DELL Technologies

Sécurité et résilience d’entreprise de Dell

Présentation

Dell Technologies Security & Resiliency Organization - Version 1.1 - Dernière mise à jour le 05/04/2023

Chez Dell Technologies, nous sommes très attentifs à la manière dont nous instaurons la confiance et sécurisons un environnement connecté. L'émergence d'un monde connecté et intelligent, de la 5G et de technologies avancées comme l'IA et l'apprentissage automatique nous permet d'aller plus loin que nous ne l'avions imaginé. Nous montrerons sécurité, résilience et adaptabilité face à ce monde en constante évolution. Et nous continuerons à mener à bien notre mission principale : protéger Dell Technologies et gagner la confiance de nos clients en intégrant la sécurité et la résilience dans chaque activité de Dell.

John Scimone, directeur de la sécurité

Security & Resiliency Organization

Protéger Dell Technologies et gagner la confiance de nos clients en intégrant la sécurité et la résilience dans chacune de nos activités

Cybersécurité

Protection des données des clients et des sociétés

Intelligence sur les menaces avancée grâce à une visibilité sur les menaces émergentes

Gestion des identités et des accès

Gestion des cyber-risques, garantie de la conformité et sécurisation appropriée de notre environnement

Résilience d'entreprise, procédures d'enquête mondiales et sécurité d'entreprise

Sécurité et résilience d'entreprise

Sécurité d'entreprise : gérer la protection des personnes, des informations, des ressources et de notre réputation contre les attaques et les événements physiques et environnementaux

Gestion des crises : gérer les événements inattendus susceptibles d'avoir un impact négatif sur Dell Technologies

Continuité d'activité : assurer la récupération rapide des processus et opérations stratégiques de l'entreprise

Gouvernance de la reprise après sinistre : assurer la récupération rapide des données et systèmes stratégiques de l'entreprise

Procédures d'enquête mondiales : gérer les incidents physiques tels que le vol, la fraude et la violence sur le lieu de travail

Sécurité des applications et des produits

Réponse aux failles de sécurité : réagir rapidement en cas de faille de sécurité pour maintenir la sécurité des applications et des produits déployés

Secure Development Lifecycle : développer des applications et des produits plus sûrs en intégrant la sécurité dans le cycle de vie de développement

Gouvernance, risques et conformité

Créer, maintenir et assurer la conformité des politiques, normes et processus de sécurité et de résilience de Dell Technologies

Garantir la conformité avec les réglementations externes telles que la loi Sarbanes-Oxley (SOX) et la norme PCI DSS (Payment Card Industry Data Security Standard) relative à la sécurité des données des cartes de paiement

Effectuer des audits, renouveler les contrats (lorsque Dell Technologies est un fournisseur du client) et fournir aux clients des informations sur les règles et les protocoles de sécurité en matière de produits et services Dell

Dell Federal | Dell Technologies Services | Dell Financial Services

Cybersécurité

La cybersécurité définit des normes, met en œuvre et entretient des programmes de sécurité et des technologies qui permettent à Dell Technologies de gérer et d'atténuer les risques, et protège nos informations, notre entreprise, nos clients et notre marque contre des adversaires chevronnés.

Chez Dell Technologies, l'équipe Cybersecurity est responsable des éléments suivants :

- Protection des données des clients et des sociétés
- Intelligence sur les menaces avancée grâce à une visibilité sur les menaces émergentes
- Gestion des identités et des accès
- Gestion des cyber-risques, garantie de la conformité et sécurisation appropriée de notre environnement

L'intérêt de la cybersécurité

4,5 heures
Temps de propagation moyen des attaquants au sein du réseau d'une société après l'intrusion initiale

6 000 milliards de $
Coût projeté des violations dans le monde en 2021

78 jours
Temps moyen de détection d'une intrusion sophistiquée

Sécurité des applications et des produits

La sécurité des applications et des produits consiste à s'assurer que les produits proposés aux clients sont protégés contre les cybermenaces et ne comportent aucune faille de sécurité.

Chez Dell Technologies, l'équipe Product and Application Security est responsable des éléments suivants :

- Secure Development Lifecycle : développer des applications et des produits d'entreprise plus sûrs en intégrant la sécurité dans le cycle de vie de développement
- Réponse aux failles de sécurité : réagir rapidement en cas de faille de sécurité pour maintenir la sécurité des applications et des produits déployés

L'intérêt de la sécurité des applications et des produits

90 %
des incidents de sécurité sont dus à l'exploitation de défauts dans les produits

Il est 100 fois
plus cher de corriger des défauts logiciels dans la phase de maintenance que dans la phase de conception

~ 60 %
des violations impliquent généralement une faille de sécurité pour laquelle un correctif existait

Global Security Operations

Les opérations de sécurité mondiales consistent à gérer la protection des personnes, des informations, des ressources et de notre réputation contre les attaques et les événements physiques et environnementaux. Chez Dell Technologies, l'équipe Global Security Operations est responsable des éléments suivants :

- Protection des personnes, des processus, des ressources et de la marque Dell Technologies dans le monde entier
- Gestion des agents et caméras de sécurité, enquêtes sur les délits et les incidents de sécurité non informatiques commis contre la société par des collaborateurs et des criminels

Exemples d'actions de l'équipe Global Security Operations :

- Gestion des crises
- Continuité d'activité
- Reprise après sinistre
- Gestion des risques de malveillances internes
- Procédure d'enquête sur les délits et les violations du Code de conduite
- Services d'agents de sécurité en uniforme
- Systèmes de sécurité des locaux
- Sécurité des événements
- Protection renforcée du personnel à haut risque
- Transport sécurisé des membres du personnel et ressources clés
- Réception de toutes les questions liées à la sécurité sur Security@Dell.com

