ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

2025

RAPPORT DE VULNÉRABILITÉS ET D'INCIDENTS

VULNÉRABILITÉS ET INCIDENTS DU CYBERESPACE BÉNINOIS.

Sommaire

Glossaire

Antivirus : Programme qui protège un ordinateur contre les logiciels malveillants.

ASIN : Agence des Systèmes d'Information et du Numérique.

Audit : Vérification méthodique d'un système ou d'une organisation pour évaluer sa conformité ou ses vulnérabilités.

Authentification : Processus permettant de confirmer l'identité d'un utilisateur.

Backdoor (Porte dérobée) : Accès secret laissé dans un système pour en prendre le contrôle.

Botnet : Réseau d'ordinateurs infectés contrôlés à distance par un acteur malveillant pour mener des activités nuisibles, comme des attaques DDoS.

bjCSIRT : Équipe nationale de réponse aux incidents de sécurité informatique du Bénin.

Brute force : Méthode d'attaque qui tente toutes les combinaisons possibles pour trouver un mot de passe.

CMS (Content Management System) : Outil pour créer et gérer des sites web.

Cross-Site Scripting (XSS) : Vulnérabilité qui permet à un attaquant d'injecter du code malveillant dans une application, pour qu'il soit interprété par un autre utilisateur ou par le système lui-même, compromettant ainsi la sécurité des données ou le fonctionnement de l'application.

CSRF (Cross-Site Request Forgery) : Attaque où l'utilisateur exécute une action à son insu sur un site authentifié.

DDoS : Attaque visant à rendre un service indisponible en le submergeant de trafic provenant de multiples sources, souvent via un botnet.

Défacement : Attaque qui consiste à compromettre l'intégrité d'un site web, en modifiant son contenu ou son apparence.

Injection SQL : Faille permettant à un acteur malveillant d'accéder ou de modifier une base de données par injection de commande injection dans une application web.

Malware : Logiciel malveillant (virus, trojan, ransomware, etc.).

OIIC : Opérateurs d'Infrastructures d'Information Critique.

Hameçonnage : Technique d'arnaque visant à obtenir des données personnelles en se faisant passer pour un service légitime.

PPIIC : Politique de Protection des Infrastructures d'Information Critiques.

PSSIE : Politique de Sécurité des Systèmes d'Information de l'Etat.

RCE (Remote Code Execution) : Exécution d'un code malveillant à distance sur un serveur.

RSSI : Responsable de la Sécurité des Systèmes d'Information.

SIEM : Solution centralisée qui collecte, corrèle et analyse en temps réel les journaux et événements de sécurité provenant de divers systèmes pour détecter les incidents de sécurité..

SPF / DKIM / DMARC : Protocoles qui permettent de vérifier l'authenticité d'un email.

SSRF : Attaque exploitant un serveur pour accéder à des ressources internes ou interdites.

Token CSRF : Jeton unique généré par une application web pour vérifier qu'une requête provient bien d'un utilisateur légitime.

WAF (Web Application Firewall) : Pare-feu dédié à la protection des applications web.

Message du **Directeur Général** de l'**ASIN**

Marc André
LOKO

Il est perceptible que l'ASIN impacte à travers ses actions, tous les secteurs d'activité clés du tissu productif national. Au regard du vaste programme de dématérialisation entrepris par le gouvernement, il est absolument nécessaire que l'ASIN fasse de la sécurité des différentes infrastructures numériques une priorité de haut rang. C'est pourquoi à travers son organigramme, elle a érigé un pôle sécurité numérique qui veille inlassablement au quotidien à la sécurité et la résilience des infrastructures.

Après bientôt trois années d'activités, il s'avère nécessaire de partager avec l'ensemble des acteurs de l'écosystème du numérique, les chercheurs, les scientifiques, les acteurs des médias, les curieux et amoureux du numérique, à travers ce premier rapport, les malveillances que les équipes ont affrontées. Classiquement, les malveillances sont constituées par la fraude, le détournement, le vol, l'endommagement, l'utilisation non autorisée, et le refus de service. Nos équipes ont été confrontées à ces formes de malveillance, ont accompagné d'autres acteurs dont les systèmes ont été menacés, et ont même identifié des attaques passées dont les victimes ignoraient l'existence.

Ce premier rapport n'a pas la prétention d'apporter une ou des solutions applicables systématiquement à des situations qui pourraient être en cours dans des organisations. Toutefois, pour palier ou faire efficacement face aux éventuels cybers incidents qui pourraient affecter les organisations publiques ou privées dans notre pays le Bénin, ce rapport vise à informer, à sensibiliser sur l'existence réelle de cyber menaces, leur typologie, les premiers réflexes à avoir lorsque l'on a la charge de la sécurité des systèmes d'information d'une organisation et enfin, la possibilité de recourir sur le plan national à de l'expertise. En outre, ce rapport contribuera à rassurer les citoyens, les clients et autres usagers des différents services dématérialisés et des autres à venir. Enfin, il y a lieu de considérer ce rapport comme un document élaboré pour servir de boussole à notre action quotidienne de sorte que nos équipes, eu égard à l'ampleur des risques, soient en mesure de développer davantage de capacité et surtout d'anticiper.

En ma qualité de Directeur Général, je m'engage à œuvrer avec tous mes collaborateurs à différents niveaux afin que nos procédures et actions de prévention et de gestion des cyber incidents soient au mieux documentés et organisés avec succès pour garantir la sécurité des différents services dématérialisés, des systèmes et infrastructures d'information dans notre pays de manière à constituer un modèle régional.

Enfin, je nourris l'espoir que le présent rapport comblera des attentes légitimes et les prochaines parutions prendront en compte les retours qui nous parviendront à la suite de cette publication.

Ensemble, œuvrons pour un Bénin numériquement sécurisé.

À PROPOS DE L'ASIN

1. INTRODUCTION

A l'ère de la transformation numérique, la sécurité des systèmes d'information et des infrastructures d'information critiques est devenue un enjeu crucial. La digitalisation offre des opportunités indéniables en matière de modernisation, d'efficacité administrative et d'accessibilité des services. Toutefois, elle expose le cyberespace béninois à de nombreux risques, allant des simples erreurs de configuration aux cyberattaques les plus sophistiquées.

Aujourd'hui, grâce aux efforts déployés dans le cadre du Programme d'Action du Gouvernement (PAG 1 & 2), de nombreuses structures publiques utilisent des plateformes numériques pour la gestion de leurs données, la communication avec les usagers ou encore la fourniture de services en ligne. Cette prolifération numérique implique une dépendance technologique et une augmentation de la surface d'attaque du cyberespace béninois à tel point que la moindre faille ou cyberattaque peut avoir des conséquences graves sur la confidentialité, l'intégrité et la disponibilité des données, mais aussi sur la continuité des activités et la confiance des citoyens.

Face à cette réalité, il est devenu essentiel d'évaluer régulièrement la posture de la sécurité des institutions officielles et des opérateurs d'infrastructures d'information critiques (OIIC). Ce rapport vise à partager les données statistiques sur les vulnérabilités identifiées au cours des années antérieures, tout en proposant des axes d'amélioration simples et réalistes. Il s'adresse à tous les acteurs, de l'écosystème, impliqués dans la gestion des systèmes d'information, mais aussi aux décideurs afin de mieux orienter les politiques et les investissements en cybersécurité.

Enfin, ce rapport présente une analyse des vulnérabilités identifiées relatives aux systèmes d'informations des institutions étatiques du Bénin et des OIIC, entre 2021 et 2024. Il s'appuie sur les données collectées par les services techniques compétents de l'Agence des Systèmes d'Information et du Numérique, en particulier le bjCSIRT, pour mieux comprendre les failles de sécurité, les types d'attaques subies et les secteurs les plus touchés. L'objectif est de proposer des solutions concrètes pour améliorer la protection des systèmes informatiques de l'État.

2. OBJECTIFS DU RAPPORT

Ce rapport de vulnérabilités et d'incidents vise à présenter une analyse des données statistiques relevés entre 2021 et 2024 sur les constituants des équipes de l'ASIN. Il s'inscrit dans une logique d'aide à la décision et de renforcement des capacités collectives face à l'évolution rapide des menaces numériques. Les données proviennent du pôle sécurité de l'ASIN, qui gère les normes et la conformité en matière de sécurité informatique, ainsi que de l'équipe de réponses aux incidents de sécurité informatique (bjCSIRT).

De manière spécifique, il s'agit de :

- Dresser un **bilan consolidé** des vulnérabilités documentées, en identifiant leurs causes techniques et organisationnelles ainsi que leur répartition par secteur ;
- Présenter une **cartographie des principales menaces** observées, notamment les incidents, avec un focus particulier sur les fuites de mots de passe ;
- Formuler des **recommandations** pour améliorer la posture de la cybersécurité des institutions officielles et des opérateurs d'infrastructures d'information critique (OIIC) ;

Ce rapport entend ainsi contribuer à une meilleure compréhension des défis cyber du pays, tout en soutenant les efforts de transformation numérique de l'État béninois.

