Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC
Sécurité informatique de la Confédération SEC

26 juillet 2023

Considération technologique

Principe «Zero Trust»

1 Introduction

Le troisième paragraphe du chapitre 3 (Principes) de la Si001 [1] faire référence au principe «Zero Trust», qui ne peut pas être défini précisément, mais peut au moins être décrit comme suit: «dans la mesure du possible, le dispositif de sécurité d'un objet à protéger devrait être conçu de manière à ce que les exigences de sécurité […] puissent être satisfaites en toute autonomie et à ce que l'objet soit isolé de son environnement, de sorte qu'il faille faire le moins d'hypothèses possibles sur la sécurité de ce dernier.» Les exigences de sécurité se réfèrent à celles mentionnées dans [1], mais peuvent en principe être adaptées.

La présente considération technologique expose le contexte dans lequel est né le principe «Zero Trust», ainsi que les possibilités et les risques que celui-ci comporte, et aboutit à des conclusions et des perspectives sur ce sujet. Étant donné que le principe «Zero Trust» ne s'applique pas uniquement à l'administration fédérale, les premières considérations se réfèrent à une infrastructure ou à un environnement informatique moderne au sens large, comme on en trouve et utilise également en dehors de cette organisation. Ce n'est qu'à la fin que les implications sur la situation et le modèle de zones de l'administration fédérale sont esquissées.

2 Contexte

Le principe ou modèle «Zero Trust» est né du constat que les infrastructures ou environnements informatiques ont fondamentalement changé au fil du temps et qu'il est aujourd'hui difficile de les compartimenter ou de les protéger à l'aide de périmètres physiques ou logiques. À titre d'exemple, l'illustration 1 montre les périmètres physiques et logiques d'un centre de calcul (a), d'une architecture typique client-serveur (b) et de l'informatique en nuage (c). On peut constater que de plus en plus de systèmes (clients et serveurs) se trouvent en dehors des périmètres et que la protection propre au périmètre logique et, plus encore, au périmètre physique, diminue. Aujourd'hui, une grande partie de l'informatique est décentralisée et comprend de nombreux terminaux dans tous les formats possibles, comme les ordinateurs personnels, les ordinateurs portables, les tablettes et les smartphones. Il devient par conséquent de plus en plus difficile pour une organisation de définir les limites de son infrastructure informatique et donc ses périmètres. L'émergence de concepts tels que la

«dépérimétrisation[1]» et des difficultés croissantes rencontrées dans le cadre de l'exploitation de technologies de sécurité informatique qui s'appuient sur les périmètres, comme les pare-feux et les serveurs proxy, témoignent de cette évolution et constituent aujourd'hui déjà un grand défi.

