Orange CyberSchool, Direction de la formation
Notes de cours éditées le 8 mars 2024, 16 h 51 CET

Architectures, Composants et Sécurité

Yann-Arzel LE VILLIO[1,2*]

Résumé
Ce document présente les architectures, Composants de cybersécurité.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Architectures, composants sécurité, SSI

[1] *Enseignant Sécurité ESIR*
[2] *Directeur Technique et Scientifique Orange CyberSchool*
***email** : yann-arzel.levillio@orange.com –

Eléments de cours

Vérifiez la disponibilité d'une version plus récente de
L-Orange-Cyberdef101-M3c-Architectures.doc.pdf sur GITHUB CYBERDEF [1]

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/L-Orange-Cyberdef101-M3c-Architectures.doc.pdf

Table des matières

Table des figures

1. Introduction Architecture

Nous allons dans ce chapitre aborder les sujets d'architectures sécurisées afin d'appréhender la complexité de l'environnement technique du client.

L'analyse des menaces et des risques sur un périmètre défini permet d'identifier les fonctions de sécurité qui réduiront les impacts et qui doivent être inscrites dans la politique de sécurité et mises en oeuvre au sein de l'architecture.

L'ensemble de ces fonctions ainsi que les composants de l'architecture doivent être sécurisés à l'aide de contrôle, de filtrage des accès, de cloisonnement et l'utilisation d'algorithmes cryptographiques.

Nous identifierons les composants services, terminaux et réseaux du système d'information afin de les intégrer dans la politique de sécurité protective.

Puis nous découvrirons l'évolution des architectures de sécurité périmétrique depuis le modèle du château fort jusqu'au ZeroTrust ainsi que les composants et services assurant les fonctions de sécurité comme le pare-feu, les proxy, les bastions et les solutions utilisées pour sécuriser les architectures de type CLOUD.

Enfin, nous étudierons dans la dernière partie de ce chapitre la sécurité du poste de travail avec les solutions déployées pour assurer la sécurité des données de l'entreprise et de l'utilisateur.

2. De l'analyse de risques aux fonctions de sécurité

Via exemples de traitement des risques

2.1 Filtrage

Afin de réduire les risques liés à la perte, l'intégrité ou la disponibilité des données de production, il est conseillé de cloisonner le système d'information et le réseau et donc de séparer les environnements de production, tests, pré-production et développement.

La notion de cloisonnement est aussi indispensable dans les cas d'hébergement et fourniture de services auprès de plusieurs clients. En effet, il est primordial d'assurer l'étanchéité et la confidentialité des données de chaque client. Le terme utilisé est celui de Multitenant et peut décrire le cas d'une solution ou application proposée et vendue à plusieurs clients ou entités.

Les services, utilisateurs ou zones d'exploitations spécifiques doivent être isolées entre elles. De plus, tout flux entre les différentes zones d'utilisateurs ou services doivent être contrôlés afin d'éviter les compromissions de données de production par celles de tests par exemple.

Nous verrons dans le chapitre 3.3 les solutions techniques pour assurer ce cloisonnement et ce filtrage.

2.2 Accès

gérer les populations, les accès et les droits associés, c'est l'IAM (RBAC, droit d'en connaître)

2.3 Cryptographie

A une époque où chaque jour la presse se fait régulièrement écho de pertes ou de vols de données, où l'on continue à investir dans la protection des données personnelles, certains s'interrogent encore sur les moyens de protéger et de partager de manière sûre son patrimoine informationnel. La cryptographie est une des disciplines de la cryptologie qui s'attache à protéger ces patrimoines en confidentialité, intégrité ou en authenticité. Il me paraissait intéressant de proposer en quelques mots, le vocabulaire et les concepts. Si la cryptographie est un outil pour déployer des mesures de sécurité, c'est aussi un ensemble de techniques utilisées par les attaquants. Au-delà des aspects mathématiques passionnants que nous ne traiterons pas ici, seuls quelques usages et arcanes techniques sont présentés.

2.3.1 Définitions

La cryptologie est par étymologie la science du secret. Elle regroupe la cryptographie, qui porte sur les moyens de coder et décoder les messages, et la cryptanalyse, qui permet de les déchiffrer (de manière non coopérative !). Ces techniques remontent à la nuit des temps. Historiquement militaires et diplomatiques, elles sont devenues civiles avec l'avènement de technologies de l'information, dont la carte à puce [2] et l'Internet.

Elles ont envahi à grande vitesse toutes les technologies numériques. « Signer, protéger, imputer, authentifier... » sont devenus des termes courants de cette vie numérique. On est toutefois surpris de l'usage, quelque fois un peu « dévoyé », de certaines expressions. « Crypter » s'oppose à « décrypter », mais si décrypter, c'est « décoder » sans connaître les secrets, crypter est humoristiquement enterrer mettre en« crypte » ! Si les expressions « coder » et « décoder » sont régulièrement utilisées, celles préconisées sont « chiffrer » et « déchiffrer ». En France, au sein des armées, les acteurs du domaine se nomment d'ailleurs des spécialistes du chiffre [3]. Face à un spécialiste, du mathématicien cryptologue au commercial de services numériques de confiance, de nombreux termes se bousculent dans les discussions : algorithmes robustes de niveau militaire, clefs très longues, protocoles sûrs, certificats de confiance...

2.3.2 Concepts

Derrière ces arguments qui pourraient, au premier abord, paraître convaincants, il convient rapidement d'opposer une petite analyse terminologique et conceptuelle.

Algorithmes Le nombre d'algorithmes mathématiques (fonctions mathématiques) en cryptographie est presque aussi grand que le nombre de mathématiciens qui travaillent dans le domaine. Il faut y ajouter le nombre d'implémentations informatiques de chaque algorithme, sans compter les différents langages utilisés pour la même implémentation. Quelques grandes révolutions ont eu lieu depuis le chiffre de César, mécanisme de chiffrement par décalage « alphabétique » utilisé dans notre enfance, et celui de la machine allemande Enigma de la dernière guerre, avec des mécanismes de substitution dits polyalphabétiques. Ces évolutions et révolutions ont lieu chaque fois que ces fameux cryptanalystes trouvent ou entrevoient une solution pour casser ce chiffre... Une longue tradition dans cette course entre la cuirasse et le canon.

Chiffrement à clefs secrètes Ces premiers algorithmes dits symétriques ou à clefs secrètes ont été et restent centraux, car ils se révèlent très rapides. Le principe est que pour déchiffrer, il faut simplement la clef qui a servi à chiffrer, d'où le terme « symétrique ». Une des grandes difficultés dans ces algorithmes est la combinatoire pour partager le secret. Si partager de manière sûre un secret entre deux ou trois correspondants est maîtrisable, le faire pour mille ne permet plus vraiment de parler d'une clef secrète ! L'histoire des célébrités technologiques retient des algorithmes comme DES, 3DES, IDEA, RC4 et le dernier réputé inviolé et issu d'un appel à projet du NIST [4] et paru dans les années 2000 : AES256.

