ivanti

Que faire AVANT que le ciel ne vous tombe sur la tête :

La cybersécurité face aux menaces extrêmes d'aujourd'hui

Table des matières

Votre sécurité est plus que jamais menacée 3
L'utilisateur : l'éternel maillon faible 4
Alors, quel est le coût réel des cyberattaques modernes ? 4
Concentrez-vous sur vos clients et vos serveurs. 4
Stratégies de sécurité mal ciblées ? Elles ne servent qu'à entraîner de lourdes dépenses. 5
Les correctifs ? Eh non, le problème n'est toujours pas résolu... 5
Autres problèmes signalés par nos clients 6
Le futur ? Des malwares transformés en armes. 6
Des stratégies de sécurité bien ciblées : La clé du succès IT 7
Progressez grâce au CIS 8
Renforcez vraiment votre sécurité, rapidement, grâce aux 5 principaux contrôles CSC 8
Nos solutions de protection en profondeur 9
Nous pouvons aussi vous aider à consulter les résultats 9
Conclusion 10

Introduction

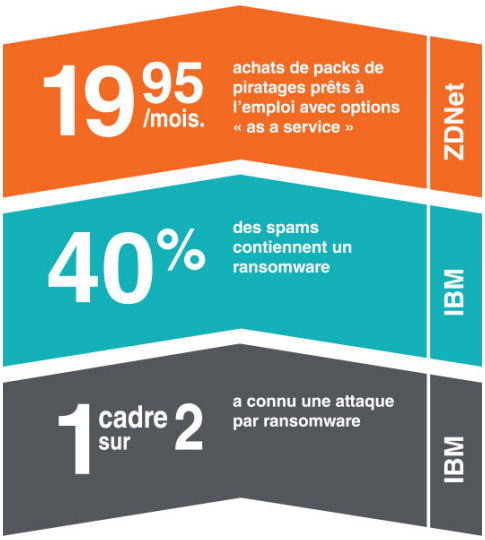
Rien qu'aux États-Unis, on a relevé plus de 500 fuites de données divulguées publiquement en 2016 (près du double de l'année précédente).[1] En février 2017, le cabinet de recherche Opinium a découvert que 78 % des décideurs IT interrogés aux États-Unis et en Europe avaient subi au moins une attaque par ransomware dans leur entreprise au cours de l'année écoulée. Les Shadow Brokers, le groupe de pirates qui a exposé la vulnérabilité ayant favorisé le tristement célèbre WannaCry, a promis d'en divulguer d'autres à intervalle régulier... et il tient déjà parole. Le monde entier a maintenant connu sa première rançon de plus d'un million de dollars divulguée publiquement.[2] Et le virus NotPetya vient de nous montrer à quoi pourraient ressembler les malwares agressifs du futur. Et voilà qu'apparaît Equifax...

Comment stopper cette vague de terreur ? Sans une stratégie de sécurité ciblée, la multiplication des périphériques coûte cher... et est incontrôlable. Les équipes IT passent bien trop de temps à gérer ces périphériques. Sans parler du manque flagrant de personnel de cybersécurité expérimenté... Les entreprises sont contraintes d'optimiser leur personnel de sécurité, et il devient évident qu'une stratégie de sécurité qui exploite des technologies exhaustives, qui simplifie la gestion et qui cible les bases de la sécurité les plus efficaces pour vous protéger des attaques « de la vraie vie » est une solution bien plus avantageuse que les autres.

Lorsque l'on sait que 93 % des fuites de données entraînent des dommages pour l'entreprise en seulement quelques minutes, voire moins,[3] il est évident que vous ne pouvez pas vous permettre de faire le mauvais choix pour la sécurisation de votre entreprise.

Votre sécurité est plus que jamais menacée

Toutes les menaces de cybersécurité les plus sérieuses se multiplient.[4] Ce n'est pas vraiment une surprise, n'est-ce pas ? Mais quelle en est précisément la cause ?



