BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

U6 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2022

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 18 pages, numérotées de 1/18 à 18/18
(sans compter la page de garde).

Cas CALEDOBANK

Ce sujet comporte 18 pages dont un dossier documentaire de 13 pages.
La candidate ou le candidat doit vérifier qu'il est en possession d'un sujet complet.

Barème :

DOSSIER A	Centralisation et exploitation des informations de supervision	28 points
DOSSIER B	Intégration de l'application de gestion des crédits à la consommation	52 points
	TOTAL	80 points

Sommaire

Présentation du contexte

Implantée en Nouvelle-Calédonie[1], la banque CalédoBank est une société anonyme dont le principal actionnaire est une banque généraliste métropolitaine. Son siège social se situe à Nouméa, chef-lieu de cette collectivité d'outre-mer. La principale activité de cette banque généraliste est l'activité de crédit. Pour gérer ses 70 000 comptes clients (particuliers et professionnels), elle dispose de 24 agences réparties sur le territoire et compte près de 40 distributeurs automatiques de billets (DAB).

Dans le système bancaire, les systèmes d'information (SI) recouvrent une grande variété d'applicatifs. Ils sont constitués d'outils permettant au conseiller bancaire de consulter les caractéristiques et les états des comptes clients dont il a la charge. Ils offrent aussi un lien au réseau de l'entreprise pour l'accès à toutes les transactions bancaires. Le SI en milieu bancaire est très fortement mobilisé en permettant de proposer au client une variété de services contribuant à améliorer la relation de conseil. L'accroissement des possibilités informationnelles offertes, augmente la performance du conseiller en lui fournissant des analyses pertinentes pour chacun de ses clients.

La maîtrise du SI représente ainsi un avantage concurrentiel primordial dans le secteur des banques en Nouvelle-Calédonie. CalédoBank l'a parfaitement compris et emploie 30 personnes au sein de sa direction des systèmes d'information (DSI), soit près d'un huitième de son effectif total de 340 salariés.

La DSI est composée de 3 équipes :

- l'équipe « management du SI » composée du directeur des systèmes d'information (DSI), de la responsable de la sécurité du système d'information (RSSI) et de la déléguée à la protection des données (DPD), de 7 employés à la maîtrise d'ouvrage (MOA) et de 4 chefs de projet technique à la maîtrise d'œuvre (MOE) ;
- l'équipe « des études » avec 4 développeurs ;
- l'équipe « infrastructures et exploitation » composée d'un responsable, 7 ingénieurs ou techniciens prenant en charge le support de niveau 2 et 3 ainsi que de 4 techniciens d'exploitation.

En 2019, CalédoBank a racheté une société de financement de crédits à la consommation afin de renforcer ses positions locales sur le marché des crédits à la consommation et à l'équipement.

Vous travaillez au sein de la DSI de CalédoBank et vous avez pour mission d'assister Léa Deschamps, la responsable de la sécurité du système d'information, dans différentes missions.

Vous participez à l'étude d'exploitation des journaux des équipements réseaux et des serveurs à des fins de surveillance et de collecte d'informations nécessaires à l'analyse de la sécurité du SI.

Dans le cadre du rachat de la société de financement de crédits à la consommation, vous étudiez les conditions de l'intégration de l'application de gestion des crédits à la consommation, en particulier les contraintes liées au Règlement général sur la protection des données (RGPD), à la sécurité des données, à son intégration dans la zone démilitarisée (*DMZ)* ainsi qu'à la dématérialisation de l'offre de prêt.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

[1] La Nouvelle-Calédonie (270 000 habitants dont 170 000 dans l'agglomération de Nouméa) est un archipel du Pacifique Sud. Elle possède une monnaie locale indexée sur le cours de l'Euro, le franc Pacifique (XPF ou CFP).

Dossier A – Centralisation et exploitation des informations de supervision

Mission A1 – Étudier l'apport de la centralisation des fichiers journaux et des métriques

En complément de la supervision en temps réel, les ingénieurs système et réseau doivent régulièrement effectuer le suivi des données obtenues via les différents systèmes de journalisation aussi bien au niveau des actifs réseaux que des serveurs. Vous avez en charge l'étude de la solution de centralisation et d'analyse des fichiers journaux et des métriques fournies par la suite logicielle Elastic Stack.

Question A1.1
Rédiger une courte synthèse expliquant en quoi les outils composant la suite logicielle Elastic Stack répondent aux besoins de la banque CalédoBank.

Peu de temps après la mise en production de la suite logicielle Elastic Stack, les informations relevées sur le tableau de bord relatif au serveur d'échange de fichiers alertent la RSSI.
Une augmentation très importante du trafic vers ce serveur a été détectée. Vous devez analyser ce flux de données anormal capturé par un équipement TAP[2] positionné avant le serveur.

Question A1.2
a) Indiquer l'adresse IP du serveur de fichiers impliqué, le numéro de port et le protocole applicatif associés.
b) Identifier le type d'attaque potentiellement subie par le serveur et les éléments qui le démontrent. Puis, indiquer, si selon vous l'attaque a réussi ou non. *Justifier la réponse.*

Question A1.3
Indiquer deux mesures que vous prendriez, au niveau de la configuration du serveur sans recours à un matériel supplémentaire, pour améliorer le niveau de protection contre ce type d'attaque. *Justifier la réponse.*

Mission A2 - Rechercher des vulnérabilités dans l'infrastructure système et applicative

Suite à une alerte du réseau CERT.FR, datant du 22 septembre 2020, indiquant une recrudescence d'attaques dans le milieu bancaire par le cheval de Troie Emotet, Léa Deschamps, la RSSI de CalédoBank, vous demande de vérifier que le système informatique n'a pas été infecté et de lui remettre un document indiquant la procédure suivie.

Question A2.1
Détailler la recherche de traces permettant d'établir si le système informatique est infecté ou non par le cheval de Troie Emotet.

Aucun indice ne semble faire penser que le système informatique soit infecté actuellement. Seulement la recrudescence de ce cheval de Troie inquiète Léa Deschamps. Elle vous demande de proposer une stratégie visant à réduire les risques de compromission par ce logiciel malveillant.

Question A2.2
Proposer trois mesures à mettre en place afin de réduire les risques de compromission par ce logiciel malveillant. *Justifier la réponse.*

[2] Le TAP (*Test Access Point*) est un équipement réseau passif, offrant sur les interfaces prévues à cet effet une copie du trafic réseau initial qui doit être la plus fidèle possible. Il peut être utilisé à des fins diverses (système de détection d'intrusion ou IDS pour intrusion detection system, monitoring, etc.), et il ne doit pas avoir d'effet sur le réseau, il se comporte comme un port « miroir » d'un commutateur sans les effets de bord (congestion de la bande passante, perte de paquets,etc.).

Dossier B – Intégration de l'application de gestion des crédits à la consommation

CalédoBank, qui jusqu'alors sous-traitait les demandes de crédit à la consommation à la société rachetée, souhaite intégrer l'activité de gestion des demandes de crédits à la consommation à son système d'information. La banque souhaite étudier le développement d'une application *web* spécifique permettant de collecter les informations du demandeur de crédit à la consommation et de lui proposer l'offre de prêt correspondante. Cette application dénommée CréditPlus sera dans un premier temps liée avec l'application CréditCal (application de demandes de crédit à la consommation) afin d'accéder à sa base de données spécifique et à l'application interne de gestion des prêts à la consommation de CalédoBank.

Mission B1 – Vérifier la procédure de demande de crédit à la consommation

La DPD souhaite vérifier que le recueil et le traitement des données envisagés dans le cadre de la nouvelle application *web* CréditPlus sont conformes au RGPD, elle vous demande de participer à l'analyse d'impact relative à la protection des données.

