C0 - PUBLIC

algoan

V.3

Technical & organisational measures

Mesures techniques et organisationnelles

November 2024

Summary / Sommaire

I. Introduction

Algoan has consistently placed great emphasis on security and compliance aspects. This vision is shared by every member in the company, especially by the technical team.

The purpose of this document is to summarize the technical and organizational measures implemented at Algoan with regard to information security and compliance, enabling us to meet our customers' regulatory requirements, but also to ensure that security is a top priority. All Algoan solutions are designed, at first, with the highest standards of security and privacy. We understand how important our customers' data is to them and those who depend on them. We don't take our responsibility lightly; we work diligently to continually improve security processes and controls, and to provide our customers with the appropriate functionality to secure data where necessary.

Algoan's information security program complies with applicable data protection regulations such as the GDPR and is aligned with cybersecurity standards (ISO-27001, OWASP and NIST). In addition, Algoan's information security management system has been certified as compliant with ISO-27001:2022 by Bureau Veritas. Algoan is also registered as an Account Information Service Provider (AISP) with the ACPR (Banque de France).

This document therefore details the actions implemented in the following categories: management system (security policies, procedures and rules), access control, business continuity, human resources security, infrastructure security, network security, third-party security, vulnerability management, audits and incident management.

II. Security organization

Algoan has a dedicated Information Security team, responsible for all security issues within the organization.

Our security team holds various certifications and other titles that attest to their skills in the field. The team includes a DevSecOps engineer with multiple Pen Testing contest awards.

III. Human resources security

1. Background checks

A reference check is systematically carried out before any recruitment to verify the information provided by the applicant. This reference check is carried out by a third party in compliance with local regulations. It should be noted that positions of responsibility or requiring privileged access receive special attention during the recruitment process.

Algoan also ensures that any employee of a subcontractor or service provider with access to customer data or to Algoan's production environment is subject to the same levels of control by the subcontractor/service provider and to the same requirements as Algoan staff.

2. Confidentiality agreement

All Algoan employees must sign non-disclosure agreements, an IT charter, a code of ethics and a code of conduct before gaining access to company systems or data. People with privileged access must undertake in writing to respect the obligations of security and confidentiality of information which continue after termination or change of employment. This commitment is a prerequisite for obtaining their access. Algoan maintains a formal disciplinary procedure for violations by Algoan personnel of its security policies and procedures.

3. Sensibilization and training

Every new employee is required to attend an information security training session when joining the company. This session is designed to make the new member of staff aware of their responsibilities, and to highlight their role in protecting against insider threats, ransomware, social engineering, the appropriate use of assets and other related aspects.

After initial training, ongoing training is provided by means of updates, notifications and internal communications carried out at least bimonthly.

IV. Suppliers management

Algoan maintains and applies a documented process for the evaluation and approval of third-party service providers prior to their integration, which includes an appropriate risk analysis of each third party's processes. We require third parties to contractually commit to confidentiality, security responsibilities, security controls and data reporting obligations. Algoan regularly assesses each supplier, taking into account Algoan's security and business continuity standards, including the type of access and classification of data accessed (if applicable), the necessary data protection controls and legal/regulatory requirements.

V. Incidents management

Algoan has established procedures for receiving security incident reports.

The Algoan team has an established incident management process. To respond to an incident, we first determine the exposure of the information and the origin of the security problem, if possible. We communicate with the customer (and any other affected customers) by e-mail or telephone (if e-mail is not sufficient). We provide any periodic updates required to ensure that the incident is properly resolved.

If you have any security concerns or are aware of an incident, please contact us via our support desk or by e-mail at support@algoan.com. If you think this is a confirmed security incident, please add security@algoan.com to your message.

VI. Access and identification management

1. Zero Trust philosophy: end-to-end security

Algoan applies the Zero Trust security model, and therefore makes no distinction between on-premises and remote security procedures. All company devices are centrally managed. They are configured to prevent physical access via automatic screen locking, full hard disk encryption, and other protections. All connections are made via VPN or IAP. End users cannot disable anti-virus software or any other security features.

