Sécurité infrastructure

14.11.2023

Session de formation

Expert : Xavier Barmaz
Mémoire : Zotrim Uka
Présent : David Guillaume, Uka Zotrim, Cardoso Rafael, Laurent Térence, Joiakim Dasek

Table des matières

Introduction

Ce rapport présente un résumé détaillé et les points clés abordés lors de la récente session de formation en cybersécurité. Cette formation a couvert divers sujets essentiels, tels que les techniques utilisées par les hackers, l'accès au dark web, l'utilisation d'outils de sécurité informatique, et l'importance de l'assurance en cybersécurité. Elle a également mis en lumière les réglementations importantes en Europe et en Suisse, notamment le GDPR et la nouvelle loi suisse sur la protection des données, soulignant leur impact sur la gestion et la protection des données personnelles..

En complément à cette introduction, le rapport se penche sur les aspects techniques et stratégiques de la cybersécurité. Il aborde l'infrastructure IT de l'Office de Tourisme de Zermatt, mettant en lumière les vulnérabilités liées au trafic des données, l'utilisation de firewalls, la gestion des serveurs et la sécurisation des données dans le cloud. Des discussions détaillées sur la cryptographie, notamment les fonctions de hachage MD5, SHA-1, SHA-2, SHA-3, et les méthodes d'authentification avancées telles que les passkeys de la Fido Alliance, sont également incluses. De plus, le rapport traite des pratiques de création et de gestion de mots de passe forts, l'utilisation de gestionnaires de mots de passe comme KeePass, et l'importance de la formation des utilisateurs en matière de sécurité des mots de passe.

Il existe deux approches principales pour établir une sécurité informatique :

L'Approche de la Page Blanche : Cette méthode implique de construire un système de sécurité depuis le début, sans se baser sur des modèles ou des structures préétablis. Elle offre une flexibilité maximale et permet une personnalisation complète en fonction des besoins spécifiques de l'organisation.

La Méthode 'Recette de Cuisine' : Cette approche suit un ensemble de procédures et de normes éprouvées, similaires à suivre une recette de cuisine. Elle est caractérisée par l'utilisation de lignes directrices et de meilleures pratiques standardisées dans le domaine de la cybersécurité, ce qui peut faciliter la mise en place et garantir une certaine cohérence dans la sécurité.

ISO 27000

L'Organisation Internationale de Normalisation (ISO), basée à Genève, joue un rôle clé dans la définition des standards de cybersécurité à l'échelle mondiale. La norme ISO 27000, élaborée par des experts et des spécialistes en cybersécurité, est une référence incontournable dans ce domaine.

La série ISO 27000 se compose de plusieurs standards, chacun ayant une portée et une application spécifiques. Parmi ceux-ci, ISO 27001 est essentiel car il établit des exigences obligatoires ('shall'), dictant ce que les organisations doivent faire pour assurer une gestion sécurisée de l'information. Cette norme comprend 94 exigences distinctes et c'est la seule norme de la série sur laquelle une organisation peut être certifiée. Pour obtenir cette certification, une organisation doit remplir un document détaillant les exigences spécifiques qui lui sont applicables.

D'autre part, d'autres standards comme ISO 27002, 27003, 27004, etc., proposent des recommandations ('should'), offrant des conseils sur les meilleures pratiques à adopter. ISO 27002, par exemple, fournit des lignes directrices sur la manière de mettre en œuvre les exigences mentionnées dans ISO 27001.

ISO 27005 se concentre sur l'analyse de risque, un aspect crucial de la gestion de la sécurité de l'information. Cette norme guide les organisations à travers un processus structuré comprenant plusieurs étapes clés :

- **Identifier** les actifs, les menaces et les vulnérabilités.
- **Évaluer** les risques en analysant la probabilité et l'impact des différentes menaces.
- **Prioriser** les risques en fonction de leur gravité et de leur potentiel de dommage.
- **Formuler** des stratégies pour gérer ou atténuer ces risques.
- **Finaliser** le plan de gestion des risques en le documentant et en le mettant en œuvre efficacement.

Ces standards, en s'appuyant les uns sur les autres, forment un cadre cohérent et intégré pour la sécurité de l'information, adaptable aux besoins variés des organisations

MSSI (Management System Security)

Le MSSI est un document crucial dans le domaine de la sécurité des systèmes de gestion, mis à jour tous les dix ans. La dernière mise à jour significative a eu lieu en septembre 2002. Bien qu'il représente un excellent point de départ pour la mise en place de la sécurité, il reste un document complexe et payant. En Suisse, de nombreuses entreprises trouvent difficile de se conformer à ces normes en raison de contraintes financières et de complexité.

Cyber Safe

En réponse à ces défis, l'association "Cyber Safe" a été fondée en 2020 avec le soutien de la Confédération. Son site web, Cyber Safe, offre des ressources et des conseils pour renforcer la sécurité informatique. Bien qu'il soit impossible de contrer les hackers les plus avancés, Cyber Safe vise à protéger efficacement les entreprises contre la majorité des cyberattaques.

Politique, Lois, Conformité et Réglementation

En Europe, le Règlement Général sur la Protection des Données (GDPR) est une loi importante concernant la protection des données personnelles des individus. Cette réglementation a un impact significatif sur la manière dont les données personnelles sont gérées par les entreprises et les organisations.

En Suisse, une nouvelle loi sur la protection des données a été mise en place le 1er septembre 2023. Cette législation vise à protéger les droits des citoyens en matière de confidentialité et de sécurité des données personnelles. Elle impose aux entreprises et aux organisations des obligations strictes en termes de traitement et de protection des données personnelles.