Question B1.1
Identifier, parmi les données personnelles collectées à travers le formulaire de demande de crédit, celles qui paraissent non pertinentes ou qui porteraient atteinte à la vie privée au regard du RGPD.

Question B1.2
a) Relever les droits de l'utilisateur du service mentionnés dans le formulaire de demande de crédit.
b) Indiquer si ces droits sont tous présents. *Justifier la réponse.*

CalédoBank a identifié les risques sur l'application de gestion des crédits à la consommation**.** Vous avez la charge de l'analyse de deux risques :

- risque 1 : vol d'une tablette par une personne externe à CalédoBank ;
- risque 2 : un pirate intercepte les données transmises via le réseau Wifi.

Question B1.3
Proposer pour chaque risque les niveaux de gravité et de vraisemblance en les justifiant ainsi que les impacts sur les critères de sécurité. *Vous vous appuierez sur la méthode préconisée dans le document B5.*

Question B1.4
Proposer, pour chacun des risques identifiés, trois mesures permettant de les diminuer.

Mission B2 – Dématérialiser la procédure d'offre de prêt

Vous avez la charge d'étudier la possibilité pour le client d'accepter l'offre de prêt en la signant électroniquement et de convaincre le DSI du bien fondé de cette proposition. Le type d'authentification prévu, permettant d'accéder à la signature électronique, est le suivant :

- la connexion à l'espace client se réalise via une authentification classique avec un nom d'utilisateur et un mot de passe ;
- pour chaque opération sensible, un code de vérification est ensuite envoyé par SMS sur le téléphone portable de la personne cliente.

Mais la lecture des nouvelles recommandations de l'ANSSI (document B6.1) alerte Léa Deschamps sur le niveau de sécurité mis en œuvre.

Question B2.1
Déterminer si l'authentification de la personne cliente dans la procédure peut être qualifiée de forte. *Justifier la réponse.*

Vous réalisez un ensemble de tests techniques afin de vous assurer du fonctionnement sécurisé de la procédure de signature par l'application CréditPlus.

Dans un premier temps, vous avez signé un document au format PDF en utilisant un ensemble de commandes sous environnement Linux sur le serveur *web*. Vous devez maintenant vérifier que la signature est conforme. Pour cela vous disposez du certificat éphémère produit par l'autorité de certification, du document qui a été signé, de la signature et de la syntaxe des commandes nécessaires.

Question B2.2
Proposer la démarche à suivre pour vérifier la signature en détaillant les commandes OpenSSL que vous utilisez.

Le principe de la dématérialisation de l'offre de prêt est adopté. Il est maintenant nécessaire de préparer le changement.

La réception d'un courriel (*mail*) par le client est le point de départ de l'acceptation de l'offre de prêt à distance. C'est pourquoi CalédoBank souhaite minimiser les risques d'hameçonnage de ses clients en affichant un avertissement sur le site de CalédoBank lors de la demande initiale de crédit. Le DSI vous confie cette tâche d'information des clients.

Question B2.3
Lister trois éléments à intégrer dans l'avertissement précisant les précautions à prendre par le client lors de la réception d'un courriel (*mail*) supposé provenir de CalédoBank.

Mission B3 – Sécuriser l'hébergement des applications de la zone démilitarisée (*DMZ*)

La RSSI, Léa Deschamps, a fait appel à une entreprise spécialisée pour réaliser un audit de sécurité concernant l'application de gestion de crédits qui serait hébergée dans la zone démilitarisée. Leurs conclusions alertent tout particulièrement sur les limites de l'architecture existante en termes de sécurité.

Suite à cet audit et à la prise en compte des recommandations de l'ANSSI, dont un extrait est fourni dans le dossier documentaire, la RSSI propose dans l'urgence, sans ajout de matériel supplémentaire, une nouvelle architecture dont le schéma de principe figure dans le document B8.2.
Vous avez la charge de produire une synthèse justifiant le bien-fondé de cette proposition à destination du DSI.

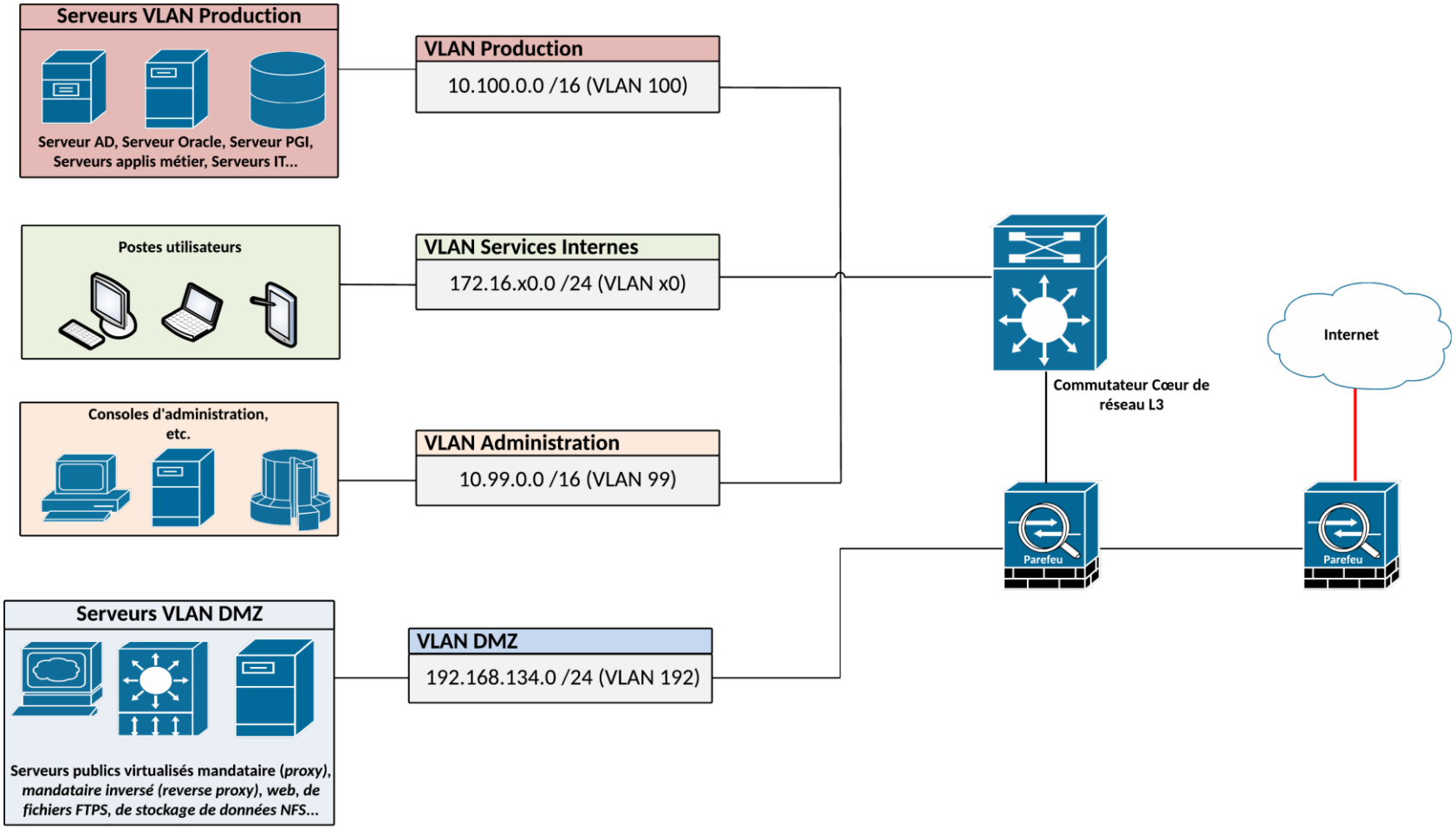
Question B3.1
a) Expliquer en quoi l'architecture actuelle est insuffisante pour garantir un niveau de sécurité au regard des recommandations de l'ANSSI.
b) Justifier en conséquence la nouvelle infrastructure physique proposée.

