thínkproject

Les composantes de la protection des données :

construire des fondations sûres pour vos fournisseurs et vous-même

Contenu

Des milliards investis dans la sécurité de l'information et la protection des données en Europe

La protection des données et la sécurité de l'information ne sont pas seulement un sujet d'actualité, mais une stratégie essentielle permettant aux entreprises de protéger leurs ressources en informations les plus précieuses.

Selon le rapport Kroll 2021[1] sur les tendances en matière de violations de données, le secteur de la construction a connu une augmentation de

800%

des violations de données signalées entre 2019 et 2021, contre une augmentation moyenne de

133%

dans les autres branches.

Parmi les facteurs déterminants, on note les difficultés à gérer la collaboration en matière de données entre entreprises, le contrôle des ressources dans un environnement géographiquement dispersé (dont le travail à distance) et une exposition croissante aux menaces basées sur l'IdO (l'Internet des Objets) à mesure que le secteur innove. Ces problématiques ont mis en évidence l'importance de s'assurer que les stratégies de numérisation et de sécurité des responsables de l'informatique et de la conformité permettent de relever efficacement ces défis.

1 www.kroll.com

Les investissements dans la sécurité de l'information ne montrent aucun signe de ralentissement

Selon l'IDC (International Data Corporation), les dépenses en matière de sécurité informatique en Europe devraient atteindre environ

€47 milliards

en 2022

avec des prévisions sur cinq ans supposant que les investissements dépasseront

€66 milliards

d'ici 2026[2].

La gestion de l'information et des cyber-risques se détache des secteurs qui ont été de gros investisseurs. La numérisation des processus de construction et le passage au DfMA (Design for Manufacturing and Assembly ou conception pour la production et l'assemblage), transférant l'industrie de la construction dans le secteur de la fabrication, s'accompagnent de ces pressions exercées sur les investissements.

2 www.idc.com

La protection des données est désormais une obligation pour toutes les entreprises

La protection des données personnelles s'inscrit dans ce cadre. Toute entreprise implantée dans l'UE a désormais connaissance du Règlement Général sur la Protection des Données (RGPD), lequel a introduit des règles strictes en matière de confidentialité des données, tant pour le client que pour l'entreprise. La protection des données sert à la fois à protéger les données (personnelles) de votre propre entreprise et à s'assurer que vous protégez les données (personnelles) de vos clients, de votre chaîne d'approvisionnement et de vos parties prenantes.

Parallèlement, la directive sur la sécurité des réseaux et les systèmes d'information (directive NIS) définit des mesures visant à garantir un niveau commun élevé de sécurité des réseaux et des systèmes d'information au sein de l'UE. La directive NIS a créé un cadre juridique uniforme pour le développement des capacités nationales de cybersécurité à l'échelle de l'UE, une plus grande coopération entre les États membres de l'UE, des exigences minimales en termes de sécurité et des obligations de déclaration pour les infrastructures critiques, ainsi que pour certains fournisseurs de services numériques tels que les services cloud et les marketplaces.

Le RGPD, tout comme la directive NIS, ont contribué de manière significative à la sensibilisation et à la discussion autour de la protection des données et de la sécurité de l'information dans toutes les entreprises.

Voici les types de menaces pour la sécurité auxquelles les utilisateurs sont le plus sensibles sont le plus sensibles

Une formation régulière du personnel à la sécurité de l'information réduit le risque d'une attaque aboutie

Logiciels malveillants

Ces logiciels malveillants sont destinés à nuire à votre système informatique et à votre réseau. Les logiciels malveillants peuvent se présenter sous de nombreuses formes : virus, logiciels espions et bien d'autres.

Les entreprises peuvent être vulnérables à ce type d'attaque, car les logiciels malveillants peuvent être, par exemple, déguisés en liens dans les e-mails permettant de tromper facilement les utilisateurs qui ne sont pas vigilants.

Rançongiciels

Les rançongiciels peuvent être particulièrement dévastateurs, car ils peuvent verrouiller vos fichiers importants et exiger un paiement pour y accéder à nouveau.

Chaque entreprise possède des données précieuses auxquelles les cybercriminels veulent accéder, et le rançongiciel peut se propager rapidement dans un réseau, affectant tous les aspects de l'entreprise.

Hameçonnage

Les criminels qui pratiquent l'hameçonnage se font passer pour des collègues de confiance afin de tenter d'accéder à votre réseau. Il est généralement question de réinitialiser des mots de passe ou de cliquer sur des liens.

Une fois l'accès accordé, un rançongiciel ou un autre logiciel nuisible peut être installé sur le système ou des données peuvent être volées.

Menace persistante avancée

On parle de menace persistante avancée lorsqu'un attaquant bien formé, généralement contrôlé par un État, s'attaque à un réseau ou à un système de manière très ciblée à des fins d'espionnage ou de sabotage sur une période prolongée, en se déplaçant et/ou en se propageant éventuellement à l'intérieur du réseau ou du système afin de recueillir des informations ou de le manipuler.

Ingénierie sociale

L'ingénierie sociale désigne toutes les techniques visant à amener une cible à révéler des informations spécifiques ou à effectuer une action spécifique pour des raisons illégitimes.

Il existe de nombreuses techniques d'attaque bien documentées qui sont souvent utilisées en combinaison pour mettre en péril une entreprise :

Déni de service (DoS) et Déni de service distribué (DDoS)

D'importantes quantités de données bombardent un site web ou une application dans le but d'utiliser toute la bande passante du réseau ou la puissance de traitement du système, le rendant ainsi indisponible. Même si elles provoquent une perturbation, les attaques DDoS sont généralement de courte durée et causent rarement des dommages irréversibles. Néanmoins, elles sont souvent utilisées comme tactique de diversion pour détourner l'attention d'une attaque plus sérieuse qui intervient au même moment.

Attaque de l'homme du milieu (MitM)

Les attaques de l'homme du milieu peuvent être difficiles à réaliser, mais si elles aboutissent, elles peuvent permettre à un attaquant de voir des données en plein texte (par exemple des mots de passe, des données de projet et des e-mails) qui sont normalement cryptées. Les acteurs de menaces peuvent également être en mesure de manipuler les données à mesure qu'elles sont envoyées.

Menaces internes

Une menace interne est le fait qu'une personne disposant d'un certain niveau d'autorisation au sein d'une organisation agisse de manière à enfreindre la sécurité. Il peut s'agir d'un acte malveillant ou involontaire, mais le risque pour une entreprise est élevé en raison du niveau d'accès aux données et aux systèmes dont elle dispose déjà.

