
LES TENDANCES
DE LA CYBERSÉCURITÉ
LA TECHNOLOGIE DEVIENT PLUS INTELLIGENTE - ET NOUS ?

TABLE DES MATIÈRES

INTRODUCTION

Puisqu'il est évident que les appareils deviennent de plus en plus intelligents, la question suivante se pose : Sommes-nous suffisamment "intelligents" pour tirer le meilleur parti de ces appareils connectés sans pour autant en subir leurs conséquences ?

Il y a quelques années encore, les appareils intelligents ne semblaient être rien d'autre qu'une vision optimiste de l'avenir. Pourtant, leur essor s'est développé si rapidement que cette technologie est devenue partie intégrante de notre vie quotidienne presque sans même que nous remarquions le changement.L'intégration graduelle mais persistante de la technologie dans les objets que nous utilisons tout le temps est susceptible de changer et d'avoir un impact sur nos coutumes sociales d'une manière qui nous est encore inconnue à ce jour.

Chaque année, en choisissant les sujets des tendances, les experts dESET décident quels aspects de la cybersécurité et de la vie privée semblent susceptibles de présenter certains des défis majeurs pour l'année à venir. Au travers des cinq chapitres qui composent ce numéro consacré aux tendances, nous examinerons diverses questions de cybersécurité relatives aux individus,aux gouvernements et entreprises, mais aussi des concepts généraux tels que la vie privée, la démocratie, la transformation numérique et bien d'autres sujets encore.

Dans le premier chapitre, Tony Anscombe aborde le thème des élections présidentielles américaines et notamment les conséquences sur celles-ci en 2016 à cause des fake news et des dénonciations des interférences étrangères. Mais les États-Unis ne sont pas le seul pays à avoir vécu cela et il est presque certain qu'en 2020, le sujet sera à nouveau d'actualité. Dans ce contexte, il est important d'examiner à nouveau comment la désinformation et les fake news pourraient jouer un rôle dans les chapitres démocratiques à venir.

Jake Moore aborde ensuite un autre sujet dont on parle beaucoup ces derniers temps : l'apprentissage automatique (ou Machine Learning), qui est souvent présenté à tort comme une intelligence artificielle. L'apprentissage automatique est utilisé pour décrire une variété de développements technologiques, mais c'est en 2019 qu'unepplication a gagné une grande notoriété auprès du grand public avec la brièvement populaire FaceApp et ses progrès fulgurants en matière de deepfake, lesquels ont ensuite été de plus en plus répandus au cours de l'année. Quelles sont les implications de l'apprentissage automatique en matière de cybersécurité ? Au-delà de son utilisation pour détecter les menaces de cybersécurité ? pourrait-on en abuser pour porter atteinte à la sécurité et à la vie privée d'individus et d'organismes ?

Toutes ces questions sont intimement liées à la vie privée des utilisateurs. Dans son chapitre, Lysa Myers examine comment les mentalités ont changé depuis le scandale de Cambridge Analytica, la mise en œuvre de la législation à différents niveaux et les implications probables pour les entreprises et les gouvernements dues au désenchantement des utilisateurs à l'égard de la confidentialité des données.

La tendance pour tout ce qui est « intelligent » a non seulement atteint les objets que les gens utilisent tous les jours, mais a commencé également à prendre de l'importance à plus grande échelle. On trouve maintenant de nombreux exemples de bâtiments intelligents dans le monde entier et on s'attend à ce que de plus en plus de villes adoptent une technologie intelligente. Cependant, cela pourrait-il conduire àdes attaques d'un nouveau genre, combinant le monde numérique et le monde physique? La cybersécurité est-elle suffisamment avancée pour que ces implantations puissent être réalisées sans compromettre les utilisateurs, les citoyens et les organisations ? Cecilia Pastorino aborde, entre autres, ces questions dans son chapitre.

Ce changement de paradigme est peut-être le plus visible dans les processus de transformation numérique actuellement appliqués par de nombreuses entreprises à travers le monde. Il s'agit d'un vrai défi pour les équipes informatiques qui se doivent de suivre le rythme de tous les changements technologiques en cours. Camilo Gutiérrez Amaya s'est penché sur cette question, en examinant les défis auxquels le monde de l'entreprise sera confronté dans un avenir proche.

L'un des meilleurs outils pour se préparer à l'avenir est de rester informé, alors pourquoi ne pas lire ce rapport pour savoir ce à quoi nous pouvons nous attendre en 2020 et dans les années à venir.

2020 : UNE ANNÉE DE PLUS DANS LE FLOU

- Les fake news
- Désinformation et propagande ciblées
- Le processus de vote
- Démystification totale ?

Tony Anscombe
Évangéliste mondial
de la sécurité chez ESET

2020: Une année de plus dans le flou

« 20/20 » signifie une note parfaite, mais cette année 2020 pourrait n'être qu'une autre année floue pour le processus démocratique. Qu'est-ce qui peut nous empêcher de prendre des décisions éclairées et fondées sur des faits ?

Nous entrons à peine en 2020 qu'une prédiction tirée de ce rapport sur les tendances est probablement garantie : il y aura des allégations d'ingérence et de manipulation dans les processus électoraux au cours de l'année.

Ces questions sont complexes et bien qu'il soit facile de suspicieusement pointer du doigt une ingérence, il s'avère plus compliqué de la prouver, hors de tout doute raisonnable. La complexité commence par le fait qu'il existe plusieurs types d'interférences qui peuvent faire en sorte que les résultats d'une élection soient influencés vers un certain dénouement ou qu'ils ne représentent pas réellement le vote de l'électorat. Lorsqu'on examine les problématiques en ligne, elles regroupent à la fois des fake news,le truquage de machines à voter, jusqu'au ciblage de certaines parties influençables de la population à l'aide d'informations biaisées

L'élection présidentielle américaine de 2016 a été entourée d'une controverse post-électorale avec des allégations de fake news, l'ingérence d'autres États-nations et le piratage potentiel du processus de vote lui-même. De plus, certains prétendent que le référendum de Brexit au Royaume-Uni a été biaisé en raison de manipulations alors qu'en Amérique du Sud, la désinformation diffusée par le biais de WhatsApp a peut-être affecté le résultat des élections brésiliennes. Comment pouvons-nous espérer que les électeurs aient confiance dans le processus démocratique alors que tous ces éléments brouillent les résultats ?

Ce chapitre résume certaines des méthodes que nous verrons sans doute utilisées par des individus, des groupes militants, des États-nations et même des cybercriminels en 2020 alors qu'ils tentent d'interférer avec les processus démocratiques du monde pour leur profit, quel qu'il soit.

Fake news

Le Collins Dictionary a décerné à ce terme le titre de *Mot de l'Année* en 2017. Sa réputation est due en grande partie à l'élection présidentielle américaine de 2016 et aux affirmations constantes des candidats selon lesquelles les articles publiés dans les médias et les informations diffusées sur les réseaux sociaux n'étaient pas factuels. La *signification de ce terme* est évidente et fait référence au sensationnalisme de la diffusion de fausses informations sous le couvert de reportages.

IDans la foulée de l'élection, Pew Research a mené un *sondage* sur les perceptions à l'égard desdites fake news. Le résultat a été surprenant, : 88 % affirment que les Américains sont très ou assez confus sur les faits essentiels en raison des fake news.

Ofcom, l'organisme de réglementation des médias du Royaume-Uni, a publié un ***rapport*** sindiquant que la moitié des adultes britanniques reçoivent des nouvelles par le biais des réseaux sociaux, 75 % d'entre eux déclarent que cela inclut Facebook comme source. Et ce, malgré le fait que les médias sociaux n'ont pas été évalués comme étant impartiaux, fiables ou précis. La télévision reste le média le plus utilisé, avec 75 % des adultes interrogés qui l'inscrivent parmi leurs sources d'information, toutefois l'influence des médias sociaux ne doit pas être sous-estimée et elle semble là pour durer.
Les fake news peuvent avoir différents buts : le profit, le gain politique, le crime, les canulars et les blagues virales.

Les genres peuvent même être combinés : créer un canular qui met un candidat politiquedans une mauvaise posture peut créer un gain politique et avec la « bonne » campagne de promotion autour de la fake news, cela peut générer un joli profit. Si les créateurs d'une telle campagne pouvaient être identifiés, il est fort probable qu'ils auraient commis un crime, mais déterminer la source n'est pas toujours possible.

À l'approche des élections générales de 2019 au Royaume-Uni, un organisme de recherche, Future Advocacy, et un artiste britannique, Bill Posters, ont créé une fausse *vidéo sur les médias sociaux* , appelée « deepfake ». La vidéo montre les deux principaux candidats qui semblent se soutenir mutuellement pour le poste de premier ministre. Cet exemple de fake news a été créé pour tenter de démontrer la difficulté d'identifier le vrai du faux et ainsi étayer le fait que la démocratie peut potentiellement être compromise.

