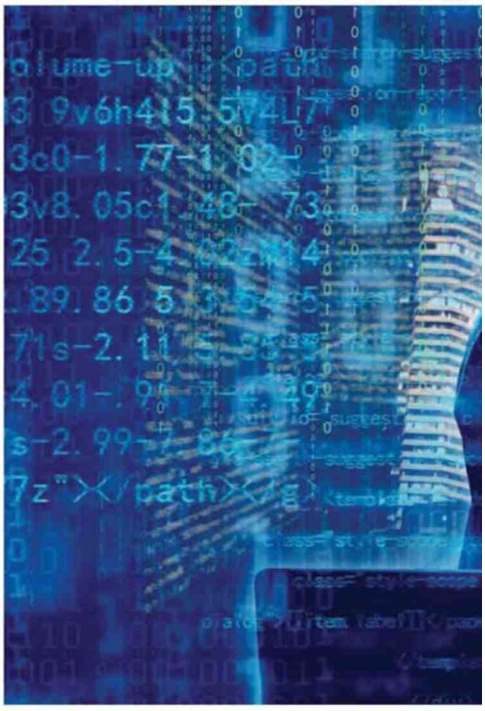
Décision Achats

PAYS : France
PAGE(S) :60-62
SURFACE :245 %
PERIODICITE : Mensuel

DIFFUSION :(44000)
JOURNALISTE : Mathieu Neu

► **1 décembre 2020 - N°221**

Ecosystème IT
La sécurité, à la hauteur des enjeux ?



Mobilité, télétravail, multicloud, interconnexion d'équipements... Le périmètre informatique des organisations évolue constamment, tout comme l'exposition aux risques. Dans ce contexte où les réseaux semblent dépourvus de frontière, les politiques de cybersécurité doivent se moderniser plus vite.

Dans une étude parue en septembre 2020, le fournisseur de solutions de sécurité unifiées Tanium souligne que 93 % des entreprises ont connu une augmentation des cyberattaques depuis le début de la pandémie de la covid-19. La transition très rapide vers le télétravail a pris les organisations au dépourvu et mis en lumière certaines failles imputables à la précipitation avec laquelle la transformation du travail s'est produite. Mais cette enquête agit aussi comme un révélateur de problématiques plus globales liées à la diversité et l'interconnexion d'outils toujours plus nombreux, à l'intérieur comme à l'extérieur des murs de l'entreprise. Les réseaux mobiles sont au cœur des difficultés rencontrées : 75 % des terminaux sont vulnérables à une demande non autorisée de localisation, 9 SMS sur 10 peuvent être interceptés et 53 % de ces malveillances se traduisent par un succès. Ces quelques chiffres publiés par le spécialiste de la cybersécurité Positive Technologies indiquent explicitement le degré d'exposition aux risques.

Les systèmes dans le cloud sont eux aussi concernés par une fragilité, du fait *« qu'ils sont parfois considérés avec un excès de confiance de la part des sociétés clientes. Elles estiment souvent à tort que les questions de sécurité sont le problème des hébergeurs. Ces derniers proposent d'ailleurs presque systématiquement une offre de protection dans leur package. Dans la réalité, les volets applications, les infrastructures restent généralement la responsabilité du client final qui doit lui-même mettre en place et financer un niveau de sécurité qui lui est adapté et suffisant »*, explique Philippe Rondel, senior security architect au sein du spécialiste CheckPoint. Certaines offres cloud mettent à disposition des briques fonctionnelles, mais qui concernent souvent des points élémentaires. *« D'autres fournisseurs proposent du contrôle d'accès qu'ils estiment suffisants, ce qui n'est pas toujours le cas »*, regrette-t-il.

Des enjeux encore mal compris

Les difficultés sur les clouds publics sont identiques que pour les infrastructures on premise. Potentiellement, l'ouverture sur le monde extérieur représente même un facteur aggravant, d'autant que les administrations de système deviennent également joignables et accessibles via Internet, par le biais des solutions SaaS par exemple. Yohann Berhouc, directeur général de la société Cyrès, spécialisée dans le conseil et l'accompagnement en projets IT, pointe aussi du doigt le fait que *« les équipes support des fournisseurs cloud ne se montrent pas nécessairement disponibles rapidement lorsqu'on n'est pas un nom prestigieux du CAC40 »*.

