LA PROTECTION DES DONNÉES

dans les petites et moyennes entreprises

- L’environnement actuel des menaces
- Les mesures de protection pour votre petite ou moyenne entreprise
- Limiter les répercussions d’une violation de données

CYBERSECURITY
EXPERTS ON YOUR SIDE

#1 LE PARTENAIRE EUROPÉEN DE VOTRE SÉCURITÉ

Depuis plus de 30 ans, ESET® développe des services et des logiciels de cybersécurité de pointe qui apportent aux entreprises et aux particuliers du monde entier une protection immédiate et complète contre les menaces mouvantes de cybersécurité.

ESET est une société non cotée de droit privé. Libres de tout prêt ou dette, nous consacrons tous nos efforts à la protection optimale de nos clients.

ESET EN CHIFFRES

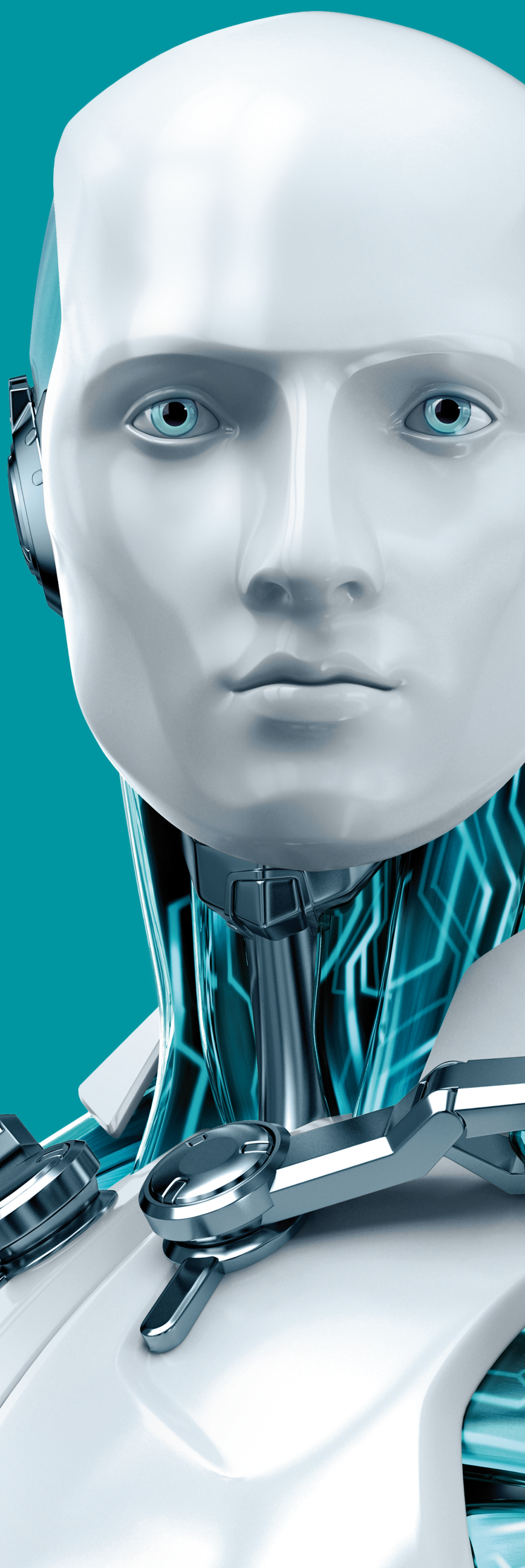
+110 millions
d'utilisateurs dans le monde

+400 milles
clients professionnels

+200
pays et territoires

13
centres de R&D dans le monde

www.eset.com/fr



SOMMAIRE

Introduction 03
À propos de ce guide. 04
Postulas 04
Icônes dans ce guide 04
Pour aller plus loin 04

Appréhender l'impératif de protection des données 05
Comprendre les répercussions commerciales d'une violation 05
Explorer l'environnement actuel des menaces 07
Examen de violations et de fuites de données récentes 09
Suivre l'évolution du cadre légal et réglementaire 10

Protection des données : vos premiers pas 14
Comprendre les fondamentaux de la protection des données. . . . 14
Prestataires de sous-traitance et de services de sécurité managés . . 20

Évaluer les risques à la sécurité des données 22
Comprendre le processus d'évaluation des risques 22
Étape 1 Identifier les opérations de traitement des données 23
Étape 2 Déterminer les répercussions commerciales potentielles . . 24
Étape 3 Identifier les éventuelles menaces et évaluer leur probabilité 25
Étape 4 Évaluer le risque 25

Appréhender la technologie de protection des données . . . 27
Protéger les données où qu'elles se trouvent 27
Sécuriser le réseau 31
Comprendre le besoin d'orchestration. 32

Explorer les contrôles d'organisation et de processus 35
Établir des contrôles organisationnels 35
Contrôles des processus 39

10 clés pour une protection des données efficace 41

Glossaire 46

INTRODUCTION

« Votre entreprise est trop petite pour être une cible. » Aucun pirate ne prononcera jamais cette phrase ! Prédateurs opportunistes, les cybercriminels ne visent peut-être pas précisément votre petite ou moyenne entreprise, mais à partir du moment où vous êtes connecté à internet, ils savent vous trouver. Et si le réseau, les serveurs, les applications, les données, les appareils mobiles, les ordinateurs portables et de bureau ne sont pas correctement protégés, on peut y pénétrer. Si toutes les violations n'exposent pas au pilori télévisuel – comme ce fut le cas pour Bupa, CEX, Clarkson, Equifax, Target, Uber ou Yahoo! – chacune frappe durement sa cible, parfois suffisamment pour entraîner la faillite. La sécurité s'impose progressivement comme un avantage concurrentiel. La présente publication constitue votre point de départ pour une meilleure hygiène numérique de l'entreprise.

Les violations de données et les cyberattaques existent depuis longtemps, mais les techniques et tactiques des cybercriminels actuels ont évolué. Elles sont particulièrement bien adaptées au milieu riche en cibles qu'est celui des petites et moyennes entreprises. En effet, au niveau mondial, celles-ci constituent plus de 95 % du tissu économique, représentent plus de la moitié des employés et contribuent à plus de 50 % au produit intérieur brut de l'économie. Parmi les modes d'attaques les plus récents, citons :

- Les techniques sophistiquées de logiciels malveillants (polymorphisme ou métamorphisme), rançongiciel (ransomware) et chevaux de Troie d'accès distant ou RAT (remote access Trojans).
- Les attaques d'annuaire ou DHA, les courriers indésirables ciblés et les campagnes d'emailing d'hameçonnage voire de harponnage.
- Un réseau de machines zombies automatisées (botnets).
- Le détournement de DNS (Domain Name System) et l'empoisonnement de cache DNS.
- Le saut de port en port (port hopping) et la dissimulation SSL (SSL hiding).
- Les attaques de déni de service distribué (DDoS).

Les menaces à la sécurité sont un problème plus grave et plus fréquent que jamais et les PME, avec leurs services IT aux ressources budgétaires et humaines limitées, sont souvent des cibles faciles pour les cybercriminels. Dans le même temps, puisque les PME sont par définition plus petites que les grandes entreprises, avec moins d'appareils connectés, elles s'avèrent plus flexibles et agiles au moment de définir et de mettre en œuvre une stratégie de protection des données. Si elles prennent les bonnes mesures, ces entreprises peuvent se rendre nettement moins attractives aux yeux des attaquants.

Cet ouvrage recense les informations, les outils et les processus des technologies de la sécurité qui permettent de renforcer les capacités de protection des données et des ressources informatiques et de réduire au minimum les répercussions d'une violation de données.

À propos de ce guide

La protection des données dans les petites et moyennes entreprises contient six chapitres très brefs :

1. Cyberattaques et tendances, cadre réglementaire et répercussions commerciales d'une violation
2. Évaluer les différentes technologies de protection des données, les options de déploiement et les modèles de service
3. Évaluer des risques : identifier les actifs, analyser les menaces et évaluer les vulnérabilités
4. Les différentes technologies de protection des données : chiffrement, protection des terminaux, pare-feu, etc.
5. Contrôles (organisation, processus) indispensables à la protection efficace des données
6. La protection efficace des données dans l'entreprise petite ou moyenne en 10 points

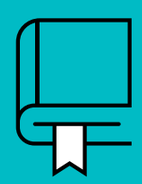
À la fin de ce guide, un glossaire permet de décoder rapidement un terme ou un acronyme peu familier.

Postulats

Ce guide s'adresse aux professionnels IT des petites et moyennes entreprises, que vous soyez manager d'une équipe IT restreinte polyvalente ou l'équipe informatique à vous seul ! Avec votre équipe, vous vous occupez de tout : du remplacement des cartouches d'encre et de la configuration des terminaux des utilisateurs à la gestion du réseau de l'entreprise et la prise en charge de la sécurité. Votre rôle exige connaissances et expérience informatiques d'une grande variété, mais qui mériteraient peut-être un approfondissement dans certains sujets, notamment la protection et la sécurité des données.

Icônes dans ce guide

Tout au long du guide, des icônes servent à repérer les informations importantes.



À RETENIR

Cette icône signale les informations à retenir pour un usage ultérieur.

CONSEIL

Cette icône signale des capsules d'information et des conseils.

ATTENTION

Il s'agit de conseils pratiques pour éviter des écueils potentiellement coûteux ou désagréables.

Pour aller plus loin

Ce livre électronique traite des informations essentielles. Pour en savoir plus, rendez-vous sur www.eset.com/fr

Dans ce chapitre

- Chiffrer le véritable coût d'une violation de données
- Appréhender l'environnement actuel des menaces
- Tirer les leçons des violations passées
- Comprendre les obligations de conformité réglementaire

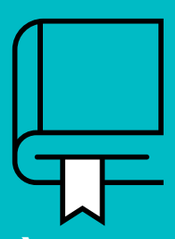
Chapitre 1

APPRÉHENDER L'IMPÉRATIF DE PROTECTION DES DONNÉES

Dans ce chapitre, vous allez découvrir les répercussions possibles d'une violation de données sur votre entreprise, l'évolution de l'environnement actuel des menaces, les conséquences de violations de données récentes sur d'autres PME, et les implications pour votre entreprise de l'évolution des obligations légales et réglementaires.

Comprendre les répercussions commerciales d'une violation

Les PME représentent 99 % de toutes les entreprises dans l'UE et plus de 95 % dans le monde. Il n'y a rien de surprenant dans ce cas à ce qu'elles soient victimes de plus de 70 % des violations de sécurité, selon le cabinet International Data Corporation (IDC). Pourtant, de nombreuses entreprises pensent que leur petite taille et leurs actifs limités les mettent à l'abri des cyberattaques. Ce n'est malheureusement pas le cas.



À RETENIR

Dans son Rapport d'enquête 2017 sur les compromissions de données (DBIR), Verizon constate que les attaques, plus précisément les tentatives d'intrusion dans les points de vente, visent désormais les restaurants et les petites entreprises. En outre, les trois quarts des victimes des six premiers actes de malveillance, à savoir le vol d'informations d'identification, les portes dérobées (backdoors), les logiciels espions, l'hameçonnage, l'exfiltration de données et les logiciels malveillants obéissant à un serveur de contrôle et commande (C2), sont des petites entreprises en ligne hors du commerce de détail.

Au Royaume-Uni, la compagnie d'assurances Zurich constate que, l'an dernier, plus de 875 000 PME ont subi une cyberattaque pour un coût supérieur à 13 000 $ pour plus d'un cinquième d'entre elles et à 69 000 $ pour un dixième. Par comparaison, le Ponemon Institute indique dans son étude 2017 sur le coût des violations de données un coût total moyen d'environ 3,62 millions de dollars pour les grandes entreprises.

Une étude sur le coût mondial imputable aux violations de données concluait que leur coût moyen a plus que doublé de 2014 à 2015. En parallèle, la valeur moyenne de chaque enregistrement volé ou perdu augmentait légèrement jusqu'à s'approcher de 150 €.
Il en ressort que le coût global d'une violation de données n'a pas subi de variation significative au fil des ans ; il s'agit donc de charges auxquelles les organisations doivent se préparer et qu'elles doivent intégrer dans leurs stratégies de protection des données.

Si le coût d'une violation est considérablement moindre dans une PME, ces entreprises n'ont généralement pas les ressources financières ou autres pour réagir face à une violation de données majeure et en récupérer. L'entrée en vigueur de réglementations comme le RGPD (règlement général sur la protection des données de l'UE), qui font obligation aux entreprises de toutes tailles d'analyser post-incident ce qu'il s'est précisément passé au cours d'une violation, risque d'en renchérir considérablement les répercussions pour les PME.

CONSEIL

La cyberassurance est un excellent moyen de réduire les coûts d'une cyberattaque ou d'une violation de données. Toutefois, elle ne vous protège pas contre une attaque ou une violation et elle NE REMPLACE PAS la mise en œuvre d'une stratégie de sécurité (bonnes pratiques, politiques, contrôles et technologies).

Le coût total d'une violation de la sécurité comprend :

- Les interruptions d'activité, notamment les pertes de temps et de productivité
- Les coûts directs, notamment les coûts d'information, d'assistance client, des services de surveillance du crédit, des mesures de rétention de la clientèle, de restitution et de remplacement de cartes
- La perte de clientèle (taux d'attrition), la détérioration de l'image de marque et la perte de réputation
- Les contentieux avec les clients, partenaires commerciaux et investisseurs
- Les amendes et pénalités prévues par la loi
- Les coûts de reprise et d'analyse post-incident qui peuvent représenter la plus grosse part des coûts
- La perte de patrimoine notamment immatériel

ATTENTION

Selon l'agence américaine de cybersécurité National Cyber Security Alliance, 60 % des petites entreprises feront faillite dans les six mois suivant une attaque.

Explorer l'environnement actuel des menaces

Dans un avenir proche, le nombre, l'ampleur et le coût des violations de données devraient poursuivre leur croissance. Ces attaques traduiront des tendances toujours prédominantes dans les entreprises de toutes tailles :

Les attaques automatisées à très grande échelle deviennent le mode opératoire des cybercriminels qui exploitent de puissants logiciels malveillants et botnets pour pénétrer tout réseau ou organisation vulnérable à portée, sans ciblage spécifique. Si vous êtes connecté à internet, on vous trouvera tôt ou tard. Personne n'est ciblé, mais tous peuvent être touchés.

Les ransomwares continueront de représenter un danger croissant. Dans une étude, Datto estimait qu'environ 5 % de toutes les PME dans le monde avaient été victimes d'attaques au ransomware l'année précédente. 35 % des prestataires de services managés (MSP) rapportent que les petites entreprises victimes paient la rançon, sans toutefois récupérer leurs données pour 15 % d'entre elles.

La fraude à la demande ou CaaS (crime-as-a-service) va se développer avec la sophistication accrue des outils malveillants. Les groupes criminels s'aventurent sur de nouveaux marchés. Ils standardisent et diffusent leurs services partout dans le monde : les incidents de cybersécurité persisteront davantage et causeront toujours plus de dégâts. L'entrée sur le marché est grandement facilitée par les cyberarmes comme les ransomwares à la demande et les sites malveillants (comme les forums de nulled.to) qui mettent le cybercrime à la portée de cybercriminels en herbe peu qualifiés.

Avec l'internet des objets (IoT), les risques non maîtrisés vont se multiplier. Les entreprises se ruent sur les objets connectés et, dans leur précipitation, oublient toute prudence : ces appareils, souvent intentionnellement conçus non sécurisés, ouvrent grand les portes aux attaques. Réfléchissez aux appareils mobiles en tant que supports de gros volumes de données.