Cryptographie à clefs publiques Le chiffrement asymétrique résout ce problème de la combinatoire, mais reste bien plus lent. Rendu célèbre par Alice et Bob, deux personnages illustrant les cours de cryptologie asymétrique, ce mécanisme utilise une paire de clés liées dites asymétriques : une clé publique et une clé privée. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète. Pour cette une paire de clés, les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante (donc si vous avez la clef publique de votre correspondant, vous pouvez chiffrer une information pour lui). Inversement, les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'avec la clé publique correspondante. Cette caractéristique est utilisée pour mettre en œuvre la signature numérique.

Figure 1. Exemple d'une encapsulation asymétrique pour un chiffrement de fichier

2. téléphonie mobile (SIM) et carte bancaire.
3. ARCSI : Association des réservistes du chiffre et de la sécurité de l'information - www.arcsi.fr
4. National institute of standards and technology.

Fonction de hachage Les fonctions de hachage cryptographique (de l'anglais « hash ») sont présentes dans tous nos systèmes numériques. Ce sont des fonctions rapides à sens unique qui permettent de transformer tout bloc d'information de taille quelconque et une donnée de taille fixe souvent courte. Ce mécanisme, qui permet de prendre une « empreinte » des données, est à la base des mécanismes de signature, de contrôle d'intégrité et de stockage de mots de passe. Les algorithmes les plus connus sont md5, sha1 et maintenant sha256, sha512 nécessaires par les fragilités découvertes sur les premiers, car ces algorithmes sont aussi sujets aux attaques !

Clefs Au cœur de la cryptographie, les clefs restent l'objet de toutes les attentions. Il est conseillé la lecture des quelques documents de référence de l'Anssi [5] sur les « mécanismes cryptographiques » [6] qui illustrent de manière pragmatique et concrète cette indispensable vigilance.

Taille de clefs Un des débats dans l'usage de la cryptographie concerne la taille optimale des clefs. Ce sujet fait l'objet de nombreuses publications. Pour les algorithmes symétriques, 1 280 bits est la taille de référence (soient 2 puissance 128 possibilités). La notion de taille de clefs pour les algorithmes asymétriques est moins simple. Cela dépend des problèmes mathématiques sous-jacents. Pour le plus célèbre RSA [7] (6), qui aura bientôt 40 ans, les experts considèrent qu'une taille de 2 048 est à l'état de l'art jusqu'en 2030. RSA est utilisé pour les transactions pour la carte bleue, les achats sur internet, les courriels sécurisés. Pour ceux basés sur le logarithme discret, la taille préconisée est de 200 bits, pour les courbes elliptiques de 256 bits. Il est donc important de spécifier les algorithmes pour comparer des tailles de clefs.

Aléas et générateur d'aléas De nos jours, une bonne clef secrète est très rarement issue de notre cerveau (même un bon mot passe mémorisable est totalement perfectible sur le pur plan cryptographique) [8]. Pour générer des clefs d'un bon niveau cryptographique, c'est-à-dire non sujettes à des biais de prédiction possibles, il est nécessaire d'utiliser un générateur de nombres aléatoires (GDA ou RNG : « random number generator ») de qualité cryptographique. Il est fondamentalement complexe de générer de véritables nombres aléatoires. Le processus de génération d'aléas doit comporter des sources fondamentalement aléatoires (bruit électronique, thermique dans des composants) combinées à des sources multiples (hash d'une zone mémoire...), le tout passé à la moulinette d'algorithmes de pseudo-aléas suffisamment imprévisibles. Ce fondamental de la cryptologie est un domaine de recherche à part entière. C'est aussi une activité industrielle autour des HSM (hardware security module) pour la génération rapide, le stockage et la protection des clefs primordiales pour les transactions numériques bancaires en particulier.

Protocoles et formats De bons algorithmes, de bonnes clefs ne suffisent pas. Il est indispensable de s'assurer de l'ensemble des mécanismes qui vont permettre de garantir que « les secrets échangés » restent bien secrets. On parle de protocole d'authentification, de signature, d'échange de clefs (Kerberos, Diffie Elmann, RSA...). C'est souvent au cœur de ces protocoles qui nécessitent une attention particulière en termes de robustesse et de preuve formelle que l'on trouve des vulnérabilités. Le format des données chiffrées (cf Fig. 1) est aussi une source de fragilité (cacher une partie de la clef en piégeant l'ordinateur, exploiter une vulnérabilité logicielle). Les solutions technologiques de chiffrement combinent pour des raisons de performance des mécanismes de chiffrement symétrique et asymétrique.

Certificats Le terme « certificat électronique » est entré dans le langage courant du numérique : « certificat machine, serveur », « certificat utilisateur ». à la base des usages des systèmes à clefs publiques, ce certificat contient la (les) clef(s) publique(s), des informations d'identification, des dates de validité, et un mécanisme de signature garantissant l'origine. Informatiquement ce « paquet » de données nécessite des standards de

5. Anssi : Agence nationale pour la sécurité des système d'information, services du Premier ministre.
6. Annexe B1 et B2 du RGSV2 (Anssi : référentiel général de sécurité) : Mécanismes cryptographiques et gestion des clefs.
7. 1978, apparition de l'algorithme à clef publique de Rivest, Shamir et Adelman (RSA).
8. Un mot de passe de qualité « cryptographique » devrait être d'au moins 20 caractères dans un alphabet de 90 symboles.

formats structurés interopérables comme le codage X.509 ou le stockage PKCS12[9].

Certificats auto-signés ! Une clef publique « valide » dans un système cryptographique de confiance, doit être signée par une autorité de confiance pour être vérifiée par la suite par son « usager ». Disposer d'une PKI (public key infrastructure) ou faire certifier sa chaîne de confiance est complexe et coûteux. Le monde informatique fait donc largement usage de l'auto-signature, c'est-à-dire de la génération des clefs, sans chaîne de confiance partagée. Lorsque les logiciels sont permissifs sur ces usages, l'ensemble du système est fragilisé.

IGC ou PKI Utiliser des mécanismes à clefs publiques nécessite donc l'utilisation d'un ensemble interopérable de confiance (algorithmes, protocoles, formats) permettant de générer les clefs (couple privée/publique), de les attribuer, de les signer (les certifier), de les distribuer, et de les révoquer (les supprimer de l'environnement de confiance). L'ensemble de ces mécanismes s'appelle une IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure). Ces outils logiciels et l'organisation globale sont indispensables à un usage structuré de confiance. Sans cette maîtrise des clefs, un système à clef publique peut s'effondrer. En effet, si des clefs de certification, ou des clefs privées d'utilisateurs sont compromises à la source, la résistance mathématique des algorithmes ou des protocoles ne vous garantira plus grand-chose... C'est dans cet esprit que sont nés les tiers de confiance, qui vous assurent que toutes les précautions sont prises pour protéger cette chaîne.

