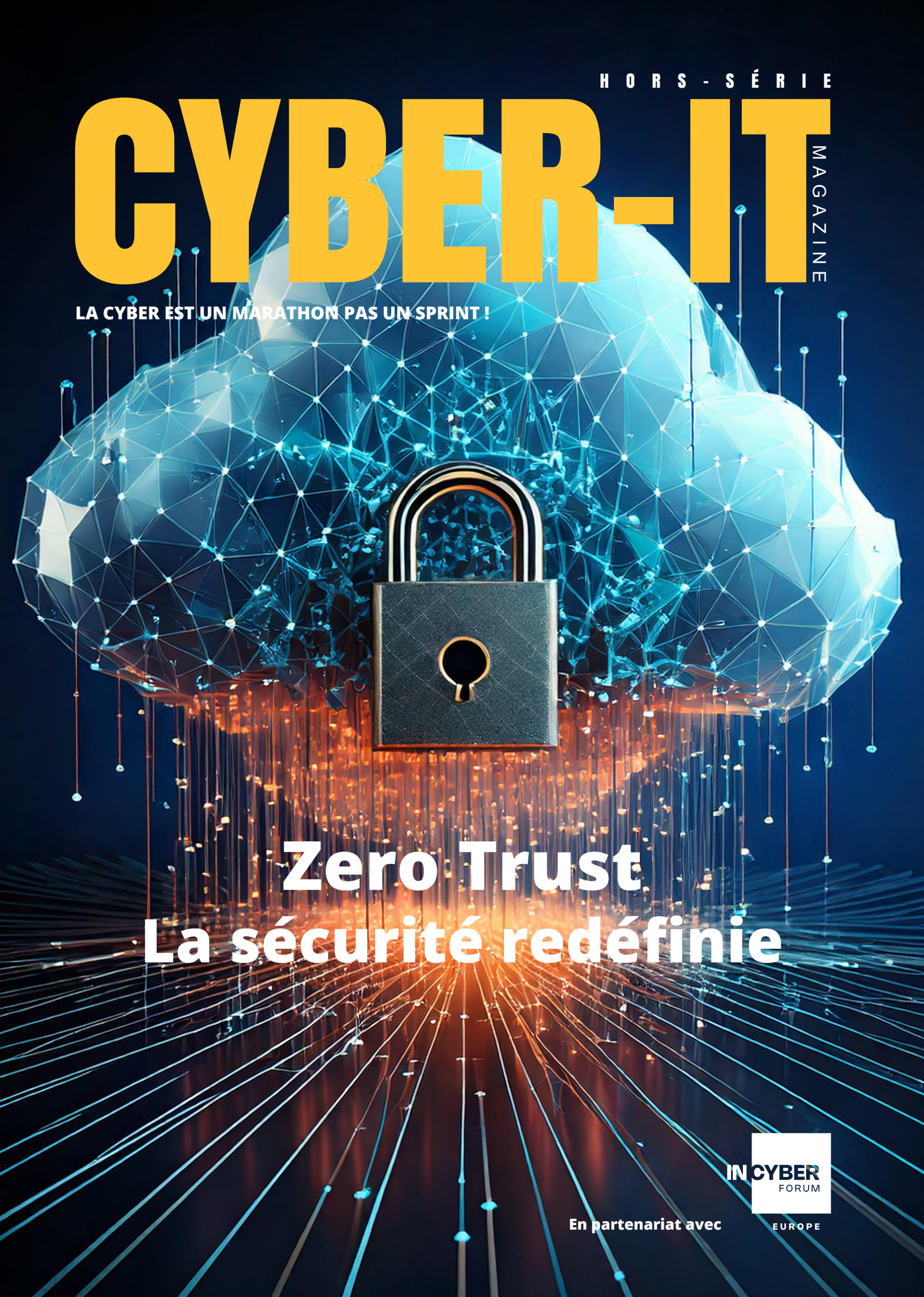
HORS-SÉRIE

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !



Zero Trust
La sécurité redéfinie

En partenariat avec

IN CYBER FORUM EUROPE

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Chers lecteurs,

Le Forum International de la Cybersécurité nous fournit une plateforme cruciale pour envisager les enjeux qui sculptent notre univers digital. Nous sommes particulièrement reconnaissants aux équipes du forum pour l'opportunité offerte au magazine de vous rencontrer en face à face et de discuter de différents sujets qui nous sont chers !

Au cours des dernières années, la montée du télétravail, l'augmentation du nombre d'appareils connectés et la complexification continue des cyberattaques nécessitent une approche fondamentalement nouvelle : le Zéro Trust.

L'application du Zéro Trust peut paraître compliquée, mais elle est indispensable pour protéger nos structures face aux menaces modernes. Cela requiert une approche globale, faisant appel à la participation de tous les intervenants, décideurs, équipes de sécurité et utilisateurs.

Dans ce hors-série, nous explorerons les différents aspects du Zéro Trust en commençant par les origines de ce concept que nous connaissons tous aujourd'hui, pour finir par une analyse de sa mise en pratique au sein des entreprises.

Le concept du zero trust peut sembler complexe à visualiser mais John Kindervag, son inventeur, a réussi à concevoir une analogie qui en facilite la compréhension.

Nous allons donc détailler cette analogie en nous basant sur ses propres déclarations.

ARNAUD LEROY

SOMMAiRE

Zero Trust
Un concept pas si récent

Le terme « Zero Trust » a été officiellement créé en 2010 par l'analyste John Kindervag, et sa définition a été incluse dans le rapport NSTAC, un document de plusieurs dizaines de pages sur le zero trust compilé en 2021 par le National Security Telecommunications Advisory Committee des États-Unis.

Zero Trust est une stratégie de cybersécurité fondée sur l'idée qu'aucun utilisateur ou actif ne doit être implicitement digne de confiance.

Elle suppose qu'une violation a déjà eu lieu ou va se produire et, par conséquent, qu'un utilisateur ne doit pas se voir accorder l'accès à des informations sensibles par une seule vérification effectuée au niveau du périmètre de l'entreprise.

Au lieu de cela, chaque utilisateur, appareil, application et transaction doit être vérifié en permanence.

Le concept Zero Trust est né en 2010, lorsque John Kindervag de Forrester Research a développé les premières conceptions. À l'époque, les approches de sécurité basées sur le périmètre du réseau étaient dominées par un modèle de confiance, qui désignait l'interface externe d'un pare-feu traditionnel comme « non fiable » et l'interface interne comme « fiable ». Dès lors Kindervag a commencé à reconnaître ce modèle de confiance comme une problèmatique persistante.

Chronologie d'un concept

1987 — Définition de la protection réseau

Des ingénieurs de la Digital Equipment Corporation (DEC) publient le premier article sur la technologie des pare-feu, inaugurant ainsi des décennies de réflexion sur la sécurité cloisonnée des réseaux

1990 — Segmentation du réseau

Les premiers efforts pour segmenter le réseau à travers l'utilisation de VLAN ou de sous-réseaux commencent à émerger. Une méthode ne nécessitant pas d'authentification, comportant des restrictions minimales et possédant peu de fonctionnalités de sécurité interne.

2001 — Contrôle d'accès au réseau

L'IEEE Standards Association publie le protocole 802.1X pour le contrôle d'accès au réseau (NAC)

2010 — Les prémices

Le forum Jericho est créé. Il prend acte du fait que les utilisateurs et les applications quittent le réseau de l'entreprise et introduit les premiers concepts de Zero Trust via le principe de « dépérimétrisation »

2010 — Naissance du Zero Trust

L'analyste John Kindervag présente le « modèle Zero Trust » dans un article pour Forrester Research. Il déplace l'authentification et la sécurité inline, et suggère la segmentation des sessions. Toujours axé sur l'accès au réseau, il déplace le périmètre à l'intérieur de celui-ci