ICT Norme (Confédération)

La Confédération a également mis en place la norme ICT, qui comprend 108 contrôles pour assurer une sécurité adéquate des infrastructures critiques telles que les hôpitaux, les transports publics, l'électricité et les assurances maladie. Inspirée du document "NIST Cybersecurity" des États-Unis, cette norme a été adaptée au contexte suisse.

Elle se décline en cinq phases principales :

- **Identifier :** Créer un inventaire complet des actifs de l'entreprise.
- **Protection :** Mettre en place des mesures de protection adéquates.
- **Détection :** Être capable de détecter rapidement les incidents de sécurité.
- **Réaction :** Réagir efficacement en cas d'incident.
- **Récupération :** Restaurer les opérations normales après un incident.

Les entreprises doivent remplir un questionnaire et atteindre une note minimale de 2.6 sur 4 pour être considérées comme conformes.

Choix des Normes en Fonction de la Taille de l'Entreprise

Selon la taille et les besoins de l'entreprise, différentes normes sont recommandées. Pour les petites entreprises (0-50 employés), Cyber Safe est la solution privilégiée. Pour les entreprises plus grandes, la conformité aux normes ISO 27000 est conseillée.

Assurance en Cybersécurité

L'assurance en cybersécurité est généralement un processus complexe qui nécessite une attention particulière, en particulier concernant les Conditions Générales d'Assurance (CGA). Il est crucial pour les entreprises de comprendre les défis et les coûts associés à l'obtention d'une couverture d'assurance adéquate en matière de cybersécurité. Cette couverture vise à protéger contre les risques liés aux incidents de cybersécurité, incluant les atteintes à la sécurité des données et les intrusions dans les systèmes informatiques. Bien que complexe, une assurance appropriée peut jouer un rôle vital dans la mitigation des pertes financières et opérationnelles consécutives à de tels incidents.

Hacking

En Suisse, l'accès non autorisé à un système informatique, communément appelé "hacking", est effectivement illégal. Selon la législation suisse, entrer dans un système informatique sans l'autorisation du propriétaire constitue une violation de la loi. Cette interdiction est en place pour protéger l'intégrité, la confidentialité et la disponibilité des données et des systèmes informatiques contre les accès et utilisations non autorisés. Les sanctions pour de tels actes peuvent inclure des amendes et, dans les cas plus graves, des peines d'emprisonnement.

Sécurité et sûreté

- La **sécurité** se réfère à tout ce qui peut être contrôlé et sur lequel nous avons la possibilité d'agir. Pour simplifier, nous utilisons le terme de sécurité pour désigner tout ce qui peut avoir des conséquences, positives ou négatives, sur la confidentialité, la disponibilité ou l'intégrité des informations. L'objectif principal en matière de sécurité est de préserver ces trois propriétés.

- La **sûreté** englobe les éléments qui sont hors de notre contrôle

Confidentialité, Intégrité, et Disponibilité :

À chaque mise en œuvre de mesures de sécurité, il est impératif de garantir trois aspects fondamentaux : la confidentialité, l'intégrité et la disponibilité des informations :
- Confidentialité
- Intégrité
- Disponiblité

- Disponibilité : garantit la fiabilité et l'accès en temps opportun aux données et ressources pour les personnes autorisées.
- Intégrité : est préservée lorsque l'exactitude et la fiabilité des informations et des systèmes sont garanties, empêchant toute modification non autorisée.
- Confidentialité : assure que les données sont gardées secrètes et protégées contre toute divulgation non autorisée à chaque étape du traitement.

Vulnérabilité, Menace, et Risque :

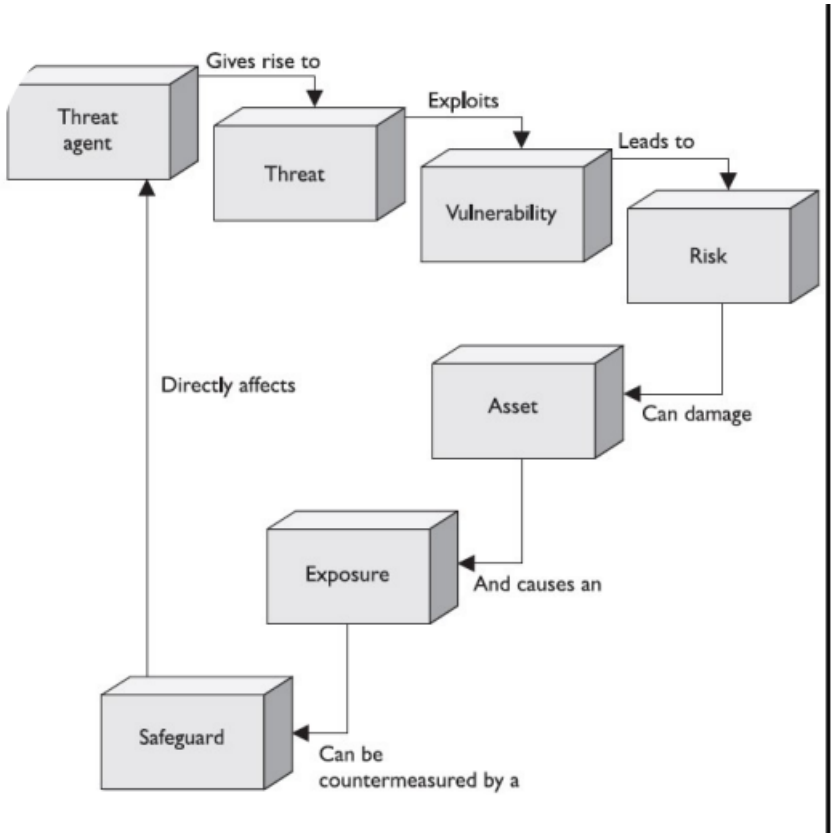
- Une **vulnérabilité** est une faiblesse, soit due à l'absence de contre-mesure, soit en raison d'une faiblesse dans une contre-mesure existante.