Inutile de nous perdre dans ce labyrinthe pour l'instant. Il suffira de dire que l'enjeu est énorme, surtout lorsqu'on sait qu'il est plus facile que jamais de s'improviser pirate. Les kits d'exploitation modernes, par exemple, simplifient les cyberattaques même pour les pirates inexpérimentés. Ces jeux d'outils malveillants contiennent du code d'exploitation prédéfini : plus besoin de savoir comment cela fonctionne. Souvent, une simple interface Web permet aux utilisateurs dotés d'une licence de se connecter, et d'afficher les victimes actives et des statistiques. Ces kits incluent même parfois un contrat de support et des mises à jour, comme un logiciel commercial légal.

De la même manière, le phénomène est lié à la très grande disponibilité actuelle d'outils sophistiqués initialement prévus pour le cyberespionnage et la guerre informatique.

Le ransomware, par exemple, a évolué : les simples piratages « pour faire peur » sont devenus des malwares à l'échelle de l'entreprise, reposant sur des outils dérobés à la NSA (Agence nationale de sécurité des États-Unis)

capables de prendre des ordinateurs en otage et de bloquer des systèmes entiers. Si l'on combine cela avec le fait que presque 40 % de tous les spams envoyés en 2016 contenait un ransomware,[5] il devient évident qu'un utilisateur peu méfiant peut à tout moment cliquer là où il ne faut pas et mettre en danger l'entreprise.

IBM X-Force a montré qu'un cadre sur deux a connu une attaque par ransomware sur son lieu de travail. Cela représente près de la moitié des cadres de votre entreprise.[6]

L'utilisateur : l'éternel maillon faible

Le rapport DBIR (Data Breach Investigations Report) de Verizon est l'un des rapports annuels les plus réputés de l'industrie de la sécurité. L'équipe RISK (Reasearch, Investigations, Solutions and Knowledge) de Verizon est l'une des plus grandes entités d'investigation IT du monde. Elle partage chaque année des informations très complètes sur l'état de la cybersécurité pour l'année en cours, y compris les principales tendances.

En 2017, cette équipe a découvert que l'hameçonnage est impliqué dans plus de 90 % des incidents et failles de sécurité.[7]

Et c'est au même rythme alarmant que les utilisateurs et leurs nombreux périphériques sont victimes de ransomwares et autres malwares via ces attaques qui ciblent l'utilisateur. D'après Verizon, 30 % des messages d'hameçonnage ont été ouverts en 2016 (contre seulement 23 % l'année précédente) et, dans 12 % des cas, un utilisateur avait cliqué pour ouvrir la pièce jointe ou le lien malveillant.[8]

Le rapport DBIR Verizon 2016 met en évidence l'émergence d'une attaque par hameçonnage en trois phases :

- L'utilisateur reçoit un e-mail d'hameçonnage contenant une pièce jointe malveillante ou un lien vers un site Web nocif.
- L'utilisateur télécharge le malware, que des pirates peuvent utiliser pour rechercher des secrets et des informations internes, pour voler les références d'authentification de plusieurs applications via un enregistreur de frappe ou crypter des fichiers afin de demander une rançon.
- Les pirates peuvent également utiliser les références d'authentification pour des attaques plus poussées : par exemple, pour la connexion à des sites Web tiers comme des sites de banque ou de vente.

Alors, quel est le coût réel des cyberattaques modernes ?

Selon les estimations du FBI, les pirates ont récupéré 209 millions de dollars, rien qu'au premier trimestre 2016, et ces rançons pourraient atteindre 1 milliard de dollars d'ici la fin de l'année.[9] Depuis, le phénomène empire. En fait, notre planète vient de connaître sa première rançon de plus d'un million de dollars.[10]

Aujourd'hui, toutefois, les malwares (même les ransomwares) ne visent pas seulement à faire de l'argent.

