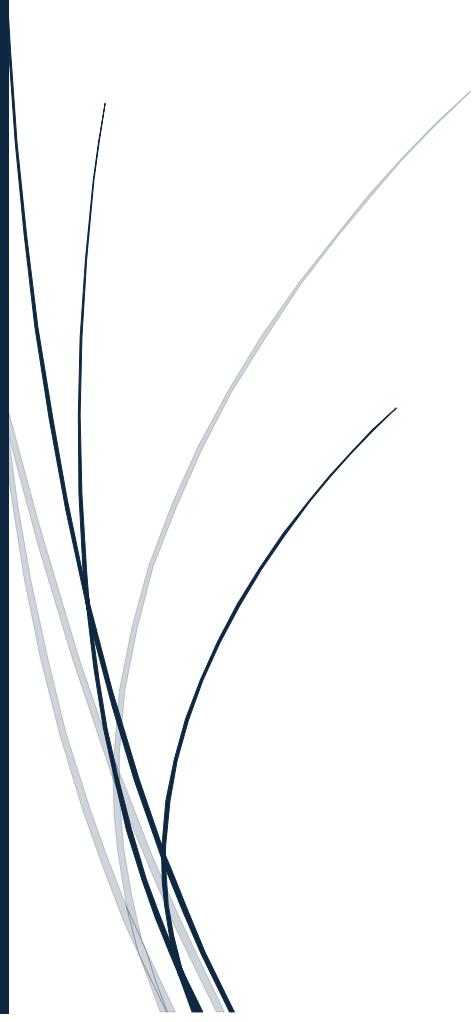
23/10/2025

Audit de cybersécurité

FORMACTION



Wladimir Bigand
CAMPUS ERMITAGE

Table des matières

Contexte et objectifs de la mission

1.1 Présentation de FORMACTION

FORMACTION est un centre de formation propose diverses formations professionnelles et initiales en informatique, comptabilité et juridique. Ils ont différents locaux répartis dans la France (6 au total) afin d'accueillir les formés et dispenser les cours localement.

