Trinaps
11 rue Sophie Germain
90000 Belfort
conseil@trinaps.com
03 39 03 40 60

GUIDE

Cybersécurité et résilience dans le secteur événementiel



trinaps.com/events

Guide rédigé par Trinaps, opérateur cloud, cyber et télécom indépendant.

Sa mission : transporter et protéger les données des entreprises, associations et collectivités depuis 18 ans. Spécialisé dans la gestion d'infrastructures critiques,Trinaps est certifié ISO27001 et Hébergeur de Données de Santé et posséde son propre datacenter 100% français basé à Belfort. Ces exigences élevées en matière de sécurité et de confidentialité permettent notamment d'intervenir sur des événements d'envergure et dans des secteurs sensibles.

© Trinaps Mai 2025

Table des matières

Checklist des 10 points essentiels 4
Résumé 5
Introduction 5
1. Comprendre les enjeux de la cybersécurité dans l'événementiel 5
1.1 Les risques spécifiques du secteur de l'événementiel et de la billetterie 5
1.2 L'importance de la protection des données personnelles 5
1.3 Les conséquences d'une cyberattaque ou d'une perte de données 5
1.4 Dépendance à l'infrastructure technique 5
1.5 La préoccupation du temps : anticipation 6
2. Cadre réglementaire et normatif 6
2.1 Le Règlement Général sur la Protection des Données (RGPD) 6
2.2 La Directive NIS2 (Network and Information Security) 6
2.3 Les normes et certifications 6
3. Gouvernance de la sécurité de l'information 6
3.1 Définir une politique de sécurité 7
3.2 Désigner un responsable de la sécurité 7
3.3 Gestion des risques 7
4. Protection des données personnelles 7
4.1 Principes du RGPD 7
4.2 Mesures techniques et organisationnelles 7
4.3 Gestion des consentements 7
4.4 Exercice des droits des personnes concernées 8
5. Sécurité des systèmes d'information 8
5.1 Sécurité du réseau 8
5.2 Sécurité des réseaux Wi-Fi 8
5.3 Sécurité des endpoints 8
5.4 Gestion des accès et des identités 8
5.5 Sécurité des applications 8
5.6 Sécurité cloud 8
6. Sécurité des opérations de billetterie 9
6.1 Sécurisation des transactions 9
6.2 Lutte contre la fraude à la billetterie 9
6.3 Gestion des accès lors des événements 9
7. Continuité d'activité et gestion de crise 9
7.1 Plan de continuité d'activité (PCA) et Plan de reprise d'activité (PRA) 9
7.2 Gestion de crise cybernétique 9
8. Formation et sensibilisation 9
8.1 Programme de sensibilisation 9
8.2 Formation technique 10
9. Surveillance et réponse aux incidents 10
9.1 Détection des menaces 10
9.2 Gestion des incidents 10
9.3 Amélioration continue 10
10. Technologies émergentes et innovation 10
10.1 Intelligence artificielle et machine learning 10
10.2 Blockchain 10
10.3 Internet des objets (IoT) 10
11. Conformité et audit 10
11.1 Audits de sécurité 11
11.2 Reporting et tableaux de bord 11
12. Collaboration et partage d'informations 11
12.1 Partenariats public-privé 11
12.2 Partage d'informations au sein du secteur 11
Conclusion 11
Exemples de scenarios 12
Glossaire 14
Ressources 16

Cybersécurité et résilience en événementiel
Checklist des 10 points essentiels

Je coche ce qui me correspond

		Je gère !	C'est en cours	Connais pas
1.	Définir une politique de sécurité claire, désigner un responsable sécurité, impliquer la direction dans la gouvernance.			
2.	Identifier et cartographier les risques et prioriser les actions à fort impact pour y faire face.			
3.	Assurer la conformité au RGPD et mettre en œuvre des mesures de protection des données personnelles.			
4.	Sécuriser l'infrastructure réseau et les systèmes (segmentation, pare-feu, chiffrement).			
5.	Prévoir des PCA/PRA simples, testés, et des scénarios de modes dégradés pour limiter les points de défaillance.			
6.	Structurer une cellule de crise avec des outils, des procédures en coordination aves les prestataires/autorités.			
7.	Former et sensibiliser régulièrement tous les employés et intervenants aux enjeux de la cybersécurité			
8.	Mettre en place une capacité de détection et de réponse aux incidents de sécurité.			
9.	Réaliser des audits réguliers et intégrer les retours d'expérience dans une boucle d'amélioration continue.			
10.	Collaborer et partager des informations sur les menaces avec les autorités, prestataires et acteurs du secteur.			

Je calcule ma maturité cyber et résilience

Je suis prêt à endurer les menaces cyber & télécoms qui plannent sur mon événement !

J'ai conscience des enjeux et des risques et je suis sur la bonne voie pour sécuriser mon événement.

Heureusement que je suis tombé sur ce guide !

www.trinaps.com

Résumé

Ce guide complet sur la cybersécurité et la résilience est conçu pour les organisateurs d'événements et les prestataires de solutions de billetterie. Il vise à fournir des conseils pratiques et techniques pour protéger les systèmes d'information, les données personnelles et assurer la continuité des activités dans le secteur de l'événementiel. En suivant les recommandations de ce guide, basées sur l'expérience accumulée et sur les meilleures pratiques du domaine, comme l'ANSSI, la CNIL ou le Clusif, les acteurs du secteur pourront renforcer leur posture de sécurité et leur résilience face aux menaces cyber. Bien entendu, les mesures et actions mises en oeuvre doivent l'être d'une part au regard de l'exposition aux risques et d'autre part aux conséquences de l'apparition de ceux-ci.

Introduction

Dans un monde de plus en plus numérisé, la sécurité des systèmes d'information et la protection des données personnelles sont plus que préoccupants pour les organisateurs d'événements et les prestataires de solutions de billetterie. Les cyberattaques, les fuites de données et les interruptions de service peuvent avoir des conséquences désastreuses sur la réputation, les finances et la confiance des clients.

Ce guide a pour objectif de fournir un cadre pour la mise en place de mesures de cybersécurité et de résilience adaptées au secteur de l'événementiel. Il s'adresse aussi bien aux professionnels techniques qu'aux décideurs, en offrant une approche pédagogique pour comprendre les enjeux et des conseils pratiques pour renforcer la sécurité.

