Guide de la Cybersécurité

Orientations en matière de cybersécurité à l'intention des décideurs

Version : Août 2023

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

Table des matières

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

1 Introduction

La cybersécurité est un domaine qui évolue rapidement. Il ne suffit plus de déployer un pare-feu et de crypter le lien entre les systèmes. Il faut au contraire adopter une approche de défense en profondeur, en mettant en place des mesures à la fois préventives et réactives qui permettent de détecter et de réagir en cas d'atteinte à la sécurité informatique.

Chaque jour, de nouveaux outils et acteurs de la menace apparaissent pour obtenir un accès non autorisé aux données, pour perturber, désactiver et refuser des services et des systèmes. Auparavant, ces outils n'étaient accessibles qu'aux services de renseignement, mais de plus en plus, ils sont à la disposition de n'importe qui, y compris des individus motivés, des hacktivistes ou des cybercriminels qui cherchent à se faire connaître, à gagner de l'argent ou simplement à faire des ravages.

Dans le monde numérique moderne, le savoir est un facteur de différenciation important et la capacité d'une partie non autorisée à accéder ou à refuser aux utilisateurs valides l'accès aux systèmes et données critiques, ou même à refuser l'accès aux propriétaires de ces systèmes et données critiques, devrait être une préoccupation majeure pour toute organisation.

De fréquents articles dans la presse ou des notifications d'incidents ou de violations de données reçues des fournisseurs prouvent que cette menace est réelle et qu'il ne s'agit pas seulement d'un risque avec une certaine probabilité.

À chaque niveau de la chaîne d'approvisionnement, un acteur de la cybermenace a la possibilité d'infiltrer et d'affecter une organisation. Cette menace peut provenir d'un employé mécontent, d'un partenaire ou d'un fournisseur de logiciels, ou même de leurs composants et bibliothèques qui ont été compromis. Il est très difficile de défendre un système contre toutes les attaques potentielles, c'est pourquoi il peut être utile de hiérarchiser les mesures de sécurité en se basant sur l'expérience réelle d'autres victimes.

Le présent document d'orientation a été élaboré à l'intention des décideurs d'une organisation, en particulier des petites et moyennes entreprises qui ne connaissent pas nécessairement le domaine de la cybersécurité ou dont les budgets consacrés à la cybersécurité sont limités. Ce guide peut aider ces entreprises à mieux comprendre certains des risques les plus importants auxquels elles peuvent être confrontées, ainsi qu'à obtenir des conseils et des ressources complémentaires. Ces conseils et ces ressources peuvent permettre d'obtenir des résultats rapides et donner un aperçu des domaines d'intérêt.

Lorsqu'une organisation a externalisé ses opérations informatiques, ce guide peut également être utilisé pour définir les exigences de cybersécurité appropriées dans le cadre d'un accord de niveau de service.

Ce document a été structuré en fonction des principaux risques organisationnels, des conseils et des ressources supplémentaires pour chacun des domaines de la défense en profondeur en matière de cybersécurité ("Identifier, Protéger, Détecter, Répondre et Récupérer").

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

2 Piloter les risques pour une organisation et les décideurs

2.1 Contexte

Comme nous l'avons expliqué dans le chapitre précédent, les cyber-attaques représentent une menace importante et croissante pour les entreprises opérant dans des secteurs clés spécifiques, y compris la technologie aérospatiale et de défense. Ces menaces peuvent également émaner de la chaîne d'approvisionnement, car les fournisseurs ont accès aux informations et aux systèmes de leurs clients, mais peuvent ne pas disposer de l'infrastructure de sécurité nécessaire pour protéger correctement ces actifs informationnels et s'exposer ainsi que leurs clients aux principaux risques en matière de sécurité.

2.2 Principaux risques

2.2.1 Absence de protection des données des clients sur le lieu de travail des fournisseurs

Il s'agit notamment d'une divulgation ou d'une fuite non autorisée due à des mesures inadéquates de contrôle de l'accès aux systèmes, pouvant conduire à une violation passive des accords de non-divulgation convenus.

