Introduction

Votre smartphone connaît vos habitudes, vos déplacements, vos contacts, vos secrets bancaires. Il en sait probablement plus sur vous que votre conjoint.

Il en va de même pour la grande majorité des GAFAM. Chaque mouvement que vous faites, chaque décision que vous prenez et même vos propres réflexions peuvent être transformés en informations utilisables.

Peut-on échapper à cette collecte de données ? En théorie, oui. En pratique, c'est quasi impossible, à moins de devenir un « fantôme numérique ». Cela supposerait de vivre sans ordinateur, sans smartphone, sans connexion internet et sans identité numérique. Autrement dit, il faudrait vivre en marge de notre société, car le monde dans lequel nous évoluons repose irrémédiablement sur le numérique. Or, ces données qui alimentent notre économie sont par nature fragiles. Rien n'est plus fugace et volatile que l'information numérique. Pourtant, ces mêmes données constituent le pilier de notre économie moderne : aujourd'hui, toute activité, de la banque au commerce, de la santé à l'industrie, passe par leur traitement et leur exploitation.

Bienvenue dans l'ère numérique, où la cybersécurité n'est plus une option pour les dirigeants, mais une nécessité vitale. Car vous devez reconnaître que votre entreprise possède un actif inestimable, qui n'est pas ses locaux, ses machines, ni même ses employés, mais vos données. Votre système d'information constitue le sang de votre organisation, et toute hémorragie ou tout empoisonnement peut s'avérer fatal. Et ce paradoxe est d'autant plus fort que ce qui menace le plus votre entreprise est précisément ce que vous ne pouvez pas toucher ou voir. Cette nature immatérielle rend le sujet difficile à comprendre, et le défi qu'est la cybersécurité devient un vrai challenge.

D'où ces questions qui hantent chaque dirigeant ou dirigeante lucide : comment protéger mon organisation sans la paralyser ? Que dois-je vraiment savoir ? Que dois-je vraiment faire ?

Ce livre a été écrit pour répondre à ces questions spécifiques. Mais il ne s'agit pas d'un manuel rempli d'acronymes destiné aux experts en informatique, ni d'une explication complexe de la réglementation qui vous ferait abandonner avant la page 10. D'ailleurs, le sujet des réglementations spécifiques à chaque activité régulée ne sera que très peu abordé dans ce livre. Ce n'est pas non plus une collection de recettes miraculeuses à appliquer sans réfléchir. L'ambition ici est simple et pragmatique : vous faire comprendre pourquoi la cybersécurité mérite votre attention, et surtout comment vous pouvez réellement gérer ce problème. Sans jargon. Sans ménagement. Avec du « bon sens paysan ».

Écartons d'emblée une idée répandue : la cybersécurité n'est pas un domaine réservé à une obscure élite mystérieuse de spécialistes qui suscitent des craintes de catastrophes, à la manière du personnage d'Hergé Philippulus qui annonce constamment la fin du monde. Et bien qu'elle soit numérique, c'est tout de même la fin du monde. En réalité, la cybersécurité est accessible à tout le monde. Pourquoi ? Parce que ses fondements existent depuis des siècles. Protéger un château médiéval ou sécuriser un système informatique moderne revient au même : évaluer les risques, restreindre l'accès, détecter les intrusions, limiter les dommages en cas d'attaque. Ce que Vauban a fait en son temps, c'est ce que le marketing d'aujourd'hui appelle la « défense en profondeur ». C'est le même concept, mais avec plusieurs siècles de décalage.

La différence fondamentale tient à la nature de l'espace que nous défendons. L'univers numérique est infiniment plus malléable, plus instantané et plus interconnecté que le monde physique. Mais le problème de sécurité, lui, reste le même dans son essence. C'est cette continuité que nous explorerons ensemble, en partant de ce que vous connaissez déjà pour aborder ce qui vous semble encore obscur.

Ce livre propose une méthode simple pour vous aider à comprendre la cybersécurité de manière concrète et opérable, sur base d'une structure organisationnelle largement répandue. Non, vous n'avez pas besoin de devenir un expert technique. Oui, vous avez besoin de maîtriser les principes fondamentaux pour prendre les bonnes décisions stratégiques. En tant que leader, votre tâche n'est pas de configurer un coupe-feu. Vous devez

comprendre les enjeux, attribuer les ressources, effectuer les arbitrages et promouvoir une vision sécuritaire au sein de votre organisation.

Ce voyage se déploiera en trois temps. Nous commencerons par explorer les fondamentaux de la cybersécurité : qu'est-ce qu'une faille ? Quelles sont les grandes familles de vulnérabilités qui menacent votre organisation ?

Une fois ces bases posées, nous passerons à l'action concrète, la méthodologie. Parce que comprendre ne suffit pas : il faut agir. Nous étudierons les mesures de sécurité nécessaires pour assurer la protection optimale de votre entreprise. Nous verrons comment passer de la théorie à la pratique applicable et comment bâtir une défense solide contre les menaces concrètes.

Enfin, nous aborderons la dimension stratégique. Comment piloter efficacement la cybersécurité de votre organisation ? Comment intégrer les contrôles intelligemment sans qu'ils deviennent un carcan ? Comment construire une stratégie de défense cohérente et maîtriser les risques sans devenir paranoïaque ?

Car la sécurité n'existe pas dans le vide : elle doit s'inscrire dans un cadre organisationnel : la gouvernance.

Il est maintenant temps de tourner la page et d'aborder la cybersécurité ensemble. Nous allons transformer ce qui peut sembler technique et complexe en une question stratégique claire. Vous verrez, ce qui vous semblait mystérieux deviendra évident. Ce qui vous semblait inaccessible deviendra réalisable. Bienvenue dans le monde fascinant de la cybersécurité pour dirigeants éclairés.

