SVP
INFORMATION
DÉCISIONNELLE

LIVRE BLANC DES EXPERTS SVP

Cybersécurité : comment protéger vos données ?

Le livre blanc des experts SVP

Le thème du livre blanc

Cybersécurité, comment protéger vos données ?

À qui s'adresse ce livre blanc ?

Directeur technique d'une collectivité, DGS, DRH, Responsable informatique, Dirigeant de TPE et de PME/PMI

Pourquoi vous proposer ce contenu ?

Pour vous accompagner dans la mise en œuvre de la cybersécurité dans votre organisation et vous donner des solutions concrètes pour répondre à la forte augmentation du risque informatique et de ses conséquences néfastes.

Quels sont les points abordés ?

Ransomware et piratage, comment réagir ? Comment créer un mot de passe fort ? Faut-il accepter l'utilisation des équipements personnels pour l'accès aux informations de l'organisation ? Que doit préciser une charte informatique ?

Comment SVP peut vous être utile ?

SVP possède un pôle d'experts spécialisés pouvant vous accompagner dans la mise en œuvre de la cybersécurité.

SOMMAIRE

Introduction

La crise générée par la pandémie liée à la Covid-19 a obligé nombre d'entreprises et de collectivités à se réinventer. La mise en place du télétravail à grande échelle en est l'une des principales conséquences. Et, avec le développement du télétravail, la transformation numérique des organisations s'est accélérée.

Mais la transformation numérique des organisations suppose de mettre en place une infrastructure informatique étendue et plus ouverte. Si, dans le monde physique, pour lutter contre les vols de matériels et les intrusions dans les locaux, il faut renforcer la sécurité de tous les accès, il en est de même avec le réseau informatique. Chaque poste informatique, dès qu'il permet l'accès vers l'extérieur (Internet, envoi et réception de courriels…), devient une porte qu'il est nécessaire de sécuriser.

Et selon un grand cabinet d'études de marché, le développement du travail hybride, avec une proportion en télétravail et l'autre dans les locaux, va encore augmenter de 30% au cours des deux prochaines années. Ce changement dans les organisations rend toujours plus complexe la réponse à apporter à la sécurité informatique.

Les cyberattaques se multiplient, avec des conséquences parfois funestes pour l'entité attaquée. Le ransomware est aujourd'hui le moyen utilisé dans plus de la moitié des cas par des groupes de hackers internationaux, de mieux en mieux équipés et organisés. Le système d'information de l'organisation n'est plus seulement bloqué, en attente d'une rançon, les données sont souvent également dérobées pour être revendues au plus offrant.

Il est évidemment nécessaire d'apporter une réponse technologique avec des antivirus régulièrement mis à jour, un VPN (réseau privé virtuel) canalisant l'ensemble des flux entrants et sortants des équipements distants ou encore un pare-feu pour sécuriser le réseau, mais cela ne suffit pas. L'ensemble des utilisateurs doit être acteur de la sécurité informatique. Il doit être informé du risque et des moyens de lutte mis en place, connaître l'importance d'un mot de passe résistant et avoir lu et compris la charte informatique.

Vous trouverez, dans ce livre blanc, quelques réponses concrètes aux nombreuses questions que vous pouvez vous poser.

.

I) Cybercriminalité : les gestes qui peuvent vous sauver

La cybercriminalité regroupe l'ensemble des actions visant à porter atteinte aux systèmes d'information des organisations. Parmi l'arsenal des pirates informatiques, le rançongiciel (ou ransomware) apparaît actuellement comme la menace la plus importante. Il chiffre les fichiers, vous empêchant d'accéder aux données de l'entreprise ou de la collectivité et vous signale que vous ne pourrez récupérer vos informations que si vous versez une rançon, généralement sous la forme de bitcoins intraçables. Mais faut-il céder à cette menace ?

A) Qu'est-ce qu'un rançongiciel ou ransomware ?