De la confiance aux usages en entreprise Comme vous l'avez noté, un système cryptographique est un ensemble de briques (fig. 2) qu'il est nécessaire de contrôler pour définir un niveau de confiance de la chaîne. Si disposer d'outils à clefs publiques sans un IGC (PKI) se révèle fragile, disposer d'une IGC sans disposer d'une maîtrise des usages l'est autant... En France, le terme de moyen (9) cryptologique est défini par loi sur la confiance numérique, mais il est à remarquer que, dans l'entreprise, il se conjugue différemment en fonction des interlocuteurs :

- pour les équipes réseaux : la cryptographie est enfouie dans les méandres des protocoles des technologies des canaux sécurisés VPN, IPSEC, VPN, chiffreurs réseaux ;
- pour les équipes des services informatiques : le déploiement, la mise à jour des certificats sur des terminaux et des serveurs concentrent une bonne partie des problèmes opérationnels ;
- pour la bureautique et le poste de travail : les produits et les services pour chiffrer les données et préserver la confidentialité dans les messageries ou sur les supports (smartdevice, disques, USB, serveur de fichiers) sont complexes à choisir pour l'interopérabilité ;
- pour les métiers de l'entreprise comme les achats ou l'archivage probant, les enjeux d'authenticité, d'imputabilité et d'intégrité ainsi que la signature électronique nécessitent des travaux transverses à l'entreprise souvent coûteux.

Figure 2. Les briques à vérifier dans la chaine de confiance

Il est à noter, le point particulier du recouvrement des données chiffrées et du séquestre des clefs. Indispensable pour les malchanceux qui perdent leur clef privée ou par nécessité (départ de l'entreprise, réquisition sur des données...), la confiance dans celui qui possède cette capacité de recouvrement est un enjeu fondamental. Acquérir et déployer un système cryptographique dans l'entreprise doit se baser sur un minimum de confiance dans l'implémentation des briques. Il est important que ces produits aient été analysés, vérifiés par des tiers (entre le constructeur ou éditeur et l'utilisateur ou acheteur). On parle ainsi de certifications de produits au titre de la norme de l'Iso 15408 (critères communs), qualification de produits et de services par l'ANSSI. Perturbant un peu l'écosystème et les frontières de gouvernance des DSI, l'usage des services dans le cloud nécessite de nouvelles technologies de chiffrement pour maintenir la confidentialité totale, mais autoriser tout de même des traitements. Le chiffrement homomorphe permet justement à un système tiers d'opérer des calculs sur des données chiffrées sans les déchiffrer et ainsi récupérer les résultats exploitables. Des solutions matures arrivent sur le marché depuis peu.

9. PKCS : Public-Key Cryptography Standards. (9) Moyen de cryptologie : Tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux)

De l'usure électronique au partage de confiance

Usure ou rupture cryptographique Si le temps n'est pas l'ami de l'archivage, il ne l'est pas non plus du chiffrement. Non par l'usure du support, mais simplement par la complexité d'une longue conservation des clefs, de l'érosion de la résistance des mécanismes. En outre, depuis des années, le terme « quantique » est apparu dans la littérature du domaine. Si la distribution quantique offre une transmission sûre de clef, l'ordinateur quantique pourrait apporter cette rupture que redoute l'industrie numérique, car capable de rompre la solidité des problèmes mathématiques sur lesquels repose une grande partie des mécanismes cryptographiques actuels.

La cryptographie quantique est un espace de recherche de cryptographie qui utilise les propriétés quantiques de la matière pour sécuriser les communications et protéger les données. Elle repose sur des phénomènes quantiques tels que l'intrication et la superposition, qui permettent de réaliser des calculs et des opérations de manière beaucoup plus rapide et plus efficace que les algorithmes classiques utilisés dans la cryptographie traditionnelle.

La cryptographie quantique est encore en développement et n'est pas encore largement utilisée dans les applications pratiques. Cependant, elle offre des avantages potentiels considérables en termes de sécurité et de vitesse de calcul. Par exemple, les algorithmes de cryptographie quantique pourraient être utilisés pour créer des clés de chiffrement plus sécurisées et pour effectuer des calculs complexes de manière beaucoup plus rapide que les algorithmes classiques.

Il est important de noter que la cryptographie quantique est également confrontée à des défis importants, notamment en ce qui concerne la stabilité des données quantiques et la difficulté à mettre en œuvre ces algorithmes de manière pratique. En outre, il existe des inquiétudes quant à la sécurité à long terme de la cryptographie quantique, car il est possible que de futurs progrès technologiques permettent de casser la confiance dans les chaînes de confiance basée sur les algorithmes actuels de manière plus efficace.

En effet, si ces technologies sont pleinement mises en œuvre et deviennent largement utilisées, cela pourrait remettre en question la sécurité de nombreux systèmes de sécurité actuellement en place qui reposent sur des algorithmes de cryptographie classiques.

On peut citer les risques suivants :

- rupture de la sécurité de la cryptographie classique : si les algorithmes de cryptographie quantique sont mis au point et deviennent largement utilisés, ils pourraient être utilisés pour cracker les codes de cryptographie classique, mettant ainsi en danger la sécurité de nombreux systèmes de sécurité actuels ;
- compromission de la confidentialité des communications : si les algorithmes de cryptographie quantique sont utilisés pour chiffrer les communications, ils pourraient être « crackés » par des parties malveillantes, compromettant ainsi la confidentialité de ces communications.

blockchain, Crypto-monnaies, NFT... Nous avons rapidement parcouru l'usage courant de la cryptographie en entreprise, mais de nouvelles révolutions des usages de la cryptographie sont déjà à nos portes. Après quelques années d'hésitation, la montée des « crypto-monnaie » comme Bitcoin donne une large expression aux mécanismes de signature pour assurer intégrité, traçabilité, imputabilité et modifie le rapport à la confiance « centralisée ». Dans l'émergence rapide de cette « décentralisation de la confiance », quelques positions établies sont remises en cause. On notera en particulier une forme naissante « d'ubérisation » des chaînes de confiance, qui bouscule déjà le marché effervescent de la cybersécurité. Les chaines de confiance sont de plus en plus utilisées dans les cryto-monaies et NFT.