3. CIBLES

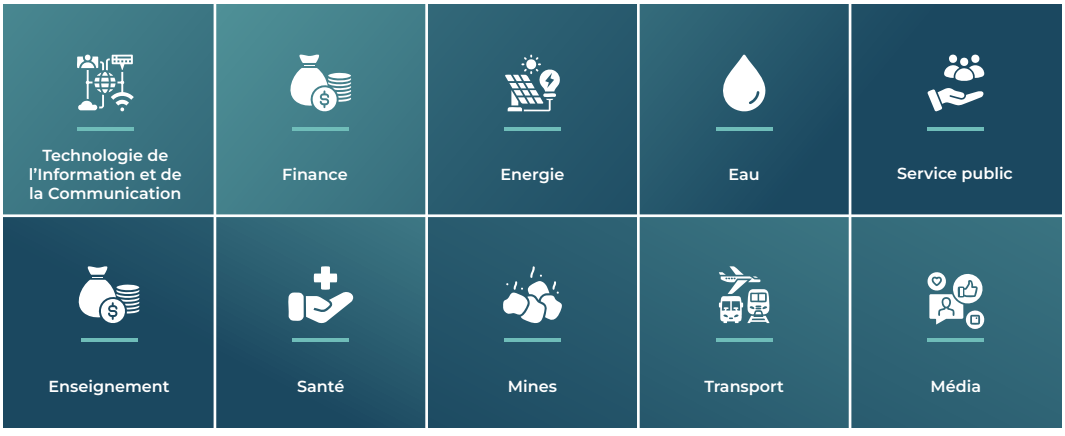
Ce rapport s'adresse en priorité aux :

- ✓✓ Décideurs des systèmes d'information des institutions officielles et OIIC ;
- ✓✓ Fournisseurs de services de sécurité numérique qualifiés (FSSNQ) ;
- ✓✓ Consultants et cabinets du secteur de cybersécurité.
- ✓✓ Responsables de la sécurité des systèmes d'information ;
- ✓✓ Chercheurs ou étudiants à la quette de données statistiques sur les vulnérabilités ;

Au-delà de ces profils, ce rapport s'adresse **à toute personne intéressée par les enjeux de cybersécurité dans le secteur public.**

Par ailleurs, ce rapport concerne les secteurs identifiés par la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) et la Politique de Protection des Infrastructures d'Information Critiques (PPIIC).

Ces secteurs sont :



Dans le cadre de cette étude, le secteur **Service Public** désigne l'ensemble des institutions étatiques et organismes publics chargés de la gestion des affaires publiques et de l'exercice des fonctions de l'État.

4. CADRE MÉTHODOLOGIQUE

L'élaboration de ce rapport repose sur une méthodologie, combinant collecte d'informations, traitement analytique et validation par des experts techniques.

ÉTAPE 1 — Collecte des données

A cette étape, les données statistiques ont été collectées de 2021 à 2024 à partir des sources suivantes :

- rapports d'incidents et d'interventions du bjCSIRT ;
- rapports hebdomadaires de monitoring et annuels du bjCSIRT ;
- mémos de sécurité du bjCSIRT ;
- bulletins d'alertes du bjCSIRT ;
- rapports d'audit organisationnel et de conformité.

ÉTAPE 2 — Validation des données collectées

A cette étape, un processus de validation a été suivi afin de s'assurer que les données collectées sont intègres par rapport à la source.

ÉTAPE 3 — Analyse des données collectées

Après la validation des données collectées, a suivi l'étape de l'analyse. A cette étape, les données ont été corrélées, classifiées selon leur type, et regroupées par année et par secteur d'activité.

ÉTAPE 4 — Rédaction du rapport

A cette étape, ledit rapport a été rédigé en intégrant les graphes issus de l'analyse des données collectées.

5. CADRE MÉTHODOLOGIQUE

Le présent rapport couvre les vulnérabilités et incidents identifiés sur les constituants du bjCSIRT conformément à son RFC 2350, à savoir :

- les ministères du gouvernement ;
- les agences gouvernementales ;
- les institutions de la République établies par la constitution ;
- les opérateurs d'Infrastructures d'Information Critiques (OIIC).

Dans ce présent rapport, les ministères du gouvernement, les agences gouvernementales et les institutions de la République établies par la constitution seront nommés les institutions officielles.

6. RESTRICTIONS ET LIMITES

Malgré la rigueur méthodologique appliquée, certaines limitations doivent être prises en compte :

- Ce rapport se base sur les incidents, attaques et vulnérabilités déclarés ou identifiés par le bjCSIRT.
- le secteur privé n'est pas concerné par ce rapport sauf les opérateurs d'infrastructures d'information critiques privés.

7. ANALYSE DES VULNÉRABILITÉS

L'analyse approfondie des vulnérabilités sur la période 2021–2024 révèle un total de huit cent soixante-dix-huit **(878) vulnérabilités** identifiées sur les systèmes d'information des institutions officielles et des OIIC. Parmi celles-ci :

30% ont un risque faible **(268 cas)** ;

23% ont un risque faible **(200 cas)** ;

24% ont un risque faible **(203 cas)** ;

23% ont un risque faible **(207 cas)**.

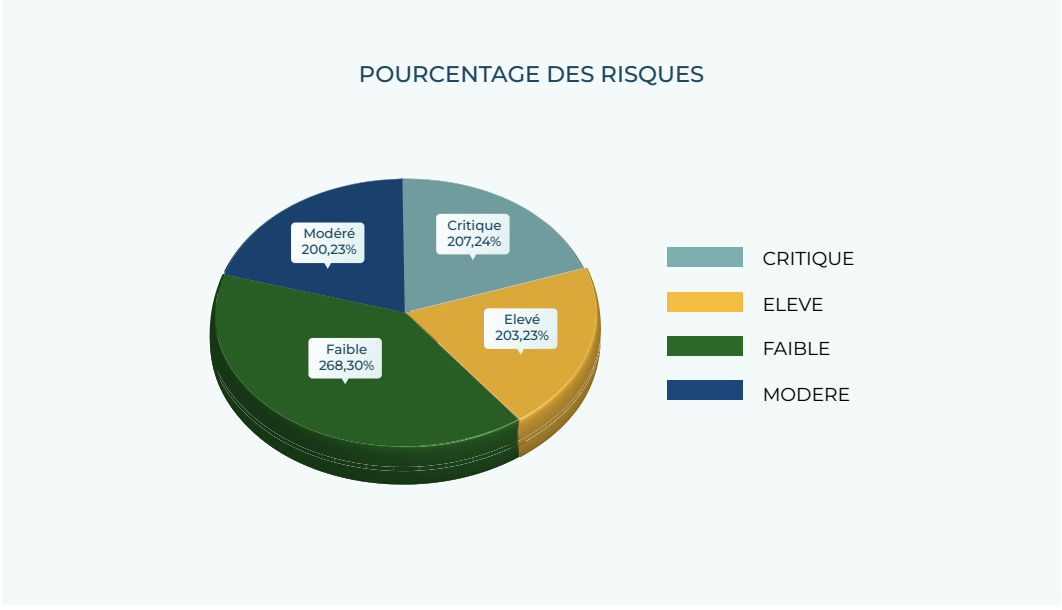


Figure 1 : Répartition des vulnérabilités selon le niveau de risque

a Analyse des vulnérabilités critiques

Une étude spécifique a été menée sur les vulnérabilités classées comme critique selon la grille d'évaluation du bjCSIRT disponible en annexe. Ces failles présentent une probabilité d'exploitation élevée et des impacts élevés sur la confidentialité, l'intégrité ou la disponibilité des systèmes.

Principales vulnérabilités critiques identifiées :

- **Broken Access Control (41 cas) :** Mauvaise gestion des autorisations donnant lieu à des accès non autorisés à des fonctions ou ressources critiques ;
- **Sensitive Information Disclosure (26 cas) :** Fuite de données confidentielles via logs, erreurs HTTP, ou fichiers accessibles publiquement ;
- **Broken Authentication (24 cas) :** Failles dans les mécanismes d'authentification permettant le contournement d'accès ou l'usurpation d'identité ;
- **Remote Code Execution (RCE) (23 cas) :** exécution de commandes arbitraires à distance ;
- **SQL Injection (18 cas) :** Vulnérabilité permettant d'injecter des requêtes malveillantes dans une base de données, en manipulant les entrées utilisateurs pour accéder, modifier ou supprimer des données de manière non autorisée.

