Dr.WEB®
depuis 1992

La sécurité numérique des TPE et PME

Evaluer et comprendre les risques
S'adapter aux nouveaux modes de travail
Construire une politique de sécurité efficace

Doctor Web, Ltd. est éditeur des solutions Dr.Web depuis 1992.

Le développement de l'antivirus Dr.Web a toujours suivi la ligne directrice de son créateur : la sécurité sans compromis. Dans cette perspective, Doctor Web investit majoritairement en R&D, afin de proposer des produits de protection de haut niveau technique luttant contre les menaces actuelles et celles à venir.

La R&D et le service de veille antivirale de Doctor Web analysent 24h/24 et 7jours/7 des millions de virus, trojans et autres codes malicieux. Doctor Web est l'un des rares éditeurs antivirus propriétaire de sa technologie de détection et de désinfection des malwares.

La force de Doctor Web réside dans la pérennité de ses équipes et de ses dirigeants.

SOMMAIRE

Introduction
Pourquoi la sécurité ?

Typologie des attaques
Phishing
Déni de service
Ransomwares
Focus Vulnérabilités logicielles
Le spam, la pollution du numérique, vecteur de nombreuses fraudes et attaques

Nouveaux modes de travail, la sécurité en jeu
Nouveaux modes d'organisation et travail à la maison versus sécurité des données
Les mobiles, cibles privilégiées, une réalité négligée ?

Anticiper et réagir, comment penser la sécurité ?
Mettre en place une politique de sécurité
Répondre à une attaque
L'externalisation, un modèle pertinent

Introduction

Pourquoi la sécurité ?

Chaque année ou presque, le même constat est établi, les TPE et PME ne sont pas suffisamment sécurisées. Manque de temps, de ressources, d'intérêt, de conscience, les raisons peuvent être multiples mais quelles qu'elles soient, cet état des choses profite au cybercrime.

Rançongiciels, sites web infectés, Trojans, adwares, e-mails frauduleux, spam, la liste des menaces informatiques qui sont susceptibles de toucher le réseau de l'entreprise est longue. Certaines ne sont pas dangereuses à proprement parler, mais polluent le travail quotidien, d'autres peuvent entraîner une perte significative de chiffre d'affaires et de données.

C'est un fait clairement établi, au fil du temps, les techniques de piratage sont de plus en plus sophistiquées et les cybercriminels multiplient les types d'attaques, les méthodes, les cibles, pour être là où on ne les attend pas.

Rappelons quelques chiffres.

D'après une étude de l'INSEE reprise par le journal Les Echos/Solutions en janvier 2020 (https://bit.ly/2Pdg4lp), le pourcentage des TPE/PME dans le tissu économique français représente 99,9%. Parmi ces entreprises, toujours d'après cet article, on compte 3 millions de TPE dont plus de la moitié n'a pas de salarié.

Ce sont donc des millions de chefs d'entreprises et des gigas de données qui se trouvent exposés à des risques de sécurité numérique. Or, le constat, comme nous l'avons dit plus haut, est toujours le même, année après année, les petites et moyennes entreprises ne sont pas ou mal sécurisées. Les cyberciminels l'ont bien compris et ces entreprises deviennent une cible, réelle, car elles sont facilement piratables et permettent des gains rapides. Le temps où seules les très grandes firmes étaient victimes d'attaques ciblées est révolu. Certains groupes criminels se « spécialisent », ciblant désormais des fonctions spécifiques dans l'entreprise, notamment les fonctions comptables, pour perpétrer par exemple des « arnaques au président ».

Parallèlement, les Laboratoires viraux reçoivent des millions de virus à analyser quotidiennement.

Le VirLab de Doctor Web reçoit pour analyse entre 500 000 et 900 000 échantillons de malwares chaque jour, environ 40 000 menaces ciblant les mobiles sont étudiées quotidiennement.

La cybercriminalité se dote de plus en plus de moyens et recrute de meilleurs développeurs. C'est une course contre la montre permanente entre éditeurs de solutions de sécurité et cybercriminels.

Mais les outils de protection se modernisent, et le travail de recherche et de développement considérable que les éditeurs effectuent permet d'anticiper des tendances et de contrer les menaces avant qu'elles ne pénètrent les systèmes, ainsi que de les détecter et de les stopper beaucoup plus rapidement qu'avant.