Our IT team performs regular updates to ensure that all devices are running the latest version of software.

2. Password and access policy

Algoan follows a strict process for granting or revoking access to its resources. System access is based on the concepts of “least privilege” and “need to know” to ensure that authorized access is in line with defined responsibilities. All employees are required to use a unique identifier to access company systems.

3. Access to Algoan premises

As noted in Section VII.1, customer data is deployed in Google Cloud data centers, not in facilities owned or operated by Algoan. In Algoan's offices, we follow industry best practice to use physical security controls appropriate to the level of risk posed by the information stored and the nature of operations in our offices.

4. Termination process

Algoan adheres to a documented termination process that outlines responsibilities for gathering information and revoking access rights from employees upon their departure from the company.

VII. Algoan product infrastructure

1. Environmental and physical conditions

We try as much as possible to be « cloud independent » and « software independent » in order to avoid lockdowns and critical scenarios. That's why we favour open-source, and we have selected alternatives for every component in our business continuity plan.

Our microservices infrastructure is hosted on the Google Cloud datacenters in E.U. Each microservice is replicated at least twice in different nodes.

Thus, our infrastructure benefits from the highest level of security of Google Cloud, which are certified from many rigorous compliance labels such as PCI-DSS and SOC 2, ISO-27001, etc.

Google Cloud data centers have 6 layers of security, and the following controls (not exhaustive) are in place:

- Closed-circuit television (CCTV) cameras
- Security agents
- Emergency power supply
- Temperature and humidity control
- Smoke detectors
- Leak detection

Finally, Algoan does not host any IT systems in its own offices.

2. Data Separation

Algoan establishes a strict separation between production and non-production environments.

In our Algoan production environment, clients' projects and customer data are never used for purposes other than those detailed in the contracts. Our non-production environments are used for development, testing and preparation. Algoan also maintains firewalls to achieve strict separation of our Algoan production environment from Algoan's internal network.

3. Software development life cycle

Algoan has a dedicated security team, reporting to the Chief Information Security Officer, which leads security initiatives in the Software Development Life Cycle (SDLC).

We develop new products and features in a multi-stage process using industry-standard methodologies that include defined security acceptance criteria and align with NIST and OWASP guidelines.

The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code validations, code version management, static and dynamic code analysis, vulnerability management, threat modeling and bug hunting, as well as automated and manual source code analysis.

4. Monitoring and alerting system

Algoan has implemented log review and monitoring tools to identify any anomalies or abuses.

Algoan monitors the health and performance of the Algoan infrastructure without the need to access customer data. Algoan maintains a centralized log management system for the collection, storage and analysis of log data for our Algoan production environment.

We use this information for status monitoring, troubleshooting and security purposes, including intrusion detection. We retain our log data for at least one year, and use a combination of automated analysis, automated alerts and human review to monitor the data. If an incident is detected, the relevant team will review, investigate and apply corrections.

Algoan collect logs, metrics and traces of our microservices and different integrations. We mainly use the Datadog solutions to aggregate it, create dashboards and alerts. Google Cloud Operations is used as a backup collecting solution.

Our various systems alert us through 4 different channels:

- internal messaging,
- email,
- SMS, and
- an automatic phone call system (to the phones of on-call personnel in the event of a critical error detected by our systems).

5. Network security

Algoan divides its system into separate networks to better protect the most sensitive data, and to separate utilities from internal services. Customer data shared with Algoan is only admitted to the production network.

We maintain an “infrastructure as code” approach to network security and firewall rules, and have alerts for any discrepancies between approved configuration and production settings.