Après validation de la proposition, vous avez la charge de mettre en œuvre cette infrastructure temporaire.

Question B3.2
a) Proposer, sur la nouvelle architecture, une répartition des sept serveurs virtuels (décrits en fin de document 2) fournissant les services exposés. *Justifier la réponse.*
b) Indiquer les opérations à réaliser sur les pare-feux, tant au niveau de l'adressage IP des interfaces qu'au niveau du principe des règles de filtrage (et non des règles elles-mêmes), pour rendre opérationnelle cette nouvelle topologie. *Vous préciserez les adresses IP attribuées aux interfaces des pare-feux.*

Documents communs

Document 1 : Schéma de l'infrastructure du réseau CalédoBank



Document 2 : Description de l'infrastructure informatique de CalédoBank

L'ensemble des serveurs virtuels utilisés par la société CalédoBank sont hébergés dans deux centres de données (*datacente*rs), l'un sur le site du siège et l'autre sur un site de secours loué à un prestataire. Ces deux sites sont éloignés d'une distance de 2 000 mètres et reliés par une liaison fibre louée avec un débit de 1Gb/s, permettant la synchronisation des données entre les 2 sites.

La connexion au réseau internet entre les agences et le siège utilise une fibre à 1Gb/s.

Chaque ferme de serveurs comporte plusieurs (4 à 7) serveurs physiques DELL, avec une baie de réseau de stockage SAN (*storage area network*) pour le stockage des données locales reliée en fibre optique à l'aide du protocole Fibre Channel aux serveurs. L'outil de virtualisation de serveurs utilisé est VMWare vSphere. Chaque serveur physique est installé avec l'hyperviseur VMWare ESXi. Chaque grappe de haute disponibilité (cluster HA - *high availability*) VMWare est géré par une machine virtuelle vCenter. Sur chaque serveur, une carte réseau est dédiée à l'administration des machines virtuelles ainsi qu'à leur sauvegarde. Un réseau local virtuel (VLAN) « Administration » spécifique a été créé pour regrouper les accès en administration des hyperviseurs VMWare ESXi, de la baie SAN et des équipements réseaux.

Les applications ont été récemment migrées depuis des serveurs PowerPC IBM sous AIX vers des serveurs virtualisés fonctionnant sous système Linux Red Hat.

La DSI applique notamment la philosophie de l'isolation des services en déployant de nouvelles machines virtuelles pour chaque nouveau besoin.
Les réseaux locaux virtuels (*VLAN*) présents sur les commutateurs et sur les pare-feux sont expressément autorisés sur les ports d'interconnexion selon les besoins.

La gestion des utilisateurs et des habilitations est confiée à un domaine Active Directory fonctionnant sous Windows Server 2016.

Les applications utilisées sont les suivantes :

- applications génériques : Office365, Outlook, Exchange Server ;
- progiciel métier : progiciel bancaire ;
- applications métiers spécifiques développées en interne : gestion des prêts à la consommation, gestion des prêts immobiliers, etc.

La zone démilitarisée (DMZ - *demilitarized zone*) est actuellement constituée de l'ensemble des serveurs virtuels exposés sur internet :

- serveur mandataire (*proxy*) ;
- serveur mandataire inversé (*reverse proxy*) servant de pare-feu *web* applicatif (*WAF - web application firewall*) et placé en frontal des serveurs *web* ainsi que du serveur de fichiers FTPS ;
- serveur *web ;*
- serveur accueillant certaines applications métiers ;
- serveur de bases de données associées aux applications métiers ;
- serveur de fichiers FTPS[3] ;
- serveur de stockage des données intégrant le service NFSv4 (*network file system* ou système de fichiers en réseau) associé notamment au serveur FTPS.

Le réseau logique associé à la zone démilitarisée (VLAN 192) est le 192.168.134.0/24.

[3] FTPS (*File Transfer Protocol Secure*) est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication.

Documents associés au dossier A

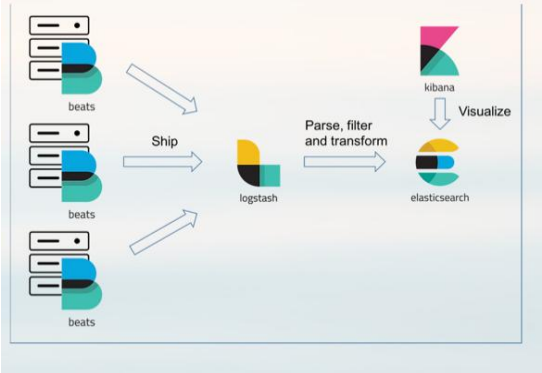
Document A1.1 : Description de la gestion des traces et de la supervision

CalédoBank dispose d'une plateforme de supervision Zabbix à laquelle tout nouvel élément actif déployé et tout nouveau serveur sont intégrés. Ces outils de supervision sont indispensables pour surveiller des systèmes toujours plus complexes, en particulier les applications critiques de la banque. La supervision se révèle très efficace en temps réel et permet de traiter les incidents et de faire remonter les problèmes aux administrateurs système et réseau du bureau Infrastructures. Néanmoins, elle convient peu à une analyse continue des données.

En ce qui concerne les journaux d'événements, chaque serveur et chaque application disposent de son propre fichier journal qui doit être conservé au minimum une année. Par ailleurs, les journaux d'événements des systèmes et des services sont une ressource indispensable pour l'administrateur qui les exploite pour analyser une activité, pour détecter une anomalie ou pour déclencher des alertes. Il est ainsi crucial de gérer de façon fiable le volume de données produites par les journaux de manière à notamment s'assurer que les configurations sont toujours fiables et pouvoir exploiter efficacement la masse d'informations.

Document A1.2 : Extraits de présentation de la suite logicielle Elastic Stack (site officiel)

La suite logicielle Elastic Stack est une solution proposant différents modules qui convient parfaitement au besoin d'analyse et de collecte de données de supervision comme les fichiers journaux (*logs*). Le tableau ci-dessous présente les principaux modules et leur articulation.



- Beats : agents légers de collecte et de transfert de données
  - Filebeat : agent dédié aux fichiers journaux
  - PacketBeat : agent dédié au réseau
  - MetricBeat : agent dédié aux métriques système
- Logstash : agrégateur de logs, transforme puis transporte les logs vers un stockage
- Elasticsearch : moteur d'indexation et de recherche, destination finale des logs et métriques
- Kibana : interface de visualisation et d'analyse pour le moteur Elasticsearch

Effectuer le suivi d'un fichier directement dans l'interface utilisateur
Gardez un œil sur tous les logs qui circulent sur vos serveurs, machines virtuelles et conteneurs, le tout, grâce à une vue centralisée. Sélectionnez des champs structurés comme le type d'IP ou d'événement, et explorez les logs associés. Avec l'application logs de Kibana, affichez tous vos logs comme sur une console, sous forme de flux en temps réel.

Analyser les tendances avec des logs catégorisés
Au lieu de faire défiler les logs à la main pour identifier ceux qui sont similaires, repérez instantanément les tendances via la vue de catégorisation des logs, analysez les événements qui ont été regroupés en fonction de leurs messages et de leurs formats.