Face à la diversité des types d'attaques et aux millions d'utilisateurs que celles-ci peuvent toucher, la responsabilité est partagée.

Informer, alerter, tel est le rôle de l'éditeur. Les dirigeants et professions indépendantes, de leur côté, doivent mettre en place des solutions, des bonnes pratiques, et des règles pour construire une politique de sécurité efficace.

Typologie des attaques

Il existe une multitude de types de virus, Trojans et autres malwares, qui, techniquement, fonctionnent différemment et sont donc capables d'effectuer différentes actions sur un ordinateur ou sur un mobile.

L'objectif des groupes cybercriminels à l'origine de ces malwares est, dans la très grande majorité des cas, de gagner de l'argent, le piratage pouvant également être perpétré à des fins d'espionnage dont le but sera le vol de données liées à la propriété intellectuelle et/ou industrielle.

Pour arriver à leurs fins, les pirates informatiques ont également développé des méthodes de fraude, regroupées sous l'acronyme « ingénierie sociale », qui vise à solliciter l'utilisateur afin qu'il effectue lui-même une action qui va lui porter préjudice, sans qu'il en ait conscience sur le moment.

Il serait bien trop long de détailler tous les types de malwares et leur fonctionnement technique, mais nous pouvons indiquer certaines méthodes et types de malwares très répandus, et nous ferons un focus sur les vulnérabilités logicielles, vecteurs de nombreux piratages.

Le Phishing

Le phishing, ou hameçonnage en français, est une méthode de piratage maintenant bien connue. Elle consiste à solliciter l'utilisateur et à l'inciter à communiquer des données personnelles et confidentielles, login et mot de passe, numéro de carte bancaire, et autres, via un lien dans un e-mail qui redirige vers le site web des attaquants. Le phishing utilise l'ingénierie sociale, un ensemble de techniques qui visent à manipuler l'internaute, soit en le mettant en confiance, par exemple, via un e-mail envoyé soi-disant de la part d'une personne de confiance ou d'une administration ; soit en lui faisant peur, en l'accusant d'avoir effectué des actions illégales sur Internet. L'ingénierie sociale se base sur la crédulité de la victime ainsi que sur la surprise induite par le message reçu, intégrant des notions d'urgence ou de gravité, ou bien, au contraire, s'insérant dans la vie quotidienne.

L'hameçonnage reste une technique de piratage très répandue, et le contenu des messages frauduleux envoyés s'est beaucoup « amélioré » au fil des années, rendant la technique encore plus redoutable.

Déni de service

Les attaques par Déni de service, ou DDoS, sont également très connues, et l'on pourrait penser que ce sont d'anciennes méthodes qui n'ont plus court. Ce n'est pas le cas. L'attaque par déni de service est, contrairement à d'autres attaques « de masse », des attaques dites ciblées. Elles sont perpétrées pour viser une entreprise en particulier, pour autant de raisons qu'il peut y avoir de sentiments humains. On considère que l'activité de l'entreprise n'est pas juste ou pas éthique, on souhaite se venger d'un ancien employeur ou associé, on veut affaiblir la concurrence etc.

Les attaques par Déni de service consistent en l'envoi d'un nombre très important de requêtes à un site web afin quil « tombe », c'est-à-dire qu'il se retrouve saturé par le nombre de requêtes et ne puisse y répondre. Il devient alors inaccessible aux internautes.

Nous pouvons considérer qu'il faudra environ une demi-journée pour réaliser que le site est tombé, souvent grâce aux clients qui appellent. Le temps de réaction/réparation peut prendre, quant à lui, entre une demi-journée et une journée entière, selon que l'entreprise a un prestataire informatique. La suspension de l'activité peut donc aller jusqu'à 48h, voire plus. Cela représente un vrai manque à gagner pour certaines sociétés, et l'image est engagée. Imaginons qu'une société vient de lancer son activité. Elle aura multiplié les annonces sur Internet, les réseaux sociaux, dans la presse, elle aura envoyé des mailings à des prospects etc. L'indisponibilité de son site peut réellement nuire à son image, car même si tout le monde sait que personne n'est à l'abri d'une attaque, lorsque cela arrive, cela effraie et « ne fait pas sérieux ».

Ransomwares

Les ransomwares, ou rançongiciels, sont des malwares qui chiffrent les données sur un ordinateur piraté et pour la récupération desquelles le groupe pirate qui se trouve derrière le malware demande une rançon.