All requests use SSL/TLS encryption (version 1.2 or higher). Our proposed webhook system has an HMAC-SHA-256 signature to ensure that there is no data tampering during each transfer. Also, to prevent information leakage, our webhook events do not contain any sensitive information (only identifiers). Information always needs to be retrieved from our APIs with authentication and authorization checks.

Finally, we implemented four intelligent security layers and separated key components into different virtual networks to enforce the strictest possible network security rules.

6. High availability and automatic failover

As described in section VII.1, each element of the Algoan production infrastructure is deployed with a minimum of 2 replicas, ensuring automatic failover in the event of a failure.

Our virtual machines are automatically provisioned across multiple availability zones within a region, offering resilience to localized site failures. Our virtual machines are independent nodes, guaranteeing continuity of service and greater resilience in the event of a virtual machine changeover. Moreover, another region is already identified, tested and configured if a failover would require switching to another region.

7. RTO/RPO/MTPD

We are really confident with our RPO/RTO/MTPD thanks to our partners, our cloud strategy and the fact our whole infrastructure is in IaC mode (Infrastructure As Code).

8. Backup and restoration

Our databases are backed up automatically every hour, day, week and month in a different data center from the one in which they are run. This managed solution also enables us to easily restore some (or all) of our databases. Backup restoration tests are carried out at least once a year.

9. Encryption

We take the confidentiality of our customers' data very seriously. That's why we encrypt all data in transit and at rest by default.

Our databases and backups are encrypted with our own private AES256-GCM key managed by KMS. Algoan manages its encryption keys in a key rotation safe using an HSM.

The secrets of our microservices are also encrypted at rest using an AES256 algorithm. In addition, all communication is encrypted using TLSv1.2+ or equivalent.

10. Shared cloud infrastructure

By default, Algoan offers a mutualized cloud service. Our customer data is logically segregated, which means that Algoan verifies that each user is authorized to make their request by checking that the user's company matches that of the requested corporate data.

11. System hardening

We apply recommanded good practices regarding system-hardening, limiting the use of systems, software and libraries to the strict minimum and privileging official and recognized versions.

VIII. Application security, incident response and communications

1. Vulnerability and patch management

A. Vulnerability analysis

Algoan maintains a documented vulnerability enumeration and management process that identifies company assets accessible on the Internet, searches for known vulnerabilities, assesses risk and tracks problem resolution. We conduct quarterly scans of the underlying systems on which Algoan is deployed, as well as of all third-party code embedded in our products. Algoan's vulnerability management policy requires technical teams to identify known vulnerabilities in system components and develop a fix within a timeframe appropriate to the severity of an identified problem. We also use automated tools in conjunction with security bulletin monitoring for relevant software and libraries, and implement patches if security issues are discovered.

For developments, we use multiple tools to detect and track security vulnerabilities and license control for modules and libraries.

B. Fixing vulnerabilities

Algoan uses a central, company-level ticketing system to track all security issues from identification to resolution. We implement patches for our operating system and applications based on update requirements, as determined in accordance with the Common Vulnerability Scoring System (CVSS).

Development tasks for all patches, bug fixes and new features are defined as issues for specific target versions and are deployed to production only after completion of the required checkpoints, including quality assurance testing, phased deployment and management review.

2. Change management and Infrastructure as Code

Algoan has a formal change management process for administering changes to the production service environment, including any modifications to its underlying software, applications and systems.

All changes to source code for production systems are subject to prior code review by a qualified engineering peer, including an analysis of security, performance and abuse potential.

3. Security monitoring

Our monitoring tools help us and alert us as soon as there is any malicious or abnormal behavior that could alter data processing or transfer.

For our employees' workstations and mobiles, we use an MDM and an antivirus solution.

4. Penetration testing and risk assessment

Algoan is regularly reviewed by internal and external security teams.

A. External

Our Algoan production environment is subject to external penetration testing by a nationally recognized security company at least once every calendar year.