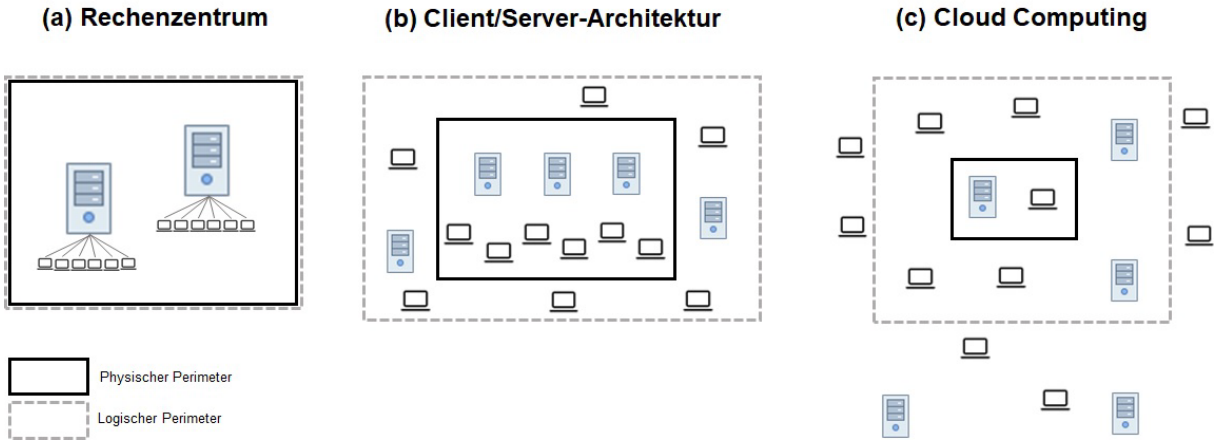

Illustration 1: évolution des infrastructures et environnements informatiques

En l'absence de périmètres définis, tant les terminaux que les systèmes serveurs fournissant des services doivent être en mesure de s'authentifier mutuellement et de démontrer qu'ils disposent de l'autorisation nécessaire ou sont en mesure de se protéger à l'aide de technologies de sécurité informatique appropriées. Pour les environnements BYOD (*Bring Your Own Device*), cela suppose notamment l'utilisation de technologies de sécurité informatique complémentaires, comme des agents ou des solutions MDM (*Mobile Device Management*). C'est dans ce contexte que John Kindervag et son équipe auprès de Forrester Research ont établi le modèle «Zero Trust» [For10], en 2009. Alors qu'à l'origine ce modèle visait à réduire les risques de sécurité émanant des initiés, à l'heure actuelle, il s'agit avant tout de repérer et d'éviter les «mouvements latéraux». Il s'agit des méthodes utilisées par les cybercriminels pour tenter de pénétrer plus avant dans un réseau après une intrusion initiale et de compromettre d'autres comptes afin d'augmenter progressivement leurs droits d'accès et de contrôler finalement la totalité du réseau attaqué.

Le modèle «Zero Trust» s'appuie sur des concepts et principes fondamentaux de la sécurité informatique tels que (i) l'accès aux ressources doit toujours être sécurisé peu importe où elles se trouvent, (ii) le contrôle des accès doit suivre le principe «Least Privilege» (cf. Si001, chap. 3, 6e paragraphe) et (iii) la totalité du trafic de données doit être considérée et, le cas échéant, enregistrée à l'aune de sa pertinence pour la sécurité. Il constitue moins un modèle d'architecture concret qu'une nouvelle approche qui vise à l'autoprotection des ressources informatiques et se passe de protection de périmètre. La notion de «changement de paradigme», parfois utilisée dans ce contexte, paraît toutefois un peu démesurée. Il semble dans tous les cas plus approprié de parler de principe «Zero Trust» ou alors de «Trust Establishment», car il s'agit en fin de compte d'établir la confiance et les relations de confiance correspondantes. À cet égard, certains aspects dynamiques doivent également être davantage pris en compte. Ainsi, l'authentification ne doit pas porter que sur les partenaires de communication au début d'une session, mais aussi sur les données échangées. La prise en compte d'aspects dynamiques doit toujours être encadrée et accompagnée par les collaborateurs compétents d'un SOC (*Security Operations Center*).

[1] https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

À partir du modèle «Zero Trust» proposé par Forrester Research, le NIST (National Institute of Standards and Technology) a présenté plusieurs possibilités de mise en œuvre d'une ZTA (*Zero Trust Architecture*) [NIST20]. Une ZTA prévoit des PDP (*Policy Decision Points*) sur le plan du contrôle et des PEP (*Policy Enforcement Point*) sur le plan des données et s'accompagne de concepts tels que la microsegmentation, la micropérimétrisation et l'EIG (*Enhanced Identity Governance*). Concrètement, cela signifie que les fonctions de sécurité ne sont plus implémentées de manière centralisée au niveau d'un périmètre, mais de manière décentralisée et à proximité des objets à protéger. L'affirmation extrême selon laquelle les identités constituent le nouveau périmètre est également caractéristique de cette approche architecturale (et de l'EIG).

3 Possibilités et risques

Selon le principe «Zero Trust», un objet à protéger doit être conçu de manière à ce qu'il puisse se protéger lui-même contre les attaques et repousser les tentatives d'accès non autorisées, ce qui est judicieux d'un point de vue technique, car un autocontrôle de sécurité effectué par l'objet à protéger offre en principe moins de possibilités de contournement. En revanche, cela se fait au détriment de la performance et de l'évolutivité. Les technologies de sécurité informatique basées sur le périmètre ont en effet été conçues et largement mises en œuvre précisément parce que les fonctions de sécurité et leur implémentation se concentrent sur un petit nombre de systèmes (centraux) et ne touchent pas les autres systèmes. L'avantage qui en résulte disparaît avec l'application du principe «Zero Trust».