L'informatique en cloud donne aux PME les moyens de concurrencer les grandes entreprises en leur ouvrant l'accès à des ressources informatiques tout aussi puissantes sans gros investissements initiaux ni assistance coûteuse. Selon le cabinet britannique de conseil et de solutions cloud BCSG, environ les deux tiers des PME utilisent déjà une moyenne de trois applications cloud à la demande (SaaS). Il s'agit typiquement des logiciels de gestion de la relation client (CRM), de collaboration en ligne, de stockage de données, de marketing en ligne, de gestion des contrats et de gestion de la chaîne logistique (SCM). Si les solutions de ce type sont par essence souvent plus sûres que leurs équivalents en interne, les entreprises doivent néanmoins s'assurer que leurs prestataires cloud, notamment sur les secteurs plus petits ou dans le cas d'applications SaaS de niche, appliquent les bonnes pratiques de sécurité, remplissent leurs obligations

légales (RGPD) et respectent des accords de niveau de service (SLA) acceptables. Quant aux PME, recourir au cloud ne les décharge pas de leur responsabilité ultime de sécurité et de confidentialité des données et de conformité réglementaire. Elles doivent assurer une gestion robuste des accès et des identités, l'authentification sécurisée aux services cloud et, en cas d'abonnement à un service d'infrastructure à la demande (IaaS), la configuration, l'exécution et la maintenance correctes des serveurs cloud.

La chaîne logistique en amont et en aval restera une cible privilégiée : l'exploitation de vulnérabilités chez des partenaires qui mutualisent des informations précieuses et sensibles est un moyen d'accéder discrètement à l'entreprise. Retenez que vous êtes, vous aussi, un rouage de la chaîne logistique de vos clients.

La loi ajoute à la complexité. Les entreprises peuvent voir leur attention et leurs investissements détournés d'autres initiatives importantes de sécurité quand leurs obligations légales exigent un surcroît de ressources, comme nous le verrons plus avant dans ce chapitre.

Pour les PME, ces tendances et leur enchevêtrement n'augurent rien de bon : elles manquent souvent des ressources en sécurité des informations et financières des grandes entreprises, ce qui en fait une cible privilégiée des cybercriminels (voir Illustration 1-1). Les cybercriminels ne sont pas seuls à semer le chaos : il faut aussi mentionner les violations internes inintentionnelles.

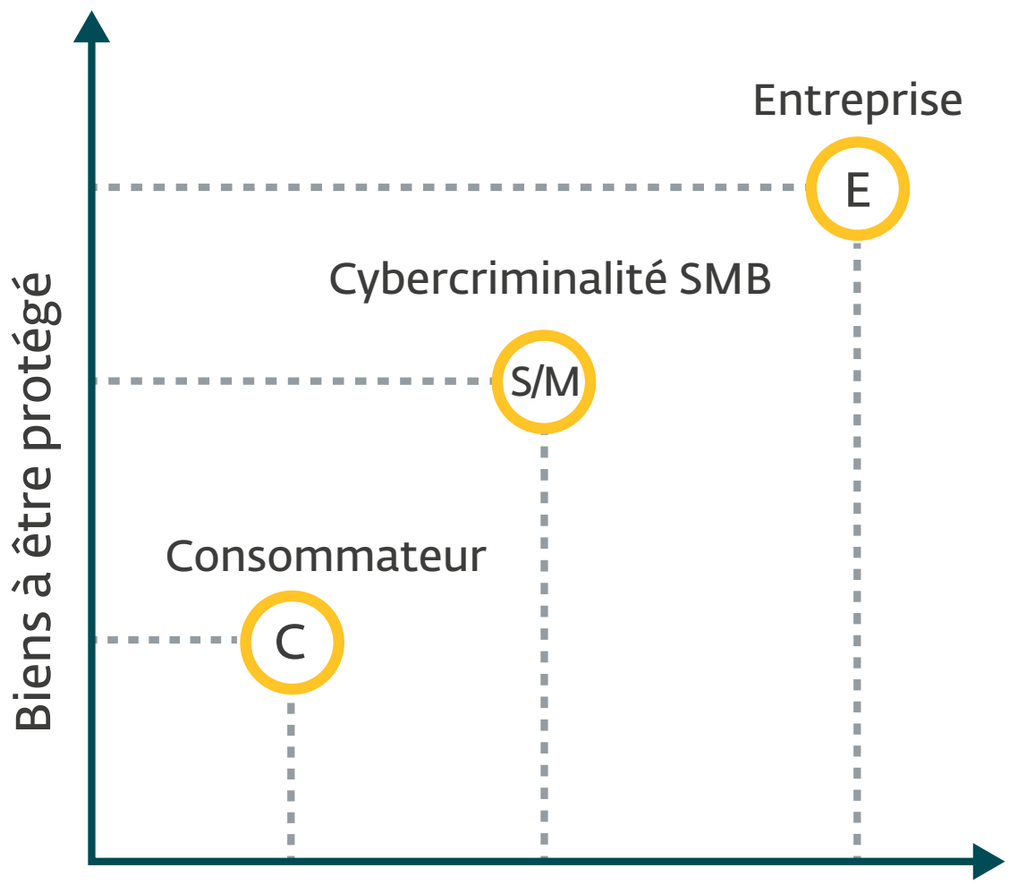


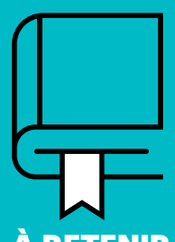
Illustration 1-1 : Les PME sont généralement des cibles plus rentables que les consommateurs et plus vulnérables que les grandes entreprises.

ATTENTION

L'Information Security Forum (ISF) note que l'intensification des violations de données et les volumes supérieurs des enregistrements touchés devraient augmenter considérablement les coûts supportés par les organisations de toutes tailles

Examen de violations et de fuites de données récentes

Si les grandes brèches de cybersécurité qui touchent de grandes entreprises et des données sensibles monopolisent l'attention des médias, les cyberattaques et les vulnérabilités des PME n'en sont pas moins fréquentes ni dommageables. De fait, si on tient compte du nombre relatif de PME aux ressources financières et sécuritaires limitées par rapport aux grandes entreprises, les répercussions d'une cyberattaque ou d'une violation de données sur les clients d'une PME et sur sa survie peuvent se révéler bien plus graves.



À RETENIR

Si les petites entreprises de moins de 50 employés et les très petites entreprises (TPE) retiennent moins l'attention de la presse à sensation, elles n'en restent pas moins vulnérables aux attaques et aux violations.

Parmi les exemples récents de violations de données et d'attaques touchant des PME, citons :

Obike

En décembre 2017 était signalé que, dès le mois de juin 2017, Obike, société singapourienne de vélos en libre-service dans plusieurs villes d'Asie-Pacifique, d'Europe et du Royaume-Uni, avait subi une violation de données dont des données clients sensibles (noms, contacts, photos de profil et localisation).

TIO Networks USA

En décembre 2017, on apprend que la société canadienne TIO Networks USA – spécialisée dans le traitement des paiements et rachetée par PayPal – a été victime d'une violation de données touchant les informations personnelles et financières d'environ 8 000 clients de la régie de service public de la commune de Tallahassee en Floride.

Cabinet médical Longs Peak Family Practice

En novembre 2017, ce cabinet médical du Colorado découvre qu'une violation de données aurait compromis les informations sensibles de ses patients (noms, dates de naissance, numéros de téléphone, adresses électroniques, numéros de sécurité sociale, numéros de permis de conduire, assurance…).

Institut britannique des aveugles (RNIB)

En novembre 2017, le Royal National Institute of Blind People (RNIB) a été victime d'une violation de données touchant les coordonnées de cartes bancaires de 817 clients de sa boutique en ligne solidaire.

Centre médical Chilton

En octobre 2017, le centre médical Chilton dans le New Jersey découvre qu'un ancien employé a volé et revendu un disque dur contenant les dossiers médicaux confidentiels de 4 600 patients.

ATTENTION

Dans son Rapport d'enquête 2017 sur les compromissions de données (DBIR), Verizon observe que dans 60 % des cas, une violation de données est un vol interne.

Centre de chirurgie plastique LBPS

En octobre 2017, le centre de chirurgie plastique et esthétique London Bridge Plastic Surgery and Aesthetic Centre (LBPS) est signalé comme victime d'une violation de données susceptible d'impliquer des photographies et des données médicales sensibles.

Centre d'assistance médicale à la procréation CCRM

En octobre 2017, un centre de PMA à Minneapolis, le Colorado Center for Reproductive Medicine (CCRM), est victime d'une attaque par ransomware susceptible d'affecter les dossiers médicaux confidentiels de près de 3 300 patients.

Services de santé Heritage Valley Health Systems

En juin 2017, Heritage Valley Health Systems, un réseau médical à la tête de deux hôpitaux et de nombreux services de soins aigus, ambulatoires et paramédicaux dans toute la Pennsylvanie occidentale, est victime d'une attaque internationale par ransomware avec des répercussions sur les soins aux patients.

Suivre l'évolution du cadre légal et réglementaire

D'innombrables réglementations de par le monde prescrivent de respecter des obligations de protection des données et de sécurité des informations. Cette conformité réglementaire est bien difficile à atteindre et à conserver pour les entreprises, quelle que soit leur taille. Parmi ces normes et réglementations, citons notamment les suivantes :

Règlement général sur la protection des données (RGPD) de l'UE

S'applique à tout organisme qui traite des données de citoyens de l'UE. Cette réglementation renforce la protection des données des citoyens de l'UE et encadre l'exportation des données personnelles hors de l'UE.

Loi fédérale sur la protection des données en Suisse (LPD)

La Suisse a récemment révisé sa loi fédérale sur la protection des données (LPD) pour se rapprocher des exigences inscrites dans le RGPD. Cette révision modernise les lois suisses de protection des données afin de conserver le statut de « pays adéquat » que lui reconnaît la Commission européenne et de garantir la libre circulation des données entre l'UE et la Suisse. Dans d'autres pays européens, les lois de protection des données sont révisées à la lumière du RGPD.

Loi de protection des données personnelles en Afrique du Sud

Cette loi dite PoPI Act (Protection of Personal Information) vise à garantir que les organisations sud-africaines collectent, traitent, stockent et partagent les informations personnelles d'une autre entité avec responsabilité. Elle octroie aux personnes des droits de protection et de contrôle de leurs informations personnelles en tant que propriétaires.

Loi américaine sur la transférabilité et la responsabilité en matière d'assurance-maladie

Cette loi dite HIPAA (Health Insurance Portability and Accountability Act) s'applique à tout organisme qui traite ou stocke des données médicales confidentielles (PHI, Protected Health Information). Elle protège la confidentialité et la vie privée des patients.

Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

Cette loi s'applique à tout organisme en affaires avec les citoyens canadiens. Elle protège la confidentialité des renseignements personnels des citoyens canadiens.

Normes de la famille 27000 de l'Organisation internationale de normalisation et de la Commission électrotechnique internationale (ISO/IEC)

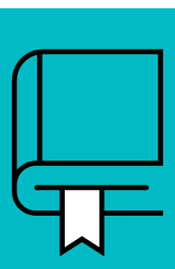
Normes internationales de sécurité des informations, notamment : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001), Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002), Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage (ISO/IEC 27017), et Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII (ISO/IEC 27018).

Norme de sécurité des données pour l'industrie des cartes de paiement

Cette norme dite PCI DSS (Payment Card Industry Data Security Standard) s'applique à toutes les entreprises qui acceptent, traitent ou stockent des transactions par carte bancaire (cartes de crédit, à débit immédiat ou de retrait).

Ces réglementations et d'autres sont certes adoptées pour garantir la mise en œuvre des bonnes pratiques de sécurité et de protection des données dans les entreprises qui

traitent des données sensibles. Elles n'en demeurent pas moins complexes, ambiguës et coûteuses à implémenter. Elles ont malheureusement pour effet secondaire de réorienter les efforts de nombreuses grandes entreprises vers le respect des obligations légales aux dépens de la protection des données et de la sécurité des informations elles-mêmes.



À RETENIR

Conformité et sécurité sont deux notions distinctes. Une entreprise peut respecter ses obligations sans être sécurisée. À l'inverse, une entreprise peut être sécurisée, mais ne pas être en conformité.

Le RGPD vise à protéger la vie privée des personnes de l'UE en leur donnant davantage de contrôle et de droits sur leurs données personnelles. Chaque personne peut ainsi :

- Recevoir les données à caractère personnel la concernant dans un format structuré, couramment utilisé, lisible par machine et interopérable
- Demander le transfert de ses données à un autre responsable du traitement (« droit à la portabilité »)
- Demander la suppression de ses informations (« droit à l'oubli »)

Avec le RGPD entrent en vigueur des règles beaucoup plus strictes sur le consentement, la notification des violations de données et les analyses d'impact obligatoires relatives à la protection des données, et des principes de protection des données dès la conception et par défaut.

Le non-respect du RGPD est puni d'amendes pouvant, pour les entreprises, s'élever jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions €, le montant le plus élevé étant retenu.

Le RGPD suggère également un certain nombre de mesures de sécurité techniques utiles dans la protection des données, notamment :

- La pseudonymisation et le chiffrement des données personnelles
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement de données personnelles
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données à caractère personnel

Pour en savoir plus sur le RGPD et sur les mesures de sécurité que vous pouvez prendre pour rendre votre entreprise conforme au RGPD, rendez-vous à https://encryption.eset.com/fr/

CONFORMITÉ RGPD DES PME : 5 ÉTAPES POUR COMMENCER

1

Déterminer et évaluer les traitements de vos données

Il est crucial de bien comprendre ce que votre entreprise fait avec ses données. Jusque récemment, la conformité au RGPD incombait uniquement aux responsables du traitement. Aujourd'hui, ces obligations s'imposent aussi aux sous-traitants. Vous devez déterminer si votre entreprise est responsable de traitement ou sous-traitante, voire les deux. Il est capital de connaître le lieu du stockage des données et les mesures de sécurité qui l'entourent, mais aussi si les données sont partagées.

2

Tirer les leçons du passé

Pour tester votre capacité à réagir à une attaque, étudiez le déroulement des violations passées et vérifiez si les mesures prises correspondent aux nouvelles obligations définies dans le RGPD. Les nouvelles règles imposent de signaler une violation de données dans un délai de 72 heures et de rendre compte de la gravité de l'attaque. Si votre entreprise en est incapable, elle pourrait écoper d'une lourde amende. Une autre étape essentielle de la mise en conformité avec le RGPD consiste à mettre à jour, voire à créer, votre plan de réponse aux incidents ainsi qu'à tester régulièrement vos capacités de réaction et leur efficacité.

3

Désigner une personne déléguée à la protection des données ou officiellement responsable de la protection des données

Ce conseil simple pour une entreprise aux budgets conséquents ajoute une dépense dissuasive pour d'autres, mais peut-être pas autant que l'amende prévue de 4 % du chiffre d'affaires. En outre, cette responsabilité n'occupe pas nécessairement un rôle à plein temps. Le délégué à la protection des données agit en toute indépendance. Rattaché aux plus hautes instances de la direction, il participe à la mise en œuvre des exigences. Budgéter en amont des ressources supplémentaires vous permettra d'assurer, outre que votre entreprise respecte ses obligations, qu'elle est en situation de gérer une violation de données. Vous réduirez aussi le risque d'une éventuelle amende.

