Romain Ranson

Cybersécurité des TPE/PME en 10 étapes clés

DUNOD

Illustration de couverture : © delikanlioguz – Shutterstock

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-089048-4

TABLE DES MATIÈRES

AVANT-PROPOS

Je me suis attelé à la rédaction de ce guide juste avant les Jeux olympiques de Paris 2024.

À cette époque, le risque d'attaques informatiques était extrêmement important du fait de cet événement. Et j'ai toujours été frappé par la différence de traitement entre les risques physiques et les risques cyber. En général, les lois, les réglementations ou les premiers réflexes des entreprises se concentrent sur le monde palpable. Mais concernant le risque cyber, c'est seulement à l'occasion d'un tel événement ou d'un incident qu'ils sont réellement pris en compte.

Alors bien sûr, les risques physiques sont essentiels, d'ailleurs nos services numériques ne sont pas totalement dématérialisés, ils tournent sur des machines plus ou moins proches de l'utilisateur. Et sans protection physique, les protections logiques ne valent rien : si vous protégez vos serveurs de toute attaque informatique mais que vous laissez la clé sur la porte, ça ne servira à rien.

Mais pourquoi donc les États délaissent-ils autant les risques cyber ? Ils condamnent les attaques bien sûr, mais finalement laissent les entreprises se débrouiller avec alors que, dans le monde physique, ils prennent en charge la protection, la sécurité, la justice, etc.

Il me semble qu'il y a plusieurs explications possibles, voire à combiner :

- ✓ Certains États sont conscients de la privation de liberté individuelle que cela pourrait engendrer et d'autres pas du tout. Le concept de liberté se concrétise de manières différentes selon les États et les gouvernements, la philosophie politique à l'œuvre dicte le niveau d'interventionnisme.
- ✓ Certains États mènent ou financent des guerres sur Internet pour des questions d'intelligence économique ou d'avantages stratégiques. Si je veux utiliser des moyens informatiques pour mener une guerre économique, j'ai intérêt à ce qu'il y ait des failles dans les systèmes pour les exploiter.
- ✓ Enfin certains États utilisent les systèmes d'information interconnectés sur Internet pour faire de la surveillance de masse, avec en tête, il faut le reconnaître, un véritable enjeu de protection des citoyens face à la menace terroriste.

Bref, certains États sont satisfaits de cette situation un peu floue, même si cela doit nuire à quelques individus ou entreprises : ce n'est pas si grave tant que le système fonctionne au global et que les risques matériels sont mieux contrôlés.

La conclusion qui s'impose : les entreprises sont seules face à leurs risques cyber, elles doivent agir pour se protéger et investir en continu pour maintenir un niveau de protection adéquat avec le temps.

Voire, elles doivent agir aussi pour répondre à certaines réglementations, en particulier en Europe, qui protègent les consommateurs et utilisateurs de services numériques. En cas de vol de données personnelles de citoyens de l'Union européenne, non seulement elles feront face à la colère de leurs clients, à une perte de chiffre d'affaires, mais encore à une amende voire à une condamnation pénale assortie d'une peine de prison.

Or bien souvent, elles sont tout aussi victimes que leurs clients.

Les entreprises de toute taille se doivent donc d'anticiper et de sécuriser leurs systèmes d'information en fonction des risques.

Lors des Jeux olympiques de Paris 2024, de très nombreuses entreprises ont été sollicitées pour contribuer à leur réussite. Et c'est particulièrement vrai des PME.

Pour l'année 2021, l'Insee[1] recensait 158 600 PME sur le territoire français, qui représentaient 29 % des salariés français, soit légèrement plus que les grandes entreprises.

Presque un tiers des travailleurs en France sont employés dans une PME, c'est un secteur clé de l'économie qui contribue directement au fonctionnement des institutions, des territoires et des grandes entreprises.

Ce guide a donc pour vocation à aider les dirigeants de PME et leurs équipes informatiques à identifier les points importants à protéger et à leur montrer comment le faire.

J'ai écrit ce guide en côtoyant d'autres entrepreneurs, en échangeant ou en accompagnant des PME dans leur sécurité informatique. Il se veut pragmatique et concret. Je devrai toutefois aborder quelques notions théoriques de temps en temps.