Les rançongiciels font partie, depuis plusieurs années, des malwares les plus répandus, les plus dangereux et les plus lucratifs pour l'industrie cybercriminelle. Des milliers de types de ransomwares existent et sont créés chaque jour.

Lorsqu'ils sont apparus dans les années 2000, ces logiciels malveillants utilisaient l'ingénierie sociale et affichaient des messages intempestifs falsifiant les logos des instances officielles, police, gendarmerie, gouvernement, ministère de l'intérieur, et accusant l'utilisateur d'activité illégale sur Internet, typiquement, visionnage de sites pronographiques ou pédo-pornographiques. Ce sont les fameux « virus-gendarmerie ». Jouant là encore sur l'effet de surprise et sur la « peur du gendarme », ces messages donnaient un lien pour payer directement en ligne une soi-disant amende, allant de 100€ à 250€. De très nombreux utilisateurs se sont fait piéger.

Avec le temps, et la technique « fonctionnant » très bien, les cybercriminels ont développé d'autres malwares de ce type afin notamment de toucher aussi les entreprises. C'est l'apparition des **ransomwares à chiffrement**. Une fois introduit sur l'ordinateur, le malware cible et chiffre un certain nombre de données, qui sont donc totalement inutilisables et semblent irrécupérables. Ces données sont peut-être des fichiers indispensables à l'activité de l'entreprise, mais aussi des données confidentielles de clients ou de patients dont la protection engage la responsabilité de l'entreprise qui les détient. L'entreprise reçoit ensuite un message lui demandant de payer une rançon pour récupérer ses données.

Aujourd'hui, de nombreuses rançons sont demandées en Bitcoin et peuvent atteindre des sommes considérables.

Bien évidemment, le premier conseil que nous donnons aux entreprises touchées est de ne surtout pas payer la rançon. D'une part parce que cela encourage les cybercriminels à continuer, d'autre part parce qu'il n'y a aucune garantie que les données seront restaurées. Mais il est vrai qu'une petite entreprise qui ne possède pas de spécialiste en sécurité peut se trouver complètement démunie face à une telle situation et céder au chantage. Il est donc primordial pour les entreprises, quelle que soit leur taille, de penser leur sécurité.

Focus Vulnérabilités logicielles

Lorsque l'on parle de piratage on pense le plus souvent que les menaces viennent de l'extérieur (email, rançongiciels, malwares bancaires, etc.). L'ennemi est à l'extérieur, certes, mais si à l'intérieur du réseau existait une porte permettant de faire entrer le cambrioleur en toute discrétion ?

Tout logiciel comporte, dans son code, des failles potentielles qui pourraient être exploitées à des fins malveillantes, c'est-à-dire pour accéder à un ordinateur de l'entreprise et partant, à son réseau entier.

Les vulnérabilités logicielles font partie du monde informatique car la perfection n'existe pas. Mais les développeurs testent en permanence les logiciels qu'ils créent et publient ce que l'on appelle des « patchs de sécurité », des pansements, qui résolvent ces failles. Le problème est que les cybercriminels peuvent continuer à les exploiter sur tous les postes qui ne sont pas mis à jour, et cela laisse un très grand nombre d'utilisateurs accessibles.

Même les plus anciennes vulnérabilités continuent à être exploitées : Les virus bien connus comme WannaCry et NotPetya sont parvenus à infecter des millions d'ordinateurs uniquement grâce aux vulnérabilités logicielles qu'ils ont pu utiliser. Dans nos rapports viraux, il est fréquent que des exploits touchant d'anciennes versions de Microsoft Office arrivent en tête du top malware. Les mobiles ne font pas exception.

En matière de logiciel, l'expression « too big to fail » ne fonctionne pas. Les logiciels les plus connus sont aussi les plus complexes et donc sujets à des vulnérabilités et surtout, les plus dignes d'intérêt pour les cybercriminels. Aujourd'hui, les vulnérabilités logicielles font partie des vecteurs N°1 d'infection des réseaux d'entreprises.

Spam, le pollueur des messageries

Il n'est pas nécessaire de rappeler ce qu'est le spam, ces e-mails non désirés que les utilisateurs reçoivent chaque jour par dizaines.

