Considérations de sécurité pour *l'Affichage Dynamique*

Livre blanc 1.0
par *SpinetiX*

08.2021

Portée du présent document

Ce livre blanc décrit les principales considérations que le personnel technique doit prendre en compte lors de la détermination des risques et exigences de sécurité pour un projet d'affichage dynamique. Nous vous recommandons d'utiliser ce document comme base lors de l'audit des solutions d'affichage dynamique par rapport à vos besoins de sécurité informatique. Ce document fait partie de notre série Sécurité & Affichage Dynamique.

La cybersécurité: une priorité pour tous

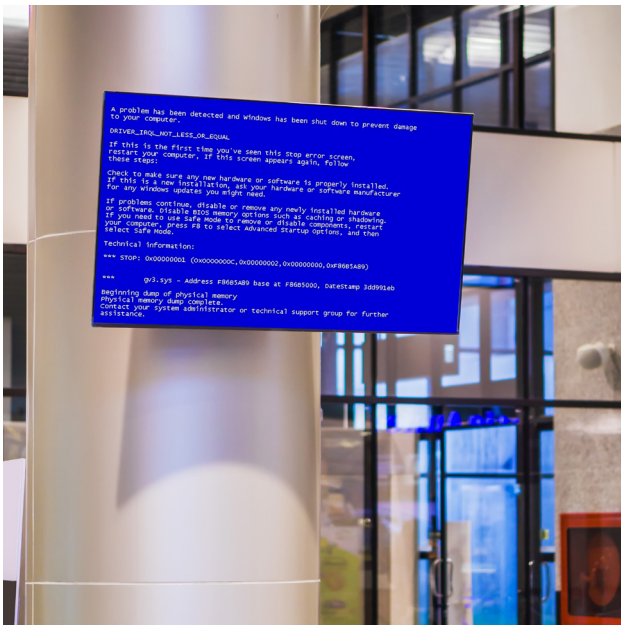
Alors que notre monde devient chaque jour plus digitalisé et interconnecté, la cybersécurité est plus importante que jamais. L'industrie de l'affichage dynamique a historiquement largement ignoré les bonnes pratiques en matière de sécurité informatique. Le bon sens dit qu'à mesure que la prévalence des systèmes d'affichage dynamique connectés augmente, le nombre d'attaques ne diminuera pas. Il est donc important de considérer la sécurité comme exigence de base lors de la planification, du déploiement et de l'exploitation de solutions d'affichage dynamique.

Lors de la sélection de produits pour un nouveau projet, l'aspect sécurité cède le plus souvent sa place à d'autres points de décision tels que le prix d'acquisition, les coûts opérationnels, les fonctionnalités et les performances. De plus, lors de la planification et du déploiement d'une installation d'affichage dynamique, vous pouvez avoir des intervenants avec des préoccupations très différentes en matière de sécurité - typiquement le marketing et le service IT. Cela risque donc de relayer la sécurité au second plan.

De nouveaux risques apparaissent sans arrêt, comme le nouveau modèle de "Ransomware en tant que service" (RaaS) qui a fait la une des journaux en 2021 avec le groupe REvil et les attaques d'infrastructures mondiales contre Kaseya et d'autres et sa nouvelle tactique de "double extorsion" qui cherche à monétiser la menace de divulguer publiquement des informations confidentielles volées. Il est donc crucial que la sécurité d'un produit soit évaluée non seulement au moment de l'achat, mais également par rapport aux politiques de support et à la disponibilité des correctifs de vulnérabilité pendant la durée de vie du produit.

Le coût caché de la sécurité

Il n'est pas rare de trouver des players d'affichage dynamique directement connectés à Internet sans mot de passe ou avec leur mot de passe par défaut. La plupart des players d'affichage fonctionnent sur des systèmes d'exploitation non corrigés et non pris en charge avec des vulnérabilités bien connues qui peuvent donner aux attaquants un accès à distance complet grâce à des kits d'exploitation prêts à l'emploi. Pourtant, effectuer des mises à jour régulières est souvent considéré comme un processus coûteux et inutile qu'il vaut mieux éviter et la sécurité est rarement un critère lors du choix d'une solution d'affichage.