1.2 Objectif de la mission de conseil

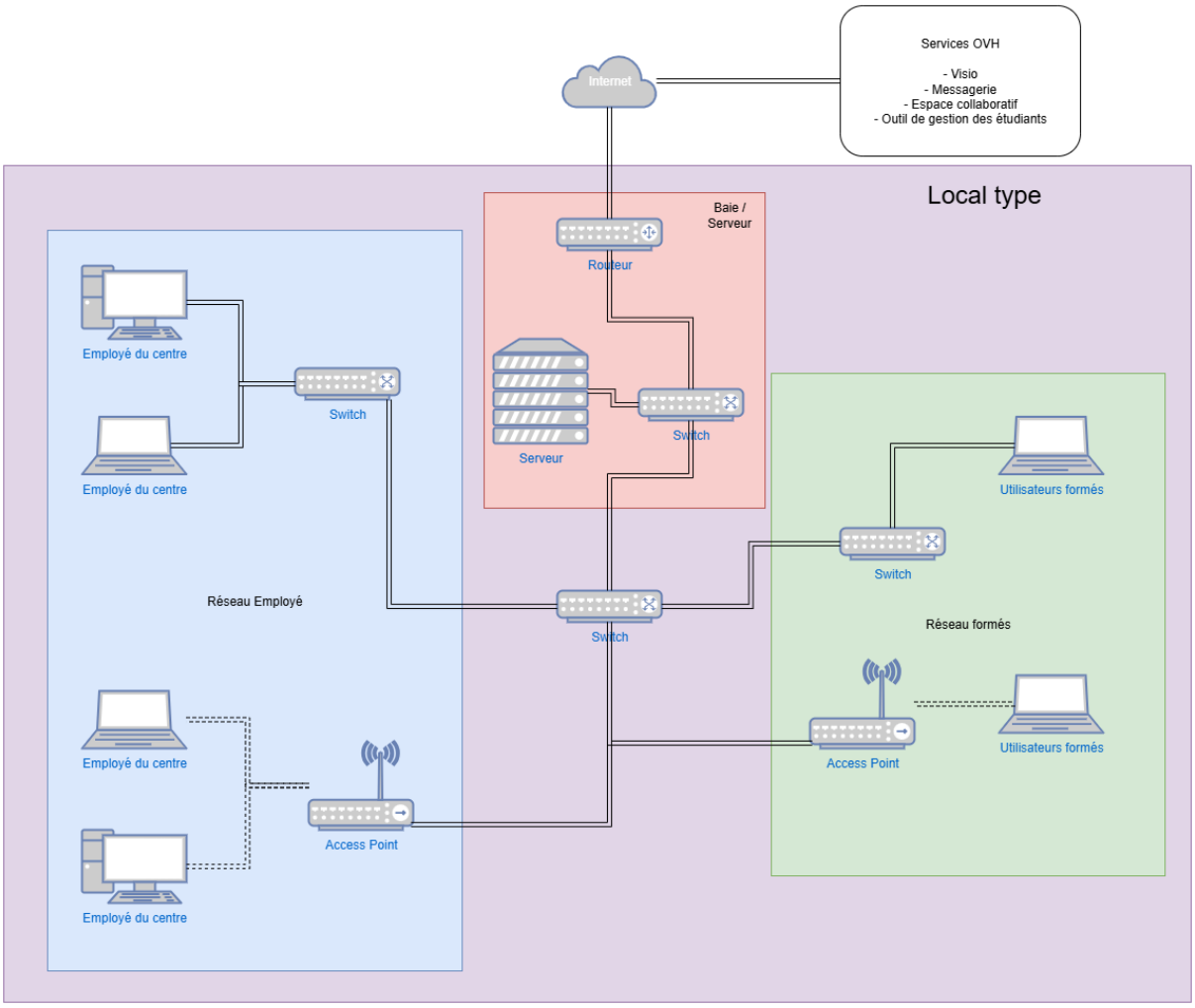
L'objectif est de conseiller le centre de formation sur la sécurité de leurs infrastructures informatiques.

Architecture du système d'information

2.1 Description générale du fonctionnement

FORMACTION opère un système d'information multisites réparti sur six locaux en France, chacun disposant d'une salle serveur attenante à la baie de brassage et desservant un réseau d'accès filaire et Wi-Fi. Les employés utilisent des postes fixes ou portables fournis par l'entreprise, tandis que les formés apportent leur ordinateur personnel lorsqu'ils sont en présentiel. L'accès à Internet s'effectue via un abonnement grand public sur chaque site. Les services de visioconférence, messagerie, outil de gestion des étudiants et des plannings, espace collaboratif, etc..., sont hébergés chez OVH et administrés par le DSI de FORMACTION.

2.2 Schéma d'architecture d'un local type



Dans ce schéma les différents postes employé et formés sont pour montrer les différentes situations de connexion au réseau, filaire ou par point d'accès.

Inventaire des actifs numériques et informatiques

3.1 Matériels (serveurs, postes, équipements réseau)

Catégorie	Equipement	Quantité
Serveur & réseau cœur	Serveur physique	6
	Routeur	6
	Switch principal	6
Réseau Employés	Switch secondaire	6
	Point d'accès Wi-Fi	6
	Postes fixes employés	12
	PC portables employés	12
Réseau Formés	Switch secondaire	6
	Point d'accès Wi-Fi	6
Périphériques externes	Écran, clavier, souris, etc.	24-36 ensembles

Le matériel ci-dessus, est le matériel total de l'entreprise sur site.

3.2 Logiciels et services en ligne

L'entreprise possède un serveur OVH qui gère le serveur de messagerie, l'outil de gestion des étudiants, des plannings, un espace collaboratif.