L'intérêt de Global Security Operations

9 000 $

C'est le coût par minute d'une panne de datacenter non planifiée

21 %

des violations de la sécurité annuelles sont dues à des vols physiques et internes

+ de 2 M

d'incidents violents sur le lieu de travail aux États-Unis par an

78 %

des homicides sur le lieu de travail sont des meurtres par balle

Sécurité organisationnelle

Chez Dell Technologies, nous veillons à ce que nos collaborateurs mondiaux sachent qu'il est de leur responsabilité de se conformer aux pratiques et aux normes de sécurité et de résilience. Pour faciliter l'adhésion à nos pratiques et normes d'entreprise, notre équipe chargée de la sécurité des informations est responsable des éléments suivants :

1. Stratégie et conformité aux politiques/normes et réglementations, sensibilisation et formation, évaluations et gestion des risques, gestion des exigences contractuelles en matière de sécurité, conseils en matière d'applications et d'infrastructures, test d'assurance et orientation de la société en matière de sécurité
2. Tests de sécurité, conception et implémentation de solutions de sécurité visant à adopter des contrôles de sécurité dans l'environnement
3. Opérations de sécurité liées aux solutions de sécurité implémentées, à l'environnement et aux ressources, et gestion de la réponse aux incidents
4. Procédures d'enquête approfondies avec l'équipe chargée des opérations de sécurité, le département juridique, le service de protection des données et les ressources humaines pour les procédures d'enquête, y compris eDiscovery et eForensics.

Votre confiance, notre transparence

Le parcours de transformation numérique de Dell Technologies repose sur les mêmes piliers que ceux que nous proposons à nos clients : transformation de l'entreprise, transformation de l'IT, transformation des modes de travail et transformation de la sécurité. Nous adoptons et suivons le principe de « sécurité intrinsèque » dans tous les systèmes et solutions qui soutiennent nos processus métier ; et nous personnalisons l'utilisation de cadres et de méthodologies éprouvés afin qu'ils correspondent à notre stratégie d'entreprise. En plus de donner la priorité aux contrôles de sécurité, tels que ceux recommandés par le Center for Internet Security (CIS) et le SANS Institute, nous surveillons les éléments les plus importants pour nos clients. Les 20 contrôles sur lesquels nos clients demandent le plus souvent des informations sont présentés ci-dessous. Nous les avons regroupés sur la base des cinq fonctions les plus générales définies dans le cadre de cybersécurité (CSF) du NIST.





Identifier	Protéger	Détecter	Réagir	Restaurer
Gestion du parc informatique	Gestion des accès	Protection contre les logiciels malveillants	Continuité d'activité	Reprise après sinistre
Conformité	Gouvernance des données	Gestion des changements	Gestion des incidents	
Gestion des risques	Recrutement Dell	Journalisation et alertes		
Chaîne logistique	Chiffrement	Gestion des failles de sécurité		
	Gestion de réseau			
	Gestion des mots de passe			
	Gestion des correctifs			
	Sécurité physique			
	Secure Development Lifecycle			

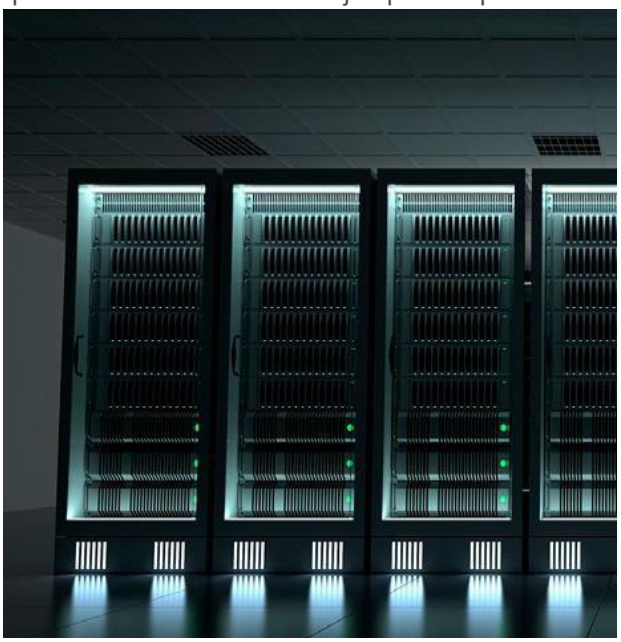
Identifier

Gestion du parc informatique

Dell a pour bonne pratique de répertorier et de gérer toutes les ressources physiques et logiques. Voici des exemples de ressources que le département IT de Dell Technologies peut répertorier :

- Les ressources d'informations, comme les bases de données identifiées, les plans de reprise après sinistre, les plans de continuité d'activité, la classification des données, les informations archivées.
- Les ressources logicielles, comme les applications identifiées et les logiciels système.
- Les ressources physiques, comme les serveurs identifiés, les ordinateurs de bureau/portables, les bandes de sauvegarde/archive, les imprimantes et les équipements de communication.

Il est très important pour Dell Technologies d'identifier, de suivre et de gérer les ressources logicielles, physiques et d'informations.
Dell Technologies dispose d'un solide programme de gestion de parc informatique, dont les règles et les activités sont communiquées à l'ensemble du personnel. Toutes les ressources sont comptabilisées, ont un propriétaire désigné et sont provisionnées et contrôlées jusqu'à ce qu'elles soient obsolètes et renvoyées.



Elles sont classées en fonction de leur importance pour l'entreprise afin de déterminer les exigences de confidentialité, d'intégrité et de disponibilité appropriées. Les recommandations de l'industrie informatique pour la gestion des données à caractère personnel fournissent la base des mesures de protection techniques, organisationnelles et physiques. Elles peuvent comprendre des contrôles comme la gestion des accès, le chiffrement, la journalisation et la surveillance, ainsi que la destruction des données.