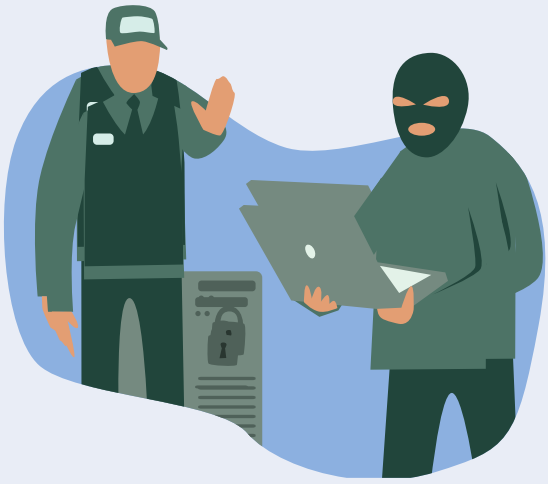


Le coût caché du matériel et des logiciels non sécurisés augmente cependant rapidement. Il y a des cas bien documentés de divers appareils réseau ciblés pour construire d'énormes botnets loués à profit: Persirai (120'000 systèmes compromis) et Mirai (600'000 systèmes).

Pour citer une analyse de Trend Micro : "Dans plusieurs attaques DDoS puissantes et très médiatisées, Mirai ciblant Linux a révélé à quel point l'écosystème de l'Internet des Objets était brisé. Le malware fait à nouveau l'actualité avec un nouveau cheval de Troie Windows qui augmente considérablement ses capacités de distribution."

Ces dernières années, il y a eu de nombreuses autres attaques moins médiatisées spécifiques à l'infrastructure d'affichage dynamique, mais non moins dommageables. Les effets vont du message relativement bénin "veuillez sécuriser votre système" à la demande de rançon et même à la diffusion d'images pornographiques dans les espaces publics, comme à la gare d'Union Station à Washington.

Pourquoi la sécurité est importante



Les décideurs considèrent souvent à tort que tous les fournisseurs de solutions offrent la même sécurité et que les chances que quelqu'un exploite une vulnérabilité sont négligeables, ou que l'impact d'une faille de sécurité est nul, ce qui ne peut être plus éloigné de la vérité dans le monde réel.

Le risque d'une attaque de sécurité est réel et non sans conséquences. Une violation peut vous coûter des temps d'arrêt, des revenus publicitaires perdus et même l'image de votre entreprise. Une installation d'affichage dynamique compromise peut également être utilisée pour attaquer d'autres infrastructures informatiques.

Une idée erronée commune est qu'un logiciel peut rester sécurisé sans aucune action. Tout logiciel aura des vulnérabilités inconnues. Il est donc important que, une fois connues, elles soient corrigées rapidement et que les correctifs puissent être déployés efficacement.

Une autre idée erronée commune est que les players d'affichage ne seront pas ciblés par les hackers. En réalité, pour un hacker toute appareil est potentiellement une cible si il n'est pas protégé car il peut être utilisé pour accéder à des cibles de plus grande valeur à l'intérieur du réseau de l'entreprise. Les attaques sophistiquées tentent toujours de trouver le point d'entrée le plus faible et les appareils internet-des-objets sont une cible de choix. Cette technique, appelée "Mouvement latéral", est devenue en 2019 l'une des menaces les plus importantes pour les réseaux d'entreprise en étendant largement la liste des points d'entrée pour les opérations réussies de ransomware ou de fuite de données au-delà de ceux qui sont habituellement plus fortement protégés. Même si les mises à jour automatiques sont devenues plus courantes, le piratage Sunburst a exposé en 2020 la réalité des attaques de la chaîne d'approvisionnement.

Il y a bien sûr des coûts directs associés aux défaillances de sécurité dans les éléments d'une solution d'affichage dynamique. Les players compromis doivent être mis hors ligne et sont coûteux à restaurer. Les players ou comptes utilisateur compromis peuvent être utilisés pour afficher du contenu portant atteinte à la réputation ou illégal. Ils peuvent conduire à une perte de revenus immédiate de la publicité ou des contrats de service. S'ils sont utilisés comme canal pour un ransomware ou une attaque d'informations personnelles sensibles, le niveau de dégâts peut être dévastateur.

