Citilog
A TAGMASTER COMPANY

GESTION DES INCIDENTS

Cybersécurité pour votre solution CT-IM

Création : Février. 2021

Dernière mise à jour : 04 décembre 2023

Rév. : B

SUIVI DES CHANGEMENTS

Liste des modifications

Révision	Date	Notes
Révision A	24/02/2021	Création de documents
Révision B	04/12/2023	Rafraichissement du document

CONTENU

1. INTRODUCTION

Au cours des vingt dernières années, les systèmes AID ont parcouru un long chemin sur le point de la technologie. Ce qui a commencé comme un système vidéo analogique fonctionnant en circuit fermé (CCTV) est maintenant souvent un système de surveillance complexe reposant sur plusieurs serveurs et un vaste réseau d'équipements divers connectés les uns aux autres, communiquant via différents protocoles et utilisant de nombreux logiciels et applications, la plupart d'entre eux offrant la possibilité de accès de n'importe où dans le monde via une connexion internet dans un souci de simplicité d'utilisation.

Dans le même temps, les méthodes utilisées pour pirater ou saboter les systèmes informatiques sont devenues plus sophistiquées et évoluent constamment. Il est souvent impossible de les identifier avant qu'une attaque ne soit lancée. De plus, plus un système est complexe, plus il offre de points d'entrée potentiels pour une attaque organisée. La cybercriminalité est devenue une menace sérieuse pour toutes les données partagées sur le système.

La question de la cybersécurité est donc devenue une priorité numéro un pour Citilog. Ce document décrit les actions entreprises par Citilog pour améliorer la protection des données des clients depuis la version CT-IM 2021R1.

1.1 DÉFINITION DES TERMES

Terme	Définition
AID	Détection automatique des incidents
SON	Système de transport intelligent
CCTV	Télévision en circuit fermé
INTERFACE GRAPHIQUE	Interface utilisateur graphique
IEEE	Institut of Electrical and Electronics Engineer (la plus grande association mondiale de professionnels techniques)
HTTPS (EN)	Protocole de transfert hypertexte sécurisé
Le TLS	Sécurité de la couche de transport
Le RTSP	Protocole de streaming en temps réel

2. APERÇU

2.1. POURQUOI PROTÉGER VOTRE SYSTÈME AID ?

Le système AID est aujourd'hui un outil essentiel pour une gestion efficace des routes, autoroutes, tunnels et autres infrastructures vitales pour notre société. S'il devient vulnérable, les conséquences peuvent avoir un impact important sur l'exploitation globale des infrastructures de transport et la sécurité de ses usagers.

En plus de cela, comme tout système informatique, il contient des données sensibles telles que des comptes d'utilisateurs (login et mot de passe) ou des images (en direct ou enregistrées) qui ne sont pas destinées à un usage externe. S'il n'est pas correctement protégé, il peut également être utilisé comme point d'entrée vers le reste du réseau, offrant un accès potentiel à différents ordinateurs, applications et autres données sensibles.

2.2. LES PRINCIPAUX RISQUES

En matière de cybersécurité, trois grandes catégories de risques sont généralement identifiées et ont été prises en compte par Citilog pour l'évaluation des risques :

- Facteur humain - souvent plus important que la technologie, le facteur humain est défini comme une menace interne, dont la source peut aller d'un manque d'attention ou d'un manque de rigueur à une intention malveillante d'un employé.
- Cyber-attaque (piratage) - ciblant une entité spécifique, une cyber-attaque est une action exécutée de l'extérieur, en utilisant Internet pour accéder à l'entité network, dans une tentative de détourner ou d'endommager leur système.
- Virus ou logiciels malveillants - une attaque à large gamme avec plusieurs résultats possibles tels que la suppression ou l'exploitation des données, mettant éventuellement fin à la défaillance du système. Ce risque résulte d'au moins un des deux risques précédents.

3. SCÉNARIOS DE RISQUE

Contexte :

Un tunnel est une infrastructure essentielle pour une ville. It aide à faciliter la circulation et permet aux conducteurs de gagner du temps sur leur trajet quotidien. Ce qui est encore plus important – cela peut devenir vital lorsqu'il s'agit de services d'urgence tels que la police, les ambulances ou les pompiers, pour qui chaque minute perdue peut être une question de vie ou de mort.

En raison de son importance, le tunnel est surveillé par un système AID pour une détection précoce et une gestion efficace de tout incident.

Dans notre exemple, son système AID est connecté à 30 caméras qui analysent le trafic en temps réel. It est également connecté à 2 panneaux à messages variables et au centre de contrôle de la circulation.

