Tout ce que vous devez savoir sur les cybermenaces sans jamais avoir osé le demander

Ben Bourne
Directeur des services à la clientèle pour l'Europe, le Moyen-Orient et l'Afrique

Magdalena Borcal
Directrice des services à la clientèle pour l'Europe, le Moyen-Orient et l'Afrique

Nathan Birtle
Vice-président des ventes et du développement pour l'Europe, le Moyen-Orient et l'Afrique

Les conseils d'administration ignorent trop souvent les risques de sécurité qui pèsent sur leur organisation.

C'est ce que le Ponemon Institute a découvert en juin dernier alors qu'il sondait les membres des conseils d'administration et experts en sécurité informatique des mêmes entreprises. Selon les chercheurs du Ponemon Institute, 30 pour cent des membres du conseil d'administration[1] reconnaissent ne pas comprendre les risques de sécurité auxquels fait face leur organisation. Pourtant, plus de la moitié des experts en sécurité informatique croient que les membres du conseil d'administration qui siègent dans leur entreprise ne comprennent pas l'environnement de sécurité dans lequel ils travaillent ni la menace qu'il représente.

C'est énorme, quand on pense au nombre de violations de données que les entreprises ont subies. D'après le rapport[2] 2015 du Kaspersky Lab, quelque 90 pour cent des grandes entreprises ont déjà connu une cyberattaque. Les tiers malveillants, ces cybercriminels résolus à collecter des informations en recourant à un logiciel malveillant ou au vol, sont souvent pointés du doigt en cas de violation.

Si les membres d'une organisation ne reconnaissent pas les principales menaces à la sécurité ni leurs conséquences fâcheuses pour l'organisation, les choses peuvent rapidement devenir coûteuses. D'ici 2019, le cybercrime devrait atteindre 2 000 milliards[3] de $ de pertes pour les entreprises. Ces pertes peuvent résulter de simples erreurs qui entraînent des violations de données : un assistant qui clique sur un lien dans un courriel d'hameçonnage, un commercial qui laisse son smartphone dans un café ou un membre du conseil d'administration qui ouvre une pièce jointe malveillante envoyée depuis un compte de messagerie usurpé. Sans avoir été sérieusement sensibilisé et formé à la sécurité, chaque personne expose celle-ci à des violations de données ou à leurs conséquences, y compris à des amendes coûteuses et, souvent, à des retombées catastrophiques pour sa réputation. Mais, pour améliorer le quotient intellectuel de sécurité, il est essentiel que chaque membre de l'organisation comprenne mieux où se situent les risques et quelles sont les mesures à prendre pour écarter toute menace potentielle.

Diligent

1. "Dell SecureWorks and Ponemon Institute Present the 2015 Global IT Security Spending & Investments Report" https://www.secureworks.com/about/press/ponemon-2015-global-security-spending-report
2. "90 per cent of companies have suffered at least one cyber attack" Ian Barker, October 7, 2015. BetaNews http://betanews.com/2015/10/07/90-percent-of-companies-have-suffered-at-least-one-cyber-attack/
3. "Cybercrime will cost businesses over $2 trillion by 2019" Juniper Research, May 12, 2015 https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

LES RISQUES

Les menaces internes

La principale menace pour la sécurité de toute entreprise provient des personnes qui ont directement accès au réseau et aux données sensibles. C'est ce qu'affirment différentes études, parmi lesquelles le rapport 2016[4] de Verizon sur les violations de données et le rapport « Battling the Big Network Security Hack »[5] [Lutte contre le piratage à grande échelle de la sécurité des réseaux] publié par la société Spiceworks, spécialisée dans la surveillance de la sécurité.

Les menaces internes se traduisent de différentes manières, mais souvent, les actions menées ne sont pas sciemment malveillantes. Mais malveillants ou pas, ces actes ont des conséquences graves pour la sécurité. Il peut s'agir parfois de la simple perte d'appareils non verrouillés, de l'utilisation de terminaux ne disposant d'aucun logiciel d'effacement des données, ou encore de la connexion à un ordinateur de dispositifs de stockage non vérifiés. Même dans une grande entreprise, il suffit d'une seule mauvaise action ou d'un simple clic pour provoquer des millions de dégâts et entraîner des coûts de réparation tout aussi élevés.

