Sécurité de l'information

Guide pratique pour les entreprises et les collaborateurs

mai 2023

YBCS

L'importance d'une culture de sécurité

Dans un monde hautement digital évoluant à toute vitesse, la sécurité de l'information est devenue un enjeu majeur pour toutes les entreprises et les collaborateurs.
L'augmentation exponentielle des cyberattaques et les vols de données de plus en plus massifs mettent en lumière l'importance d'une culture de sécurité solide et bien intégrée dans chaque organisation.

En instaurant une culture de sécurité, les entreprises contribuent à créer un environnement où la sécurité est une priorité pour tous. Les collaborateurs sont encouragés à adopter des comportements sécurisés, à signaler les incidents et à partager les meilleures pratiques.
Les dirigeants, quant à eux, doivent montrer l'exemple en mettant en place des politiques de sécurité claires et en investissant dans la formation et dans les technologies nécessaires pour protéger l'entreprise et la bonne marche de ses affaires.

Dans ce guide, nous explorerons certaines facettes de la sécurité de l'information et vous présenterons des conseils pratiques pour la renforcer. Nous traiterons des menaces et des risques, des bonnes pratiques ainsi que des outils et des astuces pour optimiser la sécurité de l'information.

Je vous souhaite une bonne lecture et espère que ce guide sera utile dans votre quotidien.

Yvann Barras
YB Conseils & Solutions Sàrl

Sommaire

Deux types de menaces

Dans le domaine de la sécurité de l'information, les menaces peuvent être nombreuses tout comme les risques qui leur sont associés. Comprendre ces dangers est la première étape pour mieux les anticiper et se protéger efficacement.

On distingue deux catégories de menaces :

- les menaces externes
- les menaces internes

Les menaces externes

Ces menaces proviennent de sources extérieures à l'entreprise comme les cybercriminels, les « hacktivistes » (contraction de hackers et activistes) et même des concurrents malintentionnés. Cette liste n'est cependant pas exhaustive.

Parmi les risques associés à ces menaces, on peut citer :

- Les attaques par phishing : des tentatives de tromperie visant à obtenir des informations sensibles, comme des mots de passe ou des données financières, en se faisant passer pour une entité de confiance.
- Les ransomwares : de petits logiciels malveillants qui chiffrent les données de l'utilisateur ou de l'entreprise entière et exigent une rançon pour les débloquer.
- Les vols de données : l'accès non autorisé et le vol d'informations sensibles, telles que les données personnelles des clients ou des employés, ou les secrets industriels.
- Les attaques par déni de service (DDoS) : des attaques qui visent à rendre indisponible un service en ligne en le surchargeant de trafic.
- Les attaque « Man in the Middle » : des attaques consistant à intercepter et potentiellement altérer les communications entres deux parties sans que celles-ci ne se doutent de la présence de l'attaquant. L'attaquant peut ainsi accéder, modifier ou voler des informations échangées voir même injecter des logiciels malveillants.

Les menaces internes

Ces menaces proviennent d'individus ou de processus directement au sein de l'entreprise ou de son environnement. Cela peut être les employés, les prestataires ou même certains partenaires commerciaux. Les menaces internes sont souvent négligées mais elles peuvent avoir un impact significatif sur la sécurité.

Les risques y relatifs peuvent être intentionnels ou involontaires, et incluent notamment :

- Les négligences ou erreurs humaines : elles peuvent résulter d'un manque de formation ou de la méconnaissance des politiques de sécurité. Par exemple, un employé peut envoyer par inadvertance un email contenant des informations sensibles à une personne non autorisée.
- Les abus d'accès et de privilèges : un collaborateur mécontent ayant accès à des données sensibles pourrait les exploiter à des fins personnelles ou pour nuire à l'entreprise. Par exemple, un collaborateur pourrait supprimer des données cruciales ou divulguer des informations confidentielles à des concurrents.
- L'usurpation d'identifiants : les noms d'utilisateurs et les mots de passe, peuvent être usurpés ou compromis par négligence. Un employé qui partage son mot de passe avec un collègue, par exemple, peut involontairement ouvrir la porte à un accès non autorisé aux systèmes et aux données de l'entreprise.