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit le rançongiciel ou ransomware comme étant une « technique d'attaque courante de la cybercriminalité qui consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement ».
Mais heureusement, elle ne fait pas que le définir, dans une alerte pour prévenir d'une campagne d'attaque par rançongiciel, elle explique surtout comment prévenir et remédier à ce risque. A commencer par sensibiliser l'ensemble des salariés et mettre en place des actions simples telles que réaliser des sauvegardes fréquentes, n'ouvrir que les courriels dont l'émetteur est fiable, éviter l'ouverture de pièces jointes avec des extensions potentiellement actives (.scr, .cab, .exe...) et surtout, ne pas payer la rançon !

B) Le « hacker », version moderne du pirate ?

Dans l'imaginaire collectif et dans certains films à grand succès, les pirates sont des personnages dotés d'une image positive. Ils sont forts mais bienveillants envers les déshérités et souvent plutôt attrayants. Pourtant, si l'on regarde de plus près qui étaient les pirates, il s'agissait d'hommes sans foi ni loi qui tuaient et jetaient à la mer leurs victimes, les marins, pour s'approprier la cargaison du navire qu'ils assaillaient.
Cette image positive a, pour beaucoup, perduré dans la version du pirate moderne, le hacker informatique. Il est, au pire, un jeune homme, particulièrement doué pour la chose informatique, qui s'amuse à montrer les failles des systèmes d'information et, au mieux, un des membres d'une organisation qui veille au bien de l'humanité, au respect des données personnelles et qui va s'attaquer aux entités terroristes ou irrespectueuses des droits de l'Homme, comme c'est le cas pour nombre de ceux qui se réclament des « Anonymous ».

C) L'hacktivisme n'est plus ce qu'il était

Une étude en anglais du "IBM X-Force Threat Intelligence", publiée en 2019 par IBM, montre une baisse de près de 95% entre 2015 et 2018, des attaques des grands groupes par des pirates informatiques. Plus particulièrement, le collectif Anonymous et les groupes associés dans différentes parties du monde ont commis moins d'attaques. Mais ces "hacktivistes", néologisme créé à partir de la contraction de « hacker » et d'activiste, qui avaient certainement, pour une grande majorité et à leurs yeux, une volonté noble dans leurs actions ne sont plus le principal danger qui menace les organisations publiques ou privées.
Les attaques informatiques et la cybercriminalité sont, à l'heure actuelle, le fait de groupes organisés qui ont plus le profil de vrais pirates des mers, avec un but de nuire ou de voler des biens immatériels et de demander des rançons. Et surtout, ils visent dorénavant des cibles qualifiées.

D) Des groupes de plus en plus organisés

Plus surprenant au regard de leurs activités criminelles, ces groupes semblent vouloir mettre en place une « charte de bonne conduite ». Par exemple, les membres du groupe Revil, opérateur d'un ransomware particulièrement actif, viennent de déclarer sur un forum russe qu'ils s'interdisent désormais les attaques sur les mondes de la santé et de l'éducation, ainsi que les administrations de tous pays. Les opérateurs du groupe Avaddon font de même en interdisant les attaques sur le secteur public, la santé et l'éducation et les organisations caritatives. Ils vont même jusqu'à obliger les utilisateurs de ce ransomware à demander une validation des cibles potentielles avant engagement !

E) Une hausse des attaques de plus de 200%

Une note de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) précise une augmentation de 255%, passant de 54 à 192 signalements d'attaque par rançongiciel entre 2019 et 2020 dans son périmètre.

Dans un communiqué de presse publié en avril 2021, Kaspersky, éditeur de solutions pour lutter contre la cybercriminalité, explique que seulement quelques groupes seraient à l'origine de plus de 75% des attaques vers les entreprises et les organisations. Il démontre que les attaques ne sont plus lancées en masse, avec l'espoir d'en retirer quelques profits, à l'image d'un immense filet de pêche pour attraper quelques poissons, mais bien des attaques ciblées sur des organisations qualifiées à « haut potentiel » de paiement par l'éditeur.