En revanche, il est intéressant de rappeler que le spam est le vecteur de nombreuses fraudes et attaques, car les messages SPAM contiennent des liens et des pièces jointes que l'utilisateur est invité à visiter ou à ouvrir et qui vont infecter le réseau de l'entreprise s'il y consent.

Comme nous l'avons vu plus haut, pour inciter une personne à effecteur une action, il faut la manipuler. Se faire passer pour une administration, une banque, un opérateur, une société de services, ou un supérieur hiérarchique fonctionne malheureusement dans de (trop) nombreux cas.

« L'arnaque au président » en est un exemple et revient en force en 2021.

Cette méthode consiste à envoyer un e-mail à un employé, par exemple des services financiers de l'entreprise, en se faisant passer pour un supérieur hiérarchique et lui demandant d'effectuer un virement bancaire. Ce peut être une autre fonction visée afin d'obtenir des données confidentielles sur l'entreprise ou ses collaborateurs. La ficelle semble simple, mais qui refuse d'effecteur une action commandée par un supérieur ?

Cette technique de fraude a été récemment modifiée, ciblant plus spécifiquement des cadres supérieurs ou dirigeants afin de leur « commander » des actions venant de personnes encore plus haut placées, PDG, président etc. elle se nomme le Whaling, ou « pêche à la baleine ».

Ces attaques sont de plus en plus préparées et ciblées, rendant leur détection plus difficile, de même les e-mails provenant de soi-disant services de l'Etat, comme l'URSSAF, et qui sont menées via des campagnes de Spam massives dont les petites entreprises sont souvent les premières victimes.

Nouveaux modes de travail, la sécurité en jeu

Nouveaux modes d'organisation et travail à la maison versus sécurité des données

Les habitudes de travail sont en pleine mutation. Alterner travail au bureau et travail à la maison devient de plus en plus fréquent. Globalement, le nombre de personnes travaillant chez elle va augmenter dans les années à venir. Dans ce contexte, comment établir un environnement de travail bien sécurisé ?

Le travail à la maison instauré dans le contexte de la crise sanitaire qui a débuté en 2020 a vu de nouvelles fonctions quitter l'enceinte de l'entreprise pour travailler depuis l'extérieur.

Comptables, chefs produits, responsables marketing, assistants, autant de fonctions qui demeuraient historiquement au sein de l'entreprise et qui alternent maintenant bureau et home office.

On pense souvent que la sécurité informatique est uniquement virtuelle, mais en réalité, elle est également liée aux usages physiques des outils de travail, ordinateurs, Smartphones, tablettes.

Comment gérer l'utilisation d'ordinateurs à la maison, comment s'assurer que les données qui sortent puis entrent à nouveau dans le réseau de l'entreprise ne sont pas infectées et ne menacent pas toute l'activité ? Comment délimiter les usages des appareils informatiques lorsque le collaborateur travaille chez lui ?

Lorsque l'on travaille chez soi, le risque est de mélanger vie privée et vie professionnelle en matière d'utilisation des outils informatiques. Un enfant qui souhaite se connecter à l'ordinateur professionnel, une consultation de messagerie pro sur l'ordinateur familial, la connexion d'un dispositif USB à l'ordinateur professionnel....autant d'usages qui mettent en danger la sécurité des données.

Mais il faut également prendre en compte tout l'environnement dans le cadre du travail à la maison, notamment la présence d'objets connectés, dans le contexte d'une croissance exponentielle de « l'Internet des objets ».

Téléviseurs, caméras de surveillance, montres, réfrigérateurs, voitures, trackers de fitness, caméras vidéo, l'Internet des Objets regorge de gadgets dits intelligents, qui sont surtout connectés à Internet, pour le meilleur et pour le pire.

Peu protégés par les fabricants en amont, ils n'éveillent pas les soupçons des utilisateurs qui les trouvent « géniaux ». Mais, par exemple, pour se connecter à certains périphériques, des combinaisons " login – mot de passe " très simples et largement connues sont installées par défaut sur des centaines de milliers de modèles. Rien de plus facile à récupérer pour des pirates via la méthode de force brute (tester toutes les combinaisons possibles pour trouver un mot de passe).

Pour les six premiers mois de l'année 2019, 73 513 303 d'attaques sur les objets connectés ont été enregistrées.