Nous considérons toutefois que l'humain est un atout essentiel en tant que premier rempart pour la sécurité des données et non un facteur de risque. Il est néanmoins primordial de sensibiliser et de former les collaborateurs à ces questions. L'instauration d'une politique de sécurité claire est également nécessaire dans ce contexte.

«Les erreurs les plus dangereuses sont celles que nous sommes tentés de considérer comme banales.»

Auteur inconnu

Les bonnes pratiques

Les mots de passe

Les mots de passe sont un sujet qui revient systématiquement quand il s'agit de sécurité de l'information. Malgré cela, ils restent, encore et toujours, **la première source de violation** à travers le monde.

La gestion des mots de passe est, et restera, un élément essentiel dans le domaine de la sécurité de l'information.

Voici quelques bonnes pratiques en matière de mot de passe :

1. Créer des mots de passe forts : les mots de passe doivent être suffisamment longs et complexes pour résister à la fois aux tentatives de devinettes et aux attaques par force brute. Un mot de passe fort devrait comporter au moins 12 caractères, inclure des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

   Évitez les mots de passe basés sur des mots du dictionnaire, des noms propres ou des informations personnelles faciles à deviner comme par exemple le prénom, l'année de naissance ou le club de foot préféré.

2. Utiliser des mots de passe uniques pour chaque accès : il est important d'utiliser des mots de passe différents le plus souvent possible afin d'éviter qu'une violation de sécurité sur un site ne compromette les autres comptes. Cela limite les dégâts potentiels en cas de vol ou de divulgation du mot de passe.

3. Mettre à jour les mots de passe : les mots de passe devraient être changés tous les ans voir même tous les six mois. Cela réduit le risque qu'un mot de passe compromis puisse être utilisé pendant une longue période sans être détecté.

   Cette mesure a été longtemps âprement prônée. Cependant avec le respect des bonnes pratiques aux points 1 et 2, elle représente un plus faible facteur de risque qu'auparavant.

4. Ne pas partager les mots de passe : il est essentiel de garder à l'esprit que les mots de passe sont confidentiels et ne doivent pas être partagés avec d'autres personnes, y compris des collègues, des amis ou des membres de la famille. Les mots de passe doivent être traités comme des informations sensibles et confidentielles.

5. Activer la double authentification (2FA) : l'authentification à deux facteurs ajoute une couche de sécurité supplémentaire en demandant à l'utilisateur de fournir un deuxième élément d'identification, comme un code reçu par SMS, en plus du mot de passe. La 2FA rend beaucoup plus difficile l'accès non autorisé aux comptes, même si le mot de passe est compromis.

La société Hive Systems publie chaque année une étude sur le temps moyen nécessaire pour «cracker» un mot de passe dans le cadre d'une attaque par force brute. **Le temps moyen nécessaire baisse significativement chaque année** à mesure que les techniques d'attaque s'améliorent.

Voici un extrait des résultats 2023 :

Nombre de caractères	Minuscules + majuscules	Minuscules + majuscules + chiffres	Minuscules + majuscules + chiffres + symboles
6	Instantané	Instantané	Instantané
8	28 secondes	2 minutes	5 minutes
10	21 heures	5 jours	2 semaines
12	6 ans	53 ans	226 ans
16	46 mio. années	779 mio. années	5 mia. années

Retrouvez toutes les infromations de cette étude sur le site www.hivesystems.io/password

On peut noter que les résultats de plusieurs semaines, années voir centaines d'années sont quand même catégorisés en orange et en jaune. Cela peut paraître exagéré, mais il faut prendre en compte, au delà du temps nécessaire en 2023, la cadence rapide avec laquelle ce temps baisse chaque année.

Par exemple en 2020, pour un mot de passe de 10 caractères (maj. + min. + chiffres + symboles), il fallait environ 5 ans contre seulement 2 semaines en 2023.