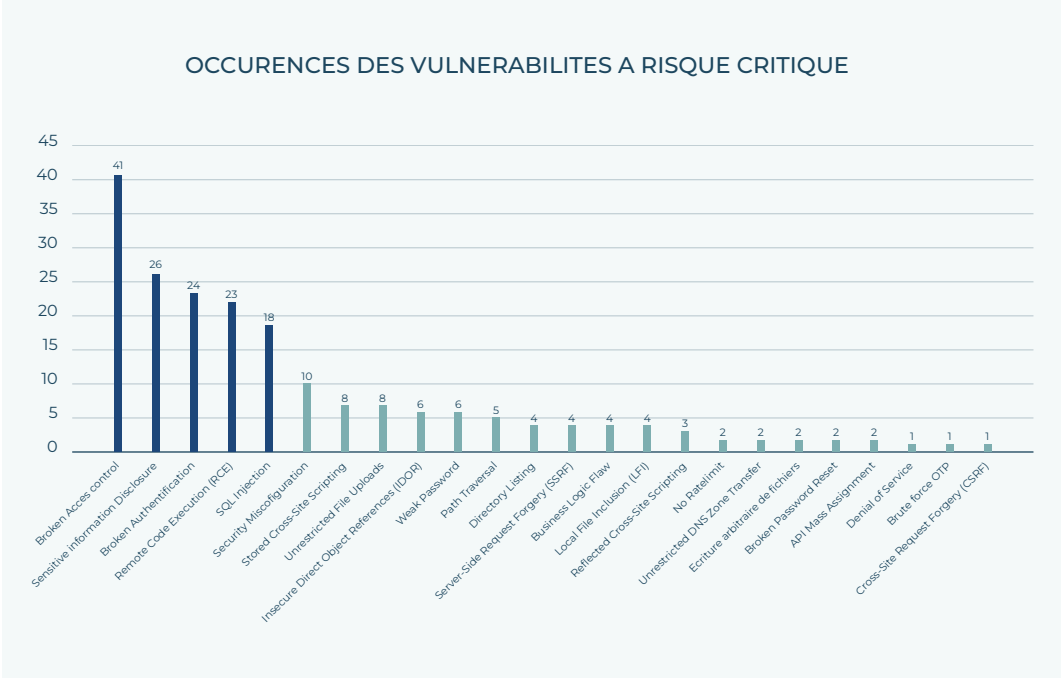


Figure 2 : Occurrences des vulnérabilités à risque critique

b Répartition sectorielle des vulnérabilités critiques

Une analyse approfondie des données a permis d'identifier les secteurs ayant été touchés par les vulnérabilités critiques :

Vulnérabilités	Secteurs les plus touchés		
Broken Access Control	Service Public : **28**	Numérique : **14**	Finance/Santé : **11**
Sensitive Information Disclosure	Service Public : **62**	Finance : **35**	Numérique : **19**
Broken Authentication	Service Public : **15**	Agriculture : **9**	Finance : **7**
Remote Code Execution (RCE)	Service Public : **9**	Finance : **9**	Numérique : **6**
SQL Injection	Finance : **7**	Service Public : **5**	Énergie/Enseignement : **2**

Il est également à noter que :

le Service Public concentre systématiquement le plus grand nombre de failles critiques ;

les secteurs Finance, Numérique et Digitalisation, et dans une moindre mesure le secteur Santé, présentent aussi une forte exposition aux risques critiques ;

le secteur Agricole, bien que moins attendu, apparaît également vulnérable sur des aspects fondamentaux comme l'authentification et la divulgation d'informations.

BROKEN ACCES CONTROL

SECTEURS TOUCHÉS PAR : BROKEN ACCES CONTROL

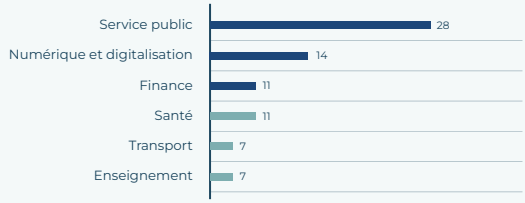


Figure 3 : Secteurs touchés par : "Broken Access Control"

SENSITIVE INFORMATION DISCLOSURE

SECTEURS TOUCHÉS PAR : SENSITIVE INFORMATION DISCLOSURE

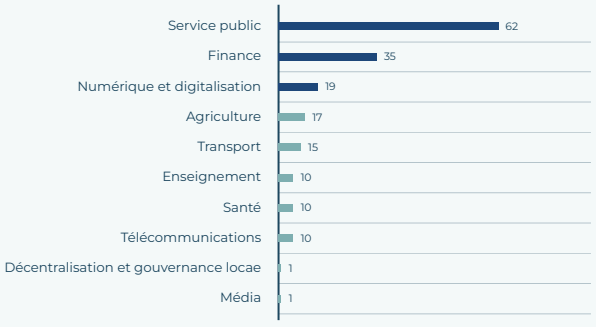


Figure 4 : Secteurs touchés par : "Sensitive Information Disclosure"

BROKEN AUTHENTIFICATION

SECTEURS TOUCHÉS PAR : BROKEN AUTHENTIFICATION

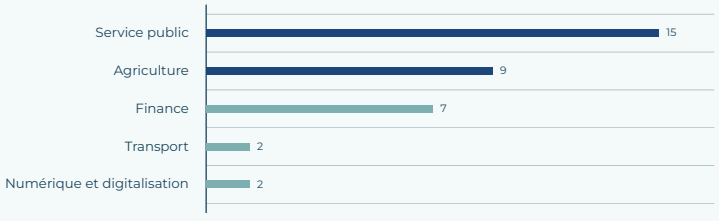


Figure 5 : Secteurs touchés par : "Broken Authentication"

REMOTE CODE EXECUTION (RCE)

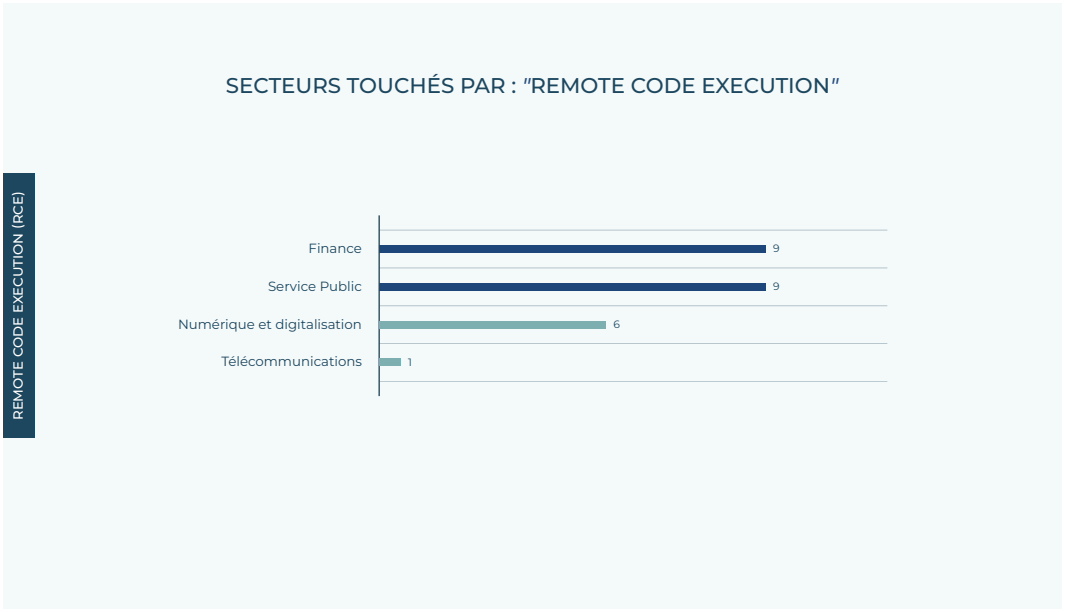


Figure 6 : Secteurs touchés par : "Remote Code Execution"