4

Sensibilisez-vous ainsi que vos employés aux règles

Parmi ses buts principaux, le RGPD vise à renforcer le droit à l'oubli des personnes et le droit de suppression de leurs données. Les entreprises doivent aussi obtenir le consentement des personnes concernées « par un acte positif » avant tout traitement de données. De plus, le cadre légal applicable aux données des enfants devient plus restrictif. Il est indispensable de savoir en quoi le règlement change la gestion du consentement et des droits des personnes dans votre entreprise.

5

Connaître votre principale autorité de contrôle

L'autorité qui traite les éventuelles réclamations à l'encontre de votre entreprise dépend du pays de votre établissement et non de celui du plaignant. Cela peut créer des difficultés pour les entreprises qui communiquent à l'international ou pour les multinationales. Certains pays ont une réglementation plus stricte que le RGPD, qu'il convient de prendre en compte.

Dans ce chapitre

- Les Fondamentaux de la protection des données
- Déploiement sur site et dans le cloud
- Bien choisir ses prestataires de services managés et d'infogérance

Chapitre 2

PROTECTION DES DONNÉES : VOS PREMIERS PAS

Dans ce chapitre, vous allez découvrir les fondamentaux des technologies de protection des données, comparer les différentes options de déploiement sur site et dans le cloud, puis explorer les options de prestataires de sous-traitance et de services de sécurité managés.

Comprendre les fondamentaux de la protection des données

Toutes les entreprises, y compris les PME, ont un impératif absolu de sécurité et de confidentialité des données sensibles de leurs clients.

La protection des données, et plus largement la sécurité des informations, embrasse toutes les mesures techniques, logiques et administratives nécessaires à la protection des informations. La triade C-I-A (voir Illustration 2-1) sert souvent de guide au développement et à la mise en œuvre d'un cadre de gestion de la sécurité des informations dans l'entreprise. Elle regroupe trois notions fondamentales en sécurité informatique :

Confidentialité (et vie privée)

Vise à empêcher l'accès, l'utilisation, la diffusion, la consultation, l'inspection et l'enregistrement non autorisés de données.

Intégrité

Vise à empêcher toute modification non autorisée ou non pertinente des données.

Accessibilité (et disponibilité)

Vise à garantir que seuls les utilisateurs autorisés ont un accès fiable et rapide aux données et à empêcher l'interruption des accès ou la destruction non autorisée des données.

Illustration 2-1 : La triade C-I-A.

Prenons un exemple : afin de protéger les données sensibles, les politiques applicables au personnel, à la confidentialité et à la sécurité désignent généralement les utilisateurs autorisés à accéder aux différentes données dans l'entreprise, à quelles fins et avec quel niveau d'autorisation. Les contrôles techniques pour garantir la confidentialité peuvent comprendre des solutions de gestion des identités et des accès (IAM), de chiffrement et de prévention des pertes de données.

Pour protéger l'intégrité des données, on peut implémenter différentes solutions techniques notamment la somme de contrôle et la validation des données saisies dans les formulaires et les bases de données. Les signatures électroniques numériques et le hachage s'appuient sur les technologies de chiffrement pour prouver l'authenticité ou la non-altération des données. Enfin, des solutions contre les programmes malveillants protègent l'intégrité des données, et potentiellement leur confidentialité et leur disponibilité.

Pour assurer l'accès aux données en cas de destruction accidentelle (suppression) ou intentionnelle (attaque par ransomware), des systèmes de sauvegarde et de restauration doublés de politiques d'archivage et de conservation des données sont mis en œuvre. Reportez-vous au Chapitre 4 pour en savoir plus sur les technologies de protection des données.

La pleine sécurité des informations dépend de la confidentialité, de l'intégrité et de la disponibilité de toutes les données sensibles de l'entreprise, notamment de ses systèmes et de ses applications de traitement et de stockage des informations.

Avec l'approche par les risques, les entreprises peuvent mettre en œuvre les contrôles appropriés pour contrer les vulnérabilités et parvenir à un niveau acceptable d'exposition des données au risque de certaines menaces. Plus le risque d'atteinte aux données est élevé, plus les mesures de protection doivent être renforcées. La gestion des risques de sécurité tient en quatre formules (voir Illustration 2-2).

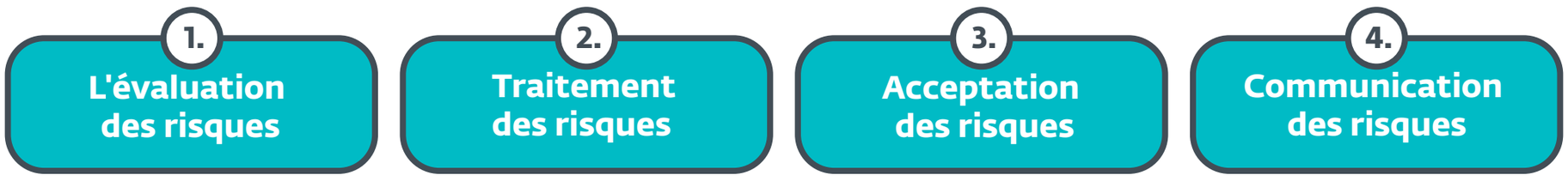


Illustration 2-2 : Processus de base de gestion des risques.

Évaluation des risques

Les nombreuses méthodes d'évaluation des risques diffèrent en termes de complexité et de coûts. Le processus élémentaire repose sur trois piliers :

- **Identification des actifs**
  Identifiez les actifs matériels et immatériels de l'entreprise à protéger, notamment la valeur selon des critères quantitatifs (coût ou part des recettes) ou qualitatifs (importance relative).
- **Analyse des menaces**
  Déterminez les circonstances ou les événements d'origine naturelle ou humaine, leurs conséquences ou répercussions potentielles, et la probabilité et la fréquence de leur survenue.
- **Évaluation des vulnérabilités**
  Repérez l'absence ou la faiblesse des contrôles ou des garde-fous dans un actif qui risquerait d'augmenter les dommages, le coût, la probabilité ou la fréquence de réalisation d'une menace.

Traitement des risques

C'est sur le socle de l'évaluation des risques que sont prises les décisions de gestion concernant un risque spécifique. Parmi les options :

- **Atténuation du risque**
  La mise en œuvre de politiques, de contrôles ou d'autres mesures visant à réduire les répercussions ou la probabilité de réalisation d'une menace donnée contre un actif précis.
- **Réaffectation du risque (transfert)**
  Transférez le risque potentiel à un tiers, par exemple un assureur, un prestataire de service ou un autre agent qui accepte explicitement le risque.
- **Évitement du risque**
  Éliminez complètement le risque, par exemple par la mise à niveau ou au rebut de l'actif ou bien par l'arrêt de l'activité qui l'introduit.

Acceptation du risque

Approbation formelle par la direction des mesures de traitement du risque mises en œuvre, et acceptation de tout risque résiduel (restant) qu'il est impossible en pratique à réduire davantage, à réaffecter ou à éviter.

Communication du risque

Les parties intéressées doivent être informées de toute prise de décision quant au traitement ou à l'acceptation du risque, notamment de leurs rôles et responsabilités personnels selon les risques spécifiques.

Options de déploiement sur site, cloud et hybride : avantages et inconvénients

De nos jours, les entreprises ont de nombreuses options techniques : déploiement sur site, en cloud, voire hybride qui combine des ressources internes et cloud.

Il n'y a pas si longtemps, le seul choix possible était une installation locale. Même les plus petites entreprises ont dû acheter plusieurs serveurs coûteux et les installer, souvent mal dans un sombre placard encombré au fin fond du bâtiment, peut-être même juste au-dessous d'un extincteur automatique qui achèverait de détruire totalement ces précieux investissements informatiques si un incendie les épargnait. Ces serveurs exigent des soins continus d'administration et de maintenance, ce qui signifie souvent du personnel ou des sous-traitants informatiques. Outre les serveurs, il a fallu installer et gérer des équipements réseau (routeurs, commutateurs) et le câblage. A minima, un pare-feu protège le réseau interne « de confiance » de l'internet non fiable.

Si l'option d'un datacenter ou d'une salle de serveurs sur site reste viable pour beaucoup d'entreprises, d'autres, tout aussi nombreuses, poussées par l'avènement ces dix dernières années de technologies toujours plus robustes et fiables de virtualisation, de connectivité réseau et d'informatique en cloud, déplacent certaines voire l'ensemble de leurs ressources informatiques vers le cloud.

Mais qu'est-ce que le cloud exactement ? Si pratiquement chaque acteur du secteur propose d'une manière ou d'une autre une offre dans le cloud, malheureusement la définition de ce cloud est parfois nébuleuse. Commençons donc par éclaircir quelques éléments centraux du cloud à l'aide des définitions impartiales de l'agence américaine des normes et technologies NIST (National Institute of Standards and Technology). L'agence classe les modèles de services en cloud comme suit :

Logiciel à la demande (mode SaaS)

L'entreprise cliente a accès à une application qui s'exécute sur une infrastructure cloud. On accède à l'application depuis différents clients (appareils ou interfaces) et l'entreprise utilisatrice ne connaît, ne gère, ni ne contrôle l'infrastructure cloud sous-jacente. L'entreprise cliente peut, dans une certaine mesure, définir les paramètres utilisateurs de l'application. La sécurité de ses données reste de sa responsabilité.

Plateforme à la demande (mode PaaS)

L'entreprise cliente peut déployer des applications prises en charge dans l'infrastructure cloud du prestataire, mais sans connaître, gérer, ni contrôler l'infrastructure cloud sous-jacente. Elle garde la maîtrise des applications déployées et de certains paramètres de configuration de l'environnement d'hébergement des applications. Elle détient les applications déployées et les données : leur sécurité est donc de sa responsabilité.

Infrastructure à la demande (mode IaaS)

L'entreprise cliente peut déployer des applications prises en charge dans l'infrastructure cloud du prestataire, mais sans connaître, gérer, ni contrôler l'infrastructure cloud sous-jacente. Elle garde la maîtrise des applications déployées et de certains paramètres de configuration de l'environnement d'hébergement des applications. Elle détient les applications déployées et les données : leur sécurité est donc de sa responsabilité.

CONSEIL

À chaque modèle de service cloud à la demande (SaaS, PaaS et IaaS) correspondent des implications de sécurité différentes. Par exemple, des offres en mode SaaS comme Microsoft 365 et Salesforce apportent la sécurité de l'infrastructure via le prestataire cloud, mais laissent au client la responsabilité de la sécurité des données et de l'authentification. Les responsabilités de sécurité de l'entreprise cliente augmentent progressivement dans les offres PaaS et IaaS. De nombreuses solutions cloud articulent désormais la sécurité autour de l'intégrité des données et de l'authentification et non plus de l'infrastructure ou des applications..

L'agence NIST définit en outre quatre modèles de déploiement d'informatique en cloud :

Cloud public

Une infrastructure cloud que tous peuvent utiliser. Elle est détenue, gérée et exploitée par un ou des tiers et se trouve dans des locaux du prestataire cloud.

Cloud privé

Une infrastructure cloud à l'usage exclusif d'une seule organisation. Elle peut être détenue, gérée et exploitée par l'organisation ou un tiers voire une combinaison des deux. Elle peut être sur site ou externalisée.

Cloud hybride

Cette infrastructure cloud combine au moins deux autres modèles de déploiement qui mutualisent une technologie propriétaire ou standardisée de portabilité des applications et des données.

Cloud communautaire (peu courant)

Une infrastructure cloud mutualisée à l'usage exclusif d'un groupe d'organisations.

Comme beaucoup d'initiatives, le passage au cloud commence souvent par des applications et des systèmes non critiques hors production, par exemple un environnement de développement ou des systèmes de sauvegarde. Progressivement, beaucoup d'entreprises se mettent à simplement déplacer leurs applications vers le cloud et à y déployer directement les nouvelles. Enfin, les organisations qui privilégient le cloud (cloud first) s'efforcent de déployer autant que possible leur environnement informatique dans le cloud et de développer pour leurs clients des applications natives cloud.

Parmi les nombreux avantages du cloud pour les entreprises, citons :

Une agilité et une réactivité accrues

Vous accédez aux applications et aux données dans le cloud de n'importe où, à tout moment et depuis n'importe quel appareil.

Un délai de mise sur le marché raccourci

Vous pouvez développer et proposer de nouveaux produits et services plus rapidement dans le cloud sur une plateforme en mode PaaS ou sur des ressources IaaS faciles à provisionner.

Évolutivité à la demande

Il est possible d'ajuster à la hausse ou à la baisse le nombre de licences logicielles ou l'infrastructure selon les variations pour répondre aux besoins des activités cycliques ou en forte croissance dont les aléas et le développement sont difficiles à prévoir précisément.

Stabilité accrue

L'infrastructure cloud est généralement installée dans des datacenters robustes construits pour offrir performances, stabilité et fiabilité et gérés par de grandes équipes de spécialistes IT.

Immobilisations moindres

Vous pouvez déployer l'ensemble de votre infrastructure informatique dans le cloud et éviter d'importantes dépenses d'équipement. Le cloud propose un modèle prévisible de services sur abonnement facturés à l'utilisation : vous pouvez budgéter vos besoins informatiques comme une dépense d'exploitation courante et ne payer que ce que vous utilisez.

ATTENTION

Déplacer vos applications et vos données dans le cloud ne supprime pas ni ne transfère votre responsabilité de sécurité sur ces actifs : elle vous incombe en dernier recours, même si le prestataire cloud en endosse certains aspects pour l'environnement lui-même. Les prestataires de services cloud se réfèrent couramment à un « modèle de responsabilité partagée » où sont clairement précisées les responsabilités de chacun dans le cloud. Nulle part dans ce modèle il n'est écrit que le prestataire cloud serait responsable de la sécurité de vos données.

Prestataires de sous-traitance et de services de sécurité managés

Ce n'est pas une mince affaire que d'assurer la sécurité, la protection, l'application des correctifs et la conformité à la réglementation des systèmes et applications informatiques dans un monde où les entreprises de toute taille sont exposées à des risques toujours croissants et des menaces toujours plus sophistiquées. La charge, particulièrement lourde pour les PME aux ressources limitées en cybersécurité et en informatique, les incite souvent à faire appel à des prestataires de services managés (MSP). Cette solution présente de nombreux atouts, notamment :

Un budget informatique mieux maîtrisé

Les partenaires MSP proposent une gamme complète de produits et services par rapport à l'offre des ressources limitées d'une PME. En adoptant ces services, une PME dispose d'une plus grande marge de manœuvre financière et rend ses coûts plus prévisibles. De plus, les plans de facturation ajustables améliorent sa maîtrise des budgets IT et sécurité.

Un conseil averti et de confiance

Les PME peuvent mobiliser les connaissances approfondies et la riche expérience des personnels IT et sécurité du partenaire MSP.

L'éclairage du spécialiste

Mieux informés des solutions de sécurité disponibles sur le marché, les partenaires MSP axés sur la sécurité peuvent proposer une offre sur mesure à leurs clients.

Innovation

Les équipes sécurité spécialisées des partenaires MSP facilitent l'adoption et la mise en œuvre de solutions innovantes. Elles aident les clients à rester en phase avec les derniers développements du secteur.

Évolution en toute fluidité

Avec un partenaire MSP, une entreprise peut ajouter ou supprimer des composants logiciels ou matériels en fonction de ses besoins actuels sans se préoccuper d'acquérir, de mettre en œuvre ou de maintenir de nouvelles ressources logicielles ou matérielles.