Les gestionnaires de mot de passe

Un gestionnaire de mots de passe est un outil qui permet de stocker et de gérer ses mots de passe de manière simple et efficace. Cela se présente généralement sous la forme d'un plugin dans le navigateur et/ou d'une application sur smartphone.

Cet outil va permettre de stocker des mots de passe très forts générés de manière aléatoire pour chaque site ou application souhaités.

Les gestionnaires de mots de passe aident à réduire la tentation de réutiliser plusieurs fois des mots de passe ou de les écrire sur des post-it cachés dans le bureau.

Il existe un grand nombre de gestionnaires sur le marché. Certains sont gratuits, d'autres payants. Certains sont adaptés aux entreprises ou encore sont hébergeables sur ses propres installations.

Il convient ici d'analyser les différentes solutions pour trouver la plus adaptée à son usage. Il est aussi important de se renseigner sur les garanties de sécurité fournies par les éditeurs.

Finalement, il est aussi intéressant de favoriser des acteurs suisses ou européens soumis à des législations strictes.

Les mises à jour

Cela peut paraître un brin évident, mais les mises à jour ne servent pas qu'à faire perdre du temps et ajouter de nouvelles fonctionnalités. Les mises à jour servent la plupart du temps à corriger ou à « patcher » des vulnérabilités.

Il est fréquent que des failles de sécurité des logiciels et des systèmes soient publiées sur le dark web.

Ainsi, il s'agit en quelque sorte d'une course contre la montre pour combler ces failles avant qu'une attaque n'ait lieu.

Il est donc essentiel de ne pas négliger ce point et de maintenir ses systèmes et ses logiciels à jour. Une simple petite porte dérobée ouverte sur un logiciel inoffensif peut conduire une entreprise entière à la catastrophe.

En mai 2017, le ransomware «WannaCry» a infecté des centaines de milliers d'ordinateurs dans plus de 150 pays. Cette attaque a exploité une vulnérabilité du système d'exploitation Windows.

La vulnérabilité avait été corrigée par Microsoft environ deux mois avant l'attaque WannaCry. Cependant, de nombreux systèmes n'avaient pas appliqué la mise à jour de sécurité, ce qui les a rendus vulnérables au ransomware.

Le National Health Service du Royaume-Uni a été l'une des victimes les plus touchées. Plus de 80 hôpitaux et autres installations médicales ont été affectés, entraînant l'annulation de milliers de rendez-vous et d'opérations, et mettant notamment en danger la vie des patients.

Les sites non sécurisés

Le petit cadenas situé à côté de la barre d'adresse du navigateur peut sembler bien anodin et pourtant, il vous précise si la liaison au site que vous visitez est sécurisée ou non.

La technologie utilisée dans ce cas permet de chiffrer la communication entre le site (respectivement son serveur) et votre ordinateur.
Ainsi, si un individu malveillant intercepte la communication (attaque « Man in the Middle ») il ne pourra pas lire directement les informations qui passent.

Il est donc important d'éviter de naviguer sur des sites non sécurisés et ce, surtout si cela concerne des achats ou pour y traiter des données confidentielles.

Le partage sécurisé de gros fichiers

Il est parfois nécessaire de transmettre à une autre personne des données trop lourdes pour être transmises par email (bien que l'email ne soit pas forcément une solution sécurisée même pour les données moins lourdes).

Dans ce cas et si l'entreprise ne fournit pas de solution spécifique pour le partage, de nombreux outils en ligne existent à cet effet. Toutefois, attention ! Il convient de vérifier attentivement les mesures de sécurité et de protection des données qu'offre le site en question.

Nous nous permettons ici de vous recommander l'outil SwissTransfer de la société suisse Infomaniak. Cet outil entièrement gratuit est très sécurisé et garanti que les données sont stockées uniquement en Suisse durant, au maximum, 30 jours. Il permet de partager des fichiers jusqu'à un poids total de 50Go.

infomaniak
SwissTransfer

Les clés USB

Bien que très pratiques et couramment utilisées de nos jours, les clés USB représentent néanmoins une des plus grosses sources de vols/pertes de données dans le monde !