Injection SQL

Les attaquants utilisent les vulnérabilités de l'injection SQL pour manipuler, supprimer ou extraire des données d'une application sans autorisation correspondante. Cela peut conduire à des vols de données à grande échelle et à la corruption du système.

Scripts intersites (XSS)

Des scripts nuisibles peuvent être introduits dans des sites web et espionner ensuite à son insu l'activité d'un utilisateur via son navigateur. Les attaquants tentent de faire exécuter leur code malveillant par leur cible en le diffusant à partir d'un site de confiance. Il existe de nombreuses failles qui permettent des attaques XSS et il peut être difficile d'y mettre un terme, car le navigateur web de la victime croit que le script provient d'un site de confiance.

Attaques par mot de passe

Cette attaque peut être mise en oeuvre de plusieurs manières, comme le craquage de mot de passe, pour accéder aux mots de passe, lesquels peuvent ensuite être modifiés ou décryptés. Les mots de passe faibles peuvent être devinés avec suffisamment de temps, mais les criminels exploitent notre tendance à utiliser le même mot de passe à plusieurs endroits en essayant des noms d'utilisateur et des mots de passe provenant de violations de données publiques pour se connecter à d'autres sites web et systèmes. Cette technique a connu un grand succès ces dernières années.

Faille 0-day

Lorsqu'un attaquant exploite une vulnérabilité inconnue, la capacité des équipes de sécurité à détecter la menace et à réagir est fortement réduite. Lorsqu'une faille est découverte, il faut normalement quelques jours aux fournisseurs de logiciels pour créer un correctif. Cet exploit est baptisé « zero-day » parce qu'il est connu depuis zéro jour, l'attaque se produit le jour même où la vulnérabilité est découverte.

Logiciels malveillants

Logiciels espions

Vers informatiques

Chevaux de Troie | Virus

Rançongiciels

Basé sur le réseau

Dos | DDos

MitM

Application Web

XXS

Injection SQL

Ingénierie sociale

Hameçonnage

Menaces internes

Faille 0-day

Attaques sur des vulnérabilités non divulguées

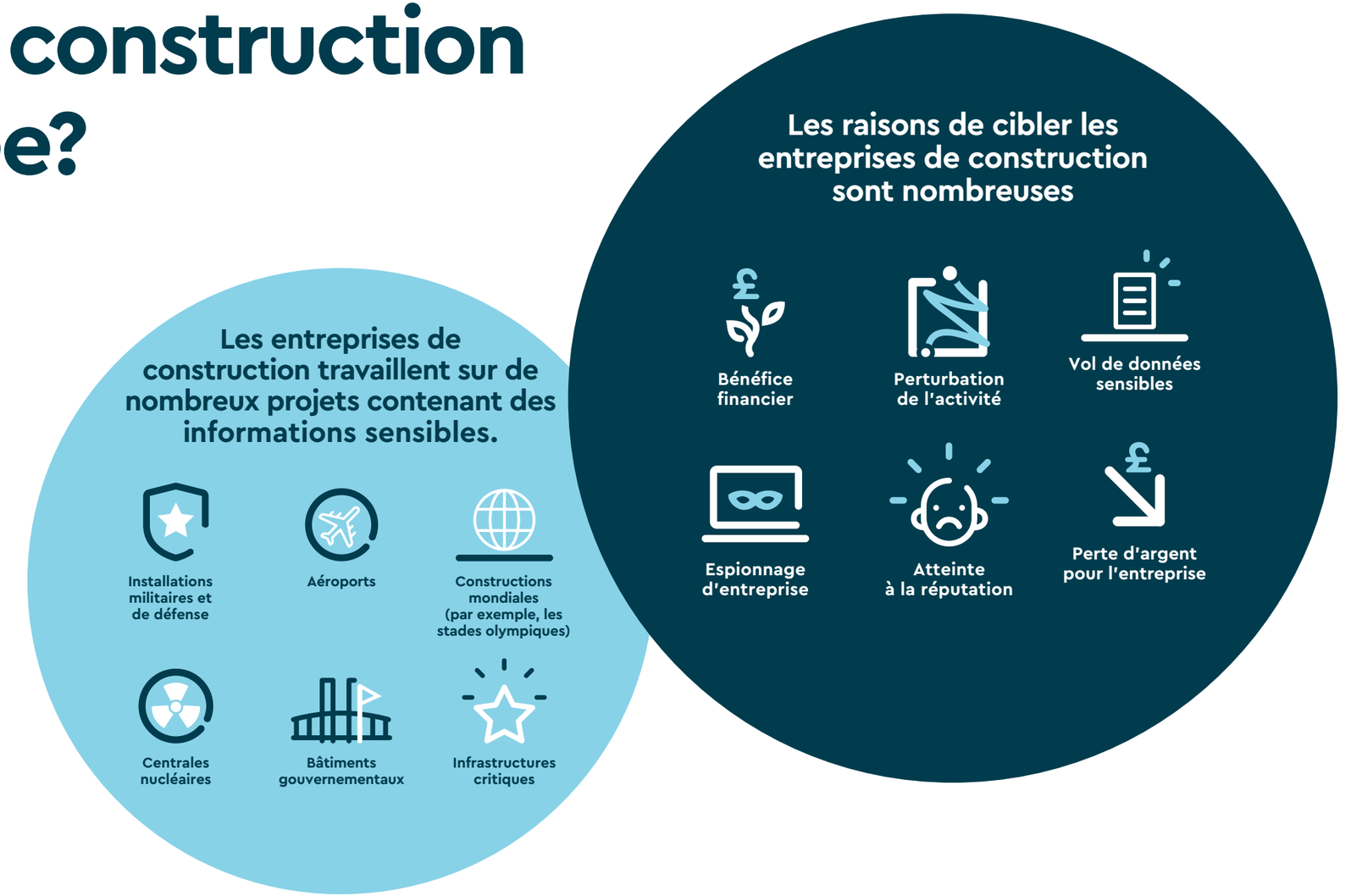
Authentification

Attaques par mot de passe

Le secteur de la construction n'est pas à l'abri des atteintes à la sécurité de l'information

La numérisation du secteur de la construction a beaucoup progressé. L'utilisation de l'automatisation, de l'IA et des méthodes numériques telles que la modélisation des données du bâtiment (BIM) nécessite des logiciels qui profitent à la construction en améliorant la qualité tout en économisant temps et argent, ainsi qu'en fournissant des informations et des analyses sur les données antérieures. Ce sont des mesures positives dans un secteur qui, par le passé, était considéré comme étant à la traîne en matière de numérisation. Néanmoins, à mesure que la présence numérique s'intensifie, le risque d'intentions malveillantes se manifeste rapidement.