En fait, bien que WannaCry n'ait pas permis de récolter autant d'argent (on comptait environ 135 000 dollars américains au 28 juin 2017), ce ransomware a été un énorme succès en matière de propagation : en une seule journée, il a infecté plus de 230 000 ordinateurs dans plus de 150 pays. Et, pour les entreprises, le coût allait bien au-delà du montant de la rançon, qui en aucun cas, n'a anéanti ces entreprises. Le paiement de la rançon ne garantit aucunement le succès et la récupération des données perdues. En outre, dans tous les cas, les vrais dommages subis sont les temps d'inactivité, les données corrompues, la productivité perdue et les perturbations des activités normales après l'attaque, l'enquête post-mortem, et la restauration des données et des systèmes... sans parler de l'énorme coup porté à la réputation de l'entreprise auprès des clients, partenaires et acteurs de la chaîne d'approvisionnement, ou de l'éventualité d'une amende si votre entreprise est déclarée coupable d'un manque de conformité.

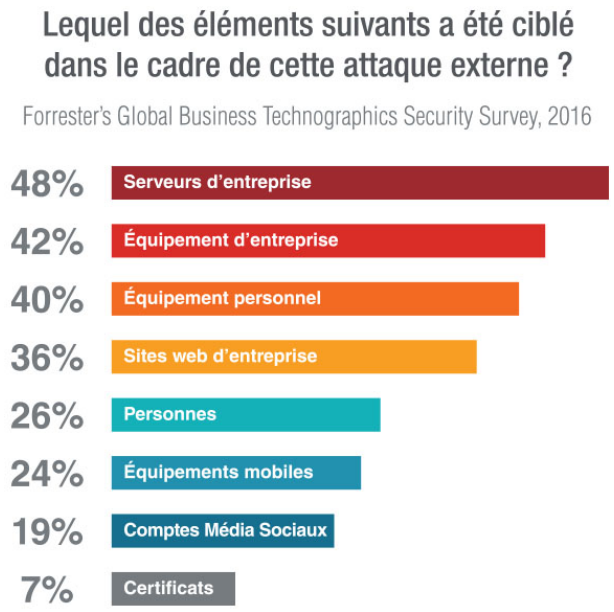
FedEx, l'entreprise pharmaceutique Merck et le géant de l'expédition Maersk en sont des exemples flagrants. Tous ont été frappés par NotPetya cette année et tous ont admis qu'ils se battaient encore pour se remettre de ces attaques, des semaines et même des mois après qu'elles aient eu lieu. FedEx pensait que ses systèmes seraient pleinement opérationnels fin septembre, soit 3 mois après l'attaque, au prix de 300 millions de dollars.[11] Maersk évalue ses coûts au même montant[12] et Merck annonce 200 à 300 millions de dollars.[13]

Concentrez-vous sur vos clients et vos serveurs

Comment donc se fait-il que les plus grandes entreprises du monde, dont tout le monde pense qu'elles sont toutes puissantes et disposent des meilleurs outils de sécurité existants, peuvent être victimes de ces attaques ?

Premièrement, un grand nombre des outils en place ne protègent pas les biens les plus vulnérables.

Dans son enquête de 2016 « Global Business Technographics® Security », Forrester a interrogé 192 décideurs chargés de la sécurité réseau, dont les entreprises (de plus de 1 000 personnes) ont subi une faille de sécurité externe au cours des 12 derniers mois. Au cours de cette enquête, les personnes ont été interrogées sur les aspects de leur infrastructure qui ont été ciblés par l'attaque externe. Les résultats sont sans équivoque : ce sont les clients et les serveurs de vos réseaux qui doivent être votre principale priorité, et non le périmètre de votre environnement IT.



Stratégies de sécurité mal ciblées ? Elles ne servent qu'à entraîner de lourdes dépenses.

Malheureusement, même si vous disposez des bons outils pour vous protéger de ces menaces, ce n'est qu'une petite partie des éléments qu'il vous faut configurer et gérer au quotidien.