Ce support de stockage ne doit pas, dans la mesure du possible, servir à partager ou à stocker des données importantes ou sensibles. Il conviendrait idéalement de chiffrer les données présentes sur la clé USB et de la formater complètement (pas de formatage rapide) lorsque les données ne sont plus utilisées.

Par ailleurs, si vous veniez à trouver une clé USB dont vous ne connaissez pas l'origine, veillez à ne jamais la connecter à votre ordinateur ! Elle pourrait contenir un virus qui s'exécuterait automatiquement dès que la clé serait insérée dans l'appareil.

De nombreuses entreprises ont déjà été victimes d'attaque par ransomware suite à la connexion d'une clé USB trouvée sur le parking. La vigilance est donc de mise.

Les réseaux publics et endroits publics

Dans la mesure du possible, évitez de travailler sur des données importantes ou sensibles lorsque vous êtes connecté à un réseau public. L'utilisation d'un VPN peut toutefois être un bon moyen de protection lorsqu'il est nécessaire de travailler sur un réseau public.

Dans le même ordre d'idées, méfiez-vous des gens qui vous entourent et qui pourraient avoir accès à des informations en posant les yeux sur votre écran par-dessus votre épaule.

Ce type de vol de données est trop souvent négligé et peut pourtant avoir de lourdes conséquences ! Utilisez par exemple, un filtre de confidentialité sur votre écran lors de vos déplacements.

Le phishing

Le phishing ou hameçonnage est une technique malveillante particulièrement répandue de nos jours et qui ne cesse de s'améliorer pour ressembler toujours plus à des communications originales.

Il s'agit de tentatives visant à obtenir des informations importantes ou sensibles en se faisant passer pour une source fiable.

Il est donc essentiel d'être particulièrement attentif aux emails que vous recevez. Même s'ils semblent provenir d'une personne de confiance.

Voici quelques points importants à vérifier :

- Soyez attentif aux détails : vérifiez l'adresse email de l'expéditeur et les liens contenus dans l'email.
- Faites attention aux fautes d'orthographe : les tentatives de phishing contiennent souvent des fautes.
- Méfiez-vous des messages qui exigent des actions urgentes : les cybercriminels utilisent fréquemment la peur et le sentiment d'urgence pour inciter les gens à agir sans réfléchir.
- Ne partagez jamais vos informations sensibles par e-mail : un interlocuteur sérieux ne vous demandera jamais de communiquer ces données par ce biais.
- En cas de doute : contactez directement l'entreprise ou la personne concernée pour vérifier l'authenticité de l'email.

Il est à noter que ces tentatives peuvent aussi avoir lieu par d'autres canaux comme le téléphone ou le répondeur. Il convient d'être particulièrement prudent et de s'habituer à effectuer ces brefs contrôles pour se protéger et pour protéger son entreprise.

Signaler les incidents

Un point clé dans la culture de sécurité est le signalement des incidents ou des suspicions de violation. Cela revêt une importance capitale puisque cela permet de prendre des mesures rapidement et de manière efficace.

Un collaborateur ne devrait jamais craindre de signaler un incident même s'il en est la cause.

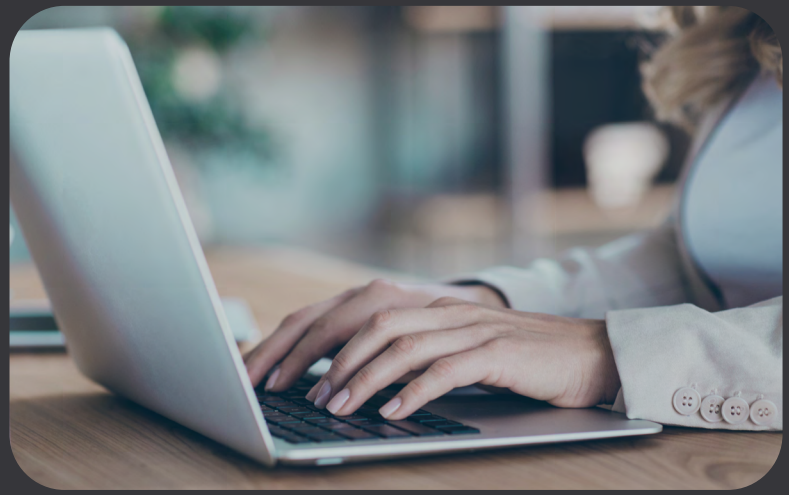
Il s'agit ici d'un aspect important de la culture de sécurité de l'entreprise et du devoir du collaborateur. Il faut garder à l'esprit que les conséquences ne seront certainement pas les mêmes si le collaborateur signale une faute de sa part plutôt que de découvrir plus tard qu'il est la cause de l'incident qu'il l'a sciemment caché.