1. Comprendre les enjeux de la cybersécurité dans l'événementiel

1.1 Les risques spécifiques du secteur de l'événementiel et de la billetterie

Le secteur événementiel, par la nature de ses activités en ligne et la manipulation de données sensibles, est exposé à des cybermenaces spécifiques, quelles soient volontaires ou accidentelles. Voici les principaux risques identifiés :

- Vol de données personnelles des participants
- Fraude à la billetterie (contrefaçon, revente illégale)
- Interruption des systèmes informatiques pour l'organisation, les secours, la billetterie ou le contrôle d'accès
- Attaques par déni de service (DDoS) ou encombrement sur les plateformes de vente en ligne ou lors de l'événement
- Compromission des systèmes de paiement
- Atteinte à la réputation via les réseaux sociaux

1.2 L'importance de la protection des données personnelles

Les organisateurs d'événements et les plateformes de billetterie collectent et traitent de nombreuses données personnelles : noms, adresses, informations de paiement, etc. La protection de ces données est non seulement une obligation légale (RGPD, voir ci-après), mais aussi un enjeu de confiance pour les clients.

1.3 Les conséquences d'une cyberattaque ou d'une perte de données

Une cyberattaque réussie peut avoir des conséquences graves :

- Pertes financières directes : fraude, rançongiciel, manque à gagner sur le cashless chaque minute (boissons, merchandising, nourriture...)
- Coûts de remédiation et de notification des personnes concernées
- Sanctions administratives (CNIL)
- Perte de confiance des clients et partenaires
- Atteinte à la réputation et à l'image de marque

1.4 Dépendance à l'infrastructure technique

L'organisation d'un événement repose sur une infrastructure numérique qui s'avère critique. Cette centralisation, si elle améliore l'efficacité, expose aussi l'événement à des risques majeurs en cas de défaillance technique.

Une panne d'un lien Internet, un routeur défectueux, une coupure de courant ou un problème dans le cloud peuvent paralyser tout ou partie de l'événement en quelques secondes, avec des effets en cascade (blocage des entrées, files d'attente, perte de revenus, panique, atteinte à l'image…).

Pour limiter cette dépendance, les bonnes pratiques suivantes doivent être mises en place :

- Évaluer les points de défaillance uniques (SPOF) et les traiter en priorité (ex. : fibre unique sans backup, serveur non redondé…)
- Prévoir des connexions Internet de secours (4G/5G dédiée, deuxième lien fibre, liaison satellite en dernier recours) avec éventuellement un basculement automatique (failover)
- Gérer la priorité des flux critiques via la QoS
- Maintenir des modes dégradés pour les fonctions vitales : billetterie avec listes papier, paiements cashless avec terminaux offline, messages de sécurité préenregistrés sur clé USB ou en local

1.5 La préoccupation du temps : anticipation

Les menaces cyber ne naissent pas au moment de l'événement : elles sont préparées en amont, parfois plusieurs semaines ou mois avant la date de l'incident. Une attaque visible durant l'événement (ex. : indisponibilité d'un service, publication d'un message intrusif, compromission de comptes) est souvent la conséquence d'un processus silencieux de reconnaissance, d'infiltration ou de compromission.

Les attaquants opèrent généralement en plusieurs phases : repérage des prestataires techniques, recherche de vulnérabilités dans les applications de billetterie, attaques ciblées contre les comptes à privilège ou exploitation de défauts d'organisation (tests insuffisants, absence de journalisation…).

Cette logique impose de raisonner sur l'ensemble du cycle de vie de l'événement :

- Avant l'événement : durcir les systèmes, surveiller les tentatives d'accès anormales, cloisonner les environnements de test, auditer les connexions externes et sensibiliser les prestataires et les équipes techniques
- Pendant l'événement en restant en alerte
- Après l'événement : analyser les journaux, identifier les anomalies, évaluer les scénarios évités ou subis, et en tirer des leçons concrètes

L'événement est par nature éphémère, le temps de réaction lors d'un incident est donc primordial pour rétablir un fonctionnement nominal le plus rapidement possible. L'anticipation permet de faire gagner un temps précieux sans les contraintes de la gestion de crise.

2. Cadre réglementaire et normatif

2.1 Le Règlement Général sur la Protection des Données (RGPD)

Le RGPD impose des obligations strictes en matière de protection des données personnelles. Les organisateurs d'événements et les prestataires de billetterie doivent :

- Obtenir le consentement explicite des participants pour la collecte et le traitement de leurs données
- Mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des données
- Respecter les droits des personnes concernées (accès, rectification, effacement)
- Notifier les violations de données à la CNIL et aux personnes concernées dans les 72 heures
- Informer sur les durées de conservation des données et les appliquer
- Mettre en place un registre des activités de traitements de données (obligation au dessus de 250 salariés, critères spécifiques en dessous, mais dans le doute... autant le faire)

Attention, ces obligations sont autant valables au format numérique que papier et que l'information soit publique ou confidentielle !

2.2 La Directive NIS2 (Network and Information Security)

La directive européenne NIS2, en cours de transposition en France, impose des exigences de cybersécurité aux secteurs critiques. Sans être juridiquement contraignante pour l'événementiel, elle constitue une excellente base de bonnes pratiques : cartographie des systèmes critiques, gestion des risques, réaction aux incidents, continuité d'activité, implication de la direction. S'en inspirer volontairement permet de structurer une cybersécurité robuste, adaptée aux enjeux éphémères et interconnectés des événements.

2.3 Les normes et certifications

Plusieurs normes et certifications peuvent guider la mise en place d'un système de management de la sécurité et de la gestion des risques :

- ISO/IEC 27001 : Norme internationale pour le management de la sécurité de l'information
- ISO 22301 : Norme pour le management de la continuité d'activité
- PCI DSS pour la sécurité des données de paiement
- HDS : Hébergeur de Données de Santé pour les événements traitants de données sensibles
- ISO/TS 22317 : lignes directrices pour l'analyse d'impact sur les activités (BIA), utile pour prioriser les fonctions critiques à rétablir en cas de crise
- NFPA 1600 (États-Unis) : standard sur la gestion des urgences, adopté dans de nombreux plans d'organisation de grands rassemblements (festivals, événements sportifs, etc.)
- ISO 22320 : bonnes pratiques pour la gestion des urgence et la coordination entre équipes internes, sécurité, secours et prestataires

L'application de ces normes, même partielle, contribue à professionnaliser la gestion des incidents, réduire les temps d'interruption, et renforcer la confiance des parties prenantes.