Or, que l'on travaille sous macOS ou sous Windows, *tous les gadgets, téléphones et ordinateurs sont reliés, interconnectés*. Les données transitent en permanence entre les différents appareils et via Internet. Les conversations peuvent être enregistrées, des caméras activées à l'insu de l'utilisateur.

Plus on utilise d'objets connectés, plus on est susceptible de recevoir des notifications, alertes, recommandations, incitant à donner ses données confidentielles.

Le risque est également de voir l'ordinateur enrôlé dans un botnet pour envoyer du spam, ou de le voir utilisé comme « récolteur » de cryptomonnaie.

Pour infecter un ordinateur, il faut à un malware moderne moins de trois minutes. Une connexion Internet s'effectue en quelques secondes. Pour une action qui va durer quelques minutes mais qui ne respecte pas certaines règles de sécurité, ce sont des kilos de données qui peuvent se trouver endommagées, chiffrées, volées, détournées, perdues, et parfois soumises à une rançon.

Penser l'organisation (ou la réorganisation) de l'entreprise dans le cadre de ces nouvelles pratiques devra être une préoccupation majeure des chefs d'entreprise. Et la sécurité des données, si elle l'était déjà, devient encore plus fondamentale dans un environnement où celles-ci circulent plus, et finiront par revenir dans le réseau de l'entreprise.

Dans les nouveaux modes de travail qui se dessinent, la sécurité doit être pensée en amont, dès le début, et intégrée à la stratégie de travail à distance.

Les mobiles, cibles privilégiées, une réalité négligée ?

Tout comme les ordinateurs peuvent être utilisés à la fois dans un cadre professionnel et personnel, le mobile est depuis longtemps devenu un outil de travail.

De nombreux collaborateurs dans les TPE et PME utilisent leur mobile personnel pour travailler. Répertoires mixtes, messagerie professionnelle consultée sur le Smartphone, envoi de fichiers sensibles ou de contrats, consultation de comptes bancaires professionnels sur le téléphone, la facilité de travailler de n'importe où avec son téléphone portable en a fait un outil indispensable à la vie professionnelle. Et de très nombreux téléphones sont utilisés sans protection. Or, le piratage des mobiles constitue un des domaines les plus lucratifs et les plus développés de l'industrie cybercriminelle.

Le Smartphone est devenu une telle « extension » de nous-mêmes qu'il semble que la majorité des utilisateurs ne prennent pas conscience qu'il est pourtant relié à Internet en permanence, et qu'il peut surtout être relié au réseau de l'entreprise.

D'après les informations de Kantar World Panel, reprises dans un article du JDN publié en février 2021 (https://bit.ly/3uCDh0B), le système mobile de Google, Android, possédait 75,4% des parts de marché des OS mobiles en France en 2020. Cela représente des millions d'utilisateurs, et cela intéresse fortement le cybercrime. Comme nous l'avons indiqué plus haut, notre Laboratoire viral analyse en moyenne 40 000 menaces ciblant Android par jour, qui représentent environ 20% de la totalité des menaces traitées.

Or, la vente de solutions antivirus Dr.Web pour les mobiles, particuliers et entreprises confondues, représente moins de 10% de la totalité des ventes de nos produits antivirus.

Une prise de conscience doit s'effectuer quant à l'utilisation des mobiles dans un cadre professionnel.

Anticiper et réagir, comment penser la sécurité ?

Mettre en place une politique de sécurité

Comme toujours en matière de sécurité numérique, il est impossible de se protéger contre toutes les menaces. Le principe hélas trop bien rôdé des attaques est qu'elles peuvent frapper à n'importe quel moment et qu'il est impossible de savoir où elles vont frapper. Il est donc très difficile d'anticiper une attaque pour une entreprise.

Mais il est bien sûr possible et très avisé de mettre en place certaines règles et certains outils qui protègent efficacement contre la fraude et l'infection par un malware.

Plus les connaissances des chefs d'entreprise en matière de sécurité seront grandes, moins les cybercriminels auront de chance de parvenir à leurs fins.

Des outils adaptés

L'ANTIVIRUS

La première barrière contre les malwares sur un poste de travail ou un mobile est l'antivirus.

Les antivirus actuels ont énormément évolué et utilisent des technologies de pointe comme l'analyse comportementale, la protection préventive, l'analyse des processus, et d'autres, qui permettent une analyse complète des ordinateurs pour détecter, bloquer et éradiquer les virus. La recherche en virologie informatique, dans laquelle investit majoritairement Dr.Web, permet de créer des outils d'analyse, de restauration et de déchiffrement de fichiers efficaces.