La responsabilité de l'entreprise

Du point de vue de l'entreprise, les défis sont nombreux et les enjeux sont énormes. Des mesures doivent être prises afin d'en limiter les risques mais aussi d'être préparé en cas d'incident afin de limiter l'impact sur l'activité, et donc, sur les revenus.

L'entreprise a un rôle crucial à jouer dans la promotion et la mise en œuvre de la sécurité de l'information. Il est de sa responsabilité de créer et de maintenir un environnement sûr pour ses collaborateurs, ses clients et ses partenaires.

Les quelques mesures ci-après peuvent représenter un bon point de départ.



La politique de sécurité

L'élaboration d'une politique de sécurité claire et cohérente sert de point de départ pour l'entreprise. Elle permet de définir les mesures à prendre et les règles à respecter en tenant compte du contexte dans lequel l'organisation évolue.

Il peut être utile de commencer par mener une analyse des risques afin d'en déduire les menaces les plus importantes et de prioriser les actions à mener.

La politique peut contenir, par exemple, les éléments suivants :

- Objectif et portée de la politique
- Responsabilités de chacun
- Classification des données
- Contrôles d'accès
- Aspects de la sécurité physique
- Gestion et réponses aux incidents
- Sensibilisation et formation des collaborateurs

Le plan de réponse

Une bonne approche consiste à réaliser un plan de réponse en cas d'incident de manière à ce que chacun sache ce qu'il doit et ne doit pas faire s'il se retrouve confronté à une violation de données.

L'analyse des risques permet ici de structurer le plan de réponse.

La formation des collaborateurs

La sensibilisation et la formation des collaborateurs sont des mesures centrales en matière de sécurité de l'information.

Comme écrit précédemment, les collaborateurs représentent le premier rempart de protection.

Néanmoins, s'ils ne sont pas correctement formés et sensibilisés à ces questions, ils peuvent représenter un risque important qu'il ne faut surtout pas négliger.

La formation des collaborateurs devrait également s'appuyer sur la politique de sécurité de l'entreprise afin de s'assurer d'une certaine cohérence.

La détection des incidents

De nombreux outils de détection des incidents existent désormais. Ils sont d'ailleurs de plus en plus faciles à intégrer.

Toutefois, la dernière technologie la plus chère ne représente pas forcément le meilleur choix pour toutes les entreprises. Il convient de se renseigner sur les solutions qui font consensus chez les professionnels de la cybersécurité.

Ces outils permettent de détecter le plus tôt possible les violations ou les tentatives de violations. Ainsi, la réponse appropriée peut être mise en place rapidement et limiter considérablement les risques ou les impacts.

L'analyse des incidents

À la suite d'un incident, il est important d'effectuer une analyse de manière poussée afin d'en tirer des enseignements qui permettront d'améliorer la stratégie de sécurité de l'entreprise.

La politique, le plan de réponse et la formation des collaborateurs devront être mis à jour en conséquence.

Il ne faut pas oublier que les attaques et les autres violations n'arrivent pas qu'aux autres. Toutes les organisations, quelle que soit leur taille ou leur secteur d'activité, vont y être confrontées tôt ou tard.

La révision

La mise en place des éléments cités précédemment représente à l'évidence une bonne approche en matière de sécurité de l'information.