3. Gouvernance de la sécurité de l'information

3.1 Définir une politique de sécurité

La mise en place d'une politique de sécurité de l'information est essentielle pour définir les objectifs, les rôles et les responsabilités en matière de cybersécurité. Cette politique doit :

- Être alignée sur les objectifs stratégiques de l'organisation
- Définir les principes directeurs de la sécurité
- Établir un cadre pour la gestion des risques
- Être régulièrement révisée et mise à jour

3.2 Désigner un responsable de la sécurité

La nomination d'un responsable de la sécurité des systèmes d'information (RSSI) est cruciale pour piloter la stratégie de cybersécurité. Soutenu (réellement) par la direction, il est en charge des missions suivantes :

- L'élaboration, la mise en œuvre et le suivi de la politique de sécurité (PSSI)
- La sensibilisation et la formation des employés
- La gestion des incidents de sécurité
- le reporting régulier à la direction et le cas échéant aux parties intéressées
- La veille sur les menaces et les réglementations

Dans le secteur événementiel, la fonction de RSSI peut être élargie ou fusionnée avec celle de Risk Manager (RM), afin de couvrir à la fois les aspects techniques de sécurité et la gestion globale des risques (juridiques, assurantiels, opérationnels). Cette approche intégrée permet d'anticiper les menaces de manière transverse, de mieux prioriser les actions en fonction des impacts potentiels, et de dialoguer efficacement avec la direction, les prestataires et les assureurs.

3.3 Gestion des risques

Une approche systématique de gestion des risques est nécessaire pour identifier, évaluer et traiter les menaces cybernétiques quelles soient volontaires (malveillance) ou non intentionnelles (accident, panne, erreur humaine) :

- Cartographier et qualifier les risques pouvant impacter l'événement
- Réaliser des analyses de risques régulières
- Mettre en place des mesures de sécurité proportionnées aux risques identifiés
- Effectuer des tests d'intrusion et des audits
  Mettre à jour régulièrement le plan de traitement des risques

Pour structurer l'analyse des impacts potentiels, une méthode simple et efficace consiste à évaluer les risques selon les quatre grands critères DICT :

- Disponibilité : le service ou l'information doivent-ils être accessibles en tout temps et en tout lieu (24h/24, accès à tous les personnels, etc)
- Intégrité : les données ou fonctions doivent-elles rester impérativement exactes et non altérées ?
- Confidentialité : les informations doivent-elles être protégées contre les accès non autorisés ?
- Traçabilité : doit-on pouvoir reconstituer l'historique des actions, accès et modifications ?

Cette grille permet de mieux qualifier les conséquences d'un incident et d'identifier les mesures de sécurité à prioriser selon les besoins métiers de l'événement.

4. Protection des données personnelles

4.1 Principes du RGPD

Les organisateurs d'événements et les prestataires de billetterie doivent appliquer les principes fondamentaux du RGPD :

- Licéité, loyauté et transparence du traitement
- Limitation des finalités
- Minimisation des données
- Exactitude des données
- Limitation de la conservation
- Intégrité et confidentialité
- Responsabilité (accountability)

4.2 Mesures techniques et organisationnelles

Pour assurer la protection des données personnelles, il est nécessaire de mettre en place des mesures techniques et organisationnelles appropriées :

- Chiffrement des données sensibles, tant au repos qu'en transit
- Pseudonymisation et anonymisation des données lorsque possible
- Contrôle d'accès strict basé sur le principe du moindre privilège
- Journalisation et surveillance des accès aux données personnelles
- Formation et sensibilisation régulière des employés aux bonnes pratiques de protection des données

4.3 Gestion des consentements

La gestion des consentements est un aspect crucial de la conformité au RGPD :

- Obtenir un consentement explicite et spécifique

pour chaque finalité de traitement
- Fournir des informations claires et compréhensibles sur l'utilisation des données
- Mettre en place des mécanismes simples pour retirer le consentement
- Conserver une trace des consentements obtenus

4.4 Exercice des droits des personnes concernées

Les organisateurs d'événements doivent faciliter l'exercice des droits des participants :

- Droit d'accès aux données personnelles
- Droit de rectification des données inexactes
- Droit à l'effacement (droit à l'oubli)
- Droit à la limitation du traitement
- Droit à la portabilité des données

5. Sécurité des systèmes d'information

5.1 Sécurité du réseau

La sécurité du réseau est fondamentale pour protéger les systèmes d'information :

- Segmentation du réseau pour isoler les systèmes critiques et séparer les usages : VLAN dédiés par fonction (billetterie, administration, prestataires, médias, public)
- Cloisonnement strict des réseaux IoT événementiels (capteurs, contrôle d'accès, équipements scéniques)
- Mise en place de pare-feu et de systèmes de détection d'intrusion (IDS)
- DMZ spécifiques pour les services exposés (billetterie en ligne, streaming, applications mobiles
- Utilisation de réseaux privés virtuels (VPN) pour les accès distants
- Contrôles de flux inter-zones basés sur le principe du moindre privilège
- Sécurisation des réseaux Wi-Fi publics lors des événements 34

5.2 Sécurité des réseaux Wi-Fi

Les réseaux Wi-Fi utilisés sur un événement doivent faire l'objet de mesures de sécurité adaptées à leur usage (public ou privé) afin de limiter les risques d'intrusion, d'interception de données ou de propagation de malware.

- Wi-Fi public : Il doit être totalement isolé des systèmes critiques. Un portail captif est recommandé pour informer l'utilisateur et obtenir son consentement. La bande passante doit être limitée pour éviter les abus. Aucun accès au réseau d'administration ou aux équipements internes ne doit être possible.
- Wi-Fi privé (équipe, billetterie, régie) : Il doit être protégé par un chiffrement fort (WPA2 ou idéalement WPA3), avec filtrage des équipements par adresse MAC et un mot de passe fort, régulièrement renouvelé. Ce réseau doit être cloisonné et surveillé.