Pourquoi la construction est-elle visée?



Comment une faille de la sécurité de l'information peut-elle affecter une entreprise ?

Imaginez le scénario suivant : des cybercriminels envoient un mail d'hameçonnage à l'un des employés d'une multinationale de construction, qui ouvre un lien contenu dans cet e-mail, suivi d'un rançongiciel qui verrouille les données du projet de l'entrepreneur tout en paralysant plusieurs sites du projet.

Les pirates informatiques parviennent à accéder non seulement aux données personnelles des employés et des clients, mais aussi à des informations sensibles concernant des projets de construction, tels que les plans de bâtiments gouvernementaux à travers le monde. Cette cyberattaque entraîne également d'importantes répercussions pour l'entreprise, ses parties prenantes, sa chaîne d'approvisionnement et ses clients. L'impossibilité d'accéder aux données du projet et de poursuivre les travaux comme prévu a un impact important sur l'échéancier global, avec des risques de pénalités de retard, pouvant entraîner une forte perte de productivité. Globalement, les préjudices financiers et les atteintes à la réputation de l'entreprise peuvent être considérables et les répercussions monétaires peuvent être encore plus graves. L'entreprise doit alors supporter les frais de justice, les coûts de remise en état et les lourdes amendes. Autre point tout aussi important : la confiance dans l'entreprise s'est effondrée et il faudra déployer des efforts, des ressources et des sommes d'argent considérables pour la rétablir. Le fait de tenter de se relever d'une attaque peut comporter des risques encore plus importants pour les industries disposant de données très sensibles, comme le secteur nucléaire ou les infrastructures critiques, où les problèmes potentiels pourraient être ressentis dans tout le pays ou dans le monde entier.

L'entreprise s'est attelée à ce problème en élaborant une stratégie de sécurité de l'information pour s'assurer que cela ne se reproduirait plus, notamment par l'authentification multi-facteur, la formation des employés à la détection des escroqueries par hameçonnage, le renforcement de la sécurité du réseau et l'amélioration des procédures de réponse aux incidents. En outre, l'entreprise a également instauré une politique de contrôle sévère pour tous les fournisseurs externes avec lesquels elle travaille, afin de s'assurer que l'ensemble de la chaîne dispose de procédures similaires. Ces mesures garantissent que l'organisation est préparée en cas de nouvelle violation et que le risque est donc minimisé.

Cet exemple montre les risques auxquels les entreprises de construction peuvent être exposées et les avantages à long terme qu'offre la priorisation de la sécurité de l'information. Les enjeux deviennent encore plus importants lorsque les cybercriminels ont l'intention de perturber des projets sensibles, tels que des infrastructures critiques[3] ou des installations nucléaires. En 2021, 56% des installations énergétiques aux États-Unis ont fait état de tentatives de cyberattaques qui ont interrompu leurs activités, le coût pour se relever d'une attaque étant estimé à 100 milliards de dollars[4]. Les effets de ces attaques sur les infrastructures peuvent s'étendre de l'approvisionnement en eau, au chauffage ou à l'éclairage des maisons.

3 www.allianz.com

4 www.firstpoint-mg.com

Cet brochure sur la sécurité de l'information vise à fournir des informations qui pourraient aider votre entreprise à rester à la pointe des meilleures pratiques, à vous indiquer ce que vous devez rechercher chez vos fournisseurs externes et comment rester en sécurité.

Décortiquer la terminologie

Comprendre la sécurité de l'information:

La sécurité de l'information peut comporter de nombreux acronymes et un jargon technique.
Utilisez notre guide de la terminologie la plus fréquemment utilisée pour vous tenir au courant.

BIA
(business impact analysis
- Analyse d'Impact Métier)

L'analyse d'impact sur l'entreprise permet de quantifier l'impact potentiel d'une menace sur les activités de l'entreprise. Il s'agit d'une étape-clé consistant à définir les contrôles nécessaires pour réduire les risques à un niveau acceptable.

Contrôle d'accès

Méthode permettant de s'assurer que les personnes n'ont accès qu'aux données dont elles ont besoin et pour lesquelles elles disposent d'une autorisation. Ces contrôles sont essentiels pour minimiser l'ampleur d'une violation de données.

Évaluation des risques

Mécanisme mis en place pour évaluer les risques et leur gravité.

ISO 27001

Reconnue mondialement comme le système de gestion de la sécurité de l'information le plus accepté et le plus mis en oeuvre. L'ISO a créé un cadre solide que les entreprises doivent suivre pour assurer une protection maximale et offre des accréditations aux organisations qui répondent aux critères.

Menace

Toute action susceptible de causer un préjudice.

PCO

Le plan de continuité des opérations est élaboré et mis en oeuvre lors d'une situation d'urgence. Il définit les mesures d'intervention et les étapes de rétablissement afin de garantir que l'entreprise continue de fonctionner pendant la crise.

Pare-feu

Dispositif qui contrôle le flux de données entre les réseaux.

Patching

Processus consistant à appliquer des mises à jour de logiciels ou de microprogrammes afin d'éliminer les failles de vos ressources.

Réponse aux incidents

Processus de gestion de l'identification, de l'endiguement et de l'élimination d'une menace pour la sécurité et le rétablissement à un état normal.

Risque

Combinaison d'une faille et d'une menace.

RSSI

Le responsable de la sécurité des systèmes d'information est un professionnel chargé de superviser et de gérer le programme de sécurité de l'information d'une organisation. Son rôle principal est de protéger la confidentialité, l'intégrité et la disponibilité des ressources en informations de l'organisation.

Sécurité de l'information

Fait référence à la protection de la confidentialité, de la disponibilité et de l'intégrité de l'information (voir : Triade CIA), ainsi que les actions entreprises pour prévenir les dommages. Elle comprend la mise en oeuvre de mesures et l'adoption de meilleures pratiques et peut concerner les réseaux informatiques, les bâtiments sur site et tout autre endroit où l'on peut trouver des informations.

SGSI

Le système de gestion de la sécurité de l'information couvre les politiques, les processus et les contrôles visant à protéger et à prévenir les informations sensibles d'une organisation.

Triade CIA

Modèle commun en trois points qui comprend la confidentialité, l'intégrité et la disponibilité, à savoir les trois grands principes de la sécurité de l'information.