SQL INJECTION

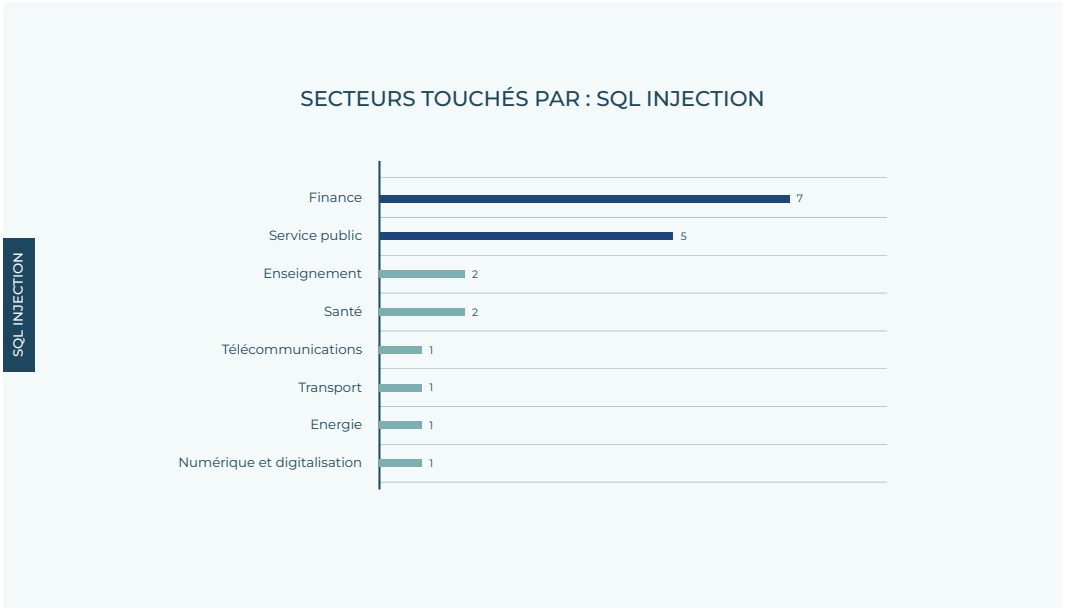


Figure 7 : Secteurs touchés par : "SQL Injection"

En ce qui concerne la classification des vulnérabilités par secteur, on observe les cinq secteurs les plus touchés, à savoir :

Service Public : **326**	Finance : **155**	Numérique et Digitalisation : **117**	Transport : **84**
Enseignement : **72**			

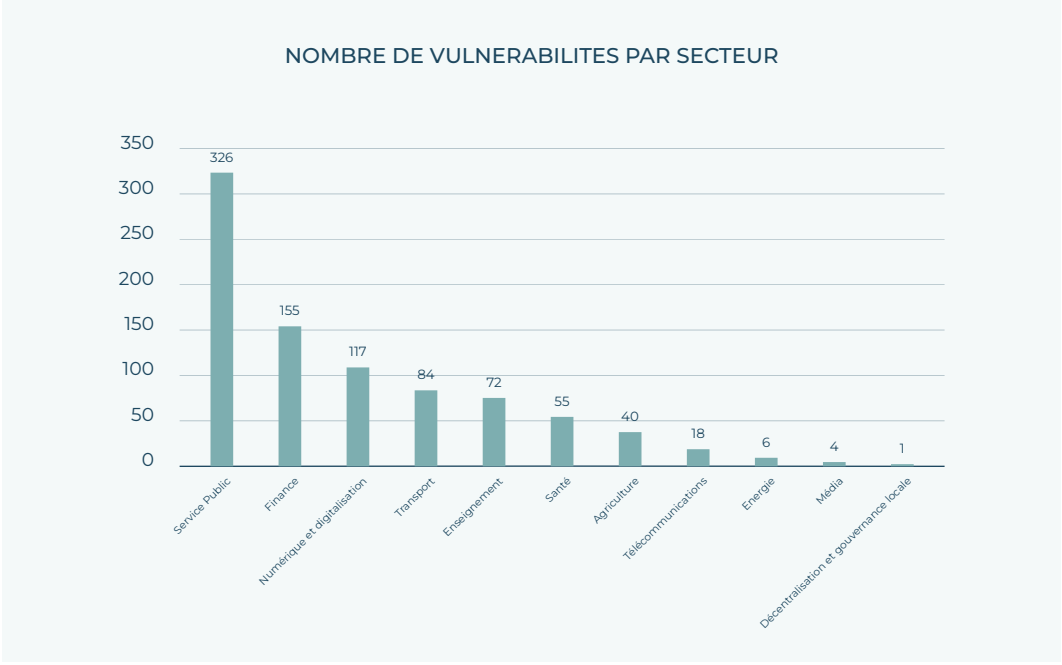


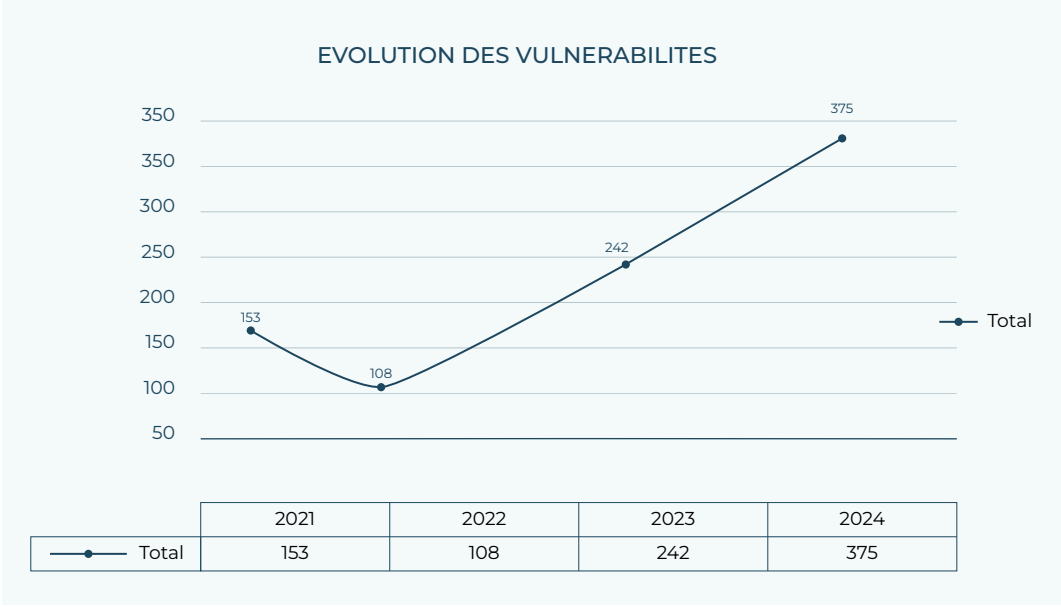
Figure 8 : Nombre de vulnérabilités par secteur

55% **Des secteurs sont touchés par des vulnérabilités**

Les secteurs **Service Public** et **Finance** sont à eux seuls touchés par plus de **50% des vulnérabilités recensées**.

C Évolution des vulnérabilités

Au regard des données collectées entre 2021 et 2024, la situation de la cybersécurité dans les institutions publiques béninoises reste préoccupante. Le nombre total de vulnérabilités recensées est passé de cent cinquante-neuf (159) en 2021 à trois cent soixante-quinze (375) en 2024, marquant une croissance significative et continue.



	2021	2022	2023	2024
Total	153	108	242	375

***Figure 9 :** Évolution des vulnérabilités de 2021 à 2024*

d Causes des vulnérabilités

Les causes techniques les plus fréquentes sont :

- **Mauvaise configuration des paramètres de sécurité :** deux cent quatre-vingt-seize (296) occurrences ;
- **Mauvaise gestion des rôles et des permissions :** cent quarante-deux (142) occurrences ;
- **Mauvaise gestion des entrées utilisateurs :** cent trente-cinq (135) occurrences ;
- **Absence de token CSRF :** soixante-neuf (69) occurrences ;
- **Exposition de fichiers sensibles sans restriction :** soixante et une (61) occurrences.