La Politique d'utilisation des ressources d'entreprise s'applique à toutes les ressources informatiques appartenant à la société, quel que soit leur emplacement, et définit plusieurs exigences visant à garantir que les collaborateurs de Dell Technologies comprennent clairement ce qui est considéré comme une utilisation acceptable de ces ressources.

Conformité

La gamme de politiques, de normes, de règles et de contrôles de Security & Resiliency Organization s'aligne sur les cadres NIST et ISO. Ces règles fondamentales portent sur le cycle de vie complet des données, nos environnements physiques et informatiques, ainsi que la contribution de chaque collaborateur à notre culture de la sécurité. Les départements Sécurité des informations, Juridique, Confidentialité et Conformité s'efforcent d'identifier toutes les lois et réglementations régionales applicables. Ces exigences couvrent des domaines tels que la propriété intellectuelle de la société et de nos clients, les licences logicielles, la protection des données personnelles de nos collaborateurs et de nos clients, les procédures de protection et de manipulation des données, la transmission de données en dehors des frontières, les procédures financières et opérationnelles, les contrôles réglementaires en matière d'exportation de technologie et les exigences propres aux procédures d'enquêtes.

Nous disposons de plusieurs mécanismes pour garantir le respect de ces exigences, y compris : le programme de sécurité des informations, le conseil exécutif en charge de la protection de la vie privée, le comité de pilotage en charge de la gestion des risques, le conseil mondial en charge de la gestion des risques et de la conformité, les audits/évaluations internes et externes, la consultation de conseillers juridiques internes et externes, les évaluations des contrôles internes, les tests de pénétration internes et les évaluations des failles de sécurité, la gestion des contrats, la sensibilisation à la sécurité, les conseils en sécurité, les examens des dérogations aux règles et la gestion des risques. Diverses accréditations de sécurité ayant passé un audit et reçu une certification de manière indépendante (y compris SOX, ISO 27001, SOC1, SOC2 et PCI DSS) sont également en place, en fonction des besoins de l'entreprise et de l'emplacement.

Notre Code de conduite détaille notre manière de mener les opérations au quotidien au sein de Dell Technologies, selon notre culture et nos valeurs, dans le respect de la lettre ou de l'esprit des lois applicables dans les pays au sein desquels nous opérons.

Gestion des risques

Nous avons mis en place un programme de gestion des risques afin de disposer de procédures adéquates pour identifier, évaluer et traiter les risques liés aux informations précieuses de l'organisation. Il aborde les incertitudes relatives à ces ressources de façon à ce que les résultats opérationnels souhaités soient atteints.

Notre programme de gestion des risques utilise un cadre intégré de contrôle et de risque axé sur les besoins clés de l'entreprise en matière de disponibilité, d'accès, de précision et d'agilité en lien avec les technologies de l'information et la sécurité des informations. Il fournit la structure et la discipline nécessaires pour garantir que les risques liés aux technologies de l'information et à la sécurité des informations sont évalués en permanence et traités de manière proactive et rentable, y compris en ce qui concerne les personnes, les processus, les données et les technologies. Les risques sont répertoriés et gérés dans le cadre du plan d'action de gestion/processus de mesure corrective (MAP) ; pour chacun d'eux, un propriétaire de risque est désigné et chargé des mesures correctives.

Chaîne logistique

Nous adoptons une approche globale et complète pour protéger notre chaîne logistique et livrer des solutions fiables aux clients. Notre stratégie de « défense en profondeur » et de « défense en largeur » implique plusieurs couches de contrôle pour limiter les risques pouvant s’introduire dans la chaîne logistique. Ces contrôles contribuent à établir l’assurance de la chaîne logistique, qui garantit que l’ensemble des processus et contrôles effectués tout au long de la chaîne logistique et du cycle de vie des produits permettra de générer et de livrer des informations, des processus et des produits exempts d’éléments non souhaités et fonctionnant comme prévu.

Notre framework de gestion des risques liés à la chaîne logistique reflète le framework complet de gestion des risques du plan américain de protection des infrastructures (NIPP). Ce dernier décrit comment le gouvernement et le secteur privé américains peuvent travailler ensemble pour limiter les risques et atteindre leurs objectifs de sécurité. Notre framework intègre un processus ouvert et itératif d’amélioration continue. Les plans de limitation des risques sont hiérarchisés et mis en œuvre selon les besoins tout au long du cycle de vie de la solution.

La gouvernance des fournisseurs est essentielle à la protection des performances et de l’intégrité de la chaîne logistique. C’est pour cela qu’elle commence par un examen approfondi des fournisseurs et partenaires potentiels avant l’intégration. Les analyses préalables à l’attribution du travail peuvent impliquer des enquêtes initiales sur site, des versions de qualification de la fabrication et des demandes d’informations (RFI) ou de proposition commerciale (RFQ) spécifiques au produit. Nous sommes parfaitement positionnés pour tirer parti des connaissances, des pratiques d’excellence, des technologies et de l’expertise des marques leaders, fiables et respectées de la gamme Dell Technologies. Nous pensons qu’il est essentiel d’écouter les clients, les fournisseurs et les partenaires, et de travailler avec eux pour continuer à améliorer la façon dont Dell Technologies garantit l’assurance de la chaîne logistique.