Dans son rapport sur « L'état de la menace rançongiciels à l'encontre des entreprises et institutions », le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), confirme cette tendance forte à la hausse de la cybercriminalité. Et ces groupes, composés indéniablement de personnes particulièrement compétentes en

développement informatique, peuvent parfois préparer plusieurs mois à l'avance leurs attaques ciblées. Le rapport fait notamment état du ransomware Netwalker dont le montant de la rançon est adapté aux revenus de l'entreprise ou encore RansomEXX dont l'échantillon du code contient le nom de la victime et dont l'extension de fichiers et l'adresse courriel de contact utilisent le nom de la victime.

F) Pourquoi ne faut-il pas payer ?

Effectivement, payer ne sert à rien et l'étude « State of ransomware 2021 » de Sophos le prouve. Son auteur indique que de plus en plus d'organisations cèdent au chantage, passant de 26% en 2020 à 32% en 2021. Mais l'étude précise que les chances de récupérer toutes les données après avoir versé la somme demandée sont très faibles, seulement 8% de ces organisations ont pu récupérer tous ses fichiers cryptés. Elle indique encore qu'en moyenne, ceux qui ont payé n'ont récupéré que 65% de leurs données, et 29% n'ont pas récupéré plus de la moitié de leurs données. Et de conclure, presque avec humour, « Quand il s'agit de ransomware, il ne paie pas de payer ».

II) Comment se prémunir de la cybercriminalité ?

Le développement du télétravail est un facteur qui rend encore plus vulnérable le système d'information de toute organisation. En effet, chaque poste de télétravail est une porte plus ou moins facile à ouvrir pour le pirate. Il est donc essentiel de sensibiliser chaque collaborateur aux dangers de la cybercriminalité.

Les collaborateurs doivent se créer des mots de passe forts, c'est-à-dire à même de résister un temps suffisant pour permettre au service en charge de la sécurité informatique de réagir.

Ils doivent disposer de moyens leur permettant de sauvegarder, sur des supports sécurisés ou amovibles, les données de leur travail, de façon périodique.

S'il est permis dans l'organisation, l'utilisation des équipements personnels doit être encadrée et la sécurité de ces matériels doit être validée par le responsable de la sécurité informatique.

Les dirigeants et les DSI ou les directeurs informatiques doivent mettre en place, a minima, une charte informatique qui précise clairement ce que le salarié peut faire et ne doit pas faire, sauf à mettre en péril le fonctionnement de son entreprise.

A) Le mot de passe

Pour accéder à son équipement informatique, il est nécessaire d'utiliser un mot de passe. L'utilisateur doit avoir conscience que ce mot de passe est un élément essentiel de la sécurité informatique et qu'il en est le garant.

Les pirates disposent de moyens informatiques importants et utilisent notamment la technique dite de « force brute ». Concrètement, les programmes d'attaque vont tester toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe, sachant que plusieurs dizaines de milliers de combinaisons peuvent être essayées en quelques secondes. Plus le temps est long pour trouver la bonne combinaison, plus il y a de chance pour que l'attaque soit détectée par le système de sécurité et donc bloquée.

1) Un mot de passe complexe

Ce mot de passe doit donc être résilient et, pour ce faire, il doit comporter un nombre important de caractères et mélanger des majuscules, des minuscules, des chiffres et des caractères spéciaux tels que ?, !. #...

Trop souvent, l'utilisateur, par peur de l'oublier, va utiliser un mot de passe trop simple (123456) ou trop évident (son prénom ou sa date de naissance). Afin de créer un mot de passe fort que l'utilisateur n'aura aucun mal à retrouver, il existe un moyen mnémotechnique. Il suffit de transformer une phrase en caractères, et en y ajoutant quelques astuces.

Par exemple, la phrase « J'ai acheté deux documents intéressants ! » devient « Ght2doc1Tré100! » ou encore, avec une expression familière, en ne reprenant que les premières lettres et des chiffres et des caractères spéciaux, « On a toujours besoin d'un plus petit que soi !» devient « Oatbd'1ppqs! ». D'autres exemples sont présentés en page suivante.

Evidemment, si vous utilisez un ordinateur en libre-service, dans un cybercafé ou un hôtel, n'enregistrez pas le mot de passe, lorsque cela vous est proposé. Il pourrait être aisément récupéré par un utilisateur malveillant qui utilise l'ordinateur après votre passage.