Enfin, il est fortement déconseillé de se connecter à des réseaux Wi-Fi non identifiés ou non sécurisés, notamment pour les postes de travail ou les terminaux d'encaissement.

5.3 Sécurité des endpoints

La protection des postes de travail et des appareils mobiles est essentielle :

- Déploiement de solutions antivirus et antimalware
- Mise à jour régulière des systèmes d'exploitation et des applications
- Chiffrement des disques durs des appareils mobiles
- Mise en place de politiques de mots de passe robustes

5.4 Gestion des accès et des identités

Une gestion rigoureuse des accès permet de limiter les risques de compromission :

- Mise en place de l'authentification multifacteur (MFA) adaptative, selon le profil de risque (organisateurs, techniciens, prestataires...)
- Gestion des droits d'accès basée sur les rôles (RBAC)
- Revue régulière des droits d'accès
- Utilisation de solutions de gestion des identités et des accès (IAM)

5.5 Sécurité des applications

Les applications de billetterie et de gestion d'événements doivent être sécurisées :

- Développement sécurisé (Security by Design)
- Tests de sécurité réguliers (tests d'intrusion, analyse de code)
- Gestion des vulnérabilités et application rapide des correctifs
- Protection contre les attaques web courantes (injection SQL, XSS, CSRF)

5.6 Sécurité cloud

Pour les solutions hébergées dans le cloud :

- Choisir des fournisseurs cloud conformes aux bonnes pratiques ou certifiés ou s'assurer auprès du prestataire du lieu d'hébergement des don-

nées et des règles de sécurité en place
- Mettre en place un chiffrement des données en transit et au repos
- Gérer rigoureusement les droits d'accès aux ressources cloud
- Surveiller en permanence l'activité et les accès aux services cloud

6. Sécurité des opérations de billetterie

6.1 Sécurisation des transactions

La sécurité des transactions financières est à suivre particulièrement :

- Utilisation de protocoles de paiement sécurisés (3D Secure)
- Conformité aux normes PCI DSS pour le traitement des données de cartes bancaires
- Mise en place de systèmes de détection de fraude
- Chiffrement de bout en bout des données de paiement

6.2 Lutte contre la fraude à la billetterie

Pour prévenir la fraude et la contrefaçon de billets :

- Utilisation de codes QR dynamiques ou de technologies NFC
- Mise en place de systèmes de vérification en temps réel des billets
- Limitation du nombre de billets par transaction
- Surveillance des activités suspectes (achats massifs, reventes)

6.3 Gestion des accès lors des événements

La sécurité physique lors des événements est tout aussi importante :

- Utilisation de systèmes de contrôle d'accès électroniques
- Formation du personnel à la détection des fraudes
- Mise en place de procédures de gestion des incidents
- Coordination avec les services de sécurité de l'événement

7. Continuité d'activité et gestion de crise

7.1 Plan de continuité d'activité (PCA) et Plan de reprise d'activité (PRA)

Dans le monde de l'événementiel, par nature éphémère et concentré sur quelques jours, il est peu pertinent de distinguer strictement un Plan de Continuité d'Activité (PCA) d'un Plan de Reprise d'Activité (PRA) comme dans les organisations classiques à fonctionnement permanent. Ceci contrairement au cas éventuel de l'équipe de préparation «à demeure» tout au long de l'année, qui doit être traitée de manière classique.

Le PCA vise en théorie à maintenir les activités critiques en cas d'incident, tandis que le PRA se concentre sur leur redémarrage après une interruption. Dans l'événementiel, ces deux logiques doivent être fusionnées pour une réponse pragmatique et orientée vers la limitation des impacts dans un laps de temps très court (heures, voire minutes).

La bonne pratique repose sur un mix entre continuité et redondance :

- Prévoir des systèmes de secours opérationnels en quelques minutes (2e lien Internet, matériel de remplacement prêt à l'emploi, alimentation de secours, connexions 4G/5G dédiées)
- Utiliser des modes dégradés pensés en amont (billetterie papier, paiements offlines, messages pré-enregistrés)
- Mettre en œuvre des équipes techniques formées à basculer rapidement d'un mode à l'autre

Dans ce cadre, un «PCA/PRA événementiel» doit être simple, documenté, testé à blanc avant l'ouverture, et centré sur les fonctions vitales : billetterie, contrôle d'accès, paiement, communication d'urgence, etc.

7.2 Gestion de crise cybernétique

La préparation à la gestion de crise est cruciale :

- Constitution d'une cellule de crise avec des rôles et responsabilités définis
- Élaboration de scénarios de crise et réalisation d'exercices de simulation
- Préparation de modèles de communication de crise
- Mise en place d'un processus de retour d'expérience post-incident

8. Formation et sensibilisation

8.1 Programme de sensibilisation

La sensibilisation de tous les employés est essentielle :

- Sessions de formation régulières sur les risques cyber et les bonnes pratiques
- Campagnes de phishing simulé pour tester la vigilance des employés
- Diffusion régulière d'informations sur les menaces actuelles
- Intégration de la sécurité dans le processus d'accueil des nouveaux employés

8.2 Formation technique

Pour le personnel IT et les développeurs :

- Formations spécifiques sur la sécurité des systèmes et des réseaux
- Ateliers sur le développement sécurisé et les tests de sécurité
- Participation à des conférences et événements sur la cybersécurité
- Certification des compétences (ex: CISSP, CEH)

9. Surveillance et réponse aux incidents

9.1 Détection des menaces

La mise en place d'une capacité de détection des menaces est cruciale :

- Déploiement de solutions SIEM (Security Information and Event Management)
- Utilisation de systèmes de détection et de réponse sur les endpoints (EDR)
- Mise en place d'une veille sur les menaces (Threat Intelligence)
- Analyse comportementale pour détecter les anomalies

9.2 Gestion des incidents

Un processus structuré de gestion des incidents doit être en place :

- Définition d'une procédure de réponse aux incidents et formation aux gestes d'urgence (information, déconnexion des machines, conservation des logs...)
- Notification et chaîne de responsabilité
- Constitution d'une équipe de réponse aux incidents de sécurité (les CSIRT peuvent être une aide)
- Mise en place d'outils de forensics et d'analyse post-mortem
- Collaboration avec les autorités compétentes (ANSSI, CNIL) en cas d'incident majeur