Mais ce problème est loin d'être nouveau. À la caisse du supermarché local, je lis souvent les titres des magazines : des célébrités qui se séparent, la famille royale britannique qui divorce ou des extraterrestres qui atterrissent sur un parking. Les lecteurs de ces magazines savent, espérons-le, que ces histoires sont fausses lorsqu'ils choisissent de les acheter, mais lorsque nous passons à des articles sur Internet,qui sont diffusés rapidement à un public beaucoup plus large, il n'est pas si facile de distinguer le vrai du faux.Certains réseaux sociaux et

moteurs de recherche tentent de manière responsable de lutter contre ce problème, sous la pression de l'indignation politique et publique.Par exemple, Twitter a récemment *annoncé une interdiction* de toute publicité politique sur les candidats, les élections et les sujets politiques jugés sensibles à l'approche de l'élection présidentielle américaine de 2020. Mais c'est un sujet complexe et on a même parlé d'atteinte à la liberté d'expression lorsque quelqu'un se voit refuser la possibilité de poster ou de diffuser des annonces avec un certain point de vue. ITOutefois, à mesure que les fake news se répandent, les consultations de pages augmentent et les revenus publicitaires sont croissance, pourtant tous les intervenants qui diffusent des annonces sur les sites web ne sont pas responsables.

Le problème est la vitesse de diffusion de la désinformation - un article paraissant dans l'heure qui suit se répandra rapidement, surtout si le créateur en fait la promotion et le diffuse à partir de plusieurs comptes et réseaux simultanément. Les entreprises responsables de ces plateformes ont innové dans les méthodes de détection et ont construit des mécanismes de signalement pour, lorsque cela est possible, détecter automatiquement ou permettre aux utilisateurs de signaler des fake news. Cependant, compter sur les signalements est une solution défaillante. Comme la désinformation a déjà été diffusée, de nombreux utilisateurs ne prendront probablement pas la peine de la signaler... Quant à ceux qui ont déjà vu (et peut-être été influencés par) un sujet de désinformation, il y a fort à parier qu'ils ne se rendront probablement pas compte de sa suppression.

En tant que professionnel de la cybersécurité, je considère que les fake news qui nuisent à la démocratie sont criminelles - au même titre que les intrusions de logiciels malveillants sur vos appareils. Il faut une solution technologique plus robuste pour empêcher la propagation de fake news dès leur apparition et les éliminer à la source. Exactement comme les exploitations zero-day peuvent être détectées par les logiciels anti-malware. Avec la généralisation de l'apprentissage automatique, il est probable que des solutions innovantes seront mises sur le marché pour détecter et supprimer ou tout du moins effacer certaines fake news avant même que l'utilisateur ne puisse la lire.

L'éducation est également une solution à long terme à ce problème, mais les résultats sont plus lents. IEn juillet 2019, le gouvernement britannique a publié de nouvelles directives de sécurité pour les écoles ; une partie de ces mesures révisées stipule que chaque enfant doit obligatoirement être informé des biais de confirmation et des risques en ligne. Cela aidera les élèves à repérer les techniques utilisées pour la persuasion et à identifier les fake news et leurs risques, mais il faudra de nombreuses années à toute une génération pour comprendre ce qui peut être réel ou faux. (Mon collègue Jake Moore traite du spectre des deepfakes dans un *autre chapitre* de ce rapport). Cependant, comprendre ce qui est vrai ou faux permettra à la prochaine génération d'avoir confiance dans le système électoral démocratique. Davantage de gouvernements sont susceptibles d'adopter cette position proactive et de l'ajouter à leurs politiques d'éducation. Si ce n'est pas le cas, alors ils devraient s'y atteler.

Désinformation et propagande ciblées

L'abus des données personnelles de Cambridge Analytica a choqué le monde entier, mais n'a pas surpris ceux d'entre nous qui ont toujours pensé que : « si vous ne payez pas pour cela, alors vous êtes forcément le produit » ; par exemple, chaque utilisateur de Facebook aux États-Unis et au Canada *génère plus de 130 dollars US* pour l'entreprise chaque année. Le scandale a fini par éclater lorsque trois organismes de presse ont combiné leurs ressources afin de provoquer suffisamment de bruit pour que tout le monde le remarque - après plus de deux ans.

Avançons un peu dans l'histoire : Facebook a été condamné à une amende de 5 milliards de dollars US par la Commission fédérale du commerce (FTC) des États-Unis pour son rôle dans la violation de données.Je ne suis pas sûr qu'on puisse vraiment parler de "violation", toutefois grâce à des documents qui sont maintenant dans le domaine public, on peut constater que Facebook savait ce qui se passait. Il s'agisst donc plutôt d'un abus de confiance à des fins financières.Le jour où l'amende de la FTC a été annoncée, le cours de l'action Facebook a augmenté. Il est clair que le marché s'attendait donc soit à

ce que la sanction soit plus sévère, soit qu'il ait compris que l'accord conclu avec la FTC était en fait en faveur de Facebook.

La militarisation de l'information, qu'il s'agisse de désinformation ou de propagande, est appelée à se poursuivre et prendra de nombreuses voies différentes à mesure que les bénéficiaires exploreront et adopteront de nouvelles méthodes pour attaquer la démocratie ou gagner de l'argent. Au centre de cette situation envahissante et dissimulée se trouve l'exploration de données, quelque chose que nous ne pouvons pas voir et qui, pour beaucoup de gens, est difficile à comprendre.Les points de données disponibles sur les individus sont nombreux puisque la grande majorité des gens *sur-partagent » sur les réseaux sociaux*.La capacité d'ajuster et de manipuler le message envoyé à un individu est rendue possible grâce à la technologie, ce qui permet d'individualiser les messages envoyés à des millions de personnes, le tout par un simple clic de souris.

Le processus de vote

La question de savoir si le bulletin de vote est vérifiable n'est pas nouvelle et concerne à la fois le papier et les systèmes de vote électronique. De plus, c'est une question qui ne sera probablement pas résolue de sitôt.

De nombreux États des États-Unis ont dépensé des millions de dollars pour moderniser les dispositifs qui seront utilisés lors des élections de 2020. Un État, la Pennsylvanie, a bénéficié de *14,5 millions de dollars US pour moderniser les dispositifs électoraux* pourtant même les nouveaux appareils peuvent être vulnérables. Cela est dû au fait que le système d'exploitation sous-jacent, Windows 7, qui - à moins que des frais ne soient payés - ne recevra plus de correctifs de Microsoft une fois que cette version du système d'exploitation atteindra sa « fin de vie » en janvier 2020, 11 mois avant l'élection présidentielle américaine de 2020.

Lors de la conférence du DEF CON 27 sur le piratage informatique en août 2019, il y a eu des défis en temps réel pour trouver les *vulnerabilities in election systems*. Unede ces expériences a montré des vulnérabilités dans un système de notation des bulletins de vote. Dans ce cas, l'attaquant avait un accès physique illimité et une connexion directe aux dispositifs, ce qui ne devrait jamais être le cas en situation réelle. IJ'espère que, si cela venait à arriver, quelqu'un remarquerait qu'un pirate démonte une borne et y connecte des fils. Cela dépend toutefois du fait que les dispositifs soient physiquement sécurisés avant et pendant le processus de vote, ce qui, dans certains cas, n'a pas été le cas lors des élections précédentes. Cela peut également devenir obsolète si les appareils restent autonomes et ne sont jamais connectés à un réseau public.Bien qu'il existe de nombreux dispositifs qui pourraient théoriquement être vulnérables, cela ne signifie pas nécessairement qu'ils peuvent être ou qu'ils seront exploités.

Il est clair que les approches technologiques pour l'inscription et le vote continueront à poser des problèmes dans le futur. Nous sommes continuellement témoins de violations massives de données et de menaces contre les systèmes dans les entreprises et les ministères, alors pourquoi la technologie ou les processus de vote seraient-ils exemptés de telles attaques ? Heureusement, l'élection présidentielle américaine de 2016 a permis de prendre conscience des vulnérabilités possibles des dispositifs électoraux utilisés, ce qui a eu pour conséquence directe l'affectation de budgets ainsi que la nécessité de sécuriser les systèmes dès leur conception.

Démystification totale ?

Pour 2020, il y aura bien sûr de nombreuses élections dans le monde entier et d'innombrables problèmes mis en évidence dans leurs dispositifs et processus, tant technologiques que physiques. L'utilisation de toutes les méthodes mentionnées ici est prévisible, mais la question est la suivante : à quelle échelle seront-elles utilisées et le parasitage modifiera-t-il le résultat ?
En tant qu'électeurs et, espérons-le, défenseurs de la démocratie, nous ferons pression sur les entreprises qui diffusent des fake news et de la désinformation afin qu'elles détectent et fassent cesser cette pratique.

Comme pour de nombreuses pratiques douteuses, telles que les abus au sujet de la vie privée des consommateurs auxquels nous avons été soumis au cours des dix dernières années, sans aucune intervention du gouvernement et sans réglementation ou législation, nous continuerons de militer jusqu'à ce que cette pratique ne puisse plus être tolérée. Toutefois, ne vous attendez pas à ce que cela arrive dans les 12 prochains mois.

ML CONTRE ML : AU SERVICE DE LA OU DE LA CYBERCRIMINALITÉ ?

- Ouvrez l'œil (et le bon)
- Tromper l'algorithme
- Bénédiction ou malédiction ?

Jake Moore
Spécialiste Sécurité chez ESET

ML contre ML : Au service de la cybersécurité ou de la cybercriminalité?