La cryptographie joue un rôle clé dans la sécurité et l'intégrité des Blockchains en permettant de protéger les données et les transactions contre la modification ou la falsification. Ces actifs numériques à caractère authentique sont basés sur ces Blockchains. Une blockchain est un registre, une base de données distribuée qui permet de stocker de manière sécurisée et transparente ces enregistrements de données. Elle est composée de blocs de données qui sont liés les uns aux autres de manière sécurisée grâce à l'utilisation de cryptographie.

Chaque bloc de la chaîne contient des informations sur les transactions qui ont été effectuées, ainsi que des données sur les blocs précédents. Lorsqu'un nouveau bloc est ajouté à la chaîne, il est vérifié et validé par plusieurs ordinateurs dans le réseau, ce qui rend la Blockchain très difficile à altérer ou à falsifier.

Les Blockchains sont principalement utilisées pour stocker et transférer des cryptomonnaies, mais elles peuvent également être utilisées pour d'autres applications, telles que la gestion de la chaîne d'approvisionnement, la gestion des actifs, la gestion de la santé, etc. Elles offrent un niveau élevé de transparence et de sécurité, ce qui les rend particulièrement utiles dans les situations où la confiance et l'intégrité des données sont importantes.

Les cryptomonnaies sont des formes de monnaies numériques qui utilisent la technologie de la Blockchain pour sécuriser les transactions et contrôler la création de nouvelles unités de monnaie. Elles sont décentralisées, ce qui signifie qu'elles ne sont pas émises ni gérées par une banque centrale ou tout autre organisme gouvernemental.

La cryptomonnaie la plus connue est probablement le Bitcoin, qui a été créée en 2009. Depuis, de nombreuses autres cryptomonnaies ont vu le jour, chacune avec ses propres caractéristiques et utilisations. Certaines sont conçues pour être utilisées comme moyen de paiement, tandis que d'autres sont plus axées sur l'investissement.

Les cryptomonnaies sont souvent utilisées comme moyen de paiement en ligne et sont acceptées par certaines entreprises et commerçants en tant que moyen de paiement. Cependant, elles restent controversées en raison de leur manque de réglementation et de leur volatilité, avec des fluctuations de prix importantes pouvant survenir en très peu de temps. En outre, leur utilisation a été associée à des activités illégales en raison de la confidentialité qu'elles offrent aux utilisateurs.

Les NFT (Non-Fungible Tokens) sont des tokens numériques qui représentent de manière unique des actifs numériques ou physiques. Ils sont stockés sur une chaîne de confiance basées sur des blockchains, comme la blockchain Ethereum, ce qui leur confère une certaine forme de rareté et de valeur.

Les NFT sont utilisés pour représenter des objets virtuels tels que des œuvres d'art numériques, des enregistrements de musique, des GIFs animés, des émoticônes, des personnages de jeux vidéo, etc. Ils permettent aux créateurs de ces actifs de monétiser leur travail de manière transparente et sécurisée, tout en offrant aux acheteurs la possibilité de devenir les propriétaires uniques de ces actifs.

Si les NFT sont de plus en plus populaires et suscitent beaucoup d'intérêt en raison de leur capacité à représenter de manière unique des actifs numériques, il est important de noter qu'il existe également des risques liés à l'achat et à la possession de ceux-ci. On note en particulier la confiance dans la sécurité globale dans ces blockchains ainsi que la stabilité et la liquidité du marché des NFT.

3. Architecture et composants de système d'information

Nous allons dans ce chapitre présenter les composants des architectures logicielles, postes de travail et réseaux.

3.1 Architecture logicielles

Les architectures logicielles ont fortement évolué ces dernières années et le classique architecture "trois tiers" se décompose de plusieurs types de solutions basées sur les dernières technologies d'intégration et de déploiement.

Les modèles dits « monolithes » (tous les composants partagent les mêmes ressources et le même espace mémoire) existent toujours et restent utilisés dans beaucoup de cas d'applicatifs qui ont des besoins élevés en capacité de traitement ou de bande passante.

L'apparition et l'utilisation des micro-services a apporté des solutions en scalabilité et résilience. Cependant, ce type d'architecture apporte aussi son lot de complexité dans le cadre de montée en version versus la solution monolithe où une seule mise à jour serait nécessaire. L'exemple de vulnérabilités impactant un fort ensemble de composants comme log4shell [10] est illustratif des difficultés à corriger (patcher) les applications vulnérables (plusieurs applications possibles, avec correctif/patch ou non disponible qui impose une montée en version

10. https://www.ssi.gouv.fr/publication/lanssi-alerte-sur-la-faille-de-securite-log4shell/

préalable et donc ajoute des difficultés à la remédiation).

Les architectures logicielles sont généralement composées des composants suivants :

- Front ou FrontEnd qui sont les composants directement consultés par le client de l'applicatif. Ils peuvent être de type applications mobiles, pages web par exemple ;
- Backend ou moteur/serveur applicatif qui vont assurer la partie métier ;
- Bases de données qui assurent le rôle de stockage des données applicatives.

3.2 Middleware

Les composants dits middleware sont de type :

- Bases de données ;
- ERP ;
- Annuaires

3.3 Endpoints

(PC, mobile, IoT)

3.4 Réseau

accès et traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

4. Introduction

Les architectures et composants de sécurité périmétrique ont beaucoup évolué depuis le modèle du château-fort à la fin du 20ème siècle jusqu'à de nos jours les architectures Cloud & Multi-Cloud sécurisées.

Ce chapitre présente cette évolution et les différents composants centraux et clés de ces architectures comme les pare-feux, les Proxy, les sondes de détection ainsi que les nouveaux modèles dits de Zerotrust ou basés sur des bastions de sécurité.

Nous aborderons dans la dernière partie de ce chapitre les solutions de type VPN et les solutions de sécurisation des architectures et solutions de type Cloud.

5. Château fort

Figure 3. Château fort

Le modèle du château-fort est un modèle de sécurité périmétrique qui existe depuis plusieurs années et demeure incontournable au niveau de la conception des architectures sécurisées.

Il propose une méthode de protection des réseaux et des accès aux différents réseaux de l'entreprise à l'aide d'un composant central : le pare-feu. Celui-ci va assurer les principales fonctions de sécurité et donc protéger **la seule entrée** possible telle que la mission historique du château fort au moyen-âge qui protégeait l'ensemble des populations et ressources au sein de sa structure. En effet, la sécurité était assurée en contrôlant scrupuleusement les entrées et sorties via la porte principale et en empêchant toute intrusion à l'aide de ses différentes défenses (fortifications, douves, mâchicoulis, etc.).

Voir ci-dessous un schéma (3) représentant une architecture de type château fort.

Ce modèle de conception d'architecture va permettre de contrôler les accès aux réseaux de l'entreprise et de cloisonner entre différentes zones, ou DMZ [11] qui auront des fonctions de sécurité distinctes :

- DMZ Publique ou Externe ;

11. définition et précisions de l'ANSSI : https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle$_{i}nternet_{s}ecurisee - v2.pdf$

- Zone serveurs Intranet ;
- LAN bureautiques ;
- Autres : zone d'échanges, DMZ métiers spécifiques, etc.

