La sécurité des datacenters modernes

Par Dr. Larry Ponemon, Président Fondateur, Ponemon Institute

Les entreprises font face à une multitude de cybermenaces. Comme l'indique l'étude de Ponemon Institute, les vulnérabilités logicielles, les logiciels malveillants (rançongiciels notamment), le phishing, les DDoS et les attaques véhiculées par le Web rendent difficile la sécurisation des data centers. Ces menaces causent de nombreux problèmes aux data centers conventionnels.

Pour preuve, des recherches récentes révèlent que le paysage des menaces ne s'améliore guère. De nouvelles menaces émergent comme la cyber-extorsion, les logiciels malveillants et les rançongiciels, qui font courir un risque accru aux entreprises. La majorité des celles-ci, analysées dans nos études, a connu une violation de données impliquant la perte ou le vol de plus de 1 000 enregistrements contenant des informations sensibles ou confidentielles sur des clients ou des entreprises. Elles déclarent avoir subi au moins deux violations de données sur cette période. Les conséquences financières de telles exactions peuvent être dévastatrices. D'après notre étude *2020 Cost of Data Breach*, le coût moyen d'une violation peut atteindre 4 millions de dollars.

Pourquoi la sécurité des data centers est-elle importante ? Les data centers regorgent d'applications sensibles, d'éléments de propriété intellectuelle, de données d'entreprise et d'informations sur les clients. Ils sont une cible évidente pour les criminels. Outre l'exfiltration de données, ces criminels veulent causer de véritables préjudices à l'entreprise ciblée en obérant ses performances, en provoquant des dysfonctionnements opérationnels et en affectant sa sécurité physique globale. Nos recherches ont révélé que l'une des principales préoccupations des entreprises est de subir des incidents de cybersécurité qui impactent lourdement leurs processus informatiques et métier. Ainsi, une sécurité efficace des data centers réduit la capacité des criminels à accéder au trafic réseau et à le manipuler.

Au cours des cinq dernières années, des changements importants sont intervenus au sein des data centers, parmi lesquels l'avènement des data centers hybrides et des data centers à grande échelle (hyperscale). Un data center hyperscale est une installation possédée et exploitée par la société pour laquelle il fonctionne. Les data centers hyperscale concernent généralement des sociétés telles qu'AWS, Microsoft, Google, Apple et desservent de grandes entreprises, notamment des institutions financières et des prestataires de soins de santé comptant de nombreux patients et clients.

Si les data centers hyperscale offrent aux particuliers ou aux entreprises des applications, des services de stockage et des bases de données hautement évolutifs, ils sont confrontés à des problèmes de sécurité qui doivent être résolus. Plus précisément, les priorités métiers toujours plus urgentes des entreprises conduisent à renoncer à la sécurité afin de préserver l'expérience utilisateur, simplement parce que peu de solutions de sécurité sur le marché sont capables de suivre le rythme qui leur est imposé. L'absence de sécurité adéquate entraîne un certain nombre de problèmes allant du trafic Web illégitime aux attaques par DDoS.

Un data center hybride est un environnement qui associe des data centers sur site et des espaces hébergés au sein de plusieurs clouds. Avec l'augmentation du trafic mondial dans les data centers, une infrastructure hybride aide les entreprises à se préparer aux fluctuations du niveau de trafic et à renchérir les capacités à la demande. Mais le cloud hybride peut entraîner une visibilité réduite en raison d'une recrudescence de zones d'ombre, d'une complexité accrue et du risque externe que représentent les acteurs malveillants qui exploitent les vulnérabilités et piratent les données.

Historiquement, le data center considérait le trafic réseau comme étant vertical (ou Nord-Sud), autrement dit un trafic client-serveur qui transite entre le data center et un endroit situé en dehors du réseau du data center. Ce trafic Nord-Sud est généralement représenté verticalement pour illustrer le trafic qui transite au-dessus ou en dessous du data center. Mais aujourd'hui, les données peuvent également se déplacer latéralement, ou d'Est en Ouest, au sein d'un data center.

La migration vers le Cloud et la transformation numérique plaident en faveur d'un data center hautement sécurisé.

La plupart des entreprises manquent de confiance, de visibilité et de définition claire des responsabilités en matière de gestion de la sécurité dans le data center, que ce dernier soit hybride ou hyperscale.