Protéger

Gestion des accès

Prévoir le cycle de vie des identités numériques et leur accès aux ressources de Dell est un facteur crucial dans la protection du réseau et des systèmes de Dell. La transformation numérique a rapidement quitté le datacenter traditionnel pour s'installer dans le Cloud, créant au passage un risque important en matière de rançongiciels et de pertes de données. Nos politiques de gestion des identités et des accès contribuent à renforcer la posture de sécurité, la conformité aux normes et l'excellence opérationnelle grâce à l'automatisation et à la hiérarchisation basée sur les risques.

Une gestion rigoureuse des identités, un accès utilisateur sur la base du « privilège minimum » et une authentification multifacteur permettent de répondre aux risques associés aux environnements hybrides, multicloud et en périphérie. L'approche de Dell comprend une gouvernance appropriée pour l'intégration, la mutation et la cessation de contrat des collaborateurs et des sous-traitants. Une analytique et une création de rapport robustes en temps réel permettent aux équipes chargées des opérations et de l'assurance de sécurité d'offrir une expérience utilisateur moderne tout en garantissant que les identités numériques (personnes, appareils et applications) disposent du « bon accès aux bonnes ressources au bon moment ».

Gouvernance des données

Notre cadre éprouvé de gouvernance des informations comprend des exigences relatives au cycle de vie des données et informations, qu'elles soient électroniques ou sur support papier. Il couvre la création, la réception, la gestion, le traitement, le stockage et l'élimination de toutes les informations utilisées dans le cours normal de l'activité, quel que soit leur format ou leur support. Les directives en matière de sécurité des informations et de confidentialité couvrent l'identification, la protection de la classification, la conservation et l'élimination de toutes les applications/bases de données et de tous les documents dans des référentiels/lieux de stockage approuvés.

- Les ressources d'informations sont identifiées et répertoriées en fonction de leur emplacement et de leurs déplacements tout au long de leur cycle de vie.
- Les données structurées et non structurées sont classées selon les catégories de classification des données adoptées (Public, Usage interne, Accès limité et Accès strictement limité). Lorsque des informations relèvent de plusieurs classifications, la catégorie de classification la plus restrictive est appliquée. Les ressources sont classées en fonction de leur importance pour l'entreprise, afin de déterminer les exigences de confidentialité appropriées.
- En fonction de la valeur, de l'utilisation et de la finalité des données, des exigences de protection sont définies pour chaque catégorie de classification des données, depuis leur création jusqu'à la fin de leur cycle de vie. Les recommandations de l'industrie informatique pour la gestion des données à caractère personnel fournissent la base des mesures de protection techniques, organisationnelles et physiques.
- Les informations sont conservées conformément à la période définie en fonction des exigences légales ou réglementaires, y compris l'obligation légale de conservation, et des besoins de l'entreprise.
- Les informations doivent être éliminées en toute sécurité une fois la période de conservation expirée.

Recrutement Dell

Les contrôles que nous avons mis en place couvrent la vérification des antécédents et des compétences de tous les candidats à l'emploi, afin de s'assurer que nos collaborateurs et nos sous-traitants comprennent leurs responsabilités et sont aptes à remplir les fonctions pour lesquelles leur recrutement est envisagé. Ces contrôles sont effectués conformément aux lois, aux règlementations et à l'éthique en vigueur, et sont proportionnels aux besoins métier, à la classification des informations accessibles et aux risques perçus qui y sont associés.

Dans le cadre du processus de recrutement, tous nos collaborateurs et sous-traitants doivent signer un accord de confidentialité et se soumettre à un processus de sélection conforme à la législation régionale.

Chiffrement

Notre politique en matière de cryptographie est conforme aux pratiques d'excellence du secteur. En outre, les normes et les contrôles qui soutiennent nos politiques sont alignés de manière dynamique sur les besoins métier et juridiques de nos parties prenantes.

Nous établissons et gérons des clés cryptographiques pour la cryptographie requise utilisée dans le système d'information, conformément aux exigences définies par l'organisation sur la génération, la distribution, le stockage et la destruction des clés, ainsi que l'accès à celles-ci. Un système de cryptographie est mis en œuvre pour les données faisant l'objet d'une classification spécifique, comme le prévoient les politiques ou les normes adoptées en la matière. Notre réseau sans fil est sécurisé à l'aide des meilleures méthodes cryptographiques standard de l'industrie.

Nos processus et systèmes cryptographiques fournissent des services pour les données au repos, en cours d'utilisation et en mouvement, ce qui inclut la prise en charge des infrastructures, des bases de données et des applications. De plus, notre solide processus de gestion des clés cryptographiques garantit que les clés, les certificats et les signatures numériques sont sécurisés tout au long de leur cycle de vie. Cela comprend la génération, la distribution, le stockage, la sauvegarde, la rotation, l'expiration, l'archivage et la destruction.

Gestion de réseau

Dell Technologies met en œuvre les mesures de protection du réseau nécessaires, telles que l'utilisation de contrôles techniques et administratifs pour gérer la sécurité du réseau et de l'infrastructure sous-jacente.

Nos contrôles sont alignés sur le cadre NIST et le Center for Internet Security pour sécuriser et renforcer les périphériques réseau. La gestion de réseau assure la connectivité à Internet et au réseau local, l'accès distant à nos ressources, ainsi que les normes de conception de réseau à partir desquelles nous sécurisons les services de réseau fournis aux utilisateurs. Grâce à des contrôles administratifs, physiques et technologiques mis en œuvre conformément aux pratiques d'excellence du secteur, nous garantissons un environnement sécurisé basé sur des couches de composants de protection complémentaires, ce qui améliore la sécurité globale.

