Azure Front Door utilise le protocole Anycast avec du split TCP, ce qui minimise le temps de latence du protocole HTTP. Dans le cas où vous souhaitez répliquer votre application et lui assurer une haute disponibilité, il intègre également un *load balancer* complet avec un moteur d'édition de règles poussé.

« Les règles WAF garantissent une sécurité face aux menaces les plus courantes sans compromettre les performances. »

Les règles WAF garantissent une sécurité face aux menaces les plus courantes sans compromettre les performances. Elles sont déployées de la même façon qu'Azure Front Door, c'est-à-dire sur des points de pré-

[7] Web Application Firewall

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

sence, stoppant les requêtes malicieuses au plus près de leur origine, avant qu'elles n'atteignent le réseau d'Azure. La localisation des règles firewall dans le cloud offre aussi l'avantage de la rapidité d'extension. Le temps de déploiement d'une nouvelle règle est d'une poignée de minutes, autorisant une réaction vive face à des menaces récentes. Différents modes d'action sont disponibles dans Azure lors de la création d'une règle firewall, permettant notamment de bloquer la requête ou de simplement la tracer.

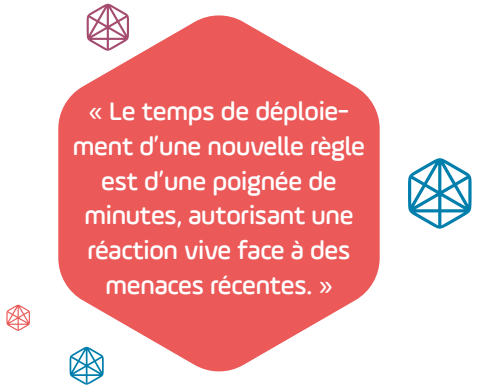
Azure Virtual Network pour une isolation des ressources

Une autre solution proposée par Azure pour sécuriser votre réseau est la construction d'un réseau privé virtuel. Ce type de protection se prête entre autres aux APIs que vous placerez derrière une passerelle d'API qui pourrait être Azure API Management dans Azure. Votre passerelle est alors accessible publiquement, mais vos APIs ne sont requêtées que par elle.

Les réseaux virtuels vous permettent d'isoler les ressources entre-elles, mais aussi de ne pas les exposer directement sur internet. Un réseau virtuel Azure est identique à celui que vous pouvez placer au sein de votre infrastructure *on-premise*. Il dispose cependant des avantages du cloud, puisqu'un VNet Azure ne met que quelques minutes à se configurer et à être disponible. Ainsi, vous pouvez paramétrer les communications entre vos services afin que seuls les flux identifiés et validés soient autorisés.

Les Network Security Groups ou NSG définissent les communications entre les sous-réseaux. Un VNet est composé d'au moins un sous-réseau ou *subnet* correspondant à une plage d'adresses IP. Ces NSG permettent de programmer des règles de trafic entrant et sortant. Ils sont actifs soit au niveau d'un sous-réseau soit directement sur une interface réseau. Les NSG tirent parti des avantages du cloud puisqu'ils peuvent être partagés entre plusieurs VNet et/ou sous-réseaux facilitant le déploiement et la réutilisation.

Pour intégrer les différents services Azure au sein d'un *subnet*, vous devez fournir une adresse IP issue du sous-réseau. Cela revient dans un mode *on-premise* à monter une interface réseau. Dans Azure, les Private Endpoints connectent vos services de façon privée et sécurisée au sein d'un VNet. Un service Azure possédant un Private Endpoint est inaccessible en dehors du VNet contenant l'adresse IP de ce Private Endpoint. Il ne permet qu'une communication entrante. Si votre service a besoin de communiquer avec



LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

un autre service Azure, ils doivent partager le même sous-réseau. Vous devez en revanche utiliser des Services Endpoint si votre service a besoin de communiquer avec une ressource Azure qui doit conserver un accès public comme un Azure Storage. En effet, les Services Endpoints rendent disponible un service Azure au sein d'un VNet tout en autorisant l'accès à l'URL publique de ce service.
Toutes ces ressources de réseau additionnées isolent efficacement vos services et limitent la surface d'attaque de votre solution cloud. Azure vous offre un ensemble d'outils de protection pour votre réseau virtuel. Ils permettent d'exposer le strict nécessaire au web public, vous garantissant une sécurité optimale s'ils sont exploités correctement. Pour cela, Microsoft vous aide notamment par rapport au firewall en mettant à votre disposition des ensembles de règles préconfigurées, basées sur les préconisations de l'OWASP.