VPN

Un réseau privé virtuel sécurise la communication entre deux réseaux ou entre l'appareil d'un utilisateur et le réseau de son entreprise, en l'envoyant dans un tunnel crypté. Un VPN dispose d'un système de cryptage permettant de bloquer les informations identifiables face aux menaces potentielles. Celui-ci est généralement utilisé pour accéder à Internet.

Clarté sur la protection des données

Pour protéger efficacement les données, il convient d'abord de comprendre ces termes courants :

AIPD

L'analyse d'impact relative à la protection des données est un processus utilisé pour identifier les risques et les conséquences du traitement et du stockage des données sur une personne. L'analyse d'impact relative à la protection des données est le plus souvent utilisée lors du traitement de catégories spéciales de données ou pour des activités de traitement de données à grande échelle et à haut risque.

Catégories spéciales de données

Sous-ensemble défini de données personnelles considérées comme sensibles, telles que la race, l'appartenance ethnique, l'orientation sexuelle ou les opinions politiques, et dont le traitement est soumis à des exigences supplémentaires.

Contrôleur de données

Personne physique ou morale, autorité publique, agence ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

Data Protection Officer (DPD)

Le délégué à la protection des données est une fonction établie par le RGPD. Le rôle principal du **délégué à la protection des données (DPD)** est de veiller à ce que l'organisation pour laquelle il a été nommé, **traite** les **données personnelles** de son personnel, de ses clients, de ses fournisseurs ou de toute autre personne (également appelée **personne concernée**) conformément aux règles applicables en matière de protection des données.

Données cryptées

Il s'agit de données qui ont été brouillées en un code secret dont le déverrouillage nécessite une clé numérique unique. Le cryptage est utilisé pour empêcher qu'elles soient lues par des personnes non autorisées, ou qu'elles soient volées, modifiées ou compromises. C'est un moyen de contrôle particulièrement puissant en cas de perte ou de vol de données.

Données personnelles

Toute information qui se rapporte à une personne identifiée identifiable (noms, adresses e-mails, identifiants, etc).

DSGVO

DSGVO est l'abréviation du terme allemand « Datenschutz-Grundverordnung » (Règlement Général sur la Protection des Données).

IPI

Les informations personnelles d'identification (IPI) constituent tous les types de données pouvant être utilisées pour identifier une personne, qu'il s'agisse de son numéro de téléphone, des informations de son passeport ou de son numéro de sécurité sociale.de son numéro de sécurité sociale.

Loi britannique sur la protection des données (2018)

La loi britannique sur la protection des données couvre les citoyens britanniques et combine des contrôles harmonisés selon le RGPD avec des thèmes étendus en matière de protection des données.

Minimisation des données

Action de minimiser la collecte de données personnelles au minimum nécessaire pour exécuter l'activité de traitement.

Personne concernée

Toute personne qui peut être identifiée en tant que personne physique par les données collectées à son sujet.

Protection des données

Contrôle de l'accès et de l'utilisation des données.

Responsable du traitement des données

Toute entité qui traite des données personnelles pour le compte du responsable du traitement.

RGPD

Le Règlement Général sur la Protection des Données est une loi de l'UE sur la protection de la vie privée, qui a permis de créer un cadre juridique consolidé en matière de protection des données dans tous les États membres de l'Union européenne (UE), ainsi qu'en Islande, au Liechtenstein, en Norvège et en Suisse – qui font partie du marché unique de l'Espace économique européen (EEE). Entré en vigueur en mai 2018, le RGPD s'applique au traitement des données personnelles des citoyens de l'UE, que le traitement ait lieu dans l'UE ou hors de l'UE.

Conditions de base sur la protection des données

SAR
(Subject Access Request
- Demande d'accès du sujet)

Une demande d'accès aux données est un mécanisme qui permet aux personnes de demander une copie de leurs données, détenues par une organisation. Elles peuvent également être utilisées par les personnes pour faire valoir leurs droits, tels que le droit de rectification ou le droit à l'oubli.

Sept grands principes

Le RGPD repose sur sept grands principes : égalité, équité et transparence, limitation des finalités, minimisation des données, exactitude, limitation du stockage, intégrité et confidentialité et responsabilité.

Traitement des données

Le traitement des données fait référence à la collecte, à l'analyse et à la transformation des données afin d'en extraire des informations significatives et de faciliter la prise de décision. Il joue un rôle capital dans de nombreux domaines, notamment les affaires, la recherche et la technologie, permettant aux organisations d'exploiter les données à des fins d'efficacité opérationnelle, de planification stratégique et d'innovation.

Violation de données

Incident de sécurité au cours duquel des parties non autorisées accèdent à des données sensibles ou à des informations confidentielles, y compris des données personnelles ou des données d'entreprise.

Vous avez élaboré une stratégie numérique, mais qu'en est-il de la sécurité de l'information ??

Ces dernières années ont été marquées par une accélération de la transformation numérique et par l'évolution des processus opérationnels dans les secteurs de l'architecture, de l'ingénierie, de la construction et des opérations (AECO).

L'essor de la numérisation, de la construction 4.0 et de la technologie de l'IA s'est certainement accéléré pendant la pandémie de 2020, les entreprises voyant de plus en plus les avantages de l'intelligence de la construction se traduire par une efficacité et une productivité accrues, ainsi que par une amélioration de la durabilité, de la santé et de la sécurité.

Se concentrer sur une stratégie numérique peut nécessiter de nombreux logiciels différents, tels que les plateformes BIM et CDE, et constitue une boîte à outils très utile tout au long du cycle de vie du projet de construction. Outre les économies en termes de temps et d'argent, les données et les analyses qui peuvent désormais être collectées sont de plus en plus précieuses et permettent d'obtenir des informations importantes qui profiteront aux projets futurs.

La numérisation est une avancée positive, mais il est important de rester vigilant face à d'éventuelles failles

La numérisation a considérablement augmenté la quantité de données collectées, traitées et stockées. Ces données comprennent souvent des données sensibles sur les clients, des données financières et des données personnelles, ainsi que des informations sur la propriété intellectuelle et des informations sensibles d'un point de vue commercial. L'ampleur des données détenues a renforcé le profil des organisations AECO et de leur chaîne d'approvisionnement auprès de la communauté cybercriminelle, augmentant le risque d'être ciblé par une série d'acteurs de menaces, des groupes de rançongiciels aux menaces persistantes avancées (APT) parrainées par l'État.