SHEFFIELD WEDNESDAY CHAMPIONS ESET I.T. SECURITY

Le Sheffield Wednesday Football Club (SWFC) est un des plus anciens clubs de football professionnels au monde. Son stade Hillsborough Stadium a accueilli la Coupe du monde et les Championnats d'Europe. Les demi-finales de la FA Cup s'y sont déroulées. Le Club est fortement implanté dans la vie locale avec notamment un programme qui encourage l'activité sportive et valorise ses installations au bénéfice de la population. Un des grands axes du programme est le développement des compétences psychosociales : le SWFC a investi en matériel informatique pour animer des sessions itinérantes en plus de celles dans ses installations permanentes.

Défis

L'antivirus n'était plus adapté à la situation et consommait beaucoup trop de ressources processeur. SWFC voulait aussi disposer d'une console d'administration centralisée et automatiser les mises à jour de ses 310 machines pour les protéger en permanence des menaces les plus récentes et garantir ainsi la continuité de l'activité.

Solution

Richard Ford, responsable IT, a adopté ESET Endpoint Antivirus et ne le regrette pas.
« ESET était exactement ce que nous cherchions : économe en ressources, il apporte une protection fiable à un coût qui s'ajuste aux besoins, il est facile à déployer et centralise la gestion. Les utilisateurs et nous ne sommes pas distraits par des problèmes annexes de ralentissement ou de faux positifs. ESET fonctionne exactement comme devraient le faire tous les antivirus : discrètement en arrière-plan. »

Bilan

- Une solution de sécurité facile à intégrer, au fonctionnement discret et à l'empreinte faible, sans effet sur le trafic réseau.
- Elle est facile à configurer et presque sans maintenance.
- La console d'administration centrale délivre aux serveurs et aux postes de travail une protection contre les menaces. Elle offre ainsi une vue d'ensemble centralisée avec des informations en temps réel.
- La solution se met à jour régulièrement une fois configurée.

Dans ce chapitre

- Processus d'évaluation des risques
- Identifier les opérations de traitement des données
- Déterminer les répercussions d'une violation de données
- Identifier les menaces sérieuses à la sécurité des données
- Implémenter les contrôles appropriés de la protection des données

Chapitre 3

ÉVALUER LES RISQUES À LA SÉCURITÉ DES DONNÉES

Dans ce chapitre, vous apprendrez à appliquer à la sécurité des données le processus de gestion des risques vu au Chapitre 2.

Comprendre le processus d'évaluation des risques

L'évaluation des risques est la première phase du processus de gestion des risques traité au Chapitre 2. Une évaluation des risques consiste à :

- Identifier les actifs matériels et immatériels
- Analyser les menaces, y compris les impacts et leurs probabilités
- Évaluer les vulnérabilités (c'est-à-dire les garde-fous ou contrôles absents ou insuffisants, pour un actif donné)

De même, l'évaluation des risques à la sécurité des données consiste à :

- Identifier les opérations de traitement des données (pour déterminer où et comment votre entreprise utilise ses actifs d'information)
- Déterminer les répercussions commerciales potentielles (si vos données sont compromises)
- Identifier les éventuelles menaces et évaluer la probabilité de leur occurrence et de leur fréquence
- Évaluer le risque (pour déterminer les garde-fous ou contrôles à implémenter pour protéger vos données)

Étape 1
Identifier les opérations de traitement des données

Au sein d'une organisation, les données ont différents profils de risque selon leur contenue, et divers utilisations dans l'entreprise. Il est dès lors important de comprendre le traitement des données dans votre organisation lorsque vous lancez un processus d'évaluation des risques. Par exemple, une PME type effectuera tout ou une partie des opérations de traitement des données suivantes :

Ressources humaines avec la gestion des salaires, le recrutement et la fidélisation des employés, les dossiers de formation, les mesures disciplinaires et les évaluations de performances.

Gestion de la clientèle, du marketing et des fournisseurs avec les informations clients, les bons de commande et les commandes clients, les factures, les listes d'e-mails, les données de marketing et de publicité, et enfin les contrats fournisseurs.

La sûreté du personnel et la sécurité physique comme les rapports d'accès de sécurité du personnel, ceux des visiteurs et de la surveillance vidéo.

Pour chaque opération de traitement de données, posez-vous les questions suivantes :

- Quelles données personnelles sont traitées ?
- Quelle est la finalité du traitement ?
- Où a lieu le traitement ?
- Qui est responsable du traitement ?
- Qui a accès aux données ?

À RETENIR

Bonne pratique de la sécurité des informations, le principe de moindre privilège énonce que les utilisateurs disposent uniquement de l'accès minimum nécessaire à la réalisation d'une tâche spécifique.

Étape 2
Déterminer les potentielles répercussions commerciales

Vous devez ensuite déterminer l'impact potentiel d'une violation ou d'une compromission de données. Une violation ou une compromission de données peut affecter leur confidentialité (par exemple, un accès non autorisé), leur intégrité (par exemple, la modification non autorisée) ou leur disponibilité (par exemple, une attaque par ransomware).

À RETENIR

Les organisations doivent protéger la confidentialité, l'intégrité et l'accessibilité (disponibilité) des données. Ce principe est connu sous le nom de triade C-I-A en cybersécurité (voir pages 14-15).

Dans une évaluation des risques classique, l'impact potentiel d'un risque donné est généralement exprimé en termes de dommage à l'entreprise comme la perte ou la destruction d'un actif matériel (par exemple un serveur, une photocopieuse ou un véhicule).

L'impact d'un risque de sécurité des données sur l'activité ressemble aux autres, mais il peut être indirect. Dans le cas de données personnelles sensibles, la personne dont les données ont été exposées ou compromises est la victime directe. Dans un tel cas, la conséquence peut être le vol de l'identité d'une personne ou de ses ressources financières ou encore la violation de sa vie privée. Les répercussions sur l'activité ne sont pas aussi directes, mais restent très coûteuses notamment à cause de :

- La perte de clientèle et la baisse du chiffre d'affaires
- L'atteinte à la marque et les mauvaises relations publiques
- Les sanctions prévues par la loi et les litiges
- Les notifications des violations et les services de surveillance du crédit
- L'analyse post-incident et la récupération

CONSEIL

L'impact sur l'entreprise est classé en trois catégories : faible, moyen ou élevé. Toutefois, la définition elle-même de chaque niveau dépend de chaque entreprise et doit tenir compte d'indicateurs objectifs (quantitatifs) et subjectifs (qualitatifs).

Étape 3
Identifier les éventuelles menaces et évaluer leur probabilité

Une menace est tout événement ou situation de cause naturelle ou humaine qui a le potentiel d'affecter négativement la confidentialité, l'intégrité et la disponibilité de données personnelles ou sensibles. Elle recouvre donc les attaques à la cybersécurité, la perte ou la diffusion accidentelle, les menaces internes, les incendies et les inondations, les séismes et les tsunamis, les événements météorologiques comme les cyclones ou les tornades, les troubles publics, les conflits du travail, et bien plus. Les entreprises doivent identifier les menaces éventuelles à leurs opérations de traitement des données et, pour chacune, évaluer la probabilité et la fréquence de l'occurrence. Assurez-vous de couvrir les menaces de domaines bien définis comme les menaces réseaux, celles visant les ressources informatiques, logicielles et matérielles utilisées dans le traitement de données, celles des processus et procédures rattachées, celles touchant aux ressources humaines, et enfin celles dues à l'échelle des traitements.

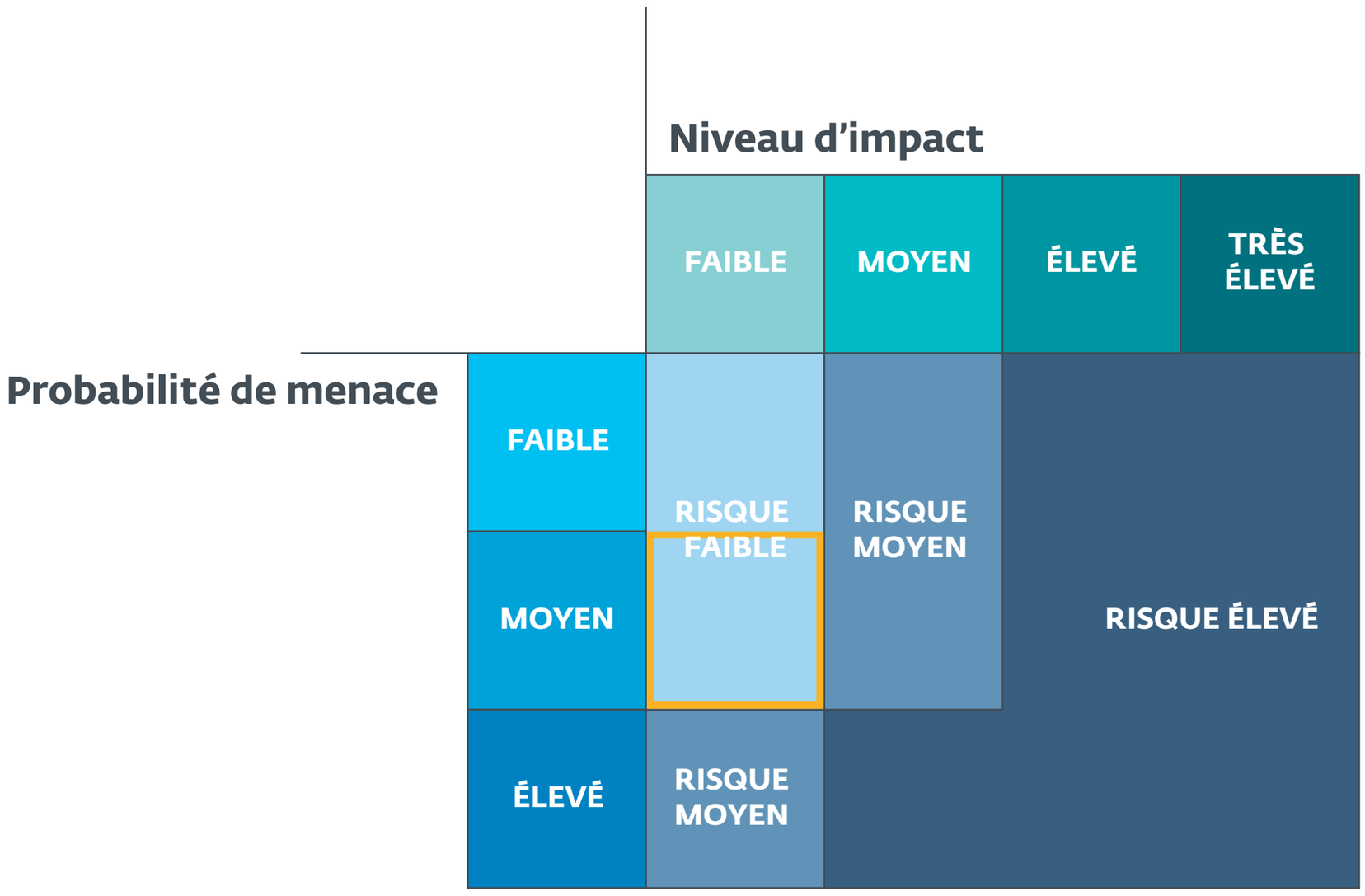
CONSEIL

Pour chaque menace identifiée, sa probabilité est classée sur la même échelle que les impacts commerciaux : faible, moyenne ou élevée. Lors de l'évaluation de la probabilité qu'une menace se réalise, pensez à la probabilité qu'elle se produise, mais aussi à sa fréquence vraisemblable sur une période donnée (par exemple, sur un an).

Étape 4
Évaluer le risque

Une fois que vous avez repéré toutes les opérations de traitement de données (et les données traitées), déterminé les potentielles répercussions commerciales d'une violation ou d'une compromission des données et identifié les menaces éventuelles, la probabilité et la fréquence de leur réalisation, vous pouvez évaluer le risque associé à chaque opération et déterminer, d'une part, les contrôles technologiques de protection des données traités au Chapitre 4 et, d'autre part, les contrôles des processus et organisationnels. Dans le cadre de l'évaluation des risques, ces contrôles de processus et organisationnels traités dans le Chapitre 5 doivent être implémentés pour sécuriser comme il se doit vos données et vos opérations de traitement des données suivant l'approche des risques.

L'Illustration 3-1 montre un modèle d'évaluation des données et un exemple d'évaluation d'opération de traitement de données.



Probabilité de menace

Pour une opération de traitement de données particulière, parcourez la liste des menaces de traitement de données possibles et évaluez la probabilité de menace. La probabilité finale doit être basée sur la somme des scores de toutes les menaces figurant dans la liste.

- **Faible** – il est peu probable que la menace se matérialise
- **Moyen** – il y a une chance que la menace se matérialise
- **Élevé** – la menace est susceptible de se matérialiser

Niveau d'impact

Pour un traitement de données particulier, évaluez l'impact possible de la confidentialité, de l'intégrité et de la disponibilité des données (triade C-I-A). L'impact le plus élevé des trois est le niveau d'impact final.

- **Faible** – Inconvénients mineurs, qui pourraient être surmontés sans aucun problème
- **Moyen** – Inconvénients importants, qui pourraient être surmontés malgré quelques difficultés
- **Élevé** – Conséquences importantes, qui pourraient être surmontées mais avec de graves difficultés
- **Très élevé** – Conséquences importantes, voire irréversibles, peuvent ne pas être surmontées

Qualification du traitement des données

- **Risque faible**
- **Risque moyen**
- **Risque élevé**

Exemple

Opération de traitement des données :
Marketing / Publicité
Données traitées : Contact info
coordonnées (par exemple, nom, adresse postale, numéro de téléphone, e-mail)
Classification des données : données personnelles
Finalité du traitement : promotion de produits et offres spéciales auprès de clients potentiels
Sujets de données : clients et prospects

Probabilité de menace

Menaces liées au réseau et aux ressources techniques (HW, SW) : Moyenne
Menaces liées aux processus et procédures : faible
Menaces de ressources humaines impliquées : Moyenne
Secteur d'activité et ampleur des menaces de traitement : Moyenne
Probabilité finale : moyenne

Niveau d'impact

Confidentialité de l'évaluation du niveau d'impact : faible
Intégrité : faible, disponibilité : faible
Niveau d'impact final : faible

Qualification du traitement des données

- **Risque faible** – le traitement des données de marketing / publicité présente un risque faible - Des mesures techniques et organisationnelles adaptées à ce risque doivent être mises en œuvre.

Illustration 3-1 : Matrice d'évaluation des risques d'une opération de traitement de données

Dans ce chapitre

- Explorer les solutions de protection des données
- Sécuriser le réseau
- Réduire les erreurs et améliorer l'efficacité par l'orchestration

Chapitre 4

APPRÉHENDER LA TECHNOLOGIE DE PROTECTION DES DONNÉES

Dans ce chapitre, vous découvrirez différentes technologies de protection des données et de sécurité des informations que vous pouvez envisager de mettre en œuvre dans votre entreprise, depuis les terminaux (endpoint) jusqu'au réseau et au-delà.