- Une **menace** représente tout danger potentiel pour les informations ou les systèmes qui exploite une vulnérabilité.
- Le **risque** est la probabilité qu'un agent menaçant (une entité exploitant une vulnérabilité) tire avantage de cette vulnérabilité et les conséquences qui en découlent.

Analyse de Risque :

- L'analyse de risque est un processus obligatoire, soulignant que le risque zéro n'est pas une réalité.

Relationship btw security components



Les techniques des hackers

1. **Première Possibilité (Exploitation de Code) :**
   a. **Vulnérabilité dans le Code :** Identification des failles dans le code.
   b. **Exploitation du Code :** Utilisation des vulnérabilités identifiées.
   c. **Payload/Opcode :** Exécution de code malveillant.

2. **Deuxième Possibilité (Ingénierie Sociale) :**
   a. **Ingénierie Sociale :** Manipulation des utilisateurs pour obtenir un accès non autorisé.
   b. **Exploitation :** Utilisation des informations obtenues via l'ingénierie sociale.
   c. **Payload :** Déploiement de logiciels malveillants.

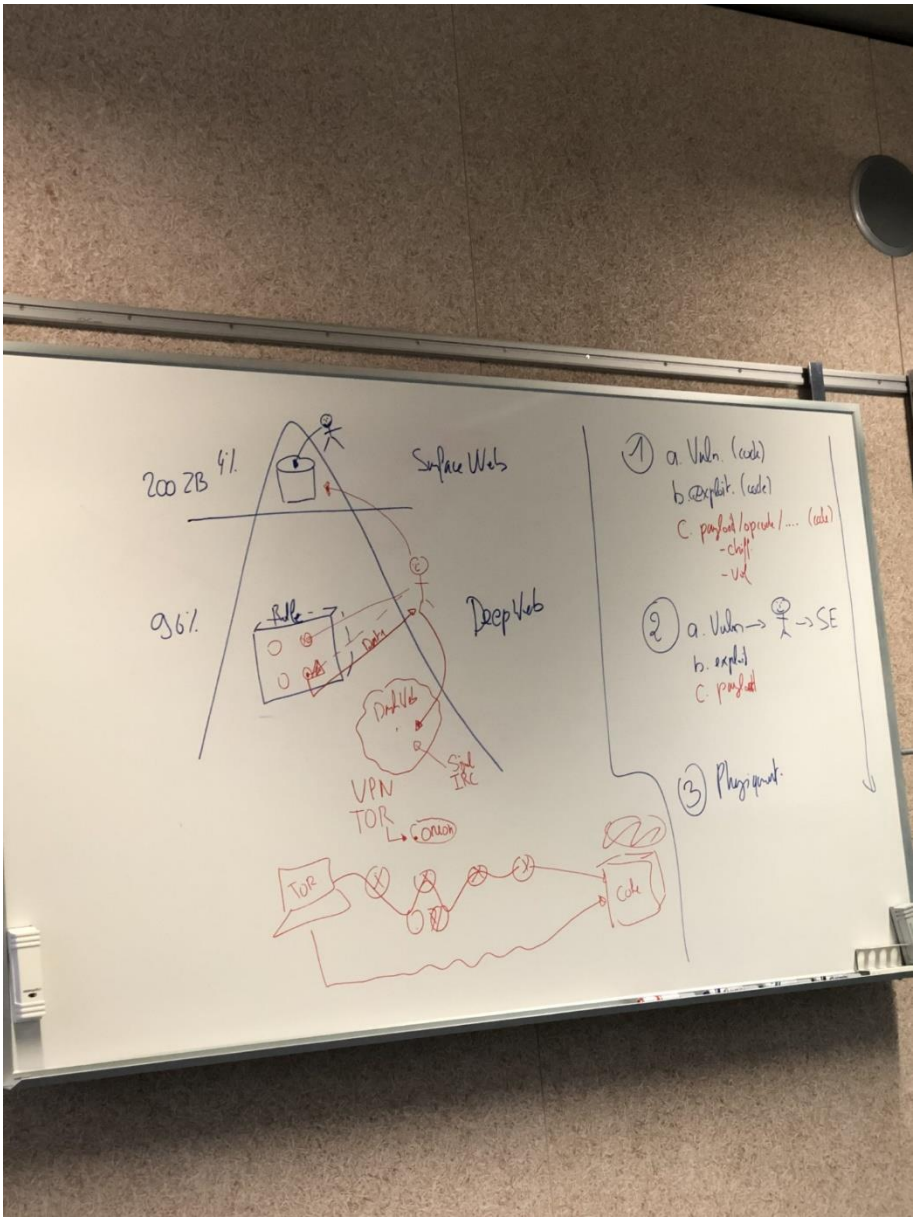
3. **Troisième Possibilité (Accès Physique) :**
   a. **Accès Physique à l'Environnement :** Obtention d'un accès direct aux systèmes ou au matériel.

Chaque technique représente une méthode distincte que les hackers peuvent utiliser pour compromettre la sécurité des systèmes informatiques.

Cybercrimintality Numbers

Répartition des Données sur Internet

Seulement 4% des données globales, soit environ 200 ZB, sont accessibles sur le surface web. La majorité des données, environ 96%, se trouve dans le deep web, y compris le dark web, et consiste en des informations non publiques.



Accès au Dark Web

Pour accéder au dark web, l'utilisation d'un VPN(Proton VPN) et du réseau TOR est indispensable. Ce dernier permet d'accéder à des sites en .onion. Les utilisateurs communiquent souvent via des plateformes sécurisées comme Signal et IRC.

