Special Report

METSYS

Microsoft

Metsys invite les entreprises à découvrir et adopter une sécurité moderne « Zero Trust »

Une démarche Zero Trust ne s'improvise pas. Elle se construit en adoptant une nouvelle culture de la sécurité et une multitude de briques de sécurité. C'est ce que Metsys a expliqué et démontré par la pratique un peu partout en France d'ateliers gratuits dédiés aux approches modernes de la cybersécurité et de la cyber-résilience des entreprises, au sein des Microsoft Labs.

L'approche Zero Trust, cette sécurité « sans confiance » au cœur des discussions actuelles sur la cybersécurité, ne se construit pas en un jour. Cette façon d'aborder la sécurité numérique des entreprises se construit progressivement, brique par brique, et présuppose la maîtrise d'un certain nombre de principes qui lui servent de fondation.

Comme le rappelle l'ANSSI dans son rapport sur « le modèle Zero Trust », « *cette approche demeure ardue, faute de maturité* ». D'autant qu'elle va exactement à l'inverse du principe de « *confiance implicite* » qui rythmait le modèle ancestral de défense périmétrique auquel trop d'entreprises restent encore attachées, alors qu'il n'a plus aucun sens dans un monde de travail hybride avec des collaborateurs travaillant à domicile et des données délocalisées dans le Cloud.

Le Zero Trust n'est pas une technologie. C'est un concept qui consiste à réduire la confiance accordée aux utilisateurs, aux administrateurs et aux appareils qu'ils utilisent en focalisant les efforts de sécurité sur les identités, le réseau, les accès, les applications, les données avec des contrôles permanents, granulaires et dynamiques.

Afin d'aider les entreprises à progresser sur le chemin du « Zero Trust », Metsys a animé avec Microsoft, des « Labs » dédiés à la cybersécurité moderne (format présentiel et en ligne, et disponibles également en replay). Au cours de ces « Labs 100% Cybersécurité », les interlocuteurs sont revenus sur les piliers d'une sécurité Zero Trust et sur les démarches et outils proposés par Microsoft pour adopter une posture « Zero Trust » complète, globale et pérenne.

Connaître son niveau de maturité

La démarche prônée par Metsys et Microsoft démarre par une compréhension du niveau de la maturité Cyber de chaque entreprise. « *Zero Trust is a journey* » (le Zero Trust est un voyage) » rappelle **Paul Dominjon**, directeur des solutions Cybersécurité chez Microsoft. « *Comme dans toute démarche, il est important de savoir d'où on part pour savoir quelles sont les étapes à suivre dans cette trajectoire qui vous mènera au Zero Trust. Applications des basiques de l'ANSSI, utilisation systématique du MFA, taux d'usage des applications cloud… Il est essentiel d'évaluer le niveau de maturité en matière de cybersécurité* ».

Microsoft a ainsi élaboré un questionnaire de maturité Zero Trust qui permet d'évaluer le degré d'avancement d'une entreprise sur la sécurisation des 6 piliers de la cybersécurité Zero Trust : les identités, le réseau, les accès, les applications, les données et l'infrastructure élargie au cloud.

Celui-ci en main, chaque entreprise peut mesurer les efforts à faire pour progresser sur ces 6 piliers avant d'adopter une posture « Zero Trust » à proprement parler. Des efforts qui doivent s'accompagner d'un changement de culture.

Un changement de culture…

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture. « *C'est un changement d'état d'esprit* » explique **Paul Dominjon**. « *Le passage en travail à distance imposé par la crise pandémique a fait exploser les dernières velléités de concevoir le SI comme un château fort* ».

Les confinements successifs et l'adoption du travail hybride qui en découle aujourd'hui ont encouragé bien des entreprises à réfléchir sur la notion de confiance, « à qui » elles pouvaient faire confiance et, au final, à prendre conscience qu'il est plus simple et plus logique de choisir par défaut de ne faire confiance à personne.