- **La migration vers le Cloud exacerbe les risques pesant sur les informations sensibles du data center.** Malgré l'importance du Cloud dans la réalisation des objectifs métier, près de la moitié des participants à l'étude Ponemon Institute[1] n'est pas convaincue que leurs data centers répond actuellement à leurs exigences en matière de respect de la vie privée et de protection des données. En fait, les entreprises sont réactives et non proactives dans la protection du trafic sensible au sein d'un environnement de data center hybride. Plus précisément, seules 44 % des personnes interrogées contrôlent les logiciels ou les plateformes basés dans le Cloud et dans les data centers pour détecter les risques liés à la sécurité des données. Seules 39 % déclarent identifier les informations trop sensibles pour être stockées dans le Cloud.

- **Un manque de visibilité sur le trafic réseau du data center met en danger les données sensibles qui sont collectées, traitées et stockées dans le Cloud.** Seulement 29 % des personnes interrogées déclarent que leur entreprise dispose de la visibilité à 360 degrés nécessaire sur les données sensibles collectées, traitées et/ou stockées dans le Cloud. Les entreprises estiment par ailleurs qu'elles ne connaissent pas forcément toutes les applications et plateformes Cloud qu'elles ont déployées.

- **La transformation digitale amplifie le risque de failles de sécurité au sein du data center.** Dans une récente étude de Ponemon Institute[2], les professionnels de la sécurité informatique s'accordent à dire que l'économie numérique est essentielle à la préservation des avantages concurrentiels de leur entreprise et à l'atteinte de ses objectifs métier. Toutefois, pour réussir dans ce nouvel écosystème métier, les entreprises doivent être en mesure de sécuriser leurs données dans le processus de transformation et l'environnement digital.

- **La complexité des processus d'entreprise, la visibilité insuffisante sur les personnes et les processus métier et le manque d'expertise en interne sont les principaux obstacles à un processus de transformation digitale sécurisé.** La complexité des processus de l'entreprise doit être surmontée pour parvenir à une transformation digitale fiable. Les entreprises doivent aussi remédier au manque de visibilité sur les personnes et les processus métier et à la pénurie de collaborateurs qualifiés ou experts, afin de sécuriser leurs informations sensibles dans le data center.

- **La progression du volume des données chiffrées.** Les entreprises utilisent le chiffrement pour protéger les données sensibles et confidentielles en transit. Mais il est très difficile de déterminer si les données sont corrompues. À moins de disposer de la clé pour les déchiffrer, le processus est fastidieux.

---

[1] *Data Protection and Privacy Compliance in the Cloud: Privacy Concerns Are Not Slowing the Adoption of Cloud Services, but Challenges Remain,* sponsorisée par Microsoft, réalisée de façon indépendante par Ponemon Institute, janvier 2020.

[2] Bridging the Digital Transformation Divide: Leaders Must Balance Risk & Growth, financée par IBM Security, réalisée de façon indépendante par Ponemon Institute, mars 2018.

- **Points faibles de la sécurité des réseaux plats.** Les réseaux plats sont des réseaux traditionnels à plusieurs niveaux basés sur des routeurs et des commutateurs qui ne procèdent pas à l'inspection du trafic, ni à l'application des règles de sécurité. Le réseau plat supprime les technologies de sécurité traditionnelles telles que le pare-feu ou le filtrage. Cette tendance entraîne des risques majeurs, notamment si elle est associée à une confiance accordée par défaut à tous les utilisateurs internes. Par exemple, lorsqu'un assaillant s'introduit dans le périmètre interne, il peut rester en sommeil pendant un certain temps puis se propager latéralement sur le réseau.

Sécuriser le data center moderne

La disponibilité est une priorité, au même titre que la sécurité. Les meilleures pratiques consistent à disposer de ressources suffisantes pour restaurer les data centers en cas de dysfonctionnement imprévu. Des recherches récentes ont révélé que les entreprises migrent leurs fonctions de sécurité du cœur de réseau vers les terminaux.

Voici quelques recommandations pour mettre en place une stratégie efficace de sécurité des data centers.

- **Adopter une approche de type zero-trust.** Le modèle zero-trust (modèle de vérification systématique) estime que chaque transaction, mouvement ou utilisation de données est potentiellement suspecte. Une sécurité zero-trust suit en temps réel le comportement du réseau et les flux de données, et contrôle toute personne extrayant des données du système. Tout comportement anormal détecté donne lieu à une alerte et les droits du compte associé peuvent être suspendus. La détection des menaces doit être robuste, qu'elle soit effectuée par différents systèmes de sécurité ou centralisée à l'échelle d'un pare-feu réseau. L'application peut s'exécuter via le pare-feu du réseau ou par un dispositif de contrôle d'accès au réseau (NAC). La sécurité peut être gérée par un centre de commande qui supervise la gestion centralisée et le contrôle opérationnel des systèmes critiques d'entreprise, généralement situés dans les data centers et au sein de systèmes informatiques d'envergure.