Délai de Détection et Correction des Vulnérabilités

La détection d'une vulnérabilité prend en moyenne sept mois. Après cette détection, la correction de la vulnérabilité nécessite environ quatre mois supplémentaires, période incluant les tests nécessaires.

Outils de Sécurité Informatique

1. **CVEdetails :** Un outil d'agrégation des informations sur les vulnérabilités. Il fournit une base de données de vulnérabilités de sécurité CVE, accessible à www.cvedetails.com.

2. **SOC (Security Operation Center) :** Un centre opérationnel qui analyse les logs. Le SOC est une fonction essentielle au sein des organisations pour surveiller et analyser la sécurité de leur réseau.

3. **SIEM (Système de Gestion des Informations et des Événements de Sécurité) :** Un système qui effectue une analyse automatique des logs, lesquels sont ensuite remontés au SOC. Le SIEM est une catégorie de solutions logicielles proposées par de nombreux fournisseurs pour améliorer la surveillance de la sécurité informatique.

Breaches et Failles dans le Modèle OSI

Les failles de sécurité peuvent affecter tous les niveaux du modèle OSI (Open Systems Interconnection), un cadre conceptuel utilisé pour comprendre et concevoir des réseaux informatiques et leurs interactions. Ces failles, pouvant survenir à n'importe quel niveau de ce modèle, menacent l'intégrité, la confidentialité et la disponibilité des données et des systèmes.

Impact des Failles sur l'Image

En matière de failles de sécurité, le dégât d'image pour une entreprise ou une organisation est souvent considéré comme moins important que les impacts financiers ou opérationnels. Toutefois, il est important de noter que l'impact sur la réputation peut avoir des conséquences à long terme sur la confiance des clients et des partenaires.

MELANI - National Cyber Security Center

En Suisse, le MELANI, ou National Cyber Security Center, joue un rôle essentiel dans la gestion des questions de cybersécurité au niveau national. Pour plus d'informations sur le NCSC, vous pouvez consulter leur site officiel à www.ncsc.admin.ch.

Ces informations fournissent une vue d'ensemble des aspects de l'assurance en cybersécurité et du rôle du NCSC en Suisse.

Partie 2

Office de tourisme Zermatt

L'Office de Tourisme Zermatt dispose de bureaux internes équipés d'un serveur contenant des données comptables, de ressources humaines, et d'autres informations essentielles. Ce système inclut également un routeur, une connexion WiFi, ainsi que deux serveurs publics. Le premier est un serveur Web dédié aux réservations, tandis que le second est un serveur Extranet, qui est interconnecté avec le premier pour le traitement des données.

Dans le domaine du Cloud et des applications, l'Office utilise une zone Cloud spécifique, ainsi que plusieurs outils tels qu'un système de gestion de la relation client (CRM), Abacus pour la gestion, CardSystem pour la gestion des cartes, et un service de messagerie.
Qu'est-ce qui ne va pas dans son système ?

Cependant, le système actuel présente plusieurs failles de sécurité. Notamment, les données transitent en clair, exposant le trafic des touristes à des risques. Cette situation signifie que les informations sensibles, telles que les détails personnels et financiers des clients, peuvent être interceptées et compromises par des tiers non autorisés. De plus, l'absence de sauvegardes adéquates pose un risque majeur. Sans des copies de sécurité fiables, toute perte de données due à des défaillances du système, des erreurs humaines ou des cyberattaques pourrait avoir des conséquences désastreuses, entravant potentiellement les opérations de l'Office de Tourisme et endommageant sa réputation.

L'utilisation d'une seule adresse IP pour tous les services est une autre préoccupation. Cette configuration peut rendre le réseau plus vulnérable aux attaques, car une fois que l'adresse IP est compromise, l'ensemble du réseau peut être exposé à des risques. En outre, cela peut entraîner des problèmes de performance et de fiabilité, car tous les services dépendent d'un seule point de connectivité.

Le pare-feu actuel est également insuffisant. Un pare-feu robuste est essentiel pour protéger le réseau contre les accès non autorisés et les menaces externes. Le manque d'un système de pare-feu efficace laisse le réseau ouvert à divers types d'attaques cybernétiques. De plus, avec deux serveurs internes gérant des données critiques, il est essentiel d'avoir un pare-feu capable de gérer et de sécuriser le trafic entre ces serveurs et le réseau externe.

Protocoles

L'identification des ports standards pour différents protocoles de communication est un élément crucial de la gestion de la sécurité réseau. Voici une brève explication de chacun des protocoles et ports que vous avez mentionnés :

1. **HTTP (Port 80) :**
    - **HTTP (Hypertext Transfer Protocol)** est le protocole de base utilisé pour la communication sur le World Wide Web.
    - Le port 80 est le port standard pour le trafic HTTP.
    - Ce protocole est moins sécurisé car il transmet les données en clair, ce qui signifie que les données peuvent être interceptées et lues facilement.
2. **HTTPS (Port 443) :**
    - **HTTPS (HTTP Secure)** est une version sécurisée d'HTTP.

    - Il utilise le port 443 et chiffre la communication entre le navigateur de l'utilisateur et le site web, offrant ainsi une couche de sécurité supplémentaire.
    - HTTPS est essentiel pour protéger les transactions en ligne et les données sensibles.
3. **FTP (Port 21) :**
    - **FTP (File Transfer Protocol)** est utilisé pour le transfert de fichiers entre un client et un serveur sur un réseau informatique.
    - Le port 21 est utilisé pour les commandes et les contrôles FTP.
    - Cependant, comme HTTP, FTP n'est pas sécurisé en soi et peut exposer les données à des risques lors du transfert.
4. **FTPS (Port 990) :**
    - **FTPS (FTP Secure)** est une extension de FTP qui ajoute des couches de sécurité.
    - Le port 990 est utilisé pour le FTPS explicite, où les données sont chiffrées via SSL/TLS.
    - FTPS assure une meilleure protection des données pendant le transfert par rapport au FTP standard.