2.2.2 Exposition des systèmes d'information des clients

Cela signifie que les attaquants peuvent utiliser une sécurité de réseau inadéquate dans les systèmes des fournisseurs et utiliser leur connectivité de données avec les clients pour des attaques ou de l'espionnage.

2.2.3 Conformité juridique/réglementaire

Cela amplifie les deux risques mentionnés ci-dessus si les données réglementées des clients sont affectées, comme les contrats, la propriété intellectuelle, le contrôle des exportations, les données personnelles (RGPD), les données classifiées de défense/militaire, etc.

2.2.4 Résilience des systèmes d'information des fournisseurs

En raison d'une panne informatique majeure due à un événement physique (incendie...) ou cybernétique (ransomware...) et d'un manque de continuité des activités et de gestion de crise appropriées, l'entreprise est incapable de fournir ses produits ou services à ses clients, ce qui a un impact sur ses résultats et sur ceux de ses clients.

2.2.5 Exposition de l'environnement industriel

Une cyberattaque met en péril l'intégrité des produits de l'entreprise ou de ses clients, par exemple par la corruption ou le vol de données de conception, le sabotage électronique de machines de production ou l'utilisation de pièces électroniques et physiques contrefaites.

3 Domaines, conseils et ressources en matière de défense approfondie de la cybersécurité

Cette section est divisée en cinq domaines de défense en profondeur de la cybersécurité afin d'aider les lecteurs à comprendre le contexte et à regrouper les sujets similaires.
Chaque domaine est assorti de conseils et d'astuces, ainsi que de ressources et de lectures complémentaires que les personnes intéressées peuvent consulter.

Les conseils et les ressources se recoupent en partie, il est donc conseillé de consulter d'autres domaines. Par exemple, certains sujets, normes de cybersécurité et méthodologies couvrent souvent plusieurs domaines (comme la série ISO 27000 ou le NIST CSF & 800-53B). Le présent guide contient une série de conseils et de

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

suggestions. Il convient toutefois de noter qu'il ne s'agit que d'un petit nombre de mesures possibles dans un environnement dynamique et changeant que toute entreprise devrait prendre en considération.

Voici les cinq cyber-domaines:

- **Identifier -** En se concentrant principalement sur les aspects organisationnels et de gouvernance, toute entreprise doit avoir une connaissance des systèmes qu'elle contrôle ou avec lesquels elle est en interface. Une entreprise n'est pas totalement isolée, c'est pourquoi le contexte dans lequel elle opère, sous quels régimes juridiques et réglementaires, et avec ses fournisseurs et partenaires, fait partie du domaine "Identifier". Ce domaine comprend une compréhension de base des risques et des contrôles de sécurité.
- **Protéger -** Il est essentiel de se concentrer principalement sur les mesures techniques visant à garantir qu'un système est protégé à un niveau minimum, qu'il s'agisse d'un portail de marketing client ou d'une interface en ligne interentreprises. L'homme reste le "maillon faible" le plus courant de tout système, et il convient de comprendre l'élément humain lors de la mise en place de mesures de protection visant à protéger un système contre les attaques, qu'elles soient externes ou internes.
- **Détecter** - La question n'est pas de savoir "si" mais "quand" quelque chose va se produire. Lorsque cela se produit, une organisation doit être en mesure de le détecter et de réagir le plus rapidement possible afin de réduire les dommages potentiels. Aujourd'hui, il est courant d'adopter une posture de sécurité qui suppose une brèche. La surface d'attaque est tellement grande que même un clic erroné sur un site web apparemment inoffensif peut compromettre l'ensemble du système. C'est pourquoi les systèmes et les contrôles permettant de détecter une éventuelle violation constituent une mesure essentielle dans les systèmes informatiques modernes.
- **Réagir** - Une fois qu'une compromission s'est produite, il devient très important de pouvoir isoler un problème, de minimiser l'impact sur les systèmes et les services et de communiquer avec les partenaires de manière efficace et contrôlée. Peut-être votre administrateur expert détecte-t-il une attaque en cours qui prend pied dans les systèmes et les serveurs de vos utilisateurs ; qui appelez-vous pour obtenir de l'aide ? Devriez-vous désactiver immédiatement tous les services des utilisateurs et toutes les connexions au réseau ? Pouvez-vous désactiver le réseau si vous travaillez dans une instance en nuage sans bloquer votre propre accès ? Il est important de se préparer à l'avance à de tels événements.
- **Récupération** - Même si la violation a été contenue et que l'impact sur l'entreprise a été minimisé, il est nécessaire d'avoir les processus et les systèmes en place pour ramener le système et les services à un état pleinement opérationnel. Il est important de comprendre la tolérance de l'entreprise à l'échec pendant une violation et après qu'elle a été contenue. Imaginez que toutes les données de l'entreprise soient corrompues, y compris toutes les sauvegardes en ligne, en quelques minutes. Comment l'entreprise peut-elle survivre à un tel scénario ? Quel est le niveau de tolérance et d'interruption qu'une organisation est prête à accepter avant que le système ne soit récupéré à partir de sauvegardes hors ligne (si les sauvegardes fonctionnent encore) ? Votre entreprise pourrait-elle survivre si vous deviez réinstaller tous les serveurs et la configuration du réseau ? Dans l'affirmative, combien de temps s'écoulerait-il avant que vos clients n'aillent voir ailleurs ?