Pare-feux réseau, pare-feux d'application Web, systèmes de prévention des intrusions, analyseurs de vulnérabilités... La prolifération des périphériques coûte cher et les équipes IT passent bien trop de temps à gérer ces périphériques... du temps qu'elles ne passent pas avec le département Sécurité pour prévenir les vraies menaces qui visent leur environnement et pour y réagir.

Les correctifs ? Eh non, le problème n'est toujours pas résolu...

Et même si les bons outils sont mis en place... Ils ne sont pas toujours correctement exploités.

Le problème des correctifs, par exemple, n'est toujours pas résolu. WannaCry et NotPetya se propagent rapidement, exploitant à la fois des vecteurs d'exploitation volés à la NSA et les faiblesses courantes des logiciels Windows... faiblesses pour lesquelles il existait un correctif.

- **Les logiciels sont vulnérables par nature.** Des centaines de milliers de lignes de code, toutes écrites par des humains. Qu'est-ce qui pourrait mal tourner, franchement ? Personne n'écrit de logiciel totalement exempt d'erreurs et immunisé contre les pirates potentiels.
- **Plus le logiciel vieillit, plus ses vulnérabilités sont exposées.** Chez Ivanti, nous comparons cela à du lait qui caille. Plus le lait reste sur votre étagère, plus il risque de cailler. Résultat ? Il est perdu. De même, plus un logiciel reste utilisé longtemps, plus ses vulnérabilités risquent d'être dévoilées, exposées et exploitées.
- **Les anciens logiciels ne reçoivent pas de correctifs.** Ce n'est pas toujours vrai. Par exemple, après l'épisode WannaCry, Microsoft a décidé de franchir le pas et de publier des correctifs pour ses anciens systèmes d'exploitation qui ne sont plus pris en charge, en raison de l'étendue de la menace. Cependant, vous ne pouvez généralement pas compter sur la mise à jour des anciens logiciels vulnérables.

- **Les correctifs des nouveaux logiciels sont mal appliqués.** Des correctifs étaient disponibles pour les systèmes d'exploitation Windows pris en charge avant WannaCry, ainsi (comme nous l'avons dit) que pour les systèmes non pris en charge après cette attaque. Pourtant, même avec tous ces correctifs et la menace de WannaCry encore si proche, des entreprises ont quand même été victimes de NotPetya un mois plus tard. Elles ne disposaient peut-être pas des outils voulus pour appliquer les correctifs de façon exhaustive à l'ensemble de leur environnement. Peut-être que leur personnel réduit travaillait aussi dur que possible, mais sans parvenir à effectuer l'opération à temps. Quelle que soit la raison, le fait que les correctifs sont disponibles ne garantit pas qu'ils sont implémentés comme ils le devraient.
- **Conclusion ? Impossible d'appliquer un correctif à tous les éléments.** Les correctifs ne vous protègent pas des exploitations « zero-day ». Et que faire si aucun correctif n'est disponible, par exemple, parce que vous utilisez des systèmes plus anciens ou que vous craignez les dommages que les correctifs pourraient infliger à votre environnement ? Vous devez bloquer les applications sans correctif à l'aide d'outils comme les listes blanches d'applications et la gestion des privilèges. Quelle que soit la façon dont l'utilisateur accède à son poste de travail et quel que soit l'endroit où il le fait, il est essentiel qu'il reçoive uniquement les applications autorisées dont il a besoin pour être productif. De plus, il ne doit pas pouvoir introduire d'applications non autorisées susceptibles de nuire à la stabilité du poste de travail, d'avoir un impact sur la sécurité, de compromettre la conformité des licences, de provoquer des périodes d'inactivité utilisateur et d'augmenter les coûts de gestion des postes de travail.

Autres problèmes signalés par nos clients

Le casse-tête de la cybersécurité ne se résume pas à cela, c'est évident. Mais, pour faire simple, les départements IT et Sécurité font de gros efforts mais ils sont contraints à l'échec.