Mon souhait est que vous y trouviez des solutions qui correspondent à votre contexte et à votre situation. Ce ne sera pas toujours pertinent car bien sûr chaque entreprise est unique et une solution qui fonctionne pour l'une ne sera peut-être pas adaptée à sa voisine.

Pour exploiter au mieux les conseils de ce livre, prenez une feuille et un stylo et notez au fur et à mesure les points que vous souhaitez mettre en œuvre dans votre entreprise avec le numéro de page. C'est simple, rapide et vous serez efficace lors de la mise en œuvre de ces mesures.

Note pour les experts en cybersécurité

Je tiens à indiquer clairement ici que les différents aspects qui sont abordés dans ce livre sont parfois sujets à des raccourcis, à des simplifications voire à de petits arrangements personnels avec la complexité réelle de la cybersécurité. L'objectif de ce livre est de proposer la vulgarisation des notions et principes mais aussi des solutions pragmatiques et concrètes pour les chefs d'entreprise, et non pas de décliner tous les détails réservés à des experts avertis.

1. « L'appareil productif français en 2021 » – Les entreprises en France | Insee : https://www.insee.fr/fr/statistiques/7678592?sommaire=7681078#onglet-2

Introduction : Quel est le risque cyber pour les TPE/PME ?

Ce guide est par la force des choses relativement générique. Chaque entreprise étant différente et disposant d'un système d'information spécifique, il est nécessaire de l'analyser voire de l'auditer pour déterminer les bonnes mesures à prendre.

Néanmoins, il y a tout de même des points communs entre les entreprises qui peuvent être identifiés. Ils sont issus de l'analyse des attaques récentes.

D'ailleurs, si vous ne l'avez pas encore fait, la lecture du guide très intéressant de CyberMalveillance.gouv.fr sur le sujet est fortement recommandée : « La cybersécurité pour les TPE/PME – enjeux et solutions »[1].

1. LES RISQUES AUXQUELS VOTRE ENTREPRISE EST EXPOSÉE

Toute utilisation d'un système informatique, comme regarder une série Netflix sur une TV connectée, présente des risques. En particulier dans le monde professionnel, ces risques sont accrus par la variété des systèmes mis en œuvre, par l'usage intensif qui en est fait mais surtout par l'importance de ces systèmes pour le fonctionnement de l'entreprise.

Avant de les parcourir, voici la légende des pictogrammes utilisés pour illustrer les risques :


Personne ayant une intention négative ou malhonnête envers votre entreprise


Risque financier


Personne n'ayant aucune mauvaise intention et agissant de bonne foi


Attaque directe sur un ou plusieurs éléments du système d'information

1. « La cybersécurité pour les TPE/PME – enjeux et solutions » : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-tpe-pme-enjeux-solutions


Communication et diffusion d'informations


Mail


Bug ou problème dans un logiciel ou matériel

Voici donc, un par un, les principaux risques qui touchent les PME :

Fraude

Acte malhonnête commis dans l'intention de tromper en contrevenant à la loi ou aux règlements. Ce type de risque peut être interne ou externe.

Les fraudes externes sont abordées plus bas.

Surtout ne négligez pas le risque interne : les relations compliquées avec certains collaborateurs, et même ceux qui sont partis de l'entreprise, peuvent constituer un risque.

Vol de compte et mot de passe

L'accès aux informations de login et mot de passe permet à un attaquant de se connecter avec vos comptes à vos services numériques et ainsi de réaliser les actions qu'il souhaite.

Pour y parvenir, les principales modalités sont le phishing ou l'ingénierie sociale, mais d'autres techniques existent.

Vol de données

Nous parlons ici d'intelligence économique ou tout simplement de tentative d'escroquerie grâce à ces données, pas nécessairement envers l'entreprise mais potentiellement aussi envers ses clients.

Le phishing et l'ingénierie sociale sont de nouveau les principaux vecteurs mais l'exploitation de failles dans les logiciels peut également être utilisée.

Perte de données

La perte de données n'est pas nécessairement le fait d'une attaque mais le plus souvent celui d'une mauvaise manipulation réalisée sur ces données.

Il peut également s'agir d'une faille dans un logiciel qui est utilisée intentionnellement ou par erreur.

Le facteur humain est donc important pour ce risque.