Toutefois, il ne serait pas judicieux de penser que sa simple mise en place suffise à moyen et long terme. Il sera nécessaire de réviser ces éléments de manière régulière afin que l'ensemble reste cohérent et prenne en condisération les menaces et les défis de demain.

Une fréquence de révision annuelle semble appropriée pour la plupart des PME.

En conclusion

Pour conclure, il apparaît évident que la sécurité de l'information est un enjeu crucial pour les entreprises et les collaborateurs à l'ère du numérique. Les menaces et les risques sont en constante évolution, et il est essentiel de mettre en place des politiques et des pratiques solides pour protéger les données.

Ce guide a pour but d'aider l'entreprise et les collaborateurs à comprendre les différents aspects de la sécurité de l'information ainsi qu'à mettre en œuvre les bonnes pratiques pour renforcer la sécurité.

N'oubliez pas que la responsabilité de la sécurité de l'information incombe à tous les membres de l'organisation, des dirigeants aux employés en passant par les partenaires commerciaux. En instaurant une culture de sécurité et en encourageant le partage des bonnes pratiques, vous pouvez créer un environnement où la sécurité est l'affaire de tous.

Nous espérons que ce guide vous a fourni des informations utiles et des conseils pratiques pour améliorer la sécurité dans votre entreprise. En fin de compte, une organisation bien protégée est une organisation mieux préparée à relever les défis et à prospérer dans le monde digital d'aujourd'hui et de demain.

«La sécurité ne dépend pas des systèmes, elle dépend des personnes.»

Steve Gibson

À
propos

YB Conseils & Solutions Sàrl est une entreprise fribourgeoise spécialisée dans le conseil, l'accompagnement et la formation des entreprises et des institutions publiques dans les domaines de la digitalisation des processus, de la sécurité de l'information et de la protection des données.

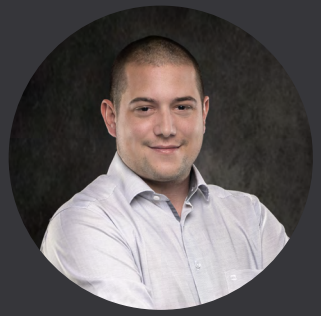
Notre approche se veut globale et innovante. Elle repose sur trois piliers essentiels : les aspects organisationnels, technologiques et juridiques. Nous sommes convaincus que cette approche intégrée est déterminante pour répondre aux défis complexes auxquels les organisations sont confrontées aujourd'hui et le seront demain en matière de sécurité de l'information et de protection des données.

En collaborant avec YB Conseils & Solutions Sàrl, vous bénéficierez de notre expertise, de notre engagement à fournir des services de qualité, de notre approche centrée sur le client et de notre détermination à vous aider à atteindre vos objectifs en matière de digitalisation.

Ensemble, construisons un environnement numérique plus sûr et résilient pour votre organisation.

YB Conseils & Solutions Sàrl

Chemin des Pruniers 39, 1630 Bulle
+41 79 275 37 01 | info@yb-cs.ch | www.yb-cs.ch



Yvann Barras
Directeur et consultant

Spécialiste certifié de la protection des données et du management de la sécurité de l'information (ISO 27001)

+41 79 275 37 01
yvann@yb-cs.ch

Nos formations

Nous proposons des formations de qualité en matière de sécurité de l'information et de protection des données adaptées aux besoins spécifiques des collaborateurs et des entreprises.

- En entreprise pour une expérience personnalisée et adaptée à votre contexte professionnel et à vos collaborateurs
- En classe en collaboration avec la SEC Formation Fribourg pour celles et ceux qui préfèrent un environnement d'apprentissage plus traditionnel et interactif favorisant l'échange entre les participants. Ces formations sont aussi ouvertes aux personnes intéressées à titre individuel.

YB Conseils & Solutions Sàrl
Chemin des Pruniers 39
1630 Bulle

+41 79 275 37 01
info@yb-cs.ch | www.yb-cs.ch

YBCS

SEC Formation Fribourg
Varis 1, case postale 521
1701 Fribourg

+41 26 321 29 21
info@secfribourg.ch | www.secfribourg.ch

société des employés de commerce
formation. fribourg.