9.3 Amélioration continue

L'amélioration continue est essentielle pour maintenir un niveau de sécurité élevé :

- Analyse régulière des incidents et des presqueincidents
- Mise à jour des politiques et procédures en fonction des retours d'expérience
- Veille technologique et réglementaire
- Benchmarking avec d'autres acteurs du secteur

10. Technologies émergentes et innovation

10.1 Intelligence artificielle et machine learning

L'IA et le ML offrent de nouvelles opportunités pour la sécurité :

- Détection avancée des menaces basée sur l'apprentissage automatique
- Analyse comportementale pour identifier les activités suspectes
- Automatisation de la réponse aux incidents
- Prédiction et prévention des menaces émergentes

10.2 Blockchain

La technologie blockchain peut renforcer la sécurité des billets :

- Création de billets infalsifiables et traçables
- Gestion sécurisée des transferts de billets
- Lutte contre la revente illégale et la fraude
- Transparence accrue des transactions

10.3 Internet des objets (IoT)

L'IoT présente des opportunités et des défis pour la sécurité des événements :

- Utilisation de capteurs pour la gestion des foules et la sécurité
- Mise en place de contrôles d'accès basés sur l'IoT
- Sécurisation des dispositifs IoT contre les cyberattaques
- Gestion de la confidentialité des données collectées par les objets connectés

Ils étendent le périmètre de menace cyber, parfois fortement si les choix de matériels et leur gestion ne tiennent pas compte de l'aspect sécurité. La dépendance à ces objects connectés dans la chaine de décision peut engendrer des problèmes en cas de défaillance (panne, faux-positif).

Des principes de précaution doivent être mis en place pour limiter ce risque :

- Mise à jour régulière et via les sites officiels
- Ajouter le cloisonnement réseau (VLAN dédiés)
- Inclure la sécurisation des cas d'usage spécifiques : contrôle d'accès, billetterie, capteurs
- Inclure le possibilité de défaillance des capteurs dans la gestion de risque

11. Conformité et audit

11.1 Audits de sécurité

Des audits réguliers sont nécessaires pour évaluer l'efficacité des mesures de sécurité :

- Audits internes et externes de la sécurité des systèmes d'information
- Tests d'intrusion et scans de vulnérabilités
- Audits de conformité RGPD
- Revues de code pour les applications critiques
- Exercices de gestion de crise (cyber ou panne informatique par exemple)

En cas d'audit demandé par un client, l'obtention de certifications peut démontrer l'engagement en matière de sécurité et raccourcir les phases de questionnement (voir le paragraphe sur les normes et certifications).

11.2 Reporting et tableaux de bord

La mise en place d'indicateurs de performance (KPI) permet de suivre l'évolution de la posture de sécurité :

- Taux de conformité aux politiques de sécurité
- Nombre et gravité des incidents de sécurité
- Temps de détection et de résolution des incidents
- Taux de sensibilisation des employés
- Taux de disponibilité d'un service particulier

Ceci durant l'événement mais également d'une édition à l'autre par exemple.

12. Collaboration et partage d'informations

12.1 Partenariats public-privé

La collaboration avec les autorités et les organismes spécialisés est importante :

- Participation aux programmes de l'ANSSI (ex: CERT-FR)
- Échanges avec la CNIL sur les bonnes pratiques de protection des données
- Collaboration avec les forces de l'ordre pour la lutte contre la fraude

12.2 Partage d'informations au sein du secteur

Le partage d'informations entre acteurs du secteur renforce la sécurité collective :

- Participation à des groupes de travail sectoriels sur la cybersécurité
- Échange d'informations sur les menaces et les incidents (dans le respect de la confidentialité)
- Partage de bonnes pratiques et de retours d'expérience

Conclusion

La cybersécurité et la résilience sont une préoccupation d'actualité pour les organisateurs d'événements et les prestataires de solutions de billetterie. En adoptant une approche globale et d'anticipation, basée sur les bonnes pratiques et les recommandations des autorités compétentes, les acteurs du secteur peuvent significativement renforcer leur posture de sécurité.

Ce guide fournit un cadre complet pour aborder ces défis en partant des risques, en couvrant les aspects techniques, organisationnels et humains de la sécurité. La mise en œuvre de ces recommandations permettra non seulement de se conformer aux exigences réglementaires, mais aussi de gagner la confiance des clients et des partenaires en rendant son événement résilient.

Dans un environnement où les menaces évoluent constamment, la vigilance et l'amélioration continue sont essentielles. En faisant de la cybersécurité une priorité stratégique, les organisateurs d'événements et les prestataires de billetterie peuvent assurer la pérennité de leurs activités et offrir des expériences sûres et mémorables à leurs clients.

Cybersécurité et résilience en événementiel
Exemples de scenarios

Attaque de type «Watering hole»

Contexte :
Lors de ce festival, de nombreux exposants utilisent des plateformes en ligne pour partager des informations sur leurs produits et services, ainsi que pour vendre des billets. Les attaquants pourraient cibler ces exposants en compromettant le site web d'une plateforme qu'ils utilisent fréquemment.

Scénario :
Un pirate informatique infecte le site utilisé par les exposants. Lorsqu'un exposant se connecte pour vérifier ses ventes ou les informations sur les participants, il est redirigé vers un site malveillant déguisé en page de connexion. En entrant ses informations d'identification, l'exposant compromet son compte, permettant ainsi à l'attaquant d'accéder à des données sensibles.

Impact :
Cette attaque pourrait entraîner le vol d'informations confidentielles, comme les coordonnées des clients, ainsi qu'une perte de confiance envers la plateforme de billetterie. Cela pourrait également perturber le bon déroulement de l'événement.

Mesures de protection :
Pour contrer cette menace, il est recommandé d'utiliser un système de sécurité comme Palo Alto, qui peut détecter et bloquer les connexions vers des sites malveillants, garantissant ainsi la sécurité des connexions des exposants.

Quishing (QR Code phishing)

Contexte :
Les festivals de musique utilisent souvent des QR codes pour faciliter les paiements sans espèces et pour fournir des informations sur les événements. Dans ce cadre, des QR codes authentiques peuvent être remplacés par des codes malveillants.