La **DMZ publique** pourra héberger des serveurs et des services à vocation d'être accessible depuis Internet. Par exemple, le site publique de l'entreprise ou tout service dit publié sur Internet. Seuls certains protocoles, voire utilisateurs seront autorisés à y accéder. Nous y reviendrons dans le prochain chapitre sur le pare feu.

Les différentes **zones ou DMZ Intranet** sont utilisées pour regrouper les serveurs dont les services ne sont et ne doivent être accessibles qu'en interne. Par exemple, les services de messagerie ou les bases de données. Il est indispensable de protéger l'accès à ces zones qui peuvent stocker des données confidentielles. Le pare feu se chargera d'interdire l'accès depuis Internet à ces zones et seuls certains flux, depuis les LANs internes par exemple, devront être autorisés afin de garantir le niveau de sécurité nécessaire.

Le modèle de château fort a dû être revu car il considérait, par définition, que l'interne est de confiance. Or de nos jours, il est inconcevable de ne pas prendre en compte les possibilités de compromissions et attaques provenant de menaces internes telles qu'un acteur malveillant ayant réussi à s'introduire dans le SI par exemple.

De plus, la multitude d'interconnexion avec le SI augmente la surface d'attaque et met à mal le modèle de contrôle en un seul point car les accès aux SI s'effectuent via plusieurs points d'entrée.

C'est pourquoi celui de **l'aéroport** est apparu avec des contrôles plus simples sur les zones d'échanges et fortement précis et minutieux pour l'accès aux zones sensibles et confidentielles (analogie avec le tarmac, tours de contrôles).

Nous verrons dans la suite de ce chapitre un peu plus en détail l'évolution des architectures et les composants de ces nouveaux modèles.

6. pare-feu

Définition (source ANSSI) : Un pare-feu (firewall), est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Le pare-feu apporte la notion de filtrage dans la sécurité des réseaux et est une pierre angulaire de l'architecture de la sécurité de l'entreprise.

Son rôle est d'inspecter les flux réseaux entrants et sortants.

Il assure le cloisonnement et la segmentation entre les sous-réseaux (Local Area Network ou LAN). L'ensemble des flux, autorisés ou non, entre ces sous-réseaux et autres réseaux externes (INTERNET, VPN partenaires, etc.) sont inscrits dans la politique de sécurité du pare-feu. Celle-ci se représente par une matrice des flux contenant l'ensemble des informations telles que :

- le nom de la règle ;
- le ou les IP source(s) ;
- le ou les IP destination(s) ;
- le protocole concerné (HTTP, FTP, SMTP, etc.) ;
- l'option éventuelle (Network Adress Translation ou NAT, authentification, application d'une politique de sécurité supplémentaire, etc. ; cela dépend de la version du pare-feu utilisé) ;
- l'action : accept, drop, reject, etc.
- l'option de journalisation sélectionnée.
- etc.

Le pare feu consulte sa politique de sécurité, i.e. ses règles de filtrage afin de déterminer s'il doit bloquer, ou non, chaque flux qui entre ou qui sort.

Voir ci-dessous un exemple de matrice de flux :

1. autorisant les postes internes à consulter le site Wiki ;
2. autorisant les flux depuis Internet vers le serveur SMTP (transfert de mails) de l'entreprise avec une translation d'adresse sélectionnée ;
3. bloquant tout autre type de flux.

ID	Source	Destination	Protocoles	Option	Décision	Log
1	LAN bureautique	@IP$_{Wiki_{Interne}}$	HTTPs	No$_{NAT}$	ACCEPT	Yes
2	ANY	@IP$_{Publique_{SMTP}}$	SMTP	NAT	ACCEPT	Yes
3	ANY	ANY	ANY	No$_{NAT}$	DENY	No

Table 1. Exemple de Matrice de flux

7. Proxy

Figure 4. Proxy

Les équipements de type Proxy permettent de sécuriser l'accès aux applicatifs et sont utilisés pour assurer un filtrage des accès Internet depuis le réseau de l'entreprise.

C'est une des fonctions primordiales de la sécurité du système d'information. En effet, il est indispensable de maîtriser les flux de sortie et d'assurer la sécurité des utilisateurs sur Internet en imposant un filtrage via des équipements réseaux de type Proxy.

Ainsi, toute requête d'accès à un site Web sera analysée par le proxy et des contrôles de types anti-virus, malware pourront être appliqués et protéger les utilisateurs et le SI en conséquence.

Plusieurs autres briques de sécurité peuvent être ajoutées sur le proxy, comme :

- l'authentification des utilisateurs (jusqu'à la gestion via un annuaire) permettant d'associer des politiques de sécurité en fonction des utilisateurs ;
- le filtrage des URL demandées en interdisant certaines catégories de sites web jugés dangereux et incompatibles avec la politique d'utilisation de l'Internet par l'entreprise ;
- des mécanismes de détection de fuites de données (Data Leak Protection : DLP) afin de détecter d'éventuels vols de données personnelles (Numéro de sécurité sociale, numéros de carte bancaires, etc.).

L'autorisation des flux vers et depuis le Proxy devra être aussi implémentée sur le pare-feu.

Voir ci-dessous en exemple un extrait simplifiée d'une matrice de flux, contenant les règles concernants le Proxy, implémentée sur un pare feu :

Source	Destination	Protocoles	Décision
LAN bureautique	Adresse IP du proxy sur le réseau local	HTTP, HTTPs	ACCEPT
Proxy	ANY	HTTP, HTTPs	ACCEPT
ANY	ANY	ANY	DENY

Table 2. Matrice de flux : règles Proxy

Seul le proxy sera donc autorisé à se connecter aux serveurs distants et effectuer son rôle de mandataire.

8. Reverse Proxy

Figure 5. ReverseProxy

Le Reverse Proxy a le rôle de protéger les serveurs des accès utilisateurs, externes ou internes. Il peut assurer une **rupture protocolaire** et donc agir en tant que mandataire auprès du serveur. Plus précisément, la connexion

TCP/HTTP par exemple entre le client A et le serveur Web **www.monexemple.com** peut s'effectuer de la manière suivante :

- le client effectue une requête DNS sur www.entreprise.com et le serveur DNS lui indique l'IP associée, cette IP est portée par le Reverse Proxy ;
- le client initie une connexion TCP/HTTP vers le Reverse Proxy : @IPClient –> @IPwww.entreprise.com ;
- le Reverse Proxy effectue éventuellement les contrôles configurés et ensuite initie à son tour une connexion TCP/HTTP vers le serveur : @IPReverseProxy –> 192.168.1.27 (adresse IP réelle du serveur en DMZ publique).