Pour l'industrie aérospatiale et sa chaîne d'approvisionnement, les mesures de sécurité suivantes sont recommandées comme base de référence :

3.1 Identifier

Les conseils de sécurité suivants sont recommandés pour aider les décideurs d'une organisation :

- Disposer d'une politique de sécurité officiellement signée par la direction et mise à la disposition de tous les employés.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

- Nommer un responsable de la sécurité (qui peut être à temps partiel pour les PME) avec les ressources appropriées (budgets, personnel, compétences et maintien des compétences).
- Tenir un inventaire des données, des équipements et des logiciels critiques sur votre réseau et ne permettre l'utilisation que des actifs autorisés.
- Établir et appliquer un système de classification et de protection des informations basé sur les risques.

  Nous vous recommandons d'éviter les termes "RESTREINT, CONFIDENTIEL ou SECRET" dans votre organisation lorsque vous définissez vos niveaux de classification pour les données commercialement sensibles, car ces termes sont généralement utilisés pour les informations de type sécurité nationale/gouvernemental. Envisagez des termes tels que "commercial confidentiel, interne, privé, données personnelles sensibles, distribution limitée, accessible au public" et envisagez d'appliquer systématiquement la convention dans vos documents et systèmes d'information.
- Connaître ses fournisseurs essentiels et leur imposer des exigences de sécurité appropriées.
  Comprendre la nature de la responsabilité partagée entre les fournisseurs et vous-même et quels modèles (le cas échéant) sont appropriés pour vos activités et services. Déterminer si des mesures supplémentaires sont nécessaires pour réduire les risques et aider l'entreprise à décider des modèles et des fournisseurs à utiliser (internalisation, externalisation, exigences supplémentaires, pénalités ou surveillance), y compris la maturité des fournisseurs en matière de sécurité, leur localisation et leurs modèles de service.

- Vérifier les réglementations et les lois pertinentes telles que le contrôle des exportations, la protection des données personnelles.
- Prendre des mesures pour protéger le savoir-faire, les données sensibles (plans, brevets) et la propriété intellectuelle. Ces mesures s'appliquent à l'organisation et aux actifs des partenaires/clients qui ne sont pas des brevets ou des éléments soumis au contrôle des exportations.

3.2 Protéger

Les conseils de sécurité suivants sont recommandés pour aider les décideurs d'une organisation :

- S'assurer de l'identité et de l'intégrité des personnes lors du recrutement.

- Réduire les risques d'erreur humaine, de vol, de fraude ou d'utilisation abusive des installations.