Analyse des risques

4.1 Identification des risques par actif

Voici les risques identifiés par actif :

- Serveur local : Absence de sauvegarde, panne du matériel, mauvaise configuration.
- Routeur / Box Internet : Accès non sécurisé, absence de pare-feu, configuration par défaut.
- Bornes Wi-Fi : Accès non autorisé, mot de passe peu robuste, possibilité d'un « Man-in-the-middle »
- Ordinateurs employés : Malwares, phishing, mise à jour
- Ordinateurs formés : Virus, intrusion via Wi-Fi
- Serveur OVH : Mauvaise configuration, attaque DDoS, faille d'application web, vol de données
- DSI : Erreur humaine, surcharge de travail, absence de supervision sécurité
- Données locales ou distantes : Absence de plan de sauvegarde 3-2-1, perte de données en cas d'incident

4.2 Synthèse des risques majeurs

Voici les risques majeurs auxquels FORMACTION peut faire face :

- Fuite ou vol de données
- Infection via poste formé
- Attaque sur services OVH
- Absence de plan de sauvegarde
- Manque de gouvernance sécurité

4.3 Matrice de criticité des risques

		Impact				
Probabilité		Très faible	Faible	Moyen	Élevé	Très élevé
	Très élevée	5	10	15	20	25
	Élevée	4	8	12	16	20
	Moyen	3	6	9	12	15
	Faible	2	4	6	8	10
	Très faible	1	2	3	4	5

Risque	Probabilité	Impact	Note
Fuite de données sensibles	Élevée	Élevée	16
Malware via BYOD	Élevée	Moyen	12
Attaque DDoS sur OVH	Moyen	Élevée	12
Absence de sauvegarde fiable	Moyen	Élevée	12
Manque de sensibilisation	Élevée	Moyen	12
Absence de segmentation réseau	Moyen	Élevée	12
DSI seul	Élevée	Élevée	16

Plan d’actions de sécurité

5.1 Mesures correctives prioritaires

Pour corriger la fuite de données sensibles, il faut mettre en place des sauvegardes chiffrées et un contrôle d’accès strict sur les données et l’objectif de cette correction est de garantir la confidentialité et la conformité au RGPD.

Pour la correction des malwares par les BYOD (apprenants), il est nécessaire de créer un réseau Wi-Fi dit « invité » afin d’isoler le réseau principal de l’entreprise et l’objectif et d’évite la propagation d’un quelconque malware sur le réseau LAN des différents sites.

Afin de corriger absence de sauvegarde faible de l’entreprise il faut mettre en place une des règles d’or en cybersécurité, celle de la sauvegarde 3-2-1 (3 sauvegardes, 2 supports différents et 1 sauvegardes hors-ligne. Cela permettra la continuité d’activité.

Pour pallier le fait qu’il n’y a qu’un seul DSI dans l’entreprise, il faut qu’il puisse déléguer des tâches ou contractualiser un prestataire externe, cela réduira les risques humains et la gestion.

Et enfin pour corriger l’absence de pare-feu UTM ou bien un routeur pro avec filtrage intelligent, cela permettra de mieux contrôler le trafic sur le réseau de l’entreprise.

5.2 Mesures préventives et organisationnelles

Pour permettre une meilleure gestion et un meilleur encadrement des incidents de sécurité, il est essentiel de se doter d’une charte informatique claire, permettant d’appeler les règles de sécurité et d’encadrer les usages des équipements à disposition des employés ou des apprenants. Cette charte permettra également d’impliquer les utilisateurs dans la protection de notre système d’information.

Le personnel et les formés doivent être sensibilisés à la sécurité de l’information par le biais d’ateliers ou campagnes régulières de prévention des comportements à risque et dans le cas de phishing, du partage de mots de passe, ou de l’utilisation des supports externes non sécurisés.

La mise en place d’une politique de mots de passe stricte doit aussi être instaurée (complexité minimale, changement régulier et, si possible, ajout d’une authentification multi facteur [MFA] pour les accès aux services critiques [OVH, messagerie, outils internes]).