Les progrès de l'apprentissage automatique ont apporté des avantages considérables aux défenseurs de la cybersécurité, mais le potentiel de cette technologie n'est pas en reste pour ceux qui cherchent à la détourner à des fins peu recommandables.

Il ne fait aucun doute que l'Apprentissage Automatique (Machine Learning/ML) change notre vie. L'augmentation de la puissance de calcul et l'utilisation de vastes banques de données améliorent rapidement nos capacités dans de nombreux secteurs. De plus, si le cousin éloigné du ML, aussi connu sous le nom d'Intelligence Artificielle (IA), prend lui aussi son envol et que les ordinateurs commencent à « penser par eux-mêmes », nous sommes dans un futur radieux où beaucoup de choses que l'on pensait autrefois inimaginables pourraient devenir possibles. Pour l'instant, cependant, l'IA autonome semble encore bien loin tandis que le ML prend de l'avance dans l'un des développements technologiques les plus passionnants de l'histoire.

Le Machine Learning a également apporté divers *avantages aux cyberdéfenseurs*, notamment un scan plus efficace, une détection plus rapide et une amélioration de la capacité à repérer les anomalies. En effet, certaines sociétés de cybersécurité tirent parti de cette technologie depuis des années afin d'améliorer les capacités de détection de leurs produits.

Cependant, que se passe-t-il si l'apprentissage automatique est utilisé à mauvais escient pour nous attaquer, nous et les systèmes que nous avons créés ? Il n'est pas difficile de voir pourquoi, et comment, *les logiciels malveillants basés sur le ML ou même l'IA* pourraient offrir de nouveaux et uniques vecteurs d'attaque - bien plus puissants que ce à quoi nous sommes actuellement habitués. Il devient donc clair que le ML sera un élément déterminant dans nos combats numériques futurs.

Cette technologie a progressé à pas de géant dans d'autres applications également. Dans ce chapitre de tendances, nous nous pencherons donc sur deux façons dont les algorithmes de ML pourraient être utilisés pour nuire.

Ouvrez l'œil (et le bon)

Vous avez sûrement vu l'une des nombreuses vidéos convaincantes de changement de visage qui apparaissent, en particulier sur les réseaux sociaux. De tels deepfakes - des vidéos, audio ou images truquées qui sont conçus pour reproduire l'apparence et le son de vrais humains - peuvent sembler d'une légitimité déconcertante voire même choquante. Les deepfakes peuvent souvent impliquer des célébrités ou des personnalités publiques qui ont apparemment un comportement inattendu ou qui disent quelque chose de scandaleux avec laquelle ils sont pourtant en contradiction

Les Deepfakes augmentent en qualité à un rythme impressionnant, comme on le voit dans des vidéos comme ***celle-ci*** où un Barack Obama généré est amené à dire quelque chose que le vrai n'a jamais dit. De plus, lorsque vous regardez *Bill Hader* se transformer sans effort en une version de Tom Cruise et Seth Rogen, vous vous rendez compte que nous pourrions bien avoir un énorme problème sur les bras si cette menace n'est pas contrée rapidement. Comme pour tout sujet sur Internet, l'avenir pourrait amener à ce que cette technologie soit utilisée pour nuire aux personnalités publiques en les faisant dire ce que l'on veut, pour faire du tort à la société, ou même pour manipuler les élections dans le monde entier.

Sommes-nous préparés au véritable impact des deepfakes ? Avec les scandales politiques, les pseudo-nudes et les scénarios presque inimaginables impliquant de fausses vidéos, il se peut que nous soyons au début d'une épidémie où la ligne entre la vérité et le mensonge soit impossible à déterminer. Quel impact les deepfakes auront-ils sur la société ? À la lumière de tout le scandale de Cambridge Analytica, dans lequel des spécialistes des données ont pu transformer des enquêtes et des données issues de graphiques sociaux de Facebook en une arme politique par le biais du profilage psychographique, il semble que les deepfakes pourraient accélérer de telles transformations en influençant le public lors des élections. Arriverons-nous à un point où nous ne ferons plus confiance ni à nos propres yeux et ni à nos oreilles ?

Après que FaceApp ait littéralement lifté nos visages et que les rires se soient rapidement éteints, une question s'est posée sur la qualité d'une telle « esbroufe » - pourrait-elle un jour possiblement créer des vidéos de personnes à leur insu ?

Vous avez besoin de nombreuses données (beaucoup de photos, de vidéos et d'enregistrements vocaux) pour réaliser même un court extrait deepfake dans lequel le "réalisateur" peut vraiment décider de ce qui est dit. Cependant, obtenir une quantité importante de données sur une personne non publique est une lourde tâche en soi. Mais rappelons-nous que nous n'étions qu'en 2019. Alors que se passe-t-il si nous pensons à l'année prochaine ou la prochaine décennie ? Pourrait-il suffire d'une courte story Instagram ou deux pour que quelqu'un produise un deepfake si réel que la majorité de vos amis en ligne le pensent vrai ? Il est très probable que cela arrive un jour et il y fort à parier que cela passe par le biais d'une application sur nos téléphones conçue pour créer de tels deepfakes sans effort.

Au cours de la prochaine décennie, nous verrons apparaître des fausses vidéos qu'on pensaitinimaginables auparavant avec des personnalités publiques, mais avec le temps, celles-ci pourraient inclure des personnes plus proches de nous, comme nos collègues, nos amis et les membres de notre famille. Il ne fait aucun doute que les sites pornographiques exploiteront les célébrités de manière obscure, mais, en outre, les cybercriminels utiliseront très certainement cette technologie avec un grand succès pour harponner leurs victimes. Les deepfakes pourraient très facilement brouiller la frontière entre la réalité et la fiction, ce qui pourrait amener certains d'entre nous à ne plus rien croire - même lorsqu'on leur présente ce que nos sens nous disent de croire.

Alors, que peut-on faire pour nous préparer à cette menace ? D'abord, nous devons sensibiliser davantage les gens à l'existence des deepfakes.Nous devrons apprendre à remettre en question les vidéos, même les plus réalistes. Aussi, et bien que cela soit difficile, la technologie devra développer une meilleure détection des deepfakes. Bien que l'apprentissage automatique soit au cœur de leur création en premier lieu, il devra exister des moyens d'agir comme antidote, de manière à les détecter sans se fier à la seule intuition humaine. De plus, les médias sociaux doivent prendre leurs responsabilités et reconnaître la menace potentielle afin d'y faire face le plus tôt possible, car c'est là que les vidéos deepfake sont les plus susceptibles de se répandre et d'avoir un impact néfaste sur la société.

Tromper l'algorithme

La *reconnaissance faciale* est de plus en plus répandue dans la technologie actuelle bien qu'elle s'attire aussi un certain nombre de détracteurs. La reconnaissance faciale n'est peut-être pas encore totalement exacte, mais nous ne sommes qu'en 2019 et les résultats ne peuvent que s'améliorer, n'est-ce pas ?

Les *villes américaines* ont interdit l'utilisation de la *reconnaissance faciale* par les forces de l'ordre après avoir identifié à tort 26 citoyens respectueux des lois comme étant des criminels.En effet, une *étude* du Government Accountability Office des États-Unis a révélé que les algorithmes du FBI étaient inexacts dans 14 % des cas et qu'ils étaient plus susceptibles de mal identifier les personnes de couleur et les femmes. De plus, Microsoft a récemment *refusé d'installer une technologie de reconnaissance faciale* pour une unité de police américaine, en raison de préoccupations concernant la partialité de l'apprentissage automatique.

C'est là que des données ont été introduites par des humains, lesquels ont tendance à avoir divers biais involontaires qui influencent le résultat de l'apprentissage automatique.

Il y a des avantages à ce que la reconnaissance faciale soit déployée partout, notamment avec les millions de caméras de surveillance qui capturent déjà presque tous nos mouvements en public. Par exemple, si vous prenez la reconnaissance faciale dans sa forme la plus élémentaire, elle offre un moyen de recueillir des informations sur qui a été où, à un certain moment. Ce n'est pas si éloigné finalement d'un bon policier qui peut reconnaître un criminel local sur son territoire (je connais des policiers qui peuvent faire cela - ils ont des souvenirs incroyables). Donc, si la reconnaissance faciale peut devenir précise à presque 100 %, alors elle pourrait bientôt surveiller chacun de nos mouvements.

Mais si les forces de l'ordre savent où se trouvent des criminels et des suspects connus, qu'en est-il des criminels qui utilisent le système à leur avantage ou qui volent d'énormes bases de données de localisation confidentielles ? Il est possible que les bases de données de visages des personnes soient compromises, ce qui signifie que les techniques de vérification telles que la reconnaissance faciale ou vocale pourraient être détournées et donc que la sécurité à plusieurs niveaux pourrait être contournée.

Bénédiction ou malédiction ?