Traitement flexible des flux de données
Avec Elastic, préparez vos logs pour une recherche rapide et centralisée est un jeu d'enfants, quels que soient le type de sources et leur nombre. L'agent Beats transfère directement vos logs et métriques vers Elasticsearch depuis vos systèmes. Les modules Beats offrent des fonctionnalités d'analyse, d'indexation et de visualisation prêtes à l'emploi pour les formats de fichier courants. L'agrégateur Logstash peut agir comme une couche dédiée au traitement des flux de données : il ingère, analyse et transforme même vos données les plus complexes.

Document A2.1 : Tableau de bord des informations du serveur d'échange de fichiers

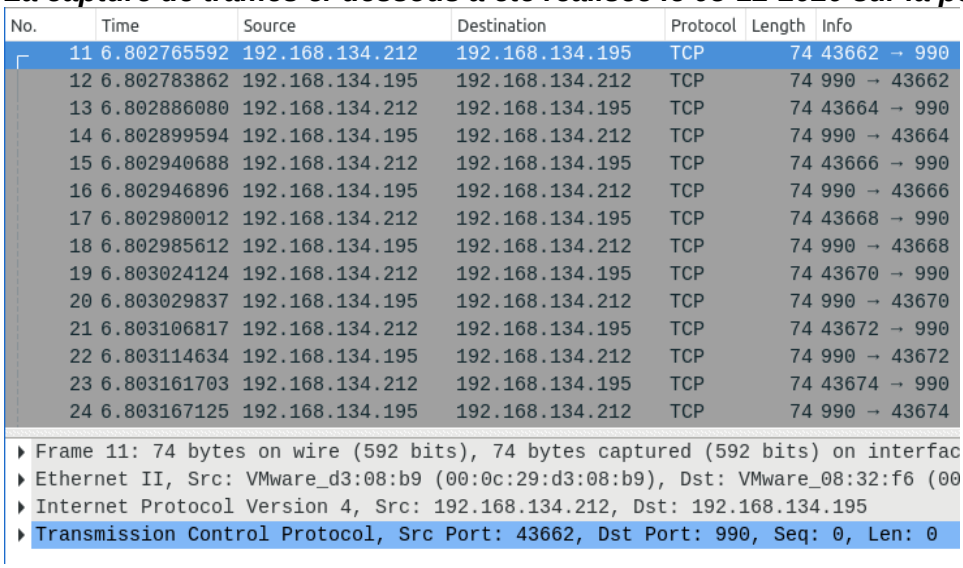
Le tableau de bord ci-dessous issu de l'interface de visualisation et d'analyse Kibana, outil de la suite logicielle Elastic Stack, permet de visualiser sur une période donnée l'utilisation du processeur (CPU), de la mémoire, le nombre de processus actifs et le nombre de tentatives de connexion réussies et échouées.

La DSI dispose d'un serveur d'échange de fichiers FTPS en zone démilitarisée (*DMZ*), accessible actuellement par les prestataires et fournisseurs externes, afin d'y déposer les devis et factures des interventions ou commandes. Ces documents sont automatiquement transférés tous les soirs vers un serveur interne et indexés dans le système de gestion électronique de documents (*GED*).

Une augmentation très importante du trafic vers ce serveur a été détectée l**e 05-12-2020 sur la période 18h-20h.**

Document A2.2 : Extrait d'une capture de trames avec l'application Wireshark

La capture de trames ci-dessous a été réalisée le 05-12-2020 sur la période 18h-20h



No.	Time	Source	Destination	Protocol	Length	Info
11	6.802765592	192.168.134.212	192.168.134.195	TCP	74	43662 → 990
12	6.802783862	192.168.134.195	192.168.134.212	TCP	74	990 → 43662
13	6.802886080	192.168.134.212	192.168.134.195	TCP	74	43664 → 990
14	6.802899594	192.168.134.195	192.168.134.212	TCP	74	990 → 43664
15	6.802940688	192.168.134.212	192.168.134.195	TCP	74	43666 → 990
16	6.802946896	192.168.134.195	192.168.134.212	TCP	74	990 → 43666
17	6.802980012	192.168.134.212	192.168.134.195	TCP	74	43668 → 990
18	6.802985612	192.168.134.195	192.168.134.212	TCP	74	990 → 43668
19	6.803024124	192.168.134.212	192.168.134.195	TCP	74	43670 → 990
20	6.803029837	192.168.134.195	192.168.134.212	TCP	74	990 → 43670
21	6.803106817	192.168.134.212	192.168.134.195	TCP	74	43672 → 990
22	6.803114634	192.168.134.195	192.168.134.212	TCP	74	990 → 43672
23	6.803161703	192.168.134.212	192.168.134.195	TCP	74	43674 → 990
24	6.803167125	192.168.134.195	192.168.134.212	TCP	74	990 → 43674

Ports courants

http(80), https(443)
ftp(21), ftps(990)
ssh(22), imap(143),
imaps(993), pop(110),
pops(995), smtp(25),
smtps(587)

Document A2.3 : Extrait du journal du serveur d'échange de fichiers

L'extrait ci-dessous du journal du serveur d'échange de fichiers a été réalisé le 05-12-2020 sur la période 18h-20h.

```
Sat Dec  5 19:58:40 2020 [pid 2536] CONNECT: Client "192.168.134.212"
Sat Dec  5 19:58:40 2020 [pid 2536] DEBUG: Client "192.168.134.212", " "SSL version: TLSv1.3, SSL
cipher: TLS_AES_256_GCM_SHA384, not reused, no cert"
Sat Dec  5 19:58:40 2020 [pid 2536] FTP response: Client "192.168.134.212", "220 (vsFTPd 3.0.3)"
Sat Dec  5 19:58:40 2020 [pid 2536] FTP command: Client "192.168.134.212", "USER admin"
Sat Dec  5 19:58:40 2020 [pid 2536] [admin] FTP response: Client "192.168.134.212", "331 Please
specify the password
Sat Dec  5 19:58:40 2020 [pid 2536] [admin] FTP command: Client "192.168.134.212", "PASS
<password>"
Sat Dec  5 19:58:43 2020 [pid 2537] [admin] FAIL LOGIN: Client "192.168.134.212"
Sat Dec  5 19:58:44 2020 [pid 2536] [admin] FTP response: Client "192.168.134.212", "530 Please
login with USER and PASS."
Sat Dec  5 19:58:44 2020 [pid 2536] DEBUG: Client "192.168.134.212", "Control connection
terminated without SSL shutdown."
Sat Dec  5 19:58:45 2020 [pid 2540] CONNECT: Client "192.168.134.212"
Sat Dec  5 19:58:45 2020 [pid 2540] DEBUG: Client "192.168.134.212", " "SSL version: TLSv1.3, SSL
cipher: TLS_AES_256_GCM_SHA384, not reused, no cert"
Sat Dec  5 19:58:45 2020 [pid 2540] FTP response: Client "192.168.134.212", "220 (vsFTPd 3.0.3)"
Sat Dec  5 19:58:45 2020 [pid 2540] FTP command: Client "192.168.134.212", "USER utilisateur"
Sat Dec  5 19:58:45 2020 [pid 2540] [admin] FTP response: Client "192.168.134.212", "331 Please
specify the password
Sat Dec  5 19:58:45 2020 [pid 2540] [admin] FTP command: Client "192.168.134.212", "PASS
<password>"
Sat Dec  5 19:58:46 2020 [pid 2539] [admin] FAIL LOGIN: Client "192.168.134.212"
Sat Dec  5 19:58:47 2020 [pid 2540] [admin] FTP response: Client "192.168.134.212", "530 Please
login with USER and PASS."
Sat Dec  5 19:58:48 2020 [pid 2540] DEBUG: Client "192.168.134.212", "Control connection
terminated without SSL shutdown."
Sat Dec  5 19:58:50 2020 [pid 2548] CONNECT: Client "192.168.134.212"
Sat Dec  5 19:58:50 2020 [pid 2548] DEBUG: Client "192.168.134.212", " "SSL version: TLSv1.3, SSL
cipher: TLS_AES_256_GCM_SHA384, not reused, no cert"
Sat Dec  5 19:58:50 2020 [pid 2548] FTP response: Client "192.168.134.212", "220 (vsFTPd 3.0.3)"
Sat Dec  5 19:58:50 2020 [pid 2548] FTP command: Client "192.168.134.212", "USER user"
Sat Dec  5 19:58:50 2020 [pid 2548] [admin] FTP response: Client "192.168.134.212", "331 Please
specify the password
Sat Dec  5 19:58:50 2020 [pid 2548] [admin] FTP command: Client "192.168.134.212", "PASS
<password>"
Sat Dec  5 19:58:52 2020 [pid 2547] [admin] FAIL LOGIN: Client "192.168.134.212"
```