Le patchwork de solutions de cybersécurité ponctuelles mis en place ? Il ne fonctionne pas bien en tant qu'entité globale, et ne fournit pas une vue intégrée complète des risques pour l'environnement. D'après le rapport annuel Cisco 2017 sur la cybersécurité, 55 % des professionnels de la sécurité font appel à au moins 6 fournisseurs de sécurité.

Et le phénomène est accentué par le manque avéré de personnel de cybersécurité qualifié. Sans le talent (ou les outils) nécessaire pour déterminer les alertes critiques et leurs causes, les professionnels de la sécurité sont souvent contraints d'ignorer tout simplement l'examen des alertes. En fait, selon ce même rapport, près de la moitié des alertes ne donne lieu à aucune investigation.

Imaginez ce que ces menaces non examinées peuvent provoquer pour votre productivité, la satisfaction de vos clients et la confiance en votre entreprise.

Encore un point à retenir : le fait de jongler entre plusieurs solutions et plateformes de plusieurs fournisseurs crée en réalité des failles propices aux attaques. C'est un facteur de risques et de coûts, qui renforce encore la pression subie par les équipes déjà surchargées de travail et menace la gouvernance IT.

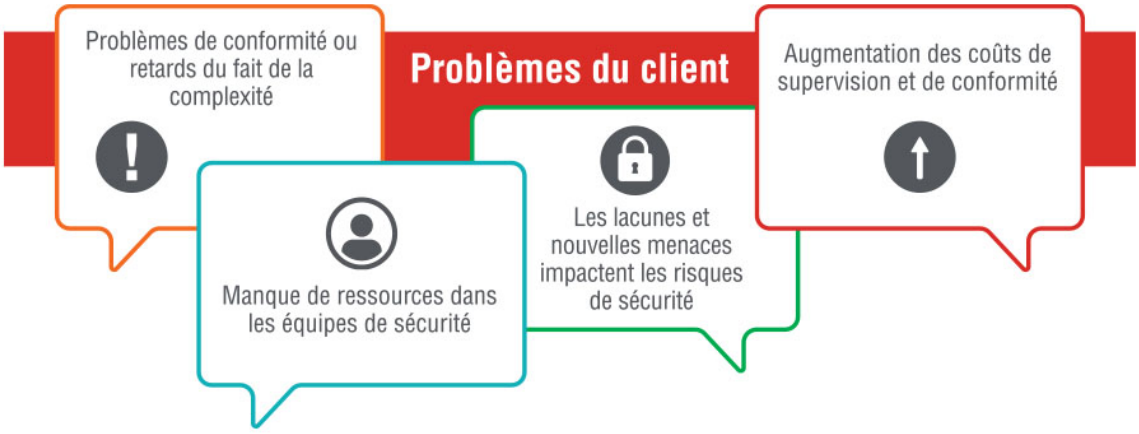
Le futur ? Des malwares transformés en armes.

Il ne fait aucun doute que les pirates modernes peuvent avoir un impact majeur sur les infrastructures critiques du monde entier (hôpitaux, systèmes bancaires, entités de pouvoir), surtout s'ils profitent de technologies vieillissantes et vulnérables comme les anciens logiciels. Et ils semblent de plus en plus désireux de se comporter ainsi.

C'est un vrai cauchemar. Les cyberattaques deviennent de plus en plus sophistiquées et de plus en plus violentes... en grande partie parce que les outils sophistiqués initialement conçus pour le cyberespionnage et la guerre sont désormais librement disponibles pour tous les cybercriminels.

Le ransomware WannaCry a bloqué des ordinateurs dans des hôpitaux, des banques et des entreprises du monde entier. Les hôpitaux anglais ont dû refuser des patients le temps de gérer les ordinateurs pris en otage. NotPetya a également affecté des hôpitaux (les forçant à annuler des opérations chirurgicales) et d'autres entreprises majeures comme des compagnies aériennes, des banques, la centrale nucléaire de Tchernobyl, et une entreprise de fret mondiale qui a été forcée de fermer ses terminaux de gestion des conteneurs dans les ports, de Los Angeles à Mumbai.