Scénario :
Un attaquant place un sticker sur un QR code affiché dans la zone de restauration du festival. Ce sticker contient un QR code malveillant qui redirige les utilisateurs vers un faux site de commande de repas avec paiement. Les participants, pensant accéder à un service de paiement légitime, pourraient entrer leurs informations de carte de crédit et d'autres données personnelles.

Impact :
Cela pourrait entraîner des pertes financières pour les participants et une atteinte à la réputation des organisateurs du festival. De plus, les utilisateurs pourraient se sentir en danger, ce qui pourrait nuire à la fréquentation des futurs événements.

Mesures de protection :
Pour minimiser les risques associés à cette attaque, l'utilisation d'un pare-feu avancé pour surveiller le réseau Wi-Fi public est essentielle. Cela permettrait de détecter et de bloquer les activités suspectes, protégeant ainsi les participants contre les tentatives de quishing.

Rançongiciel (Ransomware) ciblant l'infrastructure de l'événement

Contexte :
De nombreux festivals et événements utilisent des infrastructures IT pour gérer l'accès aux billets, les paiements cashless, les écrans numériques diffusant les annonces, ou encore les réseaux internes pour les organisateurs et exposants.

Scénario :
Un attaquant infiltre un système informatique clé, tel que le système de billetterie ou le réseau interne des organisateurs. En déclenchant un rançongiciel, il chiffre toutes les données et exige une rançon en crypto-monnaie pour les débloquer.

Impact :
Perturbation totale du festival (tickets non valables, paiements impossibles, écrans bloqués).
Perte de revenus (paiements bloqués, remboursements obligatoires).
Atteinte catastrophique à la réputation des organisateurs.

Mesures de protection :
Mise en place d'un système de sécurité avancé, capable d'identifier et de neutraliser les menaces de ransomware avant qu'elles n'infectent le système.
Sauvegardes régulières des données critiques pour une restauration rapide en cas d'attaque.
Segmentation des réseaux

Usurpation Wi-Fi (Evil twin attack)

Contexte :
Lors d'un salon professionnel, les participants se connectent souvent au réseau Wi-Fi public pour économiser leur forfait mobile ou en cas de réseau mobile faible. Les attaquants peuvent exploiter cette habitude en créant un faux réseau Wi-Fi légitime ressemblant à celui de l'événement (par exemple, «Salon2025_WiFi»).

Scénario :
Un attaquant configure un faux réseau Wi-Fi dans la zone de l'événement. Les participants s'y connectent sans méfiance, permettant ainsi à l'attaquant d'intercepter leurs données (mots de passe, informations bancaires, etc.) ou d'injecter des logiciels malveillants sur leurs appareils.

Impact :
Vol de données personnelles et financières des participants.
Infection massive des appareils connectés.
Atteinte à la confiance des participants envers l'organisation de l'événement.

Mesures de protection :
Communiquer clairement le nom officiel du Wi-Fi.
Désactiver la connexion automatique sur les appareils.
Sécuriser le Wi-Fi public avec un portail captif et cloisonner totalement ce réseau des systèmes internes.
Surveiller les réseaux suspects (détection de Rogue AP).
Sensibiliser les équipes à ne pas se connecter à des réseaux non reconnus.

Faux message d'évacuation ou d'urgence

Contexte :
Lors d'une retransmission publique d'un match de football sur écran géant, des milliers de spectateurs se rassemblent dans un espace ouvert. Les organisateurs s'appuient sur un système d'affichage vidéo et de sonorisation pour diffuser le match, les messages logistiques ou d'alerte. Ce dispositif, souvent connecté à un réseau informatique, peut devenir une cible pour un attaquant souhaitant perturber l'événement.

Scénario :
Un cybercriminel pirate les écrans numériques ou le système d'annonces sonores pour diffuser un faux message d'évacuation ou une alerte de sécurité (par exemple, une menace terroriste fictive), ou encore un message politique hors contexte ou une vidéo inappropriée. Cela provoque un mouvement de panique parmi les participants.

Impact :
Mouvement de foule incontrôlé, mettant en danger les participants. Perte de contrôle de l'événement par les organisateurs.
Enquête médiatique et atteinte à la réputation de l'événement.

Mesures de protection :
Sécuriser les systèmes d'affichage et les systèmes sonores avec des accès restreints et surveillés. (Réseau dédié)

Coupure Internet accidentelle lors d'un événement

Contexte :
Pour chaque événement, la connectivité Internet est devenue un pilier invisible mais indispensable. Elle supporte de nombreux services critiques et pourtant elle repose souvent sur une seule liaison fibre pour «particulier». Ce lien unique constitue un point de défaillance critique : un simple incident de chantier peut suffire à couper toute la connectivité du site quelques heures avant l'ouverture au public.

Scénario :
Lors d'un grand festival de plein air, la connexion Internet principale du site repose sur une fibre optique mutualisée avec la ville. Elle est utilisée pour gérer les systèmes critiques tels que la billetterie, les paiements cashless, les écrans d'affichage et les communications internes. Cependant, quelques heures avant l'ouverture des portes, un accident survient : une pelleteuse utilisée pour des travaux coupe accidentellement la fibre optique reliant le site à Internet.

Impact :
Une coupure accidentelle d'Internet peut provoquer l'interruption brutale des systèmes critiques de l'événement :
Billetterie en ligne inaccessible, terminaux de paiement cashless inopérants, écrans d'affichage figés, communications internes désorganisées. Les conséquences immédiates sont des files d'attente massives, une impossibilité de vendre sur place, une perte de chiffre d'affaires pour les exposants, et une frustration généralisée des participants.

Mesures de protection :
Prévoir une 2e connexion indépendante (4G/5G dédiée, fibre sur un autre parcours, satellite).
Mettre en place un système de bascule automatique (failover) vers la liaison de secours.
Activer des modes dégradés : billetterie papier, terminaux de paiement offline, fichiers locaux.
Sensibiliser les équipes techniques à la procédure de bascule et tester le dispositif en amont.
Identifier les points de défaillance critiques (SPOF) et les corriger dès la phase de préparation.

