CYBER DEFENSE AFRICA

CYBER DEFENSE AFRICA S.A.S.

Guide des bonnes pratiques pour la sécurité incendie des data centers

11/09/2020

CYBER DEFENSE AFRICA

Table des matières

Informations du document

Information	
Titre	Guide des bonnes pratiques pour la sécurité incendie des data centers
Auteur	CDA
Contact	contact@cda.tg
Site Web	www.cda.tg

Version du document	Date	Nature des modifications
1.0	11/09/2020	Version originale

Ressources

Titre	URL
Fire Protection of Computer Rooms - Legal Obligations and Best Practices	https://www.isaca.org/resources/isaca-journal/past-issues/2014/fire-protection-of-computer-rooms-legal-obligations-and-best-practices
Sun Microsystems Data Center Site Planning Guide	https://docs.oracle.com/cd/E19065-01/servers.e20k/805-5863-13/ch5.html
Best Practice Guide to Fire Safety	https://huttonrudbyvillagehall.org.uk/wp-content/uploads/2016/02/FIA-Best-practice-guide.pdf

1. Préambule

Un incendie dans un data center peut endommager les équipements électroniques et la structure du bâtiment de manière irréparable. La contamination d'un feu couvant peut également avoir des effets très dommageables sur le matériel et peut entraîner des coûts élevés de réparations. Même si l'incendie proprement dit est évité, la décharge du moyen d'extinction d'incendie peut avoir un impact dommageable sur le matériel. Qu'ils soient mesurés en termes de menace pour la sécurité humaine, de dommages à l'équipement informatique ou de baisse d'activité due à une perturbation des systèmes, les coûts d'un incendie peuvent être énormes.

Les mesures adoptées pour la sécurité physique et l'incendie dans un data center doivent prendre en compte à la fois le matériel et les opérateurs travaillant dans la salle. Dans la plupart des cas, les objectifs de protection des équipements électronique sont en adéquation avec les objectifs de sécurité humaine.

Ce guide de CDA recense les bonnes pratiques organisationnelles, techniques et humaines à adopter pour la protection contre l'incendie des salles hébergent les équipements informatiques.

2. Mesures organisationnelles

De nombreuses mesures peuvent être prises pour éviter les risques d'incendie dans un data center. La conformité **au standard NFPA 75** augmente considérablement la sécurité incendie dans le data center.
Dans le cadre de la protection contre le risque incendie, il est indispensable de disposer d'un plan d'incendie écrit, daté et testé annuellement approuvé par la direction, un plan de contrôle des dommages et des procédures de récupération pour la continuité des activités.
Ce plan doit comporter :

- La politique de sécurité incendie et les procédures
- L'évaluation des risques d'incendie et identification des dangers et des risques
- Les précautions générales prises contre les incendies avec les mesures de prévention et de détection des incendies
- Le plan d'urgence incendie et les moyens d'évacuation adéquats en cas d'incendie
- Le plan de maintenance de tous les systèmes et équipements de sécurité incendie
- Les procédures détaillant les actions à mettre en place lorsqu'un équipement électronique est mouillé, endommagé par la fumée ou autrement affecté à la suite d'un incendie.
- Le plan de formation et de sensibilisation des employés et de l'équipe d'intervention
- Le plan de revue et de mise à jour des procédures

3. Mesures techniques

3.1. Mesures préventives

Les précautions suivantes doivent être prises en compte dans la conception et la maintenance de la salle informatique et des zones d'assistance.

3.1.1. Évitez le stockage inutile

Les matériaux combustibles doivent être évités dans la salle. Seules les fournitures minimales absolument nécessaires au fonctionnement de la salle doivent être conservées dans son périmètre. Les matériaux d'emballage et autres articles inutiles doivent être retirés.

3.1.2. Climatisation du data center

Les serveurs et équipements réseaux hébergés dans les data center dégagent d'importantes quantités de chaleur dans un espace de plus en plus réduit en volume. Le risque d'incendie dans cet environnement est d'un niveau majeur à cause de la chaleur engendrée par les serveurs fonctionnant sans interruption. Pour éviter la surchauffe des matériels, des climatisations performantes doivent être installées dans les salles serveurs pour refroidir ces salles afin d'obtenir une température stable.