« Le client final doit lui-même mettre en place et financer un niveau de sécurité qui lui est adapté et suffisant »

Philippe Rondel, *senior security architect, CheckPoint*

Décision Achats

PAYS : France
PAGE(S) :60-62
SURFACE :245 %
PERIODICITE : Mensuel

DIFFUSION :(44000)
JOURNALISTE : Mathieu Neu

► **1 décembre 2020 - N°221**

Le manque de connaissance de ces réalités inquiète d'autant plus avec le nombre effréné des migrations vers le cloud. « *La tendance veut qu'on bascule de plus en plus d'éléments variés, avec au bout du compte un impact fort sur le degré de disponibilité des applications qui se retrouvent mises à mal par des cybercriminels. Les clouds servent souvent de passerelles pour intégrer l'entreprise directement et activer des ransomwares* », confie Philippe Rondel.

Ghaleb Zekri, Architecte Senior SDDC pour la région EMEA du fournisseur de solutions de virtualisation VMware, mentionne lui aussi la mauvaise compréhension des offres clouds comme l'un des problèmes phares à l'heure actuelle : « *Des clouds publics comme Microsoft Azure, AWS, Google Cloud, proposent des hébergements sécurisés garantissant l'absence de compromission des données clients, auxquels on peut ajouter des dispositifs sécuritaires supplémentaires. Dans un environnement pleinement maîtrisé, dans un cloud privé, on sait clairement quels sont les éléments à protéger et dans quelles proportions. Au sein d'une offre publique, on se situe par définition dans un environnement qu'on ne gère pas, mais qu'on consomme.* »

Une configuration approximative qui peut donner lieu à des failles. Les solutions de visibilité complète sur les services consommés sont alors essentielles et apportent une évaluation en temps réel de la posture de ces différents services quant aux garanties sécuritaires. L'enjeu est de ne pas être trop exposé aux risques, mais également d'éviter de surconsommer la sécurité.

À la faveur de la crise sanitaire actuelle et des problématiques relatives au travail à distance, la nécessité de procéder à des audits de sécurité semble mieux entrer dans les consciences. « *Une entreprise connaît un nombre de processus automatisés toujours plus vaste. Les questions de sécurité concernent des aspects toujours plus diversifiés : machines industrielles, flottes automobiles, systèmes informatiques locaux, réseaux mobiles... La période actuelle et la prise de recul qu'elle impose sont l'occasion d'être mieux sensibilisés à ces évolutions* », remarque Marc Lafleuriel, directeur Exploitation & Sécurité chez Cyrès.

Le cloud natif évolue vers des fonctions "as a service"

Les entreprises sont désormais davantage en demande d'opérations de contrôle d'accès dans les environnements IaaS (Infrastructure as a Service), ou de vérification de la conformité des environnements clouds. « *La plupart de nos clients sont tournés vers une configuration multicloud et ont besoin d'avoir une vue d'ensemble. Le cloud natif évolue vers des fonctions "as a service". On nous demande de vérifier le code de ces fonctions en matière de sécurité, de vérifier la dépendance à des librairies qui peuvent être vulnérables, de contrôler le respect des droits minimum et nécessaires, comme la lecture seule. Il y a une tendance à vouloir également injecter de la sécurité supplémentaire, de pouvoir être en mesure de bloquer des dérivations des tâches impliquant des lancements de fonctionnalités annexes non nécessaires* », observe Philippe Rondel.

La maturité face aux enjeux de cybersécurité dépend des secteurs mais aussi de chaque organisation. Les fonctions de contrôle et de conformité inté- ●●●

Décision Achats

PAYS : France
PAGE(S) :60-62
SURFACE :245 %
PERIODICITE : Mensuel

DIFFUSION :(44000)
JOURNALISTE : Mathieu Neu

► **1 décembre 2020 - N°221**

●●● ressent plutôt les grandes entreprises. En matière de validation de codes et fonctions, les start-ups et spin-offs ayant de forts enjeux financiers, dont la culture de sécurité informatique peut être faible, et qui évoluent dans un contexte de Time-to-Market très exigeant, sont largement représentées.