Par ailleurs, avec des besoins intensifiés par la crise de prendre le contrôle à distance des infrastructures privées mais également les besoins engendrés par une adoption massive des infrastructures dans le Cloud (IaaS), « *les entreprises ont cherché des moyens de mieux contrôler l'attribution des privilèges et de gérer avec une attention accrue les comptes administrateurs en s'assurant que les privilèges nécessaires à ces accès soient fréquemment remis à jour* » ajoute **Paul Dominjon**.

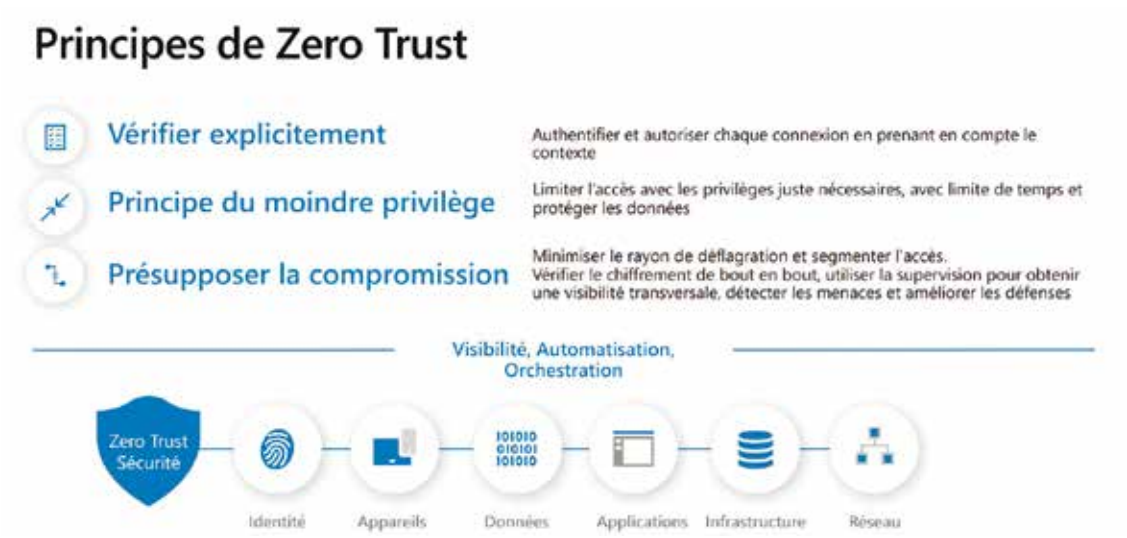
Enfin, la démarche Zero Trust est aussi marquée par un autre changement de mentalité fondamental comme l'explique **Hervé Thibault**, Chief Strategy Officer de Metsys : « *il est essentiel de présupposer que l'on est attaqué. Cela impose de savoir se projeter, de faire de la détection & réponse, et d'agir comme si le réseau était compromis* ».

… Qui nécessite un accompagnement

« *Face à un tel changement d'état d'esprit, qui demande à être expliqué, vulgarisé, assimilé, les entreprises ont besoin d'un accompagnement* » constate **Hervé Thilbault**. « *Et bien évidemment une telle approche a aussi un impact sur les outils et technologies à mettre en œuvre* ».

Microsoft propose ainsi de multiples briques permettant de couvrir l'ensemble des piliers d'une architecture Zero Trust. Ils permettent une approche progressive, éclairée par la compétence des experts cybersécurité de Metsys. « *Faire de Microsoft une fondation de sa sécurité peut encore surprendre certains responsables informatiques* » note **Hervé Thibault**. Pourtant, la division cybersécurité de l'éditeur comporte plus de 8.500 experts et réalise un chiffre d'affaires de 15 milliards de dollars, ce qui fait aujourd'hui de Microsoft l'un des tous premiers acteurs du marché de la cybersécurité.

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture.



L'approche Zero Trust repose sur 3 principes fondamentaux et 6 piliers sur lesquels se focalisent les efforts

Construit au fil du temps, ce portfolio de solutions est l'un des plus complets et des plus matures du marché. « *Aujourd'hui, les entreprises ne s'interrogent plus sur la performance des outils ou la pertinence de Microsoft en matière de sécurité. Nous sommes désormais bien plus interrogés sur l'articulation des multiples solutions qui forment la plateforme Microsoft* » confirme ainsi **Laurent Cayatte**, Président de Metsys.