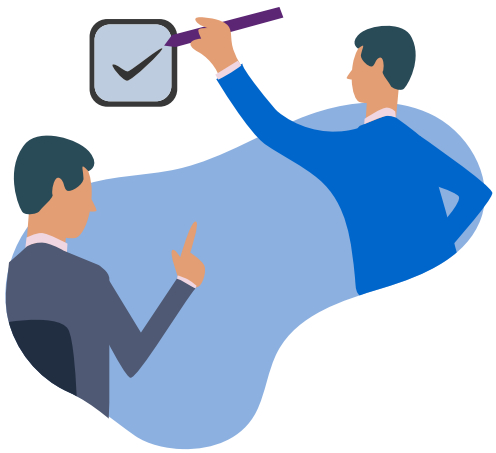
En outre, les récents changements réglementaires comme le RGPD en Europe renforcent l'importance de sélectionner des solutions qui simplifient la conformité et réduisent son coût.

Liste de contrôle de la sécurité

Ce que vous devez considérer lors de l'évaluation de la sécurité d'une installation d'affichage dynamique.

Dans un réseau d'affichage dynamique, les points faibles doivent être pris en compte. Le plus visible et le plus facile à évaluer est la sécurité physique au niveau de l'écran si celui-ci se trouve dans un lieu public ou sensible. La sécurité du player d'affichage dynamique est beaucoup plus difficile à évaluer. Il en est de même pour la sécurité de l'écran lorsqu'il est connecté et la protection du réseau sur lequel le player est installé.

Il y a ensuite la sécurité de l'acquisition, de la distribution et de la production du contenu qui doit également être évaluée. Et enfin, comment s'assurer que les opérateurs suivent les bonnes pratiques de sécurité.



Tous ces points doivent être pris en compte dès le départ lors de la sélection des produits et de la planification de votre projet d'affichage dynamique. Renforcer la sécurité après coup n'est pas toujours possible ou peut être très coûteuse une fois que vous êtes lié à un produit.

L'évaluation de la sécurité d'un système est un problème difficile, mais quelques questions de base peuvent garantir que les produits sélectionnés respectent des bonnes pratiques de sécurité. Utilisez la liste de contrôle ci-dessous pour vous aider à évaluer votre réseau et vos processus existants ou au moment de choisir votre future solution d'affichage dynamique.

DU CÔTÉ DU FOURNISSEUR :

Les réponses aux points ci-dessous vous indiqueront si vous pouvez compter sur le fabricant pour maintenir correctement son produit du point de vue de la sécurité.

- [ ] Le fournisseur de solutions est-il bien établi ? Ont-ils une bonne réputation ?
- [ ] Fournissent-ils des mises à jour de sécurité régulières en temps opportun ?
- [ ] Pendant combien de temps le produit sélectionné sera-t-il maintenu ?
- [ ] Disposent-ils d'un processus de travail pour divulguer les vulnérabilités, par exemple avec la liste CVE ?
- [ ] Ont-ils un processus de publication bien défini, y compris des notes de publication avec une liste de problèmes de sécurité corrigés dans la mise à jour ?
- [ ] Comment les mises à jour sont-elles distribuées et quel est le coût de leur déploiement ?
- [ ] Quelle est la compatibilité avec les versions précédentes des mises à jour ?
- [ ] Ont-ils un bon service d'assistance technique auquel vous pouvez accéder ?

DU CÔTÉ DE LA SOLUTION :

Utilisez les points ci-dessous pour vous aider à évaluer votre réseau et vos processus existants ou au moment de choisir votre future solution d'affichage dynamique.

