ANNEXE 1
GUIDE DE SECURISATION D'UN ENVIRONNEMENT INFORMATIQUE

G. Barrot (ACRI-ST). V1.1

Ce document présente quelques bonnes pratiques concernant la sécurisation d'un système informatique.

Évaluation des Risques

1.1 Identification des actifs

Lister et documenter tous les actifs informatiques (matériel, logiciel, données). Chaque actif doit être évalué pour comprendre son importance et son rôle dans l'organisation.

1.2 Évaluation des menaces

Identifier toutes les menaces potentielles qui pourraient affecter les actifs. Cela inclut les cyberattaques, les erreurs humaines, les catastrophes naturelles, etc.

1.3 Analyse des vulnérabilités

Évaluer les faiblesses qui peuvent être exploitées par des menaces. Cela inclut les vulnérabilités logicielles, les configurations incorrectes, et les pratiques de sécurité inadéquates.

1.4 Évaluation de l'impact

Déterminer l'impact potentiel de chaque menace sur les actifs en termes de confidentialité, d'intégrité, et de disponibilité des informations. Lien avec la RGPD.

1.5 Évaluation des risques

Prioriser les risques en fonction de leur probabilité et de leur impact. Cela permet de concentrer les efforts de sécurité sur les risques les plus critiques.

Mise en place de politiques de sécurité

2.1 Développement de politiques

Élaborer des politiques de sécurité claires couvrant divers aspects tels que l'utilisation des ressources, la gestion des accès, et la protection des données.

2.2 Communication

S'assurer que toutes les politiques de sécurité sont bien communiquées et comprises par tous les employés. Utiliser des sessions de formation et des documents écrits pour faciliter cette compréhension.

Utiliser des outils permettant le suivi des formations aux politiques de sécurité (ex. https://avantdecliquer.com/)

Sécurisation des accès

3.1 Gestion des identités et des droits d'accès

Mettre en œuvre des solutions pour gérer les identités des utilisateurs et contrôler leur accès aux ressources. Cela inclut la création, la gestion et la suppression des comptes utilisateur.

3.2 Authentification multi-facteurs (option)

Imposer l'utilisation de l'authentification multi-facteurs (ex. utilisation des smartphones) pour ajouter une couche supplémentaire de sécurité lors d'accès à des services critiques – si besoin.

Protection des données

4.1 Chiffrement

Utiliser des techniques de chiffrement pour protéger les données sensibles à la fois en transit et au repos. Le chiffrement garantit que seules les personnes autorisées peuvent accéder aux informations.

4.2 Sauvegarde des données

Mettre en place des systèmes de sauvegarde régulière.

Tester la restauration des sauvegardes pour s'assurer que les données peuvent être récupérées en cas de perte ou de corruption.

4.3 Classification des données

Classer les données en fonction de leur sensibilité et appliquer des contrôles de sécurité et de sauvegarde appropriés en fonction de leur classification.

Sécurisation des réseaux

5.1 Pare-feux et systèmes de détection et de prévention d'intrusion

Utiliser des pare-feux et des systèmes IDS/IPS pour surveiller et protéger les réseaux contre les intrusions et les activités malveillantes.

Mettre en place d'outils EDR.

5.2 VPN / P2P

Utiliser des réseaux privés virtuels (VPN) ou des liaisons dédiées pour sécuriser les connexions à distance et protéger les données en transit sur les réseaux non sécurisés.

5.3 Segmentation du réseau

Segmenter le réseau pour limiter les mouvements latéraux en cas de compromission. La segmentation aide à isoler les différentes parties du réseau et à contenir les incidents.

Gestion des mises à Jour

6.1 Mise à jour régulière

Installer régulièrement les mises à jour et les patches pour les systèmes d'exploitation, les applications et les dispositifs réseau afin de corriger les vulnérabilités.

