ESi TECHNOLOGIES

LES 10 PRINCIPALES ERREURS DE SÉCURITÉ COMMISES PAR LES ENTREPRISES

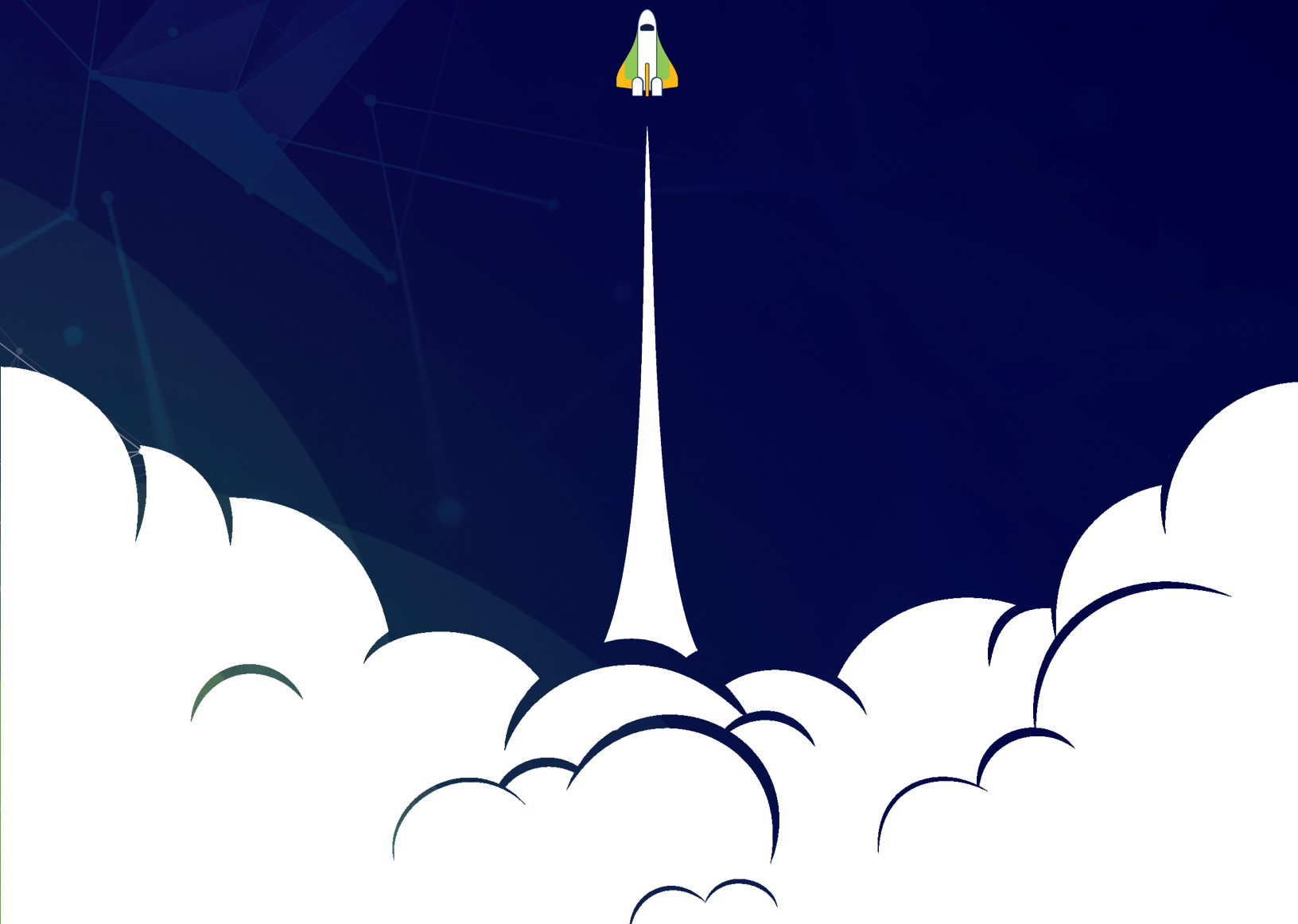


Table des matières

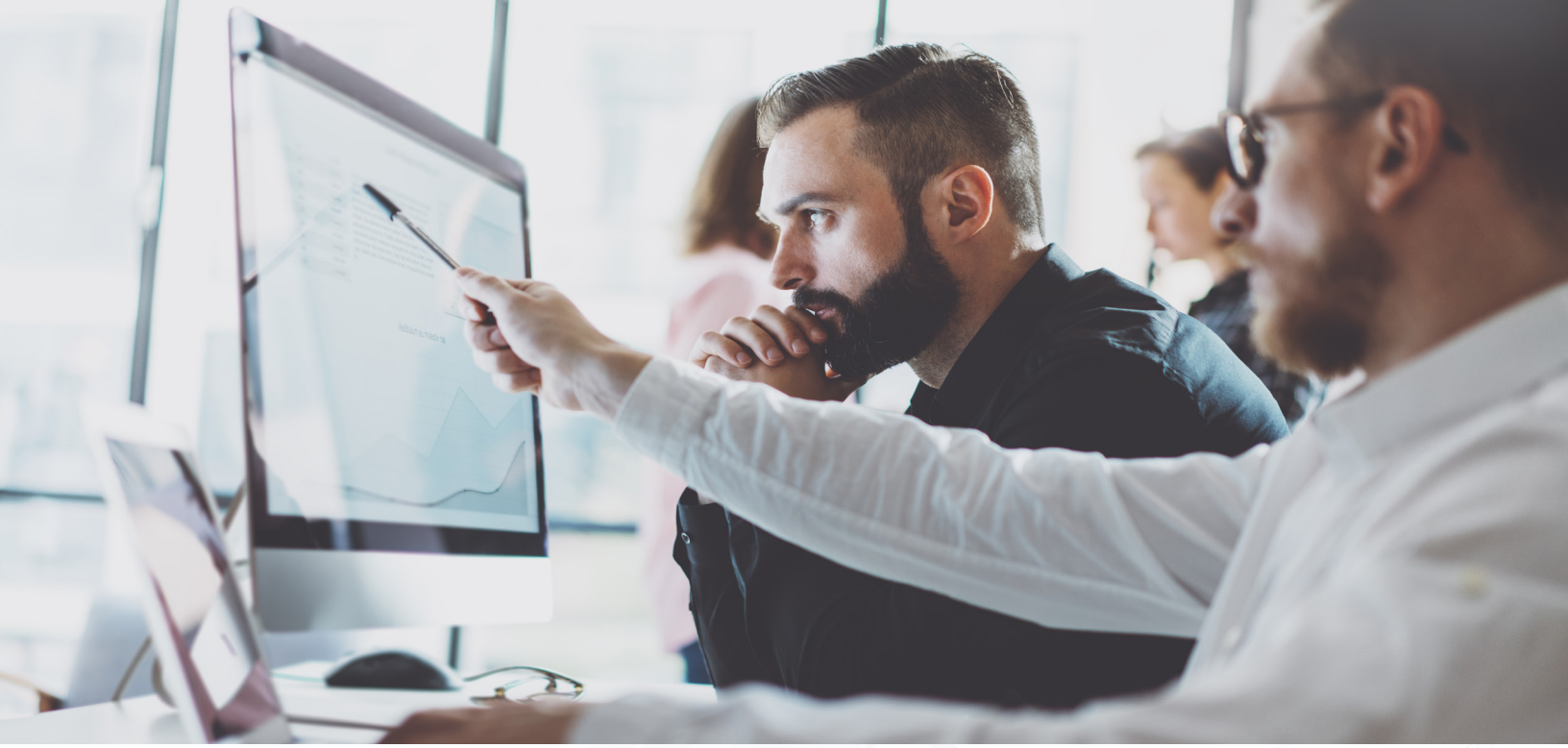
La cybersécurité, un enjeu majeur à ne pas négliger

La cybersécurité est souvent considérée comme un enjeu technologique qui nécessite des réponses technologiques. Des milliers de fournisseurs vendent des outils pour détecter, prévenir et se relever des cyberattaques. Les dépenses mondiales en cybersécurité devraient dépasser 167 milliards de dollars[1] cette année, indiquant que des sommes considérables sont investies dans la recherche de solutions.

Mais la réalité est que la grande majorité des problèmes de sécurité résultent d'erreurs humaines, du manque de connaissance et de mauvaises politiques. Plutôt que d'acquérir de nouvelles technologies, les entreprises doivent utiliser plus efficacement les outils dont elles disposent.

ESI a mis à profit les nombreuses années d'expérience de son équipe de sécurité pour développer cette liste des 10 failles de cybersécurité rencontrées le plus souvent par ses experts. Le cas échéant, nous avons suggéré des solutions technologiques, mais la plupart de ces lacunes peuvent être comblées par l'élaboration de politiques robustes, la formation des utilisateurs et le respect des meilleures pratiques.

Roger Courchesne
Directeur de pratique
d'interréseautage et de sécurité
ESI Technologies



ERREUR N° 1

Ne pas appliquer une politique de mots de passe forts

C'est l'erreur de cybersécurité numéro 1 et la plus facile à corriger. Malgré des années de mises en garde sur l'importance de choisir des mots de passe composés de chaines de caractères aléatoires, plusieurs personnes persistent à utiliser les noms des membres de leur famille, des dates de naissance, des chaines de numéros séquentiels ou d'autres codes faciles à deviner.

Pendant ce temps, les logiciels utilisés par les criminels pour déchiffrer les mots de passe ne cessent de s'améliorer.