- **Intégrer les couches de sécurité et assurer la redondance des data centers.** La sécurité des données implique des fonctions de sécurité et de validation de systèmes, intégrées au niveau de chaque couche de la structure du data center.

- **Sécuriser tous les terminaux.** Tout équipement, qu'il s'agisse d'un serveur, d'une tablette, d'un smartphone ou d'un ordinateur portable connecté au réseau du data center, est considéré comme étant un terminal (ou endpoint) devant être sécurisé.

- **Documenter les procédures de sécurité.** Il est essentiel de disposer de procédures bien définies et documentées. Une opération aussi simple qu'une fourniture régulière d'un service doit être planifiée et documentée.

- **Réaliser des audits de sécurité réguliers.** Les audits peuvent aller des contrôles de sécurité au quotidien, y compris les vérifications physiques, aux audits PCI et SOC trimestriels et à l'établissement de rapports automatisés pour détecter les erreurs de configuration et autres pratiques non conformes.

- **Les systèmes de détection et de prévention des intrusions (IDPS) sont essentiels.** Les fonctions de prévention des intrusions (IPS) sont essentielles pour protéger les infrastructures réseau critiques et les applications héritées difficiles à patcher. La détection de ce type d'attaques sur le réseau nécessite une surveillance en temps réel de l'activité du réseau et des systèmes, avec des fonctions d'intelligence artificielle/d'apprentissage automatique capables de repérer tout événement inhabituel.

- **Segmenter le système.** La segmentation du réseau à différents niveaux est essentielle pour prévenir la propagation latérale des menaces. Les approches comprennent des techniques de segmentation basées sur l'hôte et le réseau. La segmentation basée sur l'hôte nécessite d'exécuter un agent et implique de classer tout le trafic en différents segments, en fonction de l'identité du terminal. D'autres

techniques utilisent la micro-segmentation, qui se traduit par une méthode plus sophistiquée pour contrôler l'accès des utilisateurs aux applications et aux services. La segmentation réseau, dans laquelle un pare-feu réseau crée des segments, simplifie l'application des règles. Dans l'ensemble, chaque segment est isolé de tous les autres dans un sous-réseau indépendant. De plus, cette segmentation confine toutes les menaces potentielles dans un seul sous-réseau, ce qui empêche les menaces de s'en prendre aux autres terminaux et réseaux. La segmentation peut également être effectuée au niveau des applications, des ports et via des containers. Dans le cas d'une segmentation basée sur les ports, un port sur un commutateur peut être, lorsque nécessaire, neutralisé directement par un pare-feu réseau ou avec l'aide d'une solution NAC.

- **Surveiller les mouvements latéraux.** Le mouvement latéral correspond à un ensemble de techniques que les assaillants utilisent pour se propager sur les réseaux, d'un équipement à un autre, ou pour obtenir des privilèges plus importants. Une fois que les cybercriminels ont infiltré un réseau, ils cartographient tous les dispositifs et applications afin d'identifier les composants vulnérables. Si cette compromission n'est pas détectée à temps, ils peuvent obtenir un accès privilégié et, in fine, perpétrer leur exaction. La surveillance des mouvements latéraux réduit le laps de temps pendant lequel les menaces pour la sécurité des data centers sont actives à l'intérieur des systèmes.

- **Assurer la sécurité au niveau du réseau.** Le chiffrement réseau consiste à utiliser le chiffrement au niveau de la couche de transport de données, cette dernière étant responsable de la connectivité et du routage entre deux entités qui communiquent. Le chiffrement est actif pendant le transfert des données et est indépendant de tout autre chiffrement, ce qui en fait une solution autonome.

- **Déployer le SSL et la prévention des menaces.** Ces solutions assurent l'inspection SSL, y compris la dernière norme TLS1.3, pour détecter les menaces furtives, neutraliser toute exfiltration de données et juguler les attaques contre l'infrastructure de sécurité.

- **Fournir une sécurité à grande échelle (hyperscale).** Les solutions de sécurité offrent des pare-feux ultra-rapides capables d'inspecter un volume très important de trafic utilisateur et de neutraliser les attaques DDoS qui visent l'arrêt des opérations essentielles d'une entreprise.

- **Adopter l'automatisation.** Les solutions de sécurité fournissent des outils d'automatisation et d'orchestration efficaces, évolutifs et garantissant une application cohérente des politiques de sécurité sur toutes les infrastructures, quel que soit leur emplacement.