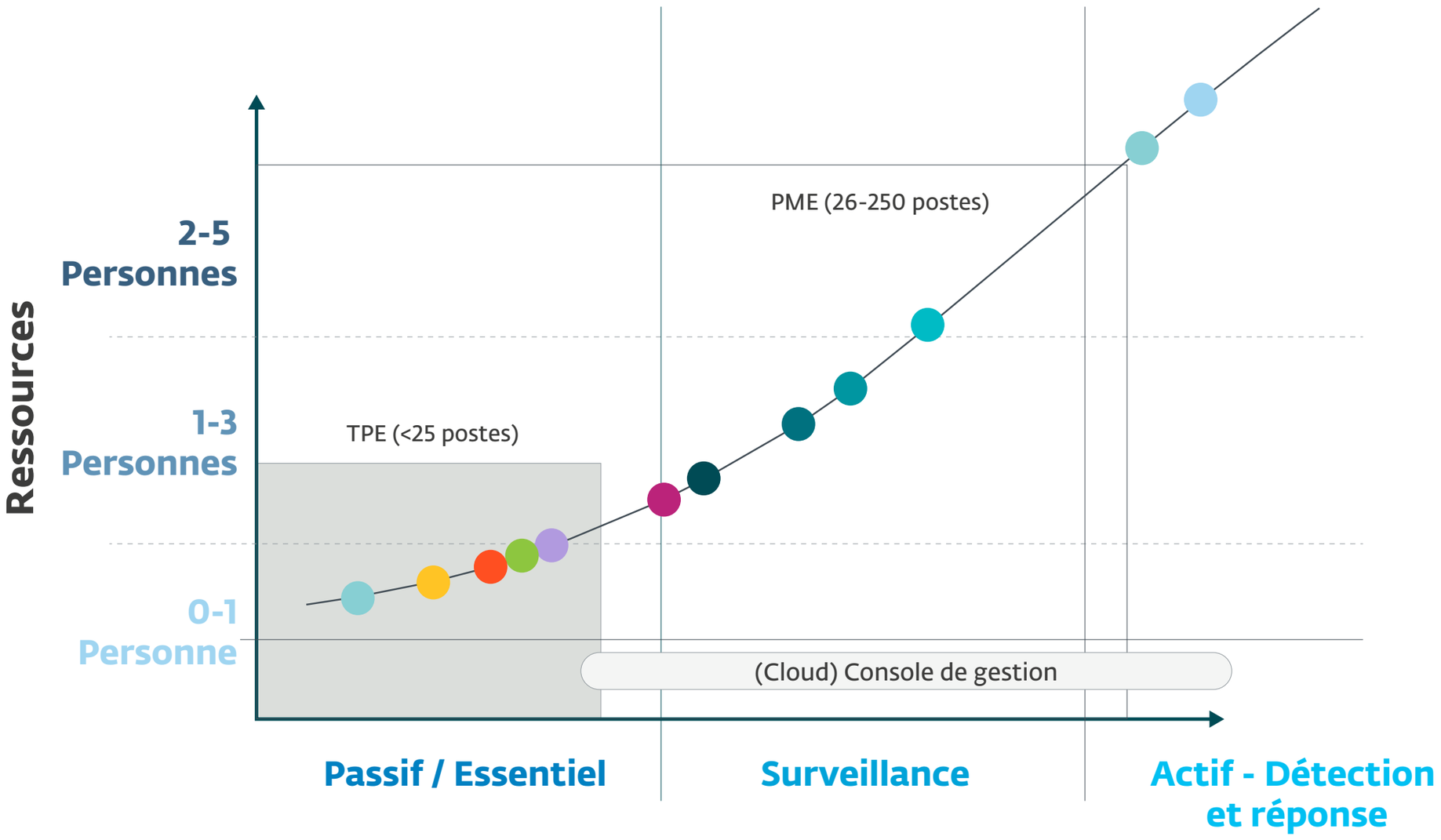
Protéger les données où qu'elles se trouvent

Les données sont un actif indispensable, mais elles représentent un risque énorme pour votre entreprise. Vous pouvez utiliser de nombreuses technologies de sécurité pour protéger les données des espaces de travail (ordinateurs, appareils mobiles, etc.), sur votre réseau ou dans le système principal (salle des serveurs sur site, datacenter cloud, etc.). L'Illustration 4-1 expose les différentes technologies de sécurité, que nous verrons en détail ci-après, à envisager dans votre implémentation en fonction du niveau de risque acceptable et de vos ressources disponibles.

Outre un logiciel antivirus, les PME devraient prendre en considération les éléments suivants :

Protection des terminaux

Au-delà de l'antivirus, la protection des terminaux est une technologie multicouche qui empêche l'infection par des programmes malveillants (virus, vers, ransomwares, logiciels espions, chevaux de Troie y compris distants, et les rootkits/bootkits), l'exploitation de failles, les attaques réseau, l'infiltration de botnets et bien plus encore (voir ci-après l'encadré « Sélectionner une solution de protection des terminaux »).



Technologies de sécurité

- AV
- Endpoint Protection
- Multi-Factor Authentication
- Firewall
- Encryption
- Backup and Recovery
- Mobile Device Management (MGM)
- NAC (Network Access Control)
- SIEM
- Patch Management
- DLP
- EDR/EDTR

Maturité de la cybersécurité

- **Passif / Essentiel** – Actions automatisées, réactions ad hoc sur les risques identifiés
- **Surveillance** – Actions automatisées, surveillance active de l'état actuel avec des actions réagissant aux alertes d'attaques ou de risques potentiels
- **Actif - Détection et réponse** – Analyse interne des données et surveillance de l'état afin de détecter les attaques ciblées, les actions selon les politiques destinées à répondre aux attaques et aux attaques possibles

Ressources

- Équipe officelle : spécialiste à temps plein **2-5 personnes**
- Dédié : spécialiste à temps partiel **1-3 personnes**
- Au besoin : « installez et oubliez » **0-1 personne**

Illustration 4-1 : Technologies de sécurité

Authentification multifacteur (MFA)

La MFA (Multi-Factor Authentication) renforce l'authentification élémentaire, par exemple de la combinaison d'un nom d'utilisateur avec un mot de passe, en y ajoutant un facteur obligatoire pour se connecter au système ou à l'application. Il s'agit généralement d'un code à usage unique envoyé séparément à une adresse e-mail ou à un numéro de téléphone mobile préalablement configuré. L'utilisateur commence par saisir son identifiant et son mot de passe. Le code peut uniquement servir à authentifier une seule session utilisateur dans un laps de temps bref, par exemple 60 secondes. L'objectif est de limiter l'efficacité des attaques replay dans lesquelles un pirate intercepte ce code puis le réutilise dans une autre session afin de s'authentifier. Avec la forme la plus récente d'authentification MFA, prise en charge par ESET Secure Authentication, l'utilisateur se contente de confirmer son authentification sur un smartphone appairé sans même saisir de code unique.

Pare-feu

(Les pare-feu sont traités plus bas dans ce chapitre.)

Chiffrement

Le chiffrement rend les données illisibles sans la clé de déchiffrement. Le chiffrement et le déchiffrement ont lieu soit sur le matériel (plus rapide) soit sur le logiciel (moins cher). Le chiffrement des fichiers, des dossiers et des e-mails assure la pleine sécurité de la collaboration entre des équipes et des groupes de travail différents, d'autant que la politique de sécurité est gérée de manière centralisée et mise en œuvre sur tous les terminaux.

Sauvegarde et restauration

Les systèmes de sauvegarde et de restauration comprennent la partie logicielle de la sauvegarde et les supports comme les disques ou bandes, sur site (avec stockage hors site), à distance ou dans le cloud. Il faut tester régulièrement les sauvegardes pour s'assurer qu'elles sont restaurables et que tous les systèmes et données nécessaires sont sauvegardés correctement, et assez souvent pour satisfaire les exigences de l'entreprise.

Gestion des appareils mobiles (MDM)

Beaucoup d'entreprises et en particulier des PME autorisent leurs collaborateurs à utiliser leurs appareils mobiles personnels pour des usages professionnels. Cette tendance est connue sous le sigle anglais « BYOD » (Bring Your Own Device). Toutefois, les entreprises doivent s'assurer que le fonctionnement de ces appareils est sécurisé afin d'éviter toute compromission de données clients ou commerciales sensibles en cas de perte, de vol ou de piratage. Les solutions de gestion des appareils mobiles apportent des fonctions d'application de politiques (par exemple utilisation d'un code secret), de chiffrement, de conteneurisation (pour cloisonner les applications et données professionnelles des personnelles), et la suppression et le verrouillage à distance.

Prévention des pertes de données (DLP)

Les logiciels DLP (Data Loss Prevention) empêchent la diffusion non autorisée, accidentelle ou intentionnelle, de certaines données comme les numéros de sécurité sociale, les dossiers médicaux confidentiels et les informations financières. Ils analysent les e-mails et les documents à la recherche de certains mots clés ou modèles de données.

ATTENTION

Pour être efficace, la prévention des pertes de données exige des ressources supplémentaires pour modifier les politiques, évaluer les incidents internes et externes et appliquer les mesures correctives. Dans le cas contraire, son efficacité sera restreinte.

SÉLECTIONNER UNE SOLUTION DE PROTECTION DES TERMINAUX

La protection des terminaux sur les stations de travail, les appareils mobiles et les serveurs forme la première ligne de défense contre les cyberattaques. En effet, les agresseurs s'attaquent généralement au maillon faible pour pénétrer le réseau. Si vous laissez la sécurité des terminaux aux bons soins d'un logiciel « gratuit » de protection contre les programmes malveillants, vous ouvrez la porte à de graves déconvenues, infections ou violations de données.

Une protection avancée des terminaux intègre plusieurs technologies de pointe comme l'apprentissage automatique, la détection pré-exécution, l'isolement « sandboxing » et d'autres pour une approche multidimensionnelle. La nouvelle génération de produits de protection des terminaux est présentée comme le prochain tournant dans la lutte contre les logiciels malveillants, mais ces nouveaux produits recouvrent aussi, et même surtout, des produits qui n'implémentent qu'un seul aspect de la protection des terminaux comme l'apprentissage automatique. Lors de votre évaluation des solutions, cherchez-en une qui comprennent TOUTES les fonctions suivantes : apprentissage automatique, détection pré-exécution, sandboxing et autres technologies de pointe en plus de la détection classique sur la signature des programmes malveillants avec mises à jour en temps réel et renseignement sur les menaces.

Une protection efficace des terminaux passe par :

Une installation peu encombrante
Un logiciel contre les programmes malveillants gourmand en espace disque, en ressources de mémoire et en utilisation du processeur risque de provoquer des ralentissements et, par conséquent, d'être contourné, c'est-à-dire désactivé, par les utilisateurs.

Fonctionnalités robustes de mise à jour
Un logiciel de lutte contre les programmes malveillants doit obtenir en temps réel les informations sur les menaces, sans point de défaillance unique ni goulot d'étranglement, par exemple grâce à un serveur de mises à jour sur le réseau. Le cloud sert de plus en plus à apporter les mises à jour et les informations sur les menaces aux terminaux.

Résilience
Les logiciels de lutte contre les programmes malveillants doivent être efficaces même hors ligne et résister aux attaques qui les ciblent précisément.

Stabilité du produit
Les logiciels publiés doivent avoir fait leurs preuves en termes de sécurité, de stabilité et d'absence de bogue.

Gestion centralisée
Au-delà du déploiement de la protection des terminaux, les entreprises doivent pouvoir vérifier que le logiciel est bien installé, qu'il s'exécute correctement et reçoit régulièrement les mises à jour. Il faut pouvoir traiter à distance les incidents de protection des terminaux et prouver que la protection du terminal fonctionne par exemple en vous y connectant pour un audit de conformité.

Sécuriser le réseau

La sécurisation du réseau d'entreprise est devenue beaucoup plus ardue ces dernières années avec la prolifération des appareils mobiles et l'avènement de l'informatique en cloud. Elle n'en reste pas moins un élément crucial de la sécurité des informations et de la protection des données. Parmi les technologies de protection des données pour le réseau, citons :

Pare-feu

Les pare-feu sont le socle de la sécurité des réseaux et peut-être à eux seuls l'investissement le plus important qu'une entreprise peut réaliser pour sécuriser son réseau. Un pare-feu de base fournit des fonctions de filtrage des paquets et d'inspection dynamique du trafic réseau. Un pare-feu nouvelle génération (NGFW) apporte une fonctionnalité de sécurité réseau avancée dont la protection contre les programmes malveillants, le filtrage de contenu, la détection et la prévention d'intrusion et le renseignement sur les menaces. Un pare-feu d'applications web (WAF) est spécifiquement conçu pour la protection des sites web d'entreprise et des applications accessibles par internet.

Systèmes de prévention et de détection d'intrusion (IPS/IDS)

Les systèmes IDS et IPS détectent le trafic réseau malveillant d'après des signatures et des règles préconfigurées. L'IDS est un système passif qui se résume à alerter l'équipe IT d'une intrusion possible. L'IPS est un système actif susceptible d'agir de manière prédéfinie, par exemple en interrompant ou en bloquant du trafic malveillant.

Logiciel à la demande (mode SaaS)

Les applications à la demande sont désormais omniprésentes : les utilisateurs cherchent et installent des logiciels simples à utiliser pour les aider au quotidien dans leurs tâches professionnelles. Parmi les applications les plus populaires, on peut citer Box, Dropbox, Google Docs et OneDrive. Il revient aux entreprises de repérer les applications SaaS en usage sur leur réseau soit pour approuver l'usage d'une application particulière et mener une action de sensibilisation soit pour la bloquer expressément.

Segmentation du réseau local virtuel (VLAN)

La segmentation du VLAN (Virtual Local Area Network) sert à cloisonner logiquement un réseau par exemple par service (comptabilité, ressources humaines, exploitation…) afin d'empêcher les accès non autorisés à certaines données et le trafic réseau excessif comme une tempête de diffusion qui pourrait ralentir le réseau.

Réseau privé virtuel (VPN)

Une appliance ou un logiciel de VPN (Virtual Private Network) sert aux utilisateurs distants à se connecter au réseau d'entreprise via internet par un tunnel chiffré. Un réseau VPN peut aussi servir à relier des réseaux de fournisseurs ou de partenaires comme un sous-traitant de votre chaîne logistique ou un prestataire cloud.

Contrôle d'accès au réseau (NAC)

Un contrôleur NAC (Network Access Control) est une solution unifiée de gestion de la sécurité. Il applique des politiques de sécurité en fonction de l'authentification de l'utilisateur ou du système : les accès à certaines parties du réseau sont autorisés en fonction de la conformité de l'utilisateur ou du système avec des règles de sécurité, par exemple correctifs de sécurité appliqués et signatures antivirus à jour, chiffrement de la connexion réseau par VPN, etc.

Gestion des informations et des événements de sécurité (SIEM)

Les solutions SIEM (Security Information and Event Management) rassemblent et analysent les informations des journaux en provenance de sources de données nombreuses et variées : pare-feu, IDS/IPS, WAF, serveurs et terminaux.

Gestion des correctifs

L'application des correctifs aux vulnérabilités connues sur les serveurs et les terminaux est au cœur des fonctions de sécurité de toutes les entreprises. Plus l'entreprise se développe, plus l'installation manuelle des correctifs de sécurité sur des centaines de serveurs et de terminaux répartis sur des sites distants se complique. Les solutions spécialisées aident à automatiser et à gérer la plupart des fonctions de gestion des correctifs.

Gestionnaire de mots de passe

L'idée est simple, mais puissante et l'implémentation de gestionnaires de mots de passe dans toute l'entreprise vaut largement la peine.

Protection DNS

Le système DNS (Domain Name System) est de nouveau un vecteur d'attaque courant, en particulier pour les attaques par déni de service (DoS). Pour renforcer la sécurité du protocole DNS, il faut encore lui appliquer les améliorations comme les extensions de sécurité DNS (DNSSEC) et implémenter les bonnes pratiques de sécurité pour la configuration des serveurs DNS, notamment la désactivation des recherches récursives. Les autres options de sécurité DNS comprennent l'installation d'appliances DNS dédiées et renforcées ou le recours à un service DNS managé.

Filtrage de contenu web

Ce filtrage empêche les utilisateurs de consulter des sites non autorisés et potentiellement dangereux, voire malveillants, sur la base de l'adresse (adresse IP ou URL) ou du contenu des sites.