Veiller à ce que les utilisateurs soient conscients des menaces et des problèmes liés à la sécurité de l'information, qu'ils soient équipés et formés pour soutenir la politique de sécurité de l'entreprise dans le cadre de leur travail normal, qu'ils minimisent les dommages causés par les incidents et les dysfonctionnements en matière de sécurité et qu'ils tirent les leçons de ces incidents.

- Empêcher les accès non autorisés, les dommages et les interférences dans les locaux et les informations de l'entreprise.

- Empêcher la compromission ou le vol d'informations et de biens matériels.

- Mettre en place un système de sécurité incendie qui prenne en compte les risques de l'entreprise.

- Veiller à ce que tous les utilisateurs du réseau et des appareils informatiques disposent d'un identifiant individuel unique et utilisent un mot de passe fort.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

- Contrôler l'accès aux systèmes et aux informations, en particulier pour les clients, en fonction des fonctions des utilisateurs.

- Appliquer strictement la gestion de bout en bout du cycle de vie de tous les utilisateurs et administrateurs (y compris la suppression/déréférencement de l'accès).

- Utiliser une authentification forte (par exemple, l'authentification multifactorielle) pour se connecter aux clients ou à distance depuis l'extérieur du réseau.

- Crypter tous les appareils mobiles et les connexions réseau qui transportent des données confidentielles ou liées aux clients.

- Veiller à ce que les modèles/signatures des mécanismes anti-intrusion et antivirus soient régulièrement mis à jour sur tous les appareils, y compris les appareils mobiles.

- Veiller à ce que des procédures formelles de contrôle des changements soient mises en place au sein de l'organisation informatique.

- Effectuer des sauvegardes régulières des données et des logiciels et les stocker physiquement et en toute sécurité à l'écart des systèmes de production.

- Veiller à ce que les équipements informatiques soient régulièrement corrigés après avoir été testés.

- Déployer des correctifs de sécurité à intervalles réguliers, surveiller les vulnérabilités critiques et appliquer des mesures d'atténuation.

- Veiller à ce que les systèmes et les processus fassent régulièrement l'objet d'un audit portant sur les aspects efficaces de la sécurité.

3.3 Détecter

Les conseils de sécurité suivants sont recommandés pour aider les décideurs d'une organisation :

- Disposer des outils et du personnel nécessaires à la prévention des incidents de sécurité, à la détection rapide et efficace et à la réaction.
- Contrôler la protection de l'infrastructure du réseau (Active Directory, pare-feu, proxies, détection des intrusions, systèmes antivirus, etc.)
- Contrôler et auditer les actifs critiques.

3.4 Réagir

Les conseils de sécurité suivants sont recommandés pour aider les décideurs d'une organisation :

- Mettre en place et tester des procédures efficaces pour identifier, analyser et réagir rapidement aux vulnérabilités des systèmes et aux incidents de sécurité.
- Veiller à ce qu'une organisation de gestion de crise et des procédures définies pour gérer les événements majeurs soient en place.
- Assurer une collaboration permanente avec les clients en cas d'incident de sécurité affectant leurs informations ou leurs systèmes et partager les informations sur les menaces.
- Disposer de "contacts critiques" et envisager des accords "de principe" ou de "coopération" à l'avance. Ces accords permettent d'accéder rapidement à des experts internes et externes en cas de violation.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

3.5 Récupérer

Les conseils de sécurité suivants sont recommandés pour aider les décideurs d'une organisation :

- Veiller à ce que des procédures et des processus de gestion de la continuité des activités soient en place afin de garantir un retour rapide à un état de fonctionnement normal.
- Veiller à ce qu'une planification et des procédures adéquates de reprise après sinistre soient en place pour préserver la confidentialité, l'intégrité et la disponibilité des systèmes et des informations en cas de sinistre informatique majeur.

  Prendre en considération des scénarios tels qu'une "cyberpandémie" ou une attaque par ransomware à l'échelle du système.
- Examiner l'incident a posteriori, analyser les enseignements tirés et prendre les mesures appropriées pour éviter qu'il ne se reproduise.

- Tester et vérifier périodiquement les processus et l'état de préparation pour faire face à un incident potentiel.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