Même les algorithmes de force brute, qui consistent à simplement combiner des caractères aléatoires jusqu'à ce qu'une correspondance soit trouvée, peuvent traiter jusqu'à 350 milliards de suppositions par seconde.

Les statistiques sur les défaillances de mot de passe sont alarmantes. Une analyse de 11 millions de mots de passe volés pour des services cloud réalisée par Skyhigh Networks[2] a révélé que 20 chaines de caractères seulement constituaient 10.3% de tous les mots de passe figurant sur la liste.

Une autre analyse[3] de 130 millions de mots de passe volés dans un piratage des systèmes Adobe en 2013 a révélé que 5 mots de passe composés de numéros séquentiels protégeaient 3.2 millions de comptes.

Une pratique tout aussi dangereuse consiste à utiliser le même mot de passe sur plusieurs comptes. Des milliards de mots de passe ont été volés dans des violations au cours des dernières années. Un attaquant pouvant compromettre un compte avec un mot de passe volé peut souvent accéder à de nombreux autres comptes détenus par le même utilisateur.

Les gens font ces erreurs pour de bonnes raisons. Mémoriser ou noter des mots de passe différents pour chaque compte est un exercice laborieux et une source d'erreurs. Les conserver dans fichier électronique n'offre qu'une protection minime, à moins que le document ne soit chiffré.

Une meilleure option consiste à utiliser l'un des nombreux gestionnaires de mots de passe numériques disponibles à un coût faible ou nul. Ces produits stockent des mots de passe dans des coffres chiffrés, remplissent automatiquement des formulaires et peuvent même conserver des informations de cartes de crédit et autres données personnelles sensibles. Ils peuvent également suggérer des mots de passe qui sont presque impossibles à déchiffrer. Les utilisateurs doivent se souvenir d'un seul mot de passe pour accéder à l'ensemble de leur coffre.