Pour aboutir, une menace doit exploiter une faille, qu'il s'agisse d'une faille technique, comme un bug logiciel, d'une faille procédurale, comme la copie de données sur une clé USB sans cryptage, ou d'une faille humaine, comme le fait de se laisser berner par un courriel frauduleux.

La protection contre la compromission nécessite traditionnellement une stratégie de sécurité de l'information garantissant que les systèmes numériques sont maintenus, renouvelés, surveillés, sécurisés et dotés de ressources tout au long de leur cycle de vie, souvent selon des normes techniques et de conformité strictes (ISO27001, SOC2, NIST-800, Cyber Essentials Plus, etc.). Le personnel doit être formé aux processus et sensibilisé aux cybermenaces, et les menaces elles-mêmes doivent être identifiées et corrigées rapidement pour que les attaquants n'aient pas le temps d'endommager le réseau. Tout cela exige non seulement un engagement important de la part de l'entreprise en matière de sécurité de l'information et de protection des données, mais aussi des investissements considérables.

Pour le secteur AECO, le défi est d'autant plus grand qu'il faut de plus en plus gérer l'accès aux données dans un environnement de collaboration inter-organisations, réunissant des utilisateurs de différentes organisations, avec des normes et des politiques de sécurité différentes, tout en veillant à ce que les exigences du client soient respectées. Les outils que vous employez doivent être flexibles et imposer des contrôles de sécurité qui ne dépendent pas d'une seule organisation.

Les exemples de violations de la sécurité de l'information laissent penser que les cyberattaques entraîneront des perturbations importantes, des pertes financières et des atteintes à la réputation. Ce qui est particulièrement important en matière de sécurité pour les entreprises de construction, des données précieuses susceptibles de tomber entre de mauvaises mains. Les logiciels de construction traitent de nombreuses informations sensibles, qu'il s'agisse de plans, de dessins et de schémas ou de données relatives aux points faibles des bâtiments ou à d'autres défauts susceptibles d'être exploités. Ces informations sensibles sont nécessaires à l'élaboration de projets exceptionnels, mais elles peuvent aussi agir contre une entreprise si des pirates informatiques y ont accès.

Enfin, et c'est tout aussi important, les entreprises doivent s'engager à protéger les données de leurs employés, de leurs clients et de l'ensemble de la chaîne d'approvisionnement. Une violation de données personnelles peut entraîner de longues procédures judiciaires et des amendes, sans parler d'une atteinte considérable à la réputation dont le rétablissement peut prendre du temps.

Comment vos parties prenantes et vous-même pouvez protéger des données précieuses

La numérisation a accru l'interconnectivité et la collaboration entre les différentes parties prenantes d'un projet de construction, notamment les architectes, les ingénieurs, les entrepreneurs et les fournisseurs. Cette connectivité accrue présente de nombreux avantages, mais comporte également le risque que les failles de sécurité affectant une partie se propagent rapidement dans l'écosystème du projet, ayant également une incidence sur d'autres parties.

Les entreprises de construction doivent prioriser la sécurité de l'information en mettant en oeuvre des mesures de sécurité solides, telles que la gestion des correctifs, la surveillance de la sécurité, le contrôle d'accès, le cryptage et la segmentation du réseau, afin de protéger leurs systèmes et leurs données contre les cybermenaces. Elles doivent également veiller à ce que leurs employés soient formés aux meilleures pratiques en matière de sécurité et soient conscients des risques de cyber-attaques. En prenant des mesures proactives pour protéger leurs systèmes et leurs données et en disposant d'une main-d'oeuvre bien informée, elles peuvent minimiser le risque d'attaques, permettre à l'ensemble de la chaîne d'approvisionnement de prospérer et constituer les meilleures ressources possibles grâce à la technologie numérique.

Élaborer sa propre stratégie de sécurité de l'information

Tout cela semble intéressant sur le papier, mais quels sont les points essentiels à prendre en compte lors de la planification d'une stratégie de sécurité de l'information ? Vous pouvez considérer les points suivants :

- Un but défini à atteindre et les objectifs pour y parvenir. Il peut s'agir d'instaurer un climat de confiance avec la clientèle, de mettre en place un plan de continuité des opérations ou de se conformer à une norme reconnue en matière de sécurité de l'information.
- Une évaluation approfondie des risques qui identifie les failles dans le stockage et le traitement des données. L'idéal est de se concentrer d'abord sur les domaines où les risques sont les plus élevés.
- La mise en place d'une équipe chargée du système de gestion de la sécurité de l'information (SGSI) afin d'assurer la gouvernance et les contrôles nécessaires au maintien de normes solides en matière de protection des données.
- L'élaboration de plans d'intervention en cas d'incident et de plans de continuité des opérations, afin que le travail puisse se poursuivre lors d'atteinte à la sécurité.
- L'établissement des rôles et des responsabilités facilitera le fonctionnement de la sécurité de l'information. Avec des décideurs clairs et une allocation de ressources suffisante, vous ne devriez pas être pris au dépourvu dans le pire des scénarios.
- Revoyez et développez en permanence les politiques et les procédures, organisez des examens réguliers des incidents. Les meilleurs résultats, quel que soit le processus, sont le fruit d'une bonne collaboration.
- Favorisez une culture dans laquelle chacun assume la responsabilité de la protection des données. Grâce à des formations régulières et des simulations d'attaques, les organisations doivent veiller à ce que leurs équipes soient régulièrement sensibilisées aux dangers des menaces telles que les escroqueries par hameçonnage.
- Faites des évaluations par un prestataire externe. Il ne s'agit pas seulement d'une case à cocher qui vous donne un badge pour votre site web. Ces évaluations externes peuvent permettre d'identifier des lacunes dans les plans de sécurité qui ne sont pas forcément visibles pour une personne qui utilise le réseau tous les jours.