Ne négligez pas le mot de passe de votre messagerie. En effet, il est souvent possible de demander la réinitialisation de son mot de passe en obtenant un lien par courriel. Si c'est le cas, le pirate peut l'utiliser et même, par la suite, modifier le courriel rattaché à l'application. Non seulement, il aura accès à l'application mais vous ne pourrez plus récupérer la main par la suite…

Enfin, peut-être évident mais il est important de le rappeler, ne notez pas votre mot de passe sur un document accessible à proximité de votre équipement. Le petit papier collé sur le bord de l'écran ou sur le mur ne doit pas être envisagé. Si vous ne parvenez pas à retenir un mot de passe, vous le notez uniquement sur un document que vous conservez sur vous ou, au pire, dans un tiroir fermé à clef.

2) Le gestionnaire de mots de passe

La direction informatique peut également mettre à disposition de l'utilisateur un gestionnaire de mots de passe, dont certains sont disponibles en licence libre. L'ANSSI a, par exemple, certifié l'outil KeePass, disponible gratuitement sous licence GPL v2. Ce petit logiciel peut, en n'en retenant qu'un seul, celui pour accéder à l'équipement, gérer et même proposer de générer tous les mots de passe des différentes applications et des sites nécessaires à l'activité du collaborateur.

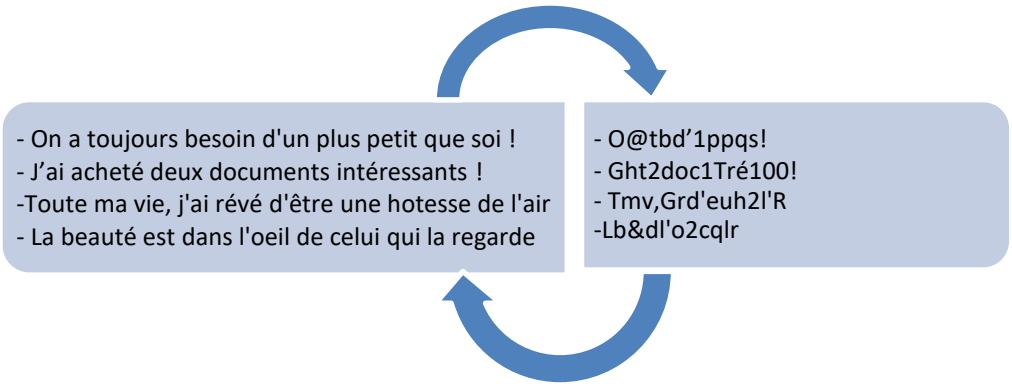
B) Comment créer des mots de passe résistants ?

A partir d'une phrase ou d'un dicton contenant idéalement au moins une dizaine de mots, il est assez simple de créer un mot de passe complexe.

Chaque mot de la phrase sera remplacé soit par sa première lettre en minuscule ou en majuscule, soit par un caractère spécial, soit encore par un chiffre. Par exemple, « a » ou « à » devient @, « e » ou « est » devient &, « un » devient 1 et « de » devenant 2.

Pour durcir encore le mot de passe, il est possible de changer des mots ou des groupes de mots par une lettre en majuscule, ainsi « j'ai » devient G et « air » devient R, voire un mot par plusieurs caractères, « intéressant » devenant 1Tré100.

Ceci peut paraître compliqué mais c'est beaucoup plus facile lorsque c'est vous qui avez créé le mot de passe, avec votre façon de penser.



Essayez par vous-même, vous constaterez que cela peut même s'avérer très amusant !

C) Les sauvegardes de données

Plus de 700 000 plaintes pour vol de téléphones sont déposées chaque année. Et les assurances ne remboursent que le matériel, pas ce qu'il contient. Vous perdrez donc vos photos, documents personnels mais peut-être aussi, le fichier de vos clients ou les contacts professionnels.