Un sondage[6] réalisé par Thomson Reuters a mis en lumière que les membres des conseils d'administration étaient eux-mêmes à l'origine de divers risques de sécurité. Par exemple, plus de la moitié des membres du conseil continuent d'imprimer et de transporter des documents de conseil qu'ils pourraient perdre ou égarer. Les données sensibles d'entreprise risquent ainsi d'être récupérées et compromises par des personnes extérieures à l'organisation.

Médias sociaux

Les réseaux sociaux constituent une arme à double tranchant. D'une part, ils permettent aux organisations d'atteindre leur public en temps réel en lui adressant un message ciblé. Ils facilitent et accélèrent aussi la communication entre l'entreprise et le client.Mais d'autre part, les médias sociaux peuvent également être la source de catastrophes de cybersécurité. D'après un rapport d'IFSEC Global[7], une communauté virtuelle spécialisée en sécurité, la majorité des professionnels de l'informatique et de la sécurité informatique ont constaté que les médias sociaux utilisés sur le lieu de travail créaient un risque majeur, mais que les organisations étaient très peu nombreuses à prendre la menace au sérieux. Les comptes de votre entreprise sur les médias sociaux pourraient être piratés et utilisés pour lancer des attaques d'ingénierie sociale destinées à escroquer les clients et toute personne associée à l'organisation. Il n'est pas à exclure que ces attaques ruinent la réputation de votre entreprise et qu'elles favorisent les téléchargements de logiciels malveillants, les vols d'informations d'identification personnelle et les fuites de données.

Appareils multiples

Un rapport[8] publié par Citrix indique que l'employé moyen utilise au moins trois appareils qu'il connecte au réseau de l'entreprise. Cette information est confirmée par une étude[9] menée par GlobalWebIndex selon laquelle une personne utilise généralement trois appareils et que leur nombre augmente avec le niveau de revenu. Compte tenu de cette réalité, on peut raisonnablement affirmer que la plupart des membres des conseils d'administration possèdent au moins quatre appareils. Plus de 60 pour cent se connecteront au réseau hors de leur bureau. Si le mouvement Bring your own device [Apportez vos appareils personnels] (BYOD) permet aux entreprises de diminuer leurs dépenses en investissements d'appareils, il implique aussi que le service informatique a moins d'emprise sur le logiciel, sur les pratiques de sécurité et sur l'accès en général. Les problèmes de sécurité liés à ces appareils devraient empirer. Selon la société de recherche Gartner[10], plus de 6 milliards d'appareils seront connectés à Internet en 2016. Les employés seraient en mesure de connecter une grande variété d'appareils au réseau Wi-Fi d'une entreprise, et en raison des vulnérabilités propres aux systèmes d'exploitation de bon nombre de ces appareils, les entreprises pourraient être exposées à des risques de sécurité et à des piratages clandestins.

Technologies émergentes

Toute nouvelle avancée technologique finira par devenir une cible pour les pirates et autres acteurs malveillants, ce qui signifie que la technologie utilisée par les membres des conseils d'administration pourrait exposer ceux-ci et l'organisation toute entière à un risque accru pour la sécurité. Selon ZDNet[11], les experts en sécurité s'accordent à dire que les voitures et bâtiments intelligents ainsi que les appareils mobiles les plus récents peuvent être et seront attaqués tôt ou tard. Même si la technologie émergente n'est pas directement connectée aux centres de données de votre entreprise, il est possible qu'elle ouvre la voie à d'autres modes d'intrusion dans votre organisation. Des voleurs pourront s'introduire dans le bâtiment si son système de sécurité est piraté. C'est ce que les chercheurs de l'université du Michigan[12] ont prouvé en parvenant à pénétrer par effraction dans le système de sécurité d'une maison intelligente.

Authentification des utilisateurs

Des systèmes d'authentification des utilisateurs tels que les mots de passe sont censés assurer la sécurité des données et des comptes, mais les mots de passe volés sont également une mine d'or pour les voleurs de données. Selon un rapport[13] de Trend Micro, si les mots de passe représentent un précieux sésame, le mode d'accès aux comptes visés peut avoir des conséquences plus graves sur la sécurité, comme un membre du conseil d'administration de Shipley Energy[14] en a fait l'expérience en découvrant qu'un pirate avait exploré ses courriels et son ordinateur travail d'exploration particulièrement simple pour les cybercriminels. En l'absence de systèmes d'authentification multi-facteurs à l'échelle de l'entreprise (y compris au conseil d'administration), les utilisateurs non autorisés n'auront aucun mal à s'introduire dans le réseau.