3.1.3. Cablage et installations électriques

Tout comme les équipements et matériels composant l'infrastructure, le câblage de la salle informatique fait partie des éléments qui contribueront à assurer ses fonctionnalités et ses performances. Le choix des fils (câbles de transfert de données et câbles d'alimentation) et des connecteurs est ainsi à faire avec soin. Ils doivent être conformes aux normes de qualité imposées par la loi.
Ensuite, la configuration du câblage, notamment la circulation des nombreux câbles dans la salle doit être bien pensée. L'objectif est de limiter la quantité de fils visibles pour ne pas gêner la vue et ceux qui traînent un peu partout dans la pièce et pouvant faire trébucher les personnes qui font le va-et-vient, le tout sans porter atteinte au bon fonctionnement du S.I.

3.1.4. Portes coupe-feu & vitrage résistant au feu

Les portes coupe-feu et les systèmes de confinement permettent d'isoler la zone du départ de feu.

3.1.5. Systèmes d'étanchéité intumescents

Une étanchéité efficace de la pièce est nécessaire pour contenir le feu afin que les systèmes de suppressions du feu soient efficaces suffisamment longtemps pour éteindre le feu.

3.2. Détection et suppression d'incendie

Les sources d'incendies les plus courantes dans les salles serveurs sont le système électrique ou le matériel. Les pannes d'isolation et le court-circuit qui en résulte peuvent entraîner une chaleur intense qui peut faire fondre les matériaux ou provoquer un incendie. Le système de détection et d'extinction spécifique dépend de la conception et des expositions spécifiques de la salle serveur.

3.2.1. Système de détection de fumée

Les incendies dans la salle informatique sont souvent petits ou couvants, avec peu d'effet sur la température de la pièce. Étant donné que la fumée elle-même peut avoir un impact sur le matériel informatique, il est nécessaire d'employer un système de détection sensible à la fumée et aux autres produits de combustion plutôt qu'à la température.

3.2.2. Système de détection automatique

Un équipement de détection automatique doit être installé pour fournir une alerte précoce en cas d'incendie. Cet équipement doit respecter les normes et standards en vigueur, doit être installé en tenant compte des courants d'air et des spécificités de la salle serveur à protéger. L'équipement doit être installé et entretenue selon le standard NFPA 72E, Standard on Automatic Fire Detectors.

3.2.3. Système de protection automatique

Un système de suppression passif réagit aux dangers détectés sans intervention manuelle. Les formes les plus courantes de suppression passive sont les systèmes de gicleurs d'eau ou les systèmes de suppression chimique (gaz).
Lorsqu'il y a un besoin critique de protéger les données en cours de traitement, de réduire les dommages matériels et de faciliter la remise en service, il convient d'envisager l'utilisation d'un agent gazeux. Les systèmes à gaz sont cependant des conceptions uniques. Si le feu n'est pas éteint lors de la décharge initiale, il n'y a pas de seconde chance. Le système de gaz ne peut pas être réutilisé tant qu'il n'est pas rechargé ou connecté à une source de secours.
Les systèmes d'eau peuvent continuer à lutter contre l'incendie jusqu'à ce qu'il soit maîtrisé. Bien qu'un système d'eau soit plus susceptible d'endommager le matériel, c'est aussi un meilleur moyen de protéger la structure du bâtiment.
Le système idéal comprendrait un système de gaz propre et un système de gicleurs d'eau à préaction.
La décision concernant les moyens d'extinction d'incendie à utiliser doit intégrer de nombreux facteurs, y compris la mission et la criticité des opérations du centre de données
Le standard NFPA recommande que les équipements électroniques, de ventilation et de climatisation soient automatiquement arrêtés en cas de décharge du système de suppression d'incendie. Les équipements électroniques peuvent souvent être récupérés après un contact avec de l'eau tant qu'ils ont été mis hors tension avant le contact. Avec les systèmes de suppression d'eau, l'arrêt automatique est recommandé principalement pour permettre la récupération de l'équipement. Avec les systèmes à gaz, le problème est qu'un défaut d'arc pourrait rallumer un feu après la dissipation du gaz.