2014 — Google entre en jeu

L'initiative BeyondCorp de Google redéfinit l'architecture de sécurité en profondeur. L'attaque Operation Aurora a conduit à la mise en œuvre du modèle Zero Trust à l'échelle de l'entreprise

2016 — Zero Trust dans le cloud

Zscaler propose la première solution Zero Trust déployée via le cloud, offrant aux entreprises la possibilité de supprimer la surface d'attaque extérieure et de réduire le risque de mouvement latéral

2019 — Gartner - ZTNA

Gartner a introduit les notions de SASE (Secure Access Service Edge) et Zero Trust Network Access

2020 — Définition du cadre par le NIST

Le NIST dévoile la norme SP 800-207 en tant que modèle unifié pour établir une architecture Zero Trust (ZTA), et présente le premier véritable changement concernant la définition de Zero Trust dans le cadre du réseau

2021 — Mise en avant du SSE

Selon Gartner, les éléments de sécurité du SASE sont considérés comme une nouvelle catégorie sur le marché, dénommée Security Service Edge

2022 — Les Etats-Unis impose le Zéro Trust

L'Office of Management and Budget exige que toutes les agences adoptent les principes du Zero Trust depuis 2024

Source : Zscaler

BIEN COMPRENDRE LE ZERO TRUST

ANALOGIE ENTRE LES SERVICES SECRETS ET LE ZERO TRUST

Article inspiré de l'interview de John Kindervag réalisé par MIEL. Propos recueillis par Kamel Mouhoubi.

John Kindervag, créateur du concept du zero trust, a été reçu par Kamel Mouhoubi lors d'un interview pour la chaine de la société MIEl. Lors de ce moment privilégié, John a fait une analogie entre les services secrets américains et le principe même du zero trust. En voici les grandes lignes.

Quand les services secrets assurent la protection du président américain, ils détiennent trois informations sur lui que nous avons généralement tendance à ignorer.

Avant tout, ils sont au courant de l'identité du président. En second lieu, ils ont toujours connaissance de l'emplacement du président. Ils ne posent jamais la question « Avez-vous vu le président ? »

Ceci ne se produit jamais !

En troisième lieu, ils sont au courant de qui devrait avoir accès au président en toutes circonstances. Voici les trois questions essentielles que vous devez vous poser, que ce soit pour la protection du président, de vos données ou de vos actifs, le principe reste identique.

L'exemple visuel le plus approprié pour démontrer ce concept est le défilé d'inauguration du président Barack Obama en 2009. On peut observer la présence d'un périmètre (dans le coin supérieur droit de l'image) entouré par des agents. Ils ne sont pas là pour fournir une protection réelle, c'est plutôt une sorte de démonstration destinée à intimider et à faire comprendre qu'il est interdit de dépasser cette limite. La sécurité réelle est garantie en bas de l'image.

La voiture incarne la zone de sécurité, elle est l'idée tactique essentielle du principe du zéro confiance. Il est crucial de comprendre ce qu'est la surface de protection, sinon l'idée même du zero trust perd toute signification. La surface de protection est donc l'opposé de la surface d'attaque. La surface d'attaque est ingérable, ce qu'il faut c'est inver-

ser le problème et le réduire à quelque chose de petit et facile à connaître. C'est ce qu'on nomme la surface de protection.

Cette protection est marquée par la présence de quatre individus (les cercles dans l'automobile symbolisent le président, son épouse et leurs deux enfants). Si à la fin de la journée, ces quatre personnes sont saines et sauves, cela signifie que les services secrets ont bien accompli leur mission. Ils identifient ce qu'ils doivent défendre, ce qui en matière de cybersécurité est identique, comprendre ce qui nécessite une protection.

On peut voir sur l'image que les services secrets se déplacent à proximité de la surface de protection. Ils établissent une petite zone qui isole le président et sa famille de tout ce qui est extérieur. Ils réalisent une tâche que nous ne sommes pas en mesure d'accomplir, gérer l'accès à ce micro périmètre.