Menaces :

#1 : Hameçonnage

Joe travaille au centre de contrôle. He aime les photos drôles avec des chats et des chiens. Lorsqu'il reçoit un email avec un objet :« ***Funny dog pictures*** », il n'y réfléchit pas à deux fois avant d'ouvrir la pièce jointe même si l'expéditeur est inconnu.

Malheureusement, le courrier électronique de Joe a été infecté par un virus qui se propagera de son poste de travail à tous les autres ordinateurs du réseau.

#2 : Piratage

Kenny est un hacker. Il est assez doué et aime montrer aux autres de quoi il est capable, même si cela ne conduit à aucun gain personnel. Les caméras à l'entrée du tunnel ont déjà attiré son attention il y a un certain temps et il veut voir s'il peut y accéder et le contrôler. Comme le réseau n'est pas protégé, le seul défi est de trouver un point d'entrée physique. Dès qu'il réussit, Kenny peut facilement surveiller les données échangées entre les caméras et le système AID. Il pourrait même prendre le contrôle des caméras et changer de position PTZ.

Kenny aura de plus en plus accès au système, lui permettant de modifier les champs de vision, les paramètres du système ou de voler des clips vidéo pour les partager sur internet.

Résultat potentiel :

#1 : Hameçonnage

Si l'application malveillante n'est pas détectée par l'antivirus, elle se propagera rapidement au réseau. Les ordinateurs commenceront progressivement à ralentir jusqu'à un crash complet. Le système AID sera en panne et l'exploitation du tunnel sera potentiellement compromise jusqu'à la fermeture du tunnel.

#2 : Piratage

Kenny va s'ennuyer à la fin, mais en jouant avec le système AID, il a totalement gâché ses paramètres. Le système ne fonctionnera plus comme prévu, ce qui peut avoir diverses conséquences, allant de l'absence d'incidents à la fermeture complète du tunnel.

Figure 1: fermeture du tunnel

Le résultat final dans les deux cas est un tunnel fermé. Pendant les heures de pointe, l'indisponibilité du tunnel peut entraîner d'importantes embouteillages, laissant les conducteurs bloqués pendant ce qui peut devenir même des heures dans le pire des cas. Cela pourrait également signifier que les services d'urgence devront utiliser une autre route pour aller d'une partie de la ville à l'autre et perdre un temps précieux.

4. COMMENT CITILOG GÈRE-T-IL LES RISQUES ?

Au cours des dernières années, l'exposition des entreprises aux cyberattaques s'est avérée plus importante que prévu et souvent due à des facteurs qui auraient pu être assez facilement éliminés. De nombreuses études montrent qu'une grande partie des attaques auraient pu être évitées simplement en corrigeant les vulnérabilités connues et en s'assurant que les configurations de sécurité sont correctement définies.

Dans ce contexte, Citilog a pris toutes les mesures nécessaires pour évaluer les risques éventuels et leur impact sur la sécurité de ses produits et pour identifier les points faibles afin de fournir une solution plus sûre et plus fiable à ses clients.

Sur la base de cette évaluation des risques, Citilog a développé et appliqué les mesures de sécurité appropriées pour minimiser les menaces externes identifiées.