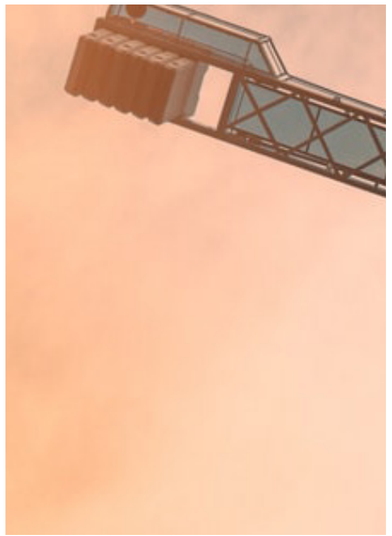
La référence absolue de la sécurité à rechercher chez votre fournisseur

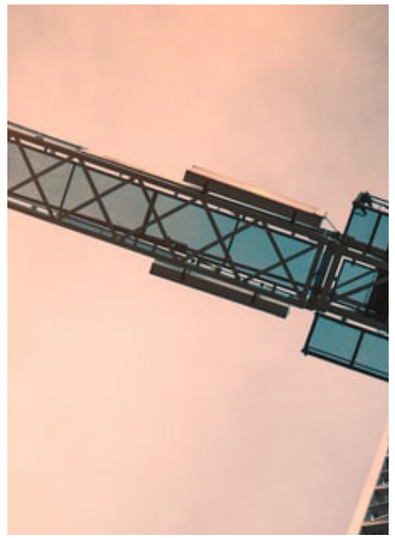
Examinons plus en détail ce que vous pouvez attendre d'un fournisseur de logiciels soucieux de la sécurité de vos données.

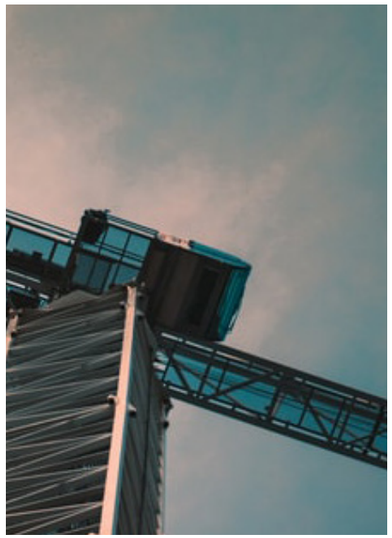
Type de sécurité	Que cela signifie-t-il ?	Chez Thinkproject
Pratiques de développement sécurisées	Les équipes de développement devraient utiliser des outils pour structurer leur travail et la remise du nouveau code dans un état validé. La livraison doit inclure des mécanismes permettant d'identifier et de corriger les failles au niveau des composants et du code, doit être conforme aux meilleures pratiques de codage et les tests du code doivent être automatisés dans la mesure du possible.	Thinkproject travaille dans le cadre d'une structure DevOps définie qui utilise les principes CI/CD pour garantir des déploiements de code fiables et bien testés en production. Pendant le développement, des outils sont utilisés pour identifier les failles dans notre pile de composants et détecter les erreurs de codage en temps réel.
Sécurité physique	Les bureaux sur site et hors site doivent toujours être sécurisés afin d'empêcher tout accès non autorisé. Il peut s'agir de cartes d'accès aux bâtiments, d'une politique d'enregistrement des visiteurs et de caméras de vidéosurveillance.	Nos bureaux sont sécurisés par des cartes d'accès et l'ensemble du personnel et des visiteurs sont tenus de s'enregistrer à l'entrée et à la sortie du bâtiment. Nous utilisons également des caméras de vidéosurveillance, nous avons une politique de bureau dématérialisé et toutes les informations sensibles ne peuvent être consultées que par des personnes autorisées.
Sécurité du réseau	Le réseau de l'entreprise doit être doté de mesures de sécurité solides et de plans de continuité et de gestion des risques actualisés. La sécurité du réseau peut inclure des pare-feu, des logiciels antivirus et des systèmes de détection des intrusions.	Nos opérations de sécurisation des réseaux de bureaux et des centres de données s'inscrivent dans le cadre de notre accréditation ISO27001 et sont régulièrement évaluées.
Formation du personnel	Toute personne employée par l'entreprise doit avoir une bonne connaissance des politiques et des procédures de sécurité de l'information en place grâce à une formation régulière. Les employés doivent également appliquer les bonnes pratiques en matière de sécurité, telles que le verrouillage de leurs appareils, le signalement des escroqueries par hameçonnage et l'utilisation de mots de passe sécurisés.	Nous organisons une formation annuelle obligatoire pour tous le personnel sur de nombreux sujets, notamment la cybersécurité et la protection des données. Toutes les politiques doivent être attestées par chaque employé.
Conformité	L'entreprise doit être au fait des réglementations applicables en matière de sécurité. Le respect de ces réglementations démontre que l'entreprise se préoccupe activement de la sécurité. Il peut s'agir du RGPD, de la norme ISO 27001 ou de Cyber Essentials Plus.	Nous procédons chaque année à des audits externes et internes dans le cadre du programme d'audit du SGSI afin d'obtenir la certification ISO 27001. D'autres certifications spécifiques à certaines régions sont obtenues.

Type de sécurité	Que cela signifie-t-il ?	Chez Thinkproject
Risque lié aux tiers	L'entreprise doit mettre en place un programme de gestion des fournisseurs afin de s'assurer que les fournisseurs tiers respectent également les mesures de sécurité correspondantes.	**Nous utilisons une procédure de gestion des fournisseurs qui respecte les exigences de notre SGSI. Cette procédure comprend l'examen de tout fournisseur externe avec notre équipe de conformité, des accords de confidentialité, des contrôles RGPD, ainsi que d'autres mesures visant à garantir la conformité avec nos normes. Nos fournisseurs tiers sont régulièrement évalués pour garantir leur conformité.**
Protection des données	Votre fournisseur doit être conforme au RGPD s'il est applicable dans votre région. De plus, l'entreprise doit être en mesure de vous fournir toutes les informations sur ses pratiques en matière de protection des données et sur la manière dont elle protège vos informations.	La conformité des entreprises thinkproject et de leurs produits au RGPD est une priorité absolue. Des délégués externes à la protection des données (DPD) sont nommés pour diverses entités juridiques et pays de Thinkproject, par exemple thinkproject Deutschland GmbH et thinkproject Holding GmbH. Dans d'autres entités, des délégués internes à la protection des données ou des coordinateurs de la protection des données sont chargés de veiller au respect des exigences du groupe en matière de protection des données. Des audits réguliers de la protection des données font partie intégrante de notre système de gestion de la protection des données. Une formation annuelle au RGPD est obligatoire pour tous les membres de notre personnel. Nous nous conformons à nos politiques de protection des données, imposées à l'échelle du groupe.
Réponse aux incidents	Il est important que le fournisseur ait instauré des plans en cas d'atteinte à la sécurité. Il peut s'agir de plans de détection, d'intervention et de restauration, ainsi que de mesures prises pour informer les clients en pareil cas.	Notre procédure de gestion des incidents est en place et est régulièrement testée et évaluée afin de garantir une réponse rapide à tout incident. Nous proposons aux employés une formation claire sur le signalement des incidents via notre portail de dénonciation et notre plateforme OneTrust.
Gestion des failles	Le fournisseur doit régulièrement mettre à jour, corriger et tester ses logiciels pour éviter qu'un pirate n'exploite les failles.	Dans le cadre de nos opérations de sécurisation des centres de données, nous disposons d'outils permettant d'identifier les failles potentielles, ce qui signifie que nous pouvons agir rapidement pour atténuer toute menace potentielle.