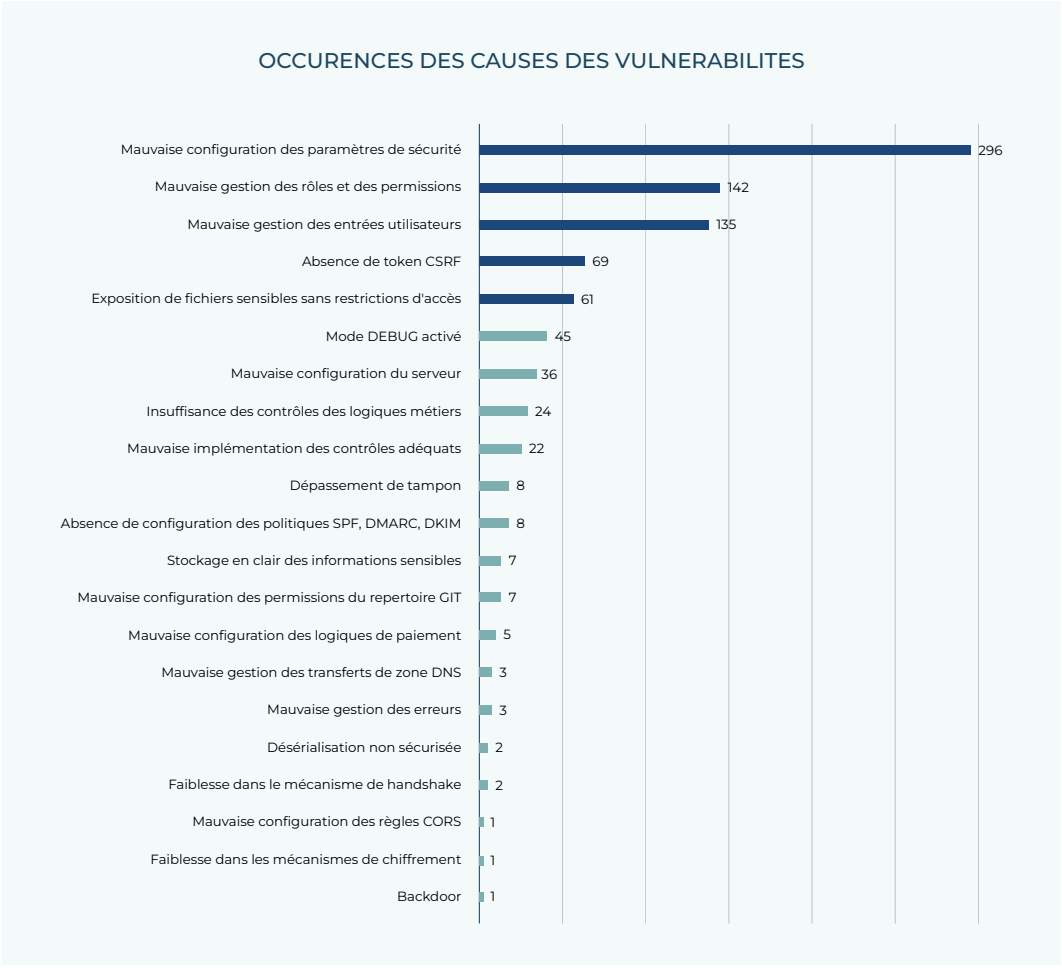


***Figure 10 :** Occurrences des causes des vulnérabilités*

Cette augmentation flagrante de vulnérabilités peut s'expliquer par :

- la multiplication des plateformes et services numériques dans l'administration ;
- la vétusté persistante des systèmes en production ;
- la non-maintenance des applications, qui laisse des failles de sécurité non corrigées ;
- le manque de Responsable à la Sécurité des Systèmes d'Informations (RSSI) dans certaines entités ;
- des ressources limitées pour la gestion de la sécurité, qui retardent la mise en place des correctifs nécessaires.

8. ANALYSE DES INCIDENTS

a Les fuites de mots de passe

Plusieurs institutions ont été confrontées à des fuites de mots de passe. Ces fuites, souvent causées par une mauvaise gestion des identifiants, les logiciels malveillants, l'utilisation des mêmes identifiants sur plusieurs plateformes ou un partage non sécurisé ; touchent en particulier les secteurs : **Finances, Service Public, Enseignement, Santé et Numérique et digitalisation.** Au total, plus de huit cent trente-deux **(832) cas** de fuites ont été recensés, dont :

- **Finance :** quatre cent six (406) cas ;
- **Service Public :** deux cent vingt-six (226) cas ;
- **Enseignement :** cent (100) cas ;
- **Santé :** cinquante-huit (58) cas ;
- **Numérique et digitalisation :** dix (17) cas.

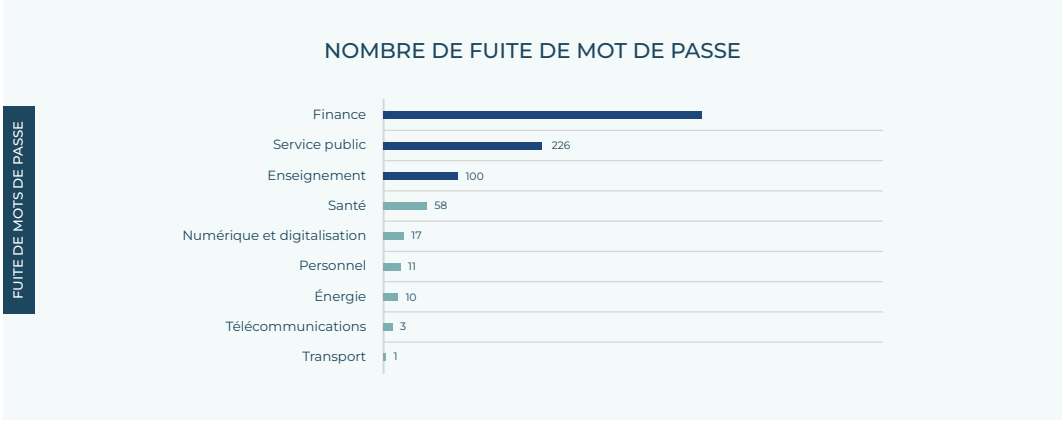


***Figure 11 :** Nombre de fuites de mot de passe par secteur*

45% **Des secteurs sont touchés par des fuites de mots de passe**

Ces fuites constituent souvent des vecteurs d'intrusion majeurs, facilitant les attaques ciblées, l'usurpation d'identité ou encore les campagnes d'hameçonnages.

b Causes des incidents

L'analyse des incidents survenus, sur les systèmes d'information ou sur les infrastructures d'information des institutions officielles et OIIC entre 2021 et 2024, met en lumière une diversité de causes, reflétant à la fois des lacunes techniques, organisationnelles et humaines. Les principales origines identifiées sont :

Causes prédominantes :

- **Utilisation de logiciels obsolètes (6 cas) :** Plusieurs structures utilisent encore des solutions logicielles non maintenues (CMS, OS, bibliothèques vulnérables), exposées à des vulnérabilités non corrigées faute de support actif ;
- **Correctifs de sécurité non appliqués (5 cas) :** Des failles ne sont pas mises à jour en temps opportun. Cela traduit une absence de processus formel de gestion des vulnérabilités ;
- **Manque de sensibilisation du personnel (5 cas) :** La méconnaissance des risques de sécurité conduit à des erreurs humaines fréquentes (clics sur des liens frauduleux, partage de mots de passe, etc.), facilitant les compromissions ;
- **Non-respect de l'hygiène numérique (4 cas) :** Issue d'une mauvaise hygiène numérique (absence de MFA, mots de passe faibles ou réutilisés) ou de compromissions antérieures non traitées ;
- **Cyberattaques ciblées (3 cas) :** Des attaques personnalisées, souvent via des mails malveillants ou de l'ingénierie sociale, ont visé spécifiquement certaines structures ou profils sensibles.

Autres causes :

- **Espaces d'hébergement partagés infectés** (2 cas) ;
- **Porte dérobée laissée active** (2 cas) ;
- **Mauvaise gestion des accès** (2 cas) ;
- **Configurations techniques erronées** (2 cas) ;
- **Absence de configuration de politiques de sécurité (SPF, DKIM, etc.)** (1 cas) ;
- **Tentative de brute force, service FTP ouvert, plugin malveillant, clé USB infectée** (1 cas chacun).

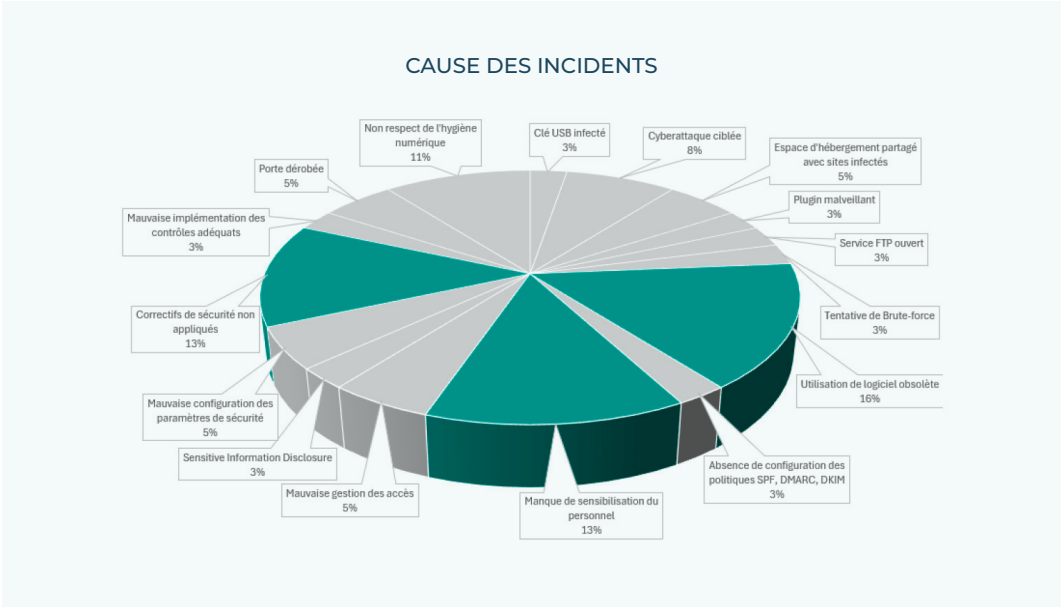


Figure 12 : *Causes des incidents de cybersécurité*

C Les fuites de mots de passe

L'étude des incidents déclarés ou identifiés a permis de dresser un panorama des menaces réelles auxquelles sont confrontées les entités concernées par ce rapport. Les incidents de type malware infection, piratage de site web et botnet sont les plus recensés.