Dans le domaine de la cybersécurité, nous réalisons nos vérifications sur l'étendue qui est aussi distante que possible de ce que nous tentons de sauvegarder. Ceci génère une seconde zone vulnérable que l'on désigne comme le réseau interne. Cela génère une zone tampon entre l'actif et le périmètre.

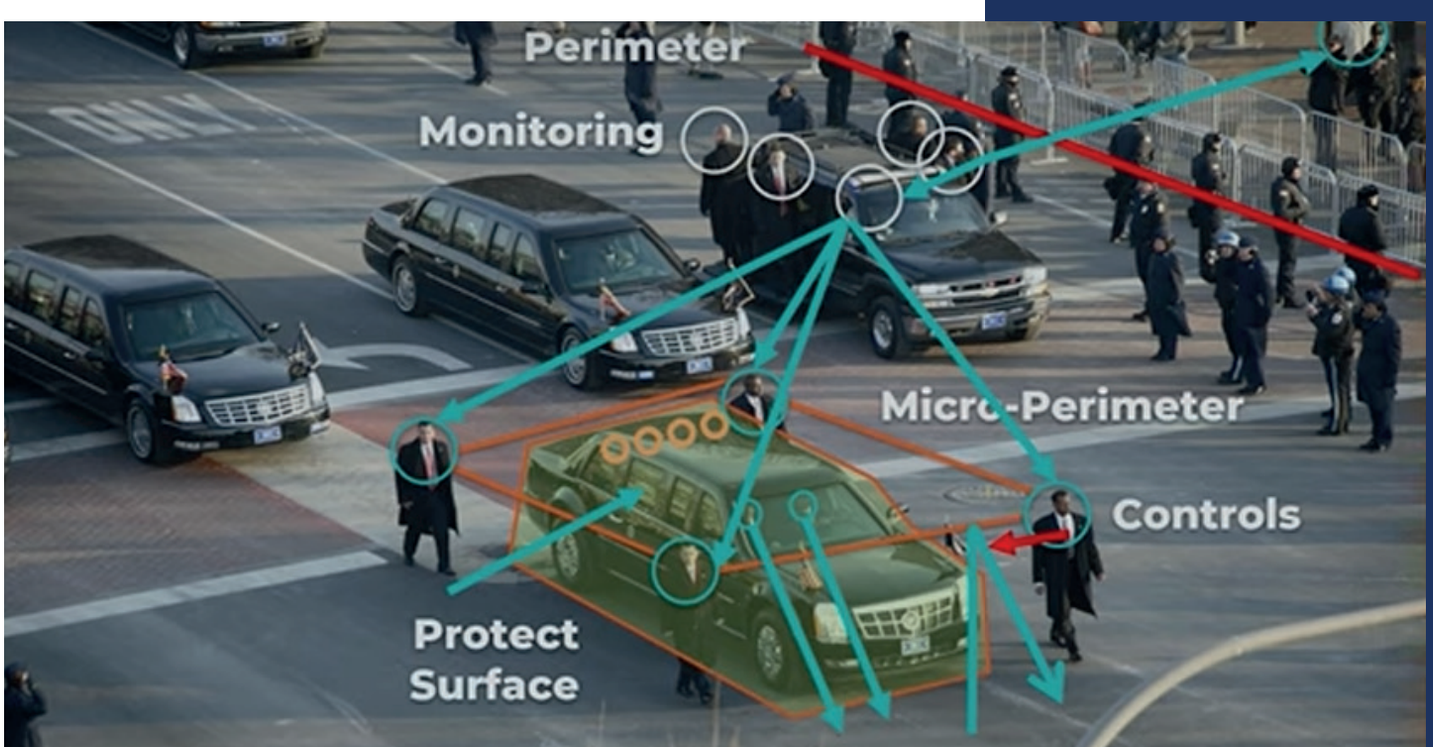
Le zero trust élimine cette zone tampon, il n'y à pas d'endroit ou se cacher car nous avons une visibilité totale de ce qui essaie d'accéder à ces ressources sensibles. La politique de sécurité est le fondement de toute stratégie de cybersécurité et du modèle zéro trust. Si un mal survient dans un contexte donné, c'est que la politique en vigueur a favorisé sa survenue.