Des attaques complexes à base d'apprentissage automatique sont à venir et n'oublions pas que certaines d'entre elles sont actuellement insondables en raison de l'ampleur de la puissance qu'elles utiliseront, elles ont donc le potentiel d'être plus importantes que ce que nous pouvons prévoir. Il est possible que le ML puisse être utilisé comme arme par des attaquants, nous devons donc être prêts pour de telles attaques et savoir comment les affronter. Les attaques à base d'apprentissage automatique pourront apprendre rapidement ce qui a fonctionné ou échoué, puis se reconvertir afin de contourner les défenses existantes. En tant que défenseurs, nous devons comprendre comment ces attaques alimentées par le Machine Learning seront créées, quelles pourraient être leurs capacités pour ainsi pouvoir s'attaquer conjointement à ces futures cyberattaques.

CHANGEMENT MAJEUR DE LA CONFIDENTIALITÉ

- Confidentialité et sécurité dès la conception
- Améliorer la technologie des publicités
- Conséquences législatives des atteintes à la confiance
- Améliorer l'authentification et la vérification
- Changeons de cap

Lysa Myers
Chercheuse en sécurité
chez ESET

Changement majeur de la confidentialité

La confiance en notre environnement numérique global n'a pas été très élevée ces derniers temps : de plus en plus de personnes sont sur le qui-vive au sujet de la protection de leurs données numériques.Qu'est-ce qui a été fait et, plus important encore, que reste-t-il à faire pour que les choses s'améliorent ?

Il y a un certain « rite de passage » qui se produit lorsque vous parlez de sécurité et de protection de la vie privée depuis quelque temps : vous devez en quelque sorte prédire le paysage des menaces dans le futur, puis dès que suffisamment de temps se sera écoulé, vous pourrez seulement vérifier si vos prédictions étaient exactes.

La plupart du temps, cela se produit dans un avenir proche, comme dans le chapitre qui suit. Parfois, c'est à l'échelle d'une décennie (ou plus). Selon ma propre expérience de ce phénomène, j'ai remarqué quelques thèmes récurrents, dont la plupart tournent autour du renforcement ou de la perte de la confiance en notre environnement numérique.

Alors que je me demandais quoi écrire pour ce chapitre, j'ai fait une recherche sur Internet pour trouver l'expression « année de la vie privée » en y ajoutant une année récente, par exemple « année de la vie privée 2018 ». Les titres incluant ces quelques mots peuvent être un bon indicateur, prouvant que l'auteur pensait qu'un grand changement était en train de se produire, notamment concernant les opinions du public sur la confidentialité, qu'elles soient positives ou négatives. Je pense que la première fois que j'ai déclaré cela, ce devait être en 2013, alors j'étais forcément curieuse de savoir combien de fois cela avait pu être énoncé ensuite sur les années suivantes. Pour chaque année de 2009 à 2015, ces termes de recherche ont donné plus d'un million de résultats.Par la suite, chaque année n'a donné « que » huit à neuf cent mille résultats.

Est-ce que cela signifie que 2016 a été l'année la plus marquante pendant laquelle de nombreuses personnes ont collectivement baissé les bras et abandonné tout espoir d'avoir le contrôle sur leurs données personnelles ? D'une certaine façon, cela a pu être le cas ; il semble y avoir eu un certain sentiment de résignation globale. Mais il semble aussi que nous avions, à ce moment-là, atteint un point où les législateurs et les jugescommençaient à comprendre la colère collective provoquée par un flot con stant de dérapages et de violations diverses de la vie privée.

Et cette prise de conscience s'est intensifiée - rien qu'en 2019, nous avons vu un certain nombre de *pays* et d'États américains *adopter ou mettre en œuvre de nouvelles lois ou extensions sur la notification des violations*. Nous avons également *plusieurs états américains* squi ont mis en place une législation sur la confidentialité des données (bien que seule la Californie ait adopté cette législation). SPlusieurs amendes notables ont été infligées à des sociétés responsables pour de *récentes fuites* de *données* bien qu'elles soient généralement considérées comme de petites punitions sans grande conséquence). Les dirigeants *des entreprises oncernées* ont dû témoigner devant les audiences du Congrès sur ces incidents.

Les changements ont été lents et on peut dire que ces efforts n'ont pas encore fait une grande différence positive. Il existe un consensus général au sein d'une grande partie de la population américaine sur le fait qu'elle estime *ne pas pouvoir faire confiance* aux entreprises pour protéger ses données et c'est également le cas dans *d'autres pays*. Cette situation, ainsi que la fraude omniprésente en plus d'autres trafics malveillants, a créé *un environnement de « faible confiance »* dans lequel nous sommes de plus en plus interconnectés et dans lequel nous nous sentons de plus en plus en danger.Lorsque l'on doit aborder tout ce qui se passe sur Internet avec paranoïa et scepticisme, les gens sont naturellement plus frileux à l'idée de s'y engager.

Dans le domaine de la sécurité, on dit souvent que la meilleure pratique consiste à « faire confiance, mais toujours vérifier » : dans la situation actuelle, la méfiance est omniprésente et les méthodes de vérification sont pleines de lacunes.Tant que nous n'aurons pas remédié à cela, Internet continuera d'être un endroit inquiétant pour la plupart des individus.

Que faut-il faire pour sortir de ce sentiment de méfiance omniprésent ?

Confidentialité et sécurité dès la conception

L'une des choses les plus importantes à faire pour améliorer la confiance des clients, c'est de créer des produits et services technologiques qui sont imaginés dès le départ avec l'idée de sécurité et de confidentialité. L'International Association of Privacy Professionals (IAPP) a créé un document décrivant ses recommandations pour les principes de *confidentialité dès la conception*

Une grande partie de ce qui y est répertorié correspond à ce à quoi on pourrait s'attendre : obtenir la confiance grâce à l'ouverture et à la transparence, mettre en place une sécurité de bout en bout, créer des politiques qui établissent la responsabilité de l'entreprise et obtenir un *consentement vraiment éclairé et en continu* auprès des clients. Mais il y a une autre recommandation particulièrement marquante et qui pourrait surprendre beaucoup de monde : permettre une fonctionnalité complète qui puisse respecter la vie privée, tout en profitant à la fois à l'entreprise et à l'utilisateur.

Le modèle actuel pour une grande partie d'Internet tend à utiliser les données des clients comme un produit à vendre, alors forcément cette recommandation particulière peut nécessiter une réflexion vraiment innovante, « hors des sentiers battus ». Les entreprises qui réussissent à accomplir cet exploit sont susceptibles d'avoir un avantage significatif sur le marché.

Améliorer la technologie des publicités

Puisque nous traitons de la vente de données sur les clients, nous devrions également discuter des améliorations nécessaires en matière de technologie publicitaire. Dans *un sondage*, moins de 20 % des personnes interrogées ont trouvé que les publicités ciblées pouvaient être considérées comme éthiques. *D'autres sondages* ont révélé que, dans certains cas, les publicités ciblées pouvaient en fait avoir l'effet inverse et causer une baisse de l'interaction avec les clients.

Les entreprises qui utilisent des tactiques de vente sous haute pression telles que *rareté et la démonstration sociale* ne s'en sortent pas bien non plus.Un sondage réalisé au Royaume-Uni a révélé que près de la moitié des sondés affirment se méfier du fournisseur en raison de ce comportement. Un tiers a exprimé une réaction émotionnelle négative (comme le dégoût ou le mépris). Et 40 % ont déclaré que ces stratégies leur donneraient envie de faire le contraire de toute action proposée.

Plus nous sommes bombardés par des stratégies de vente sous haute pression et des ruses de surveillance effrayantes, plus leur efficacité (très limitée) diminue rapidement. Grand nombre de vendeurs ont abusé de ces stratégies ce qui a probablement limité les opportunités pour d'autres entreprises également. Nous avons besoin de moyens de commercialisation plus efficaces qui soient honnêtes, transparents et respectueux de nos clients potentiels.

Conséquences législatives des atteintes à la confiance

Il y a peu de chances que le sentiment du public sur la fiabilité des entreprises technologiques s'améliore tant qu'il n'y aura pas de conséquences au moins aussi importantes pour les sociétés que leurs clients en cas d'incidents liés à la confidentialité. Bien que les récentes amendes pour violation de la vie privée aux États-Unis et au Royaume-Uni battent des records, elles représentent une goutte d'eau minuscule par rapport aux revenus que les grandes entreprises tirent de nos données. Tant que ces amendes ne seront pas suffisamment hautes proportionnellement *au revenu d'une société*, elles continueront d'être plus dissuasives pour les petites sociétés que pour les entreprises de grande envergure.