Gestion des mots de passe

Dell Technologies reconnaît qu'il est impératif que nos utilisateurs fassent preuve de diligence raisonnable pour accéder à nos systèmes, en protégeant leurs comptes d'utilisateur par des mots de passe difficiles à deviner ou à supposer. Les mots de passe constituent un aspect important de la sécurité informatique ; ils sont la première ligne de protection des comptes d'utilisateur. S'il est mal choisi, un mot de passe peut compromettre l'ensemble du réseau de l'entreprise. Il incombe donc à tous les collaborateurs, sous-traitants et tiers ayant accès aux systèmes de prendre les mesures appropriées pour choisir et sécuriser leurs mots de passe et d'adhérer à l'authentification à deux facteurs pour accéder à notre réseau interne.

Une politique et des normes en matière de mots de passe, conformes aux normes du secteur, sont en place pour garantir que tous les utilisateurs adoptent des pratiques sûres et alignées à la stratégie de protection de l'infrastructure d'informations. Il s'agit notamment de la création de mots de passe forts, de la protection de ces mots de passe et de la fréquence de leur changement. En outre, nos systèmes de journalisation, de surveillance, d'automatisation et d'alerte appliquent les politiques en matière de mots de passe et fournissent une couche de sécurité supplémentaire.

Gestion des correctifs

Nous maintenons un programme global de gestion des correctifs qui suit les normes du secteur et répond aux exigences réglementaires et de conformité. Notre processus de gestion des correctifs est conforme aux pratiques d'excellence en matière de sécurité. Il comprend les éléments suivants :

- Connaissance systématiquement à jour des correctifs disponibles.
- Liste de toutes les ressources qui nécessiteront des correctifs à l'aide d'outils de surveillance automatisés.
- Détermination des correctifs appropriés pour des systèmes particuliers, en veillant à ce qu'ils soient correctement testés.
- Installation dans le cadre d'un programme de gestion du contrôle des changements.
- Examen des processus et des résultats des correctifs et documentation de toutes les procédures associées, telles que les configurations spécifiques requises et les procédures de correctifs standard et d'urgence.

Nos applications et nos systèmes nouveaux et existants sont maintenus au niveau des derniers correctifs de sécurité.

Sécurité physique

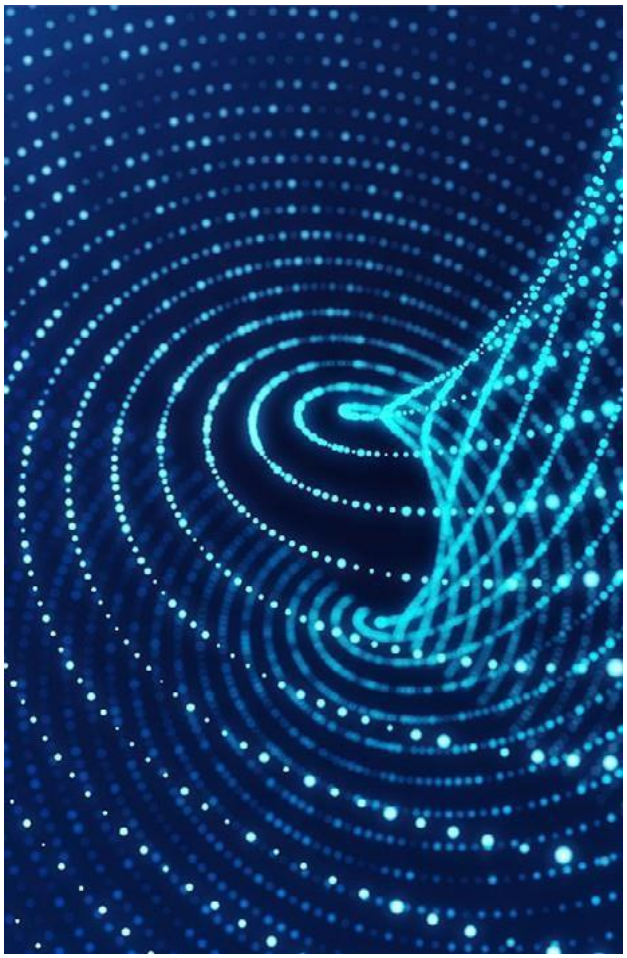
Les installations informatiques sont l'un de nos biens les plus précieux et doivent être protégées. La restriction de l'accès physique au personnel autorisé, ainsi que de solides contrôles environnementaux, protègent la confidentialité, l'intégrité et la disponibilité de nos données et de nos environnements informatiques contre un large éventail de menaces. Cela permet d'assurer la continuité d'activité, de minimiser l'impact sur l'entreprise et d'optimiser le retour sur investissement et les opportunités métier.

Le programme de sécurité physique suit les pratiques d'excellence du secteur en matière de sécurité et les exigences réglementaires, afin de garantir que les accès physiques aux locaux utilisés pour notre activité sont contrôlés par des points d'entrée physiques sécurisés et ainsi d'empêcher l'accès non autorisé, les dommages et les interférences avec les sites et les informations. L'accès aux locaux contenant des données sensibles ou stratégiques est uniquement donné au personnel ayant un besoin professionnel autorisé. Des contrôles et des vérifications régulières sont effectués pour s'assurer que cet accès est uniquement accordé au personnel approprié.

Secure Development Lifecycle

Nous utilisons un cycle de vie du développement de système robuste pour contrôler les étapes à suivre et ainsi garantir que tout le matériel, les logiciels et les firmwares distribués aux clients (internes et externes) ont été conçus, développés et conditionnés de manière appropriée dans le cadre d’un programme de gouvernance formel, tel que défini par le cycle de vie du développement.