Dans un contexte de zero trust, une politique ne permet que d'autoriser ou de refuser.

On débute avec une stratégie de refus, puis on met en place des directives d'autorisation détaillées en fonction du besoin d'un individu d'accéder à certains éléments pour l'exercice de ses fonctions. Si quelqu'un tente d'accéder au président les agents proches du véhicule l'arrêterons violemment et appliquerons cette règle de refus à ce moment précis.

Les agents, qui surveillent et actualisent constamment leurs règles, récoltent ainsi des informations sur les menaces en scrutant la foule. Par exemple, l'individu en blanc dans le coin supérieur droit de l'image est sous la surveillance du monitoring. Ils ont la capacité d'ajuster leur politique de façon dynamique, par exemple pour permettre à une personne d'accéder au président.

Tout ceci peut être transposé à la cybérsecurité .



Le Zero Trust, mission impossible ?

En effet, la transition vers Zero Trust est un objectif ambitieux, une initiative de transformation qui nécessite d'être envisagée à long terme. C'est également une véritable chance de s'adapter à un environnement qui s'est considérablement modifié au cours des dix dernières années. Voici quelques pistes de réflexion.

Bien comprendre le principe pour une bonne mise en oeuvre

L'initiation d'un projet Zero Trust requiert une connaissance approfondie des concepts Zero Trust et des éléments technologiques qui permettront leur application concrète. L'idée est d'adapter la vision en fonction de son propre contexte actuel.

L'objectif est de saisir les principes du Zero Trust qui guideront l'ensemble du projet, le choix des technologies employées et leur exploration approfondie.

Le concept de Zero Trust stipule que « tous les utilisateurs et dispositifs doivent avoir la possibilité d'accéder aux ressources appropriées depuis n'importe quelle localisation, sous les mêmes normes de sécurité ». Il s'articule autour de trois axes principaux, vérification, implémentation et présomption de compromission :

1- Vérification explicite : examiner de manière dynamique le contexte de l'accès - l'identité, le lieu d'où l'on se connecte, le dispositif employé et sa condition optimale, etc.

2- Mettre en place un accès basé sur le principe du moindre privilège : il faut s'assurer, selon ce contexte, que la personne qui a accès n'a que les privilèges nécessaires pour utiliser l'application. Cela peut être précisé en attribuant une plage horaire pour l'accès.

3- Adopter une posture de présomption de compromission : adopter une attitude où l'on reconnaît la possibilité d'être compromis et veiller à pouvoir identifier les attaques et les contenir rapidement afin de limiter leurs conséquences.

Identifier les attentes liées à la mise en place du Zero Trust

La question fondamentale sera donc : quels problèmes doit-on résoudre et dans quel ordre de priorité ?

Pour y parvenir, on adopte une approche qui implique de **« faire du brainstorming »** lors d'ateliers non techniques. L'objectif est de cerner les attentes en les exprimant sous forme de souhaits « de haut niveau », c'est-à-dire dénué de détails techniques.

Il sera ensuite nécessaire d'attribuer une priorité à chaque attente de la liste que vous aurez constituée. Par exemple, vous pourriez donner la priorité à la défense contre les ransomwares ou à la sauvegarde des données essentielles. Les options

pour répondre à chaque exigence peuvent impliquer divers piliers, diverses technologies par pilier et varier en termes de complexité de mise en œuvre.