PROTÉGER VOS RESSOURCES

Gérer l'identité de vos utilisateurs avec Azure Active Directory

Azure propose un service de gestion d'accès et d'identité appelé Azure Active Directory. Il permet entre autres de gérer l'authentification et l'autorisation des employés de votre organisation sur une plateforme web de manière complète et très sécurisée. Des fonctionnalités telles que le verrouillage intelligent ou le MFA[8] sont notamment disponibles. L'identification des différentes ressources de votre système est également prise en charge. Un employé connecté à votre portail web peut ainsi utiliser son identité pour accéder aux services d'une API. Le portail web et l'API sont alors définis en tant qu'application dans Azure AD, avec un droit pour le portail web d'accéder à l'API.

Azure Active Directory offre encore un accès à certains clients de votre organisation grâce à Azure Active Directory B2C[9]. Ils pourront se connecter par le biais de leur adresse mail ou par celui d'un fournisseur d'identité comme Google ou Facebook. L'utilisation d'Azure AD B2C évite les erreurs sur l'implémentation d'une solution équivalente. Il intègre la montée en charge de l'instance pour répondre aux besoins de protection face aux menaces courantes telles que des attaques de type déni de service ou brute force. Il s'agit donc d'une brique d'authentification hautement disponible et sécurisée nécessitant peu d'effort de mise en place, contrairement à une solution maison. Azure AD B2C propose en outre d'étendre les processus d'identification et de création de comptes pour inclure vos propres étapes. Il est aussi possible d'ajouter à vos clients des attributs personnalisés stockés dans la base utilisateurs. Cette solution se révèle donc très

[8] Multi-Factor Authentication
[9] Business to Consumer

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

fortement extensible et personnalisable.

Gérer l'identité de vos ressources avec les identités managées

Lorsque vous déployez votre infrastructure dans Azure, vous concevez plusieurs ressources. Certaines ont besoin d'accéder les unes aux autres. Ainsi, l'application du backend nécessite par exemple de se connecter à la base de données. Azure propose un service d'identités managées pour sécuriser cette connexion sans mot de passe. Chacune des ressources se voit attribuer une identité dans Azure. Il suffit ensuite de donner l'accès et les autorisations adéquates pour cette identité dans la ressource cible grâce à Azure RBAC[10].

Protéger vos données sensibles avec Azure Key Vault

Azure met à disposition Azure Key Vault, une ressource de gestion des secrets, des clés et des certificats. Vous pouvez y stocker toutes les données sensibles ayant trait à votre système. La chaîne de connexion à la base de données, l'identifiant de votre locataire Azure, la clé d'accès à une API tierce sont quelques exemples d'informations que vous pourriez placer dans votre Key Vault plutôt que dans un fichier de configuration. L'utilisation des identités managées permet à une ressource d'accéder à votre Key Vault. Vous récupérez ensuite, depuis votre code secret dans le Key Vault en utilisant le SDK[11] lié au langage de programmation de votre application.

Ainsi, avec Microsoft Azure vous détenez un procédé de protection de vos ressources en sécurisant la connexion de vos utilisateurs ; et à l'aide d'Azure AD vous défendez vos applications grâce aux identités managées. Azure vous offre également un moyen fiable et complètement sûr d'isoler vos données sensibles avec Azure Key Vault.

[10] Role-Based Access Control
[11] Software Development Kit

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

MONITORER VOS APPLICATIONS

Toute une suite de services est mobilisable dans Azure pour vous permettre de monitorer et de sécuriser vos applications.

Superviser votre application avec Azure Monitor

Azure Monitor est un service vous offrant des indicateurs de performances et de disponibilité à partir des données de télémétrie de vos applications et de vos services. Selon ces données, vous pouvez créer des alertes et agir grâce à des actions automatisées. Par exemple, vous pouvez envoyer un mail à tous vos développeurs pour les avertir d'un taux anormal de requêtes en erreur. Pour correspondre efficacement aux attentes des utilisateurs, vous pouvez également augmenter ou diminuer les capacités de votre serveur en fonction des temps de réponse moyens. Dans le portail Azure, vous créez vos propres tableaux de bord pour évaluer en un coup d'œil la santé de vos applications.