Le Reverse Proxy est un équipement ou bien une fonction portée par un service qui permet donc d'interagir avec la connexion et assurer par exemple :

- de la répartition de charges (load balancing) en utilisant des algorithmes adaptés :
  - **Round Robin** : répartition équivalente, utilisé lorsque les serveurs ont les mêmes caractéristiques
  - **Least Connection** : le serveur qui a le moins de connexions actives avec le reverse proxy sera privilégié pour prendre en charge la prochaine requête
  - Avec des poids, utilisé en général lorsque les serveurs n'ont pas les mêmes puissances de calculs (CPU, RAM, GPU, etc.)
  - Il en existe plein d'autres, en fonction des débits, de la charge, etc.
- de la réécriture d'URL [12] (Uniform Resource Locators) communément appelées **adresses web** et ajouter des fonctions :
  - d'amélioration du SEO (Search Engine Optimisation) : Des URL propres et descriptives sont mieux indexées par les moteurs de recherche, ce qui peut améliorer le classement d'un site ;
  - de facilité d'utilisation : des URL lisibles et mémorisables sont plus faciles à partager et à comprendre pour les utilisateurs ;
  - de gestion de la structure du site : la réécriture permet de modifier la structure des URL sans changer la structure réelle des fichiers sur le serveur ;
  - de sécurité : masquer les paramètres de l'URL peut aider à protéger contre certaines vulnérabilités et attaques en dissimulant la structure et la technologie sous-jacente du site ;
  - de contrôle et flexibilité : permet de rediriger les utilisateurs de manière transparente, par exemple lors de la refonte d'un site, une mise à jour ou de la modification de l'architecture des pages ; Par exemple, la réécriture de l'URL webmail.monentreprise.com vers www.entreprise.com/owa facilitera la compréhension des utilisateurs et n'indiquera pas explicitement quel webmail est utilisé.
- des fonctions de sécurité et donc assurer un rôle de pare feu applicatif/Web (Web Application Firewall : WAF) et protéger les serveurs contre les menaces listées dans le Top 10 de l'OWASP [13], comme par exemple les injections SQL.

9. Sondes de détection (IDS/IDP)

Les sondes de détection d'intrusion sont utilisées pour surveiller et analyser le trafic réseau afin de détecter des actes malveillants tels que des tentatives d'exploitation de vulnérabilités qui peuvent entraîner l'ex-filtration de données confidentielles par exemple.

Plusieurs types de sondes peuvent être utilisées :

- Réseaux :
  - NIDS Network Intrusion Detection System (NIDS)
  - Network Intrusion Prevention System (NIPS)

12. rfc1738 : https://datatracker.ietf.org/doc/html/rfc1738
13. top10 OWASP : https://owasp.org/www-project-top-ten/

- Sur les équipements :
  - Host Intrusion Detection System (HIDS)
  - Host Intrusion Prevention System (HIPS)

Voir ci-dessous un exemple de schéma d'infrastructure (6) avec positionnement des sondes. Une sonde IDS peut être positionnée en coupure des flux mais aussi en position **d'écoute**. L'IPS doit être elle en position de coupure afin de bloquer le trafic en cas de détection d'intrusion.

Figure 6. IDS/IDP

Il existe plusieurs méthodes de détection telles que :

- celle basée sur les signatures qui compare avec sa base de signatures les événements observés pour identifier des incidents potentiels ;
- celle basée sur les anomalies qui compare les définitions d'une activité considérée comme normale avec les événements observés afin d'identifier les écarts significatifs ;
- l'analyse dynamique qui compare les profils prédéterminés des protocoles, avec les événements observés, afin d'identifier les écarts. L'ensemble des résultats des sondes est consigné dans des journaux et peuvent utilisés dans les détections d'incidents de sécurité.

10. Network Access Control : NAC

Les solutions de contrôle d'accès au réseau (NAC) permettent d'empêcher les appareils et les utilisateurs non autorisés ou non conformes d'accéder au réseau de l'entreprise. Cela assure que l'ensemble des appareils connectés au réseau de l'entreprise sont conformes aux politiques de sécurité de l'entreprise. Les contrôles peuvent être au niveau des adresses physiques des interfaces réseaux ou si le poste de travail est bien configuré au niveau des paramètres de sécurité.

Le NAC est composé de deux éléments s'appuie sur le protocole 802.1X (Remote Authentication Dial In User Service : RADIUS) [14], norme IEEE relative au contrôle d'accès réseau qui définit précisément les contrôles d'authentication pour chaque utilisateur ou équipement ;

Le NAC a plusieurs fonctionnalités telles que :

- le contrôle de l'accès au réseau des appareils personnels ou **Bring Your Own Device (BYOD)** afin de s'assurer que ces équipements sont conformes aux politiques de sécurité de l'entreprise avant de les autoriser ;
- la limitation des accès des **IOT** aux seuls connus et validés car ils sont souvent la cible des acteurs malveillants et leur compromission est fréquente ;
- la limitation des accès aux invités et sous-traitants aux seuls périmètres et systèmes nécessaires ;
- la mise en quarantaine des appareils infectés et donc limiter les risques de propagation au sein du réseau de l'entreprise.

La figure (7) ci-dessous représente un exemple simple d'utilisation d'un NAC au sein d'un réseau sans fil d'une entreprise afin de contrôler les accès des équipements mobiles. Les composants clés sont :

- **contrôleur NAC** : équipement en charge de l'application des politiques de sécurité d'accès au réseau ;
- **base de données d'authentification** : contient les informations d'identification des utilisateurs et des appareils ;
- **point d'accès sans fil** : permet la connexion des appareils BYOD au réseau WiFi par exemple ;
- **serveur de gestion des politiques** : définit et gère les politiques d'accès pour différents types d'utilisateurs et d'appareils ;

14. rfc3580 RADIUS : https://datatracker.ietf.org/doc/rfc3580/

- **employé BYOD** : appareil personnel d'un employé qui doit être authentifié pour accéder au réseau ;
- **visiteur BYOD** : appareil personnel d'un visiteur qui peut se voir accorder un accès limité (par exemple, uniquement à Internet) ;
- **équipement BYOD non conforme** : appareil qui n'est pas conforme aux politiques de sécurité et se voit donc refuser l'accès au réseau.