B. Internal

Internally, Algoan's infrastructure undergoes periodic risk assessments, including the discovery of technical vulnerabilities and the analysis of business risks and concerns. Algoan's security team is also regularly involved in source code review, architecture review, code validation peer review and threat modeling.

5. Communication with customers

Algoan will notify affected customers without delay if we become aware of a data breach. Based on the information available to us, this notification will include a description of the nature and cause of the data breach, as well as the expected resolution timeframe. Where possible, we will then update affected customers with information concerning the assessment of the original cause, the potential impact, the corrective measures taken and the actions planned to prevent a similar event in the future.

XI. Documentation

Our documentation is available at docs.algoan.com.

Our Github page also provides :

- Node.js examples describing the main process for retrieving output from our products
- Fake open banking data with different credit risk personae

I. Introduction

Depuis sa création, Algoan porte une grande attention aux aspects qui concernent la sécurité et la conformité. Cette culture est partagée par chaque membre de l'entreprise et en particulier par l'équipe technique.

Ce document vise à résumer les mesures techniques et organisationnelles mises en place chez Algoan au sujet de la sécurité de l'information et de la conformité, permettant de répondre aux exigences réglementaires de nos clients, tout en plaçant la sécurité comme priorité absolue. Toutes les solutions d'Algoan sont développées, dès leur conception, avec un haut degré d'exigence vis-à-vis de la sécurité et de la protection des données.

Nous comprenons les enjeux liés à la sécurité des données de nos clients et mettons en œuvre les mesures adéquates. Nous ne prenons pas notre responsabilité à la légère ; nous travaillons avec application pour améliorer continuellement les processus et les contrôles de sécurité, ainsi que pour fournir à nos clients les fonctionnalités appropriées pour sécuriser les données.

Le programme de sécurité de l'information d'Algoan est conforme à la réglementation applicable sur la protection des données telle que le RGPD et est aligné sur les normes de cybersécurité (ISO-27001, OWASP et NIST). Par ailleurs, le système de management de sécurité de l'information d'Algoan a été certifié conforme à la norme ISO-27001:2022 par Bureau Veritas. Algoan est également enregistré en tant que Prestataire de Services d'Information sur les Comptes (PSIC) auprès de l'ACPR (Banque de France).

Ce document détaille donc les actions mises en œuvre dans les catégories suivantes : le système de management (politiques, procédures et règles de sécurité), le contrôle d'accès, la continuité des activités, la sécurité des ressources humaines, la sécurité de l'infrastructure, la sécurité du réseau, la sécurité des tiers, la gestion des vulnérabilités, les audits ainsi que la gestion des incidents.

II. Organisation de la sécurité

Algoan dispose d'une équipe chargée de la sécurité de l'information, qui est responsable de toutes les questions de sécurité au sein de l'organisation.

Les membres de l'équipe de sécurité d'Algoan sont titulaires de nombreuses certifications et autres titres qui attestent de leurs compétences dans le domaine. L'équipe est composée notamment d'un ingénieur DevSecOps qui possède de multiples récompenses de concours de Pen Testers.

III. Sécurité des ressources humaines

1. Vérification des antécédents

Une prise de référence est systématiquement réalisée avant toute embauche afin de vérifier des informations transmises par le candidat. Cette prise de référence est réalisée par un tiers dans le respect des réglementations locales. À noter que les fonctions à responsabilités ou qui nécessitent des accès privilégiés bénéficient d'une attention particulière lors du processus de recrutement.

Algoan s'assure par ailleurs que tout collaborateur d'un sous-traitant ou prestataire ayant des accès aux données clients ou à l'environnement de production d'Algoan soient soumis aux mêmes niveaux de contrôle de la part du sous-traitant/prestataires et aux mêmes exigences que le personnel d'Algoan.