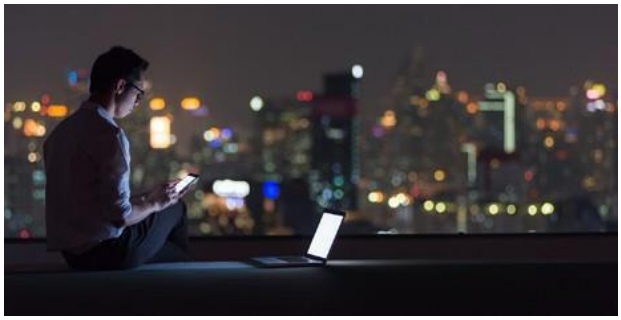
Nous nous efforçons d’intégrer la sécurité tout au long du cycle de vie du produit ou de l’application afin qu’ils soient élaborés de manière sûre et restent sécurisés. Le programme de sécurité de Dell comprend des activités d’analyse, telles que la modélisation des menaces, l’analyse du code statique et les tests de sécurité, pour identifier et corriger les défauts de sécurité tout au long du cycle de vie de développement.



Le programme Secure Development Lifecycle de Dell est conforme aux principes énoncés dans la norme ISO/IEC 27034 « Technologies de l’information, techniques de sécurité, sécurité des applications ». Dell Technologies collabore également avec de nombreux organismes de normalisation, tels que SAFECode, BSIMM et IEEE Center for Secure Design, afin de s’assurer qu’elle respecte les pratiques du secteur.

En outre, de nombreux collaborateurs Dell Technologies sont activement impliqués dans des organisations qui se concentrent sur le développement de normes de sécurité et sur la définition de pratiques de sécurité à l'échelle du secteur, y compris :

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Forum of Incident Response and Security Teams (FIRST)
- InterNational Committee for Information Technology Standards (INCITS)
- Organisation internationale de normalisation (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)



Les failles de sécurité rendues publiques par des tiers sont régulièrement examinées afin de déterminer leur impact et la possibilité qu'elles affectent notre environnement. En fonction du risque pour l'activité et les clients, il existe des temps de mise en œuvre prédéterminés pour les mesures correctives. De plus, nous utilisons une approche proactive et basée sur le risque, qui consiste à effectuer des analyses et des évaluations périodiques de nos applications et de nos infrastructures à la recherche de failles de sécurité. En outre, nous procédons à des révisions du code sécurisées et à des analyses des failles de sécurité tout au long du processus de développement et avant la mise en production, afin de détecter de manière proactive les failles de sécurité ou les risques liés au codage.

Détecter

Protection contre les logiciels malveillants

Nous avons mis en place de nombreux contrôles de détection, de prévention et de récupération, combinés à un programme de sensibilisation approprié, afin de protéger notre environnement contre les logiciels malveillants et les virus.

Nous utilisons un modèle de protection antivirus et EDR (détection et réponse au niveau des points de terminaison) à plusieurs niveaux, géré de manière centralisée. Il comprend trois niveaux de protection des passerelles de trois fournisseurs leaders sur le marché. Nous disposons également d'un ensemble de solutions définies et standardisées, installées sur tous les appareils concernés. Ces appareils doivent rester opérationnels et conformes aux paramètres de configuration fournis par le serveur et le processus de gestion des règles, selon les besoins du système d'exploitation. En outre, notre programme de protection contre les logiciels malveillants exige que tous les messages entrants et sortants soient analysés pour détecter les courriers électroniques indésirables, les virus, les stratégies DLP, la protection des pièces jointes, le phishing et les e-mails groupés.

Gestion des changements

Nous avons mis en œuvre un processus de gestion des changements basé sur les pratiques d'excellence du secteur afin de garantir que les ressources des lignes de production sont stables, contrôlées et protégées.

Ce processus garantit que les changements apportés aux ressources informatiques sont gérés de manière contrôlée et perturbent le moins possible l'activité. La gestion des changements fournit les exigences, les lignes directrices et les outils nécessaires pour régir ces changements, afin de s'assurer qu'ils sont soumis aux révisions et approbations appropriées, et qu'ils sont communiqués efficacement aux utilisateurs.

Voici quelques-uns des avantages de ce processus :

- Minimiser le risque opérationnel des changements nécessaires
- Optimiser l'efficacité des changements mis en œuvre
- Faciliter la hiérarchisation et la programmation centralisées de tous les changements au sein de l'environnement
- Simplifier les changements à venir grâce à une documentation claire et à des processus bien définis
- Fournir des niveaux de service cohérents et prévisibles pour tous les types de changements apportés à l'environnement
- Augmenter la capacité à traiter des volumes de changements importants
- Prévenir les conflits liés aux changements grâce à une planification centrale

Journalisation et alertes

Nous avons mis en place et maintenons un programme de gestion de la journalisation et des alertes qui respecte les normes industrielles, ainsi que les exigences réglementaires et de conformité en matière de journalisation des événements et de suivi des activités et des accès, autorisés ou non, aux systèmes, aux applications et aux données.

Ce programme assure l'enregistrement, la notification, le suivi et la gestion des événements de sécurité sur les systèmes, les applications, les plateformes et les périphériques réseau, en fonction de leur classification et de leur importance. Dans ce cadre, nous avons mis en place des contrôles visant à normaliser les journaux, à les conserver et à les protéger contre toute modification non autorisée. En outre, le format normalisé des informations saisies dans les journaux facilite la gestion des événements et leur identification par type, lieu, sujet, utilisateur, date et heure. Il permet même de savoir quelles données ont été consultées.

Enfin, nous utilisons des méthodes de surveillance en temps réel qui génèrent des alertes en cas d'activité suspecte ou de défaillance du journal d'audit, et déclenchent même une mesure corrective automatisée en cas d'événements bien connus.