Fournisseurs externes

Les fournisseurs externes sont responsables de quelques-unes des violations majeures observées ces dernières années. Target en est sans doute l'exemple le plus notoire, dans la mesure où la violation qu'il a subie était due à des erreurs de sécurité commises par un

4. « Leaky end users star in DBIR 2016 » [Les utilisateurs finaux à l'origine de fuites font la une du rapport d'enquête de 2016 sur les violations de données], Susan Richardson, le 23 mai 2016. Data on the Edge, http://blog.code42.com/leaky-end-users-star-in-dbir-2016/
5. « Battling the Big Hack: Inside the ring and out… IT pros plan to land some blows in 2016 » [Combattre le piratage à grande échelle : de l'intérieur comme à l'extérieur… Les pros de l'informatique prévoient d'être offensifs en 2016], Spice Works, décembre 2015 : https://www.spiceworks.com/marketing/resources/reports/it-security/?utm_function=dg&utm_channel=swemail&utm_source=securitypromo&utm_medium=email&utm_ campaign=2016itsecurity&utm_content=151216-button&mkt_tok=3RkMMJWWfF9wsRoksqrMd%2B%2FhmjTEU5z16egrXaS2glkz2E-Fye%2BLIHETpodcMTsFgNrvYDBceEJhqyQJxPr3MJNkN1NxvRhnjCQ%3D%3D
6. « Are your board members a security risk? » [Les membres de votre conseil d'administration représentent-ils un risque pour la sécurité ?] Thomson Reuters, http://www.biia.com/is-your-board-member-a-security-risk
7. « Global Survey: Malware attacks up because of social media » [Sondage international : augmentation des attaques de logiciels malveillants liées aux médias sociaux], IFSEC Global, le 12 octobre 2011. http://www.ifsecglobal.com/global-survey-malware-attacks-up-because-of-social-media/
8. « 7 Enterprise Mobility Statistics You Should Know » [7 statistiques concernant la mobilité de l'entreprise que vous devriez connaître], Citrix, le 12 juin 2015 https://www.citrix.com/articles-and-insights/workforce-mobility/jun-2015/7-enterprise-mobility-statistics-you-should-know.html
9. « Digital consumers own 3.64 connected devices » [Les consommateurs de numérique possèdent 3,64 appareils connectés], Global Web Index, le 18 février 2016 http://www.globalwebindex.net/blog/digital-consumers-own-3.64-connected-devices
10. « 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015 » [6,4 milliards d'objets connectés seront utilisés en 2016. C'est une hausse de 30 pour cent par rapport à 2015], Gartner Report, novembre 2015, http://www.gartner.com/newsroom/id/3165317
11. « A huge security breach traced back to an unsecured IoT device will happen within the next two years, warn security experts » [Les experts en sécurité tirent la sonnette d'alarme : une violation importante de la sécurité causée par un appareil non sécurisé et connecté à l'Internet des objets se produira dans les deux années à venir], Danny Palmer, le 1er juillet 2016. ZD Net, http://www.zdnet.com/article/the-first-big-internet-of-things-security-breach-is-just-around-the-corner/
12. « Hacking into homes: 'Smart home' security flaws found in popular system » [Intrusion dans les maisons : des failles détectées dans la sécurité d'un système répandu destiné aux « maisons intelligentes »], Nicole Casal Moore, le 2 mai 2016. Michiga News, université du Michigan. http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system
13. « How much your passwords are worth to cybercriminals » [Que valent vos mots de passe pour les cybercriminels ?], Market Watch, le 31 décembre 2015 http://www.marketwatch.com/story/how-much-your-passwords-are-worth-to-cybercriminals-2015-12-11
14. « Kill the password: a string of characters won't protect you » [Tuez le mot de passe : ne comptez pas sur une chaîne de caractères pour vous protéger], Mat Honan, le 15 novembre 2012. Wired, https://www.wired.com/2012/11/ff-mat-honan-password-hacker/

sous-traitant en chauffage, ventilation et climatisation. Comme MacDonnell Ulsch l'a souligné dans TechTarget[15], les fournisseurs externes bénéficient souvent d'une confiance quasi identique à celle accordée aux membres de l'organisation. Ainsi, ils disposent de toute une série d'accès à l'instar des salariés ordinaires de l'entreprise, sans être soumis au même niveau de contrôle que ceux-ci.