Comment les pros de la sécurité et de l'IT peuvent-ils protéger leur entreprise des dangers des violentes attaques sophistiquées de ce type, conçues pour avoir un impact critique ?



Des stratégies de sécurité bien ciblées : La clé du succès IT

Une stratégie de sécurité réussie comporte de nombreux aspects. Les plus efficaces d'entre elles adoptent une approche multiniveau qui offre plusieurs options de protection pour chaque situation. Éliminez toutes les faiblesses.

Mettez en place une protection en profondeur

- ***Découvrez l'étendue réelle des risques***
- ***Réduisez votre surface d'attaque***
- ***Détectez les activités malveillantes***
- ***Prenez des mesures pour résoudre les problèmes***
- ***Analysez les données pour en savoir plus sur les incidents***

Simplifiez et automatisez la sécurité pour améliorer les délais de réponse

- Fournissez une image complète des opérations réalisées dans votre environnement, car il est impossible de protéger (ou de bloquer) ce dont vous ne soupçonnez même pas la présence.
- Réduisez la surface d'attaque : empêchez les malwares et exploitations de s'exécuter pour que vos fonctions et équipes de sécurité aient une vraie chance de traquer les menaces qui atteignent vos systèmes.
- Détectez les activités malveillantes après l'exécution.
- Corrigez et contenez les activités malveillantes, ainsi que les vulnérabilités potentielles.
- Et mettez vos efforts en évidence à l'aide de données très complètes qui montrent votre situation en matière de sécurité et de conformité.

Il vous faut aussi des outils plus simples et plus fluides, qui automatisent les processus de sécurité. L'automatisation vous aide à alléger la charge de travail que représentent la détection et l'investigation pour vos équipes déjà débordées. Et, pour finir, vous devez rechercher des outils de limitation des menaces qui préservent et même boostent la productivité des utilisateurs. Parce que les utilisateurs qui ne peuvent pas travailler VONT faire appel au centre de support plus souvent, et même agir dans le dos du département IT en utilisant des solutions de « Shadow IT », générant des risques pour votre environnement.

Équilibre entre sécurité et besoins de l'utilisateur

- ***Apprenez-en plus sur vos utilisateurs et découvrez leurs besoins***
- ***Assurez la sécurité sans perturber leur travail***
- ***Fournissez des services en mode silencieux, via des mises à niveau et l'élimination des risques***
- ***Boostez la productivité avec les bons outils***

Progressez grâce au CIS

La meilleure façon de faire de cette vision une réalité passe par un cadre de sécurité renforcée. Lorsque les équipes Sécurité et Opérations IT travaillent ensemble à la mise en œuvre d'une solution de sécurité ciblée reposant sur des processus communs et un jeu d'actions hiérarchisées, les coûts diminuent et la réactivité augmente.

Les cyberveilleurs comme le CIS (Center for Internet Security) le confirment. Ils partagent leurs connaissances et leur expertise pour identifier, valider, promouvoir et soutenir l'adoption des meilleures pratiques de cybersécurité. Dérivés des leçons tirées de l'expérience pratique de la NSA, les contrôles de sécurité critiques (CSC) du CIS soutiennent et reflètent de nombreuses autres sources leaders du conseil en matière de cybersécurité.

L'objectif final ? Ils sont conçus pour vous aider à définir rapidement le point de départ de vos défenses, à aider votre personnel réduit à agir avec des résultats immédiats et une grande valeur ajoutée, puis à cibler les risques supplémentaires propres à votre entreprise.

- Liste d'actions triée par ordre de priorité
- Des résultats immédiats et de grande valeur
- Respect des réglementations
- Fondés sur une expérience née d'attaques réelles

Pour réduire les coûts tout en obtenant la stratégie efficace de protection en profondeur que vous recherchez, utilisez une structure ayant fait ses preuves et des solutions d'un seul fournisseur, capables de traiter la majorité des besoins dans l'ensemble de votre entreprise, puis comblez les vides à l'aide de solutions ponctuelles pour répondre à des besoins spécifiques.