2. Accord de confidentialité

Tous les employés d'Algoan doivent signer des accords de non-divulgation, une charte informatique, une charte de déontologie ainsi qu'une charte éthique et un code de bonne conduite avant d'avoir accès aux systèmes et aux données de l'entreprise. Les personnes ayant des accès privilégiés, doivent s'engager par écrit à respecter les obligations de sécurité et de confidentialité des informations qui perdurent après la résiliation ou le changement d'emploi. Cet engagement est un pré-requis pour l'obtention de leurs accès. Algoan maintient une procédure disciplinaire formelle pour les violations de ses politiques et procédures de sécurité par le personnel d'Algoan.

3. Sensibilisation et formation

Chaque nouvel employé doit assister à une session de formation à la sécurité de l'information lorsqu'il rejoint l'entreprise. Cette session vise à sensibiliser le nouveau membre du personnel, à ses responsabilités et à souligner son rôle contre les menaces internes, les rançongiciels, l'ingénierie sociale, l'utilisation appropriée des actifs et d'autres aspects connexes.

En plus de cette formation initiale, une formation continue est assurée au moyen de mises à jour, notifications et communications internes effectuées au moins bimensuellement.

IV. Gestion des fournisseurs

Algoan maintient et applique un processus documenté pour l'évaluation et l'approbation des fournisseurs de services tiers avant leur intégration, qui comprend une analyse appropriée des risques liés aux processus de chaque tiers. Nous exigeons que les tiers s'engagent contractuellement à respecter la confidentialité, les responsabilités en matière de sécurité, les contrôles et les obligations de déclaration des données. Algoan évalue ensuite régulièrement chaque fournisseur en tenant compte des normes de sécurité interne et de continuité d'activité d'Algoan, y compris le type d'accès et la classification des données consultées (le cas échéant), des contrôles nécessaires à la protection des données et des exigences légales/réglementaires.

V. Gestion des incidents

Algoan dispose de procédures établies pour la réception des rapports d'incident de sécurité.

L'équipe d'Algoan dispose d'un processus éprouvé de gestion des incidents. Pour répondre à un incident, nous déterminons d'abord l'exposition des informations et l'origine de l'incident, lorsque cela est possible. Nous communiquons avec le client (et tout autre client concerné) par e-mail ou par téléphone (si un e-mail ne suffit pas). Nous fournissons toutes les mises à jour périodiques nécessaires pour nous assurer de la bonne résolution de l'incident.

Si vous avez des questions concernant la sécurité ou si vous êtes informé.e d'un incident, nous vous invitons à nous contacter, via notre gestionnaire de ticket ou par e-mail à support@algoan.com. Si vous estimez qu'il s'agit d'un incident de sécurité avéré, merci de rajouter security@algoan.com à vos échanges.

VI. Gestion des accès et d’identification

1. Philosophie Zero Trust : sécurité de bout en bout

Algoan applique le modèle de sécurité Zero Trust, et ne fait donc aucune différence entre les procédures de sécurité dans les locaux ou à distance. Tous les appareils de l’entreprise sont gérés de manière centralisée. Ils sont configurés pour empêcher un accès physique via le verrouillage automatique de l’écran, le chiffrement complet des disques durs, et d’autres protections. Toutes les connexions utilisent un algorithme de chiffrement. Les utilisateurs finaux ne peuvent pas désactiver les logiciels antivirus ou toute autre fonctionnalité de sécurité.

Notre équipe informatique effectue des mises à jour régulières pour s'assurer que tous les appareils fonctionnent avec la dernière version du logiciel.

2. Politique de mots de passe et d’accès

Algoan suit un processus strict pour accorder ou révoquer l'accès à ses ressources. L'accès aux systèmes est basé sur les concepts de « principe de moindre privilège » et de « besoin d'en connaître » afin de garantir que l'accès autorisé est conforme aux responsabilités définies. Tous les employés d’Algoan sont tenus d'utiliser un identifiant unique pour accéder aux systèmes de l'entreprise.