Perte du système d'information

Lorsque tout le système d'information de l'entreprise n'est plus opérationnel, il s'agit souvent de l'accumulation de plusieurs facteurs : défaillance de l'hébergeur y compris s'il s'agit du cloud, bug dans des logiciels, erreur humaine, perte de connexion réseau, etc.

On peut penser à la coupure d'une fibre optique du fait de travaux sur la voirie par exemple.

Blocage du système d'information

Ce type d'attaque vise à rendre inopérant une application ou un système d'information complet pour vous empêcher de travailler dans de bonnes conditions. Il s'agit d'attaques appelées déni de service.

Nous trouvons aussi dans cette catégorie le rançongiciel, qui vise à verrouiller tout ou partie du système d'information et ses données dans le but d'obtenir de l'argent pour le déverrouiller.

Vous n'êtes pas non plus à l'abri d'une panne ou d'une coupure de courant ou d'un autre événement qui bloquerait votre informatique.

Vol

L'objectif premier des organisations cybercriminelles qui utilisent toutes ces techniques est de vous extorquer de l'argent.

Souvent les moyens les plus simples sont les plus efficaces : le phishing et l'ingénierie sociale permettent de collecter des informations précieuses soit pour vous contacter et vous faire agir, soit pour agir en votre nom auprès d'une banque par exemple.

Exposition de données clients

En lien avec le vol de données, ce type de risque est dramatique pour l'image de l'entreprise et peut affecter fortement votre chiffre d'affaires.

Désinformation sur l'entreprise, son activité, ses dirigeants ou ses collaborateurs

Des campagnes de dénigrement peuvent aussi être menées contre votre entreprise sur les réseaux sociaux, directement auprès de vos clients ou de partenaires.

Les partenaires sociaux peuvent d'ailleurs aussi être concernés.

Il s'agit la plupart du temps d'un acte de vengeance venant d'un concurrent jaloux, d'un client particulièrement insatisfait ou d'un ancien collaborateur.

Modification de votre site web institutionnel

Ce type de risque est moins prégnant, néanmoins une organisation pourrait s'emparer de votre site web pour le changer totalement.

Cela est souvent le fait d'activistes qui sont convaincus que votre entreprise est néfaste pour leur cause.

À tort ou à raison, ils agissent en passant des messages négatifs, affichant des faits plus ou moins véridiques directement sur votre site web.

Le graphique ci-dessous tente une représentation de ces risques en fonction de leur probabilité et de leur gravité. Notez que chaque entreprise étant unique, ces deux facteurs sont à apprécier localement en fonction de nombreux aspects que nous parcourrons lors de l'étape 1.

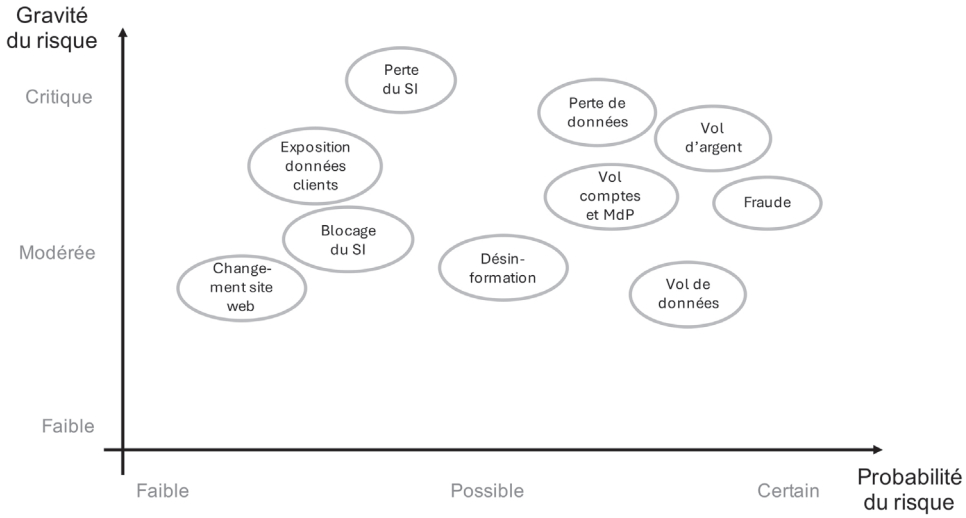

Figure I.1 – Échelle des risques