59% des utilisateurs admettent réutiliser le même mot de passe partout.

Security Boulevard, mai 2018[4]

Les bonnes pratiques à mettre en œuvre en entreprise

Les organisations peuvent aider à renforcer la sécurité des mots de passe avec quelques procédures de base.

1

Exiger que les mots de passe par défaut soient immédiatement modifiés chaque fois que de nouveaux périphériques sont installés. Le fait de laisser les valeurs par défaut sur un routeur, par exemple, peut permettre à un attaquant d'accéder facilement à l'ensemble du réseau d'une entreprise.

2

Définir les règles standard que les utilisateurs doivent respecter, telles que la modification des mots de passe des applications stratégiques tous les trois mois. La plupart des services d'annuaire et des applications infonuagiques permettent aux administrateurs d'imposer des modifications de mots de passe selon un calendrier prédéfini. L'utilisation d'un gestionnaire de mots de passe facilite le processus.

3

Fournir aux employés des conseils sur la sélection de bons mots de passe. En général, plus le mot de passe est long, mieux c'est. Les logiciels de piratage de mots de passe sont devenus tellement sophistiqués que les experts affirment désormais qu'une longueur minimum de 13 caractères est nécessaire. La sélection des caractères doit être vraiment aléatoire; substituer $ pour S et 1 pour I ne trompe pas le logiciel utilisé par les criminels. Une pratique de plus en plus répandue consiste à adopter de très longs mots de passe, tels que des citations mémorables ou des passages de livres.

4

Encourager les employés à utiliser une authentification à deux facteurs (2FA) chaque fois que c'est possible. Cette technique, qui complète le mot de passe avec une seconde forme de vérification, telle qu'un message texte au téléphone portable de l'utilisateur, est prise en charge par de plus en plus de fournisseurs de services cloud. Selon Symantec[5], l'utilisation de 2FA permettrait d'éviter 80% des violations.

Utiliser des logiciels obsolètes et non corrigés

Se tenir au courant des mises à jour et des correctifs logiciels constitue un défi de taille pour les entreprises informatiques les plus riches en ressources. Pour les petites entreprises disposant d'un budget limité, la tâche est presque impossible. Une vérification du National Vulnerability Database[6] du NIST illustre l'ampleur du problème. Des centaines de correctifs (qui ne sont pas tous critiques) sont publiés chaque mois et impossibles à maintenir à jour. Ceux qui doivent être appliqués doivent souvent être téléchargés, testés et déployés rigoureusement afin d'éviter de causer d'autres problèmes.

Les logiciels non corrigés sont un problème croissant qui a fait la une des dernières failles de sécurité. La violation dévastatrice subie par Equifax en 2017[7], qui a révélé les informations personnelles sur plus de 140 millions d'Américains, s'est produite lorsque des attaquants ont exploité une vulnérabilité dans une plateforme d'application Web open source qui avait été corrigée plusieurs mois auparavant. Le réputé Ponemon Institute[8] a estimé que 60% des organisations victimes d'une violation de données sur une période de deux ans l'ont été à cause d'un exploit d'une vulnérabilité connue mais non corrigée.

La prévalence d'anciens ordinateurs et systèmes d'exploitation est un problème important. Par exemple, au début de 2019, NetApplications Inc. estimait[9] que la base installée de Windows 7 dépassait toujours celle de Windows 10, alors que Windows 7 n'est plus pris en charge depuis 2015. En fait, plus de 4% des ordinateurs utilisent encore Windows XP, introduit en 2001 et qui n'a pas été mis à jour depuis près de cinq ans.

L'enjeu des appareils mobiles

Une complication additionnelle est le nombre croissant d'appareils mobiles que les entreprises doivent prendre en charge. Les ordinateurs portables, les téléphones intelligents et les tablettes sont difficiles à rassembler et les utilisateurs en déplacement sont plus susceptibles aux virus introduits par le biais de canaux tels que les réseaux sans fil ouverts et les clés USB.

Pour suivre le déluge de correctifs, il faut automatiser et définir des priorités. Les administrateurs de serveurs doivent souscrire à toutes les alertes pertinentes de leurs fournisseurs de logiciels stratégiques et accorder la priorité aux correctifs jugés les plus critiques. Une bonne stratégie de test consiste à utiliser un deuxième serveur dans une partition virtuelle qui reflète l'environnement de production.

La protection des terminaux client

La sécurité des terminaux est un problème plus difficile. L'organisation doit auditer tous les points d'entrée potentiels du réseau sur une base régulière, idéalement une fois par trimestre. Cela inclut les ordinateurs de bureau, les ordinateurs portables, et les équipements réseau connectés à Internet. Tous les systèmes exécutant des systèmes d'exploitation non pris en charge tels que Windows XP ou Windows 98 doivent être immédiatement supprimés et remplacés. Les ordinateurs fonctionnant sous Windows 7 doivent être mis à jour vers Windows 10 avec les correctifs automatiques activés.

Solution technologique

Heureusement, il existe des solutions qui protègent même contre les exploits « zero-day ». Un exemple est la solution Advanced Malware Protection for Endpoints[10] (AMP) de Cisco qui utilise une combinaison de détection de modèle et une base de données de vulnérabilités globale pour détecter et traiter rapidement les infections par des logiciels malveillants. La solution va au-delà de l'application de correctifs pour inspecter en permanence l'activité sur les périphériques terminaux afin de détecter tout signe de comportement anormal. Lorsqu'il est détecté, AMP fournit un « bac à sable » qui isole les fichiers suspects pour les analyser sans les exposer à d'autres logiciels en cours d'exécution. Si un fichier qui semble propre lors d'une inspection initiale s'avère malicieux, AMP peut fournir un historique complet du comportement de la menace afin d'obtenir de l'aide pour le confinement et la correction.