3. Accès aux locaux d’Algoan

Comme indiqué dans la section VII.1, les données client sont déployées dans les centres de données de Google Cloud, et non dans des installations détenues ou exploitées par Algoan. Dans les bureaux d’Algoan, nous suivons les meilleures pratiques de l'industrie en utilisant des contrôles de sécurité physique adaptés au niveau de risque posé par les informations stockées et à la nature des opérations dans nos bureaux.

4. Processus de résiliation

Algoan suit un processus de résiliation qui définit les responsabilités en matière de collecte des informations et de suppression des droits d'accès des employés lorsqu'ils quittent l'entreprise.

VII. Infrastructure des produits Algoan

1. Conditions environnementales et physiques

Nous cherchons au maximum à d'être “cloud independant” et “software independant”. Cela implique que nous privilégions des solutions non propriétaires et que le plan de continuité d’activité d’Algoan possède des alternatives pour chaque composant au niveau de son infrastructure.

Notre infrastructure possède une architecture orientée micro-services. Elle est hébergée dans les centres de données de Google Cloud en U.E. Chaque micro-service est répliqué au minimum 2 fois dans des nœuds différents.

De ce fait, notre infrastructure bénéficie du plus haut niveau de sécurité de Google Cloud. Pour rappel, Google possède de nombreuses certifications telles que PCI-DSS, SOC 2 et ISO-27001, etc.

Les centre de données de Google Cloud possèdent 6 couches de sécurité, et les contrôles suivants (non exhaustifs) sont mis en place :

- Caméras de télévision en circuit fermé (TVCF)
- Agents de sécurité
- Alimentation électrique de secours
- Contrôle de la température et de l'humidité
- Détecteur de fumée
- Détection des fuites

Enfin, Algoan n'héberge pas de systèmes informatiques dans ses propres bureaux.

2. Séparation des données

Algoan établit une séparation stricte entre les environnements de production et de non-production.

Concernant l’environnement de production d’Algoan, les projets et les données client ne sont jamais utilisés à des fins différentes des usages détaillés dans les contrats. Nos environnements hors production sont utilisés pour les développements, les tests et la préparation. Algoan maintient également des pare-feu afin de parvenir à une séparation stricte des environnements de production et du réseau interne d’Algoan.

3. Cycle de vie du développement logiciel

Algoan dispose d'une équipe de sécurité dédiée, relevant du responsable de la sécurité de l'information, qui dirige les initiatives de sécurité dans le cycle de vie du développement logiciel (SDLC).
Nous développons de nouveaux produits et fonctionnalités dans le cadre d'un processus en plusieurs étapes en utilisant des méthodologies standard qui incluent des critères d'acceptation de sécurité et s'alignent sur les directives du NIST et de l'OWASP.

Le SDLC comprend des révisions régulières du code, des politiques et procédures documentées pour le suivi et la gestion de toutes les modifications apportées à notre code, l'intégration continue des validations de code source, la gestion des versions du code, l'analyse statique et dynamique du code, la gestion des vulnérabilités, la modélisation des menaces et la chasse aux bogues, ainsi que analyse automatisée et manuelle du code source.

4. Surveillance et système d’alerte

Algoan a mis en place des outils d'examen et de surveillance des registres afin d'identifier toute anomalie ou abus.

Algoan surveille par ailleurs la santé et les performances de son infrastructure sans avoir besoin d'accéder aux données client. Algoan maintient un système centralisé de gestion des journaux pour la collecte, le stockage et l'analyse des données de journaux pour l’environnement de production d’Algoan.

Nous utilisons ces informations à des fins de surveillance de l'état, de dépannage et de sécurité, dont la détection des intrusions. Si un incident est détecté, l'équipe compétente examinera, mènera une enquête et appliquera des corrections adéquates.

Algoan collecte des logs, métriques et traces des micro-services et des différentes intégrations.

Nos différents systèmes nous alertent sur 4 canaux différents :

- messagerie interne,
- email,
- SMS, et
- un système d’appel téléphonique automatique (sur les téléphones des personnes d’astreinte en cas d’erreur critique détectée par nos systèmes).