6.2 Gestion des correctifs

Utiliser des outils de gestion des correctifs pour automatiser et gérer le processus de mise à jour. Ces outils aident à suivre l'état des correctifs et à garantir que toutes les mises à jour nécessaires sont appliquées.

La centralisation et le contrôle des postes de travail à distance facilite cette tâche (le parc est géré le plus automatiquement possible).

Surveillance et détection

7.1 Journalisation et surveillance

Mettre en place des systèmes de journalisation et de surveillance pour détecter les activités suspectes. La journalisation permet de suivre les événements et les actions dans le système.

7.2 Analyse des journaux (logs)

Analyser régulièrement les journaux pour identifier les signes d'intrusion ou d'autres incidents de sécurité.

Réponse aux incidents

8.1 Plan de réponse aux incidents

Développer et maintenir un plan de réponse aux incidents pour gérer et minimiser l'impact des incidents de sécurité. Ce plan doit inclure des procédures pour l'identification, la non-propagation, l'éradication et la remise en état.

8.2 Équipe de réponse aux incidents

Constituer une équipe dédiée à la gestion des incidents de sécurité. Cette équipe doit être formée et équipée pour répondre rapidement et efficacement aux incidents.

8.3 Plan de gestion de crise

L’équipe de réponse aux incidents doit définir un plan de crise à déployer en cas de corruption du système informatique (personnes à contacter, numéros de téléphone, continuité d’activité hors système informatique, etc).

Formation et sensibilisation

9.1 Formation des employés

Former régulièrement les employés sur les meilleures pratiques en matière de cybersécurité. Les formations doivent couvrir des sujets tels que la gestion des mots de passe, l'identification des emails de phishing, et la protection des données sensibles.

9.2 Simulations de phishing

Réaliser des simulations de phishing pour sensibiliser les employés aux techniques d'ingénierie sociale. Ces simulations aident à évaluer la vigilance des employés et à améliorer leur capacité à reconnaître les tentatives de phishing.

Audits et conformité

10.1 Audits de sécurité

Effectuer des audits de sécurité réguliers pour évaluer l'efficacité des mesures de sécurité en place. Les audits permettent d'identifier les lacunes et d'améliorer les pratiques de sécurité.

10.2 Conformité

Assurer la conformité aux réglementations et normes pertinentes (ISO27001). Maintenir une documentation à jour et effectuer des revues de conformité régulières.

Renforcement des applications

11.1 Tests de pénétration

Effectuer des tests de pénétration pour identifier et corriger les vulnérabilités des applications. Ces tests simulent des attaques réelles pour évaluer la résilience des applications.

ANNEXE 2
L'accompagnement du SICTIAM face à la cybermenace

Préambule
de la rencontre du Mardi 2 Juillet 2024

Jérôme VIAUD, Président de l'ADM06, Maire de Grasse et Président de la Communauté d'Agglomération du Pays de Grasse a organisé cette rencontre en presence du conseil de développement de la CAPG suite à une annonce qu'il a réalisée il y a 3 Mois à Mandelieu sur le theme de la gestion et de l'anticipation aux risques.

L'objectif étant de mieux se preparer face aux risques de la cybermenace.

Il est demandé autour du groupe de travail composé de M. ROZELOT, M. MASSE, M. BOUILLON, M. BONNICI, M.BARROT et M. AMMENDOLA d'établir une feuille de route à proposer à M. Le Président, Jérôme VIAUD.

Les objectifs :

1. Développer une filière de la cybersécurité en créant une formation diplomante sur le territoire de la CAPG pour répondre aux besoins en matière de recrutement dans les domaines de la cybersécurité.
2. Favoriser la prise en conscience des enjeux de la cybermenace et proposer des actions clés en main pour en réduire les risques.
3. Créer un grand évènement cyber au Palais des Congrès à Grasse pour valoriser les actions à venir, en cours et à développer sur le territoire.

PRÉSENTATION

L'OFFRE CYBER DU SICTIAM

QUELLES SONT LES AIDES ?