Gestion des failles de sécurité

Afin d'atteindre les objectifs métier de l'entreprise et d'assurer une protection efficace de notre environnement et de nos opérations, nous avons mis en place une stratégie globale de gestion des correctifs de sécurité et des failles de sécurité. De nombreux contrôles ont été mis en place afin que notre environnement soit soigneusement géré et efficacement protégé contre les menaces internes et externes. Nous protégeons l'intégrité, la disponibilité et la confidentialité des données, des applications, des infrastructures et des données des clients, conformément aux normes du secteur.

Dans le cadre de notre stratégie de gestion des failles de sécurité, des informations sur les cybermenaces sont compilées à partir de ressources fiables et des alliances sont conclues avec des fournisseurs clés. Nos actifs et nos systèmes sont analysés à la recherche de failles de sécurité. Des correctifs et des mesures correctives sont exécutés en fonction de nos règles, de nos priorités et de l'impact potentiel en matière de risque.

Réagir

Continuité d'activité

Face à l'évolution rapide de l'activité mondiale de Dell Technologies, une approche flexible de la résilience opérationnelle est nécessaire. Elle permet de faire face aux risques avec des interruptions de service minimales et de fournir une infrastructure adaptable pour favoriser la croissance tout en protégeant les intérêts de nos clients, de nos collaborateurs, de nos partenaires commerciaux et de nos parties prenantes. Nous avons recours à un programme mondial de continuité d'activité, qui définit le cadre de nos normes en matière de résilience opérationnelle et aide les divisions de Dell Technologies à planifier et à atténuer les risques, afin de nous aider à répondre aux besoins de nos clients dans un monde en constante évolution.

Le programme de résilience de l'entreprise est basé sur les risques et aligné sur des normes sectorielles internationales reconnues, dont la norme ISO 22301. Il charge les divisions de spécifier des procédures alternatives et de récupération en cas de perte de dépendances fonctionnelles clés, et ce d'une manière qui permet à la société de continuer à assurer les prestations de service sans affecter les niveaux de service, la perte de données maximale admissible (PDMA) ni les objectifs de temps de reprise (RTO) convenus avec les clients. Une analyse des résultats pour l'entreprise (BIA) est utilisée pour définir les fonctions les plus stratégiques.

Pratiques de sécurité

Fournie par le Global Business Continuity Office (GBCO), l'orientation générale du programme de Dell est dirigée par du personnel disposant d'une expertise et de certifications en matière de pratiques de continuité d'activité. Le GBCO fournit des conseils à la société sur la façon d'éviter toute interruption d'activité, de s'y préparer et, le cas échéant, de s'en remettre, avec un programme de continuité d'activité de pointe digne d'un fournisseur de niveau 1. Le programme demande aux divisions de spécifier des procédures alternatives et de récupération pour la perte de dépendances fonctionnelles clés, et ce d'une manière qui permet à la société de continuer à assurer les prestations de service sans affecter les niveaux de service, la perte de données maximale admissible (PDMA) ni les objectifs de temps de reprise (RTO) convenus avec les clients. Une analyse des résultats pour l'entreprise est utilisée pour définir les fonctions les plus stratégiques.

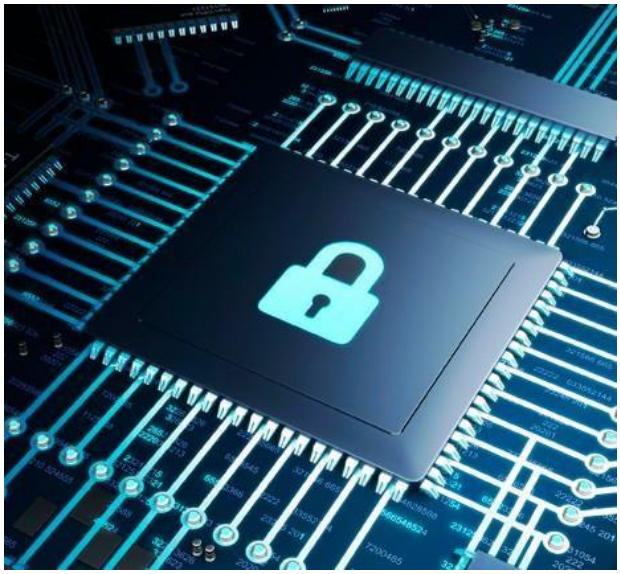
Le processus de planification de la continuité d'activité de Dell comprend une politique d'entreprise qui témoigne d'un engagement en faveur d'une approche globale, à l'échelle de l'entreprise et soutenue par les cadres dirigeants. Les plans de continuité d'activité traitent de la planification de scénarios stratégiques pour inclure la continuité et la récupération en cas de perte de :

- Capital humain et expertise dans le domaine concerné
- Infrastructure essentielle
- Locaux
- Ressources incluant les documents essentiels, la propriété intellectuelle, les données stratégiques
- Applications et infrastructures IT
- Dépendances internes et externes stratégiques
- Services tiers et gérés par des fournisseurs

Dell Technologies demande à toutes les fonctions stratégiques de l'entreprise d'actualiser et de tester chaque année leur plan de continuité d'activité.

Communication

Un plan de communication a été établi afin de garantir que les décideurs clés et les experts appropriés puissent collaborer en cas de menace d'interruption de l'activité. Ce plan prévoit de contacter les clients lorsque la société est menacée d'une interruption d'activité qui pourrait les affecter.




Évaluation des risques

Une évaluation des risques est réalisée chaque année afin de déterminer les événements d'origine naturelle ou humaine les plus susceptibles d'avoir un impact sur les opérations métier, et de s'y préparer.

Fournisseurs/tiers

La politique de Dell Technologies exige que les fournisseurs respectent les normes de résilience de l'entreprise. Pour cela, elle évalue leur capacité, en contrôlant leur conformité à intervalles réguliers, en établissant des sources d'approvisionnement alternatives et en disposant d'un plan pour traiter les articles contrefaits, volés ou illégaux.