5. Sécurité réseau

Algoan divise son système en réseaux séparés pour mieux protéger les données les plus sensibles et pour séparer les services publics des services internes. Les données des clients partagées avec Algoan ne sont admises que dans le réseau de production.

Algoan maintient une approche « d'infrastructure en tant que code » pour la sécurité du réseau et les règles de pare-feu et dispose d'alertes pour toute divergence entre la configuration approuvée et les paramètres de production.

Toutes requêtes utilisent le chiffrement SSL/TLS (version 1.2 ou plus). Le système de webhook proposé possède une signature HMAC-SHA-256 afin d'assurer qu'il n'y a pas d'altération de la donnée durant chaque transfert. Aussi, dans le but d'éviter une fuite d'information, les évènements de webhook ne possèdent aucune information sensible (seulement les identifiants).
Les informations ont toujours besoin d'être récupérées depuis nos API avec une vérification de l'authentification et des autorisations.

Enfin, Algoan a mis en place 4 couches de sécurité intelligentes et a dissocié les composants clés sur différents réseaux virtuels dans le but d'avoir des règles de sécurité réseaux les plus strictes que possible.

6. Haute disponibilité et basculement automatique

Comme décrit dans la section VII.1, chaque élément de l'infrastructure de production est déployé avec un minimum de 2 replicas, ce qui assure un basculement automatique en cas de panne.

Les machines virtuelles sont automatiquement provisionnées sur plusieurs zones de disponibilité au sein d'une région, offrant ainsi une résilience aux pannes de sites localisées. Nos machines virtuelles sont également des nœuds indépendants, garantissant une continuité de service et une plus grande résilience lors d'un changement de machine virtuelle. De plus, une autre région est déjà identifiée, testée et configurée si un basculement nécessitait de passer sur une autre région.

7. RTO/RPO/MTPD

Compte tenu de la stratégie cloud retenue par Algoan et par le fait que la totalité de l'infrastructure d'Algoan est en mode IaC (Infrastructure As Code), nous sommes très confiants sur les niveaux de RTO/RPO/MTPD garantis.

8. Sauvegarde et restauration

Nos bases de données possèdent des sauvegardes automatiques toutes les heures, jours, semaines et mois dans un centre de données différent de celui d'exécution. Cette solution managée permet ainsi de restaurer très facilement une partie (ou la totalité) des bases de données. Des tests de restauration des sauvegardes sont effectués au moins une fois par an.

9. Chiffrement

Algoan prend très au sérieux la confidentialité des données de ses clients. C'est pourquoi nous chiffrons toutes les données en transit et au repos par défaut.

Nos bases de données et les sauvegardes sont chiffrées avec notre clé privée AES256 gérée par notre KMS. Algoan administre ses clés de chiffrement dans un coffre-fort gérant la rotation des clés et utilisant un HSM.

Les secrets de nos micro-services sont aussi chiffrées au repos avec un algorithme AES256. De plus, toutes les communications sont chiffrées et utilisent le protocole TLSv1.2+ ou équivalent.

10. Infrastructure mutualisée de cloud

Algoan offre, par défaut, un service mutualisé de cloud. Les données clients sont logiquement séparées, ce qui signifie qu'Algoan vérifie que chaque utilisateur est autorisé à effectuer sa requête en vérifiant que la société de l'utilisateur correspond à celle des données d'entreprise demandées.

11. Durcissement des systèmes

Nous appliquons les bonnes pratiques de durcissement des systèmes en limitant l'utilisation des systèmes, logiciels, bibliothèques au strict minimum et en privilégiant des versions officielles et reconnues.