Les recherches et les études de cas du CIS montre que le fait de configurer les systèmes IT selon la configuration de référence fixée par le CIS élimine 80 à 95 % des vulnérabilités de sécurité connues.

Renforcez vraiment votre sécurité, rapidement, grâce aux 5 principaux contrôles CSC

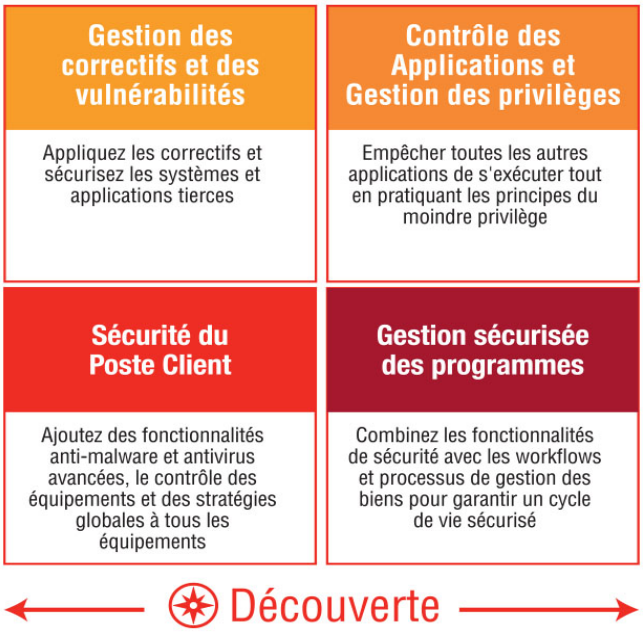
Plus précisément, les 5 principaux contrôles de sécurité critiques (CSC) du CIS établissent des bases solides pour une amélioration spectaculaire de la situation d'une entreprise en matière de sécurité. C'est pourquoi nous les désignons sous l'expression « cyberhygiène de base ».

1. **Inventaire des périphériques autorisés et non autorisés**
   Le CIS en parle lui-même :[14] « Gérez activement (inventaire, suivi et correction) tous les périphériques matériels du réseau afin que seuls les périphériques autorisés aient accès au système, et que les périphériques non autorisés et non gérés soient détectés et interdits d'accès. »
2. **Inventaire des logiciels autorisés et non autorisés**
   La même chose, mais pour les logiciels : « Gérez activement (inventaire, suivi et correction) tous les logiciels du réseau afin que seuls les logiciels autorisés soient installés et puissent s'exécuter, et que les logiciels non autorisés et non gérés soient détectés, et que leur installation et leur exécution soient interdites. »
3. **Configurations sécurisées pour le matériel et les logiciels**
   « Établissez, implémentez et gérez activement (suivi, rapports, correction) la configuration de sécurité des ordinateurs portables, serveurs et postes de travail à l'aide d'un processus strict de gestion des configurations et de contrôle des changements, afin d'éviter que des pirates exploitent les services et paramètres vulnérables. (Telle que fournie par les fabricants et revendeurs, la configuration par défaut des systèmes d'exploitation et des applications vise normalement la facilité de déploiement et d'utilisation, pas la sécurité.) »
4. **Évaluation et correction en continu des vulnérabilités**
   « Collectez continuellement de nouvelles informations, évaluez-les et prenez des mesures afin d'identifier les vulnérabilités, de les corriger et de limiter les possibilités d'attaque. »
5. **Utilisation contrôlée des privilèges d'administration**
   « L'abus de privilèges d'administration est l'une des principales méthodes qui permettent aux pirates d'atteindre l'entreprise ciblée. » Fournissez des processus et des outils pour « suivre/contrôler/interdire/corriger l'utilisation, l'affectation et la configuration des privilèges d'administration des ordinateurs, réseaux et applications. »

Nos solutions de protection en profondeur

La conclusion est la suivante : pour chaque bien critique de votre entreprise, vous devez comparer vos contrôles de sécurité existants aux contrôles CSC du CIS. Identifiez précisément les sous-contrôles que vous appliquez déjà et ceux qui vous manquent. Ensuite, en fonction des faiblesses identifiées, ainsi que des risques et inquiétudes propres à votre entreprise, prenez des mesures immédiates pour implémenter les 5 principaux contrôles et développez un plan stratégique pour implémenter les autres.