Les attentes se regroupent en deux volets : une amélioration de la sécurité et une approche réfléchie face à de nouveaux scénarios, en harmonie avec les défis récents. La sécurité occupe, de fait, une place prépondérante étant donné que le Zero Trust représente un modèle de sécurité récent.

Cependant, il est également important d'évaluer les avantages sous l'angle commercial. Il est crucial de transformer l'approche négative et alarmante de la sécurité en une perspective qui la perçoit comme un outil d'adaptation tout en préservant les ressources et le fonctionnement de l'entreprise dans un contexte devenu extrêmement complexe.

Définir son niveau de maturité

Lors de votre transition vers le Zero Trust, **vous ne partez pas de zéro** : vous devez tenir compte de l'existant et il est possible que vous ayez déjà mis en place des outils ou technologies qui représentent un premier pas vers l'adoption du modèle Zero Trust.

Il est possible que vous ayez déjà appliqué certaines règles de contrôle d'accès conditionnel pour protéger l'accès à diverses applications, ou mis en place l'authentification multi-facteurs pour une section de vos collaborateurs ? Pour évaluer votre niveau de maturité Zero Trust, vous pouvez consulter le livre blanc ZERO TRUST MATURITY MODEL de Microsoft dont le tableau ci-dessous fournit une vue d'ensemble pour les piliers Identités et Appareils.

Selon les fonctionnalités que vous avez déjà mises en œuvre, vous pourrez vous situer dans un niveau **Traditionnel**, **Avancé** ou **Optimal** selon les piliers.

Cette évaluation du degré de maturité vous offre une première opportunité d'examiner votre situation actuelle. Cette activité est essentielle car elle vous offre l'opportunité de répertorier les solutions existantes susceptibles de s'inscrire dans la perspective Zero Trust, le niveau de complexité potentiel pour leur incorporation, ainsi que les solutions à substituer.

Prenons l'exemple de la détection des attaques de rançongiciel : c'est actuellement le point faible, si votre SIEM ne permet pas d'identifier efficacement ce type d'attaque et de réagir sans délai. Un EDR devrait être envisagé éventuellement couplé à un SIEM qui pourrait détecter rapidement des postes compromis et les isoler pour éviter la propagation.

Ou encore, la capacité de reconstruction d'un nombre important de postes dans un délai court est trop compliqué ? Une solution automatisée et performante, idéalement sous forme de service cloud serait à envisager.

niveau de complexité potentiel pour leur incorporation, ainsi que les solutions à substituer.

Déterminer en premier lieu les quick wins

Les quick wins ont un aspect positif : ils sont à la fois **stimulants** pour les équipes et procurent rapidement des résultats concrets. Ils apportent aussi des garanties à un niveau supérieur concernant la faisabilité et les effets bénéfiques du projet Zero Trust. L'inconvénient, c'est qu'ils peuvent donner une fausse impression de conclusion du projet et faire croire que « voilà, nous sommes Zero Trust ».

La mise en place du SSO pour les applications les plus

	Traditionnel	Avancé	Optimal
Identités	Le référentiel d'identité est on-premises Pas de SSO entre le cloud et les applications on-premises Visibilité limitée sur les risques liés à l'identité	L'identité Cloud est fédérée avec le système on-premises Les politiques d'accès conditionnel contrôlent l'accès et fournissent des actions correctives L'analyse des signaux améliore la visibilité	L'authentification sans mot de passe est activée L'utilisateur, l'appareil, l'emplacement et le comportement sont analysés en temps réel pour déterminer les risques et fournir une protection continue
Appareils	Les appareils sont joints au domaine et gérés avec des solutions telles que Group Policy Object ou Config Manager Les appareils doivent être connectés au réseau pour accéder aux données	Les appareils sont enregistrés auprès du fournisseur d'identité cloud Accès uniquement accordé aux appareils gérés et conformes dans le cloud Les stratégies DLP sont appliquées pour les appareils d'entreprise et BYO	Un EDR (Endpoint threat detection) est utilisée pour surveiller les risques liés aux appareils Le contrôle d'accès est basé sur le risque de l'appareil pour les appareils d'entreprise et BYO

Tableau d'évaluation du niveau de maturité Zero Trust par Microsoft

populaires ou les plus critiques seraient visibles et pas obligatoirement complexes.