L'utilisation appropriée de ces protocoles et la configuration correcte des ports sont essentielles pour maintenir la sécurité du réseau de l'Office de Tourisme de Zermatt. Il est particulièrement important de s'assurer que les données sensibles, telles que les informations personnelles des clients et les transactions financières, sont transmises via des protocoles sécurisés comme HTTPS et FTPS, plutôt que leurs homologues non sécurisés HTTP et FTP.

Certificat

Certificats : Les certificats sont au cœur de la sécurisation des communications entre les clients (navigateurs web) et les serveurs. Lorsqu'un utilisateur accède à un site sécurisé de l'Office de Tourisme, son navigateur reçoit un certificat du serveur. Ce certificat contient la clé publique du serveur et est essentiel pour établir une connexion sécurisée. Il existe des options de certificats gratuits et payants, ces derniers offrant souvent des niveaux de garantie et de sécurité supplémentaires.

Clé Privée et Clé Publique (RSA) :

- **RSA** est un algorithme de cryptographie asymétrique introduit en 1973.
- Chaque entité dispose de deux clés :
    - Une **clé publique**, accessible à tous.
    - Une **clé privée**, maintenue secrète.
- Le système garantit la confidentialité et l'authenticité des données : ce qui est chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante, et inversement.

Performance des Clés Publiques : Le chiffrement avec des clés publiques, surtout de grande taille (comme 2048 bits), peut être lent en raison de la complexité mathématique du processus de chiffrement et de déchiffrement.

Cryptographie Symétrique vs Asymétrique :

- **Cryptographie symétrique** : Utilise une seule clé pour le chiffrement et le déchiffrement. Plus rapide, mais nécessite une gestion sécurisée de la clé.
- **Cryptographie asymétrique** : Utilise une paire de clés pour une sécurité accrue, mais avec une vitesse réduite.

TLS (Transport Layer Security) : TLS est un protocole essentiel pour sécuriser les communications sur un réseau informatique. Il combine la cryptographie symétrique et asymétrique pour une sécurité optimale. Initialement, une clé publique est utilisée pour établir une connexion sécurisée et négocier une clé symétrique, qui sera ensuite employée pour le reste de la communication.

Firewall

Types de Firewall :

- **Firewall Logiciel :** S'installe et fonctionne sur des serveurs ou d'autres dispositifs informatiques. Il offre une grande flexibilité et est facilement mis à jour.
- **Firewall Matériel :** Il s'agit d'un dispositif physique distinct, spécialement conçu pour gérer et filtrer le trafic réseau.

Configuration du Firewall :

- **Multiples Interfaces :**
  - **Physiques ou Logiques :** Le firewall peut être configuré avec des interfaces matérielles (réelles) ou logiques (virtuelles), offrant une segmentation détaillée et un contrôle du trafic réseau.
- **Règles de Sécurité :**
  - Définition de règles spécifiant qui peut accéder à quoi, et dans quel sens le trafic peut s'écouler.

Opération du Firewall :

- Les firewalls opèrent principalement aux **couches 2 à 4 du modèle OSI** (Liaison, Réseau, Transport).
- Pour les **couches 5 à 7** (Session, Présentation, Application), des licences supplémentaires peuvent être requises pour un filtrage plus avancé.

Utilisation de Deux Firewalls :

- Employant **deux technologies différentes**, cette approche (FW-DMZ-FW) crée une zone tampon (DMZ) qui offre une sécurité accrue. La DMZ isole les serveurs publics, tels que le serveur Web, du reste du réseau interne.

VPN et Firewall :

- **Intégration VPN :** Les VPNs sont souvent gérés via les firewalls pour créer des connexions sécurisées, simulant la présence physique au sein de l'entreprise.
- **Split Tunneling :** Une fonctionnalité clé qui permet de déterminer quel trafic passe par le VPN et quel trafic accède directement à Internet, optimisant ainsi la performance du réseau et l'utilisation de la bande passante.