Nous pouvons vous aider. Ivanti offre une gamme complète de solutions ciblées qui gèrent les 5 principaux contrôles du CSC et les autres contrôles, afin d'aligner opérations IT et sécurité pour mieux répondre aux besoins de cybersécurité des clients.



Les solutions Ivanti comportent des fonctions automatisées comme la découverte, la gestion des correctifs, le contrôle des applications et des périphériques, la gestion des privilèges d'administration et la configuration sécurisée... tous des aspects essentiels des 5 principaux contrôles du CIS. De plus, Ivanti aide ses clients à implémenter ces contrôles avec succès, facilement et à bas coût, avec un impact minimal sur la productivité des utilisateurs. Les utilisateurs n'ont pas besoin de faire appel au centre de support toutes les 5 minutes pour obtenir des droits d'accès. Les solutions de contournement en « Shadow IT », non autorisées et non sécurisées, sont éliminées. Les activités de l'entreprise ne ralentissent pas.

Nous pouvons aussi vous aider à consulter les résultats.

Comme il n'existe pas de vraie sécurité sans connaissance approfondie de l'environnement, Ivanti Xtraction vous permet de créer des rapports à l'aide d'une simple case à cocher. Il fournit des données à la demande, et vous permet de créer facilement de nouveaux tableaux de bord et rapports pour apporter les données voulues à la Direction, aux responsables, aux chargés de gamme de produits (LOB) et aux propriétaires d'application.

Grâce à nos connecteurs prédéfinis compatibles avec presque tous vos outils (centres de support, outils de surveillance et d'ITAM, systèmes téléphoniques, etc.), vous n'avez besoin d'aucun codage, gourou en matière de Business Intelligence ou feuilles de calcul... Et aucun silo de données n'est créé. En outre, Xtraction peut être personnalisé pour se connecter à encore plus de systèmes, si bien que tous les utilisateurs peuvent voir les données de l'ensemble de l'entreprise en contexte. La masse énorme des informations se transforme en données critiques importantes, pour une prise de décisions plus rapide, plus pertinente et plus facile.

Conclusion

Ne gaspillez plus votre argent en solutions inadaptées, et ne laissez plus vos équipes Sécurité et IT s'arracher les cheveux pour protéger les éléments voulus dans votre entreprise sans les ressources et l'expertise nécessaires pour y parvenir. Implémentez un programme de cybersécurité solide, afin de cibler les éléments les plus importants pour améliorer vos résultats. Choisissez ensuite des solutions conçues pour répondre à vos besoins essentiels en matière de sécurité et protéger votre environnement des cybermenaces actuelles, sophistiquées et très étendues.

www.ivanti.fr

+33 (0)1 49 03 77 80

sales@ivanti.com

1 Privacy Rights Clearinghouse

2 **https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/**

3 Rapport 2016 de Verizon sur les fuites de données (DBIR)

4 Enquête 2016-17 d'EY sur la sécurité mondiale des informations

5 Recherches 2016 d'IBM X-Force, **http://www-03.ibm.com/press/us/en/pressrelease/51230.wss**

6 Op. cit.

7 Rapport DBIR Verizon 2017

8 Rapport DBIR Verizon 2016

9 **http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/**

10 **https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/**

11 **https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/**

12 **http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html**

13 **http://files.shareholder.com/downloads/ABEA-3GG91Y/5005768664x0x954059/3E9E6E5C-7732-4401-8AFE-F37F7104E2F7/Maersk_Interim_Report_Q2_2017.pdf**

14 **https://www.cisecurity.org/controls/**