Et monsieur Ulsch ajoute : « C'est la raison pour laquelle la gestion des tiers et les contrats de service sont essentiels pour gérer le risque. »

Bien entendu, bon nombre de fournisseurs tiers prennent ces risques au sérieux et tiennent compte en permanence des besoins de sécurité de leurs clients. S'ils sont professionnels, les fournisseurs externes ont tendance à se montrer ouverts et disposés à discuter des besoins de sécurité du client, ainsi qu'à veiller avec lui à la sécurité des réseaux et à répondre à toutes ses préoccupations.

TYPES D'ATTAQUES

Logiciel malveillant

« Logiciel malveillant » est le terme général qui désigne les cybermenaces les plus répandues et les plus connues telles que les virus, les chevaux de Troie, les vers informatiques et les logiciels de rançon ou ransomwares. Les logiciels malveillants sont souvent classés par familles en fonction du code utilisé. D'après la publication commerciale Help Net Security[16], plus de 1 500 familles de logiciels malveillants ont été répertoriées à l'automne 2015. Conficker, Sality et Cutwail comptent parmi les plus connues. Une fois dans le système, chaque souche du programme joue un rôle particulier. Certaines ciblent les états financiers ou d'autres types de données, d'autres sont conçues pour rendre votre système inopérant, et elles sont encore plus nombreuses à pouvoir transformer votre machine en robot et à envoyer des spams.

Personne n'est à l'abri des attaques de logiciels malveillants, et il se peut que les membres des conseils d'administration courent un risque encore plus grand, puisqu'il leur arrive de travailler dans plusieurs organisations. Les acteurs malveillants utilisent une large variété d'attaques pour infecter votre système par des logiciels malveillants. Ces attaques incluent :

- **Les attaques d'hameçonnage** imitent les communications légitimes afin de duper le destinataire du courriel et de l'amener à cliquer sur un mauvais lien ou à ouvrir une pièce jointe contenant un logiciel malveillant. Selon la société de sécurité Tripwire[17], elles se présentent sous différents formats. Le courriel d'hameçonnage est généralement envoyé de manière aléatoire, son expéditeur espérant que quelqu'un mordra à l'hameçon. Les attaques de spear phishing ou harponnage sont davantage ciblées directement sur des personnes particulières et proviennent souvent de sources fiables partageant des contenant un logiciel malveillant. Selon la société de sécurité Tripwire[17], elles se présentent sous différents formats. Le courriel d'hameçonnage est généralement envoyé de manière aléatoire, son expéditeur espérant que quelqu'un mordra à l'hameçon. Les attaques de spear phishing ou harponnage sont davantage ciblées directement sur des personnes particulières et proviennent souvent de sources fiables partageant des documents de travail légitimes. Le whaling est un harponnage de haut niveau, il cible des dirigeants et des personnes en vue telles que des célébrités ou des politiciens. Les courriels de whaling sont extrêmement personnalisés et difficiles à détecter.

- **Les attaques par déni de service distribué** font exactement ce que leur nom indique : elles visent à rendre le service indisponible pour le réseau. Ces attaques, comme les a définies le département de la Sécurité intérieure, constituent la méthode préférée des organisations de pirates activistes telles qu'Anonymous, qui ferment des sites Web en signe de protestation ou pour faire une déclaration politique.

- **Les menaces avancées persistantes (APT)** sont le pire cauchemar des entreprises. Selon un article publié dans le magazine Network Security[18], leur objectif est de voler le plus d'informations possible. Un pirate, qui fait généralement partie d'un cercle de cybercriminels, infiltre le réseau et s'y maintient durant de longues périodes sans être détecté. Ainsi, le pirate dispose d'un accès pratiquement illimité aux informations circulant dans l'infrastructure. Différents événements permettent de reconnaître la prise de contrôle par une APT : une activité de connexion inhabituelle ou des transferts non planifiés de gros volumes de données.