Si on considère l'objectif de la lutte contre les rançongiciels, la mise en place d'un EDR apportera rapidement une visibilité sur les menaces provenant des postes et permettra de réagir en conséquence.

Un quick win est considéré comme une étape tactique, offrant un bénéfice direct et perceptible, mais qui doit s'intégrer dans une approche stratégique symbolisée par la transition vers le modèle Zero Trust.

Accorder la priorité au pilier Identité

Dans le modèle Zero Trust, l'identité est l'élément crucial, liée à l'appareil utilisé pour accéder. On soutient même que « l'identité est le nouveau champ d'action » étant donné que nombre de violations concernent le vol d'identifiants ou des usurpations d'identité.

La compromission de l'identité est le point d'entrée de la plus grande majorité des attaques perpétrées sur les entreprises ou organisations, selon le rapport 2024 Trends in Securing Digital Identities 90 % des organisations ont connu au moins un incident lié à l'identité au cours de l'année écoulée.

Il est possible de mettre en place l'authentification sans mot de passe qui supprime de facto les faiblesses liées à l'utilisation des mots de passe. L'authentification peut s'appuyer sur une caractéristique biométrique telle qu'un visage ou une empreinte digitale, ou un code confidentiel propre à un appareil et qui n'est pas transmis sur le réseau.

A l'authentification forte s'ajoute l'élément clé du Zero Trust, le contrôle d'accès conditionnel, qui prend en temps réel les décisions d'accès aux ressources en prenant en compte le contexte de la requête : utilisateur avec évaluation du risque sur l'identité, appareil avec évaluation de la conformité, de l'état de santé, endroit depuis lequel est effectuée la demande et l'ensemble de signaux collectés