Pour les mobiles, l'antivirus effectue une analyse en temps réel des applis téléchargées, offre la possibilité de mettre des filtres pour la consultation des sites web, un système antivol, un filtrage des appels et des SMS.

Le point le plus important est que l'antivirus doit être correctement paramétré.

Un antivirus présent sur un poste mais mal paramétré ne sera pas pleinement opérationnel et ne remplira pas son contrat, alors qu'il en a toutes les capacités. Dans la majorité des cas, les paramètres configurés par défaut procurent une sécurité optimale, il ne faut pas désactiver de fonctionnalités !

LES OUTILS DE SAUVEGARDE

Il est nécessaire d'utiliser des outils de sauvegarde, de s'assurer qu'ils sont bien reliés au réseau de l'entreprise et surtout qu'ils sont actifs et opérationnels (outils de type NAS).

En cas d'attaque entraînant un chiffrement ou une perte de données, la sauvegarde est vitale.

Des « bonnes pratiques » à respecter en permanence

On ne le répétera jamais assez, la sécurité des données numériques est liée au facteur humain et passe par le respect de certaines règles simples par tous les collaborateurs de l'entreprise. Il suffit d'une personne performant une seule action qui ne respecte pas la politique de sécurité pour que toute l'activité soit mise en danger.

Ces règles et bonnes pratiques peuvent être édictées dans une Charte informatique, fournie à tous les collaborateurs.
Nous pouvons distinguer les règles de sécurité dont la responsabilité incombe au Chef d'entreprise des bonnes pratiques que chacun devrait appliquer.

Les règles de sécurité de base

- Ne pas autoriser la connexion automatique des dispositifs USB sur les ordinateurs professionnels
- Changer régulièrement les mots de passe des serveurs, des postes, mais aussi des services en ligne divers utilisés par l'entreprise. Les mots de passe doivent être « forts », et contenir au moins 8 caractères, majuscule, minuscule, symbole, chiffre.
- Il est vivement recommandé de ne pas utiliser un mot de passe identique pour plusieurs services en ligne. Il est également possible de se doter d'un gestionnaire de mot de passe, qui permet de modifier régulièrement les mots de passe automatiquement.
- L'accès à l'antivirus sur l'ordinateur professionnel doit également être protégé par un mot de passe.
- Utiliser un VPN (Réseau Privé Virtuel) pour accéder au réseau de l'entreprise
- Mettre à jour les logiciels sur tous les postes de travail, que l'on télétravaille, que l'on soit profession indépendante ou au bureau. C'est primordial car les mises à jour corrigent régulièrement des failles de sécurité ou des vulnérabilités. Le plus simple est d'autoriser les mises à jour automatiques des logiciels, y compris l'antivirus !
- Gérer la consultation d'Internet sur les postes des collaborateurs. Il est possible de mettre en place des restrictions, notamment via l'antivirus, afin d'éviter l'accès aux réseaux sociaux et autres sites qui pourraient être porteurs de malwares.
- Pour les mobiles, la meilleure des sécurités est d'investir dans une flotte de mobiles professionnels sur lesquels ne sera pas autorisé le téléchargement d'applis non liées à l'activité professionnelle. Et doter ces mobiles d'un antivirus.

Les bonnes pratiques au quotidien

En parallèle des outils de protection sur les appareils, l'autre barrière contre la contamination est tout simplement la vigilance !

Un pourcentage très important de contaminations est dû à une action effectuée par l'utilisateur lui-même, qui déclenche l'infection ou le déploiement de malwares sur le poste.

Les dirigeants devraient informer leurs collaborateurs des dangers et leur demander d'être attentifs et vigilants. Ce qui s'explique en une réunion d'une heure peut permettre de protéger l'entreprise.