Même avec ces protections en place, l'immunité n'est pas garantie. Par exemple, les exploits « zero-day » sont un type d'attaque qui frappe en même temps que de nouvelles vulnérabilités sont découvertes. En raison du temps insuffisant écoulé pour la diffusion d'un correctif, les organisations ne parviennent pas à les appliquer à temps.

Utiliser des périphériques vulnérables

De nombreuses organisations offrent un service sans fil gratuit par courtoisie aux clients, mais le fait de ne pas respecter quelques protections de base peut transformer ce service en un cauchemar de sécurité.

Les risques des services sans fil

Les points d'accès sans fil publics ne doivent jamais être connectés au réseau de l'entreprise. Les organisations peuvent négliger ce blocage de base et ce suivi pour des raisons de coût ou de commodité, mais elles le font à leurs risques et périls. Ajouter la sécurité par mot de passe aux points d'accès publics est une protection faible pour toutes les raisons mentionnées au point 1. La meilleure approche consiste à faire appel à un fournisseur de services Internet commercial dont le réseau est indépendant du vôtre.

La plupart des points d'accès sans fil publics ne sont pas chiffrés, ce qui signifie que les données qui y sont transmises restent au format texte. Les cybercriminels peuvent facilement « renifler » ce trafic pour capturer tous les paquets traversant le réseau. Pour cette raison, les employés, les sous-traitants et même les clients doivent être mis en garde contre l'utilisation de points d'accès publics pour les entreprises.

Face à leur prolifération, les entreprises ont du mal à conserver un inventaire de tous leurs points d'accès potentiellement vulnérables.

Un facteur qui contribue à cette ignorance est la facilité avec laquelle des périphériques individuels peuvent désormais créer des vulnérabilités à l'insu du service informatique. Par exemple, de nombreux ordinateurs et téléphones intelligents sont livrés avec une option par défaut pour les configurer en tant que point d'accès sans fil ouverts. Les employés peuvent utiliser cette fonctionnalité pratique pour configurer des groupes de travail au besoin ou économiser sur les coûts de données sans fil, mais oublient ensuite de la désactiver. Lors de la connexion au travail, ils créent essentiellement une rampe d'accès ouverte au réseau de l'entreprise.

La moitié des professionnels de la sécurité croient qu'ils ne sont pas conscients de tous les périphériques connectés accédant à leurs réseaux et 60% ne savent pas quand de nouveaux appareils connectés viennent dans le bureau.

Pwnie Express
Internet of Evil Things Report[11]

Les sites Web à usage spécifique

Un autre sujet de préoccupation concerne les sites Web temporaires ou à usage spécifique qui se connectent au réseau de l'entreprise sans bénéficier d'un ensemble complet de protections. C'était un problème dans l'attaque massive de JP Morgan Chase[12] en 2014, qui avait compromis l'information sur 76 millions de ménages et 7 millions de petites entreprises. La société avait mis en place un serveur Web public pour organiser une course et avait permis aux employés de se connecter avec leurs informations d'identification professionnelles sans chiffrer ni protéger les informations. Les attaquants ont pu utiliser un certificat de sécurité volé à un sous-traitant pour intercepter le trafic sur le service, y compris les identifiants de connexion.

Les informations de connexion compromises par un sous-traitant ont également joué un rôle dans la violation des magasins Target[13] plus tôt dans la même année.

Le sous-traitant avait obtenu un niveau de privilège que les attaquants ont pu utiliser pour installer un logiciel sur les systèmes de points de vente de la société qui a capturé les numéros de carte de crédit et d'autres informations sensibles.

Solution technologique

Le pare-feu de nouvelle génération (NGFW)[14] de Cisco est une excellente source de protection de la périphérie du réseau. Il associe un moteur de détection et de prévention des intrusions à une sécurité basée sur l'identité et sur le périphérique qui fonctionne au niveau 7 pour identifier le contenu et les applications des utilisateurs sur le réseau. Les administrateurs peuvent non seulement appliquer des stratégies de sécurité sur chaque périphérique, mais ils peuvent également bloquer le trafic provenant de certaines destinations et hiérarchiser le trafic plus exigeant, tel que la vidéoconférence.

Les dangers de l'Internet des objets

Malheureusement, l'IoT ne fera qu'aggraver la situation. Les entreprises installent de plus en plus de dispositifs, tels que des thermostats programmables, des caméras et des systèmes d'éclairage intelligents, et les connectent à leur réseau. Ces dispositifs peuvent être peu ou pas sécurisés, ce qui en fait des proies faciles pour les criminels. En tant que protection de base, modifiez les mots de passe par défaut sur tous les périphériques ajoutés à votre réseau et utilisez la segmentation du réseau pour limiter l'accès à l'infrastructure et aux informations critiques.

ERREUR N° 4

Ne pas surveiller et protéger adéquatement les services de messagerie

Malgré les efforts des administrateurs de la sécurité pour appliquer les bonnes pratiques en matière de mots de passe et pour colmater les failles des réseaux, ils ne peuvent rien faire pour protéger les utilisateurs contre leurs propres erreurs. La boite de réception reste une menace persistante pour la sécurité.

Les statistiques parlent d'elles-mêmes. FireEye estime[15] que 91% de la cybercriminalité commence par la messagerie électronique. Selon le rapport de 2018 de Verizon[16] sur la violation des données, 92% des logiciels malveillants étaient diffusés par ce canal.

Les rançongiciels, qui était la catégorie de logiciels malveillants à la croissance la plus rapide en 2017, commencent généralement leur parcours dans une boite de réception.