Dès que vous constatez le vol, il faut, bien sûr, déposez plainte pour pouvoir éventuellement bénéficier de l'assurance mais surtout, prévenez le responsable informatique, afin qu'il change l'ensemble de vos identifiants et que l'accès à vos applications ne soient pas possible avec le matériel dérobé.

Et parfois, le vol n'est pas seulement un hasard, il peut s'agir d'un acte malveillant destiné à récupérer des données confidentielles…

Sauvegarder pour préserver ses données

Les sauvegardes sont trop souvent considérées comme chronophages, voire inutiles.

Pourtant, si votre smartphone ou votre ordinateur professionnel est dérobé, vous risquez de perdre les données contenues dans ces équipements, si elles n'ont pas été sauvegardées en lieu sûr. Elles pourront même parfois être utilisées pour nuire à votre entreprise.

Avant de commencer, il est nécessaire de faire un audit des équipements et de ce qu'ils contiennent, afin de déterminer ce qui nécessite une sauvegarde externe et la périodicité de cette sauvegarde.

Certains vont, par exemple, considérer que la sauvegarde de photos personnelles est essentielle et doit être faite plusieurs fois par an, alors que d'autres estimeront que celle-ci peut être effectuée une seule fois l'année. En revanche, concernant les documents professionnels, la périodicité doit être importante, la perte d'une seule journée de travail peut s'avérer catastrophique.

La sauvegarde doit être effectuée sur un support chiffré, s'il est connecté. Il existe de nombreuses solutions permettant de sauvegarder des données qui ont été préalablement rendues illisibles avec un algorithme de chiffrement. Ces données peuvent alors être déposées sur un site distant sans risque puisque seul le détenteur de la clé de déchiffrement peut les lire.

Il est également possible de sauvegarder ses données sur un support mobile (disque amovible, par exemple) qui sera conservé dans un lieu protégé (tiroir ou armoire fermée à clef ou coffre-fort).

Si la sauvegarde est mise en place au sein de l'entreprise, il peut s'avérer opportun de se rapprocher d'éditeurs de solutions de sauvegarde automatique.

Celles-ci vont, sans action de la part de l'utilisateur, procéder toutes les nuits, par exemple, à la récupération des données modifiées dans la journée précédente, afin de les préserver d'une disparition ultérieure.

Selon les fournisseurs, les données seront stockées sur des serveurs protégés et dupliqués en temps réel ou sur des supports physiques, cette dernière solution étant de moins en moins privilégiée.

III) BYOD or not BYOD

Est-il souhaitable de permettre aux utilisateurs d'utiliser leur smartphone ou leur PC portable pour accéder à la messagerie d'entreprise ou à l'intranet ?

La question se pose notamment pour les salariés qui ne disposent pas d'un équipement mobile professionnel et qui souhaitent se tenir au courant des informations publiées par la direction ou par le CSE.

Et cet usage est assez facile puisqu'il suffit souvent d'indiquer son identifiant (nom ou adresse courriel) et son mot de passe. Si l'entreprise n'a pas mis en place un contrôle des accès supplémentaires, le collaborateur peut lire ses mails professionnels et toutes les communications sur le réseau d'entreprise.

Mais l'utilisation de moyens personnels pour accéder au réseau de l'entreprise est toujours dangereuse.

En effet, le téléphone portable et l'ordinateur personnel ne disposent généralement pas des moyens de protection mis en place par l'entreprise pour protéger son système d'information.

De plus, l'utilisation, à titre personnel, de nombreuses applications qui ne disposent pas du même niveau de sécurité que les solutions mises en place dans l'environnement professionnel, génère de nouveaux risques.

Si vous souhaitez permettre l'accès au réseau des collaborateurs avec leur propre équipement, ce que les anglo-saxons appellent le BYOD (Bring Your Own Device), il est très important d'avoir fait valider la protection de celui-ci par la personne en charge de la sécurité informatique de l'entreprise (DSI, RSSI ou autre).

Les équipements personnels sont souvent des portes plus facilement ouvertes par les hackers, leur permettant ainsi d'accéder à l'ensemble du système d'information.