- **Les attaques immédiates de type « zero-day »** profitent des vulnérabilités d'un programme logiciel. Les pirates se pressent de s'engouffrer dans ces failles avant qu'elles soient découvertes et fassent l'objet d'un correctif. D'après la société Malwarebytes, les experts exhortent les utilisateurs à installer des correctifs logiciels dès qu'ils sont disponibles pour éviter une attaque de type « zero-day ».

- **Les attaques de l'homme du milieu (HDM)** sont une sorte d'espionnage des communications qui permet au pirate de s'immiscer dans les conversations en ligne afin d'obtenir des informations. Selon les experts de Veracode[19], une attaque HDM pourrait, par exemple, détourner la transaction financière entre un particulier et une banque. Son auteur aurait ainsi accès aux numéros de compte, aux noms et aux mots de passe.

- **Les publicités malveillantes et téléchargements à la dérobée** sont des types d'attaques différents, mais se caractérisent tous deux par le fait que l'acteur malveillant prend le contrôle du site Web d'une tierce personne. Le code malveillant est injecté sur le site, presque toujours sans que le propriétaire s'en aperçoive. Dans une attaque de publicité malveillante, le logiciel malveillant est téléchargé au moment où l'utilisateur clique sur une publicité infectée. Fox Business[20] précise que les téléchargements à la dérobée infectent un système au moment où un internaute visite le site.

Logiciels de rançon

Techniquement, le logiciel de rançon est malveillant, mais les attaques deviennent tellement sophistiquées qu'il doit être traité comme un vecteur d'attaque individuel. Le logiciel de rançon prend les données en otage en les chiffrant et force leur propriétaire à payer une rançon

15. « Third-party risk management: Horror stories? You are not alone » [Gestion des risques liés aux tiers : des scénarios d'horreur ? Vous n'êtes pas seul], MacDonnell Ulsch, Tech Target, http://searchsecurity.techtarget.com/feature/Third-party-risk-management-Horror-stories-You-are-not-alone
16. « Top malware families targeting business networks » [Les principales familles de maliciels responsables d'intrusions dans les réseaux d'entreprise], Help Net Security, le 30 novembre 2015 https://www.helpnetsecurity.com/2015/11/30/top-malware-families-targeting-business-networks/
17. « 6 Common Phishing Attacks and How to Protect Against Them » [6 attaques répandues d'hameçonnage et les moyens à mettre en œuvre pour s'en prémunir], David Bisson, le 5 juin 2016 http://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
18. « Advanced Persistent threats and how to monitor and deter them » [Menaces avancées persistantes, modes de surveillance et de prévention], Colin Tankard, août 2011. Elsevier, http://www.sciencedirect.com/science/article/pii/S1353485811700861
19. « Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks » [Tutoriel sur les attaques de l'homme du milieu : découvrez ce que sont ces attaques, les vulnérabilités et les modes de prévention de ce type d'intrusion], Veracode,
http://www.veracode.com/security/man-middle-attack
20. « What You Need to Know About 'Drive-By' Cyber Attacks » [Ce que vous devez savoir sur les cyberattaques de type « téléchargement à la dérobée »], Jason Glassberg, le 4 février 2015. Fox Business, http://www.foxbusiness.com/features/2015/02/04/what-need-to-know-about-drive-by-cyber-attacks.html

avant l'expiration d'un certain délai au terme duquel il lui remettra une clé de déchiffrement. Une étude menée par PhishMe[21] a révélé que durant le premier trimestre de 2016, 93 pour cent des e-mails sur une pièce jointe contenant un logiciel de rançon, la manœuvre pourrait infecter le réseau de l'organisation et coûter à celle-ci des centaines de milliers de dollars pour récupérer les données.

Bien que ce type d'attaque existe depuis longtemps, le logiciel de rançon reste populaire en raison de différents facteurs : les paiements sont effectués de façon anonyme, généralement par l'intermédiaire de Bitcoin ou d'autres devises en ligne ; les kits de programmation sont disponibles facilement et les pirates ne doivent pas développer en permanence de nouveaux logiciels malveillants pour être efficaces ; par ailleurs le système est rapidement lucratif une fois l'attaque perpétrée.