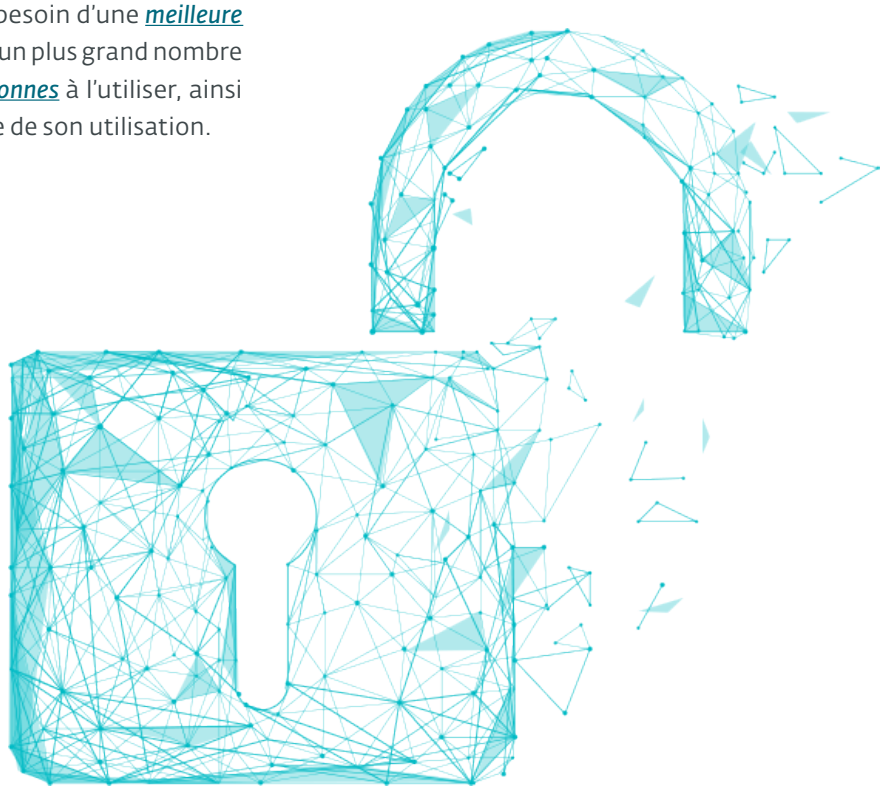
Améliorer l'authentification et la vérification

Les noms d'utilisateur et les mots de passe ne suffisent tout simplement plus à protéger l'identité des individus. Cela peut diminuer la confiance des utilisateurs de comptes en ligne ainsi que celle des personnes qui interagissent avec des comptes potentiellement détournés. L'authentification multifacteur *améliore considérablement* cette situation, mais *très peu de gens* l'ont encore adoptée. Pour changer cela, nous aurons besoin d'une *meilleure éducation* sur cette technologie, d'un plus grand nombre d'entreprises pour *inciter les personnes* à l'utiliser, ainsi que d'une amélioration constante de son utilisation.

Changeons de cap

On m'a initialement demandé de prédire l'état de la sécurité sur Internet dans dix ans, il y a un peu plus de dix ans.. J'ai dit que je voyais les choses de deux façons : soit nous nous ressaisissions collectivement et les choses ase dérouleraient pour le mieux, soit nous ne nous en occupions pas et nous laissions Internet devenir un « terrain miné ».Personne ne peut affirmer sans hésiter que les gens utilisent moins Internet qu'il y a dix ans, toutefois nous faisons face à davantage de déchets sur Internet qu'il n'y en avait dans les années 2000.

Les anciens parmi nous qui travaillent dans le domaine de la cybersécurité depuis les débuts de l'industrie vivent dans cet état de méfiance depuis des décennies ; nous avons vu l'Internet se construire sur des fondations chancelantes et peu de choses ont été faites (voire même rien du tout) pour empêcher les abus.Heureusement, nous avons également réfléchi - et parlé - de ce qui devait être fait pour y remédier. Il n'est pas trop tard pour prendre des mesures significatives afin de remettre les efforts de protection de la confidentialité dans la bonne direction. J'espère que le désir de faire les changements nécessaires continuera de croître, de sorte que nous puissions apporter ces améliorations avant la fin de "ma" prochaine décennie dans ce domaine.



L'INTELLIGENCE ARTIFICIELLE DONNE : DE L'IOT AUX VILLES INTELLIGENTES

4

- Bâtiments intelligents
- Villes intelligentes
- Attaques des infrastructures intelligentes
- Malware
- Vol d'identité et de données
- Conclusion

Cecilia Pastorino
Chercheuse en Sécurité
chez ESET

L'intelligence artificielle donne le la : De l'Iot aux villes intelligentes

Alors que de plus en plus de villes sont dotées de technologies intelligentes qui modifient la façon dont les municipalités gèrent leurs opérations et leurs services de base, que signifient ces développements pour ce qui est de la sécurité ?

Depuis 1994, date de l'apparition du tout premier téléphone intelligent, le mot « intelligent » en est venu à décrire tout type d'appareil obtenant une fonctionnalité améliorée grâce à un logiciel et généralement une connexion Internet. Puis, en 1999, l'informaticien Kevin Ashton est devenu la première personne à utiliser l'expression « Internet des objets » (IoT). Depuis, les attentes autour de cette notion n'ont cessé d'augmenter.Les années 2010 ont été marquées par la révolution de l'Internet des objets et des produits tels que les montres, les thermostats, les lumières, les serrures, les appareils photo, les jouets, les réfrigérateurs et autres appareils intelligents font maintenant partie de nos maisons, bureaux, immeubles et même de villes intelligentes.

Aujourd'hui, le potentiel de l'Iot ne se limite pas seulement à l'automatisation des tâches, mais comprend des processus analytiques qui peuvent être réalisés sur les vastes quantités d'informations obtenues. Les structures intelligentes utilisent une variété de technologies interdépendantes, comme l'apprentissage automatique, divers protocoles de réseau sans fil, l'informatique dans le cloud et les capteurs et dispositifs de l'IoT La vaste quantité d'information générée par les capteurs et les dispositifs en réseau est stockée dans d'énormes bases de données et traitée au moyen de l'apprentissage automatique et de l'analyse des données à grande échelle, dans le but d'améliorer l'efficacité opérationnelle et de développer un environnement sûr et productif. De telles caractéristiques ont permis de qualifier ces systèmes d'« intelligents », mais « intelligents » ne signifie pas toujours « sécurisés ». Tandis que la technologie continue de faire d'énormes progrès, certains d'entre nous se demandent quand, enfin, la sécurité sera intégrée à ces changements dès la conception.

Bâtiments intelligents

Les bâtiments intelligents utilisent la technologie pour contrôler un large éventail de paramètres dans leur environnement, dans le but de fournir plus de confort et de contribuer à la santé et à la productivité des personnes qui y travaillent ou y vivent. Pour ce faire, ils utilisent les systèmes d'Immotique. Grâce à des équipements tels que divers capteurs (lumière, température, qualité de l'air), des caméras, des contrôles d'accès, etc., un système immotique est capable d'analyser, de prévoir, d'exécuter des diagnostics et de maintenir diverses conditions environnementales, ainsi que d'automatiser des processus et de surveiller de nombreux paramètres en temps réel. Parmi les exemples, citons l'optimisation de la consommation d'énergie pour le contrôle de la température et de l'éclairage des pièces, ainsi que la surveillance automatique des systèmes de caméras de sécurité, des ascenseurs et des parkings, entre autres.

Les avantages du recours aux dispositifs intelligents sont multiples. Par exemple, comme *le raconte Tony Anscombe, évangéliste mondial de la sécurité chez ESET*, un hôtel bien connu de Las Vegas a automatisé la climatisation pour qu'elle ne fonctionne que lorsque les chambres sont occupées, ce qui a permisd'économiser 2 millions de dollars US au cours de la première année suivant l'installation du système. Selon le rapport *Smart Buildings Market 2019-2024* , dans des pays comme les États-Unis, le marché des bâtiments intelligents - y compris les entrepôts, les usines, les immeubles de bureaux et autres structures d'entreprises, industrielles et gouvernementales - devrait croître de 16,6 % d'ici 2020 par rapport à 2014. Ainsi, plus de 80 % des nouveaux bâtiments d'aujourd'hui intègrent au moins un élément de l'IoT et des technologies liées au marché des bâtiments intelligents.

Villes intelligentes

En 2019, le *CES* comprenait une zone entière consacrée aux initiatives de villes intelligentes actuellement en cours de réalisation (ou en planification) dans le monde. Certaines d'entre elles visent à améliorer les transports en utilisant des capteurs pour évaluer les flux de circulation, puis à contrôler les feux de circulation sur la base de ces mesures.D'autres servent à automatiser l'éclairage grâce à des capteurs de lumière, à mesurer les températures, à incorporer des systèmes de surveillance constitués de réseaux de caméras et de nombreux autres capteurs pour recueillir des informations qui sont ensuite analysées dans une station de surveillance afin d'avoir un aperçu de tout ce qui se passe dans la ville. Tout comme dans les bâtiments intelligents, mais à plus grande échelle, tout tourne autour de capteurs qui recueillent des informations et où l'apprentissage automatique est utilisé pour analyser les données afin d'automatiser efficacement un service correspondant.

