Cybersécurité : les partenaires sont au cœur de la prévention

La sécurité informatique est un des sujets les plus complexes auxquels font face les entreprises et organisations publiques. Les cyber-menaces sont exponentielles et de plus en plus sophistiquées (malware, ransomware, phishing, attaque DDOS, attaque par force brute).

Face à ces enjeux, les budgets restent sous pression et les solutions du marché n'adressent les risques que partiellement. En témoigne le nombre de solutions de sécurité installées dans les entreprises, avec plus de 26 produits dédiés utilisés par un tiers d'entre elles.

A chaque outil, une interface utilisateur spécifique, des stratégies d'administration différentes et des nouvelles compétences pour les opérer. Les partenaires et prestataires de services sont variés : consultants, revendeurs, intégrateurs, opérateurs de SOC (Security Operation Center), MSSP (Managed Security Service Providers).

Voici six axes qui permettront à ces acteurs d'échanger avec leur client afin de limiter la multiplication des solutions monofonctionnelles partielles et coûteuses, et adopter une nouvelle stratégie de sécurité adaptée à leurs activités, leur personnel mobile, leurs applications et leur réputation.

1. Promouvoir la rapidité de réaction au lieu de la protection du périmètre

Le modèle de cybersécurité existant qui consiste à protéger le périmètre du réseau à l'aide d'un pare-feu pour ensuite reboucher les trous créés par les nouvelles technologies (appareils mobiles, Cloud,…) à l'aide de solutions mono-fonctionnelles, est tout simplement inadapté au monde professionnel d'aujourd'hui. En effet, cette approche traditionnelle du « château fort » statique est soit inefficace, trop complexe, trop coûteuse, ou trop diffici à gérer (ou tout en même temps).

Pourquoi ? Parce que la surface d'attaque dont profitent les logiciels malveillants s'est considérablement élargie, et que les attaques sont toujours plus élaborées et nécessitent une réactivité et une sécurité adaptative liée au comportement des applications et des utilisateurs. Les failles de sécurité sont inévitables. L'important est donc de savoir les prévenir, les détecter et en maîtriser les effets rapidement et efficacement.

Les partenaires, via les plateformes de supervision (SIEM) et les solutions d'EDR (Endpoint Detection and Response) sont en mesure de piloter et remédier aux incidents chez leurs clients.

2. S’assurer que les clients sont en mesure de se préparer aux imprévus

Le fait que les entreprises courent toujours autant après les menaces (la plupart encore inconnues) est un problème de taille. En effet, cette approche met davantage l’accent sur les pirates que sur l’entreprise (et les ressources) à protéger. Pire, l’industrie continue d’investir l’essentiel de ses efforts en R&D, innovation et de son temps dans des solutions de détection réactives et de moins en moins efficaces.

Ainsi, nombreuses sont les entreprises qui investissent trop peu dans des solutions préventives. Mais savoir à quoi ressemblent des comportements légitimes et être en mesure de détecter les déviations est bien plus efficace. Personne ne connaît vos applications, données, appareils et votre environnement utilisateur mieux que vous.

L’usage de l’intelligence artificielle, de l’apprentissage automatique et du big data issu des données mondiales permettent aux prestataires de services managés d’anticiper les attaques chez leurs clients et d’agir avant d’en subir les conséquences.

D’autre part, les sociétés de conseil doivent gérer le facteur humain : assurer l’accompagnement, la sensibilisation et la formation des utilisateurs au sein de l’entreprise, y compris en simulant des attaques ou en testant la réaction des utilisateurs face à un faux mail de phishing.

3. Aider les entreprises à se protéger de l’intérieur

Les entreprises d’aujourd’hui font la part belle à la collaboration et à la connectivité. La sécurité doit refléter cette vision et être conçue de l’intérieur : au sein de l’application, du réseau, et au niveau des utilisateurs et des contenus. Une nouvelle approche s’avère donc nécessaire. Imaginez que vous soyez le maire d’une ville dont les maisons courent en permanence le risque d’un incendie. Allez-vous recruter toujours plus de pompiers ou chercher à rendre leurs maisons moins inflammables ?

À court terme, les pompiers sont évidemment essentiels ; mais à long terme, il faudra une approche différente et préventive.

C’est précisément ce à quoi le principe de sécurité intrinsèque fait référence : le fait d’intégrer dès le départ une couche de sécurité aux applications et au réseau. Les intégrateurs qui font l’architecture, déploient ou opèrent les infrastructures informatiques et clouds de leurs clients ont un rôle clé dans le choix des solutions d’avenir. Celles-ci doivent intégrer la sécurité « by design » dès leur conception, puis correctement paramétrées pour assurer protection et continuité de service.