Une offre qui couvre l'intégralité des besoins

L'offre Microsoft couvre aujourd'hui les 6 piliers de la sécurité Zero Trust :

* **L'identité** avec des concepts comme le MFA, le passwordless, l'accès conditionnel, la gestion dynamique des comptes à privilèges tous pris en charge par Azure AD et renforcé par son bouclier « Microsoft Defender for Identity ».
* **Le réseau** avec cette idée qu'Internet devient le réseau de l'entreprise et qu'il faut diminuer la surface d'attaque en pratiquant une segmentation (avec Azure Networking) et en s'appuyant sur Azure Firewall, Azure WAF, Azure Security, Microsoft Sentinel et Microsoft Defender XDR.
* **Les appareils et points d'accès** avec notamment la mise en œuvre de l'accès conditionnel Azure AD, mais aussi la sécurité des appareils avec Microsoft Defender for Endpoint et Microsoft Endpoint Manager mais aussi Microsoft Defender for IoT afin de protéger les appareils dans toute leur diversité.
* **Les applications** avec la solution CASB et Microsoft Defender for Cloud Apps,
* **Les données** avec une surveillance accrue des accès mais aussi le chiffrement et le classement automatique via Microsoft Information Protection.
* **L'infrastructure élargie au Cloud** avec Azure Security et Microsoft Defender for Cloud qui s'étend au-delà du Cloud Microsoft dans une véritable approche multicloud.

> Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain

Progresser sur ces piliers et assembler ce puzzle en un tout cohérent à même de soutenir une démarche Zero Trust est devenu une priorité pour bien des entreprises.

« *Ce qu'on a voulu montrer au travers des 4 ateliers, c'est toute la pertinence de l'approche Microsoft et la complétude de l'offre,* explique ainsi **Laurent Cayatte**, *mais aussi l'importance pour l'entreprise de se faire accompagner face à ce qui peut sembler un énorme défi à relever.* »

Special Report

En route vers le Zero Trust

Pour les DSI, les RSSI, les responsables d'entreprises, l'approche Zero Trust a quelque chose de très marketing. Derrière, se cachent des méthodes de travail nouvelles, des modes de fonctionnement nouveaux, et de nouveaux composants défensifs. Tout ceci ne se décide pas d'un claquement de doigts, ne s'implémente pas d'un clic et ne se maîtrise pas en un jour.

« *Les outils de sécurité ne sont pas là pour combler l'absence de stratégie et de bonnes pratiques* » explique **Laurent Cayatte**. « *À l'inverse, ils sont là pour implémenter les stratégies et la posture de sécurité élaborées conjointement par les responsables de l'entreprise, les responsables métiers, la DSI et le RSSI* ».

Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain, habitués à insuffler les bonnes pratiques et à mettre en œuvre les outils pour servir les besoins réels des entreprises. Des experts aussi capables de soutenir au plus près les clients lorsqu'ils sont attaqués.

« *Notre métier est d'avoir désormais une approche globale dans la construction de la sécurité d'infrastructure hybride, cloud et multicloud, dans la sécurisation des applications, dans la protection des données, dans la sécurisation des identités et jusqu'à la sécurisation de tous les appareils, du PC aux smartphones en passant par les équipements connectés (imprimantes, enceintes, etc.)* » conclut **Laurent Cayatte**.

Pour aller plus loin

Cybersécurité Metsys
https://www.metsys.fr/offres/cybersecurity/

Les ateliers gratuits proposés
https://www.metsys.fr/offres/cybersecurity/nos-offres-cybersecurite#programmes-financements-ms

Le maturity model Microsoft
https://www.microsoft.com/fr-FR/security/business/zero-trust/maturity-model-assessment-tool

METSYS
www.metsys.fr

Conception éditoriale & réalisation : Agence COM4MÉDIAS www.com4medias.com - crédit photos : Shutterstock