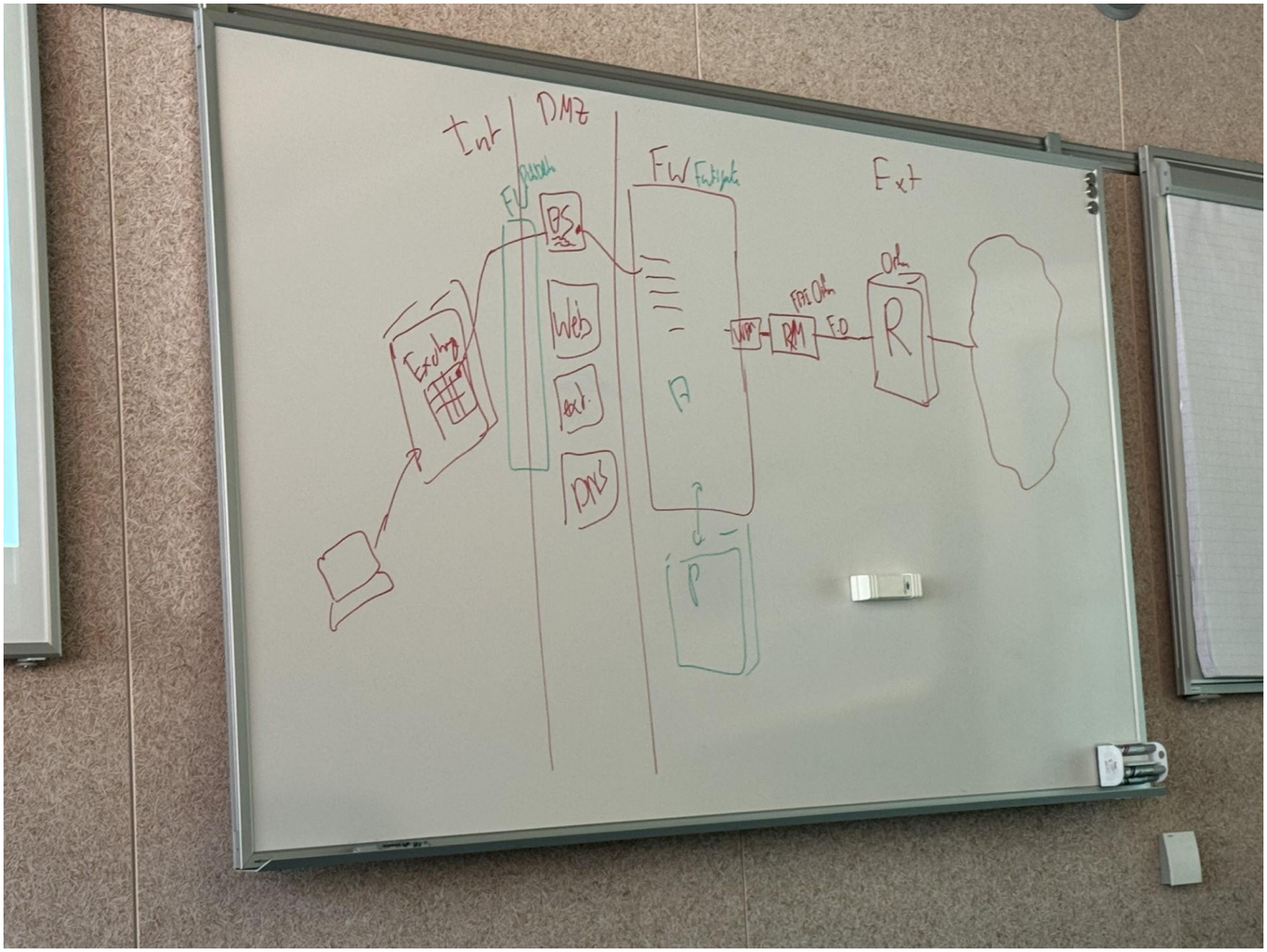
  En conclusion, l'implémentation et la gestion appropriées des firewalls sont cruciales pour assurer la sécurité du réseau de l'Office de Tourisme de Zermatt. Un système bien configuré non seulement protège contre les attaques externes mais assure également un contrôle adéquat du trafic interne, en tenant compte des besoins spécifiques en matière de sécurité et d'efficacité opérationnelle.

DMZ :

DMZ (Zone Démilitarisée) :

La DMZ est une partie cruciale de l'architecture réseau, agissant comme une zone tampon entre le réseau interne sécurisé d'une organisation et le réseau externe, généralement Internet.

- **Fonction de la DMZ :**
    - Elle est utilisée pour héberger des services qui doivent être accessibles depuis l'extérieur, comme le serveur Web et le serveur Extranet de l'Office de Tourisme de Zermatt.
    - En plaçant ces serveurs dans la DMZ, ils sont isolés du reste du réseau interne, ce qui réduit le risque qu'une compromission de ces serveurs entraîne un accès non autorisé au réseau interne complet.



Norme RFC pour HTTP :

La norme RFC définit les standards pour les protocoles Internet, y compris HTTP (Hypertext Transfer Protocol).

- **Rôle de la Norme RFC :**
    - Elle assure que le protocole HTTP est utilisé de manière cohérente et sûre sur Internet, facilitant ainsi la communication et le transfert de données sur le Web.

Principe de Backups (3-2-1) :

Ce principe est une stratégie reconnue pour la sauvegarde des données, visant à maximiser la fiabilité et la disponibilité des données.

- **Règles du Principe 3-2-1 :**
    - **3 Copies :** Deux sauvegardes et une en production.
    - **2 Sites Différents :** Les sauvegardes doivent être stockées sur deux sites géographiquement distincts pour se protéger contre les catastrophes naturelles ou d'autres incidents majeurs.

- **1 Offline/Off-Site :** Au moins une copie de sauvegarde doit être déconnectée de tout réseau (offline) et stockée hors-site pour une protection contre les cyberattaques, comme les ransomwares.
- **WORM ou Immutabilité :** Les sauvegardes doivent être protégées contre les modifications après écriture (Write Once, Read Many) pour prévenir toute altération malveillante.

Gestion des Adresses IP et Protection des Endpoints

La gestion efficace des adresses IP et la protection des points de terminaison sont essentielles pour la sécurité globale du réseau.

- **Utilisation des WLAN :**
  - Il est conseillé de diversifier les adresses IP au lieu d'utiliser la même pour différents services. L'utilisation de réseaux locaux sans fil (WLAN) distincts peut aider à segmenter le réseau et à réduire les risques.
- **Protection des Endpoints :**
  - Les points de terminaison, tels que les ordinateurs et les appareils mobiles des employés, doivent être sécurisés avec des logiciels antivirus, des firewalls, et d'autres mesures de sécurité pour empêcher l'accès non autorisé au réseau.

Stratégie de la Zone Cloud

Lorsqu'une organisation envisage de déplacer des données ou des services dans le cloud, plusieurs considérations importantes doivent être prises en compte.