Type de sécurité	Que cela signifie-t-il ?	Chez Thinkproject
Historique des incidents de sécurité	Le fait de se renseigner sur les incidents de sécurité antérieurs constitue un bon moyen d'évaluer la transparence de l'organisation. Celle-ci devrait être en mesure de vous donner son point de vue sur les enseignements tirés, la manière dont l'incident a été géré et ce qui a été mis en oeuvre depuis l'événement.	**Tous les incidents sont suivis à l'aide de l'outil OneTrust.** **Pour chaque incident, une analyse des causes profondes et les enseignements tirés sont mis en oeuvre conformément à notre procédure de gestion des incidents.**
Engagements contractuels en matière de sécurité	Les accords contractuels et les accords de niveau de service (SLA) doivent être clairs et faciles à comprendre.	**Tous nos produits Thinkproject ont des accords de niveau de service qui peuvent être fournis sur demande.**







Le point de vue d'un expert

Ralf Hundhammer, directeur technique de Thinkproject, partage son point de vue sur la sécurité de l'information

Nous avons demandé à Ralf Hundhammer de nous faire part de ses réflexions sur une série de questions relatives à la sécurité de l'information. Ralf compte plus de 20 ans d'expérience à son actif dans ce domaine et nous donne des indications précieuses.

Si vous étiez une entreprise novice en matière de sécurité de l'information, par où commenceriez-vous pour protéger vos données et mettre en oeuvre une stratégie de sécurité de l'information ?

L'élaboration d'une stratégie de sécurité peut sembler être une tâche colossale, mais comme tout processus, elle peut être décomposée en petites parties qui se combinent pour fonctionner ensemble. Tout d'abord, il est important de prendre du recul et d'apprendre à connaître vos données. Comprenez pourquoi vous les avez et pourquoi vous en avez besoin. Ces données sont-elles nécessaires? Pouvez-vous les crypter ? Voici quelques questions auxquelles il convient de réfléchir. Si vous savez quelles données votre entreprise traite, cela vous aidera, vous et votre équipe de sécurité, à évaluer les risques associés et à les protéger comme il se doit.

Il est essentiel que votre équipe de sécurité se tienne informée via la formation continue. De nouvelles menaces apparaissent régulièrement et votre équipe doit en être consciente. Investissez de l'énergie dans le perfectionnement de votre équipe de sécurité, car une violation de données est bien plus coûteuse. Cela vaut également pour l'ensemble de votre personnel: toute l'entreprise doit être en mesure d'évaluer une menace potentielle, que ce soit en simulant régulièrement des attaques par hameçonnage ou en modifiant périodiquement les mots de passe. Pensez également à votre espace physique. Par exemple, chez Thinkproject, nous appliquons une politique de bureau claire et dématérialisée, ce qui signifie qu'il y a moins d'informations qui traînent.

Une fois ces principes mis en place, le reste devrait venir naturellement. Créez des politiques claires pour la sécurité de l'information, mettez en pratique des méthodes d'authentification solides et assurez-vous que tout est mis à jour. Préparez votre plan d'intervention en cas d'incident, faites-vous auditer et appuyez-vous sur votre solide base de connaissances pour obtenir ces accréditations qui indiquent au client que vous êtes une entreprise soucieuse de la sécurité.

Les cyberattaques sont de plus en plus élaborées. Quel est, selon vous, le risque le plus important et comment le secteur AECO doit-il y faire face ?

L'une des plus grandes préoccupations est la compromission potentielle des infrastructures critiques et des données sensibles des projets. Avec l'utilisation généralisée de systèmes intégrés, de plateformes cloud et d'appareils de l'Internet des objets (IdO), la portée d'une attaque s'est massivement étendue. En combinant une défense technique solide à une main-d'oeuvre qualifiée, les organisations peuvent atténuer efficacement les cyber risques et protéger leurs ressources critiques.

La technologie continue d'évoluer et les attaques ne cessent également de se complexifier. Votre SGSI doit être revu régulièrement et être suffisamment souple pour s'adapter aux changements à mesure que les attaques progressent. Il s'agit d'un exercice d'équilibre entre la volonté de s'adapter et le respect d'une feuille de route claire que l'ensemble de l'organisation peut comprendre.

Les organisations devraient prioriser la collaboration et le partage d'informations entre entreprises, ainsi que le partenariat avec des experts en cybersécurité afin que le secteur soit le mieux informé possible. En travaillant tous main dans la main, nous pouvons atténuer les risques, en particulier grâce aux « enseignements tirés » qui servent aux autres entreprises.

Quelles sont les meilleures pratiques mises en place par Thinkproject pour protéger les clients avec lesquels elle travaille ?

Depuis notre création, nous prenons la protection des données très au sérieux. En tant qu'entreprise allemande basée en Europe, nous sommes très au fait de la protection des données ! Notre équipe de conformité déploie des efforts considérables pour s'assurer que l'ensemble de notre personnel suit une formation régulière sur le RGPD, le SGSI et nos plans d'urgence.

Nous sommes fiers des mesures solides que nous prenons pour garantir la sécurité des données de nos clients, de nos employés et de notre entreprise. Notre tableau pratique montre les mesures que nous avons mises en place et comment elles sont régulièrement évaluées et mises à jour.

Sécurité garantie : protéger vos ressources en informations

Ces conseils vous aideront à mettre en place un système solide et résilient pour la sécurité de l'information et la protection des données.