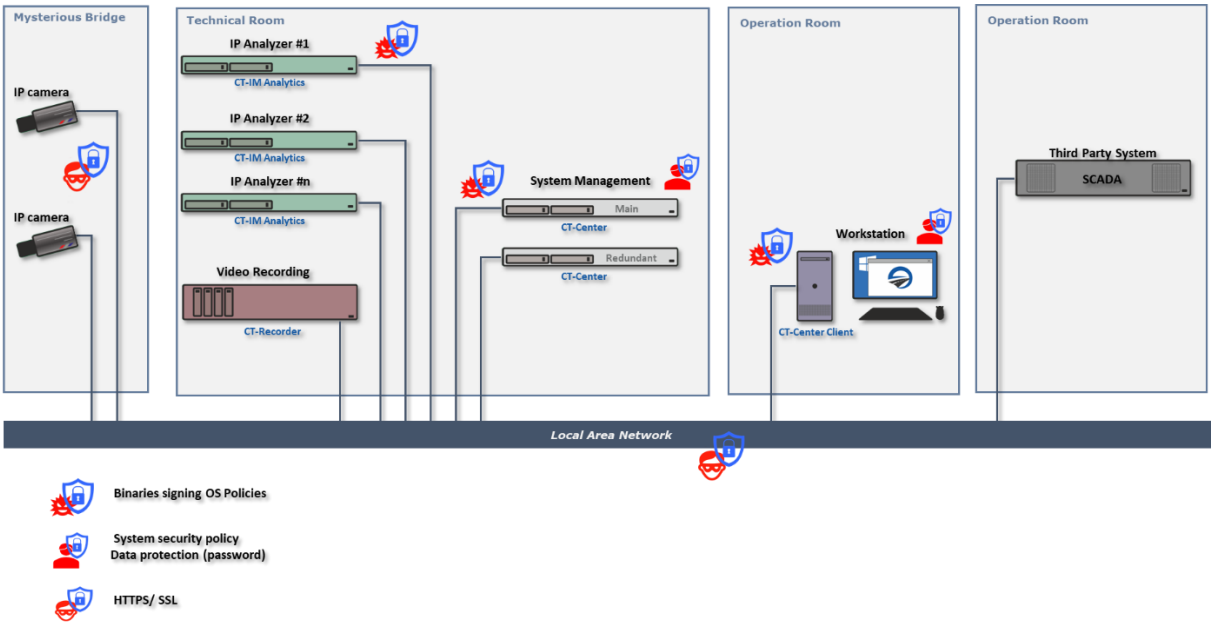

Figure 2: Analyse des risques Citilog et mesures de sécurité

4.1. FACTEUR HUMAIN

Les mises à niveau techniques sont importantes, minimiser les erreurs humaines est encore plus crucial. Les gens se sont avérés être le maillon faible dans de nombreux attaques. Les procédures standard, les paramètres mal configurés, les mots de passe faibles ouvrent tous la porte à des attaques potentielles.

Bien que les risques associés au facteur humain ne puissent pas être complètement éliminés, Citilog a mis en place différents mécanismes de sauvegarde pour limiter au mieux ces risques.

1. ***Verrouillage automatique de la session d'administration***

Pour s'assurer qu'aucune personne non autorisée n'obtient jamais l'accès aux paramètres de l'application qui ont pu être laissés ouverts sur le poste de travail, la solution Citilog IM est verrouillée en cas d'inactivité prolongée.

Après un délai prédéfini, l'administrateur devra entrer le mot de passe pour revenir à sa session.

2.***Passe***

Chaque utilisateur - opérateur, administrateur ou autre - a son propre mot de passe personnel. CT-IM impose l'utilisation de mots de passe forts et complexes incluant la combinaison de caractères alphanumériques et de caractères spéciaux pour une meilleure sécurité.

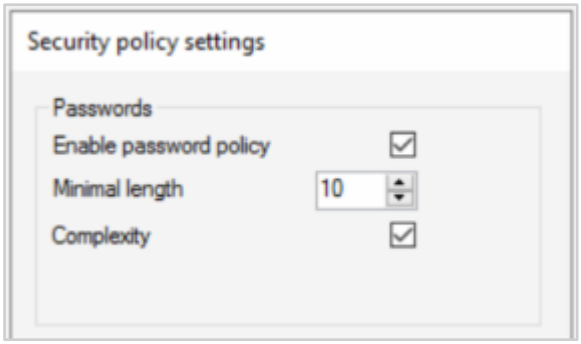

Figure 3: Client CT-Center - Paramètres de stratégie de sécurité

En plus de cela, les mots de passe sont cryptés dans le système et ne peuvent pas être affichés sur l'interface graphique. La longueur réelle des mots de passe est également invisible.

Figure 4: Client CT-Center – informations d'identification cachées

4.2. CYBERATTAQUE (PIRATE)

Nous avons assisté à une augmentation importante des cyberattaques récemment et souventes pirates informatiques ne travaillent plus seuls, mais se rassemblent dans des groupes criminels efficaces et bien organisés qui peuvent causer des dommages substantiels en attaquant le système de l'extérieur de l'entreprise, par le biais d'un réseau.

Pour attaquer l'AID, les criminels informatiques devront d'abord vaincre les mesures de sécurité déployées par l'administrateur réseau telles que les ***pare-feu, l'authentification IEEE 802.1x,*** le ***protocole TLS (Transport Layer Security),*** etc.

Néanmoins, lorsque les mesures de sécurité sont faibles, le logiciel Citilog peut être exposé à une cyberattaque.

Pour réduire le risque d'intrusion, toutes les communications entre les différents éléments du système Citilog sont cryptées (à l'aide de Transport Layer **Security)** rendant impossible l'accès aux données confidentielles transmises via le réseau entre les composants du système.

Reportez-vous au chapitre *Mesures de sécurité* pour obtenir la liste complète des fonctionnalités implémentées.