Des attaques de plus en plus raffinées

Les attaques par courrier électronique ont évolué au cours des dernières années, car les criminels ont affiné leur capacité à cibler les messages. Les filtres antipourriels sont maintenant tellement efficaces que peu d'utilisateurs voient même les pourriels, mais grâce à la technique du harponnage, les criminels peuvent contourner même les meilleurs contrôles.

Un sondage réalisé auprès de 1 300 professionnels de la sécurité indique que 56% d'entre eux ont déclaré que les attaques ciblées par hameçonnage constituaient leur principale menace pour la sécurité.

CyberArk
Global Advanced Threat Landscape Report 2018[17]

L'origine du problème est la confiance. Le courrier électronique est un outil tellement essentiel pour les professionnels qu'il est facile pour les gens de tomber dans le piège consistant à croire que chaque message est authentique.

Le harponnage profite de cette complaisance. Les criminels extraient des informations personnelles issues de profils de réseaux sociaux et les font correspondre à des adresses électroniques. Ils peuvent également analyser l'activité récente d'une personne pour rechercher des éléments qui établissent une relation de confiance, tels que l'appartenance à une organisation ou des achats récents. Et ils consultent les réseaux d'amis pour trouver le nom des personnes que leurs cibles connaissent déjà.

Munis de ces informations, les attaquants peuvent facilement usurper l'identité d'un expéditeur d'un message électronique pour qu'il semble provenir d'un ami. Le fait d'inclure une information personnelle glanée sur un réseau social rassure le destinataire.

Le message inclut un lien vers un site Web malveillant qui installe un logiciel ou demande des informations de connexion. Les habitués de l'hameçonnage sont si compétents aujourd'hui que même les professionnels de la cybersécurité ont avoué en être la proie.

Les attaques par courrier électronique sont extrêmement difficiles à défendre, car elles sont spécifiques à chaque utilisateur du réseau. Un simple clic sur une pièce jointe ou un lien malveillant peut déclencher une multitude de logiciels malveillants qui se propagent rapidement dans toute l'organisation.

Le rançongiciel est un nouveau facteur particulièrement nocif. Il chiffre instantanément le disque dur de l'utilisateur et exige un paiement par rançon en cryptomonnaie en échange de la clé de déchiffrement. Certaines formes de ransomware se copient également sur d'autres ordinateurs du réseau et les chiffrent également.

Solutions technologiques

La technologie rendue possible par l'apprentissage machine entre également en jeu. La suite Cisco Email Security[18] offre une protection supplémentaire grâce à une approche par couches qui surveille les communications entrantes et sortantes. Le logiciel utilise l'apprentissage machine pour identifier rapidement les expéditeurs frauduleux, y compris ceux qui risquent d'échapper même aux utilisateurs les plus prudents. La validité des URL incorporées dans les messages peut être vérifiée, de même que la réputation des domaines de l'expéditeur par rapport aux listes noires et aux enregistrements publics.

Cisco offre également une protection contre le détournement de domaine, une tactique courante des pirates informatiques. Les utilisateurs sont immédiatement notifiés si un domaine a été compromis.

Une autre technologie utile est le filtrage d'URL[19] qui limite les destinations que les utilisateurs peuvent visiter. Le filtrage permet aux administrateurs de contrôler l'accès aux sites Web en fonction des informations contenues dans une liste d'URL. Les entreprises peuvent gérer une liste d'URL locale ou des services de flux d'URL basés sur le cloud comme Cisco Umbrella[20] qui surveille le contenu du site Web également au niveau de la couche DNS. Bien que le filtrage n'empêche pas les utilisateurs de cliquer sur des liens malveillants, il peut limiter considérablement les dommages.

Les moyens d'améliorer la protection

Heureusement, la défense contre les attaques par courrier électronique est assez simple. Elle consiste à éduquer les gens sur quelques pratiques de base.

1

Ne **cliquez jamais sur des liens ou des pièces jointes** dans les messages, sauf si vous êtes absolument certain de l'identité de l'expéditeur. Cette information peut être facilement vérifiée en consultant l'en-tête du message, qui est différent du champ « de ».

2

N'envoyez jamais d'informations personnelles telles que des numéros de compte bancaire des mots de passe par courrier électronique. Aucune organisation réputée ne vous demandera jamais de le faire.

3

Si vous êtes dirigé vers une page de connexion à partir d'un courrier électronique, **vérifiez que l'adresse Web correspond à celle attendue**. Les pirates peuvent créer de fausses pages Web très semblables aux sites légaux des banques, commerces en ligne et réseaux sociaux.

4

Choisissez judicieusement les informations que vous partagez publiquement sur les réseaux sociaux.

ERREUR N° 5

Avoir une mauvaise visibilité du réseau

Il a fallu 191 jours en moyenne, soit plus de 6 mois, aux entreprises pour détecter une faille en 2017. C'est inacceptable compte tenu du fait qu'une équipe d'intrusion peut généralement accéder aux informations d'identité d'administrateur de domaine en 3 jours environ.

2017 Cost of Data Breach Study

Ponemon Research[21]

Vous ne pouvez pas empêcher les attaques d'appareils que vous ne voyez pas. Malheureusement, plusieurs organisations n'ont pas une visibilité complète de leurs réseaux. Elles voient peut-être les adresses IP, mais elles ont peu d'informations sur ce que sont ces périphériques.

Une mauvaise visibilité augmente le risque que les attaquants pénètrent dans un réseau et restent inconnus pendant des semaines ou des mois, ce qu'on appelle un « temps d'arrêt ». Pendant cette période, les intrus peuvent siphonner de grandes quantités d'informations graduellement afin d'échapper à la détection.