Le problème est que bon nombre de ces villes ne sont pas totalement préparées à gérer en toute sécurité les grands flux d'information produits par ces systèmes, et un pirate pourrait facilement avoir accès aux capteurs, ajuster les mesures et apporter des modifications aux services utilisés dans les transports, la circulation, l'éclairage ou d'autres infrastructures essentielles. Nous avons déjà vu des démonstrations de principe de différents types d'attaques contre les villes intelligentes et les *systèmes automatisés*lors de conférences telles que *Black Hat* et DEF CON.De plus, si des villes comme Atlanta, dont *l'objectif est de devenir une ville intelligente de premier plan mondial*, n'ont pas réussi à éviter les menaces qui existent déjà, comme notamment les *rançongiciels* comment pouvons-nous imaginer qu'elles seront en mesure de faire face à des menaces encore plus importantes ? Les experts s'inquiètent du fait que les villes intelligentes connaissent une croissance rapide, mais que notre capacité à les rendre sécurisées *ne suive pas*

Attaques des infrastructures intelligentes

D'une part, il semblerait que les attaques contre les bâtiments et les villes intelligents ne puissent être menées qu'à l'aide de plans détaillés dans lesquels les cybercriminels visent une cible spécifique. Mais d'autre part, de nombreux systèmes immotiques, ainsi que les capteurs et appareils utilisés dans les villes intelligentes, sont directement exposés à Internet. Actuellement, les recherches sur des outils tels que Shodan et Censys renvoient les résultats de plus de 35 000 systèmes immotiques, ainsi que des centaines de milliers d'appareils indispensables et accessibles au public sur Internet.

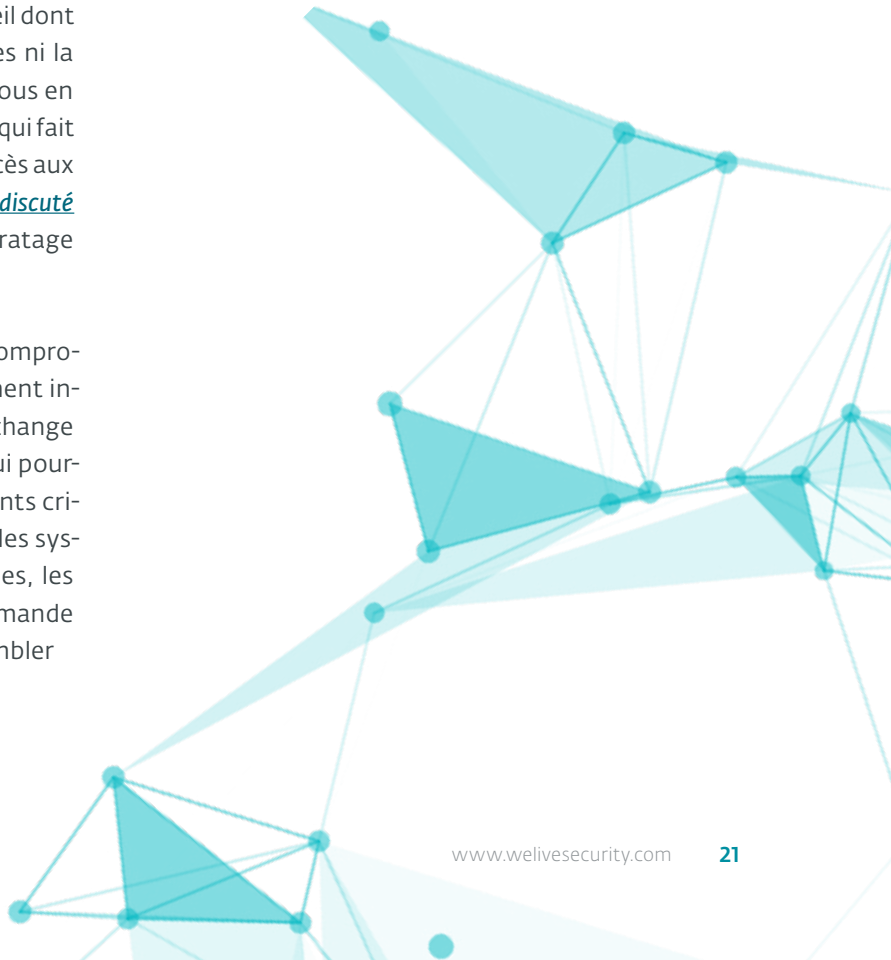
Beaucoup de ces dispositifs et systèmes n'ont pas de systèmes d'authentification suffisamment solides, ni de protection contre les attaques par force brute, ne sont pas mis à jour, ne sont pas protégés par une solution de sécurité quelconque ou ont simplement des configurations non sécurisées qui pourraient permettre à un attaquant de prendre le contrôle de l'équipement.

Malware

Bien que les systèmes utilisés par les bâtiments intelligents et les villes ne naviguent pas sur le web ou n'ouvrent pas de courrier électronique, ils doivent néanmoins se protéger contre les logiciels malveillants, qui pourraient donner à un cybercriminel l'accès à des informations critiques ou causer des dommages matériels. Un code malveillant peut être propagé par l'interface d'accès web utilisée pour administrer les dispositifs IoT, par les vulnérabilités des systèmes et même par l'accès physique à des ports USB non protégés ou à la portée de toute personne passant par là. Il est également important de ne pas négliger la protection du réseau, en particulier dans les endroits où les utilisateurs brancheront des appareils personnels, qui pourraient être compromis.

Les systèmes utilisés par les bâtiments et les villes intelligents pourraient être attaqués, par exemple, par des *botnets*qui visent les appareils intelligents. Est-ce exagéré d'imaginer que, dans un avenir proche, les ressources de l'IoT d'une ville entière pourraient être détournées par un attaquant pour générer des millions de dollars grâce à l'extraction de crypto-monnaies ? Et le cryptojacking n'est pas la seule menace. Il y a trois ans dans *nos tendances 2017: Personne n'est épargné* nous avons présenté le concept de jackware pour décrire un malware qui tente de prendre le contrôle d'un appareil dont le but premier n'est ni le traitement de données ni la communication numérique. Immédiatement nous en avons déduit le concept de *Ransomware of Things*, qui fait référence aux malwares capables de bloquer l'accès aux appareils intelligents. Cette année-là, *nous avons discuté d'une démonstration de faisabilité* concernant le piratage à distance d'une voiture en mouvement.

Que se passerait-il si un attaquant parvenait à compromettre le système d'automatisation d'un bâtiment intelligent et menaçait de causer des dégâts en échange d'une rançon à payer ? Les types de systèmes qui pourraient être compromis comprennent des éléments critiques tels que le chauffage et la climatisation, les systèmes de détection et d'extinction des incendies, les contrôles d'accès, l'éclairage et le centre de commande et de contrôle du bâtiment. Ce scénario peut sembler être l'intrigue d'un film de science-fiction, mais en fait des incidents qui mélangent le concept de rançongiciel avec celui d'immotique ont déjà été signalés - et *nous l'avons baptisé siegeware*



Vol d'identité et de données

L'accès physique aux bâtiments intelligents tend à être contrôlé par des systèmes informatiques dans lesquels les utilisateurs s'identifient à l'aide de données biométriques ou de jetons d'authentification. Ces systèmes peuvent être compromis par l'ingénierie sociale ou par des lacunes dans leur application, ce qui pourrait permettre à une personne non autorisée d'avoir un accès physique à des secteurs restreints.

De plus, le vol d'identité numérique peut causer des dégâts si les attaquants obtiennent des privilèges d'administrateur, qui leur permettent de contrôler le(s) système(s) à leur guise.Une fois que les attaquants parviennent à disparaître avec les autorisations d'accès de la victime, ils peuvent continuer à installer des codes malveillants, à voler des informations, à naviguer dans le système et à effectuer toutes sortes d'activités dommageables.

Les capteurs et dispositifs de l'IoT utilisés dans la plupart des bâtiments et infrastructures intelligents peuvent également servir de point d'entrée au réseau. C'est le cas d'un casino qui a *été victime d'une attaque* dans laquelle des cybercriminels sont entrés dans son réseau après avoir exploité une vulnérabilité dans le thermostat intelligent d'un aquarium dans le hall. Ils ont ensuite accédé à la base de données du casino, volant des informations qui comprenaient les données personnelles des joueurs.

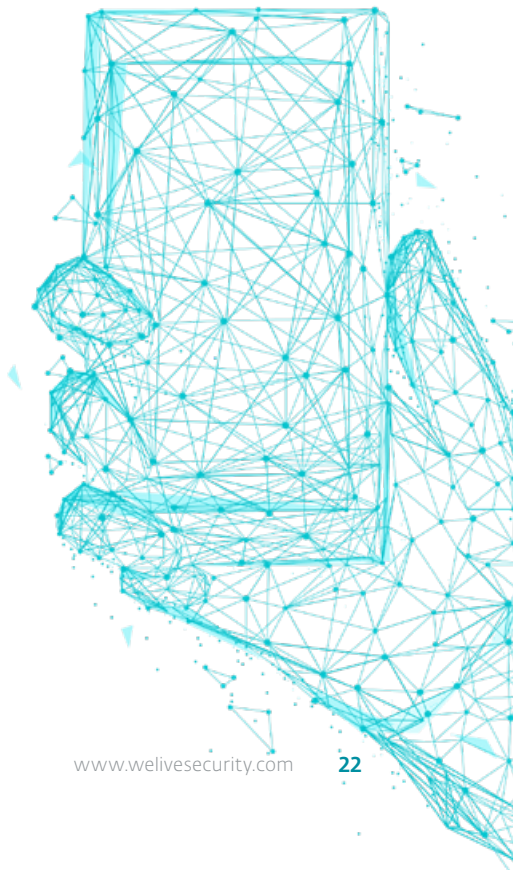
Conclusion

Les villes et les bâtiments intelligents ne sont plus l'objet d'une lubie de science-fiction, mais une réalité du monde dans lequel nous vivons. Jusqu'à présent, les incidents de sécurité signalés ont été suffisamment rares pour qu'on puisse les considérer comme des cas isolés. Pourtant, il est clair que les systèmes de contrôle des bâtiments et des villes sont devenus des cibles pour les cybercriminels.