Vers des pratiques adaptées aux développements futurs

Au même titre que la mobilité technologique qui permet une continuité d'activité en toute situation, *« la sécurité doit être transverse et consommable comme n'importe quelle autre ressource. C'est une notion qui doit être intrinsèque »*, estime Ghaleb Zekri. Compte tenu de la complexité croissante de la configuration du système d'information des organisations, les outils globaux de supervision s'avèrent souhaitables. À l'heure actuelle, des métropoles entières sont également clientes de telles solutions. *« Dans le cadre du développement des villes intelligentes, nous avons plusieurs grandes capitales parmi nos clients. À Mexico, on récupère des données sur de nombreux équipements publics (pylônes électriques, supervision du trafic...). À Singapour, la ville a souhaité mettre en place un ensemble de captation de données, notamment pour la mesure de la vitesse du vent. Il s'agit alors de procéder à une veille constante sur les questions de sécurité des systèmes »*, décrit Fabien Pereira Vaz, Technical Sales Manager chez Paessler, spécialiste des solutions de surveillance des réseaux. Avec l'essor des objets connectés et du big data, la demande de ce type d'outil devrait croître rapidement, notamment dans les filières industrielles. Les fournisseurs du secteur de la sécurité sont nombreux à avoir d'ores et déjà anticipé les exigences des déploiements 5G.

Surveillance élargie

L'outil proposé par Paessler se veut simple et accessible, avec l'objectif d'apporter une vision globale de la configuration des réseaux et infrastructures. Les informations recueillies proviennent de tous types d'équipements (serveurs SQL, systèmes de messagerie, logiciels, objets connectés, etc.). Collecter ainsi l'information de manière proactive, en temps réel, permet d'identifier les faiblesses, déceler des fragilités de sécurité, anticiper les dangers. *« En somme, c'est une tour de contrôle permettant d'avoir un temps d'avance quant aux dommages éventuels »*, résume Fabien Pereira Vaz. Dans un contexte où les environnements professionnels sont de plus en plus connectés, la solution a également été développée pour détecter les risques physiques. *« Nous nous connectons aux capteurs des bâtiments pour repérer les mouvements anormaux, les anomalies des systèmes pouvant déclencher des problèmes graves (taux de gaz, d'humidité, niveaux de tensions électriques permettant d'anticiper un risque d'incendie, etc.) ou encore les comportements anormaux (intrusions, négligences, etc.) »*, ajoute-t-il.

Ghaleb Zekri rappelle par ailleurs que dans le monde informatique actuel, les applications ne sont plus statiques comme par le passé, ce qui change nécessairement les réflexions dans ce domaine : *« Elles se développent très rapidement, sont disponibles sur des clouds publics, privés. Les nouveaux flux qui en découlent imposent une adaptation de l'application aux nouveaux risques. Un autre point important est l'exposition à l'inconnu, aux attaques qu'on ne peut pas prévoir. Avec un système de surveillance global, on peut ainsi avoir une connaissance granulaire de cette exposition et ajuster la politique de sécurité. L'identification de la bonne réponse selon les cas de figure est une clé de développement qui doit être en constante amélioration. »* ● MATHIEU NEU

« La collecte d'informations permet d'avoir un temps d'avance quant aux dommages éventuels »

Fabien Pereira, *Technical Sales Manager, Paessler*

Focus

Une approche trop brouillonne

Une étude du magazine Forbes souligne que les entreprises disposent en moyenne de 26 produits différents de cybersécurité dans leur infrastructure. Le dispositif global en place prend ainsi des allures de millefeuille sans cohérence. *« L'interopérabilité est alors l'un des grands obstacles. Pour chaque problème de sécurité, on a proposé une solution, ce qui fait que les clients se retrouvent au fil du temps avec une multitude de couches produits qui ne sont pas corrélées. La notion de contexte est pourtant très importante pour une gestion efficace dans ce domaine »*, assure Ghaleb Zekri.

Les pratiques du shadow IT, c'est-à-dire le fait que les petites directions d'entreprise s'équipent elles-mêmes de solutions pour bénéficier de services qui n'existent pas ailleurs dans l'entreprise complexifient la vue d'ensemble de l'organisation, et imposent d'aller à la rencontre des différentes unités. Par ailleurs, lorsque des audits de sécurité sont menés, le périmètre concerné n'est pas toujours suffisant. Ils doivent par exemple inclure la nature exacte des consignes données par un donneur d'ordre à un fournisseur accédant à certaines informations pour assurer sa mission de maintenance d'équipements.

La plupart des entreprises sont involontairement contaminées par des fournisseurs. C'est ce qu'on entend d'ailleurs par l'expression "origine interne". *« Mais le collaborateur qui quitte l'entreprise en mauvais termes, dans un contexte de désaccord important, peut aussi être une source de problèmes et de craintes »*, indique Marc Lafleuriel.