Partage d'informations

Le problème est aggravé par la nature ouverte des réseaux IP. Le protocole Internet a été conçu pour que les informations puissent être découvertes librement, ce qui signifie que les périphériques partagent volontiers des informations sur les autres périphériques du même sous-réseau, notamment les versions de système d'exploitation et les applications en cours d'exécution. Un pirate peut exploiter ces informations pour trouver un logiciel vulnérable qui pourrait être exploité pour prendre le contrôle d'autres machines.

Défaillances dans la segmentation du réseau

Les mauvaises pratiques de segmentation du réseau amplifient le problème. La segmentation est un moyen utile pour les administrateurs de limiter l'accès à certains types d'informations en regroupant des périphériques dans des sous-réseaux dotés de niveaux d'autorisation différents. Cependant, de nombreuses entreprises ne prennent pas la peine de créer des sous-réseaux, exposant ainsi l'ensemble de leur réseau à toute personne pouvant franchir un pare-feu. À l'inverse, la sursegmentation crée une complexité qui peut également révéler des vulnérabilités. Par exemple, 30 sous-réseaux avec 25 stratégies de permission créent chacun 750 règles à administrer. Les erreurs et les oublis sont facilement omis dans un environnement aussi complexe.

Solution technologique

Une solution de visibilité réseau telle que Cisco Stealthwatch[22] offre non seulement aux administrateurs réseau et de sécurité une vue complète des périphériques de leur réseau, mais elle surveille également le trafic pour détecter les logiciels malveillants même dans des flux de données chiffrés. Stealthwatch peut également recommander des stratégies de segmentation optimales et prendre en charge des stratégies de sécurité pour chaque sous-réseau.

ERREUR Nº 6

Mal gérer les appareils mobiles

Presque tout le monde possède désormais un téléphone intelligent, mais plusieurs entreprises ont du mal à les traiter comme faisant partie de leur infrastructure informatique. Les règles de type BYOD qui ont dominé les premières années de la révolution du téléphone intelligent, sont dangereusement inadéquates pour régir l'utilisation des puissants appareils actuels.

Que les utilisateurs se servent de leurs propres téléphones ou que l'entreprise les leur fournisse, les appareils mobiles exigent les mêmes considérations de sécurité que les ordinateurs de bureau et portables. En fait, ils exigent une attention supplémentaire en raison de la facilité avec laquelle ils sont perdus ou volés, à raison de quelque 70 millions[23] chaque année.

Les appareils mobiles présentent de nouvelles menaces uniques pour la sécurité. En raison de leurs caméras et de leurs enregistreurs audio intégrés, les téléphones compromis peuvent devenir des dispositifs d'écoute et d'enregistrement vidéo à l'insu de l'utilisateur. Leur GPS intégré les rend également vulnérables à la localisation, une fonctionnalité particulièrement utile aux criminels se livrant à l'espionnage d'entreprise.

La sécurité des téléphones mobiles s'améliore, mais les organisations informatiques ne doivent pas compter uniquement sur les fonctionnalités intégrées pour la protection. Des chercheurs ont montré que les codes NIP et les motifs de balayage peuvent être détectés à une distance maximale de 4.5 mètres et qu'aucune protection biométrique n'est à toute épreuve. Une meilleure pratique consiste à utiliser deux formes d'authentification.

Mais les criminels n'ont pas à accéder physiquement à un appareil mobile pour faire des dégâts. Les logiciels malveillants mobiles constituent désormais une catégorie bien établie, avec plus de 4 000 familles de menaces et variantes répertoriées au début de 2018.

McAfee Mobile Threat Report Q1, 2018 [24]

Tandis que certains de ces programmes malveillants se frayent un chemin vers des magasins légitimes d'applications, beaucoup se propagent par le biais de programmes d'hameçonnage qui envoient des messages texte à des utilisateurs involontaires, les dirigeant vers des sites Web qui installent des programmes malveillant sur leurs appareils.

Une sécurité mobile efficace commence par des règles bien définies et bien communiquées. Les étapes de base incluent la mise à jour des périphériques avec les dernières versions du système d'exploitation et des correctifs de sécurité, la sauvegarde régulière des données et l'utilisation du chiffrement pour les données à la fois sur le périphérique et en transit.

Les utilisateurs doivent éviter les points d'accès sans fil publics et ne jamais cliquer sur des liens inconnus dans les messages texte ou le courrier électronique.

Solution technologique

Les entreprises peuvent utiliser des outils de gestion des périphériques mobiles tels que le gestionnaire de systèmes Meraki EMM/MDM[25] de Cisco pour obtenir des niveaux de protection supplémentaires.

Par exemple, les administrateurs MDM peuvent surveiller et diagnostiquer tous les appareils mobiles de leur réseau et obtenir un inventaire des logiciels installés. Les stratégies de sécurité peuvent être administrées à distance, y compris la désactivation des caméras, l'interdiction des captures d'écran et la désactivation de la synchronisation automatique.

Les appareils peuvent également être verrouillés à distance ou effacés en cas de vol. Enfin, MDM offre une visibilité réseau améliorée en offrant aux organisations un inventaire complet de tous leurs appareils mobiles, de leur statut et de leur emplacement.

Négliger les politiques de privilèges d'accès

Au milieu de la pression des affaires quotidiennes, les détails sont facilement oubliés, ou laissés sans solution. Lorsque ces détails concernent les privilèges d'accès, c'est un problème.

De nombreux utilisateurs finaux ne comprennent pas le fonctionnement des privilèges d'accès ou ne prêtent pas attention aux conseils fournis par les service TI. Résultat: des informations confidentielles peuvent facilement être laissées à la vue de tous.