Il est conseillé de formaliser un plan de sauvegarde et restaurations documenté avec tests mensuels de restauration pour contrôler l’intégrité et la fiabilité des copies des sauvegardes.

5.3 Mesures techniques complémentaires

À moyen terme, FORMACTION pourra renforcer davantage la sécurité de son infrastructure par la mise en place de mesures techniques supplémentaires.

La segmentation du réseau en plusieurs VLAN permettra de séparer les flux employés, formés et serveurs, évitant ainsi qu'une compromission d'un poste n'affecte l'ensemble du système.

La mise à jour automatique des systèmes d'exploitation et des logiciels doit être activée sur tous les postes et serveurs afin de corriger rapidement les vulnérabilités connues.

L'utilisation d'un VPN administrateur pour accéder aux services hébergés chez OVH est également conseillée. Cela garantit la confidentialité des communications entre le DSI et les serveurs distants.

De plus, la mise en place d'un gestionnaire de mots de passe sécurisé (tel que Bitwarden ou KeePass) facilitera la gestion et la protection des identifiants. Combiné à l'authentification multi facteur, cela offre une double barrière de sécurité efficace.

Enfin, l'intégration d'une solution de supervision et de journalisation (comme Wazuh ou Graylog) permettra de détecter rapidement les comportements anormaux, les connexions suspectes ou les tentatives d'intrusion sur le réseau de l'entreprise.

Recommandations générales au DSI

6.1 Bonnes pratiques à mettre en œuvre

Il est recommandé au DSI de FORMACTION de mettre en place une politique globale de sécurité afin d'encadrer les pratiques et de réduire les risques liés à l'utilisation du système d'information.

Cette politique doit inclure la sécurisation des accès distants (via VPN et authentification multi facteur), la gestion rigoureuse des comptes utilisateurs et la mise à jour régulière des systèmes et logiciels utilisés sur l'ensemble des sites.

L'adoption d'un plan de sauvegarde 3-2-1 formalisé et testé régulièrement doit être maintenue dans la durée afin de garantir la continuité d'activité en cas d'incident majeur.

Il est également conseillé au DSI de déléguer certaines de ces tâches ou contractualiser un prestataire externe, cela réduira les risques humains et la gestion.

Enfin, le DSI devrait mettre en place une veille de sécurité active (par exemple via l'ANSSI ou Cybermalveillance.gouv.fr) afin de rester informé des nouvelles menaces et vulnérabilités.

6.2 Sensibilisation et gouvernance

La sensibilisation doit être un point primordial chez FORMACTION, comme dans toutes autres entreprises.

Il est conseillé d'organiser des sessions régulières de formation pour les employés et les apprenants afin de rappeler les réflexes essentiels :

- Vérification des liens et pièces jointes,
- Création de mots de passe robustes,
- Usage responsable d'Internet et des réseaux,
- Signalement rapide de toute anomalie ou suspicion d'attaque.

Le DSI pourra également désigner un référent sécurité dans chaque site pour assurer un relais local et faciliter la communication des bonnes pratiques au quotidien.

Conclusion

7.1 Synthèse globale de l'audit

L'audit réalisé pour le centre de formation FORMACTION a permis de mettre en évidence plusieurs faiblesses dans la gestion de la sécurité du système d'information.

Les principaux constats concernent une absence de gouvernance claire, une protection réseau insuffisante, et une forte dépendance à un seul DSI, ce qui accroît le risque opérationnel en cas d'incident.

Les recommandations proposées dans ce rapport visent à renforcer la sécurité de manière progressive et réaliste, en tenant compte des contraintes budgétaires et humaines du centre.

Les mesures prioritaires (sauvegardes chiffrées, pare-feu avancé, réseau invité pour le BYOD, délégation de certaines tâches, etc.) constituent la première étape essentielle vers une meilleure résilience.

Les actions préventives et techniques complémentaires permettront, quant à elles, de structurer la démarche sécurité dans la durée et d'assurer une protection plus complète des infrastructures et des données.

WLADIMIR BIGAND