Agréger et analyser vos logs avec Application Insights

Application Insights vous offre la possibilité de connaître l'utilisation faite de vos applications. Vous pouvez entre autres suivre le parcours de vos utilisateurs, le nombre de connexions ou la durée des sessions. Avec Application Insights, vous gardez également les performances au centre de vos préoccupations en consultant les temps de chargement de vos pages web ou en suivant les requêtes en échec. Vous êtes donc proactifs sur les problèmes de vos applications, sans attendre les remontées de vos utilisateurs. Grâce à Azure Log Analytics, vous bénéficiez d'un langage puissant pour le traitement de vos traces applicatives. Ainsi, vous profitez de tous les outils pour superviser vos applications, détecter et diagnostiquer les problèmes pour agir en conséquence dans votre code source.

Protégez-vous des menaces grâce à Azure Security Center

Avec Azure Security Center, vous disposez d'un système centralisé de gestion de la sécurité de votre infrastructure que vous soyez sur une offre PaaS, IaaS ou même avec des serveurs *on-premise*. Azure Security Center évalue constamment l'état de vos ressources grâce à des agents Log Analytics et collecte énormément de données. Après leur analyse, vous tirez parti de recommandations pour sécuriser davantage votre système.

LES SERVICES D'AZURE POUR UN DÉPLOIEMENT SÉCURISÉ (suite)

Réagir aux menaces de façon automatisée avec Azure Defender

Azure Defender va plus loin en générant des alertes dès lors qu'un danger est détecté. Elles comprennent tous les détails de la menace et fournissent des éléments pour sa résolution. Vous pouvez ensuite les connecter à Azure Sentinel, un service basé sur l'intelligence artificielle, pour y répondre automatiquement ou pour déclencher une série d'actions logiques. Vous pouvez par exemple expédier un mail avec toutes les précisions sur la menace et une demande d'approbation, créer un ticket d'incident ou envoyer un message dans Microsoft Team dès la réception d'une alerte.

« Azure Defender va plus loin en générant des alertes dès lors qu'un danger est détecté. »

Microsoft Azure fournit donc des outils vous permettant de surveiller et d'analyser votre infrastructure et vos applications, mais aussi de les sécuriser davantage.

CONCLUSION

Les entreprises déploient de plus en plus d'applications sur le web sans toujours en connaître complètement les risques. Il est impératif de mesurer les impacts liés au choix de l'infrastructure qui hébergera votre application.

Les offres cloud sont devenues une excellente solution. Si elles nécessitent certaines compétences au sein de vos équipes, elles vous permettront par ailleurs d'accélérer votre transformation, de bénéficier de performances accrues tout en maîtrisant votre budget.

Plusieurs solutions se présentent à vous si vous faites le choix d'un hébergement dans le cloud. Grâce à l'IaaS, vous gardez la main sur les machines virtuelles, depuis le système d'exploitation jusqu'aux applications installées. L'offre PaaS vous permet en revanche de vous focaliser sur l'application elle-même, laissant la gestion de l'infrastructure à votre fournisseur de cloud.

Microsoft Azure est l'un des fournisseurs de cloud parmi les plus reconnus du marché. Il dispose de toutes sortes de services pour la sécurisation de votre réseau, la protection de vos ressources et la surveillance de votre application. Vous bénéficiez avec lui de tous les moyens pour déployer votre solution en toute sécurité dans le cloud.

Si vous êtes intéressés par le déploiement de votre solution sécurisée dans le cloud, Dcube, partenaire Gold de Microsoft, dispose des talents nécessaires pour vous accompagner dans cette démarche. L'entreprise a des expériences reconnues en matière de création d'applications sur mesure ou de migration de solutions dans le cloud Azure. Si vous le souhaitez, nous pouvons dans un premier temps réaliser un audit de votre situation.

DÉCOUVRIR **ÉGALEMENT**

Vous pouvez aussi télécharger **« 5 étapes pour sécuriser votre site web hébergé dans Azure »**

dans lequel nous abordons le sujet de la sécurité d'une application web déployée en mode PaaS dans Azure.

Télécharger le livre blanc

PRENDRE CONTACT **AVEC DCUBE**

Si vous le souhaitez, nous pouvons **réaliser un audit de votre situation.**

Prendre contact avec DCUBE

LES AUTEURS
DE CE LIVRE BLANC

Romain LAPREE-KAMINSKI
Azure Cloud Developer
romain.lapree@dcube.fr

Etienne POMMIER
Technical Lead .net
etienne.pommier@dcube.fr

DCUBE est LE cabinet de conseil en transformation digitale,
partenaire Microsoft de vos projets Data / AI.

dcube

make it happen

contact@dcube.fr
+33 (0)1 82 83 32 20

www.dcube.fr