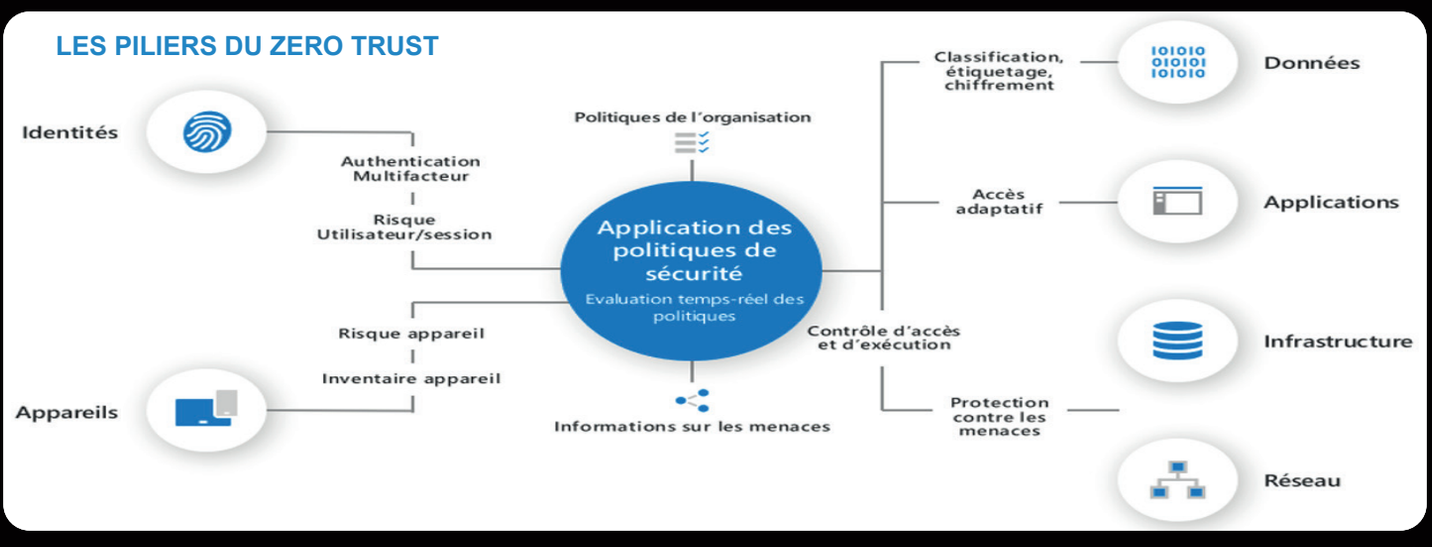
Superviser la sécurité

L'un des fondements du Zero Trust est la présomption de compromission, c'est-à-dire que, malgré toutes les mesures de sécurité en place, on doit supposer qu'une attaque pourrait se produire et donner accès au système d'information.

Si la supervision de la sécurité n'est pas spécifiée comme pilier du Zero Trust, elle n'en constitue pas moins une composante transversale, comme l'indique la plupart des professionnels du secteur.

Le pillier identitaire étant considéré comme le « nouveau périmètre » et la cible principale des attaques, il est devenu essentiel de le surveiller.

Le SIEM, regroupe les signaux provenant d'une diversité de sources variées pour essayer d'en tirer les signaux faibles, générer des alertes pertinentes et permettre une enquête sans avoir à naviguer entre différentes consoles. Il est regrettable que les solutions SIEM traditionnelles soient susceptibles



Source : Microsoft

de générer des faux positifs.

Les solutions plus modernes basées sur le cloud et l'Intelligence Artificielle (IA) se montrent plus performantes pour gérer ces grandes quantités de signaux, réduire les faux positifs et proposer des options d'orchestration et de réaction automatique.

Considérer Internet comme un réseau d'entreprise

L'un des principes du Zero Trust est d'assurer un niveau de sécurité uniforme, peu importe l'emplacement d'où l'utilisateur et son appareil accèdent à l'application ou au service.

Par ailleurs, une majorité d'applications est aujourd'hui accessible en ligne, qu'il s'agisse d'applications de fournisseurs tiers en mode SaaS ou d'applications internes transférées vers le cloud.

Quand vos identités sont administrées dans votre Active Directory, que tous les postes de travail sont gérés via des services basés sur le cloud, que les applications peuvent être utilisées à distance et que les systèmes de sécurité ont la capacité d'opérer depuis le cloud, l'idée même du réseau devient banale.

Cela contribue au constat que, ,« Internet se transforme en réseau d'entreprise ».

Les pratiques recommandées en matière d'architecture de sécurité réseau pour les applications internes sont également pertinentes pour les applications hébergées dans le cloud, notamment en ce qui concerne la segmentation des sous-réseaux, les DMZ et l'utilisation des contrôles réseau.

Il est recommandé d'implémenter une segmentation du réseau pour les ressources qui demeurent localisées en interne. Concernant les systèmes OT et IoT, il est recommandé de procéder à une segmentation plus précise en respectant plusieurs niveaux selon le modèle Purdue, développé par Theodore J. Williams.

Établir une feuille de route

La feuille de route représente la conclusion de vos réflexions lors de cette étape préliminaire de votre projet Zero Trust. Il s'agit de la tâche que vous devez accomplir pour classer tous les sujets à aborder, les organiser et estimer le temps qu'ils nécessiteront.

Il est essentiel de considérer les priorités principales, les quick wins, bien qu'ils ne soient pas explicitement mentionnés dans la stratégie globale et de préciser les étapes clés. Les thèmes seront distribués en fonction des six principaux axes du Zero Trust.

Voici donc quelques réflexions sur l'approche Zero Trust, qui vous aideront à envisager la transition avec plus de tranquillité et à renforcer la sécurité de votre entreprise.

CREDITS

Rédacteur : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume POUPARD

Avril 2025