Document A3 : Extrait du bulletin d'alerte "CERTFR-2020-ALE-019" du CERT.FR

Objet : Recrudescence d'activité du cheval de Troie Emotet en France

A. Caractéristiques du cheval de Troie Emotet

Observé pour la première fois mi-2014 en tant que cheval de Troie bancaire, Emotet a évolué pour devenir un cheval de Troie modulaire. Ses différents modules actuels lui permettent :

- de récupérer les mots de passe stockés sur un système ainsi que sur plusieurs navigateurs et boîtes courriel ;
- de dérober la liste de contacts, le contenu et les pièces jointes attachées à des courriels ;
- de se propager au sein du réseau infecté en tirant parti de vulnérabilités SMB ainsi que des mots de passe récupérés.

Le code malveillant est distribué par le réseau de robots (*botnet*) du même nom au travers de campagnes massives de courriels d'hameçonnage. Ces courriels d'hameçonnage contiennent généralement des pièces jointes Word ou PDF malveillantes, et plus rarement des URL pointant vers des sites compromis ou vers des documents Word contenant des macrocommandes.

Depuis 2017, Emotet n'est plus utilisé en tant que cheval de Troie bancaire, mais distribue fréquemment au sein des systèmes d'information qu'il infecte, d'autres codes malveillants. Ainsi, la détection et le traitement au plus tôt d'un évènement de sécurité lié à Emotet peut prévenir de nombreux types d'attaques, dont celles par rançongiciel avant le chiffrement.

B. Fonctionnement et description de l'attaque

Après une absence de cinq mois, Emotet a refait surface en juillet 2020. Depuis, nombre de ses campagnes d'hameçonnage exploitent une technique de détournement des fils de discussion des courriels. Une fois la boîte courriel d'un employé ou celle générique de l'entité victime elle-même compromise, le code malveillant Emotet exfiltre le contenu de certains de ses courriels. Sur la base de ces derniers, les attaquants produisent des courriels d'hameçonnage prenant la forme d'une réponse à une chaîne de courriels échangés entre l'employé et des partenaires de l'entité pour laquelle il travaille. Ces courriels, d'apparence légitime, sont envoyés à des contacts de la victime, et plus particulièrement aux tierces parties de l'entité (clients et prestataires notamment) ayant participé au fil de discussion originel, afin d'accroître leur crédibilité auprès des destinataires. Dans tous les cas, il apparaît que les courriels d'hameçonnage sont envoyés depuis l'infrastructure des attaquants sur la base d'adresses courriel expéditrices souvent vraisemblables .

C. Moyens de détection relatifs au logiciel malveillant Emotet

Les chercheurs en cybersécurité de Cryptolaemus fournissent sur leur site *web* (https://paste.cryptolaemus.com/) des expressions régulières permettant de détecter les liens utilisés dans les courriels malveillants.
Emocheck, un outil créé par le centre gouvernemental de veille, d'alertes et de réponses aux attaques informatiques (CERT) japonais, permet de détecter la présence du trojan Emotet sur une machine Windows. Emotet utilisant un dictionnaire prédéfini pour le nom de ses processus, ce programme vérifie si un programme en cours d'exécution correspond à ce dictionnaire précis. L'outil est disponible en source ouverte : https://github.com/JPCERTCC/EmoCheck.
Des sites spécialisés comme Feodotracker (https://feodotracker.abuse.ch/browse/) recensent la liste des serveurs de commandes et de contrôle (C&Cs) des réseaux de machines zombies (*botnet*) sollicités lors d'une attaque par Emotet.

Documents associés au dossier B

Document B1 : Interview de monsieur Lefranc, directeur des systèmes d'information

Quelles démarches doit réaliser un client pour réaliser une demande de crédit à la consommation ?

Tout d'abord, le client potentiel doit faire une demande de crédit à la consommation en ligne sur notre site internet *(voir document B4)*. Les données, saisies dans le formulaire, sont enregistrées dans une base de données implantée sur le serveur.

Une fois cette demande réalisée, un conseiller financier contacte le client afin de prendre rendez-vous dans l'objectif de valider le dossier du client. Lors du rendez-vous, le conseiller passe en revue les différents éléments saisis lors de la demande en ligne et vérifie que toutes les informations enregistrées sont correctes. Pour cela, le conseiller utilise l'application CréditPlus grâce à une tablette mise à sa disposition. L'application permet de visualiser toutes les données enregistrées sur le serveur.

Il récupère ensuite les différents documents, apportés par le client, nécessaires au traitement du dossier de demande de crédit à la consommation. Les documents sont numérisés grâce à la tablette. Les documents sont stockés sur la tablette puis transmis au serveur. C'est lors de cette étape que le conseiller vérifie et valide l'identité du client. Les tablettes sont stockées dans le bureau de l'accueil, accessibles librement à l'ensemble des salariés qui viennent en récupérer une dès qu'ils en ont besoin. Les données présentes sur la tablette ne sont pas chiffrées mais sont purgées chaque fin de semaine. Les tablettes fonctionnent sous Android et sont connectées au réseau sans-fil de l'agence. Le réseau Wifi a pour nom CB_Wifi et est sécurisé par une clé WPA2/TKIP.

À partir de l'ensemble des documents et informations fournis par le client, un traitement de nuit sur le serveur hébergeant l'application analyse la capacité de remboursement du client et procède à des vérifications de solvabilité auprès de la Banque de France.

Si la demande est acceptée, une offre de prêt est émise présentant toutes les caractéristiques du prêt. Cette offre est envoyée par voie postale au client.

Après réception de l'offre, un délai de réflexion légale de 10 jours démarre, le client peut ensuite accepter son offre de prêt en venant directement en agence afin de signer une version papier de l'offre de prêt.

Document B2 : Droits de l'utilisateur d'un service numérique sur ses données personnelles

Les droits de l'utilisateur d'un service numérique sur ses données personnelles sont :

- droit d'accès aux données à caractère personnel (DCP), de rectification et d'effacement des données (inexactes, incomplètes, équivoques, ou périmées) ;
- droit à la limitation du traitement dans les conditions prévues par la réglementation ;
- droit d'opposition ;
- droit d'introduire une réclamation auprès d'une autorité de contrôle (CNIL) ;
- droit à la portabilité des données ;
- droit de retirer le consentement à tout moment.

Les conditions d'exercice de ces droits, notamment le recours à un délégué à la protection des données personnelles (DPD) doit être garanti.