Nombreux sont les ordinateurs personnels qui sont infectés par un logiciel espion qui fait remonter les informations sensibles vers la personne malveillante qui l'a diffusé.

En effet, certains logiciels espions fonctionnent comme des enregistreurs de frappe et alimentent ainsi en mots de passe, informations personnelles et données confidentielles, un pirate qui pourra ensuite monnayer ces informations sur le « darknet », par exemple.

Et une fois qu'ils sont installés sur l'équipement, il est souvent difficile de les déloger ou même de les détecter si l'on ne dispose pas d'une protection informatique suffisante.

IV) La charte informatique

La charte informatique d'une entreprise ou d'une collectivité fixe les règles et les conditions dans lesquelles les équipements informatiques et les applications peuvent être utilisées par les collaborateurs (salariés ou agents).

Elle prévoit aussi les éventuelles sanctions dont est passible l'utilisateur s'il ne respecte pas ces règles et ces conditions.

La charte est un des éléments essentiels de la sécurité informatique, dans la mesure où elle vient en amont des outils de protection informatique. En effet, elle va expliciter les usages plutôt que de les contrôler.

L'entreprise doit donc sensibiliser les utilisateurs au respect de la charte en lui faisant prendre conscience qu'elle n'est pas mise en place pour le contraindre mais bien pour protéger les biens immatériels de l'entreprise tels que le fichier clients, les documents liés à la propriété intellelectuelle et notamment ses propres données confidentielles.

Pour l'écriture de cette charte, il est utile de se référer aux excellents conseils de la CNIL qui précise qu'une charte doit au moins comporter les éléments suivants :

- Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.
- Le champ d'application de la charte, qui inclut notamment :
    - les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
    - les moyens d'authentification utilisés par l'organisme ;
    - les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
        - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
        - ne jamais confier son identifiant/mot de passe à un tiers ;
        - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
        - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
        - ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;
        - respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.

A ces règles, l'entreprise peut utilement y ajouter celles relatives à la création de mots de passe et à l'utilisation des équipements personnels.

Il est également possible d'y inclure les règles d'application pour le droit à la déconnexion définies par l'organisation, conformément à la loi El Komri.

V) Communiquer : le nerf de la guerre

La sensibilisation de tous à la sécurité informatique est le point essentiel de la lutte contre la cybercriminalité.

Les informations concernant les risques liés à cette cybercriminalité doivent être connues par l'ensemble des collaborateurs, qu'ils disposent ou non de moyens informatiques.

La création et l'affichage de fiches synthétiques résumant les bonnes pratiques peuvent être mises en place.

Pour se faire, il est également possible de s'inspirer des informations disponibles sur le site cybermalveillance.gouv.fr.

Le lecteur y trouvera un guide des bonnes pratiques pour les entreprises et les collectivités qui décrit, dans un langage simple, politique d'équipements des télétravailleurs, maîtrise et sécurisation des accès et des mots de passe, sauvegarde des données et communication pour informer les salariés.

Un « kit de sensibilisation aux risques numériques » est également disponible abordant, au travers de fiches, les nombreux visages de la cybercriminalité et les actions à mettre en œuvre pour s'en protéger.

A mettre impérativement entre toutes les mains…

Comment SVP peut vous être utile ?

Née en 1935, SVP fournit de l'information opérationnelle aux décideurs, en entreprise et collectivité, pour les aider au quotidien dans leur pratique professionnelle. Elle leur apporte pour cela les réponses immédiates dont ils ont besoin pour gérer et développer leurs activités.

La société accompagne à ce jour 7 000 clients et 30 000 décideurs grâce à 200 experts organisés par domaine de compétences : ressources humaines, fiscalité, vie des affaires, communication/marketing, finance, sourcing...

Grâce à leurs compétences multiples et aux outils documentaires sans équivalent mis à leur disposition, ces experts répondent ainsi en toute confidentialité – et principalement par téléphone - à près de 2 000 questions posées quotidiennement.

SVP
INFORMATION DÉCISIONNELLE

TÉL. **01 47 87 11 11**
WEB **www.svp.com**