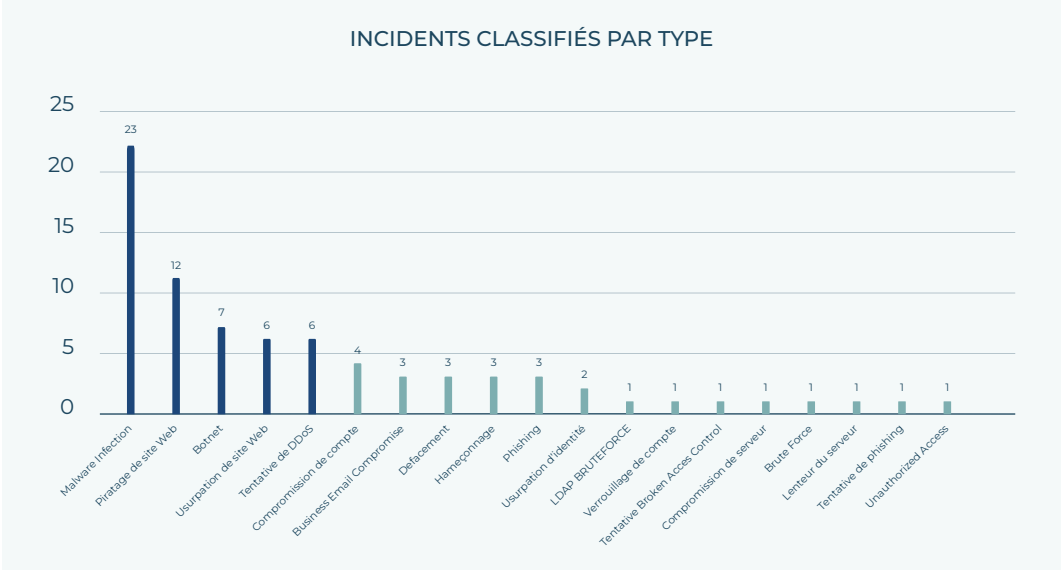


Figure 13 : *Incidents de cybersécurité classifiés par type*

Incidents les plus fréquents :

- **Malware Infection (23 cas) :** Détection de codes malveillants introduits par clé USB, plugin infecté, ou à la suite d'un téléchargement frauduleux ;
- **Piratage de site Web (12 cas) :** Résultant de failles d'injection, de mauvaises configurations ou de CMS non à jour ;
- **Botnet (7 cas) :** Présence de machines compromises intégrées à des réseaux de botnets, souvent à l'insu des responsables systèmes ;
- **Tentatives de DDoS (6 cas) :** Des pics de trafic anormaux ont été enregistrés sur des services critiques, provoquant des ralentissements ou des indisponibilités temporaires ;
- **Usurpation de site Web (6 cas) :** Création de copie frauduleuse d'un site légitime pour tromper les utilisateurs.

Incidents les plus fréquents :

- **Compromission de compte utilisateur ou serveur** (4 cas) ;
- **Défacement (altération de l'apparence de sites web)** (3 cas) ;
- **Usurpation d'identité numérique** (2 cas) ;
- Utilisation de comptes non autorisés, tentative d'escalade de privilèges, injection SQL, etc.

La prédominance des attaques basées sur **l'erreur humaine**, les **failles d'authentification** démontrent que les attaquants ciblent en priorité les faiblesses les plus accessibles. Dans plusieurs cas, l'incident aurait pu être évité par :

- La mise en œuvre de l'authentification multi-facteur ;
- La limitation du nombre de tentatives de connexion ;
- Le renforcement des campagnes de sensibilisation ;
- Une détection précoce d'activités suspectes via journaux ou SIEM.

d Classification des types attaques par secteur

Les données collectées ont permis de classifier les types d'attaques par secteur, notamment les infections par logiciels malveillants et les compromissions de sites web.

Infections par logiciels malveillants

Les attaques de type infections par **logiciels malveillants** ont touché plusieurs secteurs, avec une concentration particulière sur :

- **Service Public (9 cas) :** Infection fréquente via périphériques externes (clés USB), téléchargements de logiciels de sources inconnues ou pièces jointes infectées. Le manque de filtrage réseau ou de protection EDR contribue à la propagation ;
- **Finance (9 cas) :** Le secteur financier, très ciblé pour ses données sensibles, est exposé aux trojans bancaires, ransomwares et autres malwares furtifs ;
- **Secteur de l'Eau (3 cas) :** Bien qu'inattendu, ce secteur a enregistré plusieurs infections ;
- **Numérique et Digitalisation / Transport (1 cas chacun) :** Présence ponctuelle, souvent liée à des configurations faibles ou des utilisateurs non sensibilisés et non formés.

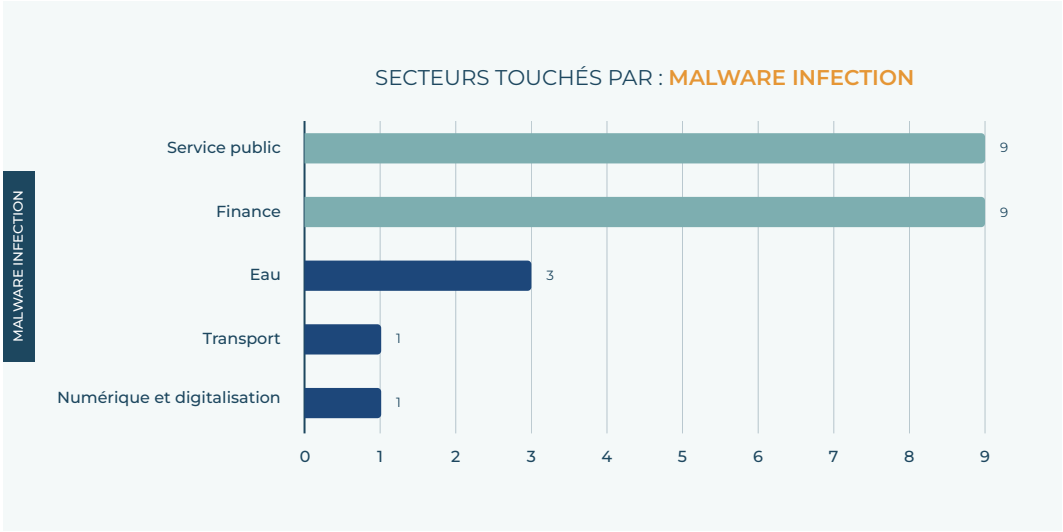


Figure 14 : Secteurs touchés par : Malware Infection

Ces infections soulignent l'absence d'une politique de **filtrage et de contrôle des périphériques**, de **mises à jour d'antivirus centralisées**, et d'**isolement réseau** pour limiter les propagations.

Ce type d'attaque renvoie à une **prise de contrôle partielle ou totale** de sites web institutionnels, souvent pour du défacement ou l'injection de scripts malveillants.

- **Service Public (6 cas) :** Fortement touché en raison du nombre élevé de sites publiés ;
- **Finance (4 cas) :** secteur stratégique, où une défiguration ou compromission peut affecter la crédibilité institutionnelle ;
- **Santé / Enseignement (1 cas chacun) :** les plateformes périphériques ne sont pas exemptes de risques, surtout si elles sont conçues avec des CMS vulnérables ou non mis à jour.