Document B3 : Obligations incombant au responsable du traitement et au sous-traitant

Article 57, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En application de l'article 24 du règlement (UE) 2016/679 du 27 avril 2016*, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à ce même règlement et à la présente loi.

Le responsable du traitement et, le cas échéant, son représentant tiennent le registre des activités de traitement dans les conditions prévues à l'article 30 de ce règlement. Ils désignent un délégué à la protection des données dans les conditions prévues par la section 4 du chapitre IV du même règlement.

**communément appelé Règlement général sur la protection des données (RGPD)*

Document B4 : Nouveau formulaire de demande de crédit à la consommation CalédoBank

VOTRE DEMANDE DE CRÉDIT – Remplissez le formulaire ci-dessous

Profil					
Vous êtes client :		Veuillez renseigner ci-dessous vos numéros de compte pour ces organismes bancaires :			
O CalédoBank		N°……			
O BCI		N°……			
O BNC		N°……			
O Autre		N°……			
Nom et prénom du demandeur :		Date de naissance du demandeur :		N°Sécurité sociale :	
		jj / mm / aaaa			
Votre communauté d'appartenance (facultatif)					
O Kanake O Européenne	O Wallisienne et futunienne	O Tahitienne ONivanuataise	O Indonésienne O Vietnamienne	O Métisse	O Autre (précisez)
Votre situation familiale					
O Célibataire	O Union libre (durée)	O PACS (date)	O Marié (date)	O Divorcé (date)	
Nombre de personnes à charge					
Enfants mineurs (Nombre)	Enfants majeurs (Nombre)	Parents à charge (Nombre)	Cause du handicap (Indiquez ici la raison de la prise en charge)		
Contacts					
Téléphone	Mobile	Adresse courriel			

Demande	
Vous souhaitez :	Objet du financement
O Crédit bail mobilier O Crédit classique	
Montant du financement souhaité	Durée

Finaliser	
Sélectionnez l'agence avec laquelle vous souhaitez prendre rendez-vous :	Message :
O Agence Nouméa Centre O Agence Victoire…	(Écrivez ici les demandes complémentaires pouvant accompagner votre dépôt de dossier)

Traitement des données

O En soumettant ce formulaire je confirme avoir bien pris connaissance de mes droits et consent au traitement des données personnelles renseignées dans ce formulaire, par CalédoBank, dans la limite des dispositions prévues par la Réglementation générale sur la protection des données (RGPD).

Protection des données

CalédoBank est conduite à recueillir des données à caractère personnel vous concernant, en qualité de responsable de traitement. Les données collectées font l'objet d'études et sont nécessaires au bon traitement de votre demande de crédit en ligne. Vos données à caractère personnel pourront être conservées pour une durée de cinq (5) ans à compter de la clôture du compte ou de la cessation de la relation (les informations concernant une personne non-cliente seront supprimées dès la fin de leur traitement, répondant à leur demande, où dans un délai de cinq (5) ans après la réception). Le transfert de données à caractère personnel rendus nécessaires interviennent dans les conditions et sous des garanties propres à assurer la confidentialité et la sécurité de ces données. À ce titre, CalédoBank met en œuvre toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité de vos données à caractère personnel. Vous disposez d'un droit d'accès à vos données à caractère personnel, de rectification et d'effacement, de limitation du traitement ainsi que d'un droit à l'opposition dans les conditions prévues par la réglementation applicable. Vous pourrez exercer vos droits ainsi que contacter le délégué à la protection des données personnelles en vous adressant à l'agence où est géré/ouvert le compte, par courrier électronique à l'adresse suivante dpd@caledobank.nc. Vous avez le droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité de contrôle en charge du respect des obligations en matière de données à caractère personnel.

Attention - Un crédit vous engage et doit être remboursé. Vérifiez vos capacités de remboursement avant de vous engager. Offre valable sous réserve d'acceptation de votre dossier par CalédoBank.

Document B5 : Analyse des risques (source : la CNIL)

La méthode EBIOS Risk Manager (expression des besoins et identification des objectifs de sécurité) développée par l'ANSSI (agence nationale de la sécurité des systèmes d'information) initialement prévue pour la gestion des risques informatiques a été adaptée aux traitements de données à caractère personnel (DCP) par la CNIL (commission nationale de l'informatique et des libertés).

La gravité représente l'ampleur d'un risque. Elle est déterminée en fonction du :

- **caractère identifiant (CI) des DCP** c'est-à-dire avec quelle facilité peut-on identifier les personnes concernées ? : l'échelle va du niveau « 1 - négligeable » (il semble impossible d'identifier les personnes avec par exemple un seul prénom) à « 4 - maximal » (il semble extrêmement facile d'identifier les personnes avec par exemple le nom, prénom, date de naissance et l'adresse postale) en passant par « 2 - limité » et « 3 - important » ;
- **caractère préjudiciable (CP)** de ces impacts potentiels c'est-à-dire quelle serait l'importance des dommages correspondant à l'ensemble des impacts potentiels ? : l'échelle va du niveau « négligeable » (les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté) à « maximal » (les personnes concernées pourraient connaître des conséquences significatives comme des dettes importantes) en passant par « 2 - limité » et « 3 - important ».

La vraisemblance traduit la faisabilité d'un risque. Elle est directement liée :

- **à la vulnérabilité des supports (VS**) c'est-à-dire dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ? : l'échelle va du niveau « 1. négligeable » (il ne semble pas possible de réaliser la menace en s'appuyant sur les caractéristiques des supports comme un vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès) à « 4. maximal » (il semble extrêmement facile que la menace se réalise en s'appuyant sur les caractéristiques des supports comme le vol de supports papier stockés dans le hall public de l'organisme) ;
- **aux capacités des attaquants (CA**) à les exploiter c'est-à-dire quelles sont leurs capacités à exploiter les vulnérabilités compte tenu de leurs compétences, proximité du système, motivation, etc. ? : l'échelle va du niveau « 1. négligeable » (les sources de risques ne semblent pas avoir de capacités particulières comme le détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints) à « 4. maximal » (les sources de risques ont des capacités certaines, comme le détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges d'administration illimités).

La gravité et la vraisemblance se déterminent en additionnant respectivement les valeurs des deux critères retenus.	**CI + CP**	**Gravité**	**VS + CA**	**Vraisemblance**
	<5	1 : Négligeable	<5	1 : Négligeable
	=5	2 : Limité	=5	2 : Limité
	=6	3 : Important	=6	3 : Important
	>6	4 : Maximal	>6	4 : Maximal

Exemple de risque à analyser : vol de données par un informaticien de CalédoBank sachant que tous les informaticiens ont accès aux données du serveur hébergeant la base de données

Gravité : **7>6 d'où une gravité maximale**

- **CI : 4** car les DCP des clients sont stockées dans la base de données et ces dernières identifient parfaitement les personnes
- **CP : 3** car compte tenu du type des données, cela peut être très préjudiciable.

Vraisemblance : **5 d'où une vraisemblance limitée**

- **VS : 4** car la base de données est accessible par TOUS les informaticiens sans distinction de privilèges.
- **CA : 1** on suppose ici que l'informaticien n'a pas de motivation particulière de nuire et qu'il est peu probable qu'il en arrive à voler des données.

Impact : confidentialité (transmission / vente de données client) et intégrité des données (modification des données client). Aucun impact sur la disponibilité.

