Institutions spécialisées du Canton de Fribourg
Guide de bonnes pratiques de cybersécurité

Version date
30/01/2025

Contact details:
immunIT sàrl
44-46 Chemin des Plantaz
1260 Nyon - Switzerland

Contact person:
Alain Sullam
asullam@immunit.ch
+41 76 488 00 28

Table des matières

Introduction 6

Objectifs du guide 6

Contexte des institutions spécialisées dans le canton de Fribourg 6

Enjeux de la cybersécurité dans ces institutions 7

Évaluation de la maturité et priorisation des recommandations 8

Définition des niveaux de maturité 8

Stratégie de mise en œuvre 9

Inventaire des systèmes et des services 10

Cartographie des systèmes informatiques internes et externes 10

Classification des données et des systèmes 10

Identification des prestataires externes (hébergement, cloud, services) 11

Interconnexions et dépendances entre services 11

Mise à jour et maintien de l'inventaire 12

Sécurité du réseau et segmentation 13

Introduction 13

Principes de la segmentation du réseau 13

Bonnes pratiques pour la segmentation et la ségrégation des réseaux internes 13

Surveillance et maintenance des dispositifs de sécurité périmétrique 15

Conclusion 15

Configuration et gestion des firewalls 16

Comprendre le rôle des firewalls dans la protection du périmètre 16

Politiques de filtrage du trafic entrant et sortant 16

Bonnes pratiques pour la gestion des règles de firewall 16

Surveillance et maintenance des dispositifs de sécurité périmétrique 17

Configuration avancée des firewalls 17

Réponse aux incidents et récupération 18

Conclusion et recommandations 18

Sauvegardes et restauration des données 19

Stratégies de sauvegarde 19

Choix de l'emplacement des sauvegardes 19

Fréquence et planification des sauvegardes 20
Tests de restauration : bonne pratique et fréquence 20
Recommandations supplémentaires 20
Sécurisation des services exposés sur Internet 22
Identification des services exposés 22
Réduction de la surface d'attaque 22
Sécurisation des services de communication (SSL/TLS) 23
Contrôles d'authentification et d'autorisation 23
Test de vulnérabilités et gestion des correctifs 23
Durcissement des configurations 24
Surveillance et détection d'intrusions 24
Conclusion 24
Gestion des vulnérabilités et des mises à jour 25
Processus de gestion des vulnérabilités 25
Politique de mise à jour des logiciels et systèmes 25
Automatisation des mises à jour et surveillance continue 26
Bonnes pratiques pour la gestion des vulnérabilités et des mises à jour 26
Protection des postes de travail et serveurs 28
Solutions antivirales et EDR (Endpoint Detection and Response) 28
Configuration des politiques de sécurité pour les endpoints 29
Bonnes pratiques pour la gestion des privilèges locaux 29
Renforcement de la sécurité des sessions utilisateur 30
Gestion des accès à privilèges 31
Introduction à la gestion des comptes à privilèges 31
Principes de sécurité pour les comptes à hauts privilèges 31
Identification et classification des comptes privilégiés 31
Mise en œuvre d'une solution PAM (Privileged Access Management) 32
Surveillance et audit des actions des utilisateurs privilégiés 32
Politique de révision des comptes privilégiés 32
Sécurité des comptes de service et des comptes applicatifs 32
Éducation et sensibilisation des utilisateurs privilégiés 33
Surveillance et monitoring de l'infrastructure 34

Introduction à la surveillance de l'infrastructure 34
Objectifs de la surveillance 34
Types de surveillance 34
Outils de surveillance 35
Principales étapes pour la mise en place d'une surveillance efficace 35
Réponse aux incidents détectés par le monitoring 36
Bonnes pratiques de surveillance 36
Conclusion 36
Formation et sensibilisation des utilisateurs 38
Objectifs de la sensibilisation à la cybersécurité 38
Contenu de la formation 38
Méthodes de sensibilisation 39
Suivi et évaluation de l'efficacité de la formation 39
Engagement de la direction 40
Gestion des prestataires IT externes 41
Identification des prestataires et des services externalisés 41
Sélection et évaluation des prestataires IT 41
Contrats et accords de niveau de service (SLA) 42
Surveillance et audit des prestataires 42
Gestion des incidents et réversibilité des prestations 42
Plans de continuité et de réponse aux incidents 44
Élaboration d'un plan de réponse aux incidents (IRP) 44
Objectifs du plan de réponse aux incidents 44
Éléments essentiels du plan de réponse aux incidents 44
Tests réguliers des procédures de réponse aux incidents 45
Stratégies de reprise après sinistre (DRP) et continuité des affaires (BCP) 45
Coordination avec les tiers 46
Conclusion 46
Conformité réglementaire et audit 47
Conformité aux lois et régulations 47
Élaboration d'une politique de conformité 47
Audit interne et externe de la sécurité informatique 48

Revue régulière des politiques et procédures de sécurité 48

Checklist des bonnes pratiques 49

Inventaire des actifs 49
Sécurité du réseau et segmentation 49
Configuration et gestion des firewalls 49
Sauvegardes et restauration des données 49
Sécurisation des services exposés sur Internet 49
Gestion des vulnérabilités et des mises à jour 50
Protection des postes de travail et serveurs 50
Gestion des accès à privilèges 50
Surveillance et monitoring de l'infrastructure 50
Formation et sensibilisation 50
Gestion des prestataires IT externes 50
Plans de continuité et de réponse aux incidents 51

Introduction

Objectifs du guide

Ce guide a pour vocation de fournir aux institutions spécialisées du canton de Fribourg un ensemble de recommandations et de bonnes pratiques en matière de cybersécurité. Face à l'évolution constante des menaces et des risques liés à l'utilisation des systèmes d'information, il est crucial que ces institutions adoptent des mesures de sécurité robustes et adaptées à leurs besoins spécifiques. Le guide vise à soutenir les responsables informatiques, les administrateurs systèmes, les prestataires externes ainsi que les dirigeants dans l'élaboration et la mise en œuvre d'une stratégie de cybersécurité cohérente, efficace et durable.

Les objectifs principaux de ce guide sont :

- Sensibiliser les institutions aux enjeux de la cybersécurité.
- Fournir des directives pratiques et adaptées à la taille et à la complexité des infrastructures.
- Aider à la mise en place de mesures de protection contre les cybermenaces actuelles.
- Favoriser une culture de sécurité au sein de l'ensemble du personnel, des utilisateurs jusqu'aux équipes techniques.

Ce guide de bonnes pratiques a également pour but de clôturer un projet de cybersécurité global mené auprès des institutions spécialisées du canton de Fribourg. Durant ce projet, des actions telles que la sensibilisation aux utilisateurs, une campagne de phishing ainsi que des audits individuels des institutions ont été menés afin d'obtenir à la fois un état des lieux de la situation, ainsi que de proposer des mesures d'améliorations destinées à renforcer la posture de sécurité de l'ensemble des membres d'INFRI.

Contexte des institutions spécialisées dans le canton de Fribourg

Les institutions spécialisées du canton de Fribourg se caractérisent par une grande diversité en termes de taille, de mission et de moyens informatiques. Certaines peuvent compter seulement quelques employés, tandis que d'autres gèrent des centaines de collaborateurs avec des besoins en infrastructures informatiques variés. De plus, ces organisations sont souvent décentralisées et peuvent externaliser la gestion de leur informatique à des prestataires tiers, héberger leurs données en interne, ou utiliser des solutions cloud comme Microsoft Office 365.

Cette diversité se traduit également dans les types de services informatiques utilisés : certains systèmes critiques sont gérés en interne, d'autres sont entièrement sous-traités à des fournisseurs externes, et dans bien des cas, il existe une hybridation entre ces deux approches. L'hétérogénéité des systèmes et des processus rend parfois la gestion de la cybersécurité plus complexe, nécessitant des mesures adaptées au contexte particulier de chaque institution.

L'objectif de ce guide est donc d'accompagner ces institutions, quelles que soient leur taille et leur configuration informatique, en leur fournissant des recommandations concrètes et modulaires pour répondre aux exigences de cybersécurité actuelles.

Enjeux de la cybersécurité dans ces institutions

Les institutions spécialisées du canton de Fribourg gèrent souvent des données sensibles, qu'il s'agisse de données personnelles, de données de santé, ou d'informations critiques pour leur activité. Ces données doivent être protégées contre des cyberattaques de plus en plus fréquentes et sophistiquées, qu'il s'agisse de vols de données, d'attaques par ransomware ou encore de compromissions de systèmes via des vulnérabilités non corrigées.

Les principaux enjeux de la cybersécurité pour ces institutions sont :

- **Protéger les données sensibles :** Les institutions sont souvent responsables d'un volume important de données critiques, notamment des données médicales, sociales ou administratives. La protection de ces données est essentielle pour assurer la continuité de leurs services et préserver la confidentialité des personnes concernées.
- **Assurer la continuité des services :** Les cyberattaques peuvent interrompre les services fournis par ces institutions, ce qui peut avoir des répercussions graves sur leurs opérations quotidiennes. Par conséquent, des stratégies de continuité d'activité et de reprise après sinistre doivent être mises en place pour minimiser les impacts potentiels.
- **Se conformer aux obligations légales et réglementaires :** Les institutions sont soumises à divers cadres législatifs et réglementaires, notamment en ce qui concerne la protection des données (LPD) et la gestion des risques liés à l'utilisation des technologies de l'information. Le non-respect de ces obligations peut entraîner des sanctions financières, juridiques ou une perte de confiance de la part des utilisateurs et partenaires.
- **Anticiper et répondre aux cybermenaces :** Les cyberattaques évoluent rapidement, tant en termes de fréquence que de sophistication. Il est crucial que les institutions spécialisées mettent en place des systèmes de défense proactive, mais également qu'elles soient capables de réagir rapidement en cas d'incident.

En résumé, ce guide vise à offrir un cadre complet permettant aux institutions spécialisées de Fribourg de répondre à ces enjeux et d'adopter une posture de cybersécurité proactive et résiliente.

Évaluation de la maturité et priorisation des recommandations

Afin de faciliter la mise en œuvre des recommandations de ce guide, chaque mesure de cybersécurité a été associée à un niveau de maturité allant de 1 à 3. Ce classement permet aux institutions spécialisées de prioriser leurs efforts en fonction de leur situation actuelle, de leurs ressources disponibles et de leur niveau d'exposition aux risques.

L'objectif de cette classification est d'offrir une feuille de route progressive permettant aux organisations de renforcer progressivement leur posture de cybersécurité, tout en tenant compte de leurs contraintes opérationnelles et budgétaires.

Définition des niveaux de maturité

Niveau 1 - Maturité Faible (Actions prioritaires et essentielles)

Ce niveau correspond aux mesures fondamentales et critiques de cybersécurité qui doivent être mises en place en priorité pour protéger l'organisation contre les risques les plus courants et les plus impactants.

Objectif : Mise en conformité minimale et réduction des risques majeurs.

Caractéristiques :

- Absence ou faible formalisation des pratiques de cybersécurité.
- Protection insuffisante contre les menaces les plus répandues (exemple : phishing, ransomware).
- Gestion réactive des incidents de sécurité.
- Faible sensibilisation et formation des collaborateurs.
- Peu ou pas d'outils de surveillance et de contrôle.

Niveau 2 - Maturité intermédiaire (Optimisation et renforcement)

Ce niveau représente un renforcement significatif des mesures de cybersécurité et vise à instaurer une gestion proactive des menaces et des vulnérabilités.

Objectif : Passer d'une posture réactive à une approche préventive.

Caractéristiques :

- Processus de cybersécurité formalisés et documentés.
- Mise en place d'outils avancés de surveillance et de gestion des accès.
- Sensibilisation et formation régulière du personnel aux cybermenaces.
- Application systématique des correctifs et mises à jour de sécurité.

- Surveillance proactive des infrastructures et des logs de sécurité.

Niveau 3 - Maturité élevée (Cybersécurité avancée et gouvernance)

Ce niveau reflète une maturité avancée en cybersécurité, caractérisée par une gestion stratégique et intégrée de la sécurité, des capacités avancées de détection et réponse aux menaces.

Objectif : Anticiper les menaces et garantir une résilience optimale face aux cyberattaques.

Caractéristiques :

- Gouvernance cybersécurité intégrée à la stratégie globale de l'organisation.
- Automatisation avancée des processus de sécurité.
- Tests d'intrusion réguliers et simulations de cyberattaques.
- Surveillance en temps réel avec détection des comportements anormaux.
- Mise en place d'un SOC (Security Operations Center) interne ou externalisé.

Stratégie de mise en œuvre

Le passage d'un niveau de maturité à un autre doit être progressif et adapté aux ressources de l'institution. Voici quelques conseils pour structurer cette montée en maturité :

1. **Prioriser les actions de niveau 1 :** Ces actions constituent la base de la sécurité et doivent être mises en place en premier.
2. **Évaluer régulièrement la progression :** Effectuer des audits internes pour mesurer le niveau de maturité atteint.
3. **Planifier les investissements nécessaires :** Les niveaux 2 et 3 nécessitent souvent des outils et des expertises supplémentaires.
4. **Impliquer la direction et les employés :** La cybersécurité est une responsabilité collective et doit être soutenue par une gouvernance efficace.

Inventaire des systèmes et des services

La première étape fondamentale pour garantir la cybersécurité d'une organisation est d'établir un inventaire complet et à jour des systèmes informatiques, des services et des données qu'elle gère. Cet inventaire sert de base pour évaluer les risques, planifier les mesures de protection et assurer une gestion continue de la sécurité. Il permet aussi de prendre conscience des éventuelles interdépendances entre les services internes et ceux fournis par des prestataires externes, ce qui peut avoir un impact direct sur la sécurité globale.

Cartographie des systèmes informatiques internes et externes

Chaque institution dispose d'une infrastructure informatique spécifique, qui peut inclure un mélange de systèmes gérés en interne, des services fournis par des prestataires externes, ou encore des solutions cloud. Il est essentiel de dresser une cartographie exhaustive des systèmes existants. Cela inclut :

- Serveurs physiques et virtuels : Identifiez tous les serveurs, leur fonction (serveurs de fichiers, serveurs d'applications, bases de données, etc.) et leur emplacement physique ou virtuel (data centers, cloud, sur site).
- Systèmes de gestion de bases de données : Listez toutes les bases de données utilisées, les versions des logiciels de gestion, leur localisation (sur site ou cloud) et les personnes ou services responsables de leur gestion.
- Postes de travail et équipements périphériques : Incluez les ordinateurs de bureau, ordinateurs portables, appareils mobiles, imprimantes et autres périphériques connectés au réseau de l'institution.
- Réseaux internes : Décrivez les segments de réseau utilisés au sein de l'institution (réseaux administratifs, réseaux invités, réseaux de production, etc.) ainsi que leurs interconnexions.
- Réseaux et services externes : Identifiez les connexions VPN, les réseaux utilisés par les partenaires ou prestataires, ainsi que les services hébergés à l'extérieur de l'institution.

Classification des données et des systèmes

Toutes les données ne possèdent pas la même sensibilité ou valeur pour l'institution. Une bonne classification des données est primordiale pour définir les priorités en termes de protection et de gestion des risques. Cette classification doit être réalisée selon :

- Niveaux de confidentialité : Classez les données en fonction de leur caractère public, privé ou confidentiel. Par exemple, les informations sensibles (données personnelles des bénéficiaires, informations financières, etc.) doivent être classées de manière à garantir leur protection renforcée.

- Criticité des systèmes : Identifiez les systèmes critiques dont l'indisponibilité pourrait gravement affecter les opérations de l'institution (par exemple, les systèmes de gestion des bénéficiaires dans une institution).
- Données réglementées : Mettez en évidence les données soumises à des régulations spécifiques, telles que la LPD (données personnelles) ou des réglementations locales (données de santé).

Une bonne classification permet d'établir des priorités dans la gestion des incidents et d'appliquer des mesures de sécurité adaptées selon les niveaux de sensibilité.

Identification des prestataires externes (hébergement, cloud, services)

Les institutions spécialisées peuvent dépendre de prestataires externes pour l'hébergement de leurs systèmes, la gestion de certains services informatiques ou l'accès à des solutions cloud. L'inventaire des prestataires externes doit être précis pour s'assurer que les mesures de sécurité appliquées par ces prestataires respectent les exigences de l'institution.

- Prestataires de services d'hébergement : Notez les détails des entreprises qui fournissent des services d'hébergement physique ou cloud. Vérifiez les conditions contractuelles relatives à la sécurité, notamment les accords de niveau de service (SLA), et les politiques de sauvegarde, de chiffrement et de gestion des accès.
- Fournisseurs de solutions SaaS (Software-as-a-Service) : Recensez les applications tierces utilisées dans le cadre de services cloud (par exemple, Microsoft Office 365, Google Workspace). Assurez-vous que ces services respectent les standards de sécurité requis (gestion des identités, sécurité des accès, chiffrement des données, etc.).
- Prestataires de maintenance et support : Dressez une liste des prestataires externes qui accèdent à vos systèmes pour des raisons de maintenance, de support ou de gestion. Définissez les modalités d'accès à vos systèmes et les niveaux de privilège octroyés.

Interconnexions et dépendances entre services

Les systèmes informatiques ne fonctionnent généralement pas en isolation. Il est fréquent qu'une institution utilise des services interconnectés entre eux ou que certaines parties de son infrastructure dépendent de ressources externes. Il est crucial de comprendre ces interdépendances pour éviter des vulnérabilités dans la chaîne de sécurité. Parmi les exemples courants :

- Connexions aux services cloud : Par exemple, une solution de messagerie ou de gestion de documents hébergée dans le cloud, avec des données synchronisées localement.
- Interconnexions avec des services tiers : Par exemple, les systèmes de paiement, les services de communication avec d'autres organisations (partenaires, gouvernements, fournisseurs de services).
- Dépendances aux API et intégrations logicielles : Recensez les interfaces utilisées pour connecter des applications entre elles (par exemple, des API pour échanger des données entre votre système ERP et une application tierce).

Cette vue d'ensemble des interdépendances permettra d'anticiper des points de défaillance potentiels et d'instaurer des mesures de sécurité à tous les niveaux concernés.

Mise à jour et maintien de l'inventaire

L'inventaire des systèmes et services doit être tenu à jour en permanence. Les changements dans l'infrastructure, l'ajout ou la suppression de nouveaux services, ainsi que les modifications des dépendances avec les prestataires externes doivent être régulièrement documentés. Un processus de mise à jour automatisé ou semi-automatisé (par exemple, à l'aide de logiciels de gestion d'inventaire) est fortement recommandé pour garantir l'exactitude de l'inventaire à tout moment. Une attention particulière doit être portée aux points suivants :

- Mise à jour en cas de modification d'infrastructure (nouveaux serveurs, migration vers le cloud, suppression de systèmes obsolètes).
- Suivi des accès externes, notamment pour les prestataires qui peuvent se connecter aux systèmes de l'institution.
- Documentation des nouveaux équipements et terminaux ajoutés au réseau (ordinateurs, mobiles, etc.).

Sécurité du réseau et segmentation

Introduction

La sécurité du réseau est un pilier essentiel pour protéger les systèmes d'information des institutions, particulièrement dans un contexte où les systèmes et les données sensibles sont de plus en plus exposés aux menaces cybernétiques. La segmentation du réseau, qui consiste à diviser le réseau en sous-réseaux logiques, est une stratégie clé pour limiter la propagation des menaces en cas de compromission d'un segment. Elle permet également de restreindre l'accès aux ressources critiques en fonction des besoins, en appliquant le principe de moindre privilège.

Cette section décrit les meilleures pratiques pour sécuriser les réseaux internes des institutions spécialisées et propose des recommandations pour la segmentation, en prenant en compte les environnements variés de chaque institution (taille, personnel interne, prestataires externes).

Principes de la segmentation du réseau

La segmentation du réseau permet de compartimenter les systèmes et les données, réduisant ainsi le risque qu'un attaquant compromette tout le réseau. Une segmentation efficace repose sur les principes suivants :

- **Isolation des segments critiques :** les systèmes critiques, tels que les serveurs de bases de données et les systèmes de gestion des informations sensibles, doivent être isolés dans des segments dédiés. Cela limite les accès uniquement aux utilisateurs et services autorisés.
- **Principe de moindre privilège :** seuls les utilisateurs et services ayant un besoin opérationnel doivent pouvoir accéder aux segments critiques. Les règles d'accès doivent être définies en fonction des rôles des utilisateurs et de la sensibilité des systèmes.
- **Limitation de la surface d'attaque :** en limitant les connexions entre les différents segments, on réduit les vecteurs de propagation potentiels des attaques. Par exemple, le réseau administratif devrait être séparé du réseau de production pour limiter les risques d'attaques latérales.

Bonnes pratiques pour la segmentation et la ségrégation des réseaux internes

Pour implémenter une segmentation réseau efficace, voici des recommandations pratiques :

Classification des ressources

- Identifiez les ressources critiques, les applications sensibles et les données confidentielles.
- Élaborez une carte des ressources du réseau, en indiquant la classification de chaque système (confidentiel, sensible, public, etc.) pour mieux définir les besoins de segmentation.

Création de zones de sécurité

- Zone publique : regroupe les services et applications accessibles depuis Internet, tels que les sites web publics et les serveurs de messagerie électronique. Ces services doivent être isolés pour limiter leur exposition aux autres parties du réseau.
- Zone de DMZ (zone démilitarisée) : cette zone intermédiaire est utilisée pour isoler les services accessibles depuis l'extérieur, tout en maintenant un niveau de protection supplémentaire. Elle limite l'accès direct aux systèmes internes en forçant les connexions à passer par des pares-feux et des proxys.
- Zone interne : inclut les systèmes internes de l'organisation, tels que les serveurs de fichiers et les postes de travail des utilisateurs. Cette zone devrait être inaccessible directement depuis Internet.
- Zone sensible : dédiée aux ressources critiques (bases de données sensibles, applications de gestion interne, etc.), cette zone est hautement restreinte et son accès doit être strictement contrôlé.

Contrôle des accès inter-zones

- Implémentez des contrôles d'accès rigoureux entre les différentes zones du réseau. Par exemple, les utilisateurs de la zone interne ne devraient pas avoir accès à la zone sensible sans justification.
- Utilisez des pares-feux internes pour définir les politiques de contrôle entre chaque zone. Les connexions entre zones devraient être limitées aux protocoles strictement nécessaires (par exemple, bloquer les connexions FTP ou RDP vers les zones sensibles).
- Adoptez une approche "deny-by-default" (refuser par défaut), en autorisant uniquement les flux de communication explicitement nécessaires.

Segmentation logique avec VLANs

- Utilisez des VLANs (Virtual Local Area Networks) pour créer des sous-réseaux logiques. Par exemple, un VLAN pour le service administratif, un autre pour la production, et un pour les visiteurs.
- Assurez-vous que les VLANs sont configurés correctement, avec des règles de routage strictes pour éviter les accès non autorisés entre eux.
- Limitez l'accès aux VLANs aux seuls utilisateurs autorisés et appliquez des politiques de sécurité spécifiques à chaque VLAN.

Sécurisation des points d'accès et des connexions VPN

- Les accès VPN (Virtual Private Network) doivent être placés dans une zone DMZ et non directement connectés aux zones internes sensibles.
- Mettez en place une authentification multi-facteurs (MFA) pour l'accès VPN et limitez les droits d'accès des utilisateurs VPN aux ressources strictement nécessaires.
- Surveillez et enregistrez les connexions VPN pour détecter toute activité suspecte.

Utilisation des pares-feux internes pour le filtrage du trafic

- Utilisez des pares-feux pour filtrer le trafic entre les différents segments du réseau. Les pares-feux doivent être configurés pour autoriser uniquement le trafic essentiel.

- Établissez des règles de pare-feu strictes entre les VLANs et les sous-réseaux, en appliquant un filtrage granulaire selon les adresses IP, les ports et les protocoles.

Surveillance et maintenance des dispositifs de sécurité périmétrique

La sécurité de la segmentation repose sur la surveillance continue et la maintenance régulière des dispositifs de sécurité du réseau, notamment les pares-feux et les systèmes de détection d'intrusion (IDS/IPS).

Surveillance active du réseau

- Implémentez des systèmes de surveillance pour détecter et alerter en cas d'anomalies ou de tentatives d'intrusion entre les segments du réseau.
- Intégrez un SIEM (Security Information and Event Management) pour analyser les journaux des pares-feux et des systèmes réseau et détecter les comportements suspects.

Mise à jour et tests de sécurité

- Assurez-vous que tous les équipements de sécurité réseau (pares-feux, routeurs, etc.) sont régulièrement mis à jour pour combler les vulnérabilités connues.
- Effectuez des tests de pénétration réguliers pour vérifier l'efficacité de la segmentation et identifier les points faibles.

Audit des règles de segmentation

- Réalisez des audits périodiques des règles de segmentation pour vérifier leur pertinence et leur conformité avec les exigences de sécurité.
- Révisez et optimisez régulièrement les règles de pare-feu et de routage pour garantir une segmentation optimale et ajuster les contrôles d'accès aux besoins évolutifs.

Conclusion

La segmentation du réseau est une mesure essentielle pour protéger les ressources internes d'une institution contre les menaces externes et internes. En appliquant une segmentation rigoureuse, associée à un contrôle strict des accès et à une surveillance continue, les institutions peuvent grandement réduire la probabilité d'incidents de sécurité majeurs et protéger efficacement leurs données et systèmes critiques.

Configuration et gestion des firewalls

Les firewalls sont des dispositifs de sécurité essentiels pour protéger le périmètre du réseau des institutions et prévenir les accès non autorisés. Leur configuration correcte permet de limiter les risques d'intrusion tout en garantissant la continuité des services pour les utilisateurs autorisés. Cette section présente les bonnes pratiques pour la configuration, la gestion et la maintenance des firewalls.

Comprendre le rôle des firewalls dans la protection du périmètre

Les firewalls agissent comme une barrière entre le réseau interne d'une institution et les réseaux externes, y compris Internet. Ils filtrent le trafic entrant et sortant en fonction de règles définies pour bloquer les menaces potentielles et autoriser uniquement les communications légitimes. Une configuration efficace des firewalls est cruciale pour :

- Protéger les données et les systèmes critiques contre les attaques externes.
- Limiter l'exposition des services internes sur Internet.
- Assurer la segmentation entre différents sous-réseaux pour une meilleure isolation des systèmes sensibles.

Politiques de filtrage du trafic entrant et sortant

Principe du moindre privilège : Configurer le firewall de manière à autoriser uniquement le trafic essentiel pour les opérations de l'institution. Toute autre connexion doit être bloquée par défaut.

Filtrage des ports et des services : Identifier les ports et les services nécessaires, et autoriser uniquement ceux qui sont strictement indispensables.

Règles de géofencing : Limiter les connexions aux seules zones géographiques nécessaires. Par exemple, si l'institution ne travaille qu'avec des partenaires locaux, limiter les accès à la Suisse et à l'Europe.

Surveillance du trafic sortant : Contrôler les connexions sortantes pour prévenir les fuites de données ou les connexions non autorisées à des sites malveillants.

Bonnes pratiques pour la gestion des règles de firewall

Documenter toutes les règles de firewall : Maintenir une documentation claire et précise de chaque règle de firewall, y compris son objectif, les ports ouverts, les IP concernées, et les raisons de son implémentation.

Minimiser la complexité des règles : Éviter l'accumulation de règles redondantes ou obsolètes qui pourraient causer des erreurs ou des failles de sécurité.

Mettre en place des groupes de règles par fonction : Classer les règles de firewall par groupes (ex: accès Internet, accès aux services internes, etc.) pour une meilleure lisibilité et une gestion simplifiée.

Revue régulière des règles de firewall : Organiser des revues périodiques pour évaluer la pertinence de chaque règle. Supprimer ou mettre à jour les règles qui ne sont plus nécessaires.

Surveillance et maintenance des dispositifs de sécurité périmétrique

Surveillance continue : Mettre en place une surveillance 24/7 pour détecter les tentatives d'intrusion ou les anomalies de trafic. Utiliser des outils de détection d'intrusion (IDS/IPS) en complément du firewall.

Journalisation et audit : Activer les journaux (logs) des firewalls pour tracer les connexions et les tentatives d'accès. Ces logs doivent être conservés pendant une durée définie (souvent entre 6 mois et 1 an, selon les obligations réglementaires) et être régulièrement audités pour détecter des activités suspectes.

Mises à jour et correctifs : S'assurer que le firmware du firewall est régulièrement mis à jour pour combler les failles de sécurité connues. Activer les notifications de mise à jour du fournisseur et prévoir des créneaux pour appliquer les correctifs sans interruption de service.

Tests d'intrusion réguliers : Effectuer des tests d'intrusion périodiques pour évaluer la robustesse des règles de firewall. Ces tests peuvent être réalisés en interne ou par des tiers pour valider les configurations et identifier les vulnérabilités potentielles.

Configuration avancée des firewalls

Détection et prévention des intrusions (IDS/IPS) : Beaucoup de firewalls modernes intègrent des fonctions IDS/IPS pour identifier les signatures d'attaques et réagir automatiquement. Configurer les règles IDS/IPS pour bloquer les menaces courantes et recevoir des alertes en cas de détection de trafic suspect.

Inspection approfondie des paquets (DPI) : Utiliser l'inspection approfondie des paquets pour analyser en détail le contenu des communications et détecter les attaques dissimulées, notamment les malwares.

VPN et accès à distance sécurisé : Pour les accès distants, privilégier les connexions via VPN avec une authentification forte. Restreindre les accès à distance uniquement aux utilisateurs qui en ont besoin pour minimiser l'exposition.

Filtrage applicatif : Configurer le firewall pour filtrer le trafic non seulement au niveau des ports mais également au niveau des applications. Cela permet de limiter les accès uniquement aux applications approuvées.

Réponse aux incidents et récupération

Plan de réponse aux incidents : Définir un plan de réponse spécifique pour les incidents impliquant le firewall, comme les tentatives de force brute ou les dénis de service (DoS). Ce plan doit inclure des procédures pour bloquer rapidement les adresses IP suspectes et restaurer le service.

Sauvegarde et restauration de la configuration : Sauvegarder régulièrement la configuration du firewall et s'assurer qu'une copie est disponible pour une restauration rapide en cas de défaillance. Tester régulièrement le processus de restauration pour vérifier son efficacité.

Coordination avec les équipes de sécurité : En cas d'incident, le firewall doit être intégré dans la chaîne de réponse de l'institution, avec une communication fluide entre les administrateurs réseau, les équipes de sécurité et les responsables de l'institution.

Conclusion et recommandations

Une gestion efficace des firewalls nécessite une attention continue et des révisions régulières. Il est recommandé de :

- Maintenir une documentation à jour et accessible pour chaque règle et configuration.
- Éduquer et sensibiliser les administrateurs réseau et les utilisateurs sur les bonnes pratiques de cybersécurité.
- Investir dans des outils de surveillance et de détection pour assurer une protection proactive contre les menaces.

La bonne configuration et gestion des firewalls constituent un des piliers de la cybersécurité pour les institutions. Cela réduit considérablement les risques d'intrusion et assure la disponibilité et l'intégrité des services numériques.

Sauvegardes et restauration des données

La mise en place d'une politique de sauvegarde efficace est un élément clé de la stratégie de cybersécurité. La sauvegarde régulière des données et la capacité à restaurer rapidement les systèmes en cas de sinistre (panne matérielle, cyberattaque, erreur humaine, etc.) sont indispensables pour assurer la continuité des activités des institutions spécialisées. Cette section propose un cadre de bonnes pratiques pour définir et gérer les processus de sauvegarde et de restauration des données.

Stratégies de sauvegarde

Les stratégies de sauvegarde doivent être adaptées aux besoins spécifiques de chaque institution en fonction de la sensibilité des données, de la fréquence de modification des informations et des exigences légales. Voici les principaux types de sauvegardes recommandés :

Sauvegardes complètes : Une copie intégrale de toutes les données est effectuée à intervalle régulier. Bien que cette méthode soit la plus exhaustive, elle peut nécessiter un temps et un espace de stockage importants.

Sauvegardes incrémentielles : Seules les données modifiées depuis la dernière sauvegarde (complète ou incrémentielle) sont sauvegardées. Cette méthode est plus rapide et économise de l'espace de stockage, mais elle peut rallonger le processus de restauration.

Sauvegardes différentielles : Seules les données modifiées depuis la dernière sauvegarde complète sont sauvegardées. Cette méthode réduit également le volume des données sauvegardées par rapport à une sauvegarde complète, mais la restauration nécessite moins d'étapes qu'une sauvegarde incrémentielle.

Sauvegardes en continu (CDP - Continuous Data Protection) : Cette méthode permet de sauvegarder les données en temps réel. Elle est idéale pour les données critiques, car elle minimise le risque de perte de données entre deux sauvegardes.

Choix de l'emplacement des sauvegardes

L'emplacement des sauvegardes est un élément crucial pour garantir leur disponibilité en cas de besoin. Les institutions peuvent opter pour différentes options :

- **Sauvegardes locales :** Les données sont stockées sur des disques durs ou serveurs locaux. Cette option permet une restauration rapide mais peut être vulnérable en cas d'incident affectant le site physique (incendie, inondation).
- **Sauvegardes externes :** Les données sont sauvegardées chez un prestataire externe. Cela assure une protection contre les sinistres locaux, mais dépend de la fiabilité et de la sécurité de l'infrastructure du prestataire.

- **Sauvegardes dans le cloud :** Les données sont stockées sur une plateforme cloud, offrant flexibilité et redondance. Cependant, il est essentiel de s'assurer que le prestataire cloud respecte les normes de sécurité et de confidentialité.
- **Approche hybride :** Cette stratégie combine les sauvegardes locales et dans le cloud pour bénéficier des avantages des deux options. Par exemple, une copie locale permet une restauration rapide, tandis qu'une copie dans le cloud garantit une redondance géographiquement éloignée.

Fréquence et planification des sauvegardes

La fréquence des sauvegardes doit être définie en fonction des besoins de l'institution et du niveau de criticité des données. Voici quelques recommandations :

- **Données critiques :** Pour les données sensibles et régulièrement mises à jour, une sauvegarde quotidienne (ou même en continu) est recommandée.
- **Données moins critiques :** Pour des informations moins stratégiques, une sauvegarde hebdomadaire ou mensuelle peut suffire.
- **Tests de sauvegardes :** Il est essentiel de vérifier périodiquement l'intégrité des sauvegardes et de s'assurer qu'elles fonctionnent correctement. Un test trimestriel ou semestriel est recommandé.

Tests de restauration : bonne pratique et fréquence

La capacité à restaurer des données à partir d'une sauvegarde est aussi importante que la sauvegarde elle-même. Sans un processus de test de restauration, il est impossible de savoir si les sauvegardes peuvent être utilisées efficacement en cas de sinistre.

- **Test de restauration :** Planifier des tests réguliers pour vérifier la capacité à restaurer les données. Cela inclut des restaurations partielles (fichiers ou dossiers spécifiques) et des restaurations complètes (systèmes entiers).
- **Fréquence des tests :** Les tests de restauration doivent être effectués au moins une fois par trimestre, et après toute modification majeure de l'infrastructure ou des données.
- **Documentation des procédures de restauration :** Il est essentiel de documenter le processus de restauration, afin que les équipes sachent comment procéder en cas de crise. Cette documentation doit être mise à jour régulièrement et accessible en cas d'urgence.

Recommandations supplémentaires

Sécurité des sauvegardes : Les données sauvegardées doivent être chiffrées pour éviter tout accès non autorisé. De plus, l'accès aux systèmes de sauvegarde doit être restreint aux personnels autorisés.

Politique de rétention des sauvegardes : Définir une politique de conservation des sauvegardes en fonction des besoins de l'institution. Certaines données peuvent nécessiter une conservation à long terme pour des raisons légales ou de conformité.

Audit des sauvegardes : Mettre en place un audit régulier des procédures et des systèmes de sauvegarde pour s'assurer qu'ils sont conformes aux meilleures pratiques et qu'ils fonctionnent correctement.

Gestion des journaux : Conserver des journaux de toutes les opérations de sauvegarde et de restauration pour faciliter l'audit et la résolution d'incidents.

Formation des utilisateurs : Former les équipes techniques sur les procédures de sauvegarde et de restauration pour garantir qu'elles peuvent réagir efficacement en cas de problème.

Sécurisation des services exposés sur Internet

Les services exposés sur Internet représentent un point d'entrée privilégié pour les attaquants, qui peuvent cibler ces services pour exploiter des vulnérabilités ou accéder aux ressources internes d'une organisation. Il est donc crucial de mettre en œuvre des stratégies de sécurité adaptées pour réduire les risques associés à l'exposition de services sur Internet. Cette section propose des recommandations pour l'identification, la protection et le durcissement de ces services.

Identification des services exposés

La première étape de la sécurisation consiste à identifier tous les services exposés à Internet. Cette identification doit inclure :

- **Le recensement de tous les services accessibles publiquement :** notamment les serveurs web, les services de messagerie, les VPN, les serveurs FTP, les bases de données, les interfaces d'administration, etc.
- **L'évaluation de la nécessité de chaque service exposé :** chaque service accessible sur Internet devrait être justifié par un besoin métier clair. Dans le cas contraire, il est recommandé de le retirer.
- **La documentation des configurations de chaque service exposé :** inclure les informations sur les ports ouverts, les protocoles utilisés et les configurations de sécurité appliquées.

Cette phase de recensement peut être facilitée par des outils de découverte réseau (ex. : Nmap) et des solutions de gestion des actifs (Asset Management).

Réduction de la surface d'attaque

Une fois les services identifiés, il convient de réduire autant que possible la surface d'attaque, notamment en :

- **Fermant les ports inutilisés :** tout port qui n'est pas strictement nécessaire doit être fermé pour éviter une exposition inutile.
- **Limitant les adresses IP autorisées :** si possible, restreindre l'accès aux services à certaines adresses IP ou plages d'adresses IP, afin de limiter l'exposition publique.
- **Utilisant des proxys ou des passerelles sécurisées :** pour intercaler un dispositif de sécurité entre le service exposé et Internet, permettant de filtrer et surveiller le trafic entrant.
- **Implémentant des pare-feu applicatifs (WAF) :** pour les applications web, l'utilisation d'un WAF (Web Application Firewall) permet de filtrer les requêtes malveillantes et de protéger contre des attaques courantes comme l'injection SQL, les scripts intersites (XSS), etc.

Sécurisation des services de communication (SSL/TLS)

L'utilisation de communications chiffrées est essentielle pour protéger les données échangées entre les utilisateurs et les services exposés :

- Forcer l'utilisation du protocole HTTPS pour tous les services web exposés.
- Utiliser des certificats SSL/TLS valides et émis par des autorités de certification de confiance. Éviter les certificats auto-signés pour les services accessibles au public.
- Désactiver les protocoles obsolètes (comme SSL 2.0, SSL 3.0, TLS 1.0 et TLS 1.1) au profit de TLS 1.2 et TLS 1.3, qui offrent une meilleure sécurité.
- Configurer des suites de chiffrement robustes et éviter les algorithmes de chiffrement faibles (comme DES, RC4).
- Mettre en place HSTS (HTTP Strict Transport Security) pour forcer les navigateurs à n'accepter que les connexions sécurisées vers le service.

Contrôles d'authentification et d'autorisation

Les services exposés doivent intégrer des contrôles d'authentification et d'autorisation solides pour limiter l'accès aux utilisateurs autorisés uniquement :

- **Exiger une authentification forte :** utiliser des mécanismes d'authentification multifactorielle (MFA) pour tous les accès sensibles.
- **Limiter les accès administratifs :** restreindre les privilèges d'administration aux utilisateurs qui en ont strictement besoin et limiter l'accès administratif à des réseaux de confiance.
- **Mettre en place des sessions sécurisées :** utiliser des jetons de session (session tokens) et appliquer des restrictions sur la durée de vie des sessions et l'inactivité.
- **Activer la journalisation et l'audit des accès :** consigner les accès aux services exposés, y compris les tentatives réussies et échouées, pour faciliter les audits et la détection d'activités suspectes.

Test de vulnérabilités et gestion des correctifs

La sécurité des services exposés doit être vérifiée régulièrement par le biais de tests de vulnérabilités et d'une gestion proactive des correctifs :

- **Effectuer des scans de vulnérabilités périodiques :** utiliser des outils de scan (comme Nessus, OpenVAS) pour identifier les failles de sécurité potentielles.
- **Corriger rapidement les vulnérabilités critiques :** les vulnérabilités exposées sur des services publics doivent être corrigées sans délai. Prioriser les correctifs de sécurité en fonction du niveau de criticité.
- **Mettre en œuvre un processus de gestion des correctifs :** établir une procédure régulière pour appliquer les mises à jour de sécurité, y compris pour les systèmes d'exploitation, les logiciels tiers et les équipements réseau.

Durcissement des configurations

En plus des correctifs, il est crucial de durcir les configurations pour limiter les opportunités d'exploitation :

- **Appliquer les guides de durcissement des services exposés :** par exemple, utiliser les benchmarks CIS (Center for Internet Security) pour les configurations de serveurs web, bases de données, etc.
- **Désactiver les fonctionnalités non nécessaires :** limiter les fonctionnalités aux besoins stricts du service exposé.
- **Renforcer les permissions :** s'assurer que les services exposés ne disposent que des permissions minimales nécessaires pour fonctionner.

Surveillance et détection d'intrusions

La surveillance continue des services exposés permet de détecter des tentatives d'intrusion ou d'abus :

- **Mettre en place une solution de détection d'intrusion (IDS/IPS) :** une solution IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System) permet de surveiller le trafic et d'alerter en cas de comportements suspects.
- **Analyser les journaux de sécurité :** surveiller les journaux d'accès et d'erreurs pour identifier des comportements anormaux.
- **Configurer des alertes sur les activités suspectes :** mettre en place des alertes pour être notifié de toute tentative de connexion anormale, attaques par force brute, etc.

Conclusion

La sécurisation des services exposés sur Internet est un processus continu qui nécessite une attention constante pour adapter les mesures de sécurité aux nouvelles menaces. En suivant les bonnes pratiques décrites dans cette section, les institutions peuvent réduire significativement les risques liés à l'exposition de leurs services sur Internet. Il est également recommandé de revoir régulièrement la sécurité des services exposés et d'ajuster les contrôles en fonction des évolutions technologiques et des nouvelles menaces identifiées.

Gestion des vulnérabilités et des mises à jour

La gestion des vulnérabilités et des mises à jour est cruciale pour protéger les systèmes informatiques contre les menaces croissantes et les attaques ciblées. Une vulnérabilité non corrigée peut être exploitée par des cybercriminels pour obtenir un accès non autorisé aux systèmes, exécuter du code malveillant, ou perturber le bon fonctionnement des infrastructures. Cette section décrit les bonnes pratiques pour identifier, prioriser, et corriger les vulnérabilités de manière proactive et continue.

Processus de gestion des vulnérabilités

La gestion des vulnérabilités est un processus continu comprenant plusieurs étapes :

1. **Identification des vulnérabilités :** Utiliser des outils de scan de vulnérabilités pour identifier les failles dans les systèmes, applications et réseaux. Les outils courants incluent Nessus, Qualys, et OpenVAS. Des scans réguliers, au moins mensuels, sont recommandés pour maintenir une vision à jour des vulnérabilités.
2. **Évaluation de l'impact et de la criticité :** Chaque vulnérabilité doit être évaluée en fonction de son impact potentiel et de sa criticité. Les normes telles que le Common Vulnerability Scoring System (CVSS) permettent de prioriser les vulnérabilités en fonction de leur score de gravité (critique, élevée, moyenne, faible).
3. **Priorisation des corrections :** Les vulnérabilités critiques doivent être corrigées en priorité. Les critères de priorisation incluent le niveau de sévérité, l'exposition publique du système, et l'impact potentiel sur les opérations de l'organisation.
4. **Planification des actions correctives :** Établir un calendrier pour corriger les vulnérabilités, avec une attention particulière aux correctifs de sécurité fournis par les éditeurs de logiciels et les développeurs de systèmes d'exploitation. Des changements majeurs peuvent nécessiter des tests pour éviter des interruptions de service.
5. **Validation et tests post-correction :** Après application d'un correctif, effectuer un test pour s'assurer que la vulnérabilité a été corrigée sans causer de problèmes supplémentaires. Les scans de vulnérabilités doivent être réitérés pour vérifier la correction effective.
6. **Documentation et suivi :** Maintenir un registre des vulnérabilités identifiées, des correctifs appliqués et des tests de validation. Un suivi permet d'avoir une trace des actions entreprises et de mesurer l'efficacité du processus de gestion des vulnérabilités.

Politique de mise à jour des logiciels et systèmes

Une politique de mise à jour rigoureuse permet de réduire l'exposition aux vulnérabilités connues. Voici les éléments clés pour une gestion efficace des mises à jour :

- **Automatisation des mises à jour critiques :** Dans la mesure du possible, activer l’installation automatique des mises à jour pour les composants critiques, en particulier

pour les correctifs de sécurité des systèmes d'exploitation et des applications essentielles.

- **Mise à jour planifiée pour les systèmes critiques :** Établir une routine de mise à jour pour les systèmes et applications critiques qui ne peuvent pas être mis à jour automatiquement. Par exemple, les mises à jour peuvent être planifiées en dehors des heures de production pour minimiser l'impact sur les utilisateurs.
- **Tests pré-déploiement :** Pour les systèmes critiques, tester les mises à jour dans un environnement de préproduction avant de les appliquer en production. Cela permet d'identifier les éventuels conflits ou problèmes de compatibilité.
- **Gestion des correctifs pour les appareils obsolètes :** Certains systèmes ou logiciels peuvent ne plus recevoir de mises à jour de sécurité de la part des éditeurs. Dans ces cas, envisager des mesures alternatives comme la segmentation réseau, la restriction des accès ou l'isolement des systèmes obsolètes pour réduire leur exposition.
- **Surveillance des mises à jour de sécurité :** Maintenir une veille continue sur les publications de correctifs et les bulletins de sécurité des éditeurs de logiciels et de matériel. Par exemple, Microsoft, Adobe, Cisco et d'autres éditeurs publient régulièrement des correctifs de sécurité à surveiller.

Automatisation des mises à jour et surveillance continue

Pour améliorer l'efficacité et la rapidité de l'application des correctifs, il est recommandé d'automatiser certaines parties du processus de mise à jour :

- **Outils de gestion des correctifs :** Utiliser des outils de gestion des correctifs (ex. WSUS ou SCCM pour Windows, Chef, Ansible) pour appliquer des mises à jour de manière centralisée et automatisée. Ces outils permettent de programmer, suivre et vérifier l'installation des mises à jour sur l'ensemble des dispositifs.
- **Surveillance de la conformité des correctifs :** Mettre en place un tableau de bord de suivi des mises à jour pour identifier rapidement les systèmes non conformes aux politiques de sécurité. Les systèmes qui ne sont pas à jour doivent être rapidement identifiés et corrigés.
- **Alertes en temps réel :** Configurer des alertes pour détecter les tentatives d'exploitation de vulnérabilités connues et pour signaler les systèmes critiques qui ne sont pas à jour. Cela permet une réponse rapide en cas de menace active exploitant une vulnérabilité.

Bonnes pratiques pour la gestion des vulnérabilités et des mises à jour

- **Éduquer les utilisateurs et le personnel :** Informer les utilisateurs des risques liés aux logiciels non mis à jour et des pratiques de sécurité générales. Une vigilance de la part de tous peut contribuer à éviter des erreurs humaines pouvant exposer des vulnérabilités.
- **Rétroaction continue et amélioration du processus :** Évaluer régulièrement l'efficacité de la gestion des vulnérabilités et des mises à jour pour identifier des améliorations possibles. Réaliser des audits réguliers pour garantir le respect des bonnes pratiques et la cohérence du processus.

- **Revue périodique de la stratégie de patch management :** La stratégie de mise à jour doit être revue périodiquement pour s'assurer qu'elle reste adaptée aux nouvelles menaces et aux évolutions des systèmes et applications utilisés par l'organisation.

Protection des postes de travail et serveurs

Les postes de travail et les serveurs sont des composants critiques de l'infrastructure d'une organisation et sont souvent la cible privilégiée des cyberattaques. La protection de ces équipements est essentielle pour limiter les risques de compromission, de perte de données et d'interruption des opérations. Cette section présente les bonnes pratiques pour sécuriser les postes de travail et les serveurs, notamment en utilisant des solutions antivirales et de détection et réponse des endpoints (EDR), en configurant des politiques de sécurité adaptées, et en gérant les privilèges locaux de manière rigoureuse.

Solutions antivirales et EDR (Endpoint Detection and Response)

Antivirus

- **Mise en place d'un antivirus de qualité :** Un antivirus doit être installé sur tous les postes de travail et serveurs. Choisissez une solution reconnue et régulièrement mise à jour pour bénéficier des dernières définitions de menaces.
- **Mises à jour fréquentes :** Configurez les postes de travail pour que les mises à jour de l'antivirus soient effectuées automatiquement, assurant ainsi que les nouvelles signatures de virus sont intégrées rapidement.
- **Scans réguliers :** Programmez des scans réguliers (au minimum hebdomadaires) sur les postes de travail et les serveurs pour détecter toute anomalie ou logiciel malveillant dormant.

Endpoint Detection and Response (EDR)

En remplacement des solutions antivirales « classiques », il est possible de choisir une technologie de type « EDR » qui dans la plupart des cas sera plus efficaces. En comparaison avec un antivirus, une solution EDR apportera entre autre :

- **Détection avancée :** L'EDR offre une surveillance continue des endpoints pour détecter des comportements anormaux et des menaces émergentes non identifiées par les solutions antivirales classiques.
- **Réponse automatisée :** Les solutions EDR sont capables de réagir automatiquement en isolant un endpoint compromis, en interrompant une activité malveillante, ou en déclenchant des alertes en temps réel pour les équipes de sécurité.
- **Enquêtes sur les incidents :** En cas de compromission, l'EDR permet de retracer le vecteur de l'attaque, d'identifier les failles potentielles et de mener des analyses post-incident pour renforcer la protection future.

Configuration des politiques de sécurité pour les endpoints

Stratégie de renforcement (hardening) des endpoints

- **Désactivation des services inutiles :** Pour minimiser la surface d'attaque, désactivez tous les services et protocoles non essentiels sur les postes de travail et les serveurs.
- **Configuration des politiques de pare-feu local :** Utilisez les pares-feux intégrés aux systèmes d'exploitation pour bloquer les connexions non autorisées. Configurez des règles strictes pour limiter le trafic entrant et sortant sur chaque endpoint.
- **Contrôle des ports et des périphériques :** Limitez l'accès aux ports USB, CD-ROM, et autres périphériques physiques, souvent utilisés comme vecteurs d'attaque pour introduire des logiciels malveillants.

Gestion des mises à jour de sécurité (patch management)

- **Mise à jour régulière des systèmes :** Assurez-vous que tous les systèmes d'exploitation et les logiciels installés sur les postes de travail et les serveurs sont à jour. Programmez des mises à jour automatiques pour éviter les vulnérabilités connues.
- **Test des mises à jour critiques :** Avant de déployer des mises à jour majeures, effectuez des tests dans un environnement de test pour vérifier leur compatibilité et éviter les interruptions de service.

Utilisation d'un chiffrement de disque

En cas de vol ou de perte de l'équipement, le chiffrement des disques assure que les données ne peuvent pas être lues par des tiers non autorisés. Utilisez des solutions de chiffrement telles que BitLocker pour Windows ou FileVault pour macOS.

Bonnes pratiques pour la gestion des privilèges locaux

- **Principe du moindre privilège (POLP) :** Les utilisateurs doivent avoir seulement les droits nécessaires pour accomplir leurs tâches. Limitez les privilèges administratifs aux utilisateurs ayant des besoins spécifiques pour réduire les risques de propagation en cas de compromission.
- **Séparation des comptes administratifs et standards :** Exigez que les utilisateurs disposant de droits administratifs aient un compte distinct pour les activités administratives et un compte standard pour les tâches quotidiennes. Cela réduit les risques d'exécution de logiciels malveillants avec des privilèges élevés.
- **Contrôle des accès administratifs temporaires :** Si des droits élevés sont requis pour une tâche spécifique, accordez ces privilèges temporairement via un processus d'approbation. Utilisez des solutions de gestion des privilèges pour automatiser ce processus, limiter les accès temporaires et enregistrer les actions effectuées.
- **Surveillance et audit des activités privilégiées :** Mettez en place des journaux d'activité détaillés pour suivre les actions des utilisateurs disposant de droits élevés. Analysez régulièrement ces journaux pour détecter des comportements anormaux ou des tentatives de compromission.

Renforcement de la sécurité des sessions utilisateur

- **Verrouillage automatique des sessions :** Configurez les postes de travail et les serveurs pour qu'ils se verrouillent automatiquement après une période d'inactivité. Cela réduit le risque d'accès non autorisé lorsque les utilisateurs quittent leur poste.
- **Authentification multifacteur (MFA) :** Activez la MFA pour tous les utilisateurs, notamment ceux ayant des privilèges élevés, afin de renforcer l'authentification et de minimiser le risque d'accès par mot de passe compromis.
- **Surveillance des tentatives de connexion :** Implémentez des alertes et des verrouillages en cas de tentatives de connexion répétées échouées, afin de détecter et d'empêcher les attaques par force brute.

Gestion des accès à privilèges

La gestion des accès à privilèges (PAM, pour Privileged Access Management) est un domaine essentiel de la sécurité informatique, particulièrement critique pour les institutions qui souhaitent protéger leurs actifs les plus sensibles. Les comptes à privilèges, tels que les comptes administratifs, les comptes de service et autres utilisateurs disposant d'autorisations étendues, représentent un vecteur d'attaque privilégié pour les cybercriminels. Par conséquent, une approche structurée et méthodique de leur gestion est indispensable pour assurer la sécurité du système d'information.

Introduction à la gestion des comptes à privilèges

- **Définition :** Les comptes à privilèges sont des comptes ayant des droits d'accès étendus sur les systèmes d'information, leur permettant d'accomplir des tâches administratives telles que l'installation de logiciels, la gestion de configurations et l'administration des systèmes.
- **Enjeux de sécurité :** Une compromission de ces comptes peut avoir des conséquences majeures, allant de l'accès non autorisé à des données sensibles à l'altération de configurations critiques ou la propagation de menaces à l'échelle du réseau.

Principes de sécurité pour les comptes à hauts privilèges

- **Principe du moindre privilège :** Chaque utilisateur ou compte doit disposer du minimum d'autorisations nécessaires pour accomplir ses tâches. Cela limite les risques en cas de compromission.

- **Séparation des tâches :** L'accès à des privilèges élevés doit être réparti de manière à éviter qu'une seule personne puisse mener des actions critiques sans supervision ou contrôle.

- **Gestion centralisée des comptes privilégiés :** L'utilisation de solutions PAM permet de centraliser la gestion des accès, d'assurer une surveillance en temps réel et de réduire les risques associés aux comptes à hauts privilèges.

Identification et classification des comptes privilégiés

- **Cartographie des comptes :** Effectuer un inventaire exhaustif des comptes privilégiés existants, y compris les comptes locaux, les comptes de domaine, les comptes de service et les comptes utilisés par des applications.

- **Classification des accès :** Catégoriser les comptes selon leur niveau d'accès, leur importance et leur usage (comptes d'administration réseau, comptes applicatifs, comptes de service, etc.).

- **Évaluation des risques associés :** Analyser l'impact potentiel d'une compromission de chaque type de compte pour prioriser les efforts de sécurité.

Mise en œuvre d'une solution PAM (Privileged Access Management)

- **Gestion des mots de passe privilégiés :** Utiliser des coffres-forts sécurisés pour stocker, gérer et contrôler l'accès aux mots de passe de comptes privilégiés. Les solutions PAM permettent également de changer automatiquement les mots de passe après leur utilisation pour renforcer la sécurité.
- **Contrôle d'accès juste-à-temps (JIT) :** Octroi d'accès temporaire pour l'exécution de tâches spécifiques, avec révocation automatique des droits après usage.
- **Session management :** Enregistrement et supervision des sessions initiées par des comptes à privilèges pour une meilleure traçabilité et un contrôle accru des actions réalisées.
- **Double authentification :** Exiger une authentification forte (par exemple, authentification multifactorielle) pour l'accès aux comptes à privilèges.

Surveillance et audit des actions des utilisateurs privilégiés

- **Surveillance continue :** Mettre en place des outils de surveillance en temps réel pour suivre et enregistrer l'activité des utilisateurs à privilèges. Cela permet d'identifier rapidement tout comportement suspect.
- **Audits réguliers :** Réaliser des audits de sécurité périodiques pour s'assurer que les politiques de gestion des accès à privilèges sont respectées et que les contrôles de sécurité fonctionnent correctement.
- **Logs et rapports :** Conserver les logs d'accès et d'activité des utilisateurs privilégiés dans un format sécurisé et immuable, permettant une analyse a posteriori si nécessaire.

Politique de révision des comptes privilégiés

- **Révision périodique :** Évaluer régulièrement les besoins d'accès des utilisateurs et supprimer ou modifier les droits des comptes qui ne sont plus nécessaires.
- **Désactivation automatique :** Mettre en place des politiques de désactivation automatique des comptes qui ne sont pas utilisés pendant une période déterminée.
- **Contrôle des comptes orphelins :** S'assurer que les comptes créés par d'anciens employés ou des prestataires ne sont pas laissés actifs, en particulier les comptes disposant de privilèges élevés.

Sécurité des comptes de service et des comptes applicatifs

- **Gestion des identifiants de service :** Remplacer les mots de passe statiques des comptes de service par des identifiants gérés dynamiquement par une solution PAM.
- **Authentification sécurisée :** Utiliser des mécanismes d'authentification forte ou d'intégration avec des certificats et des clés sécurisées pour les comptes applicatifs.
- **Mise à jour des identifiants :** Changer régulièrement les identifiants et s'assurer qu'ils ne sont pas codés en dur dans le code source des applications.

Éducation et sensibilisation des utilisateurs privilégiés

- **Formation spécifique :** Proposer des sessions de formation dédiées aux utilisateurs ayant des privilèges étendus, en mettant l'accent sur la gestion sécurisée de leurs accès et la reconnaissance des menaces potentielles.
- **Politiques de sécurité adaptées :** Établir des politiques claires sur les comportements attendus, les restrictions et les meilleures pratiques pour les utilisateurs ayant des accès privilégiés.

Surveillance et monitoring de l'infrastructure

Introduction à la surveillance de l'infrastructure

La surveillance de l'infrastructure informatique est un pilier central de la sécurité des systèmes. Elle vise à collecter, analyser et alerter sur les événements critiques pouvant avoir un impact sur la sécurité ou la disponibilité des services informatiques. En détectant rapidement les incidents de sécurité et les anomalies de fonctionnement, la surveillance réduit le temps de réaction et limite l'impact des menaces.

Objectifs de la surveillance

Les objectifs principaux de la surveillance de l'infrastructure sont :

- Détection précoce des menaces et des attaques potentielles.
- Analyse des événements pour identifier les activités suspectes.
- Réduction des temps de réponse aux incidents.
- Suivi de la performance et de la disponibilité des services.
- Renforcement de la conformité avec les exigences réglementaires.

Types de surveillance

Il existe plusieurs aspects de la surveillance de l'infrastructure à considérer :

Surveillance des journaux d'événements (Logs)

La collecte et l'analyse des logs issus des serveurs, applications, équipements réseaux, pares-feux et autres systèmes sont essentielles pour une visibilité complète. Les logs permettent de détecter des anomalies, des accès non autorisés et d'autres comportements suspects.

Monitoring réseau

Surveiller le trafic réseau permet de détecter les anomalies, comme les pics de trafic inhabituels, les communications avec des sites malveillants, ou les tentatives d'intrusion. Des outils tels que des systèmes de détection/prévention d'intrusion (IDS/IPS) peuvent renforcer ce monitoring.

Surveillance de l'intégrité des systèmes

Cela consiste à vérifier que les fichiers critiques des serveurs ou des applications n'ont pas été altérés de manière non autorisée, ce qui peut indiquer une compromission.

Surveillance de la performance et de la disponibilité

Les indicateurs de performance (CPU, mémoire, disponibilité des services, temps de réponse) doivent être surveillés pour garantir le bon fonctionnement des systèmes. Une baisse soudaine de la performance peut indiquer une attaque ou une panne imminente.

Surveillance des activités des utilisateurs privilégiés

Les actions des utilisateurs avec des droits élevés doivent être surveillées de manière continue pour prévenir les abus et détecter les comportements suspects. Cela inclut les modifications critiques de configuration, les accès non autorisés ou les tentatives de contournement des politiques de sécurité.

Outils de surveillance

Pour assurer une surveillance efficace, divers outils et technologies peuvent être utilisés :

Systèmes de gestion des événements et des informations de sécurité (SIEM)

Un SIEM centralise les logs provenant de multiples sources, corrèle les événements, alerte en cas de détection d'activités suspectes, et aide à analyser les incidents de sécurité. Ces solutions sont essentielles pour une vision unifiée et en temps réel de la sécurité de l'infrastructure.

Outils de monitoring réseau et système

Des solutions telles que Nagios, Zabbix, ou encore des plateformes cloud intégrées permettent de surveiller la disponibilité et la performance des services, de générer des alertes en cas d'incident et d'anticiper les pannes.

Sondes de détection d'intrusion (IDS/IPS)

Ces dispositifs analysent le trafic réseau et les paquets en temps réel, identifient les attaques connues (via des signatures) ou les comportements anormaux (via l'analyse heuristique).

Principales étapes pour la mise en place d'une surveillance efficace

Évaluation des besoins et des risques

Comprendre les risques et les besoins spécifiques des systèmes et des données de l'institution.

Définition des indicateurs clés (KPI) et des seuils d'alerte

Déterminer quels événements doivent déclencher une alerte et les seuils à partir desquels une intervention est nécessaire.

Mise en place de solutions de collecte de logs

Collecter les logs de manière centralisée à partir de toutes les sources critiques. Assurez-vous que les journaux sont horodatés et conservés conformément aux exigences réglementaires.

Implémentation d'une solution de corrélation des événements (SIEM)

Corréler les données issues de différentes sources pour détecter des comportements malveillants.

Surveillance continue et mise à jour des politiques

Les configurations de surveillance doivent être mises à jour en fonction des nouvelles menaces et des changements de l'infrastructure. Les fausses alertes doivent être réduites pour garantir que seules les alertes pertinentes sont investiguées.

Réponse aux incidents détectés par le monitoring

Gestion des alertes

Toutes les alertes doivent être évaluées, catégorisées et investiguées pour déterminer si elles représentent une menace réelle.

Plans de réponse aux incidents

En cas de détection d'un incident, des procédures de réponse doivent être appliquées rapidement. Cela inclut l'isolement des systèmes compromis, l'investigation, la résolution de la faille, et la communication avec les parties prenantes.

Revue post-incident

Chaque incident doit faire l'objet d'une analyse post-mortem pour comprendre les causes, évaluer l'efficacité de la réponse et améliorer les procédures.

Bonnes pratiques de surveillance

Automatisation des tâches répétitives

Utiliser des scripts et des outils pour automatiser la collecte de données, la corrélation d'événements et la réponse à certaines alertes.

Examen périodique des configurations

Les configurations des outils de monitoring doivent être revues régulièrement pour s'assurer qu'elles restent pertinentes et efficaces face à de nouvelles menaces.

Formation continue des opérateurs

Les personnes en charge de la surveillance doivent être formées de manière continue pour reconnaître de nouvelles menaces, utiliser efficacement les outils et respecter les bonnes pratiques de réponse aux incidents.

Conclusion

La surveillance et le monitoring de l'infrastructure sont des processus dynamiques qui nécessitent une attention continue pour assurer une protection efficace des systèmes et des données. En

combinant outils, processus et expertise humaine, les institutions peuvent réduire les risques, améliorer leur réactivité et garantir la sécurité de leur infrastructure.

Formation et sensibilisation des utilisateurs

La sensibilisation et la formation des utilisateurs constituent une des composantes essentielles pour garantir une cybersécurité robuste au sein des institutions spécialisées. Une grande partie des cyberattaques réussies repose sur des erreurs humaines, telles que la divulgation de données sensibles, l'exécution de pièces jointes malveillantes ou la réutilisation de mots de passe faibles. Il est donc crucial d'instaurer une culture de cybersécurité solide par des programmes de formation réguliers et ciblés. Cette section propose une approche structurée pour développer et maintenir un programme de sensibilisation à la cybersécurité au sein des institutions.

Objectifs de la sensibilisation à la cybersécurité

- **Renforcer la conscience des menaces :** Informer les utilisateurs sur les cybermenaces actuelles, telles que le phishing, les rançongiciels, les malwares et les attaques ciblées.
- **Développer des compétences pratiques :** Enseigner des mesures pratiques et des comportements sécurisés à adopter pour minimiser les risques.
- **Promouvoir une culture de la sécurité :** Encourager la vigilance constante et le signalement proactif des incidents.
- **Conformité réglementaire :** Assurer que le personnel respecte les normes et exigences légales applicables.

Contenu de la formation

La formation doit couvrir les aspects suivants :

- Sécurité des mots de passe :
    - Création de mots de passe forts et utilisation de gestionnaires de mots de passe.
    - Politique de changement de mots de passe et sensibilisation à la non-réutilisation.
- Reconnaissance des tentatives de phishing et d'escroquerie :
    - Identification des e-mails, SMS et appels suspects.
    - Pratiques pour vérifier l'authenticité des expéditeurs et des messages.
- Utilisation sécurisée des e-mails et de la messagerie :
    - Bonne gestion des pièces jointes et des liens dans les e-mails.
    - Prévention du partage de données sensibles.
- Sécurité des dispositifs personnels et mobiles (BYOD) :
    - Politiques d’utilisation sécurisée des appareils mobiles connectés au réseau de l'institution.

    - Installation et utilisation de solutions de protection telles que des antivirus ou des solutions EDR (Endpoint Detection and Response).
- Accès physique aux systèmes :
    - Protection des postes de travail par des écrans de verrouillage automatiques.
    - Surveillance des zones sensibles et respect des politiques d'accès.
- Sécurité des connexions réseau :
    - Meilleures pratiques pour se connecter aux réseaux Wi-Fi publics ou non sécurisés.
    - Utilisation de VPN lors de l'accès à des systèmes sensibles.
- Mises à jour et gestion des correctifs :
    - Importance de maintenir les systèmes à jour avec les correctifs de sécurité.
    - Processus pour appliquer les mises à jour de manière sécurisée.
- Utilisation de clés USB et périphériques externes :
    - Sensibilisation aux dangers des périphériques inconnus ou non approuvés.
    - Politique de validation des périphériques avant utilisation.

Méthodes de sensibilisation

- **Campagnes de sensibilisation périodiques :** Mise en place de campagnes thématiques régulières pour rappeler les principes de sécurité (e.g., « Mois de la cybersécurité »).

- **Sessions de formation interactive :** Formations en présentiel ou en ligne avec des démonstrations pratiques, des études de cas, des questions-réponses et des ateliers pratiques.

- **Modules e-learning :** Accès à des modules en ligne pour permettre aux employés de suivre la formation à leur rythme.

- **Simulations d'attaques :** Organisation de campagnes de simulation de phishing pour tester et renforcer la vigilance des utilisateurs.

- **Bulletins de sécurité :** Diffusion de bulletins périodiques contenant des informations sur les menaces émergentes, les meilleures pratiques et les succès observés.

- **Kits de formation pour les nouveaux arrivants :** Intégration de la sensibilisation à la cybersécurité dès l'entrée de nouveaux collaborateurs au sein de l'organisation.

Suivi et évaluation de l'efficacité de la formation

- **Questionnaires et tests :** Évaluation régulière des connaissances des utilisateurs pour mesurer la compréhension des concepts.
- **Analyses de comportement :** Surveillance du comportement des utilisateurs (p. ex., réactions aux tests de phishing) pour évaluer l'adoption des pratiques enseignées.
- **Rapports de formation :** Suivi des taux de participation aux formations, des résultats aux tests et de la progression globale.

- **Amélioration continue :** Adaptation du contenu de la formation en fonction de l'évolution des menaces, des incidents passés et des retours d'expérience des utilisateurs.

Engagement de la direction

Pour garantir l'adhésion de tous les utilisateurs, il est essentiel que la direction s'implique activement en soutenant et en participant aux programmes de sensibilisation. Cela contribue à instaurer une culture de la cybersécurité et montre l'importance accordée à la protection des systèmes et des données de l'institution.

Gestion des prestataires IT externes

Les institutions spécialisées du canton de Fribourg font souvent appel à des prestataires IT externes pour gérer une partie ou la totalité de leur infrastructure informatique, notamment l'hébergement des systèmes, la gestion des services cloud, l'administration des réseaux et la cybersécurité. Une gestion rigoureuse de ces prestataires est essentielle pour garantir la sécurité des systèmes et la protection des données sensibles.

Identification des prestataires et des services externalisés

Avant d'engager un prestataire, il est crucial de bien définir les besoins et les responsabilités de chaque acteur impliqué. Voici les principales catégories de services externalisés :

- **Hébergement et stockage de données :** Data centers, cloud providers (Microsoft 365, AWS, Google Cloud).
- **Gestion des infrastructures IT :** Administration des serveurs, virtualisation, maintenance réseau.
- **Sécurité informatique :** SOC (Security Operations Center), gestion des firewalls, services d'audit de sécurité.
- **Support et assistance utilisateur :** Helpdesk, maintenance technique.
- **Développement et maintenance d'applications :** Services logiciels spécifiques, mises à jour d'applications internes.

Chaque institution doit établir un inventaire détaillé des prestataires impliqués et des services qu'ils fournissent.

Sélection et évaluation des prestataires IT

Avant d'engager un prestataire, il est essentiel de mener une évaluation rigoureuse basée sur les critères suivants :

- Expérience et réputation : Vérification des références et des certifications en cybersécurité (ISO 27001, SOC 2, etc.).
- Conformité réglementaire : Respect des normes en vigueur en Suisse (RGPD, LPD, réglementations cantonales).
- Niveau de sécurité offert : Gestion des accès, protection des données, sécurisation des environnements.
- Engagements contractuels et clauses de sécurité :
    - Accords de niveau de service (SLA)
    - Engagements en matière de continuité et reprise après sinistre (BCP/DRP)
    - Processus de gestion des incidents et des fuites de données

Un audit préalable peut être effectué pour évaluer la maturité en cybersécurité du prestataire.

Contrats et accords de niveau de service (SLA)

Les contrats avec les prestataires doivent inclure des clauses spécifiques garantissant la protection des actifs numériques de l'institution :

- Définition des responsabilités : Qui est responsable de quoi (mise à jour des systèmes, monitoring, gestion des accès, etc.).
- Disponibilité et performance : Engagements de temps de réponse et de résolution en cas d'incident.
- Sécurité et conformité :
    - Protection des données sensibles et exigences de chiffrement.
    - Obligations en matière de gestion des incidents de sécurité.
    - Droit d'audit et contrôle périodique par l'institution cliente.
- Gestion des accès et de la confidentialité :
    - Règles strictes pour l'accès aux infrastructures critiques.
    - Obligation de mise en place de mécanismes d'authentification forte (MFA).
    - Processus de révocation des accès en cas de fin de contrat ou de changement d'affectation.
- Plan de continuité et de reprise après sinistre (BCP/DRP) :
    - Engagements du prestataire en cas de panne majeure.
    - Tests réguliers des plans de reprise pour garantir leur efficacité.

Surveillance et audit des prestataires

Une fois le prestataire sélectionné, il est impératif de surveiller continuellement son niveau de sécurité et sa conformité aux engagements contractuels :

- **Audit régulier de cybersécurité :** Vérification de la conformité aux politiques de sécurité.
- **Contrôle des accès et des logs :** Surveillance des connexions et actions effectuées par les prestataires.
- **Évaluation continue des performances :** Analyse des indicateurs clés (temps de réponse aux incidents, disponibilité des services, etc.).
- **Tests d'intrusion et scans de vulnérabilités :** Réalisation d'évaluations techniques pour identifier d'éventuelles failles.

Gestion des incidents et réversibilité des prestations

Lorsqu'un prestataire est impliqué dans un incident de cybersécurité, un processus de gestion structuré doit être mis en place :

Identification et notification :

- Délais et procédures de signalement d'incidents.
- Coordination entre le prestataire et l'institution.

Analyse et résolution :

- Actions correctives et plan de remédiation.
- Documentation des causes et des leçons apprises.

Communication et reporting :

- Information aux parties prenantes et aux autorités compétentes si nécessaire.
- Mise en conformité avec les exigences légales en cas de fuite de données.

Enfin, un plan de réversibilité doit être prévu dans le contrat afin de garantir une transition fluide vers un autre prestataire ou un retour en interne en cas de changement stratégique.

Plans de continuité et de réponse aux incidents

Élaboration d'un plan de réponse aux incidents (IRP)

Le Plan de Réponse aux Incidents (IRP) est un document stratégique visant à garantir que l'organisation puisse identifier, évaluer et réagir rapidement aux incidents de sécurité. La mise en place d'un IRP clair est essentielle pour limiter les dommages causés par un incident et restaurer le fonctionnement normal aussi rapidement que possible.

Objectifs du plan de réponse aux incidents

- **Détection précoce des incidents de sécurité :** surveiller les systèmes, les journaux et les flux de données pour identifier rapidement tout comportement anormal.
- **Coordination efficace :** mettre en place des procédures pour garantir que chaque acteur impliqué connaît son rôle et ses responsabilités.
- **Atténuation des impacts :** contenir les incidents pour limiter les dommages sur l'organisation, ses systèmes et ses données.
- **Rétablissement rapide :** définir des étapes pour restaurer les opérations à la normale le plus rapidement possible après la résolution de l'incident.
- **Amélioration continue :** évaluer chaque incident pour tirer des leçons et renforcer les mesures préventives.

Éléments essentiels du plan de réponse aux incidents

- **Équipe de réponse aux incidents (IRT) :** formation d'une équipe composée de membres clés, incluant la direction, les responsables IT, la sécurité informatique, et les représentants légaux, selon le cas.
- **Processus de détection et de notification :** procédures pour détecter les incidents et les signaler rapidement.
- **Évaluation de l'incident :** identifier la nature, l'étendue et la gravité de l'incident.
- **Mesures de confinement :** mise en place de mesures pour limiter la propagation de l'incident.
- **Analyse post-incident :** enquête approfondie sur les causes de l'incident, ses impacts, et ses éventuelles vulnérabilités exploitées.
- **Rapport et documentation :** consigner chaque étape, chaque décision, et les résultats pour fournir une base solide pour les leçons tirées et les audits futurs.

Tests réguliers des procédures de réponse aux incidents

La seule élaboration d'un plan ne suffit pas ; il est crucial de le tester régulièrement pour s'assurer de son efficacité. Les tests permettent de vérifier si les membres de l'équipe connaissent leurs rôles et d'évaluer la robustesse des processus.

Méthodologies de test

- **Simulations d'incidents :** effectuer des exercices simulés basés sur des scénarios réalistes.
- **Tabletop exercises :** exercices où les membres de l'IRT discutent et résolvent théoriquement les actions à entreprendre en réponse à un scénario donné.
- **Tests périodiques :** planifier des tests à intervalles réguliers, tels que trimestriels ou annuels.

Évaluation des résultats des tests

- **Rapport de performance :** analyser la rapidité de la détection et de la réponse.
- **Retour d'expérience (RETEX) :** organiser des sessions pour identifier ce qui a fonctionné, ce qui n'a pas fonctionné et les améliorations possibles.
- **Mise à jour du plan :** ajuster le plan en fonction des retours obtenus pour corriger les failles ou les inefficacités identifiées.

Stratégies de reprise après sinistre (DRP) et continuité des affaires (BCP)

La continuité des opérations doit être assurée même en cas d'incident majeur. Cela inclut la planification de la reprise après sinistre (DRP) et de la continuité des affaires (BCP), deux composantes essentielles pour minimiser l'impact d'une interruption majeure sur les activités de l'organisation.

Plan de Reprise Après Sinistre (DRP)

- **Objectif :** restaurer les systèmes critiques à un état opérationnel le plus rapidement possible.
- **Analyse d'Impact sur les Activités (BIA) :** identifier les processus essentiels de l'organisation et leur dépendance en matière de systèmes et de données.
- **Sites de secours :** prévoir des sites de sauvegarde ou de secours pour héberger les activités critiques en cas de défaillance des installations principales.
- **Stratégies de sauvegarde des données :** garantir que les sauvegardes sont actualisées, protégées et récupérables rapidement.

Plan de Continuité des Affaires (BCP)

- **Évaluation des risques :** déterminer les risques les plus probables et leurs impacts potentiels.
- **Planification des scénarios de continuité :** mise en œuvre de stratégies pour maintenir les fonctions critiques en activité malgré des perturbations.

- **Communication en période de crise :** mise en place de protocoles pour informer les parties prenantes internes et externes (clients, partenaires, etc.).
- **Entraînement et sensibilisation :** veiller à ce que tous les employés connaissent le BCP et sachent comment réagir lors d'une perturbation majeure.

Coordination avec les tiers

Les institutions doivent également travailler en étroite collaboration avec leurs prestataires de services, fournisseurs de technologies et autres parties prenantes externes pour garantir une réponse coordonnée et harmonisée aux incidents, en particulier dans les cas où des systèmes ou des données sont externalisés.

Conclusion

L'élaboration et le maintien de plans de réponse aux incidents et de continuité des opérations constituent des piliers de la résilience organisationnelle en cybersécurité. La vigilance continue, les tests fréquents et l'amélioration des processus garantissent une meilleure capacité de résistance face à des menaces évolutives. Ce processus exige une collaboration de l'ensemble de l'organisation pour maintenir des niveaux de sécurité optimaux et assurer la pérennité des opérations.

Conformité réglementaire et audit

La conformité réglementaire et l'audit de la sécurité informatique sont des composantes essentielles pour garantir que les institutions respectent les lois, les régulations en vigueur ainsi que les standards de l'industrie en matière de protection des données et des systèmes informatiques. Cette section propose un cadre pour assurer que les mesures de sécurité sont conformes, documentées et régulièrement auditées pour prévenir tout écart ou risque non identifié.

Conformité aux lois et régulations

La conformité aux lois et régulations est une responsabilité incontournable pour toute institution manipulant des données sensibles, que ce soit des données personnelles, des informations financières ou des données de santé. Les institutions du canton de Fribourg doivent respecter un certain nombre de réglementations, notamment :

Le Règlement Général sur la Protection des Données (RGPD) : Ce règlement européen impose des exigences strictes en matière de collecte, de traitement, et de protection des données personnelles. Les institutions doivent :

- Documenter les traitements de données personnelles.
- Mettre en place des mesures de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des données.
- Nommer un Délégué à la Protection des Données (DPO) si nécessaire.
- Assurer que les transferts de données hors de l'UE soient conformes aux dispositions du RGPD.

Les lois suisses sur la protection des données (LDP) : En complément du RGPD, les institutions doivent également respecter les lois locales, telles que la nouvelle LPD, qui impose des obligations similaires, notamment :

- La transparence et l'information des personnes concernées.
- Le respect des droits des personnes (accès, rectification, suppression, etc.).
- L'obligation de notifier les violations de données personnelles à l'autorité compétente.

Les normes et standards de l'industrie : Selon l'activité des institutions, certaines normes sectorielles peuvent s'appliquer (ex. : ISO/IEC 27001 pour la gestion de la sécurité de l'information, PCI-DSS pour les paiements par carte).

Élaboration d'une politique de conformité

Les institutions doivent adopter une politique de conformité clairement définie, qui détaille les obligations réglementaires spécifiques, les mesures de contrôle mises en place et les responsables chargés de la mise en conformité. Cette politique doit inclure les éléments suivants :

- **Cartographie des données :** Identifier les données sensibles, leur localisation et les flux associés.

- **Contrôles techniques et organisationnels :** Mise en place de mesures telles que le chiffrement des données, l'authentification forte, la gestion des accès, etc.
- **Formation des employés :** Informer régulièrement les collaborateurs sur les obligations légales et les bonnes pratiques en matière de conformité.
- **Procédures de gestion des incidents :** Développer des protocoles pour répondre rapidement à des violations de données ou autres non-conformités.

Audit interne et externe de la sécurité informatique

Pour assurer un niveau constant de conformité et de sécurité, il est indispensable de réaliser des audits réguliers. Ces audits permettent d'évaluer l'efficacité des mesures mises en place, de détecter les écarts et de prendre les mesures correctives nécessaires.

Audit interne

- Réalisation par une équipe interne dédiée ou un responsable de la conformité.
- Vérification des politiques, procédures et dispositifs de sécurité en place.
- Évaluation de la conformité des processus par rapport aux exigences réglementaires.
- Préparation de rapports internes avec des recommandations pour les améliorations.

Audit externe

- Effectué par une tierce partie indépendante ou un cabinet spécialisé.
- Audit de conformité selon des standards reconnus (ISO 27001, RGPD).
- Revue approfondie des contrôles de sécurité, des incidents passés, et de la gestion des risques.
- Production d'un rapport d'audit incluant les observations, les risques identifiés et les plans d'action recommandés.

Revue régulière des politiques et procédures de sécurité

La mise en conformité n'est pas un effort ponctuel, mais un processus continu. Il est crucial de :

- Effectuer des revues périodiques pour s'assurer que les politiques de sécurité sont mises à jour en fonction des changements réglementaires, des nouvelles menaces ou des évolutions des activités institutionnelles.
- Évaluer l'efficacité des mesures de contrôle au travers d'audits réguliers.
- Planifier des tests et simulations de crise pour vérifier que les procédures de réponse aux incidents sont robustes et efficaces.

La mise en place d'une démarche de conformité rigoureuse et bien documentée non seulement protège les institutions contre les risques juridiques, mais renforce également leur résilience face aux cybermenaces.

Checklist des bonnes pratiques

Cette check-list permet de vérifier la mise en œuvre des bonnes pratiques de cybersécurité mentionnées dans le guide :

Inventaire des actifs

- ☐ Effectuer une cartographie des systèmes et services.
- ☐ Classifier les données sensibles.
- ☐ Identifier les prestataires externes.

Sécurité du réseau et segmentation

- ☐ Appliquer la segmentation du réseau (séparer les réseaux internes, DMZ, etc.).
- ☐ Configurer les accès réseau avec des contrôles stricts.
- ☐ Utiliser des VPN pour les connexions à distance avec authentification multi-facteurs (MFA).

Configuration et gestion des firewalls

- ☐ Définir des politiques de filtrage strictes.
- ☐ Effectuer une revue périodique des règles de firewall.
- ☐ Maintenir à jour son/ses firewalls avec les dernières versions de firmware disponibles.

Sauvegardes et restauration des données

- ☐ Planifier des sauvegardes régulières (journalières, hebdomadaires, mensuelles).
- ☐ Tester régulièrement les restaurations de sauvegardes.
- ☐ Chiffrer les sauvegardes sensibles.

Sécurisation des services exposés sur Internet

- ☐ Limiter au maximum le nombre de services exposés sur internet.
- ☐ Limiter l'accès aux services uniquement aux utilisateurs autorisés, avec une authentification à multi-facteurs (MFA).
- ☐ Effectuer des tests réguliers de sécurité sur les services exposés.

Gestion des vulnérabilités et des mises à jour

- ☐ Maintenir un inventaire des logiciels et systèmes.
- ☐ Appliquer les mises à jour critiques rapidement.
- ☐ Mettre en œuvre une gestion centralisée des correctifs.

Protection des postes de travail et serveurs

- ☐ Installer et configurer des solutions antivirales au minimum, EDR idéalement.
- ☐ Appliquer des politiques de sécurité (pare-feu local, contrôle des périphériques USB).
- ☐ Définir des permissions minimales pour les utilisateurs.

Gestion des accès à privilèges

- ☐ Appliquer des politiques strictes de gestion des comptes à privilèges.
- ☐ Enregistrer les activités des utilisateurs privilégiés.
- ☐ Utiliser des solutions de gestion des accès à privilèges (PAM).

Surveillance et monitoring de l'infrastructure

- ☐ Implémenter un système de monitoring (SIEM).
- ☐ Définir des règles de détection d'anomalies.
- ☐ Mettre en place des alertes et des procédures de réponse rapide.

Formation et sensibilisation

- ☐ Organiser des sessions régulières de formation pour les employés.
- ☐ Conduire des campagnes de sensibilisation à la cybersécurité.
- ☐ Tester périodiquement la vigilance du personnel (ex : tests de phishing).

Gestion des prestataires IT externes

- ☐ Connaître précisément l'ensemble de ses prestataires IT ainsi que leurs périmètres de responsabilités.
- ☐ Sélectionner ses prestataires IT selon des critères définis et pragmatiques.
- ☐ Etablir des contrats avec ses prestataires IT, prenant notamment en compte des niveaux de services garantis (SLA), un droit d'audit ainsi qu'une facilité à la réversibilité des services.

Plans de continuité et de réponse aux incidents

- ☐ Élaborer un plan de réponse aux incidents (IRP).
- ☐ Tester le plan de réponse aux incidents et le plan de reprise après sinistre (DRP).
- ☐ Documenter les leçons apprises après chaque incident.

immunIT sàrl

Chemin des Plantaz 44-46, 1260 Nyon

+41 22 565 33 71

info@immunit.ch

https://www.immunit.ch