- Ne jamais cliquer sur un lien dans e-mail si l'expéditeur n'est pas sûr. La même chose pour une pièce jointe.
- Ne jamais donner d'identifiants, login/mot de passe, quelle que soit la personne ou l'organisme qui le demande. Les banques, services d'impôts ou autre ne demandent jamais d'identifiants par e-mail.
- Les pirates essaieront de se faire passer pour un supérieur hiérarchique, un patron, ou le dirigeant lui-même pour extorquer de l'argent via une demande virement. Il convient de vérifier avant d'agir !
- Sur mobile, ne pas télécharger d'applications en dehors des catalogues officiels, et même dans ce cas, il faut conserver sa vigilance. Très peu d'applis demandent des accès privilégiés à toutes les fonctions de l'appareil, si c'est le cas, méfiance.
- Ne pas transférer de fichiers confidentiels ou de haute importance via la messagerie du Smartphone, et ne pas conserver de fichiers importants sur son téléphone portable
- Eviter d'utiliser les réseaux wi-fi publics pour travailler
- Ne pas noter ses mots de passe

Répondre à une attaque

Des ordinateurs qui ralentissent ou fonctionnent mal, un problème au niveau de la messagerie de l'entreprise, un site web qui n'est pas opérationnel... ces symptômes peuvent indiquer une cyberattaque.

Le premier facteur et le plus important en cas d'attaque est le facteur temps.

Plus la réaction sera rapide, plus on pourra limiter les dégâts à tous points de vue : fonctionnement du réseau, perte de données, image de l'entreprise.

Pour les entreprises qui n'ont pas de responsable informatique, il est aujourd'hui indispensable d'avoir un prestataire ayant des compétences en sécurité, qui saura intervenir rapidement.

Quels réflexes adopter si un piratage est constaté ?

S'il s'agit d'un rançongiciel, il ne faut pas payer la rançon ! Cela n'apporte aucune garantie de restauration des fichiers chiffrés, et cela permet à ce système criminel de perdurer.

Au niveau du poste touché, voici quelques conseils d'actions à éviter :

- Ne pas tenter de mettre à jour l'antivirus ou de lancer un scan – cela pourrait détruire les traces du malware dans l'ordinateur
- Ne pas tenter de réinstaller le système d'exploitation !
- Ne pas tenter de supprimer des fichiers ou logiciels sur le disque dur
- Ne pas utiliser un ordinateur sur lequel a eu lieu une fuite d'identifiants pour se connecter à un système de e-banking, même en cas d'urgence.

Isoler le poste touché du réseau et attendre qu'il soit analysé.

Si c'est le service comptable qui a été attaqué et que des identifiants bancaires ont été dérobés, l'entreprise doit immédiatement prévenir sa banque et il est également judicieux d'aller porter plainte. De nombreuses entreprises touchées par une infection virale ne portent pas plainte mais les autorités ont besoin de ces plaintes pour enquêter, et il existe des services de police spécialisés dans la cyberdéfense. L'accumulation de plaintes et de données techniques peuvent permettre de remonter une filière cybercriminelle.

L'externalisation, un modèle pertinent

La sécurité informatique est un métier et gérer la sécurité d'une entreprise requiert des compétences et du temps, ce que ne possèdent pas la plupart des dirigeants de TPE et PME.

Mais, et nous espérons l'avoir fait comprendre dans ce Livre blanc, le piratage est une réalité qui peut toucher tout le monde, à n'importe quel moment.

De très nombreuses entreprises réagissent après avoir essuyé une attaque ou une infection.

Il faut à un malware moderne moins de trois minutes pour infecter un réseau. Mais certains logiciels malveillants restent en sommeil pendant un certain temps avant de se mettre en action.

Si le malware est devant la porte, il est déjà trop tard.

Dans ce contexte, l'externalisation est un modèle pertinent car il associe réactivité, contrôle quotidien du réseau, respect de la politique de sécurité.

Travailler avec un prestataire informatique ayant des compétences en sécurité est avantageux en termes de coût et de nombreux prestataires travaillent main dans la main avec leurs clients « comme s'ils étaient en interne ». De plus, le fournisseur bénéficie du support technique de l'éditeur avec lequel il travaille, ce qui apporte une garantie supplémentaire de la bonne gestion de la sécurité de l'entreprise et d'une bonne réactivité en cas de problème.

Toutes les entreprises devraient être accompagnées sur ce terrain.

Doctor Web travaille avec un réseau de partenaires de confiance qui connaissent ses produits et possèdent les compétences nécessaires à l'organisation et la mise en place d'une politique de sécurité efficace.

Doctor Web France
333b, avenue de Colmar – 67100 Strasbourg
Tél. : 03 90 40 40 24