Comprendre le besoin d'orchestration

À mesure que votre activité se développe, le besoin d'automatisation et d'orchestration de vos processus IT se fait plus pressant, en particulier si votre équipe informatique a des ressources restreintes. L'installation et la configuration manuelle des terminaux, stations de travail, appareils mobiles et serveurs, ne sont pas tenables dans une entreprise en pleine croissance, encore moins en cas de multiplication des sites distants.

Au-delà du manque d'efficacité dû au déplacement physique nécessaire pour chaque équipement, les processus manuels introduisent un risque d'erreur, notamment de paramétrage incorrect ou incohérent.

L'automatisation et l'orchestration améliorent l'efficacité de votre équipe informatique, renforcent la productivité de vos utilisateurs finaux en réduisant les interruptions de service, et diminuent les erreurs de configuration potentiellement coûteuses. Les plateformes de gestion aident à automatiser les processus manuels et à définir des politiques standard.

CONSEIL

Pour une PME sans les ressources nécessaires au déploiement d'une plateforme de gestion sur site, une solution cloud ou un prestataire de services managés (MSP) peut apporter les services d'automatisation et d'orchestration pour accompagner une croissance rapide et assurer la prise en charge d'un environnement informatique toujours plus complexe.

ESET PROTÈGE VOS TERMINAUX SUR SITE, DISTANTS ET MOBILES

Mercury Engineering est la plus grande firme d'ingénierie et d'études techniques en Irlande. Elle emploie environ 4 000 personnes, en grande partie mobiles et qui travaillent souvent à distance dans plus de 30 pays, dans des conditions diverses et difficiles. Beaucoup d'employés se connectent à des réseaux non sécurisés comme des Wi-Fi publics et des réseaux cellulaires.

Défis

Chez Mercury, l'approche IT se focalise surtout sur la sécurité des données dans ces environnements potentiellement dangereux. Les informations commerciales de la société nourrissent sa croissance : les données des soumissions et des devis sont au cœur de l'acquisition et de la fidélisation des clients. La sécurité de ces informations est vitale. L'intégrité de chaque machine revêt aussi une importance extrême pour Mercury. De nombreux collaborateurs travaillent dans des délais particulièrement courts et les configurations matérielles et logicielles sur mesure de leurs ordinateurs rendent difficile l'échange rapide d'une machine compromise.

Malgré la mise en œuvre de produits de lutte contre les programmes malveillants, Mercury a subi plusieurs infections de logiciels malveillants et de graves infections virales. Il arrivait fréquemment que des collaborateurs n'arrivent plus accéder à leur ordinateur. Le personnel de l'assistance de Mercury perdait de longues heures à traiter ces infections, souvent à l'aide de logiciels gratuits dépourvus des fonctionnalités de gestion, d'évolutivité et de reporting nécessaires en entreprise. Le système principal était particulièrement complexe, difficile à gérer et cher avec une maintenance lourde. Il fallait faire appel à des services professionnels pour tout changement ou mise à niveau. La solution de gestion et de surveillance avait une fonctionnalité très limitée, notamment pour les terminaux distants hors du réseau. En l'absence d'informations en temps réel sur les terminaux, les dégâts s'étendaient avant qu'on ne découvre l'infection en fin de journée, trop tard pour la contenir. Le service IT faisait des heures supplémentaires pour pallier les faiblesses des anciens produits de lutte contre les programmes malveillants.

Solution

Depuis que Mercury utilise ESET, le processus est rapide. « Son déploiement a pris quelques heures et non des jours. » Sa mise en œuvre aussi s'est déroulée sans accroche : un seul administrateur système de Mercury, épaulé par l'assistance technique d'ESET Irlande, a suffi à mettre le nouveau réseau en production. Tout le réseau ESET s'administre désormais depuis une seule petite machine dotée d'un simple processeur et de 4 gigaoctets de mémoire qui prend en charge la gestion de plus de 1 000 ordinateurs et 200 serveurs sur plusieurs pays et sur des réseaux publics dans le monde entier.
La console garantit aussi que la sécurité de Mercury est conforme aux obligations et normes internationales comme ISO 27001.

« La solution est transparente pour l'utilisateur final, il ne se rend pas compte de ce qui se passe : le logiciel s'exécute en arrière-plan avec discrétion et efficacité. Les activités commerciales quotidiennes se déroulent normalement et nous restons protégés sans aucune répercussion sur l'utilisateur. La meilleure preuve réside dans les statistiques de notre assistance : depuis le lancement d'ESET, il n'y a eu aucun dossier d'assistance pour des problèmes liés à l'antivirus ou aux logiciels malveillants ! » se réjouit le responsable de l'infrastructure informatique de Mercury.

Bilan

- Plus de quatre ans sans aucun problème de virus ou de programme malveillant
- Discrétion et faible empreinte de la solution ESET
- Surveillance en temps réel pour réagir rapidement aux menaces (atténuation et remédiation)
- Gestion des terminaux distants et mobiles hors du réseau d'entreprise
- Sécurisation des informations confidentielles, comme les offres et les devis

CONSEIL

De nombreuses PME s'appuient sur ESET Security Management Center (ESMC) et ESET Cloud Administrator (ECA) pour gérer en toute facilité et sécurité leurs ressources distantes et cloud respectivement, sans coûteux déploiements matériels complexes sur site

SECURITY MANAGEMENT CENTER

EN SAVOIR PLUS

CLOUD ADMINISTRATOR

EN SAVOIR PLUS

Dans ce chapitre

- Renforcer les contrôles techniques par des contrôles organisationnels
- Identifier le besoin de contrôles de processus

Chapitre 5

EXPLORER LES CONTRÔLES D'ORGANISATION ET DE PROCESSUS

Dans ce chapitre, vous verrez comment l'alliance des contrôles organisationnels et techniques aide votre entreprise à protéger ses données.

Établir des contrôles organisationnels

La protection efficace des données ne se résume pas à des solutions techniques. Vous devez établir des contrôles organisationnels et administratifs pour garantir le déploiement, la configuration et l'exécution corrects des contrôles techniques qui viennent soutenir une stratégie structurante de gestion de la sécurité. Voici quelques axes des contrôles organisationnels :

Données personnelles sensibles et confidentielles

Le recours à des contrôles techniques, via du chiffrement par exemple, et la prévention des pertes de données (DLP) doit être rationalisé en raison des coûts associés, tant au niveau financier qu'en termes de performances. En effet, Le chiffrement consomme des ressources de traitement pour chiffrer et déchiffrer les données. Les solutions DLP, quant à elles, analysent et recherchent des mots clés / modèles pour repérer les données sensibles ou confidentielles (numéros de cartes bancaires, dossiers médicaux et numéros de sécurité sociale). Établir une grille de classification des données peut aider vos utilisateurs à déterminer les données à protéger, pour quelles raisons et comment.

Audit et documentation des données

Les entreprises qui collectent, traitent et stockent des données sensibles doivent documenter leurs motivations, les moyens / sources utilisés, ainsi que la façon dont elles exploitent et protègent celles-ci. Documenter les politiques de confidentialité et de sécurité des données participe à répondre à ces questions et aux critères d'audit, notamment dans le cadre de la Loi américaine sur la Transférabilité et la Responsabilité en matière d'Assurance Maladie (HIPAA), mais également pour être en vigueur avec le Règlement Général Européen sur la Protection des Données (RGPD).

Politiques de sécurité

Les politiques n'ont pas à être encyclopédiques ; souvent, quelques paragraphes suffisent amplement. Elles doivent définir clairement les rôles et responsabilités de chacun en relation avec la protection des données personnelles. Parmi les politiques de sécurité importantes à définir dans toute entreprise, citons les règles sur :

- Le bon usage du courrier électronique et d'internet
- Les appareils personnels (BYOD)
- Les accès à distance
- Les logiciels autorisés

Ressources humaines

Il s'agit des politiques et procédures qui garantissent que les données personnelles (candidatures à un poste, données sur les rémunérations, dossiers de formation et dossier disciplinaires) collectées, tenues à jour et traitées par les ressources humaines soient protégées. D'autres traitements sont également inclus : la vérification des antécédents préalable à l'embauche, les tests antidopage et les rotations d'emplois.

Utiliser un modèle de maturité de la sécurité

Un tel modèle peut vous aider à déterminer vos capacités de sécurité , mais aussi à identifier les potentielles écarts entre la situation actuelle et celle souhaitée. Votre objectif dépend de différents facteurs tels que :

- Les données à protéger : données sensibles, des informations financières, des actifs immatériels, des équipements médicaux ou une infrastructure critique.
- Votre secteur d'activité : la santé, la finance, le commerce de détail, la défense ou les services d'utilité publique.
- Vos obligations de conformité légale et réglementaire : devez-vous respecter la Loi américaine sur la Transférabilité et la Responsabilité en matière d'Assurance Maladie (HIPAA), le Règlement Général européen sur la Protection des Données (RGPD), la Loi Canadienne sur La Protection des Renseignements Personnels et les Documents Electroniques (LPRPDE), la Norme de Sécurité des Données pour l'Industrie des Cartes de Paiement (PCI DSS) ou autres ?
- Votre profil de menaces : vous trouvez-vous dans une région hostile ou instable, une ville à la criminalité croissante ou un secteur industriel ou dangereux ?

Formation et test des employés

Il est indispensable de former et de sensibiliser à la cybersécurité tous les employés pour éviter qu'ils ne deviennent le maillon faible de la protection des données dans votre entreprise. Il convient de couvrir les thèmes de la sécurité des mots de passe, des courriers indésirables et de l'hameçonnage, de la protection contre les programmes malveillants, des critères de conformité réglementaire et de la protection des données (classification des données, types de données sensibles et technologies de protection des données). Les tests peuvent revêtir de multiples formes de façon à mobiliser les esprits et à renforcer la formation tout au long de l'année.

Réaliser une analyse d'impact relative à la protection des données (AIPD)

L'AIPD est obligatoire dans le cadre du RGPD pour toutes les opérations de traitement des données « susceptibles d'engendrer un risque élevé pour les droits et libertés d'une personne physique ». L'AIPD ressemble au processus de base de gestion des risques traité au Chapitre 2, mais y ajoute des paramètres relatifs au traitement des données personnelles.

Implémentation de la protection des données dès la conception et par défaut

Le RGPD exige la « protection des données dès la conception et par défaut », ce qui signifie que les entreprises doivent mettre en œuvre des mesures techniques et organisationnelles visant à limiter les informations personnelles collectées, traitées et stockées.

PRINCIPES ÉLÉMENTAIRES DE LA PROTECTION DES DONNÉES

Cette approche systématique de la cybersécurité peut vous aider à protéger les précieuses données de votre entreprise. Ce n'est pas si compliqué.

Évaluer les actifs, les risques et les ressources

Répertoriez tous les systèmes et services informatiques que votre entreprise utilise. Si vous ne savez pas ce que vous avez, vous ne pouvez pas le protéger. Pensez à inclure les appareils mobiles comme les smartphones et les tablettes qui servent à accéder aux informations de l'entreprise ou des clients. Ce point est d'autant plus important que le Ponemon Institute estime que 60 % des employés contournent les fonctions de sécurité sur leurs appareils mobiles et que 48 % désactivent les paramètres de sécurité exigés par leur employeur. Et n'oubliez pas les services cloud comme Box, Dropbox, iCloud, Google Docs, Office365, OneDrive et SalesForce.

Ensuite, reprenez votre liste et réfléchissez aux risques associés à chaque ligne. Posez-vous aussi la question de l'utilité de chaque système, logiciel ou service. Qui ou quelle est la menace ? Une autre question intéressante à se poser est : qu'est-ce qui pourrait mal se passer ? Certains risques sont plus vraisemblables que d'autres, mais énumérez-les tous, puis classez-les selon les dommages qu'ils entraîneraient et la probabilité qu'ils se produisent.

Vous aurez peut-être besoin d'aide pendant ce processus : il est temps de dresser une autre liste, celle des ressources sur lesquelles compter pour les questions de cybersécurité… peut-être un membre du personnel qui aime et connaît la cybersécurité, un partenaire ou un fournisseur. Les organisations professionnelles nationales ou les associations régionales d'entreprises disposent aussi de ressources et peuvent offrir de bons conseils. L'organisme National Cyber Security Alliance met gratuitement à disposition des supports de sensibilisation, des fiches conseils et des suggestions de formation pour les employés. Prenez contact avec les autorités de votre pays (vous devriez au moins consigner les noms et les numéros à appeler au cas où vous seriez victime de cybermalveillance).

Élaborer vos politiques

La solidité d'un programme de sécurité est basée sur l'implication de la direction quant à la mise en place de politiques globales sur ce sujet. Les salariés doivent également être sensibilisés sur l'importance que revêt la sécurisation des données traitées. Si vous êtes le relai de ces politiques au sein de votre entreprise, vous devez expliciter ces dernières.

Exemple : Signifier aux salariés qu'aucun accès non autorisé aux systèmes / données de l'entreprise ne sera toléré et que les employés auront interdiction de désactiver les paramètres de sécurité sur leurs applications mobiles.

Choisir ses contrôles

Vous utilisez des contrôles pour assurer l'application des politiques. Par exemple, pour appliquer le principe de tolérance zéro des accès non autorisés aux systèmes et données de l'entreprise, vous pouvez choisir de contrôler tous les accès aux systèmes de l'entreprise à l'aide d'une combinaison unique d'un identifiant, d'un mot de passe et d'un token d'authentification.

Pour contrôler que seuls les programmes autorisés s'exécutent sur les ordinateurs de l'entreprise, vous pouvez décider de ne pas octroyer aux employés les droits d'administration. Pour empêcher toute atteinte aux données à la suite de la perte ou du vol d'applications mobiles, vous pouvez exiger le signalement de tout incident le jour même de son apparition en précisant que les appareils seront verrouillés et leurs données effacées à distance.

Vous avez besoin d'au moins trois technologies de sécurité de base :

- **Un logiciel contre les programmes malveillants** pour empêcher le téléchargement de codes nuisibles comme les virus et les ransomwares sur vos appareils.
- **Le chiffrement** qui rend les données inaccessibles même en cas de vol ou de perte de l'appareil.
- **L'authentification multifacteur** pour ne pas ouvrir l'accès à vos systèmes et données sur la foi d'un simple identifiant et de son mot de passe (par exemple avec l'ajout d'un code à usage unique envoyé sur un téléphone mobile préenregistré).

Déployer les contrôles

Assurez-vous que les contrôles déployés fonctionnent. Par exemple, si une politique interdit tout logiciel non autorisé sur les systèmes de l'entreprise, un des contrôles sera un logiciel qui analyse le code pour détecter les programmes malveillants. Vous devez installer et vérifier par des tests que le scénario ne gêne pas le fonctionnement normal de l'entreprise. Vous devez aussi documenter les procédures à suivre en cas de détection d'un programme malveillant.

Sensibiliser les collaborateurs, les partenaires et les fournisseurs

Les employés ne doivent pas seulement connaître les politiques et procédures de sécurité, ils doivent aussi en comprendre leur utilité. Pour cela, la sensibilisation et la formation s'avèrent souvent la mesure de sécurité la plus efficace à mettre en œuvre.

La collaboration avec vos équipes est la sensibilisation aux problèmes comme l'hameçonnage par e-mail. Dans son Rapport d'enquête 2017 sur les compromissions de données (DBIR), Verizon a montré que 23 % des e-mails d'hameçonnage envoyés aux employés étaient ouverts et 11 % des destinataires ouvraient la pièce jointe, deux comportements qui multiplient les risques d'une violation de données et d'un vol d'informations.