Document B6.1 : Extrait des recommandations relatives à l'authentification multifacteur et aux mots de passe publiées par l'ANSSI

L'authentification multifacteur est souvent confondue avec l'appellation authentification forte, ce qui laisserait entendre qu'une authentification multifacteur est nécessairement plus robuste qu'une authentification avec un unique facteur.
Il convient ainsi de différencier authentification multifacteur et authentification forte. Une authentification multifacteur est une authentification faisant intervenir plusieurs catégories de facteurs. Néanmoins, ces facteurs, pris indépendamment ou ensemble, ne sont pas forcément considérés comme étant forts.

Une authentification forte, qui repose généralement sur un facteur unique, est une authentification reposant sur un mécanisme cryptographique (ex : paire de clés SSH ou PGP) dont les paramètres et la sécurité sont jugés robustes.

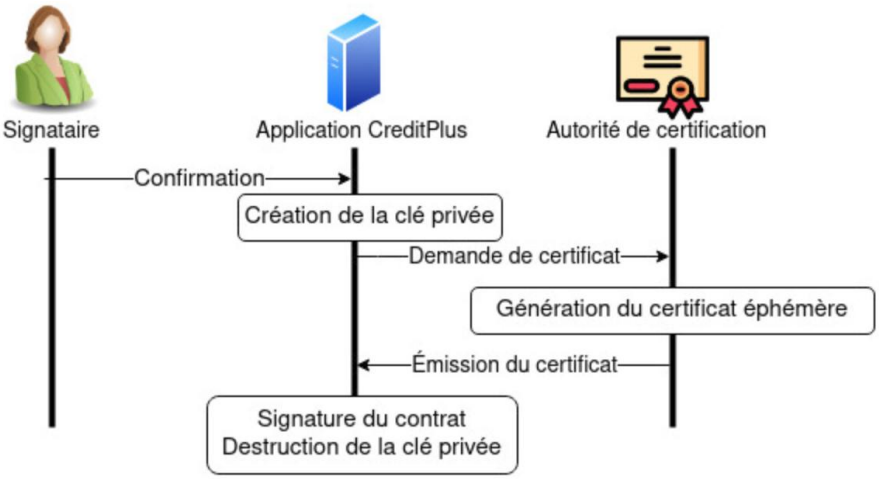
Document B6.2 : Déroulement de l'acceptation de l'offre de prêt via l'espace client

Étape 1 : Suite à l'émission de l'offre de prêt, un courriel est envoyé au client l'invitant à se rendre sur son espace client pour consulter les différents documents relatifs au prêt.
Étape 2 : à compter de la date de réception du courriel, le client dispose d'un délai de 30 jours maximum pour accuser réception de l'offre. Pour ce faire, une fonctionnalité est à disposition dans l'espace client. Il suffit de cocher une case pour confirmer. À partir de ce moment, le délai de réflexion est de 14 jours. Durant cette période, seule la consultation de l'offre est possible.
Étape 3 : passé le délai de réflexion, le client reçoit un courriel l'invitant à signer de manière électronique l'offre de prêt en se connectant à l'espace client.
Étape 4 : le client se connecte à son espace client afin de signer numériquement l'offre. L'objectif est de permettre au client d'identifier tous les éléments lui permettant de signer les documents souhaités en toute connaissance de cause. Le client doit consulter et valider tous les documents en cochant des cases indiquant que le client confirme avoir pris connaissance des documents et donne son consentement. Cela inclut la mise à disposition de conditions générales de service de signature visant à reprendre de manière synthétique les conditions de signature, les obligations du fournisseur et celles du signataire. Enfin, il déclenche la signature électronique grâce à un bouton mis à disposition. Le client reçoit ensuite un code de confirmation par SMS sur son téléphone portable ; il dispose de cinq minutes pour saisir ce code. S'il est correct, la signature électronique du document est réalisée.

Document B6.3 : Schématisation du principe de réalisation de la signature électronique

Afin de permettre la signature à distance, un système de certificat éphémère est utilisé grâce à la présence d'un serveur ayant pour rôle celui d'autorité de certification (CA).

(1) À la suite du déclenchement
clé privée.
(2) L'application effectue ensuite
(3) L'autorité de certification éme
de certification puis envoyé à l'ap
(4) Une fois le certificat éphémè
crédit grâce à la clé privée qui es



Document B7.1 : Fichiers et commandes Linux utilisés pour la création de la signature

Fichiers utilisés :

- contrat_test.pdf : le document à signer
- srvdbapp.key : la clé privée du serveur d'application CréditPlus

OpenSSL est une commande en ligne Linux permettant la création de clés, de certificats, de calcul d'empreintes, le chiffrement et déchiffrement, la signature. La syntaxe générale de la commande est :

`openssl <commande> <options>`

Réalisation de la signature

Étape 1 - Hachage du document :

`openssl dgst -sha512 -out contrat.dgt contrat_test.pdf`

Cette commande produit un fichier contrat.dgt qui constitue l'empreinte du document contrat_test.pdf.

La commande **openssl dgst** permet de réaliser une empreinte d'un fichier. L'option -sha512 définit la fonction de hachage sha avec une empreinte de 512 bits.

Étape 2 - Signature[4] de l'empreinte avec la clé privée :

`openssl rsautl -sign -in contrat.dgt -inkey srvdbapp.key -out contrat.sig`

Cette commande produit un fichier contrat.sig qui constitue la signature du document contrat_test.pdf.

La commande **openssl rsautl** avec l'option -sign permet de signer une empreinte à l'aide d'une clé privée (ici srvdbapp.key) indiquée par l'option -inkey.

Document B7.2 : Fichiers et commandes Linux proposés pour la vérification de la signature

Fichiers mis à disposition :

- srvdbapp.crt : le certificat éphémère émis par l'autorité de certification
- contrat_test.pdf : le document signé
- contrat.sig : signature du document contrat_test.pdf
- contrat.dgt : empreinte originale du premier document contrat_test.pdf

Commandes à utiliser :

La commande **openssl x509** permet d'extraire la clé publique d'un certificat et de la stocker dans un fichier :

- `openssl x509 -pubkey -noout -in [certificat] > [fichier.pem]`

La commande **openssl rsault** avec l'option verify permet de vérifier une signature grâce à une clé publique. Cette commande produit en sortie un fichier correspondant au résultat obtenu :

- `openssl rsautl -verify -in [signature] -pubin -inkey [clé publique] -out [fichier.dgt]`

La commande **diff** permet de comparer deux fichiers. Cette commande renvoie les différences entre les deux fichiers, rien si les deux fichiers sont identiques :

- `diff fichier1 fichier2`

[4] L'opération consistant à signer avec une clé privée est différente de celle consistant à chiffrer avec une clé privée. Les schémas utilisés lors de la signature ont pour objectif de garantir la non-répudiation alors que ceux utilisés lors du chiffrement ont pour objectif de garantir la confidentialité.

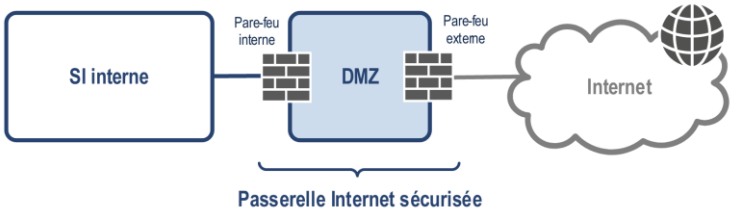
Document B8.1 : Recommandations relatives à la zone démilitarisée (*DMZ*) extraites du guide ANSSI-PA-066

Pour de nombreuses entités, l'interconnexion de leur SI avec internet est nécessaire, mais ce dernier constitue une source de menaces. Parmi les plus courantes, il est possible de citer :

- l'exfiltration de données depuis le SI de l'entité vers internet, portant atteinte à leur confidentialité ;
- l'intrusion pour porter atteinte à l'intégrité ou la disponibilité du SI de l'entité ;
- l'usurpation d'identité en accédant à des ressources de l'entité pour rebondir et mener des attaques vers d'autres cibles ;
- le déni de service pour nuire à la disponibilité de l'accès internet et donc à la productivité ou à l'image de l'entité ;
- l'accès par les collaborateurs à des sites *web* interdits par la charte d'utilisation interne voire par la loi.