Les mesures de sécurité à prendre pour faire face à ces nouvelles menaces sont les mêmes que nous mettons toujours en avant à chaque nouvelle vague d'évolution technologique : allouer un budget suffisant pour la sécurité, acheter auprès de fournisseurs qui ont intégré la sécurité au moment de l'achat, mettre en place des programmes de traitement des vulnérabilités, tenir les systèmes à jour, surveiller le réseau et les périphériques et vous assurer que vous disposez d'outils de sécurité et du soutien de partenaires ayant des connaissances dans le domaine de la sécurité

De plus, il y a un besoin évident d'appuyer la législation pour rendre obligatoire la sécurité dès la conception des dispositifs intelligents, et c'est quelque chose qui risque de se produire dans les années à venir, surtout à la lumière des *initiatives récentes au Royaume-Uni* et en Californie. Tout comme il existe des normes pour réglementer les équipements essentiels, il est temps de commencer à analyser quelles normes et mesures de sécurité devraient être des exigences minimales pour les appareils intelligents qui interagissent avec nos données et notre vie privée.

Beaucoup d'entre nous vivent déjà dans des villes avec des myriades de capteurs et de caméras connectés à Internet. IDans un avenir relativement proche, nous passerons une grande partie de notre vie quotidienne à travailler et à faire des achats dans des bâtiments hyperconnectés et remplis de technologie. Et si tous ces progrès peuvent sembler passionnants et impressionnants, nous ne devons pas oublier que derrière tout cela, il y a avant tout des personnes intelligentes.



SÉCURISER LA TRANSFORMATION NUMÉRIQUE

- Les changements informatiques doivent être changements dans la gestion de la cybersécurité
- La diversité technologique comme vecteur de changement
- La voie vers la mobilité
- Concepts à retenir dans la transformation numérique
- Quelles mesures doivent prendre les entreprises ?

Camilo Gutiérrez Amaya
Chercheur en sécurité
chez ESET

Sécuriser la transformation numérique

En s'engageant ou en poursuivant sur la voie de la transformation numérique, les organisations doivent repenser tous les aspects de leurs activités. Il semble compliqué de récolter les "lauriers" de la transition digitale sans jamais subir les aléas négatifs liés à l'incapacité à relever les défis sous-jacents de la cybersécurité.

À cause de la dynamique du marché, la transformation numérique est devenue une question essentielle qui a un effet sur tous les aspects des affaires d'une organisation. Le déploiement de toutes ces nouvelles technologies - un processus que de nombreuses organisations ont amorcé il y a quelques années en vue d'offrir plus de valeur à leurs clients - exige un changement culturel au niveau administratif. Rien d'étonnant donc à ce que cela représente un défi majeur pour toutes les organisations concernées.

Naturellement, la sécurité de l'information ne doit pas être considérée comme indépendante de ces efforts. Il s'agit plutôt d'une étape importante des objectifs que les entreprises doivent planifier afin d'éviter d'être en retard dans la course en raison de lacunes en matière de cybersécurité.

La transformation numérique tend à impliquer de repenser les processus et les stratégies de chaque organisation et, ce faisant, de permettre à tous de bénéficier de la technologie numérique. D'autre part, cela entraîne de nouveaux risques - et les entreprises ne doivent pas perdre de vue ces dangers.

Les changements informatiques doivent être accompagnés d'évolutions dans la gestion de la cybersécurité

Les organisations qui subissent déjà des changements qui font partie de leur transformation numérique ont découvert qu'elles étaient désormais confrontées à l'élaboration de modèles économiques comportant une importante composante technologique et, par conséquent, leurs équipes informatiques ont dû s'adapter afin de soutenir la vitesse de ce changement.

Tous ces changements signifient que, peu à peu, les organisations passent de la concentration de la majorité de leurs ressources à l'adoption d'une pléiade de nouveaux services et actifs pour soutenir leurs activités quotidiennes, entraînant une diversification des technologies et des plateformes à surveiller.

TCe délicat processus de transformation - qui, selon une enquête de *McKinsey*, a été entrepris par huit organisations sur dix au cours des cinq dernières années - a eu des conséquences directes sur la posture de ces dernières en matière de cybersécurité. Les organisations doivent œuvrer activement à limiter les risques d'être victimes d'une cyberattaque ou d'une fuite de données. Par conséquent, les membres de la direction se sont retrouvés plongés dans de nouveaux paradigmes qui leur permettent d'accomplir cette mission, sans pour autant nuireà leurs activités commerciales normales. Afin de fonctionner correctement dans un écosystème numérique, les sociétés doivent être en mesure de sécuriser leurs données pendant la phase de transformation.

Selon une *étude* réalisée par le Ponemon Institute dans plusieurs pays en 2018, 72 % des professionnels de la sécurité informatique estiment qu'un sentiment d'urgence autour de la transformation numérique augmente le risque de fuite de données.Si l'on ajoute à cela le fait que 45 % des organisations disent ne pas avoir de stratégie pour faire face à la transformation numérique, c'est pour le moins préoccupant.

Il est essentiel pour les équipes de sécurité d'avoir un flux constant d'informations sur tous les changements qui se produisent au sein de leur organisation. C'est pourquoi les technologies intelligentes, y compris la surveillance des menaces, sont importantes pour fournirune base sur laquelle d'autres processus peuvent être exécutés en toute sécurité, en maintenant la conformité aux normes dans toute l'organisation.

La diversité technologique comme vecteur de changement

Les entreprises doivent prendre en compte la sécurité de l'information dans le cadre du processus de numérisation. Comme de multiples technologies sont maintenant disponibles pour ce processus - notamment le *cloud computing*, les plateformes mobiles, la connectivité 5G et l'apprentissage automatique, pour n'en citer que quelques-unes - il est important de comprendre qu'aucune technologie ou application ne suffira à elle seule à garantir la sécurité des données et la pérennité des activités.

L'un des obstacles principaux pour les entreprises qui se lancent dans le processus pourrait être de savoir par où commencer. En réalité, le point de départ consiste à comprendre que cette transformation change aussi radicalement et rapidement la société dans son ensemble, à savoir la façon dont nous travaillons, échangeons, achetons des choses et interagissons à tous les niveaux de notre vie quotidienne.

La voie vers la mobilité

De tous ces scénarios de changement au sein des entreprises, il en est un en particulier qui s'avèrera un facteur majeur d'accélération du processus en 2020 : la mobilité des salariés. Sans aucun doute, notre capacité à rester connecté aux réseaux, où que nous soyons, ne cesse d'augmenter les possibilités d'attaques contre les entreprises et leur exposition aux risques.

Tous ces changements ont eu lieu lentement mais sûrement au cours des dernières années, mais la vitesse toujours croissante d'adoption de la technologie mobile par les entreprises se fait souvent sans tenir compte de la sécurité. C'est pourquoi il est important que les sociétés cessent de penser à la sécurité de manière traditionnelle et envisagent plutôt d'adopter des modèles évolutifs qui peuvent répondre aux changements.

Et plus urgent encore, les équipes de sécurité informatique doivent se plonger tête la première dans l'utilisation des technologies de contrôle, car celles de détection seulement ne suffisent plus.Il est important pour les entreprises d'élaborer des processus d'intervention en cas d'incident, puis de ramener les opérations à la normale en réglant ces incidents et en appliquant les mesures correctives appropriées.

Concepts à retenir dans la transformation numérique

Outre ces technologies spécifiques, qui de toute façon continueront d'évoluer, nous ne devons pas perdre de vue des concepts clés comme la confidentialité. Nous vivons à une époque où de nouvelles *lois plus strictes sur la protection des données personnelles* sont continuellement adoptées. Il en résulte que les gens prennent progressivement conscience de leurs droits et sont de plus en plus préoccupés par la façon dont les entreprises traitent leurs données.

Au cours des prochains mois, les organisations entreprendront des changements majeurs dans la quasi-totalité de leurs domaines d'activité. Le dénominateur commun de toutes ces transformations résidera dans la manière dont les entreprises géreront les informations et les données dans le cadre de leurs opérations. Ainsi, les modèles commerciaux qui favorisent la confiance des clients seront un facteur de distinction.

Quelles mesures doivent prendre les entreprises ?