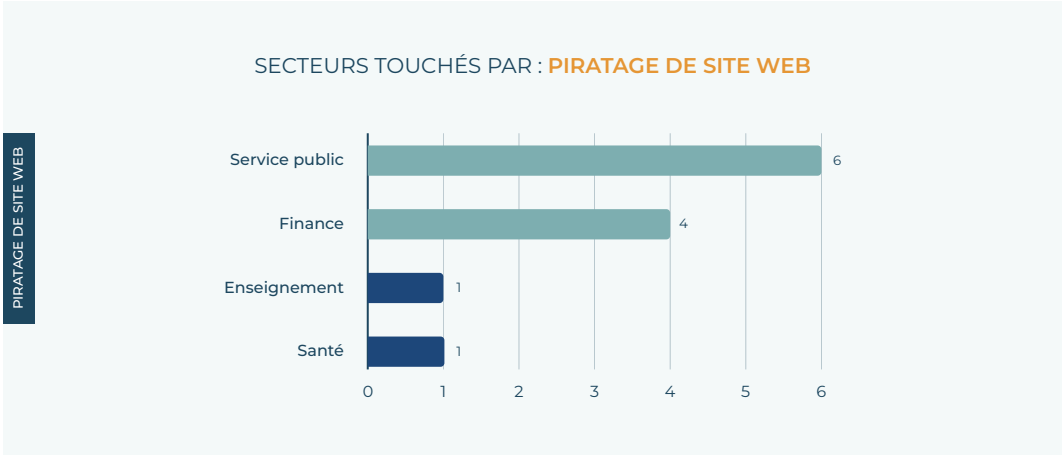


Figure 15 : Secteurs touchés par : Piratage de site web

e Evolution des attaques

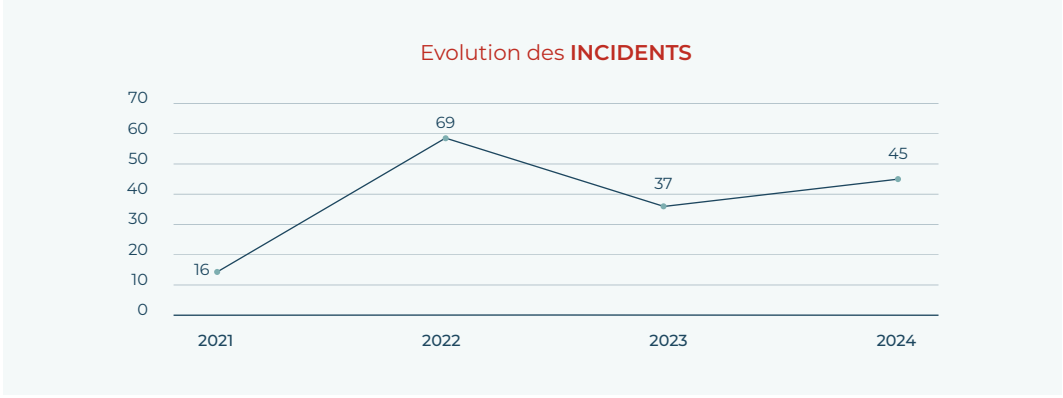


Figure 16 : Évolution des attaques de 2021 à 2024

Le pic de 2022 constitue un point critique, avec cinquante-neuf (59) incidents déclarés, contre seize (16) en 2021. Cette flambée pourrait traduire :

- Une meilleure capacité de détection et de remontée des incidents ;
- Ou une réelle intensification des attaques ciblées contre les systèmes publics.

Les causes profondes sont bien identifiées : défauts de configuration, absence de correctifs de sécurité, mauvaise gestion des accès, ou encore sensibilisation insuffisante du personnel. La majorité des incidents graves comme les fuites de données, le piratage de sites web ou les infections par logiciels malveillants trouvent leur origine dans des failles techniques et organisationnelles largement évitables.

9. LES ÉCARTS DE CONFORMITÉ À LA PSSIE

Parmi les facteurs qui pourraient expliquer la persistance des vulnérabilités et la répétition des incidents dans les institutions publiques, **le niveau de conformité à la PSSIE** apparaît comme un élément déterminant. Cette politique, conçue pour encadrer la sécurité des systèmes d'information de l'État, prévoit un ensemble de mesures structurantes (gouvernance, politiques internes, contrôles techniques, suivi des incidents, etc.). Lorsque sa mise en œuvre est partielle, absente ou mal comprise, cela peut conduire à des environnements peu sécurisés, laissant place à des failles facilement exploitables.

En effet, après l'adoption de la PSSIE par le décret N° 2021-550 du 27 octobre 2021, l'ASIN s'est lancée dans une démarche d'accompagnement de vingt-cinq (25) structures prioritaires en commanditant des audits de conformité de leur système d'information avec la PSSIE.

Ces audits ont permis de faire un état des lieux de la sécurité des systèmes d'information desdites structures en relevant notamment différents écarts et en déterminants des taux de conformité.

a Panorama des écarts de conformité

Pour l'ensemble des structures auditées, nous avons recensé dans le tableau ci-dessous, les écarts de conformité les plus courants :

N°	Domaine de la PSSIE	Écart de conformité
1	Organisation de la sécurité du système d'information	◢ Absence de comité de sécurité ◢ Absence de charte définissant les responsabilités des administrateurs informatiques ◢ Absence de procédure de veille de sécurité ◢ Absence de nomination des RSSI ◢ Absence de relation formelle avec l'ASIN
2	Sécurité des ressources humaines	◢ Absence de procédures de gestion des départs et de la mobilité ◢ Manque de sensibilisation et de formation en ce qui concerne les bonnes pratiques en matière de sécurité des systèmes d'information. ◢ Absence de procédures de gestion des sanctions en cas de violation de la PSSI ◢ Pas de circuit formalisé d'intégration des nouvelles recrues ◢ Absence de vérification des antécédents (background check) ◢ Absence d'un cycle de formation régulier
3	Gestion des actifs du système d'information	◢ Absence de procédures de gestion des actifs et de leur cycle de vie ◢ Responsable d'actifs SI non identifié. ◢ Absence de charte de bonne utilisation des systèmes d'information ◢ Absence de classification des actifs ◢ Absence de procédures de gestion des supports numériques. ◢ Absence des mesures de chiffrement des données

N°	Domaine de la PSSIE	Écart de conformité
4	Contrôle d'accès logique au système d'information	◢ Absence de politiques et procédures formalisées sur le contrôle d'accès ◢ Absence de politiques et de gestion des mots de passe ◢ Manque de sécurisation et de supervision des accès
5	Sécurité physique des locaux abritant les actifs SI	◢ Absence de procédures de gestion des accès physiques ◢ Absence de procédure sur l'encadrement des visites dans les locaux techniques ◢ Absence de consignes de sécurité dans les locaux abritant les actifs SI ◢ Absence de gestion formalisée des actifs des locaux techniques.
6	Sécurité des réseaux informatiques	◢ Cloisonnement insuffisant des réseaux ◢ Absence de contrôle des flux et des accès réseau ◢ Absence de durcissement des équipements ◢ Absence de gestion centralisée des interconnexions avec les réseaux externes ◢ Absence de supervision des réseaux
7	Sécurité du poste de travail utilisateur	◢ Absence de processus de gestion des postes de travail ◢ Présence de logiciels sans licence ou craqués sur certains ordinateurs ◢ Absence de politique de gestion des équipements personnels ◢ Pas de chiffrement des unités de stockage des postes de travail
8	Sécurité des équipements itinérants	◢ Absence de procédure pour la gestion du stockage des données sur les postes de travail nomades ◢ Absence de filtre de confidentialité sur les postes nomades ◢ Absence de procédure en cas d'incident, vol ou perte d'équipement nomade.

N°	Domaine de la PSSIE	Écart de conformité
9	Sécurité liée à l'exploitation des SI	◢ Absence de formalisation des processus d'exploitation ◢ Absence de supervision des actifs critiques ◢ Absence de surveillance des événements de sécurité ◢ Absence de politique de sauvegarde de données ◢ Pas de politique formalisée sur la lutte antivirale
10	Sécurité dans l'acquisition, le développement et la maintenance des SI	◢ Absence de procédure formalisée pour intégrer la sécurité dans les projets ◢ Absence de tests de sécurité ◢ Les exigences de sécurité ne sont pas prises en compte lors du développement des applications internes
11	Sécurité des e-services	◢ Absence de méthode d'authentification grâce à la cryptographie à clef publique et aux signatures numériques offertes par la PKI nationale
12	Sécurité des applications web	◢ Absence de gestion des risques liés aux applications web ◢ Absence d'exigences de sécurité pour le développement web ◢ Absence de durcissement des infrastructures qui hébergent les applications web
13	Mesures cryptographiques	◢ Absence de politique de cryptographie ◢ Non-utilisation des certificats électroniques ◢ Absence de procédures de protection des clés cryptographiques

N°	Domaine de la PSSIE	Écart de conformité
14	Contrôle d'accès logique au système d'information	• Absence d'exigences de sécurité dans les contrats avec les tiers • Absence de procédure de gestion des accès physiques ou logiques pour les intervenants externes • Absence de charte engageant les prestataires individuellement vis-à-vis des entités • Absence de procédure de gestion des actifs SI confiés aux prestataires
15	Sécurité du cloud computing	• Absence d'analyse des risques liés au Cloud • Absence de clause de non-divulgation (NDA) dans les contrats avec les fournisseurs Cloud • Absence de stratégie définie pour la priorisation des besoins en externalisation
16	Gestion des incidents de sécurité	• Absence de procédures de gestion des incidents de sécurité • Absence de suivi des incidents de sécurité • Absence de procédure garantissant la sécurité des preuves numériques
17	Gestion de la continuité de la sécurité du SI	• Absence de plan de continuité de la sécurité des systèmes d'information • Absence de plan de continuité d'activité
18	Conformité, audit et contrôles de sécurité.	• Certains logiciels et applications utilisés ne disposent pas de licences officielles • Absence de charte d'audit de sécurité formalisée • Absence de suivi interne de la conformité à la PSSIE et PSSI