Un récent rapport de Varonis[26] basé sur une analyse de 6.2 milliards de fichiers de 130 entreprises est éloquent à cet égard. Parmi les découvertes :

- 21% de tous les fichiers étaient accessibles à chaque employé;
- 58% des entreprises avaient plus de 100 000 dossiers ouverts; et
- 41% des entreprises n'avaient aucune restriction d'autorisation sur plus de 1 000 fichiers sensibles.

Ces omissions sont significatives étant donné qu'environ les deux tiers des incidents de sécurité sont causés par la négligence d'un employé ou d'un sous-traitant, contre 22% à peine par des personnes malveillantes, selon une étude de l'Institut Ponemon[27].

Le manque de connaissances est le plus grand coupable. Les employés peuvent ignorer les procédures d'attribution de privilèges ou déposer des fichiers dans des dossiers non sécurisés en pensant qu'ils sont protégés. Les dossiers situés au cœur d'un système de fichiers peuvent contenir des autorisations qui ne sont pas visibles au niveau supérieur, ce qui induit les administrateurs en erreur.

La sensibilisation et la formation sont les meilleurs remèdes. L'équipe TI doit expliquer comment attribuer des autorisations de fichiers et de dossiers et transmettre les meilleures pratiques, telles que l'attribution d'accès au niveau du groupe et jamais à des utilisateurs individuels. Une approche encore plus sécurisée consiste à limiter la création de nouveaux dossiers aux administrateurs informatiques, même si cela n'est pas pratique dans tous les cas.

Des solutions techniques sont disponibles sous la forme de systèmes de gestion de contenu d'entreprise, qui régulent l'accès au contenu et sa distribution dans l'ensemble de l'organisation. Ces systèmes incluent souvent également des fonctionnalités sophistiquées de gestion du flux de travail qui pevent rationaliser les processus et améliorer l'efficacité.

Les comptes actifs mais non utilisés sont la cible privilégiée des cyberattaquants, car ils offrent une apparence de légitimité. Une fois à l'intérieur du réseau, les intrus bénéficient de tous les privilèges attribuées au compte, ainsi que d'un risque de détection moindre, car ils sont effectivement entrés par la porte principale.

ERREUR Nº 8

Mal gérer les répertoires

Lorsqu'un employé quitte l'entreprise, les gestionnaires sont naturellement plus soucieux du travail à faire et de pourvoir le poste vacant que de désactiver les privilèges d'accès. Malheureusement, avec le temps, cela peut créer une grande brèche dans les défenses de l'organisation.

Les personnes qui affichent aujourd'hui l'ensemble de leurs antécédents professionnels sur des réseaux sociaux comme LinkedIn, permettent aux pirates d'identifier facilement des candidats en recherchant des personnes qui ont récemment changé d'emploi et dont les informations d'identité sont peut-être encore valables. Ils peuvent mettre en corrélation croisée ces informations avec les milliards de noms d'utilisateur et de mots de passe volés disponibles sur le dark Web afin de réduire leur liste de candidats.

Le taux de roulement n'est pas la seule vulnérabilité. Les comptes sont souvent configurés pour les sous-traitants et les travailleurs temporaires sans accorder une attention particulière aux autorisations d'accès. Les administrateurs oublient alors de les fermer à la fin d'un contrat, ou les laissent ouverts en cas de retour du travailleur temporaire.

Le rapport Varonis cité précédemment fait référence à ces entrées de répertoire sous le nom de « comptes fantômes ». Son enquête a révélé que le tiers des comptes sont activés mais non inutilisés et que 65% des entreprises ont plus de 1 000 comptes fantômes.

Parmi les autres problèmes fréquents liés aux répertoires, citons l'attribution trop généreuse des privilèges et l'affectation de membres à des groupes sans vérification préalable des exigences en matière d'accès.

Pour traiter le problème des comptes fantômes, les entreprises doivent désigner une personne au sein du service des ressources humaines pour veiller à ce que les privilèges d'accès soient révoqués pour les employés qui quittent. C'est aussi une bonne idée de vérifier annuellement la liste des comptes et de supprimer ceux qui sont inutilisés. L'administration des répertoires doit être limitée à quelques personnes formées aux meilleures pratiques pour le service de répertoire choisi.

ERREUR Nº 9

Mal protéger les services infonuagiques

Le chiffrement des données

La plupart des fournisseurs infonuagiques de logiciels (SaaS) et d'infrastructures (IaaS) offrent une excellente sécurité, mais cela ne signifie pas que les clients doivent supposer qu'ils n'ont plus à s'en préoccuper.

Par exemple, les fournisseurs IaaS peuvent prendre en charge le cryptage des données mais laisser la responsabilité du cryptage et de la gestion des clés de décryptage entre les mains de leurs clients. Ils peuvent également fournir des contrôles pour empêcher le téléchargement d'informations mais laisser cette option désactivée par défaut. Chaque fournisseur a ses propres politiques et il appartient aux clients de faire leurs devoirs.

La prévention des fuites de données

Les erreurs utilisateur sont la cause la plus fréquente de problèmes de sécurité dans le cloud.

Les hypothèses selon lesquelles les données sont sécurisées ont conduit à de nombreux incidents embarrassants, tels que la fuite dont a été victime FedEx en 2018[28] de plus de 119 000 documents contenant des informations personnelles laissées au format texte sur un serveur infonuagique non sécurisé.

Les entreprises doivent limiter le nombre de fournisseurs de stockage cloud qu'elles utilisent et appliquer des contrôles administratifs pour limiter ce que les utilisateurs peuvent partager et télécharger.

Il est généralement dangereux de supposer, en particulier en ce qui concerne les services infonuagiques. Les employés peuvent se déplacer pour poser des questions relatives à la sécurité à leurs administrateurs TI, mais la plupart de gens ne parlent même jamais aux entreprises qui fournissent des services cloud. Cela peut conduire à des hypothèses risquées sur qui est responsable de quoi.