Le principe «Zero Trust» et les variantes de mise en œuvre d'une ZTA décrites dans [NIST20] donnent la possibilité de simplifier et d'épurer les structures des réseaux et les zonages correspondants. Étant donné qu'il n'y a plus de périmètre dans une ZTA, il n'est plus nécessaire de classer les ressources informatiques comme «internes» ou «externes». Toutes les ressources sont traitées sur un pied d'égalité, dans la mesure où elles doivent elles-mêmes assurer des fonctions et des services de sécurité. Ces fonctions et services peuvent toujours être fournis de manière centralisée, mais leur utilisation est organisée de manière décentralisée et peut être discutée au cas par cas. Les services d'authentification, par exemple, sont toujours judicieusement fournis de manière centralisée, alors que les services d'autorisation sont plutôt décentralisés tout en étant encore éventuellement coordonnés de manière centralisée (cette approche est notamment à la base du système d'authentification et de distribution de clés Kerberos). Il en résulte davantage de flexibilité et de liberté d'organisation. En revanche, les fonctions et les services de sécurité nécessaires risquent de ne pas être assurés ou alors seulement de manière insuffisante. Il faut décider au cas par cas si cela est supportable pour un objet à protéger, en fonction de la protection dont il a besoin.

4 Conclusion et perspectives

Alors que, par le passé, la sécurité informatique misait très fortement sur la protection de périmètre et la centralisation correspondante des fonctions de sécurité informatique, on assiste depuis quelque temps à une forte tendance à la décentralisation et à l'application de nouvelles méthodes de «Trust Establishment» dans le cadre du principe «Zero Trust» et des ZTA. Heureusement, les technologies de sécurité informatique basées sur un périmètre et le principe «Zero Trust» ne s'excluent pas mutuellement. En effet, certaines de ces technologies restent applicables à un périmètre (de manière centralisée), tandis que d'autres sont plutôt mises en œuvre (de manière décentralisée) sur des objets à protéger ou à proximité de ceux-ci. Le principe «Zero Trust» n'est donc pas non plus la solution miracle applicable

dans tous les cas. Il peut en revanche être utilisé de manière bien dosée dans certaines situations afin d'améliorer un dispositif de sécurité dans son ensemble.

Dans l'administration fédérale, il peut par exemple être intéressant d'assouplir l'exigence S1 de la norme Si001 [1] afin qu'un système informatique ne doive plus nécessairement être «affecté à une zone et exploité conformément à la réglementation de cette zone», mais qu'il puisse aussi être chargé de la mise en œuvre des services de sécurité, conformément au principe «Zero Trust». Un tel assouplissement peut notamment être utile lorsque des systèmes informatiques ou des applications sont exploités dans un nuage public. Il convient toutefois de vérifier analytiquement ou empiriquement si, dans un tel environnement, la mise en œuvre du principe «Zero Trust» en tant que nouvelle méthode de «Trust Establishment» peut réellement être appliquée et si elle est efficace. Pour ce faire, il est bien entendu nécessaire de disposer de valeurs empiriques internes et externes à l'administration fédérale.

Abréviations

BYOD	Bring Your Own Device (prenez votre propre appareil)
EIG	Enhanced Identity Governance (gouvernance améliorée des identités)
MDM	Mobile Device Management (gestion des appareils mobiles)
NIST	National Institute of Standards and Technology
PDP	Policy Decision Point (point de décision de politique)
PEP	Policy Enforcement Point (point d'application des règles)
SOC	Security Operations Center
ZTA	Zero Trust Architecture (architecture «Zero Trust»)

Références

[Si001] NCSC, Si001 – Protection informatique de base dans l'administration fédérale, version 5.0 du 1er mars 2022

[For10] Forrester Research, «No More Chewy Centers: Introducing The Zero Trust Model Of Information Security», 2010 (en anglais uniquement)

[NIST20] NIST Special Publication 800-207, Zero-Trust Architecture, août 2020 (en anglais et japonais uniquement)