4.3. VIRUS

Tout aussi important est un problème de virus. Même si elle ne vise pas nécessairement directement une entreprise en particulier, elle n'en reste pas moins dangereuse. Affecté la propagation à d'autres ordinateurs, il exploitées défauts de l'sécurité du système d'exploitation et peut perturber le

fonctionnement de l'ordinateur infecté à des degrés divers.

Il peut utiliser plusieurs points d'entrée comme des clés USB non sécurisées, des pièces jointes non vérifiées dans l'e-mail ou même un logiciel installé imprudemment à partir d'Internet. Une fois exécuté, il se réplique et affecte d'autres programmes et peut entraîner un arrêt complet de l'ensemble du système.

Pour éviter toute interférence non autorisée, toutes les mesures de sécurité du système d'exploitation doivent être appliquées :

- **Contrôle de compte d'utilisateur**
- **Antivirus**
- **Dernières mises à jour Windows**

La solution CT-IM est compatible avec l'antivirus Windows Defender inclus dans Windows 11 Professionnel et Windows Server 2022.

Chaque nouvelle version de la solution CT-IM est testée dans un environnement où Windows Defender est activé.

4.4. MESURES DE SÉCURITÉ

Les fonctionnalités suivantes ont été implémentées dans la dernière version de la solution CT-IM pour contrer d'éventuelles failles de sécurité :

Caractéristique	Description
Authentification IEEE 802.1x	Agent de sécurité permettant à l'utilisateur ou à un appareil de s'authentifier avant de lui permettre d'accéder au réseau - l'identité de l'utilisateur doit être validée avant d'obtenir une adresse IP et un adaptateur filaire ou sans fil entièrement fonctionnel.
Protocole TLS (Transport Layer Security)	Crypte les transactions en ligne et les données confidentielles relayées entre les caméras et les systèmes de gestion vidéo en gardant les connexions entre l'équipement et le serveur sécurisées et privées. TLS nécessite l'utilisation d'un certificat numérique.
Protocole de transfert hypertexte sécurisé (HTTPS)	Protocole de communication garantissant une communication sécurisée sur un réseau informatique. Il est crypté via TLS.
RTSP avec authentification	Possibilité d'utiliser RTSP avec authentification dans le système. Les flux vidéo nécessiteront un identifiant et un mot de passe pour être visualisés.
Authentification de l'utilisateur	Applique une stratégie de mot de passe fort.
Pas de comptes de porte dérobée	Citilog n'implémente aucune porte dérobée dans ses systèmes de support à distance.
Authentification Digest	Seule une version cryptée d'un mot de passe est enregistrée sur le serveur, ce qui le protège d'un décodage facile.
Système auto-verrouillage	L'élément très sensible de l'interface graphique (tel que l'onglet Administration) est protégé par une fonction de verrouillage automatique qui verrouille automatiquement l'accès à l'interface graphique si le système n'est pas utilisé.
Interface graphique orientée cybersécurité	L'interface graphique du client CT-Center est conçue pour dissimuler les mots de passe et leur longueur.
Compatibilité du pare-feu	La solution CT-IM est compatible avec tous les pare-feu et Citilog fournit une liste de ports qui peuvent être ouverts en toute sécurité pour la configuration réseau.
Compatibilité antivirus	La solution CT-IM est entièrement compatible avec Windows Defender (Windows 11 Professionnel et Windows Server 2022).
Mises à jour logicielles Citilog	Citilog publie régulièrement des correctifs corrigeant les dernières menaces de cybersécurité.

Mises à jour du firmware	Des versions de nouvelles versions de firmware améliorant la stabilité du logiciel et la cybersécurité sont régulièrement fournies pour les caméras Axis.
Mises à jour du système d'exploitation	Citilog recommande d'installer toutes les mises à jour de Microsoft pour une meilleure protection, détection et réponse aux menaces de cybersécurité émergentes.

5. LISTE DES FIGURES

6. CONTACTER CITILOG

Si vous avez besoin d'un support supplémentaire pour l'exploitation, la configuration, la mise à jour ou la maintenance de votre solution Citilog, veuillez contacter soit l'équipe de support Citilog qui s'occupe habituellement de votre système, soit le partenaire Citilog de votre région.
Vous trouverez la liste des partenaires Citilog sur notre site web à l'adresse https://www.citilog.com/partners-resellers. Sinon, veuillez contacter Citilog par le biais de notre site web en utilisant le formulaire de contact à l'adresse https://www.citilog.com/contact-us.