4. Utiliser des logiciels pour sécuriser le réseau et l'infrastructure de façon intrinsèque

Comment s'y prendre ? Compte tenu de la complexité de la tâche, le logiciel est l'unique solution. L'abstraction logicielle du réseau et autres infrastructures permet d'utiliser des technologies telles que celle de la micro-segmentation. Grâce à cette dernière, le réseau virtuel peut être divisé en segments extrêmement granulaires au niveau des applications et processus.

Par défaut, chaque micro-segment est isolé des autres, ce qui, sur le plan fonctionnel, revient plus ou moins à protéger chaque application à l'aide d'un pare-feu « zero trust », puis à définir à quel type de connectivité elle peut avoir droit en établissant des règles de conduite. Cette approche limite les effets des failles, les logiciels malveillants ne pouvant se propager qu'au micro-segment suivant avant de se retrouver face à un nouveau pare-feu.

En outre, tout ceci étant mis en œuvre via logiciel, les stratégies de sécurité peuvent être automatisées, ce qui permet de prendre en charge un degré de complexité jusqu'ici inaccessible. Ce modèle garantit une autogestion efficace, et évite l'achat d'équipements coûteux et rigides, ainsi que l'erreur humaine. En d'autres termes, plus besoin de tenter l'impossible et de chercher à reconnaître l'avalanche de nouveaux logiciels malveillants ; au lieu de cela, concentrez-vous sur votre entreprise en profitant d'une sécurité intrinsèque.

Le partenaire sera l'architecte de cette nouvelle approche agile et définie par le logiciel. Il aura à concevoir, faire évoluer et automatiser ce nouveau réseau interne au datacenter afin de résoudre une équation technico économique insoluble via d'autres moyens : escalade des menaces et course contre la montre pour y répondre dans un budget limité.

5. Faire du réseau le cœur d'un nouveau modèle de sécurité

La plupart des entreprises sont entrées dans leur transition numérique. Si cette dernière promet de nouvelles expériences pour les clients, employés et partenaires, elle donne également de sérieux maux de tête aux équipes IT, car les modèles existants ne sont pas conçus pour faire face à un environnement aussi varié et complexe.

La sécurité a besoin d'un socle, et il s'agit du réseau. Les applications modernes étant toujours plus modulaires, existant sous la forme de micro-services interconnectés, ou étant exécutées depuis une multitude de conteneurs ou entre Clouds distribués, l'unique dénominateur commun est le fait que les éléments modulaires de chaque application sont connectés les uns aux autres grâce à un réseau étendu et multi-cloud.

Celui-ci devient critique et s'appuie sur des technologies de type SD-WAN (Software Defined Wide Area Network) qui est au réseau IP MPLS traditionnel ce que l'iPhone dernière génération est au premier GSM Nokia. Le partenaire intégrateur ou opérateur télécom trouvera sur ce sujet un marché en pleine effervescence et des opportunités de projets stratégiques chez tous les clients disposant de plusieurs sites géographiques.

6. Du Cloud à l'Edge, et au-delà

Il y a 5 ans, le principe de l'Edge Computing paraissait impossible, car tout tournait autour du data center. Mais tout comme les menaces, les capacités offertes par les systèmes informatiques évoluent presque au quotidien. Le réseau a ainsi pris les commandes, permettant à l'Edge Computing et à l'IoT d'offrir de nouvelles opportunités à chaque industrie qui génère et utilise des données. La quantité d'informations exploitables et utiles générées à proximité de capteurs est telle qu'il est tout simplement impossible désormais de les renvoyer dans le Cloud pour les traiter en temps réel.

C'est ici qu'intervient l'Edge Computing, qui consiste à traiter ces données à proximité de leur point de collecte pour pouvoir les utiliser en temps réel. Nous ne sommes bien sûr qu'au début de cette révolution et nous ignorons encore ce que nous réserve l'avenir, cependant deux choses sont claires : les logiciels au cœur de l'Edge doivent être intrinsèquement sécurisés, et le réseau sera le socle idéal pour y parvenir.

Avec une telle vision de la sécurité, c'est-à-dire celle d'une pièce constitutive de l'infrastructure elle-même, plutôt qu'un élément à positionner au niveau des frontières de l'entreprise devenues obsolètes, on favorise la mise en place et la pérennité de technologies fondamentales telles que l'Edge et l'IoT.

Les entreprises doivent aujourd'hui affronter une situation très complexe avec la multiplication des interactions, la prolifération d'objets connectés et des capteurs, la dispersion géographique des employés et font ainsi face à l'augmentation exponentielle de leurs vulnérabilités. Les partenaires ont désormais une opportunité unique de réorienter leurs échanges avec leurs clients en les invitant à mettre en place une sécurité intrinsèque à l'infrastructure qui répondra à leurs exigences actuelles et futures.