Menez des actions pédagogiques auprès de toute personne qui utilise vos systèmes, notamment la direction, les fournisseurs et les partenaires. Et souvenez-vous qu'une violation des politiques de sécurité doit avoir des conséquences. Une politique non appliquée sape tous les efforts de cybersécurité.

Évaluer, mener des audits et tester sans cesse

La cybersécurité, quelle que soit l'entreprise, grande ou petite, est un processus sans fin. Ce n'est pas un projet ponctuel. Prévoyez une réévaluation régulière, au moins annuelle, de votre sécurité. Tenez-vous informé des menaces émergentes en suivant les contenus informatifs des sites spécialisés tels que WeLiveSecurity.com, KrebsOnSecurity.com et DarkReading.com.

Vous devrez peut-être actualiser vos politiques et contrôles de sécurité plus d'une fois par an en fonction des évolutions de votre activité comme de nouveaux partenariats avec des fournisseurs, de nouveaux projets, de nouvelles recrues ou des départs d'employés (notamment en pensant à révoquer tous les accès des personnes quittant l'entreprise). Envisagez de faire appel à un prestataire pour mener un test d'intrusion et un audit de sécurité afin de découvrir vos points faibles et les traiter.

Contrôles des processus

Les contrôles de processus participent à réduire les répercussions d'une violation ou d'une perte de données sur l'entreprise. Par exemple, selon une étude récente du Ponemon Institute, les entreprises réduisent le coût moyen par enregistrement d'une violation de données de 141 $ à 122 $ si un processus efficace de réponse à incident a été mis en place pour raccourcir les délais d'identification et de circonscription de la violation de données. L'équipe d'intervention en cas d'incident peut être en interne, en sous-traitance chez un partenaire ou formée d'une combinaison des deux. Pour une atteinte aux données touchant 10 000 enregistrements, l'économie moyenne est d'environ 190 000 $, un montant qui vaut largement l'investissement.

Les entreprises doivent tenir compte des aspects suivants lors de création des contrôles de processus.

Mobiliser tout le monde

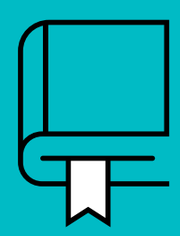
Il ne s'agit pas de suivre une approche hiérarchique. Mobiliser les personnes véritablement impliquées dans les différents processus et la technologie participe à créer des contrôles judicieux dont l'implémentation sera efficace.

Définir les responsabilités

Les responsabilités individuelles doivent être clairement définies et comprises : chacun doit connaître son rôle.

Expliquer l'utilité des contrôles des processus

Les mesures de sécurité sont souvent vécues comme un fardeau ou une gêne. Au bout du compte, elles risquent d'être ignorées ou contournées si les collaborateurs ne comprennent pas leur nécessité et leur importance pour l'activité.



À RETENIR

Selon le Ponemon Institute, il faut en moyenne 191 jours pour repérer une violation de données et 66 pour la contenir. Les délais nécessaires pour identifier et circonscrire la violation de données ont des répercussions directes sur son ampleur et son coût total.

Les entreprises qui créent des processus de transfert sécurisé des données peuvent aussi réduire les coûts d'une violation ou d'une perte de données. Par exemple, toujours selon le Ponemon Institute, le chiffrement réduit en moyenne le coût par enregistrement de 16 $. Dans de nombreux cas, chiffrer ses données et apporter la preuve d'un chiffrement adéquat peut déclencher une exonération de responsabilité aux termes de nombreuses réglementations sur la protection des données. Les entreprises qui suivent cette voie échappent à l'obligation de notification des violations de données : les coûts aussi bien directs (notifications, services de surveillance du crédit, litiges, etc.) qu'indirects (détérioration de l'image de marque et perte de clientèle) en sont considérablement réduits. Encore une fois, si 10 000 enregistrements sont concernés, le chiffrement peut réduire le coût total de la violation de données d'environ 160 000 $.

Parmi les contrôles de processus importants, citons les suivants :

Politiques de contrôle d'accès

Elles définissent les personnes autorisées à accéder à chaque système, application et jeu de données et les finalités de ces accès.

Gestion des actifs et ressources

Il est essentiel de savoir ce que vous protégez et pour quelles raisons (valeur ou risque pour l'entreprise). Au-delà d'un inventaire exact des actifs, ressources de données et supports informatiques, les entreprises doivent assurer une bonne hygiène numérique. Pour cela, il leur faudra actualiser leurs systèmes / applications avec les correctifs de sécurité les plus récents, et supprimer sans délai les données sensibles non-utiles à leur activité conformément aux politiques établies de rétention, d'archivage et de destruction des données.

Gestion des changements

Elle garantit que les modifications apportées aux systèmes / applications sont consignées, testées et validées afin de pouvoir mesurer l'impact d'un changement par rapport à l'approche sécuritaire globale de l'entreprise.

Réponse aux incidents

En cas d'incident de sécurité comme une violation de données ou une attaque, les entreprises doivent disposer d'un plan de réponse aux incidents clairement défini. L'objectif est de garantir une intervention rapide et efficace, notamment quant à la limitation des dégâts, la reprise, la conservation des preuves, les communications internes / externes et l'analyse des causes profondes.

Continuité de l'activité

Un plan de continuité de l'activité réduit les répercussions commerciales d'une interruption de service et permet de poursuivre l'exploitation jusqu'au retour complet à la normale.

Enfin, les entreprises peuvent s'appuyer sur des services de sécurité spécialisés en plus de leurs capacités internes. Ces activités comprennent la surveillance et le renseignement au quotidien ainsi que la détection, la remontée de problèmes et l'intervention en cas d'incident. Elles revêtent une importance particulière dans le cadre des investigations et de l'analyse post-incident.

À RETENIR

Les contrôles organisationnels et des processus mis en œuvre doivent correspondre au niveau du risque.

Dans ce chapitre

- Contrôles administratifs : vos premiers pas
- Savoir ce que vous protégez et pour quelles raisons
- Mettre en œuvre des contrôles techniques
- Assurer la sauvegarde et la restauration, la réponse aux incidents et la reprise de l'activité
- Collaborer avec vos utilisateurs et les experts en cybersécurité

Chapitre 6

10 CLÉS POUR UNE PROTECTION DES DONNÉES EFFICACE

Dans ce chapitre, nous allons traiter dix bonnes pratiques de sécurité pour vous aider à mettre en œuvre une protection des données efficace dans l'entreprise.

Créer des politiques de sécurité

Beaucoup d'entreprises ne pensent pas à formaliser leurs politiques de sécurité et passent directement aux contrôles techniques ; Comme par exemple à un pare-feu, une protection des terminaux ou autres, pouvant être implémentés sans contrôles administratifs – à savoir sans politiques ou procédures – sont généralement mis en œuvre à posteriori en l'absence d'une stratégie de sécurité réfléchie, fédératrice et complète et d'un cadre de gestion de la sécurité (que vos politiques aident à dessiner avec l'analyse de la sécurité des informations). Des dépenses supplémentaires sont alors inévitablement engagées dans des solutions techniques mal ou peu efficacement déployées et à la protection insuffisante ou inadaptée.

Identifier vos actifs

Vous devez savoir ce que vous protégez : il faut donc tenir à jour un inventaire précis de tous vos logiciels et matériels informatiques. Sans la liste complète, vous risquez d'omettre certains systèmes vulnérables de votre réseau et d'augmenter votre exposition aux attaques. Par exemple, lors de la violation de données dont a été victime le groupe américain de grande distribution Target en 2013, les attaquants ont accédé à distance à un système de maintenance de la climatisation réversible (HVAC) pour finalement atteindre les informations de carte bancaire et les données personnelles de 110 millions de clients. Pour commencer, il existe de nombreux outils gratuits pour scanner votre réseau et vos terminaux. Vous trouverez des solutions commerciales pour vous aider à tenir à jour en permanence l'inventaire de vos actifs. Beaucoup d'entre elles apportent en outre des fonctionnalités de gestion à distance pour l'installation, la suppression et la mise à jour des logiciels. Vous devez réduire la surface d'attaque de tous vos actifs connectés à internet, y compris les appareils mobiles personnels, en y installant une protection appropriée à actualiser régulièrement.

Connaître votre approche de la sécurité

Il s'agit simplement de créer une feuille de route ou un modèle de maturité qui indique votre état actuel et, en suivant l'approche par les risques, de relever les menaces vraisemblables à l'encontre des actifs de votre environnement (voir le conseil précédent) et les mesures de protection des données et de cybersécurité appropriées. Vous pouvez ensuite mener une analyse des écarts pour déterminer les dispositions à prendre et les investissements à réaliser. Reportez-vous au Chapitre 3 pour plus d'informations sur l'évaluation des risques de sécurité des données.

Classer toutes vos données

Dans beaucoup d'entreprises, les données client sensibles et d'autres informations confidentielles représentent les « joyaux de la couronne », mais pour des raisons notamment pratiques, toutes les données n'ont pas à bénéficier de la même protection ou de contrôles identiques. Réfléchissez plutôt à définir les données dont le vol ou la perte vous feraient perdre le sommeil. Quelles seraient les répercussions d'une violation de données sur votre image de marque, sur la fidélité de vos clients et même sur la viabilité de votre entreprise ? Créez et documentez des règles intuitives de classification des données qui précisent les étiquettes de classement (« réservé à l'usage interne », « données sensibles » et « diffusion publique autorisée ») et les obligations de protection des données (chiffrement, sauvegarde, autorisation de diffusion et destruction) selon les différentes catégories.

CONSEIL

Le règlement général sur la protection des données (RGPD) impose aux organisations de supprimer les données à caractère personnel sur demande de la personne concernée. Pour commencer à répondre à ces critères, concevez votre stratégie de classification des données de manière à identifier ou signaler les données personnelles, notamment les copies de sauvegarde, appelées à être supprimées ou modifiées à l'avenir.

Chiffrer vos données sensibles

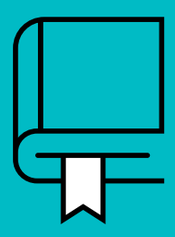
Le chiffrement de données convertit des données en texte clair en un format illisible dit « cryptogramme » le rendant inexploitable par des tiers non autorisés qui ne possèdent pas les clés de chiffrement et de déchiffrement. Le secret d'un chiffrement efficace réside dans la protection de ces clés. A minima, il faut chiffrer les données au repos (stockées). On peut ajouter un chiffrement aux données « en mouvement » ou « en transit », par exemple un chiffrement SSL (Secure Sockets Layer). Enfin, utilisez, s'il existe, le chiffrement intra-applicatif pour les données en cours d'utilisation. Le chiffrement peut être matériel ou logiciel.

CONSEIL

De nombreuses réglementations sur la violation des données incluent des clauses d'exonération applicables aux données chiffrées qui peuvent réduire considérablement le coût et les répercussions d'une violation de données.

Sauvegarder, récupérer les données et tester

S'assurer de sauvegardes régulières et fiables des systèmes et données, tel est le socle des bonnes pratiques de sécurité. Une bonne sauvegarde garantit de pouvoir récupérer un fichier accidentellement supprimé ou un disque dur corrompu. Les coûts des sauvegardes sur disque ne cessent de baisser et les solutions en cloud sont faciles et économiques : il n'y a aucune excuse de ne pas en faire. Avec l'essor des ransomwares ces dernières années, les sauvegardes sont le seul moyen de récupérer ses données en cas d'attaque. En plus, vous n'aurez pas à payer la rançon.



À RETENIR

Vous devez tester régulièrement votre capacité à récupérer vos systèmes et données critiques à partir de vos sauvegardes. Vous vérifiez ainsi que celles-ci ne sont pas corrompues, et que vous et vos équipes connaissez le processus de reprise.

Investir dans la protection des terminaux

« Investir » ne signifie pas télécharger un antivirus gratuit sur internet, mais protéger tous vos terminaux, stations de travail, appareils mobiles, serveurs, à l'aide d'une solution de protection robuste des terminaux. De nos jours, les données sont partout et, plus que jamais, les terminaux sont l'endroit où tout se recoupe. Ils valent donc la peine qu'on y investisse.

Planifier et se préparer

Toute entreprise doit avoir des plans de réponse aux incidents, de continuité d'activité et de reprise d'activité. Votre équipe d'intervention en cas d'incident doit être formée aux procédures élémentaires d'analyse post-incident. L'objectif est de traiter chaque incident de sécurité comme s'il allait entraîner des suites judiciaires et de s'assurer de l'intégrité de la chaîne de contrôle à des fins de preuve. Les plans de continuité de l'activité et de reprise sur incident aident votre entreprise à reprendre une activité commerciale normale au plus vite après un sinistre ou un événement majeur. Enfin, la précision et la rapidité de votre communication, interne comme externe, en sont un élément essentiel.

Former vos utilisateurs

Dans toute entreprise, le maillon faible de la sécurité a toujours été l'utilisateur final, mais il n'en est pas forcément responsable. Il y a peu de chance qu'aucun de vos employés n'ait été recruté sur son expertise en cybersécurité. Les attaquants le savent bien. Ils utilisent des techniques de manipulation pour amener les utilisateurs innocents, entre autres, à cliquer sur des liens malveillants dans des e-mails indésirables ou d'hameçonnage, à révéler leurs mots de passe (voir « Comment créer un mot de passe fort ? » ci-dessous) et à visiter des sites web malveillants. Animez régulièrement de brefs exercices pertinents et mobilisateurs pour sensibiliser vos utilisateurs à la cybersécurité : leur sécurité est la vôtre !

Ne pas rester "seul"

Les cybercriminels ne sont pas solitaires. Ils s'allient à d'autres personnes peu recommandables pour atteindre leurs objectifs et réutilisent du code malveillant qu'ils se sont procuré sur le « dark web ». Ils enrôlent aussi à leur insu des victimes dont les terminaux piratés, devenus machines zombies, rejoignent une armée de botnets pour cibler d'autres victimes. Mais rassurez-vous, vous n'êtes pas seuls non plus ! Appuyez-vous sur la grande famille des experts en sécurité : des forces de l'ordre aux associations professionnelles en passant par les services de sécurité managés et en sous-traitance, le renseignement cloud sur les menaces en temps réel et bien plus encore.

COMMENT CRÉER UN MOT DE PASSE FORT ?

La moindre activité en ligne exige de se connecter et, à chaque fois, de s'authentifier pour vérifier que nous sommes bien la personne que nous prétendons être. Votre mot de passe doit donc être aussi unique et complexe que vous ! Voici quelques conseils.

UTILISEZ de longs mots de passe et phrases secrètes

Comptez au moins 8 caractères dans un mot de passe, mais sa longueur ne doit pas vous empêcher de le retenir (voir la suite des conseils). Pensez également à vérifier que votre mot de passe n'a pas été dévoilé suite à une fuite de données. Pour cela, consultez le site https://haveibeenpwned.com/Passwords.

UTILISEZ des phrases uniques et des caractères spéciaux

Une courte phrase d'au moins une trentaine de caractères – peut-être avec quelques chiffres, des lettres capitales et de la ponctuation – sera plus facile à retenir qu'un mot de 8 caractères avec des substitutions classiques comme le « 3 » à la place du « E ».

UTILISEZ un gestionnaire de mots de passe (gratuit ou payant)

Un gestionnaire de mots de passe s'avère utile pour créer, stocker, gérer et se rappeler des mots de passe forts et uniques qui ouvrent l'accès à vos différents appareils, systèmes et applications. Il vous évite aussi la pratique courante d'écrire vos mots de passe sur un papier ou une note autoadhésive.