3.2.4. Les extincteurs

Des extincteurs portatifs homologués du type au dioxyde de carbone ou du type à agent halogéné doivent être fournis pour la protection des équipements électroniques. Un panneau doit être placé à côté de chaque extincteur portatif et indiquer clairement le type d'incendie auquel il est destiné.

3.2.5. Moyens d'évacuation et signalisation

Des moyens d'évacuation et les signalisations adéquats doivent être fournis en prenant en compte les distances qui permettent aux individus de s'éloigner du feu jusqu'à atteindre une sortie finale le long des voies d'évacuation sans fumée.

4. Ressources humaines

Le personnel désigné pour constituer l'équipe d'intervention doit être continuellement et soigneusement formé au fonctionnement du système d'alarme, à la réponse souhaitée aux conditions d'alarme, à l'emplacement de tous les équipements et outils d'urgence et à l'utilisation de tous les équipements d'extinction disponibles. Cette formation doit englober les capacités et les limites de chaque type d'extincteur disponible et les procédures de fonctionnement appropriées des systèmes d'extinction.
L'organisation, la formation et les équipements dont disposent cette équipe doivent être adéquats pour répondre à urgence incendie avant l'intervention des pompiers.

Le standard NFPA 600, Standard on Industrial Fire Brigades, décrit les exigences de l'organisation,
La formation et l'équipement de protection individuelle des équipes d'intervention.

4.1. Organisation de l'équipe d'intervention

Dans sa forme la plus simple, l'équipe se compose du responsable incendie assisté du personnel sélectionné. Dans les data centers complexes ou lorsque la protection de toute l'entreprise est nécessaire, l'équipe d'intervention peut s'organiser en sous-équipes selon les spécificités de l'entreprise. La collaboration avec les pompiers peut également affecter l'organisation de l'équipe d'intervention.

4.2. Les formations

L'employeur devrait proposer un programme de formation et garantir un effectif suffisant pour exécuter les tâches assignées lors d'une urgence d'incendie. L'ensemble du personnel de l'entreprise devrait recevoir une formation annuelle sur les extincteurs. L'équipe d'intervention devraient recevoir des formations avancées avec des "travaux pratiques". L'employeur doit s'assurer que la formation et la sensibilisation à l'ensemble du personnel sont dispensées assez fréquemment.

La formation devrait inclure les principes et les pratiques de lutte contre l'incendie et la gestion des autres urgences en adéquation avec le rôle de l'équipe d'intervention mis en place. Le data center étant en constante évolution, le programme de formation doit être adapté aux nouveaux dangers des biens et équipements neufs acquis par l'entreprises et leurs procédures de protection.

Le standard NFPA 600 demande à ce que « La formation fournisse un moyen par lequel tous les membres de l'équipe d'intervention augmentent leurs connaissances et développent des compétences pour être performant individuellement ou en tant que membre de l'équipe. Le travail d'équipe et les compétences sont la colonne vertébrale d'une bonne équipe d'intervention. »

4.3. Exercices

Des exercices devraient être utilisés pour vérifier la capacité des membres de l'équipe, de la direction, et de l'ensemble des employés à l'utilisation des équipements et l'efficacité du fonctionnement de l'équipe.
La fréquence et le contenu des exercices varient en fonction de la typologie de l'équipe. À l'occasion, des exercices devraient être menées dans des conditions météorologiques défavorables pour élaborer les procédures spéciales à ces conditions.
Une critique doit suivre chaque exercice pour discuter pleinement de ce qui s'est passé, corriger les défauts dans les procédures et découvrir tous les domaines qui pourraient nécessiter une formation supplémentaire.

5. Normes et standards du secteur

Les normes et standards du secteur utilisé pour l'élaboration de ce guide sont :

- NFPA 72E - Standard for Automatic Fire Detectors
- NFPA 75 - Standard for the Fire Protection of Telecommunications Facilities
- NFPA 76 - Standard for the Fire Protection of Information Technology Equipment
- NFPA 600 - Standard Industrial Fire Brigades states
- ISO 27001 2013 Annexe A.11 - Physical & Environmental Security