PRÉVENTION ET PROTECTION

Pour prévenir et protéger, il est essentiel de s'engager à appliquer de bonnes pratiques en matière de sécurité. Pensez, par exemple, à effectuer des tests de pénétration réguliers, à introduire des politiques sécuritaires, à mettre à jour et apporter rapidement des correctifs aux logiciels et à réglementer les appareils connectés au réseau. De plus, les experts en sécurité suggèrent les mesures suivantes :

Sensibilisation

Des formations de sécurité doivent obligatoirement être données à l'ensemble des employés. Il est essentiel que chaque personne qui accède au réseau comprenne les risques liés à la cybersécurité et les tactiques de prévention. Cette sensibilisation doit comprendre :

- Des communications fréquentes telles que des conseils de sécurité prodigués chaque semaine ou chaque mois concernant les dernières menaces, de même que des explications relatives aux attentes en matière de sécurité.
- Des formations pratiques régulières. Il existe des modules virtuels de cybersécurité destinés à des formations mensuelles ou trimestrielles sur la détection des arnaques d'hameçonnage et autres attaques potentielles.
- Les bonnes pratiques des réseaux sociaux qui indiquent ce qu'il ne faut pas partager dans les médias sociaux et comment reconnaître l'ingénierie sociale.
- La mise en place et l'application de politiques sécuritaires en matière de BYOD.
- Une ligne de communication ouverte. Chaque personne qui a accès au réseau doit pouvoir faire part de ses inquiétudes au service informatique ou aux responsables de la sécurité. Toute question et tout commentaire est à prendre au sérieux

Mettre l'accent cur les données ey non sur les réseaux

Davantage d'experts en sécurité recommandent aux organisations de restructurer leur approche de la protection des réseaux en protégeant les données. Comme il existe énormément de terminaux depuis lesquels il est possible d'accéder à des données sensibles et que bon nombre de ces informations sont stockées ailleurs que sur un serveur installé sur site, les méthodes traditionnelles de sécurisation du périmètre ne sont plus aussi efficaces. Ainsi, il est nécessaire de sélectionner soigneusement les sous-traitants externes, en particulier les fournisseurs de cloud, et de tenir compte du niveau de protection qu'ils accordent aux données. Les bonnes pratiques de cybersécurité incluent :

- le chiffrement des données stockées ;
- l'utilisation d'options de courriel sécurisées ;
- le recours à des outils de sécurité pour chaque terminal, y compris les smartphones et les tablettes.

Utiliser les avancées technologiques

La technologie peut aussi améliorer la sécurité. Dans un portail pour conseils d'administration, par exemple, les communications et les documents sont chiffrés, de sorte qu'ils sont plus difficiles à voler pour les potentiels pirates. Grâce à ces portails, les membres des conseils disposent par ailleurs d'un point d'entrée unique depuis pour accéder à l'information. Ainsi, ils ne doivent pas se préoccuper de savoir si les courriels ou documents sont stockés dans des systèmes non sécurisés ou obsolètes qui sont plus vulnérables et davantage exposés à un risque d'exploitation.

Mike Rogers, le directeur de la NSA, a indiqué au Wall Street Journal[22] que la question n'était pas de savoir si vos réseaux seront pénétrés, mais bien à quel moment ils le seront, et chaque organisation, quelle que soit sa taille, doit accorder plus d'importance à la cybersécurité.

21. « 93 % of phishing emails are now ransomware » [93 % des e-mails d'hameçonnage sont désormais des logiciels de rançon], Maria Korolov, 1er juin 2016. CSO, http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html
22. « NSA Chief Expects More Cyberattacks Like OPM Hack » [Le chef de la NSA s'attend à une hausse des cyberattaques comparables au piratage du Bureau américain de gestion du personnel], Robert Wall et Alexis Flynn, le 15 juillet 2015. The Wall Street Journal, http://www.wsj.com/articles/nsa-chief-expects-more-cyberattacks-like-opm-hack-1436985600

Dans un portail pour conseils d'administration, les communications et les documents sont plus difficiles à voler pour les pirates.

Courriel: info@diligent.com
Appelez le: +33 (0)1 56 60 58 58
Visitez: www.diligent.com