1. **Détermination de ce qui est déplacé dans le cloud :**
   - L'Office doit identifier quels éléments (données, applications, services) peuvent bénéficier d'un déplacement vers le cloud. Cela peut inclure des applications moins critiques, des données moins sensibles, ou des services nécessitant une élasticité et une évolutivité importantes.
2. **Évaluation de la perte de contrôle :**
   - L'une des principales préoccupations lors du déplacement des ressources vers le cloud est la perte de contrôle sur ces ressources.
   - L'Office doit être prêt à accepter que, une fois dans le cloud, ils auront moins de contrôle direct sur la gestion et la sécurité des données et des services.
   - Cette perte de contrôle doit être équilibrée par les avantages du cloud, tels que la réduction des coûts, l'augmentation de l'efficacité, et l'amélioration de l'accessibilité.
3. **Sécurité et Conformité dans le Cloud :**
   - L'Office doit s'assurer que leurs fournisseurs de cloud respectent les normes de sécurité et de conformité nécessaires.
   - Des mesures de sécurité supplémentaires peuvent être nécessaires pour protéger les données sensibles et assurer la conformité avec les réglementations en vigueur.
4. **Tout ce qui est déplacé dans le Cloud :**
   - Tout ce qui est transféré dans le cloud doit être soigneusement considéré et géré.
   - Cela inclut non seulement les données et les applications, mais aussi les processus opérationnels et les politiques de sécurité qui doivent être adaptés pour l'environnement cloud.

En conclusion, la décision de l'Office de Tourisme de Zermatt d'utiliser une zone cloud doit être guidée par une compréhension claire des avantages et des inconvénients du cloud computing. Bien que le cloud puisse offrir de nombreux avantages en termes de flexibilité et d'efficacité, il est essentiel de gérer soigneusement

la sécurité des données, la conformité réglementaire, et d'accepter un certain niveau de perte de contrôle sur les ressources informatiques externalisées.

Magic quadrant gartner

Le "Magic Quadrant" de Gartner, un outil d'analyse et de visualisation très répandu utilisé pour évaluer la position de diverses entreprises dans un certain secteur technologique. Le Magic Quadrant classe les entreprises sur deux axes : leur capacité à exécuter et leur vision complète. Voici une explication de chaque quadrant :

1. **En Bas à Gauche - Les Nouveaux Arrivants (Niche Players) :**
    - Ces entreprises sont souvent spécialisées dans un segment particulier ou une niche de marché.
    - Elles peuvent offrir des solutions innovantes mais manquent parfois de la portée ou de la capacité d'exécution des leaders établis.

2. **En Bas à Droite - Les Visionnaires (Visionaries) :**
    - Ces entreprises ont une vision forte et innovante de leur marché.
    - Elles sont souvent à la pointe des nouvelles tendances technologiques, mais peuvent ne pas avoir encore prouvé leur capacité à exécuter pleinement leur vision.

3. **En Haut à Droite - Les Leaders :**
    - Ces entreprises sont considérées comme dominantes dans leur secteur.
    - Elles combinent une capacité d'exécution éprouvée avec une vision complète et sont souvent des références dans leur domaine.

4. **En Haut à Gauche - Les Challengers (Challengers) :**
    - Ces entreprises possèdent une forte capacité d'exécution mais peuvent ne pas avoir une vision aussi complète que les leaders.

- Elles sont souvent des acteurs établis avec des produits et services solides, mais peuvent être moins innovantes.

Pour l'Office de Tourisme de Zermatt, la compréhension du Magic Quadrant de Gartner peut être utile pour évaluer les fournisseurs de technologie et choisir ceux qui correspondent le mieux à leurs besoins spécifiques. En examinant où un fournisseur se situe dans le quadrant, ils peuvent obtenir des informations sur la solidité, la stabilité, et l'innovation potentielle de ce fournisseur, ce qui est crucial lors de la prise de décisions stratégiques concernant les partenariats technologiques.

Gestion des mots de passe

Les fonctions de hachage cryptographiques telles que MD5, SHA-1, SHA-2 et SHA-3 jouent un rôle crucial dans la sécurité informatique, notamment en ce qui concerne la gestion des mots de passe et la protection des données. Chacune de ces fonctions présente des caractéristiques et des niveaux de sécurité différents, ce qui est essentiel à comprendre pour l'Office de Tourisme de Zermatt.

1. **MD5 et Fonctions de Hachage :**
   - MD5 est une fonction de hachage unidirectionnelle qui convertit les mots de passe en une empreinte fixe, rendant difficile leur rétro-ingénierie. Toutefois, MD5 n'est plus considéré comme sécurisé pour les mots de passe en raison de vulnérabilités connues.
2. **SHA-1 (Secure Hash Algorithm 1) :**
   - SHA-1 génère un hachage de 160 bits, offrant théoriquement plus de sécurité que MD5. Cependant, SHA-1 est aussi vulnérable aux attaques de collision et n'est plus recommandé pour des applications de sécurité critiques.
3. **SHA-2 :**
   - SHA-2 comprend plusieurs variantes (SHA-224, SHA-256, SHA-384, SHA-512), les chiffres indiquant la longueur du hachage en bits. SHA-2 est plus robuste que SHA-1 et MD5, et est actuellement recommandé pour les applications de sécurité.

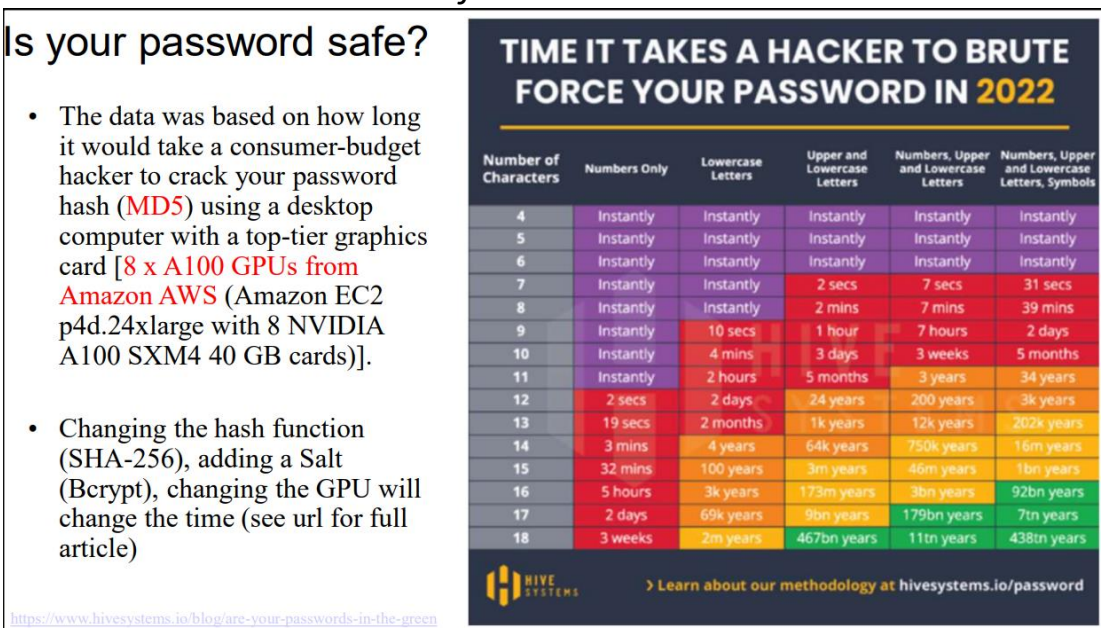
4. **SHA-3 :**
    - SHA-3 est une famille d'algorithmes distincte et complémentaire à SHA-2, utilisant une structure de conception différente (Keccak). Elle offre une alternative sécurisée si des vulnérabilités sont découvertes dans SHA-2.

Différences Clés avec MD5 :

- **Sécurité :** SHA-1, SHA-2 et SHA-3 offrent une sécurité supérieure à MD5, avec SHA-2 et SHA-3 considérés comme sécurisés pour les applications modernes.
- **Longueur de Hachage :** SHA-1/2/3 produisent des hachages plus longs que MD5, augmentant la résistance aux collisions.
- **Utilisation Recommandée :** MD5 et SHA-1 sont déconseillés pour la plupart des usages de sécurité, tandis que SHA-2 et SHA-3 sont recommandés pour garantir l'intégrité des données et la sécurité des systèmes.

Il est crucial pour l'Office de Tourisme de Zermatt d'utiliser SHA-2 ou SHA-3 pour les applications nécessitant des fonctions de hachage afin de garantir une sécurité optimale. La transition vers ces algorithmes plus robustes est essentielle pour protéger les informations sensibles des clients et maintenir l'intégrité de leurs systèmes informatiques.

Gestion des Mots de Passe et Authentification :



Is your password safe?

- The data was based on how long it would take a consumer-budget hacker to crack your password hash (MD5) using a desktop computer with a top-tier graphics card [8 x A100 GPUs from Amazon AWS (Amazon EC2 p4d.24xlarge with 8 NVIDIA A100 SXM4 40 GB cards)].
- Changing the hash function (SHA-256), adding a Salt (Bcrypt), changing the GPU will change the time (see url for full article)

https://www.hivesystems.io/blog/are-your-passwords-in-the-green

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS › Learn about our methodology at hivesystems.io/password

- **Création de Mots de Passe Forts :** Un mot de passe fort doit comporter au moins 16 caractères, incluant un mélange de lettres majuscules et minuscules, de chiffres et de symboles, pour équilibrer confort et sécurité.

- **Gestionnaires de Mots de Passe :** Des outils comme KeePass aident à stocker et gérer de manière sécurisée des mots de passe complexes, permettant de créer et de conserver des mots de passe uniques pour chaque compte.

- **Formation des Utilisateurs :** Éduquer les utilisateurs sur la création et la gestion de mots de passe forts est essentiel pour renforcer la sécurité globale.

- **Méthode de Création de Mots de Passe :** Choisir une phrase et utiliser certaines de ses lettres, en variant pour différents comptes, peut-être une technique efficace.

- **Fido Alliance et Passkeys :** La Fido Alliance, composée de membres tels que Microsoft, Google, Apple, Amazon, Facebook, Mastercard, American Express, VISA, PayPal et OneSpan, se consacre à la promotion de méthodes d'authentification plus sûres. Elle met en avant les "passkeys", une technologie basée sur des paires de clés privées et publiques, offrant une meilleure sécurité que les mots de passe traditionnels. Cette approche d'authentification renforcée est soutenue par l'expertise et l'engagement de ces grandes entreprises technologiques et financières.

Exemple d'Authentification par Clé Privée et Publique :

Lors de la création d'un compte sur un site, au lieu d'entrer un mot de passe, l'ordinateur génère une paire de clés privée et publique. La clé publique est envoyée au serveur, associant l'utilisateur à cette clé. L'authentification est prouvée avec la clé privée, possédée uniquement par l'utilisateur. Ce système améliore la sécurité mais soulève des questions sur la gestion et le stockage sécurisés de ces clés.
En résumé, bien que les mots de passe traditionnels soient toujours largement utilisés, les avancées technologiques et les préoccupations en matière de sécurité encouragent l'adoption de méthodes d'authentification plus sophistiquées comme les passkeys de la Fido Alliance. La formation des utilisateurs et l'utilisation de gestionnaires de mots de passe restent des pratiques essentielles pour maintenir la sécurité des comptes en ligne.