Évaluer régulièrement les risques

Identifier les failles potentielles

Rechercher les menaces éventuelles

Évaluer les menaces et les classer par ordre de priorité

Utiliser vos conclusions pour élaborer un plan de gestion des risques

Instaurer des politiques de sécurité claires

Définir les meilleures pratiques

Donner des conseils sur la manière d'utiliser le système et de traiter les données

Guider vos employés quant à leurs responsabilités

Réviser régulièrement la politique et les procédures

Donner au personnel les moyens d'acquérirdes connaissances

Proposer des formations et des évaluations régulières

Sensibiliser le personnel aux meilleures pratiques (comme par exemple : des mots de passe forts)

Partager avec le personnel les enseignements tirés des menaces

Utiliser des contrôles d'accès stricts

Veiller à ce que seules les personnes autorisées puissent accéder aux données dont elles ont besoin

Mettre en place des méthodes d'authentification pour une sécurité accrue (comme par exemple : la gestion des accès privilégiés)

Maintenir l'infrastructure à jour

Mettre à jour et corriger régulièrement tous vos systèmes

Utiliser des pare-feux pour empêcher les intrusions

Sécuriser les réseaux afin empêcher tout accès non autorisé

Conseils

Conseils a continué

Se conformer aux réglementations

Les réglementations applicables dans votre domaine vous aideront à garantir les meilleures pratiques au sein de votre propre organisation

Le RGPD, le CCPA, etc., vous donneront les conseils les plus récents pour sécuriser votre réseau

Crypter les données sensibles

Même si les données sont compromises, elles ne peuvent pas être lues lorsqu'elles sont cryptées

Les politiques RGPD doivent comprendre le cryptage des données

Élaborer un plan d'intervention en cas d'incident

Élaborer et tester régulièrement votre plan d'intervention pour vous assurer que les facteurs les plus récents sont inclus

Définir des rôles et des responsabilités ainsi que des canaux de communication clairs

Collaborer et partager avec d'autres organisations

L'échange d'informations avec vos collègues est unbon moyen de comprendre le paysage actu des attaques

Le partage des meilleures pratiques permet à chacun de rester protégé

Évaluer souvent la chaîne d'approvisionnement et les fournisseurs

Vos fournisseurs de logiciels et de prestations cloud doivent disposer de leurs propres politiques pour protéger les données de votre organisation

Ces politiques doivent être conformes à vos propres normes de sécurité

Tendances en matière de sécurité de l'information que toutes les entreprises devraient connaître en 2023

Dans un paysage en constante évolution et de plus en plus numérique, les choses évoluent incroyablement vite. En matière de sécurité de l'information, ce qui était la norme il y a quelques années peut rapidement devenir obsolète. C'est pourquoi il est important de rafraîchir régulièrement ses connaissances sur les meilleures pratiques afin de s'assurer que votre entreprise se protège au mieux.

Découvrez ci-dessous nos principales tendances :

Sécurité zéro confiance :

la mise hors ligne de votre site web à la suite d'attaques est une chose, mais lorsque l'ensemble de votre système est compromis par une cybermenace, c'est une catastrophe majeure pour votre entreprise. La sécurité zéro confiance est une approche de la sécurité des réseaux qui part du principe que tout le trafic est potentiellement hostile et exige une vérification avant d'accorder l'accès, rendant ainsi plus difficile l'atteinte des cibles par les cybermenaces.

Authentification multifacteur (MFA) :

l'authentification multifacteur peut réduire considérablement le risque de compromission des comptes et d'atteinte à la sécurité. En exigeant plusieurs formes d'authentification (par exemple : un mot de passe puis un code envoyé à l'appareil mobile correspondant), un pirate potentiel aura beaucoup plus de difficulté à accéder aux données de votre entreprise.

IA et apprentissage automatique :

l'intelligence artificielle (IA) et l'apprentissage automatique (Machine Learning ou ML) offrent désormais des moyens de renforcer la sécurité. L'IA et le ML ont été utilisés pour analyser des quantités massives de données en temps réel, en analysant les tendances et en identifiant les comportements ou les activités inhabituelles.

Investissement dans les talents en matière de cybersécurité :

l'avènement de la cybersécurité étant relativement récent, nous connaissons actuellement une pénurie de talents dans ce domaine, ce qui signifie que si une entreprise souhaite disposer d'un professionnel spécialisé dans la sécurité de l'information, elle devra investir dans la formation, le développement et la mise à niveau du personnel existant. En même temps, la cybersécurité attire de plus en plus de formations, attirant ainsi de jeunes talents désireux de progresser au sein des entreprises.

Réglementation en matière de confidentialité des données :

l'accent étant mis de plus en plus sur la confidentialité des données, les entreprises doivent s'assurer qu'elles respectent bien les réglementations applicables, telles que le RGPD. Cela implique de mettre en oeuvre des mesures de sécurité adéquates, telles que le cryptage des données et les contrôles d'accès, et de s'assurer qu'elles ont instauré des politiques et des procédures pour protéger la confidentialité des données de leurs clients.

Faire preuve de proactivité afin de surmonter les menaces pour la sécurité.

En conclusion, face au paysage numérique actuel en pleine évolution, les entreprises doivent être proactives pour protéger leurs informations et celles de leurs clients contre les cybermenaces.

Comme nous l'avons lu, les conséquences des violations de données et des attaques sont souvent dévastatrices pour les entreprises et les particuliers. En adoptant un état d'esprit proactif et une politique de sécurité globale, les entreprises peuvent identifier les failles, évaluer les risques et mettre en oeuvre des mesures de sécurité solides qui (sous réserve d'une maintenance régulière) peuvent servir à l'entreprise pendant des années. En outre, il est essentiel de se tenir au courant des tendances en matière de sécurité et de se conformer aux réglementations dans le cadre d'une approche proactive de la sécurité de l'information. Ce sont des signes positifs à observer dans toute entreprise, que vous soyez le client ou le fournisseur.

Pour en savoir plus sur la manière dont Thinkproject associe des solutions logicielles innovantes en matière de construction à un niveau de sécurité optimal, visitez notre Centre de confiance.

Thinkproject Trust Centre

thinkproject

Thinkproject est le premier fournisseur européen de solutions SaaS pour l'Environnement Commun de Données, la gestion des actifs, du BIM, du suivi de chantier et du contrôle du projet. Depuis plus de 20 ans, Thinkproject digitalise l'activité des entreprises du secteur de la construction, les entreprises générales, les maîtrises d'oeuvre et les maîtrise d'ouvrage grâce à une technologie puissante et flexible, associée à une expertise de conseil issue de la connaissance de projets complexes de grande envergure.

Avec plus de 650+ employés dans le monde, Thinkproject offre des solutions digitales qui couvrent l'ensemble du cycle de vie d'un projet de construction.

75000
PROJETS

3250
CLIENTS

300000
UTILISATEURS

60
PAYS

650+
EMPLOYÉS FOCALISÉS SUR LES BESOINS CLIENTS

23
BUREAUX

Thinkproject.com