Chapitre 1

Les principes

Le premier piratage de l'histoire

Imaginez la France de 1834. Pas d'ordinateurs, pas d'Internet, pas même d'électricité dans les foyers. Pourtant, l'État français dispose déjà d'un réseau de communication révolutionnaire : le télégraphe optique Chappe. Un système de tours dispersé sur tout le territoire, capable de transmettre un message sur plusieurs centaines de kilomètres en quelques heures seulement. Le principe ? Un opérateur utilise des signaux optiques pour transmettre un message à son collègue de la tour suivante, qui l'observe à la longue-vue avant de le retransmettre à son tour. Archaïque, peu fiable par mauvais temps, mais diablement efficace pour l'époque. Un véritable ancêtre de nos réseaux modernes.

Cette infrastructure, réservée exclusivement à l'État, attise naturellement les convoitises. Et c'est là que notre histoire commence. Deux frères, François et Louis Blanc, spéculateurs à la Bourse de Bordeaux, comprennent

avant tout le monde une vérité encore valable aujourd'hui : celui qui obtient l'information avant les autres détient un avantage décisif.

Les cours de la Bourse parisienne mettent plusieurs jours à atteindre Bordeaux par les moyens conventionnels. Mais avec le télégraphe Chappe, quelques heures suffiraient. Le problème est que le réseau est interdit au public.

Les frères Blanc ne se laissent pas décourager. Ils observent, analysent, cherchent et trouvent la faille.

Le détournement fonctionne à la perfection pendant deux longues années. Les frères Blanc accumulent des profits considérables grâce à leur connaissance anticipée des cours boursiers. Leurs succès répétés éveillent les soupçons, certes, mais rien de concret. Le système est trop ingénieux, trop bien pensé.

Sans le savoir, les frères Blanc viennent d'inventer le *hacking* moderne. Près de deux siècles avant l'ère informatique, ils ont appliqué exactement la même méthodologie que les pirates informatiques d'aujourd'hui : observer minutieusement un système, en comprendre les vulnérabilités, identifier une procédure légitime détournable, corrompre un élément humain de la chaîne si nécessaire, puis exploiter cette succession de failles[1] pour en tirer profit.

Leur histoire, bien que datant de deux siècles, illustre une vérité fondamentale de la cybersécurité : les principes n'ont pas changé, seuls les outils ont évolué. Le télégraphe Chappe a laissé place à Internet, les tours optiques aux routeurs, les longues-vues aux pare-feux. Mais la logique de l'attaque reste identique. Comprendre cette continuité historique est essentiel pour tout dirigeant : **la cybersécurité ne traite pas de problèmes nouveaux, elle traite de problèmes anciens, mais dans un monde moderne**.

Revenons un instant sur cette attaque des frères Blanc. Elle démontre brillamment l'une des règles essentielles en matière de cybersécurité : l'apparition de toute nouvelle technologie entraîne inévitablement de nouvelles vulnérabilités.

L'innovation est généralement entourée d'un nuage de doutes et d'inconnu. Nous ne maîtrisons jamais immédiatement ce que nous venons de créer. Le télégraphe Chappe en 1837, l'intelligence artificielle aujourd'hui, le principe

1. Dans le jargon cyber, on parle souvent de kill chain*.*

reste le même. Entre le moment où une technologie émerge et celui où nous en comprenons véritablement toutes les implications, il existe une zone grise, un espace de vulnérabilité. Ce processus est intrinsèque : la maîtrise nécessite du temps, de l'expérience et la capacité de rectifier ses idées fausses.

C'est précisément cette faille due au manque de recul que les frères Blanc ont exploitée. En observant attentivement la conception du système télégraphique, ils ont découvert un problème dans sa logique de fonctionnement. Un processus légitime, destiné à corriger des erreurs, a été détourné de son objectif initial. Ils ont compris qu'un mécanisme prévu pour corriger devenait, entre des mains malveillantes, un vecteur pour injecter de l'information clandestine.

Cette approche méthodique résume l'essence même du piratage, hier comme aujourd'hui. Observer. Comprendre. Détourner. Un pirate ne casse pas frontalement un système, il le manipule pour lui faire accomplir ce qu'il souhaite, pour le détourner de sa fonction initiale à son profit. Il peut parfois utiliser la force brute, mais va préférer la subtilité d'une erreur de conception.

Dans le jargon de la cybersécurité actuelle, ce type d'écart est appelé *vulnérabilité* lorsqu'il devient exploitable. Et la raison fondamentale pour laquelle ces failles existent est très simple à comprendre : tous les systèmes d'information, sans exception, sont créés par des humains. Et l'humain est faillible. Toujours.

Voici un constat dur, mais émancipateur pour tout dirigeant : **la sécurité totale est un mythe**[2]. Elle ne peut pas exister. L'erreur humaine est inhérente à tout processus de création. Le développeur qui écrit une ligne de code, l'architecte qui conçoit un réseau et l'administrateur qui configure un serveur peuvent tous commettre une erreur. Une seule suffit parfois. Une virgule mal placée, une vérification oubliée, une procédure mal pensée.

Évidemment, les frères Blanc ne connaissaient rien à l'informatique, parce qu'elle commençait tout juste à exister dans l'esprit de Charles Babbage. Mais ils ont appliqué instinctivement les mêmes tactiques que celles utilisées pour les cyberattaques modernes : identifier la nature du fonctionnement d'un système, repérer où la vulnérabilité a pu se glisser, puis l'exploiter méthodiquement. Le télégraphe optique comptait un processus de

2. Certains diront même que c'est un échec.