VIII. Sécurité des applications, réponse à incident et communications

1. Vulnérabilité et gestion des corrections

A. Analyse des vulnérabilités

Algoan maintient un processus documenté d'énumération et de gestion des vulnérabilités qui identifie les actifs de l'entreprise accessibles sur Internet, recherche les vulnérabilités connues, et évalue les risques et suit la résolution des problèmes. Nous effectuons des analyses trimestrielles des systèmes sous-jacents sur lesquels Algoan est déployé, ainsi que de tout le code tiers intégré dans nos produits. La politique de gestion des vulnérabilités d'Algoan exige que les équipes techniques identifient les vulnérabilités connues dans les composants du système et développent une correction dans le délai adapté à la gravité d'un problème identifié.
Enfin, nous utilisons également des outils automatisés en conjonction avec la surveillance des bulletins de sécurité pour les logiciels et bibliothèques pertinents, et met en œuvre des correctifs si des problèmes de sécurité sont découverts.

Pour les développements, nous utilisons divers outils pour détecter et suivre les failles de sécurité et le contrôle des licences des modules et bibliothèques.

B. Correction des vulnérabilités

Algoan utilise un système de tickets central à l'échelle de l'entreprise pour suivre tous les problèmes de sécurité jusqu'à leur résolution. Nous implémentons des correctifs pour le système d'exploitation et les applications en fonction des besoins de mise à jour conformément au Common Vulnerability Scoring System (CVSS).

Les tâches de développement pour tous les correctifs, corrections de bogues et nouvelles fonctionnalités sont définies comme des problèmes pour des versions cibles spécifiques et sont déployées en production uniquement après avoir effectué les points de contrôle requis, notamment les tests d'assurance qualité, le déploiement par étapes et l'examen de la direction.

2. Gestion des managements et Infrastructure as Code

Algoan dispose d'un processus formel de gestion des changements pour administrer les modifications apportées à l'environnement de production des services, y compris toute modification de ses logiciels, applications et systèmes sous-jacents.

Tous les changements apportés au code source destiné aux systèmes de production sont soumis à un examen du code préalable par un pair qualifié en ingénierie, qui comprend une analyse de la sécurité, des performances et du potentiel d'abus.

3. Surveillance de sécurité

Nos outils de monitoring nous aident et nous alertent dès qu'il y a un comportement malintentionné ou anormal qui pourrait altérer le traitement ou le transfert de la donnée.

Concernant les postes et mobiles des salariés, Algoan utilise un MDM ainsi qu'une solution antivirale.

4. Test de pénétration et évaluation des risques

Algoan est soumis à des examens réguliers de la part des équipes de sécurité internes et externes.

A. Externe

Notre environnement de production est soumis à un test d'intrusion externe. Ce test est réalisé par une société de sécurité reconnue au niveau national au moins une fois par année civile.

B. Interne

En interne, l'infrastructure Algoan est soumise à des évaluations périodiques des risques, y compris la découverte de vulnérabilités techniques et l'analyse des risques et des préoccupations de l'entreprise. L'équipe de sécurité d'Algoan est également régulièrement impliquée dans l'examen du code source, l'examen de l'architecture, l'examen par les pairs de la validation du code et la modélisation des menaces.

5. Communication avec les clients

Algoan informera sans délai les clients concernés si nous avons connaissance d'une violation de données. Compte tenu des informations dont nous disposons, cet avis comprendra une description de la nature et de la cause de la violation de données ainsi que le délai de résolution prévu. Dans la mesure du possible, nous mettrions ensuite les clients concernés à jour avec des informations sur l'évaluation de la cause originelle, l'impact potentiel, et les mesures correctives et les actions prévues pour empêcher un autre événement similaire.

XI. Documentation

Notre documentation est disponible sur docs.algoan.com.

Notre page Github fournit aussi :

1. Des exemples Node.js qui décrivent le processus principal pour récupérer le résultat de nos produits
2. Des jeux de tests cohérents avec différents profils de risque

algoan

Leading-edge technology
for better & fairer credit decisions

www.algoan.com