Glossaire

A Accès (contrôle d') : Ensemble des mécanismes permettant de limiter l'accès aux ressources d'un système d'information aux seules personnes, entités ou processus autorisés

Algorithme : Suite d'étapes permettant d'obtenir un résultat à partir de données d'entrée. Utilisé notamment en intelligence artificielle et en cryptographie

Anonymisation : Procédé qui consiste à transformer des données personnelles de façon irréversible pour qu'elles ne permettent plus d'identifier une personne de façon directe ou indirecte

Authentification : Procédure permettant de vérifier l'identité d'un utilisateur, d'un appareil ou d'un service avant d'autoriser l'accès à un système

B Backdoor (Porte dérobée) : Mécanisme caché permettant d'accéder à un système ou à des données sans passer par les procédures de sécurité normales

Base légale : Fondement juridique qui autorise un organisme à collecter ou utiliser des données personnelles dans le cadre d'un traitement

BCR (Binding Corporate Rules – Règles d'entreprise contraignantes) : Ensemble de règles internes adoptées par un groupe d'entreprises pour encadrer les transferts de données personnelles hors de l'Espace économique européen

Big Data (Données massives) : Ensemble de données numériques volumineuses, variées et produites à grande vitesse, nécessitant des outils spécifiques pour leur traitement et leur analyse

Biométrie : Techniques informatiques permettant de reconnaître automatiquement un individu à partir de caractéristiques physiques, biologiques ou comportementales

Blockchain : Technologie de stockage et de transmission d'informations, transparente, sécurisée et décentralisée, constituant une base de données chronologique d'échanges

Botnet : Réseau de machines compromises contrôlées à distance pour mener des attaques coordonnées

C Cheval de Troie : Programme malveillant déguisé en application légitime, permettant un accès non autorisé

Chiffrement : Procédé de transformation de données en une forme inintelligible pour les personnes non autorisées, afin d'en garantir la confidentialité

CNIL (Commission Nationale de l'Informatique et des Libertés) : Autorité administrative indépendante française chargée de veiller à la protection des données personnelles

Consentement : Manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle une personne accepte le traitement de ses données personnelles

CSIRT (Computer Security Incident Response Team) : Équipe spécialisée dans la réponse aux incidents de sécurité informatique, chargée de détecter, analyser et réagir rapidement à des cyberattaques

D DMP (Data Management Platform – Plateforme de gestion des données) : Service collectant et gérant des données utilisateurs issues de différentes sources pour optimiser les campagnes marketing et publicitaires

DMZ (Demilitarized Zone) : Zone réseau intermédiaire entre un réseau interne sécurisé et l'extérieur (Internet), permettant d'exposer certains services (site web, billetterie...) tout en limitant les risques pour le reste du SI

Délégué à la protection des données (DPD ou DPO – Data Protection Officer) : Personne chargée de veiller à la conformité d'un organisme au RGPD et à la protection des données personnelles traitées

Directive NIS (Network and Information Security) : Directive européenne visant à assurer un niveau élevé de sécurité des réseaux et systèmes d'information au sein de l'Union européenne

Données personnelles : Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement

E EDR (Endpoint Detection and Response) : Solution de surveillance et de réponse aux menaces sur les postes de travail (ordinateurs, tablettes, etc.) capable de détecter et bloquer des attaques en temps réel

Endpoint (Point de terminaison) : Appareil connecté à un réseau informatique (ordinateur, smartphone, tablette, etc.) qui peut constituer une cible pour des attaques

Ensemble d'entraînement/d'apprentissage : Jeu de données utilisé pour entraîner un modèle d'intelligence artificielle à effectuer une tâche spécifique

ENT (Espace Numérique de Travail) : Plateforme intégrée de services numériques destinée aux acteurs de la communauté éducative

Exploit : Code tirant parti d'une vulnérabilité pour exécuter des actions non autorisées

F Failover : Procédé automatique de bascule vers un système ou une connexion de secours en cas de défaillance, afin d'assurer la continuité de service

Fast-flux : Technique de dissimulation de sites malveillants en changeant rapidement d'adresses IP

FSN (Fournisseur de Services Numériques) : Entreprise fournissant des services numériques essentiels, soumise à certaines obligations de sécurité (notamment dans le cadre de la directive NIS)

G Gestion des accès : Ensemble des procédures et outils permettant de gérer les droits d'accès des utilisateurs aux ressources d'un système d'information

I IAM (Identity and Access Management – Gestion des identités et des accès) : Ensemble de processus et technologies permettant de gérer les identités numériques et les droits d'accès aux ressources informatiques

Incident de sécurité : Événement ayant un impact négatif sur la sécurité d'un système d'information, tel qu'une intrusion, une fuite de données ou une attaque informatique

ISO/IEC 27001 : Norme internationale pour le management de la sécurité de l'information, définissant les exigences pour établir, mettre en œuvre et améliorer un système de gestion de la sécurité de l'information

ISO 22301 : Norme internationale relative au management de la continuité d'activité, visant à assurer la résilience des organisations face aux incidents majeurs

M MFA (Multi-Factor Authentication – Authentification multifacteur) : Procédure d'authentification nécessitant au moins deux preuves distinctes de l'identité de l'utilisateur (mot de passe, code SMS, biométrie, etc.)

Malware (Logiciel malveillant) : Programme conçu pour nuire à un système informatique, voler des données ou perturber le fonctionnement d'un appareil

O OSINT (Open Source Intelligence) : Collecte et analyse d'informations accessibles publiquement (sites web, réseaux sociaux, forums, documents officiels, etc.) dans le but d'en tirer des renseignements exploitables

P PCA (Plan de Continuité d'Activité) : Ensemble de mesures et de procédures visant à assurer le maintien des activités essentielles d'une organisation en cas de crise ou d'incident majeur

PRA (Plan de Reprise d'Activité) : Planification des actions à mener pour restaurer les activités après un incident ayant interrompu le fonctionnement normal de l'organisation

Pare-feu (Firewall) : Dispositif de sécurité permettant de filtrer les flux de données entre différents réseaux afin d'empêcher les accès non autorisés ou malveillants

Payload : Charge utile d'un malware, représentant l'action malveillante exécutée

Pharming : Technique de redirection du trafic vers un site frauduleux malgré une URL correcte

Phishing (Hameçonnage) : Technique d'ingénierie sociale visant à tromper un utilisateur (par e-mail, SMS ou autre canal) pour l'amener à révéler des informations sensibles (identifiants, mots de passe, données bancaires), souvent via un faux site

Pot de miel (Honeypot) : Système leurre destiné à attirer et analyser les attaques