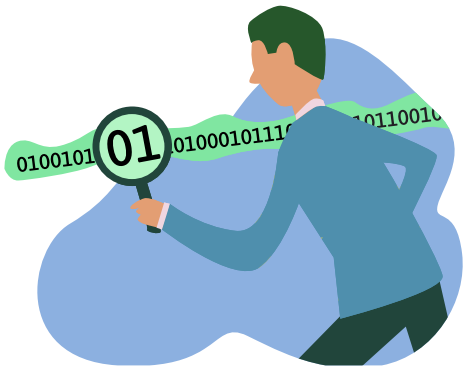
- ☐ Le contenu à l'écran est celui qui était planifié.
  - ☐ Éviter la diffusion de contenu malveillant ou illégal par des intrus ou des initiés et les atteintes à la réputation du prestataire de services qui en découlent.
  - ☐ Éviter les pertes de revenus si la publicité vendue n'est pas affichée au moment et à l'endroit convenus.
  - ☐ Les cibles de disponibilité et de résilience garantissent la distribution en temps opportun d'un contenu à jour.
- ☐ Le player ne doit pas être une menace pour la sécurité des autres équipements du réseau : ne fournit pas un point faible d'attaque qui pourrait être exploité par le vol de données ou la diffusion d'un malware, spyware ou ransomware.
- ☐ Protéger les données des clients sur le player ou le cloud contre une exposition à des tiers non autorisés. En cas d'incident de sécurité ou de violation de données, fournir des outils pour une enquête judiciaire.
- ☐ S'intègre parfaitement avec les propres politiques de sécurité IT du client pour protéger son réseau hôte en prenant en charge les protocoles de niveau entreprise.
- ☐ Faciliter le respect des obligations réglementaires comme par exemple la mise en oeuvre du RGPD en Europe ou du CCPA/CPRA aux États Unis.

Le prix de la sécurité

Tout cela a un coût, et il ne faut pas s'étonner qu'une solution sécurisée soit plus coûteuse, bien que l'inverse ne soit évidemment pas vrai. Développer des systèmes sécurisés est difficile et a donc un coût supplémentaire. Maintenir une plate-forme sécurisée et surveiller activement les détections de vulnérabilités prend du temps et entraîne également des coûts supplémentaires.

Une fois que vous avez sélectionné un fournisseur adapté à vos besoins de sécurité, vous devez également appliquer des principes de sécurité rationnels dès le déploiement et tout au long de la mise en service de l'installation. Diminuez autant que possible la surface d'attaque en désactivant les services inutiles et n'exposez pas les services sur le réseau au-delà de ce qui est réellement requis pour les opérations.

N'exposez pas vos appareils directement sur Internet et utilisez un pare-feu pour protéger le réseau du player. Assurez-vous que les utilisateurs sont correctement formés pour ne pas être victimes d'attaques d'ingénierie sociale et, qu'ils utilisent des mots de passe forts et uniques.



Conclusion.

Tout cela peut sembler beaucoup à considérer, mais si les bonnes questions de sécurité sont prises en compte dès le début du projet et que les aspects de sécurité sont intégrés dans le processus de sélection, il ne devrait pas être difficile de choisir les bons produits qui diminueront le risque d'être victime d'une attaque réussie.

Quelques mots sur **les auteurs**

Jean-Claude Michelou,
Vice-Président Recherche & Développement

Au sein de SpinetiX, Jean-Claude apporte son expérience dans le développement de grandes infrastructures logicielles et en réseau et la gestion de projets technologiques complexes. Il est responsable du développement de produits novateurs.

Diplômé de l'École Polytechnique (X94) à Paris, Jean-Claude a occupé plusieurs postes d'ingénieur et de recherche dans des startups de la Silicon Valley comme AltaVista et BigVine. Il a ensuite cofondé VisioWave où, en tant que vice-président R&D et architecte en chef des logiciels, il a développé la technologie de streaming vidéo qui sécurise des centaines de systèmes de transport public dans le monde.

Diego Santa Cruz, PhD
Architecte de solutions

Diego Santa Cruz se passionne pour la sécurité des produits SpinetiX depuis plus de 10 ans, en s'efforçant de fournir des produits sûrs, fiables et bien intégrés. Il a co-fondé SpinetiX et est responsable du développement des systèmes au sein de la société.

Son expertise principale couvre le développement de systèmes et de kernel, les protocoles de réseau, la sécurité, l'informatique et l'électronique, ainsi que les systèmes d'image et de vidéo, dans lesquels il s'est spécialisé et a obtenu son doctorat. Auteur de plusieurs brevets et pionnier dans l'utilisation de Linux, Diego a contribué aux comités JPEG et MPEG.

SPINETIX™
N°1 IN DIGITAL SIGNAGE SOLUTIONS

Vous faites vos premiers pas en affichage dynamique ?

Vous avez besoin de conseils en sécurité ?

Contactez-nous:

sales@spinetix.com

Lisez plus de publications issues de notre série Sécurité & Affichage dynamique :

spinetix.com/security