Conformité aux normes et programmes connexes

Dell Technologies a mis en place des procédures et des politiques nécessaires au maintien de la conformité avec les lois et réglementations applicables aux produits et aux opérations, par exemple, en matière de sécurité sur le lieu de travail, de sécurité des produits, de protection de l'environnement, de conditions de travail, de codes de construction et de conformité en matière d'importation et d'exportation. En outre, les principaux sites et/ou processus métier sont certifiés selon des normes volontaires pertinentes, notamment ISO 9001, ISO 14001, OHSAS 18001, ISO 20000, etc. Les procédures et processus de Dell sont adaptés en fonction des besoins pour refléter les changements dans les opérations internes et les facteurs externes (par exemple : le changement climatique, la croissance démographique et l'accès à l'énergie et à l'eau).

Sécurité

Des contrôles et des procédures de sécurité physique ont été mis en place pour surveiller, prévenir et détecter les menaces physiques pesant sur les ressources stratégiques qui soutiennent la prestation de services Dell Technologies, mais aussi pour protéger ces ressources des menaces en question. Ces procédures sont proportionnelles aux risques évalués et à la valeur des ressources, et leur efficacité fait l'objet d'un contrôle régulier. Des contrôles pertinents de la sécurité des données, y compris le contrôle d'accès, le chiffrement et la classification des informations, ont été mis en place pour protéger à la fois les données de Dell Technologies et celles des clients. Un plan existe également pour assurer la sécurité de nos collaborateurs et pour atténuer l'impact d'éventuelles interruptions de travail dues à des réductions imprévues de la main-d'œuvre.

Amélioration continue

Dell Technologies demande à la direction de vérifier et d'approuver les stratégies de continuité et de récupération au moins une fois par an. Les entités Dell Technologies sont tenues par la politique de la société d'analyser les processus opérationnels pour détecter les risques et les points de défaillance uniques et de mettre en œuvre des stratégies pour combler les lacunes inacceptables.

Si vous avez d'autres questions sur le programme de continuité d'activité de Dell Technologies, veuillez contacter votre représentant de compte Dell Technologies.

Gestion des incidents

L'objectif principal du programme de réponse aux incidents de cybersécurité est d'atténuer et de contenir les risques associés aux incidents de sécurité informatique.

Il est de la plus haute importance pour la société de protéger notre réputation et nos relations. Un programme efficace de cybersécurité de bout en bout joue un rôle clé dans la mise en place de cette protection, en contribuant à sauvegarder les informations et les ressources de la société. Notre plan de réponse aux incidents de cybersécurité est une composante essentielle d'un tel programme et vise à décrire la façon dont nous identifions les incidents de cybersécurité, les évaluons, y répondons et les corrigeons. Le plan définit également les rôles et responsabilités des différentes parties prenantes qui participent à notre réponse à un incident de cybersécurité.

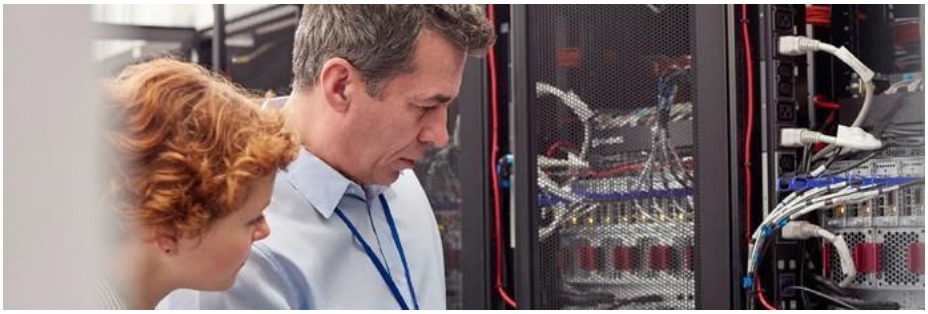
Un plan de réponse de l'entreprise aux incidents de cybersécurité est en place. Il décrit l'objectif, le périmètre, l'identification, l'évaluation, la réponse et les mesures correctives liés aux incidents de sécurité, y compris les notifications aux organismes de réglementation, aux contrôleurs et/ou aux personnes concernées, selon les besoins.

Restaurer

Reprise après sinistre

Nous reconnaissons l'importance d'une approche cohérente, évolutive, flexible et coordonnée de la résilience dans l'environnement mondial de plus en plus incertain et difficile qui est le nôtre.

Si un incident affecte gravement notre capacité à mener nos activités normalement, notre programme de reprise après sinistre prévoit la restauration en temps utile des processus, applications, données et systèmes stratégiques qui soutiennent nos opérations essentielles.



Le programme de reprise après sinistre établit des normes, des processus et des contrôles pour une récupération rapide des données, applications, systèmes et infrastructures stratégiques utilisés pour gérer et soutenir les fonctions clés de notre entreprise. Ces exigences garantissent également la continuité de ces ressources.

Notre programme et notre méthodologie garantissent que les applications et les infrastructures auxquelles ont recours nos clients possèdent des fonctionnalités de résilience alignées sur les contrats de niveau de service, les RTO et les PDMA. Un site de récupération désigné, ainsi que la disponibilité du personnel chargé de la reprise après sinistre, ont été préétablis afin d'être rapidement mobilisés en cas d'interruption de l'activité. En outre, les plans de reprise après sinistre sont révisés et testés au moins une fois par an, lorsque de nouvelles applications sont mises en ligne ou que des changements interviennent dans l'environnement informatique. Les méthodes de test sont proportionnelles au degré d'importance de l'application/du système.