La sélection des mots de passe

Une mauvaise sélection de mot de passe peut laisser des applications et des données critiques exposées à tous sur Internet. Le recours à une authentification à deux facteurs peut réduire ce risque.

Les utilisateurs doivent également être informés des meilleures pratiques en matière de partage de données infonuagiques. Par exemple, les données sensibles ne doivent être partagées qu'avec des personnes nommées, et non par une URL globale permettant l'accès en édition.

Solution technologique

Le portefeuille de solutions de sécurité Cisco Cloud[29] peut automatiser une grande partie de ce processus en offrant une visibilité sur l'activité Internet, en détectant les menaces et en y réagissant, et en étendant les contrôles sur site aux applications fonctionnant sur une infrastructure de cloud public.

Cisco Cloudlock[30] fournit un courtier en sécurité d'accès qui se situe entre les applications logicielles et les utilisateurs pour surveiller l'activité et appliquer les politiques de sécurité.

Utiliser de mauvaises pratiques de destruction des données

L'équipement qui a atteint la fin de sa vie utile peut constituer un risque important pour la sécurité si des pratiques d'élimination appropriées ne sont pas appliquées. De nombreuses personnes pensent que le simple fait de supprimer toutes les données d'un disque ou de formater le support constitue une protection suffisante, mais aucune de ces mesures ne supprime beaucoup de données.

Au lieu de cela, ils suppriment les pointeurs des répertoires, mais laissent jusqu'à 90% des données intactes et facilement récupérables à l'aide d'un logiciel spécial. Même plusieurs séances de formatage peuvent encore laisser des quantités importantes de données en place.

L'élimination des actifs TI (ITAD pour « IT Asset Disposal ») est une discipline spécialisée dans la destruction de données. Les fournisseurs ITAD utilisent des techniques allant de l'effacement avec des aimants puissants à la destruction physique de supports utilisant des machines qui réduisent les disques en poudre.

Les services professionnels fournissent également un certificat de destruction qui répond à la plupart des demandes de renseignements réglementaires.

Certains peuvent également remettre en état des équipements et récupérer une certaine valeur en les vendant sur des marchés secondaires.

Les services ITAD peuvent être coûteux et ne sont pas nécessaires dans tous les cas. Les organisations doivent disposer d'un processus d'évaluation des équipements en fin de vie et d'identification de ceux qui méritent une manutention spécialisée.

Ce processus doit s'appliquer à tout équipement contenant des données, notamment des serveurs, des ordinateurs personnels, des téléphones intelligents et des clés USB.

La sécurité du bon sens

Les propriétaires de petites entreprises peuvent penser être protégés des cyberattaques, car leur taille en fait une cible peu attrayante, mais 58% des victimes d'attaques de logiciels malveillants en 2017 étaient de petites entreprises, selon Verizon[31].

Les criminels supposent que les petites entreprises ont des ressources limitées et ne disposent pas des technologies sophistiquées de détection et de prévention des grandes entreprises. Alors que les grandes entreprises sont bien équipées pour résister aux violations de données les plus importantes, l'impact peut être dévastateur pour les entreprises opérant sur des marges plus réduites. Les cyberattaques coûtent en moyenne 2,2 millions de dollars aux petites et moyennes entreprises en 2017, selon Ponemon[32].

Heureusement, prêter attention aux 10 problèmes énumérés ici peut déjouer la grande majorité des cyberattaquants.

Pour explorer davantage la question, communiquez avec nous pour une présentation.

expertise@sitechnologies.com

ESI Technologies
www.esitechnologies.com
1-800-260-3311

MONTRÉAL
TORONTO
QUÉBEC

1550 rue Metcalfe, bureau 1100
Montréal, QC H3A 1X6
514 745-2524 1-800-260-3311

Ressources

[1] https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

[2] https://www.skyhighnetworks.com/cloud-security-blog/you-wont-believe-the-20-most-popular-cloud-service-passwords/

[3] https://www.zdnet.com/article/just-how-bad-are-the-top-100-passwords-from-the-adobe-hack-hint-think-really-really-bad/

[4] https://securityboulevard.com/2018/05/59-of-people-use-the-same-password-everywhere-poll-finds/

[5] https://www.slideshare.net/cheapsslsecurity/vip-strong-authentication-no-passwords-infographic-by-symantec

[6] https://nvd.nist.gov/vuln/full-listing

[7] https://www.wired.com/story/equifax-breach-no-excuse/

[8] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf

[9] https://netmarketshare.com/operating-system-market-share

[10] https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731874.pdf

[11] https://www.pwnieexpress.com/2018-internet-of-evil-things-report

[12] https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

[13] https://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

[14] https://www.cisco.com/c/en/us/products/security/firewalls/index.html

[15] https://www.fireeye.com/offers/rpt-email-threat-report.html

[16] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

[17] https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018/

[18] https://www.cisco.com/c/en/us/products/security/email-security/index.html

[19] https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html

[20] https://umbrella.cisco.com/

[21] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

[22] https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

[23] https://www.awingu.com/what-is-the-true-cost-of-a-lost-mobile-device/

[24] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

[25] https://meraki.cisco.com/solutions/emm

[26] https://www.varonis.com/2018-data-risk-report/

[27] https://securityintelligence.com/media/2016-cost-data-breach-study/

[28] https://www.zdnet.com/article/unsecured-server-exposes-fedex-customer-records/

[29] https://www.cisco.com/c/en/us/products/security/cloud-security/index.html

[30] https://www.cisco.com/c/en/us/products/security/cloudlock/index.html

[31] https://enterprise.verizon.com/resources/reports/dbir/

[32] https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html