Recommandations minimales de l'ANSSI :

- l'interconnexion entre internet et la zone démilitarisée (*DMZ*) doit être protégée de façon périmétrique par un pare-feu dédié nommé pare-feu externe ;
- l'interconnexion entre le réseau interne et la zone démilitarisée (*DMZ*) doit être protégée de façon périmétrique par un pare-feu spécifique nommé pare-feu interne.



Une passerelle internet sécurisée est constituée d'une ou plusieurs zones démilitarisées (*DMZ*) protégées par des pare-feux périmétriques et servant, en leur sein et autant que possible, à la rupture protocolaire[5] et à l'analyse du trafic échangé entre un réseau public et le SI interne de l'entité.

La zone démilitarisée (*DMZ*) est ici considérée comme une zone neutre et perdable. En effet, sa sensibilité n'est pas nulle (des données du SI de l'entité peuvent y être exposées ou au moins y transiter) mais une attaque en intégrité ou en confidentialité sur ses composants ne doit pas remettre en cause de manière irréversible et durable le bon fonctionnement du SI de l'entité. À titre d'exemple, la compromission d'un relais de messagerie au sein d'une zone démilitarisée (*DMZ*) pourrait amener à décider sa destruction et sa reconstruction sans que les boîtes aux lettres électroniques hébergées et protégées de manière ad hoc dans le SI interne de l'entité ne soient elles-mêmes détruites. Ainsi, une zone démilitarisée (*DMZ*) intermédiaire permettant de séparer les services des données est fortement recommandée.

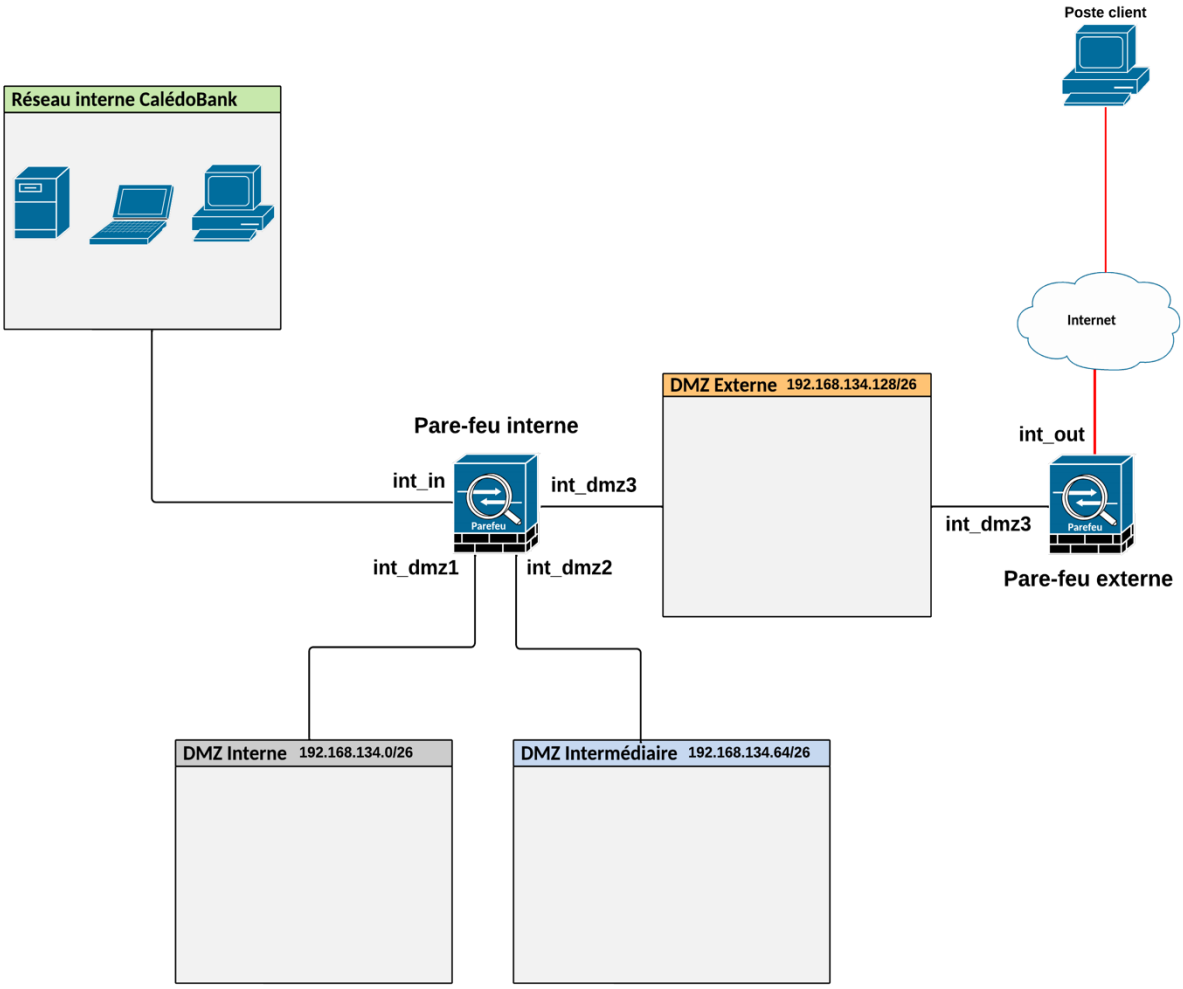
Il est donc nécessaire de distinguer quatre principaux types de zones réseaux :

- la zone de services relais pour la rupture protocolaire et l'analyse des flux, située entre le pare-feu interne et le pare-feu externe, appelée *DMZ externe*.
- la zone de services exposés pour l'hébergement éventuel de serveurs métier appelée *DMZ intermédiaire* ;
- la zone hébergeant les données accessibles par les services exposés appelée *DMZ interne ;*
- la zone de services internes pour les ressources mises à disposition du réseau local.

5 Une rupture protocolaire consiste à casser en entrée et reconstruire en sortie la communication entre deux ressources (généralement un client et un serveur) au niveau d'une des couches du modèle OSI (open system interconnections). Les protocoles en entrée et en sortie peuvent être distincts suivant les contraintes techniques de l'environnement et les objectifs de sécurité.

Document B8.2 : Architecture physique et logique proposée pour la zone démilitarisée (DMZ)

Schéma de principe :



Topologie logique :

Le réseau logique 192.168.134.0/24 actuellement affecté à la zone démilitarisée (*DMZ*) sera découpé en trois sous-réseaux de taille identique :

- zone démilitarisée interne : 192.168.134.0/26
- zone démilitarisée intermédiaire : 192.168.134.64/26
- zone démilitarisée externe : 192.168.134.128/26

Les adresses IP des interfaces de chaque pare-feu se verront affectées les dernières adresses IP disponibles sur le sous-réseau.

Les interfaces sont nommées par convention int suivi de la zone réseau (dmz1 pour la zone démilitarisée DMZ interne, dmz2 pour la zone démilitarisée DMZ intermédiaire, dmz3 pour la zone démilitarisée DMZ externe) sur laquelle elles sont connectées.

Aucun ajout de réseaux locaux virtuels (*VLAN*) n'est nécessaire.