UTILISEZ des mots de passe que vous arrivez à retenir

Les mots de passe aléatoires, trop complexes et difficiles à retenir, peuvent se révéler contre-productifs et affaiblir la sécurité du compte. En effet, ils encouragent de mauvaises pratiques comme de noter les mots de passe ou de les réutiliser dans différents comptes professionnels et personnels.

UTILISEZ l'authentification multifacteur (MFA)

Dès que possible, activez l'authentification multifacteur pour vos comptes en plus ou à la place des mots de passe. La MFA exploite au moins deux facteurs d'authentification (un facteur mémoriel comme votre identifiant ou le mot de passe, et un facteur matériel comme un dispositif matériel ou logiciel ou un smartphone). Quand vous vous connectez à un compte à authentification multifacteur, un code à usage unique est généré par le dispositif ou envoyé par SMS à votre smartphone. Le code n'est pas réutilisable et ne fonctionne que pendant un court laps de temps, généralement de une à cinq minutes. Cette méthode rend extrêmement difficiles l'interception du code et sa réutilisation pour accéder à votre compte à votre insu avant l'expiration du code.

N'UTILISEZ JAMAIS deux fois le même mot de passe, même s'il est très bon

Si votre mot de passe est compromis à un endroit, par exemple votre compte de messagerie Yahoo!, les cybercriminels essaieront de l'utiliser ailleurs, par exemple pour accéder à votre banque en ligne.

NE COMMUNIQUEZ JAMAIS un mot de passe à quiconque !
Vos mots de passe sont encore plus sacrés que votre brosse à dents, que vous pouvez parfois partager avec votre conjoint.

N'UTILISEZ JAMAIS de mots du dictionnaire
Les programmes de piratage automatisé de mots de passe recourent facilement aux dictionnaires, même en langues étrangères ou dans différents domaines comme le médical, le juridique ou la construction. Évitez aussi les répétitions de caractères, par exemple « aaaa », une séquence « 1234 » ou des modèles reconnaissables comme « azerty ».

N'UTILISEZ JAMAIS d'informations personnelles dans votre mot de passe
Les réseaux sociaux facilitent la quête de renseignements des cybercriminels : ils y trouvent votre deuxième prénom, votre date de naissance, votre adresse, votre école, le nom de votre enfant ou de votre partenaire et même le lieu de vos dernières vacances !

GLOSSAIRE

Adware

Programmes publicitaires intempestifs généralement installés avec des logiciels gratuits ou partagés, et parfois considérés comme une forme de malware. Voir aussi malware.

Attaque d'annuaire (Directory Harvest Attack - DHA)

Une technique de force brute utilisée par les spammeurs pour tenter de trouver des adresses e-mail valides dans un domaine.

Attaque par déni de service (distributed denial-of-service - DDoS)

Une attaque à grande échelle qui utilise généralement des bots dans un botnet pour planter un réseau ou un serveur ciblé. Voir aussi bot et botnet.**Bot**
Un ordinateur cible infecté par des logiciels malveillants et faisant partie d'un botnet. Voir aussi botnet et malware.

Backdoor

Malware qui permet à un attaquant de contourner l'authentification normale pour accéder à un système compromis. Voir aussi malware.

Bombe logique

Un programme malveillant, ou une partie de celui-ci, conçu pour exécuter une fonction malveillante lorsqu'une circonstance prédéterminée se produit (date système, lancement d'une commande, etc.)

Bootkit

Une variante de malware représentant le noyau d'un rootkit, couramment utilisée pour attaquer les ordinateurs protégés par un chiffrement complet du disque. Voir aussi malware et rootkit.

Bot

Un ordinateur cible infecté par des logiciels malveillants et faisant partie d'un botnet. Voir aussi botnet et malware.

Botnet

Un vaste réseau d'appareils infectés (bot) par des logiciels malveillants travaillant ensemble et contrôlés par un attaquant via des serveurs de commande et de contrôle (C2). Voir aussi bot et malware.

BYOD (bring your own device)

Une politique sur les appareils mobiles qui permet aux employés d'utiliser leurs appareils mobiles personnels, tels que les smartphones et les tablettes, sur le lieu de travail pour une utilisation professionnelle et personnelle.

Cheval de Troie

Un programme malveillant qui prétend exécuter une fonction donnée, mais remplit plutôt une autre fonction (généralement malveillante). Voir aussi malware.

Chiffrement (Encryption)

Processus de transformation du texte chiffré en texte brut afin d'en rendre la compréhension impossible à toute personne ne possédant pas la clé de déchiffrement. Voir aussi texte chiffré et texte en clair.

Cryptomonnaie

Un actif numérique qui utilise la cryptographie pour sécuriser les transactions, contrôler la création d'unités supplémentaires et vérifier le transfert des actifs. Le Bitcoin est un exemple populaire de crypto-monnaie.

Empoisonnement du cache DNS

Un type d'attaque, également connu sous le nom d'usurpation DNS, qui exploite les vulnérabilités du DNS pour détourner le trafic Internet des serveurs de destination légitimes vers de faux serveurs. Voir aussi DNS (Domain Name System).

Endpoint (Terminal / poste de travail)

Un appareil informatique d'utilisateur final, tel qu'un ordinateur de bureau ou portable, une tablette ou un smartphone.

Exploit

Logiciel ou code qui tire parti d'une vulnérabilité dans un système d'exploitation (OS) ou une application et provoque un comportement involontaire dans le système d'exploitation ou l'application, comme une élévation de privilèges, un contrôle à distance ou un déni de service.

Hameçonnage (phishing)

Une technique d'ingénierie sociale dans laquelle un e-mail qui semble provenir d'une entreprise légitime (telle qu'une institution financière) tente d'inciter le destinataire à cliquer sur un lien incorporé dans l'e-mail ou à ouvrir une pièce jointe contenant un malware ou un exploit. Le lien intégré redirige le navigateur du destinataire vers un site Web malveillant pour saisir des informations personnelles sensibles (telles que les informations de compte). Alternativement, le site Web malveillant peut diffuser des logiciels malveillants ou utiliser un exploit en arrière plan du navigateur sur l'appareil de la victime. Voir également le téléchargement en voiture, ou sur vos terminaux de logiciels malveillants.

Health Insurance Portability and Accountability Act (HIPAA)

Applicable à toute organisation qui traite ou stocke des informations de santé protégées (PHI) aux Etats-Unis. Protège la confidentialité des patients et la confidentialité des données.

Ingénierie sociale

Une méthode d'attaque à faible technologie qui utilise des techniques telles que l'espionnage par-dessus l'épaule et la plongée dans une benne à ordures pour obtenir des informations sensibles, telles que des mots de passe, d'un utilisateur.

Internet protocol (IP)

Le protocole de communication principal de la suite de communications TCP / IP pour le routage à travers les frontières du réseau (routeurs) et Internet. Voir aussi Protocole TCP (Transmission Control Protocol).

Les informations de santé protégées (protected health information - PHI)

Toute information sur la santé, la fourniture de soins de santé ou le paiement de soins de santé créé ou collecté par une organisation, comme un fournisseur de soins de santé, un assureur ou une autre entité de ce type, qui peut être liée à une personne spécifique..

Loi sur la protection des renseignements personnels et les documents électroniques (Personal Information Protection and Electronic Documents Act - PIPEDA)

Applicable aux organisations qui font affaire avec des citoyens canadiens. Protège la confidentialité des renseignements personnels des citoyens canadiens.

Malware (logiciel malveillant)

Logiciels ou codes malveillants qui endommagent ou désactivent généralement, prennent le contrôle ou volent des informations d'un système informatique. Les malwares incluent largement les virus, vers, chevaux de Troie, bombes logiques, ransomwares, rootkits, bootkits, backdoors, spywares et adwares.

Manipulation de l'espace des noms de domaine (DNS hijacking)

Une technique d'attaque utilisée pour rediriger les requêtes DNS loin des serveurs DNS légitimes. Voir aussi Système de noms de domaine (DNS).

Métamorphisme

Une technique utilisée pour réécrire le code du malware à chaque itération afin que chaque nouvelle version soit différente de la version précédente. Voir aussi malware et polymorphisme.

Norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry (PCI) Data Security Standards (DSS))

Applicable à toute entreprise qui accepte, traite ou stocke les transactions par cartes de paiement (telles que les cartes de crédit, de débit et les cartes de paiement).

Organisation internationale de normalisation (International Organization for Standardization - ISO)

Un organisme international de création de normes. ISO est dérivé du mot grec «isos», qui signifie égal.

Polymorphisme

Une technique utilisée pour réécrire une partie du code malveillant à chaque itération afin que chaque nouvelle version soit légèrement différente de la version précédente. Voir aussi malware et métamorphisme.

Port hopping

Une technique utilisée par les applications pour améliorer l'accessibilité, mais également utilisée dans les cyberattaques pour commuter dynamiquement les ports TCP, disséminer les flux de communication et, ainsi, échapper à la détection. Voir aussi TCP (Transmission Control Protocol).

Ransomware (Rançongiciel)

Logiciel malveillant qui chiffre les données d'une victime et lui demande de payer une rançon spécifiée (généralement en crypto-monnaie) pour décrypter les données (bien que le paiement d'une rançon ne garantisse pas que les données de la victime seront décryptées). Voir aussi crypto-monnaie et malware.

Règlement général sur la protection des données - RGPD (General Data Protection Regulation - GDPR)

Applicable à toute organisation faisant affaire avec des citoyens de l'UE. Renforce la protection des données pour les citoyens de l'UE et traite de l'exportation de données personnelles en dehors de l'UE.

Réseau local virtuel (VLAN)

Un domaine de diffusion partitionné et isolé dans un réseau local.

Réseau privé virtuel (VPN)

Un réseau privé utilisé pour communiquer en privé sur des réseaux publics. Les VPN utilisent le chiffrement et l'encapsulation pour protéger et simplifier la connectivité.

Rootkit

Malware qui fournit un accès privilégié (au niveau racine) à un ordinateur. Voir aussi malware.

Secure Sockets Layer (SSL)

Un protocole de couche transport qui fournit un chiffrement et une authentification basés sur la session pour une communication sécurisée entre les clients et les serveurs sur Internet.

Spam

Courriel en masse non sollicité qui est couramment utilisé pour propager des logiciels malveillants via des liens ou des pièces jointes malveillants. Voir aussi malware.

Spear phishing

Une tentative de phishing ciblée qui semble plus crédible à ses victimes et qui a donc une plus grande probabilité de succès. Par exemple, un e-mail de spear phishing peut usurper une organisation ou un individu que le destinataire connaît. Voir aussi phishing.

Spyware

Logiciels malveillants qui collectent des informations sur une personne ou une organisation à leur insu ou sans leur consentement. Voir aussi malware.

SSL hiding

Une technique qui utilise le cryptage SSL (Secure Sockets Layer) pour masquer le contenu du trafic réseau, par exemple, pour échapper à la détection par les défenses du réseau tout en volant des données sensibles (appelées exfiltration de données).

Système de détection d'intrusion (IDS)

Une application matérielle ou logicielle qui détecte les intrusions suspectées sur le réseau ou l'hôte.

Système de noms de domaine (DNS)

Une base de données hiérarchique décentralisée pour les ordinateurs, les services et autres ressources connectées à un réseau ou à Internet qui fournit la correspondance des adresses IP numériques avec les noms de domaine, ainsi que d'autres informations. Voir aussi Protocole Internet (IP).

Système de prévention d'intrusion (IPS)

Une application matérielle ou logicielle qui détecte et bloque les intrusions suspectées sur le réseau ou l'hôte.**Unified threat management (UTM)**
Un dispositif de sécurité qui intègre diverses fonctionnalités de sécurité telles que le pare-feu, l'anti-malware et les capacités de prévention des intrusions sur une seule plateforme.

Téléchargement furtif (drive-by download)

Logiciels, souvent des logiciels malveillants, téléchargés sur un ordinateur à partir d'Internet à l'insu ou sans l'autorisation de l'utilisateur. Voir aussi malware.

Texte brut (Plain text)

Un message dans son format lisible d'origine ou un message chiffré qui a étécorrectement déchiffré pour produire le message lisible d'origine. Voir aussi texte chiffré et déchiffrement.

Texte Chiffré

Un message en clair qui a été chiffré en un message brouillé qui est inintelligible sans la clé de déchiffrement appropriée. Voir aussi déchiffrement, chiffrement et texte en clair.

Transmission Control Protocol (TCP)

L'un des principaux protocoles de la suite Internet Protocol, TCP est l'un des deux composants originaux de la suite, complétant le protocole Internet (IP), et par conséquent, la suite entière est communément appelée TCP / IP. TCP fournit une livraison ordonnée et fiable d'un flux d'octets d'un programme sur un ordinateur à un autre programme sur un autre ordinateur. TCP est le protocole sur lequel s'appuient les principales applications Internet telles que le World Wide Web, le courrier électronique, l'administration à distance et le transfert de fichiers. Voir aussi Protocole Internet (IP).

Trojan de type RAT (cheval de Troie pour les connexions à distance)

Un programme malveillant qui comprend une porte dérobée pour fournir le contrôle administratif d'un ordinateur cible.

Un pare-feu de nouvelle génération (next-generation firewall - NGFW)

Une plate-forme de sécurité réseau qui intègre pleinement les fonctionnalités traditionnelles de pare-feu et de prévention des intrusions réseau avec d'autres fonctions de sécurité avancées qui offrent une inspection approfondie des paquets (DPI) pour une visibilité complète, une application précise, le contenu et l'identification des utilisateurs, et un contrôle granulaire basé sur des politiques. Voir aussi système de prévention des intrusions (IPS).

Unified threat management (UTM)

Un dispositif de sécurité qui intègre diverses fonctionnalités de sécurité telles que le pare-feu, l'anti-malware et les capacités de prévention des intrusions sur une seule plateforme.

Uniform Resource Locator (URL)

Une adresse web.

Vers (Worm)

Malware qui a généralement la capacité de se répliquer d'un ordinateur à l'autre sans avoir besoin d'interaction humaine. Voir aussi malware.

Virus

Un programme malveillant dont l'objectif principal est de s'incorporer dans un autre programme informatique afin de se répliquer. Voir aussi malware.

Vulnérabilité

Un bogue ou une faille dans un logiciel qui crée un risque de sécurité qui pourrait être exploité par un attaquant. Voir aussi exploiter.

Web application firewall (WAF)

Un pare-feu conçu pour protéger les applications Web et les serveurs Web.

VOS DONNEES SONT SOURCES DE REVENUS

PROTÉGEZ VOTRE ENTREPRISE DE TOUTES TENTATIVES DE VIOLATION DE DONNÉES. NOTRE SOLUTION, ESET ENDPOINT ENCRYPTION, EST FACILE À DÉPLOYER ET ASSURE LA SÉCURITÉ DE VOS TERMINAUX.

- ✔ Chiffrez en toute sécurité les disques durs, les supports amovibles, les fichiers et les e-mails
- ✔ Renforcez la sécurité de vos informations et respectez le RGPD
- ✔ Ajoutez une couche de sécurité supplémentaire avec ESET Secure Authentication

VISITEZ NOTRE SITE WEB ESET POUR PLUS D'INFORMATIONS.

CYBERSECURITY
EXPERTS ON YOUR SIDE

WWW.ESET.COM/FR

CYBERSECURITY
EXPERTS ON YOUR SIDE

WWW.ESET.COM/FR

Nos remerciements à Lawrence Miller pour la préparation de ce livre électronique et à Marie-Louise Desfray et Virginie Walbrou pour la traduction en français.