Figure 7. NAC : exemple utilisation contrôle BYOD

Les opérations effectuées par le contrôle d'accès réseau 802.1X sont les suivantes :

1. **lancement** : l'authentificateur (par exemple un commutateur réseau) ou le demandeur (l'équipement client) envoie une requête de lancement de session. Un demandeur envoie un message de réponse EAP [15] à l'authentificateur, qui encapsule le message et le transmet au serveur d'authentification. A noter qu'il existe plusieurs méthodes EAP en fonction des besoins :
   - avec des certificats ou tunnels TLS : EAP-TLS, EAP-TTLS (Tunneled Transport Layer Security), PEAP (Protected EAP),
   - orientés réseaux mobiles : EAP-SIM (Subscriber Identity Module), EAP-AKA (Authentication and Key Agreement),
   - propriétaires ou moins utilisés car considérés comme peu sécurisés : EAP-MD5, EAP-FAST (Flexible Authentication via Secure Tunneling, CISCO), EAP (Lightweight EAP, CISCO),
   - utilisant des tokens : EAP-GTC (Generic Token Card) ;
2. **authentification** : les messages transitent entre le serveur d'authentification et le demandeur via l'authentificateur pour valider plusieurs informations ;
3. **autorisation** : si les données d'identification sont valides, le serveur d'authentification informe l'authentificateur d'accorder l'accès au port au demandeur ;
4. **comptabilité** : le processus de comptabilité RADIUS enregistre les informations de session, notamment l'utilisateur, l'équipement, le type de session et le service ;
5. **clôture** : les sessions sont clôturées en déconnectant le point de terminaison ou en utilisant un logiciel de gestion.

11. Zero Trust

Les modèles actuels de sécurité périmétrique atteignent leurs limites face à l'augmentation du télétravail, de l'utilisation des infrastructures Cloud et l'utilisation de terminaux mobiles pour se connecter au SI d'entreprise.

Le principe du ZeroTrust est de ne plus faire uniquement confiance aux contrôles et filtrage des équipements classiques tels que les parefeux et proxies et d'ajouter un système de contrôle d'accès supplémentaire et dynamique aux ressources.

Tout accès à un service ou à une application sera contrôlé plus précisément en fonction de l'utilisateur, de son IP et de ses droits d'accès.

L'équipe du National Institute for Standards and Technology (NIST) décrit les principes de la confiance zéro et définit une architecture abstraite à confiance zéro (ZTA) dans son document NIST SP 800-207 [16]. Voir ci-dessous un extrait de ce document présentant un schéma des différents composants d'un exemple d'architecture ZTA "idéale" :

Figure 8. ZTA NIST SP800-207

Les composants impliqués sont :

15. rfc3748 EAP : https://datatracker.ietf.org/doc/html/rfc3748
16. https://csrc.nist.gov/pubs/sp/800/207/final

- Policy engine (PE) : This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policyadministrator executes the decision.
- Policy administrator (PA) : This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service ; here, it is divided into its two logical components. The PA communicates with the PEP when creating the communication path. This communication is done via the control plane.
- Policy enforcement point (PEP) : This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components : the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone (see Section2) hosting the enterprise resource.

Comme l'indique l'ANSSI [17], attention cependant à la mise en oeuvre de ce modèle afin de ne pas ajouter plus de vulnérabilités.

12. Bastion

L'administration des différents équipements de sécurité ou serveurs de l'entreprise est une activité essentielle et risquée. En effet, les droits administrateurs permettent d'effectuer des actions de création, modification et suppression qui doivent être contrôlées et tracées.

Un bastion peut être utilisé pour concentrer et contrôler les accès d'administration d'une entreprise. L'accès à ce type d'équipement doit être via un réseau sécurisé et un SI de confiance car il héberge des secrets (comptes, clés) critiques qui doivent donc être protégés. Il est souvent associé à des notions de coffre-fort numérique dans lequel ces informations sont stockées afin d'assurer leur confidentialité et intégrité.

La figure (9) ci-dessous représente un bastion et décrit le chemin qu'un administrateur utilise pour se connecter à l'équipement final. Tout d'abord il doit se connecter sur une interface WEB ou directement avec un protocole RDP ou SSH sur le bastion et ensuite en fonction de ses droits d'atteindre l'équipement qu'il doit configurer via un protocole classique.

Figure 9. Bastion

13. VPN

L'utilisation d'un Virtual Private Network (VPN) répond aux besoins :

- de connecter des utilisateurs nomades au système d'information de l'entreprise avec une technologie fiable et sécurisée ;
- d'inter-connecter des partenaires au SI de l'entreprise en maîtrisant les flux autorisés ;

17. https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/

- de sécuriser les données en transit au travers d'un réseau en les chiffrant afin de se protéger des attaques de type 'Man in the middle' [18]

Il existe différents types de tunnels VPN. Nous allons étudier deux des plus utilisés, les tunnels L2TP/IPSec et TLS/SSL.

L'utilisation de tunnels L2TP/IPSec (Layer Two Tunneling Protocol [19]/Internet Protocol Security [20]) permet de raccorder des équipements réseaux (routeurs ou firewalls) point à point, et ainsi étendre les systèmes d'information à d'autres sites géographiques internes, externes ou partenaires.

La technologie TLS/SSL (Transport Layer Security/Secure Socket Layer) est utilisée généralement avec un navigateur WEB et le protocole HTTPS. Elle ne nécessite donc pas de client dédié mais il en existe pour faciliter l'accès à certaines applications par exemple.

Voir ci-dessous un schéma (10) représentant les deux technologies. Dans le cas du tunnel L2TP/IPSec, le point de terminaison peut être un pare feu sur lequel sera implémenté les règles permettant (ou non) l'accès depuis le poste externe aux différents réseaux privés de l'entreprise. La négociation des protocoles utilisés pour l'authentification et le chiffrement s'effectue entre les deux points de terminaison.

Figure 10. VPN IPSec vs VPN SSL

Le deuxième cas représente l'utilisation d'un tunnel TLS/SSL entre un client avec un navigateur Internet et une passerelle VPN SSL dédiée.

La passerelle est positionnée en DMZ et ainsi protégée par un parefeu.

Les règles, routage et paramétrage des autorisations s'effectuent sur la passerelle qui peut supporter par exemple de l'authentification (LDAP, Radius, SAML ou autres).

14. Cloud

Un des enjeux majeur pour les entreprises est la résilience de leurs services. Un grand distributeur et marchand en ligne ne peut pas se permettre d'être à l'arrêt complet lors de périodes fastes comme les fêtes de fin d'année. Il est arrivé que certains soient bloqués car ils avaient migré l'entièreté de leurs applications dans un Cloud publique qui malheureusement fut inaccessible pendant plusieurs heures. Le résultat commercial fut catastrophique pour le marchand (et leur fournisseur Cloud aussi). La disponibilité est aussi de la sécurité et doit être assurée en évitant de mettre « tous ses oeufs dans le même panier ».

MultiCloud En ce qui concerne l'hébergement dans le CLOUD, les entreprises prennent donc le choix du Multi-Cloud, i.e. de dupliquer leurs architectures sur des clouds providers (CSP) différents. Ce choix peut apporter son lot de complexité et des coûts associés non négligeables car il sera nécessaire d'adapter les déploiements/configurations par rapport aux spécifications du CSP utilisé.