Pseudonymisation : Traitement de données personnelles visant à rendre impossible l'identification d'une personne sans informations supplémentaires conservées séparément

PSSI (Politique de Sécurité des Systèmes d'Information) : Document stratégique définissant les objectifs, principes et règles en matière de cybersécurité d'une organisation

Q QoS (Quality of Service) : Mécanisme de gestion du trafic réseau permettant de prioriser certains flux (par exemple la billetterie ou la vidéo surveillance) pour garantir leur performance même en cas de congestion

R RBAC (Role-Based Access Control – Contrôle d'accès basé sur les rôles) : Méthode de gestion des droits d'accès attribués selon le rôle de chaque utilisateur dans l'organisation

Règle de détection : Ensemble de critères définissant une activité suspecte (signature, comportement)

RGPD (Règlement Général sur la Protection des Données – GDPR en anglais) : Règlement européen encadrant la protection des données personnelles et la vie privée des citoyens de l'Union européenne

Risque : Possibilité qu'un événement ou une action ait un impact négatif sur la sécurité des systèmes d'information ou sur la protection des données

Rogue AP : point d'accès Wi-Fi installé sans autorisation, souvent par un attaquant, pour imiter un réseau légitime. Il sert à piéger les utilisateurs en les incitant à s'y connecter, afin d'intercepter leurs données ou d'injecter des logiciels malveillants

Rootkit : Logiciel malveillant permettant de dissimuler la présence d'autres programmes malveillants

RSSI (Responsable de la Sécurité des Systèmes d'Information) : Personne en charge de la définition et de la mise en œuvre de la politique de sécurité des systèmes d'information dans une organisation

S SI (Système d'Information) : Ensemble des ressources (matériels, logiciels, données, procédures, personnel) permettant de collecter, stocker, traiter et diffuser de l'information dans une organisation

SIEM (Security Information and Event Management) : Outil qui collecte et analyse les journaux (logs) de sécurité pour détecter en temps réel les comportements anormaux ou les incidents de sécurité

Smishing : Variante du phishing utilisant des messages SMS pour tromper l'utilisateur

Sniffer : Outil capturant le trafic réseau pour en analyser le contenu

SOC (Security Operations Center) : Centre de supervision de la sécurité regroupant des experts en charge de la surveillance, de la détection et de la réponse aux incidents de sécurité 24/7

SPOF (Single Point of Failure – Point de défaillance unique) : composant ou un maillon unique d'un système dont la défaillance entraînerait l'arrêt total ou partiel du service. Dans le contexte d'un événement, cela peut être un seul lien Internet, un serveur central, un switch réseau ou même une personne clé sans backup

T Test d'intrusion (Pentest) : Simulation d'attaque informatique réalisée afin d'identifier les vulnérabilités d'un système et d'évaluer son niveau de sécurité

Threat Intelligence : Veille sur les menaces cyber permettant de suivre l'évolution des techniques d'attaque et d'anticiper les risques spécifiques à un secteur ou à un événement

Tracking : Ensemble des techniques permettant de suivre le comportement des utilisateurs sur un site web ou une application, souvent à des fins publicitaires ou d'analyse

V VPN (Virtual Private Network – Réseau privé virtuel) : Technologie permettant de créer une connexion sécurisée entre un utilisateur et un réseau, en chiffrant les données échangées

Vulnérabilité : Faiblesse d'un système d'information pouvant être exploitée par une menace pour compromettre sa sécurité

Ressources

Acteurs de la cybersécurité :

Agence nationale de la sécurité des systèmes d'information (ANSSI)
https://cyber.gouv.fr/

Commission nationale informatique et liberté (CNIL)
https://cybermalveillance.gouv.fr

Réseau des CSIRT
https://www.cert.ssi.gouv.fr/csirt/

Guides :

Crise d'origine cyber, Les clés d'une gestion opérationnelle et stratégique - ANSSI
https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique

Guide de la sécurité des données personnelles : nouvelle édition 2024 - CNIL
https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024

EBIOS Risk Manager - ANSSI
https://cyber.gouv.fr/la-methode-ebios-risk-manager

Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - ANSSI
https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection

Sensibilisation du collaborateur, Le maillon essentiel de la cybersécurité - Clusif
https://clusif.fr/publications/sensibilisation-collaborateur-cybersecurite/

Normes :

ISO/IEC 27001:2022 - Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences
https://www.iso.org/fr/standard/27001

ISO 22301:2019 - Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences
https://www.iso.org/fr/standard/75106.html

ISO/TS 22317:2021 - Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour le bilan d'impact sur l'activité
https://www.iso.org/fr/standard/79000.html

ISO 22320:2018 - Sécurité et résilience — Gestion des urgences — Lignes directrices pour la gestion des incidents
https://www.iso.org/fr/standard/67851.html

HDS - Hébergeur de Données de Santé
https://esante.gouv.fr/produits-services/hds

PCI DSS - Norme de sécurité de l'industrie des cartes de paiement
https://www.pcisecuritystandards.org/lang/fr-fr/

NFPA 1600 - Standard on Continuity, Emergency, and Crisis Management
https://www.nfpa.org/codes-and-standards/nfpa-1600-standard-development/1600

Ressources diverses :

Plan de Continuité d'Activité - Wikipédia
https://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9_d%27activit%C3%A9

Cyber Resilience Act - Commission Européenne
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Cybersecurity Best Practices - CISA
https://www.cisa.gov/topics/cybersecurity-best-practices

Glossaire des menaces - Clusif
https://clusif.fr/services/glossaire-des-menaces/

CyberDico - ANSSI
https://cyber.gouv.fr/le-cyberdico

Radar RSSI - Wavestone
https://www.wavestone.com/fr/insight/radar-rssi-2025/

MOOC - ANSSI
https://secnumacademie.gouv.fr/

Formation SensCyber
https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre

Diagnostic « victime »
https://www.cybermalveillance.gouv.fr/diagnostic/profil#

Notification de violation de données personnelles
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Contactez-nous

03 39 09 40 60

conseil@trinaps.com

TRINAPS · S.A.S. au capital de 48 000 €
11 rue Sophie Germain 90000 BELFORT
SIRET 499445906 00021 · RCS Belfort
APE 6110Z · TVA Intracom. FR70499445906

www.trinaps.com