Un Syndicat
au plus près des territoires

COMPLÉMENTARITÉ

Faciliter le quotidien des collectivités membres en utilisant le levier de la mutualisation.

COMPÉTENCES

Ne laisser personne au bord du chemin et ce qu'elle que soit la taille de la collectivité.

DISPONIBILITÉ

Personnaliser les liens avec chacun des adhérents et organiser une animation territoriale de cette communauté.

Le SICTIAM
en quelques chiffres

1989

ANNÉE DE CRÉATION.
À l'initiative de 14 collectivités membres fondatrices

96

COLLABORATEURS au service des entités publiques

3

LIEUX pour accueillir : Sophia-Antipolis, Nice et Gap

Une offre déclinée
en formation

218 actions de formation

Formations mutualisées
Certaines formations éligibles au format distanciel
453 conventions de formation

Nos offres de services

AMÉNAGEMENT DU TERRITOIRE ET RÉSEAUX
Système d'Information Géographique
Énergies renouvelables / Éclairage public / Fibre optique / Distribution Publique d'électricité et gaz / Adressage des rues / Sobriété énergétique

GESTION DE L'INFORMATION ET CYBERSÉCURITÉ
Open Data / DPO externalisé / Cybersécurité

PILOTAGE E GESTION DES SERVICES
SESILE / STELA / Certificats électroniques / Convocation aux assemblées / Dématérialisation des marchés publics / Gestion Financière Ressources Humaines / Gestion de la Dette & Trésorerie / Services Techniques / Observatoire fiscal / Gestion du courrier/ Tableaux de Bord (PowerBI)

RELATIONS AVEC LES USAGERS
Aide sociale / Communication numérique / École Numérique / Élections / Enfance / Facturation / État civil / Gestion de la Relation Usagers / Cimetières / Gestion de l'eau / Vidéo protection / Saisine par Voie Électronique / Wifi public / Agent conversationnel IA / Réalité virtuelle / Application mobile citoyenne

ENVIRONNEMENT DETRAVAIL
Bureautique / Fournitures informatiques / Gestion de parc informatique / Impression & reprographie / Services de télécommunication / Systèmes de téléphonie / Outils collaboratifs et messagerie / Cloud / Sobriété numérique

SICTIAM - DES SERVICES ADAPTÉS

La criminalité numérique est une activité aussi rentable que le trafic de drogue.

Source : rapport de la société de sécurité Symantec

Les données ont une valeur

prix moyen proposé sur le darkweb

« Ce n’est pas ma priorité »
« Je n’ai pas le budget »
« Je ne suis pas concerné »
« Je n’ai pas le temps »

Les organismes publics
victimes d’actes de cybermalveillance

Depuis 2019

Centre Hospitalier
Établissement public de santé

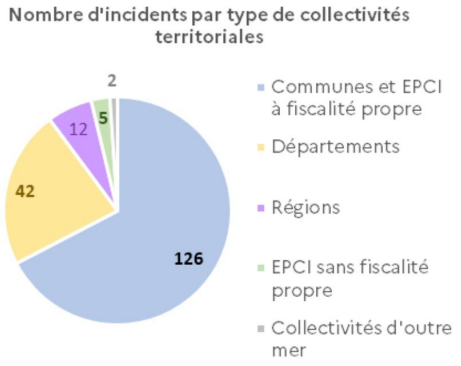
Région
Département

Métropole
Communauté d’agglomération
Communauté de communes

Mairie

http://u.osmfr.org/m/821557/

Cyberattaques : quelques chiffres



10

incidents par mois ont affecté des collectivités entre janvier 2022 et juin 2023, représentant 17% des cas traités par l'Anssi

Source : cyber.gouv.fr

40%

des collectivités victimes témoignent d'une interruption de service ou d'activité. 20 % de perte de destruction de données ou de perte financière.

Source : cybermalveillance.gouv.f

Cyberattaques : les plus courantes

L'hameçonnage (ou phishing)
Pratique qui consiste à envoyer des mails frauduleux.

Les rançongiciels (ou ransomware)
Programmes malveillants conçus pour extorquer de l'argent en bloquants les accès à un fichier ou à un système.

L'ingénierie sociale
Technique de manipulation psychologique pour piéger et récupérer des informations.

Déni de service
Attaque visant à altérer le fonctionnement du réseau ou à le rendre indisponible.

Main in the middle
Technique de piratage consistant à intercepter des échanges entre entités.

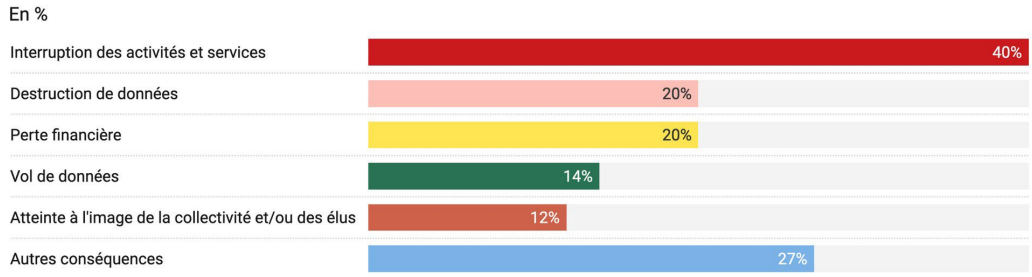
Zéro day
Faille dans le code informatique inconnue ou non corrigée par l'éditeur du produit concerné. Les pirates profitent de cette dernière pour injecter des logiciels malveillants.

SICTIAM - ACCOMPAGNEMENT

"On a vécu l'enfer , et on est encore loin d'en être sorti ".

Source : rapport de la société de sécurité Symantec

Principales conséquences des cyberattaques des collectivités



Graphique: Vie-publique.fr / DILASource: Étude- Maturité des collectivités en matière de sécurité

« Le SICTIAM apporte les meilleures réponses possibles pour améliorer les process de repérage des cyberattaques et les process de réponse et de gestion de crise lors d'une attaque. »

Les acteurs
de la cybersécurité

- SICTIAM
- Association des Maires ruraux de France des Alpes - Maritimes
- ociation des Maires et idents de munautés des s - Maritimes

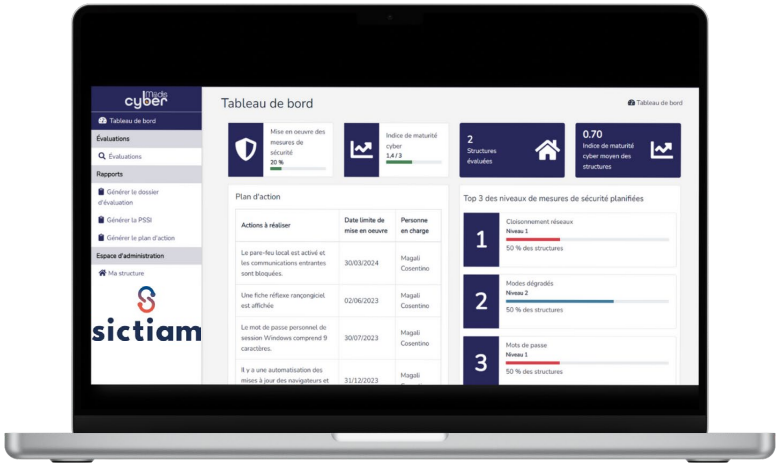
- Agence nationale de la sécurité des systèmes d'information
- Gendarmerie Nationale

SICTIAM - PARTENAIRES

Notre offre d'accompagnement cybersécurité

+de 300 personnes sensibilisées depuis 2023

Offre d'accompagnement cybersécurité



SICTIAM - ACCOMPAGNEMENT

Des réponses spécifiques pour chaque collectivité

ACCOMPAGNEMENT - SICTIAM

Intégrer la sécurité dès la conception est 10 fois moins coûteux que de sécuriser l'environnement après coup.

Aide aux collectivités
SMART DEAL

Dans le cadre du Rapport d'Aides aux collectivités et du SMART DEAL, le Conseil Départemental des Alpes-Maritimes subventionne les dépenses d'investissement des collectivités et établissements Publics.
La politique SMART Deal, portée par le Département encourage des projets qui permettront, au travers du numérique, de répondre à trois objectifs complémentaires :

- Simplifier et améliorer le fonctionnement de l'administration et des établissements pour personnes âgées et adultes en situation de handicap ;
- Accélérer la lutte contre la fracture numérique et l'acculturation au numérique des maralpins ;
- Encourager l'innovation par le numérique dans les Alpes-Maritimes.

Aide aux collectivités
SMART DEAL

https://www.departement06.fr/documents/A -votre-service/Solidarite-Territoriale/Guide_des_aides_aux_collectivites/RAC_Fiche_15.pdf

Dispositif d'aide :

Actions pouvant être soutenues	Taux de la dépense subventionnable
Ecoles primaires numériques * *(classes informatiques mobiles, tablettes et ordinateurs, tableaux ou écrans numériques interactifs serveurs, logiciels, vidéoprojecteurs, ENT, imprimantes, équipements réseaux, WIFI.*	Barème départemental
Accompagnement à l'informatisation des établissements communaux (mairies, établissements sociaux-médicaux, espaces culturels, autres espaces communaux) et des établissement de statut public habilités à l'aide sociale accueillant des personnes âgées ou adultes en situation de handicap *(matériels informatiques, logiciels de gestion, imprimantes, équipements réseau , WIFI, études liées à l'informatisation et suivies d'acquisitions).*	Barème départemental
Mise en œuvre de solutions techniques de cybersécurité visant à limiter les risques de cyberattaques (solutions antivirales, dispositifs pare-feu, réplications systèmes).	Barème départemental
Mise en œuvre de solutions numériques favorisant la relation et les interactions avec les usagers pour faciliter les démarches administratives et faire connaître le territoire dans le but de développer son attractivité et son rayonnement économique, sportif et culturel (téléservices en ligne, applications mobiles).	Barème départemental
Mise en œuvre de lieux numériques pour les usagers visant à faciliter la réalisation de leurs démarches en ligne, leurs formations au numérique ou le coworking (mobilier et travaux associés, matériels informatiques, équipements réseaux, WIFI, études d'aménagement type « design thinking » préalables à des opérations).	Barème départemental
Mise en œuvre de solutions numériques innovantes pour un « territoire intelligent et durable » notamment pour permettre une meilleure gestion énergétique des installations techniques (éclairage public, maîtrise énergétique des bâtiments) ou de l'espace public (espaces verts, gestion des déchets, gestion de la circulation) *Ex : capteurs, solutions de traitement des données.*	Barème départemental
Mise en oeuvre de solutions d'intelligence artificielle permettant une amélioration de l'efficience de l'action publique (science de la donnée, apprentissage machine).	Barème départemental

*** Ecoles primaires numériques : pour le développement du numérique dans les écoles, le SICTIAM peut accompagner les projets des communes notamment via la centrale d'achat et le marché « école numérique » notamment dans :**

- l'aide à l'élaboration et à la concrétisation des projets pédagogiques autour du « socle numérique » ;
- la préconisation et l'assistance dans le choix des équipements conformes au projet pédagogique choisi ;
- le pilotage de la mise en service des équipements jusqu'à la formation des enseignants à leur utilisation ;
- le pilotage de la maintenance des équipements mis en service pour en garantir sa pérennité.

SICTIAM - SUBVENTIONS

Le Conseil de Développement remercie tout particulièrement Messieurs Gilbert Barrot et José Ammendola pour leurs contributions à la rédaction de cette annexe.