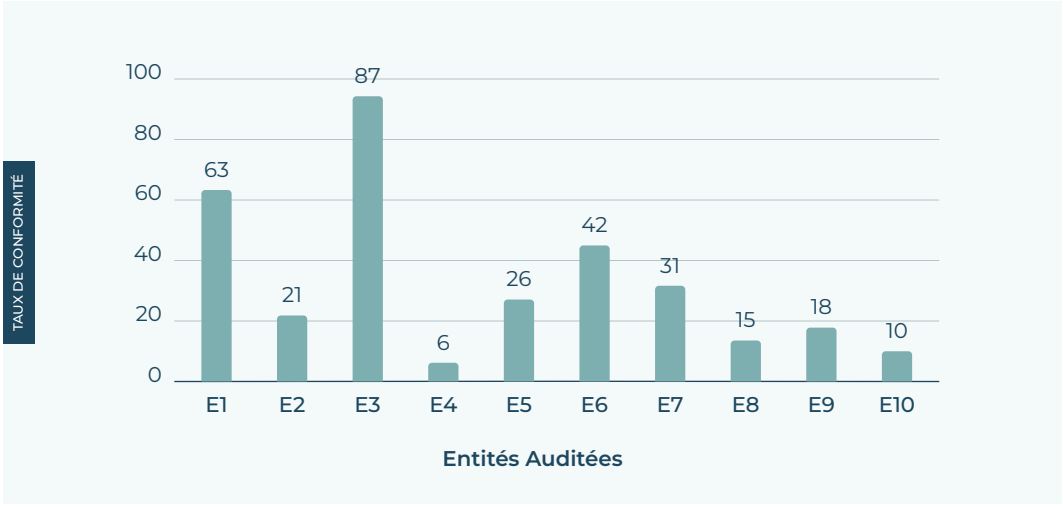


Figure 18 : *Vue d'ensemble des taux de conformité*

Globalement, d'après le graphique ci-dessus, les taux de conformité des entités varient largement de 6 % à 87 %.

31.9% **Des structures prioritaires sont conformes à la PSSIE**

Cela montre que la mise en conformité est globalement faible et que la majorité des exigences de la PSSIE ne sont pas respectées.

10. RECOMMANDATIONS

Pour répondre efficacement aux défis, plusieurs axes d'actions sont recommandés aux structures publiques :

- Poursuite des efforts de sensibilisation des hauts dirigeants aux enjeux de cybersécurité ;
- Mise en œuvre des actions en vue de l'institutionnalisation de la fonction RSSI au sein de l'AOF type des ministères et institutions étatiques ;
- Mise en place d'une ligne de crédit budgétaire au sein des entités et dédiés aux actions de mise en conformité à la PSSIE ;
- **Poursuite des efforts d'opérationnalisation de la fonction RSSI au sein des entités visées par la PSSIE** ;
- **Poursuite des efforts de renforcement de capacités au profit des RSSI** ;
- **Mise en place de dispositifs de surveillance** du système d'information de l'entité (journaux d'accès, alertes en temps réel, tableaux de bord de sécurité) ;
- **Renforcement des politiques d'accès**, avec des mots de passe complexes, une gestion rigoureuse des droits et une authentification à deux facteurs ;
- **audits de sécurité annuels**, accompagnés d'un plan d'actions ;
- **mise à jour systématique des logiciels** et infrastructures, en évitant les versions obsolètes ;
- **Maintien à jour des systèmes et infrastructures :** Assurer la mise à jour régulière des applications et systèmes ; suivre les bonnes pratiques de configuration : éviter les configurations par défaut ;
- **Renforcement des capacités humaines :** Intégrer la cybersécurité dans la formation continue du personnel technique et non technique ; organiser ou participer à des exercices de simulation de gestion de crise cyber ;
- **Audit et contrôle régulier :** Instituer des audits obligatoires de sécurité chaque année ; suivre l'application effective des recommandations post-audit ;
- Implémenter les recommandations issues des alertes émises par le bjCSIRT.

11. CONCLUSION

Ce rapport présente l'état de la cybersécurité au sein des constituants du bjCSIRT, à travers l'analyse des vulnérabilités, des incidents de sécurité et des écarts de conformité. Au fil de l'étude, une réalité se dessine : celle d'un environnement encore vulnérable, en proie à diverses menaces, mais où se manifestent aussi des efforts de prévention et de réponse des équipes de l'ASIN.

Les vulnérabilités identifiées révèlent l'étendue de la surface d'exposition des secteurs touchés et rappellent l'urgence de renforcer l'hygiène numérique à tous les niveaux, des pratiques individuelles aux mécanismes organisationnels. En parallèle, la nature des incidents recensés : fuites de données, attaques ciblées, compromissions et autres souligne l'importance de garder une posture de sécurité active, fondée principalement sur l'anticipation.

Les écarts relevés par rapport aux exigences de la PSSIE traduisent quant à eux une marge de progression importante dans l'alignement des pratiques. Ils rappellent que la conformité ne se limite pas à un cadre réglementaire, mais constitue une véritable culture de sécurité à bâtir, au quotidien, dans chaque structure.

Ce rapport n'est pas une fin en soi. Il doit être lu comme une sensibilisation à l'endroit des décideurs et comme un rappel essentiel pour renforcer les capacités et accompagner les actions des équipes de l'ASIN en ce sens. C'est aussi une invitation à l'action collective : renforcer la collaboration, mutualiser les ressources, et inscrire durablement la cybersécurité comme un pilier de la résilience numérique nationale.

ANNEXE

Le bjCSIRT évalue la criticité des risques associés aux vulnérabilités trouvées en se basant sur la méthodologie d'évaluation OWASP.

L'évaluation du risque associé aux vulnérabilités se quantifie par l'évaluation de l'impact de la menace et celle de la probabilité d'occurrence : **Risque = Impact x Probabilité.**

Impact

Les impacts technique et commercial d'une vulnérabilité sont échelonnés en termes de gravité comme suit :

Elevé	Modéré	Faible

- **Elevé :** les vulnérabilités à impact élevé sont des vulnérabilités ayant des conséquences négatives graves sur la confidentialité, l'intégrité, la disponibilité ou la non-répudiation des systèmes d'information, des données qu'elles hébergent ou qui y transitent, ainsi que le métier qui les utilise. Ces conséquences peuvent être la compromission du système d'information, la perte d'intégrité ou de la confidentialité des données jugées sensibles, l'indisponibilité partielle ou totale du service.
- **Modéré :** les vulnérabilités à impact modéré sont des vulnérabilités ayant des conséquences négatives certaines pouvant perturber le bon fonctionnement des systèmes d'information et des données qu'elles hébergent.
- **Faible :** les vulnérabilités à impact faible sont des vulnérabilités ayant des conséquences mineures sur les systèmes d'information si elles venaient à être exploitées.

Probabilité d'occurrence

La **probabilité de découverte et d'exploitation** (dénommée ci-après probabilité d'occurrence) d'une vulnérabilité est échelonnée comme suit :

Elevé	Probable	Faible

- **Elevé :** vulnérabilité facile à découvrir et à exploiter.
- **Probable :** il existe une certaine probabilité qu'un attaquant pertinent puisse découvrir cette vulnérabilité et arrive à l'exploiter.
- **Faible :** vulnérabilité difficile à découvrir et surtout à exploiter. Il requiert un attaquant expérimenté qui cible particulièrement la plateforme.

Risques associés

A partir de l'impact et de la probabilité d'occurrence, nous arrivons à la matrice de classification du risque ci-après :

	RISQUES ASSOCIES AUX VULNERABILITES			
IMPACT	Élevé	Modéré	Élevé	Critique
	Modéré	Faible	Modéré	Élevé
	Faible	Note	Faible	Modéré
		Faible	Probable	Élevé
		PROBABILITÉ		

Cette matrice est utilisée pour évaluer les risques associés aux vulnérabilités découvertes.

RAPPORT DE VULNÉRABILITÉS ET D'INCIDENTS
VULNÉRABILITÉS ET
INCIDENTS DU CYBERESPACE
BÉNINOIS.

Suivez-nous sur nos canaux digitaux

@asinbenin

www.asin.bj