Il y a au moins cinq points clés sur lesquels les entreprisesdevront se concentrer au cours de l'année à venir pour gérer cette transformation en toute sécurité :

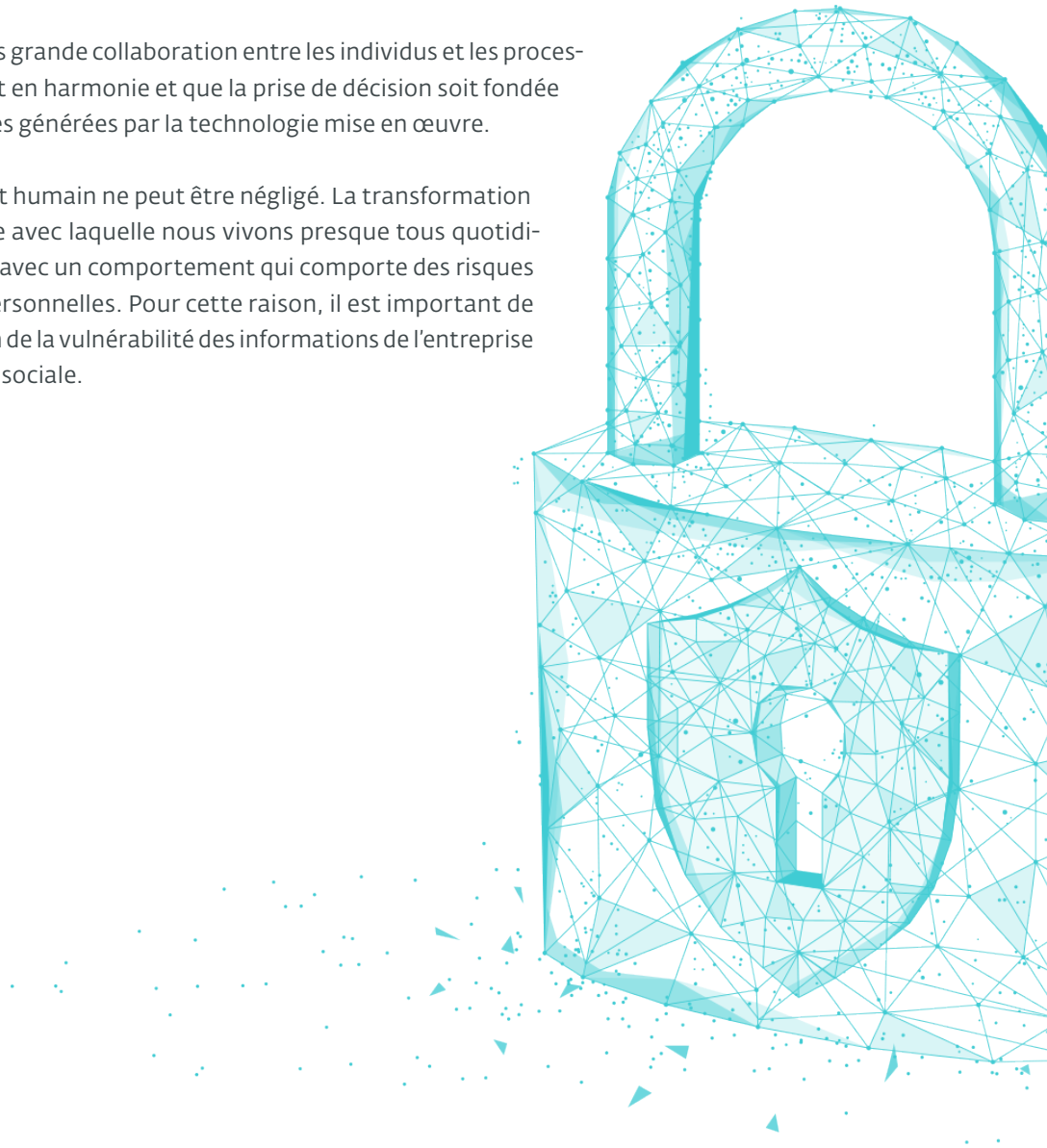
1. Trouver un équilibre entre l'implantation de nouvelles technologies et la cybersécurité. Si elles ne sont pas équilibrées dès le départ et si la sécurité n'est pas perçue comme un élément moteur pour l'entreprise, il y aura plus de problèmes que de solutions.

2. Développer des projets qui facilitent à la fois la visibilité et le contrôle des technologies. Il ne faudra pas seulement se concentrer sur la prévention des incidents, mais aussi sur la détection et l'intervention en cas d'incident.

3. La sécurité ne peut pas être axée uniquement sur les appareils, car la quantité d'équipements et de technologies ne cesse d'augmenter, ce qui complique le déploiement de la sécurité sur chaque appareil individuellement.

4. Il faudra favoriser une plus grande collaboration entre les individus et les processus afin que ceux-ci soient en harmonie et que la prise de décision soit fondée sur des données partagées générées par la technologie mise en œuvre.

5. Et bien entendu, l'élément humain ne peut être négligé. La transformation numérique est une chose avec laquelle nous vivons presque tous quotidiennement, mais souvent avec un comportement qui comporte des risques pour nos informations personnelles. Pour cette raison, il est important de travailler sur la prévention de la vulnérabilité des informations de l'entreprise aux menaces d'ingénierie sociale.



CONCLUSION

Les défis à venir sont sans aucun doute importants et nous devons nous y préparer, tant du point de vue technologique que pédagogique.De cette manière, les générations actuelles et futures disposeront de meilleurs outils pour relever ces défis, tandis que la technologie aura la possibilité de libérer son véritable potentiel, ce qui se traduira par une meilleure qualité de vie pour toute l'humanité.

Comme cette édition de nos tendances l'a amplement démontré, notre monde est manifestement appelé à continuer d'évoluer dans son utilisation de la technologie et à devenir (encore) plus « intelligent » qu'il ne l'est actuellement. Mais ce n'est que lorsque les progrès de l'intelligence artificielle auront réellement permis aux machines de penser par elles-mêmes, lorsque la transition vers ce que nous considérons comme des villes intelligentes sera devenue un phénomène mondial et enfin lorsque le processus de transformation numérique que de nombreuses entreprises engagent actuellement sera passé à l'histoire, que nous pourrons éventuellement analyser avec plus de précision quels ont été les coûts réels de ce processus.

Ce qui est certain, c'est qu'au vu de la situation actuelle, la cybersécurité continuera d'être considérée comme une question d'importance secondaire en matière de développement technologique. Et cela aura des conséquences à court terme.

D'une part, il y a des signes encourageants qui montrent que de plus en plus de gens commencent à reconnaître l'importance de la cybersécurité et la nécessité pour elle de jouer un plus grand rôle à l'avenir. Cependant, étant donné qu'au cours des cinq dernières années, huit entreprises sur dix se sont engagées sur la voie de la transformation numérique, et compte tenu de *l'augmentation des atteintes à la protection des données* à l'échelle mondiale et de *la hausse prévue des coûts* que les entreprises devront supporter pour y faire face, il semble impossible d'éviter ce type d'incidents

De plus, si l'on s'arrête de penser à la croissance prévue pour la construction de villes et de bâtiments intelligents, et au fait que de nombreuses villes qui sont actuellement investies dans le concept « d'intelligence » ont été victimes de menaces telles que les rançongiciels, quelles raisons avons-nous d'être optimistes et de croire que l'avenir sera meilleur en termes de pratiques sur la sécurité des données?

De même, si nous prenons comme points de référence les progrès actuels dans l'utilisation positive de l'apprentissage automatique, le phénomène des fake news, et ce que nous pouvons supposer du développement de l'IA dans le futur, le défi d'être préparé à ce qui nous attend réellement pourrait nous donner l'occasion de prendre des mesures qui donnent réellement à la cybersécurité un rôle significatif.

Les deepfakes nous ont déjà donné une idée de leur impact potentiel, en créant de la confusion et de l'incertitude sur ce qui est prétendument vrai ou faux. IEn retour, cela crée de la méfiance chez les personnes qui, en étant plus interconnectées, continuent d'exposer leurs données et leurs informations personnelles par manque de connaissance - ou de mise en œuvre - des pratiques de sécurité de base. De plus, beaucoup de ces personnes doivent voter lors des élections dans les pays qui ont opté pour le vote électronique, malgré les problèmes évidents que posent de tels systèmes.

Pour revenir à la question que nous avons posée plus tôt, il y a toutefois des signes positifs qui nous donnent des raisons d'être optimistes Des entreprises comme Facebook, ainsi que d'autres grands groupes et universités, ont démontré leur volonté de lutter contre des phénomènes tels que les deepfakes en lançant des initiatives telles que le *Deepfake Detection Challenge (DFDC)*, qui vise à promouvoir le développement de nouvelles technologies capables de lutter contre les deepfakes.

Par ailleurs, le paysage législatif et réglementaire relatif à la protection des données a récemment connu des changements. Bien que ceux-ci aient été lents à se produire et qu'ils n'aient peut-être pas encore eu un impact significatif, ils constituent au moins un progrès qui va dans la bonne direction.

Il y a encore beaucoup de travail à faire et les gouvernements doivent intervenir et promouvoir des mesures qui établissent un cadre et une directive pour la suite des choses. D'une part, il y a encore des lacunes dans la sensibilisation à de nombreux aspects de la sécurité des données.

D'autre part, la méfiance de nombreuses personnes à l'égard de la protection de leurs données personnelles reflète le fait qu'elles sont de moins en moins protégées par l'impact de la cybersécurité et de la confidentialité sur leur vie. Cela peut indiquer que, parmi l'ensemble des questions abordées dans le présent rapport de tendances, une meilleure éducation des consommateurs aux questions de cybersécurité est un facteur important à prendre en considération.


CYBERSECURITY
EXPERTS ON YOUR SIDE