Cloud Hybride Le MultiCloud ayant ses avantages mais aussi ses inconvénients, beaucoup d'entreprises décident de déployer leurs infrastructures dans un Cloud Publique et dans un cloud privé. En effet, ils configurent le déploiement sur le cloud publique comme le « maitre ou master » et puis la partie sur l'infrastructure privée, dit « on premise » comme l' « esclave ou slave ».

15. Cloud Access Security Broker - CASB

Le Cloud computing a apporté un lot d'évolution technologique qui nous force à repenser les stratégies de sécurité nécessaires pour protéger et surveiller les applications et les données hébergées dans le Cloud. Les solutions de Cloud Access Security Broker (CASB) agissent comme un pont entre les services et infrastructures

18. définition ANSSI de l'homme-au-milieu : https://www.ssi.gouv.fr/entreprise/glossaire/h/
19. rfc2661 : https://datatracker.ietf.org/doc/html/rfc2661
20. rfc6071 : https://datatracker.ietf.org/doc/html/rfc6071

« on premises » et les différents services Cloud utilisés par l'entreprise. Les CASB peuvent proposer les fonctionnalités suivantes :

- authentication,
- single sign-on,
- authorization,
- credential mapping,
- device profiling,
- encryption,
- tokenization,
- logging,
- alerting,
- malware detection/prevention.

Les CASB peuvent être intégrés comme composants au sein d'architectures de type Secure access service edge (SASE).

16. Secure access service edge (SASE)

Les évolutions des méthodes de travail avec l'explosion de l'utilisation du télétravail, des accès professionnels via les terminaux mobiles et l'utilisation de plus en plus fréquente du edge computing [21] nécessitent une évolution des architectures de sécurité afin de faire face à de nouvelles menaces liées à ces changements.

Les architectures de type Secure access service edge (SASE) assurent des fonctionnalités réseau et sécurité, dans un environnement « Cloud Natif » incluant les technologies/services, dits « Cloud Based » suivants :

- SD-WAN (Software Defined WAN)
- SWG (Proxy sortant sécurisé)
- CASB (Cloud Access Security Broker)
- NGFW (firewalls de nouvelle génération)
- zero trust network access (ZTNA)

- Le modèle du château fort demeure mais évolue
- les technologies de protection et de filtrage évoluent et restent indispensables à la SSI

  –> #FirewallNextGeneration #ProxydansleCloud
- les contrôles d'accès administrateurs et utilisateurs sont de plus en plus fins et imposent une rigueur d'implémentation et de gestion dans le temps

  –> #Bastion #ZeroTrust
- La sécurité périmétrique s'étend jusqu'au Cloud

  –> #CASB #SASE

17. Sécurité Endpoints

La sécurité des endpoints est l'ensemble des solutions et techniques qui visent à protéger les équipements de type ordinateurs de bureau, ordinateurs portables, terminaux mobiles, etc. contre les cyberattaques.

Selon Gartner [22], une plateforme de protection des endpoints (EPP) "permet de déployer des agents ou des capteurs pour sécuriser les Endpoints gérés, notamment les ordinateurs de bureau, les ordinateurs portables,

21. Edge computing : https://www.redhat.com/fr/topics/edge-computing/what-is-edge-computing
22. https://www.gartner.com/reviews/market/endpoint-protection-platforms

les serveurs et les appareils mobiles. Les EPP sont conçus pour empêcher une série d'attaques malveillantes connues et inconnues. De plus, ils offrent la possibilité d'enquêter et de remédier à tout incident qui échappe aux contrôles de protection."

Les solutions de protection analysent les fichiers, les processus et l'activité système pour y débusquer des indicateurs d'actes suspects ou malveillants. Elles intègrent les fonctionnalités comme l'antivirus classique ou de nouvelle génération qui se charge de la partie détection.

La détection qui utilise des bases de données de signatures identifie le logiciel malveillant en comparant le code d'un programme au code de types de virus connus qui ont déjà été rencontrés, analysés et enregistrés dans une base de données. Voir ci-dessous le schéma du fonctionnement classique d'un antivirus :

Quid des zero days ? Comment les identifier lorsque ces bases de données de signatures ne sont pas à jour ? Pour répondre à ces enjeux, les antivirus ont évolué et la nouvelle génération (NGAV) s'appuie sur l'intelligence artificielle et le machine learning pour gagner en efficacité. En plus de comparer les signatures, d'autres éléments sont collectés comme les hash des fichiers, des URLs ou IP contactées.

De plus, les solutions historiques basées sur la signature sont de moins en moins efficaces contre les menaces appelées « fileless ». Les attaques fileless malware opérent directement dans la mémoire vive du système visé, sans laisser de traces de création de fichier sur le disque dur. Il est alors difficile de les détecter par les analyses heuristiques et comportementales basées sur l'analyse de fichiers.

Comment alors procéder ? OrangeCyberDéfense [23] indique dans son article dédié à ce sujet que, je cite, pour détecter un fileless malware, les entreprises peuvent s'appuyer sur la recherche d'indicateurs d'attaque « IoA : Indicators of Attack ». En effet, si le fileless malware ne laisse pas de trace sur les disques, les indicateurs d'attaques peuvent donner des signes qu'une cyberattaque est en cours : exécution d'une commande par un utilisateur non habilité, connexion d'un utilitaire système à un serveur ayant une IP malveillante, etc. En analysant et en corrélant ces différents événements (à l'aide d'un SIEM par exemple), les indicateurs d'attaque peuvent aider à bloquer des activités malveillantes, même si celles-ci sont réalisées à partir d'éléments légitimes.

En complément, les solutions de type Endpoint Detection and Response (EDR), d'après Gartner [24], "enregistrent et stockent les comportements au niveau du système des points finaux, utilisent diverses techniques d'analyse de données pour détecter les comportements suspects du système, fournissent des informations contextuelles, bloquent les activités malveillantes et fournissent des suggestions de mesures correctives pour restaurer les systèmes concernés. Les solutions EDR doivent fournir les quatre fonctionnalités principales suivantes :

- Détecter les incidents de sécurité
- Contenir l'incident au point final
- Enquêter sur les incidents de sécurité
- Fournir des conseils de remédiation"

- Les solutions de protection évoluent pour faire face aux nouvelles menaces sur les endpoints –> #Antivirus #NGAV #filelessMalware #IoA
- Associées aux systèmes de protection, les solution de détection permettent d'agir en cas d'attaque –> #EDR #XDR

23. https://www.orangecyberdefense.com/fr/insights/blog/quest-ce-quun-fileless-malware
24. https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions