La Cybersécurité dans le commerce

Enjeux & bonnes pratiques

Observatoire prospectif du commerce

Avec le développement des plateformes numériques et l'accroissement exponentiel des transactions numériques en ligne et en points de vente, le secteur du commerce s'expose de plus en plus aux dangers que représentent les attaques des cybercriminels comme, par exemple, la défiguration de sites internet. Mettre en place une politique active de cybersécurité revêt donc un enjeu majeur pour les entreprises du secteur.

Etre mieux protégé grâce à la Cybersécurité

Dans ce contexte, des études sur la cybersécurité[1] dans les entreprises du commerce ont été conduites en 2019 visant à :

- **savoir quelles sont les informations qu'il est important de protéger,** ce qui impose une culture de la prévention et de la résilience,
- **sensibiliser/informer ses salariés aux enjeux de la sécurité,** aux règles à respecter et aux bons comportements à adopter en matière de sécurité des systèmes d'information, à travers des actions de sensibilisation et de formation.

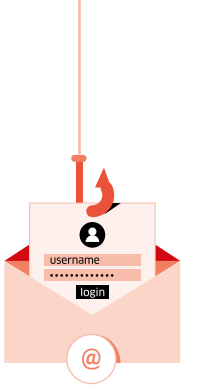
Ces études ont été pilotées par l'Observatoire Prospectif du commerce en partenariat avec l'Etat, dans le cadre d'un EDEC (Engagement de Développement des Emplois et des Compétences).

La branche des Grands Magasins et Magasins Populaires a souhaité mettre à disposition de ses entreprises adhérentes les enseignements de ces études sous la forme de deux supports complémentaires :

- **ce guide** présentant de façon synthétique les principaux enjeux de cybersécurité dans le commerce,
- **une page web dédiée, accessible sur : alliancecommerce.org/nos-publications/**, abordant pour la branche, de façon plus pragmatique, les formations spécifiques et les bonnes pratiques à adopter pour s'adapter aux enjeux de la cybersécurité.

(1) études menées par le Cabinet Lafayette associés de septembre 2018 à janvier 2019.

Commerce et Cybersécurité : les enjeux



QU'EST-CE QUE LA CYBERSÉCURITÉ ?

Il s'agit de l'ensemble des moyens utilisés pour assurer la protection des systèmes d'information (SI) et des données informatiques, au sein d'une entreprise notamment, contre les cybercriminels et leurs cybermenaces.

Les principales cybermenaces

La défiguration de sites internet

Il s'agit de l'altération, par un pirate informatique, de l'apparence d'un site internet - devenant tout noir ou tout blanc ou envahi de messages, d'images, de logos… - le rendant inutilisable, ce qui pour un site marchand peut entraîner des pertes directes de revenus et de productivité.

L'attaque en déni de service

Cette attaque informatique rend inaccessible - temporairement ou pour longtemps - un serveur par saturation (envoi de milliers de requêtes) ou par panne ou dégradation du service (exploitation d'une faille de sécurité). Elle laisse supposer la prise de contrôle du serveur et donc la récupération de données sensibles, pouvant entraîner des pertes directes de revenus et de productivité.

L'hameçonnage

C'est une technique frauduleuse largement employée par les cybercriminels pour récupérer, via de faux messages, des données personnelles (comptes d'accès, mots de passe…) afin de les exploiter. Une version plus sophistiquée, dite « spear fishing » parce qu'elle cible des personnes précises dans l'entreprise, est apparue.

Les rançongiciels

Ce sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels.

Toutes les entreprises, quelle que soit leur taille, sont susceptibles d'être la cible de cybermenaces.

Les risques pour l'entreprise

Ces différentes menaces informatiques font peser **3 grands risques** sur l'entreprise :

1. **Atteintes à la protection des données ou des secrets industriels.**
2. **Perte de chiffres d'affaires.**
3. **Baisse de confiance des clients.**

Les idées reçues sur la cybersécurité

Face à ces risques réels, plusieurs **idées reçues** freinent la mise en place d'une stratégie de cybersécurité :

Idée reçue n°1

La cybersécurité coûte cher

La mise en sécurité des installations informatiques nécessiterait des investissements importants.

Réponse : la 1ère étape d'audit des SI peut avoir un coût élevé mais les mises à jour sont moins onéreuses et l'investissement est vite rentabilisé face aux risques.

Idée reçue n°2

On minimise les risques encourus

A cela s'ajoute un sentiment d'invulnérabilité face aux attaques.

Réponse : il n'existe pas de risque « zéro » et toutes les entreprises sont exposées.

Idée reçue n°3

La sécurité informatique relève uniquement des services techniques

Non : la sécurité informatique concerne toutes les équipes.

Réponse : l'ensemble des collaborateurs, quelle que soit leur fonction, doivent connaître les enjeux de la cybersécurité.

Résultat Les entreprises ne sont pas suffisamment protégées.
Investir dans la cybersécurité permet d'éviter les risques liés aux cybermenaces et peut représenter un avantage concurrentiel important.

De l'importance de **former / sensibiliser** ses salariés

Une démarche managériale

Installation d'antivirus, configuration de serveurs, gardiennage de data centers, etc. : les entreprises du commerce investissent dans des technologies et services de sécurité pour se protéger des cyberattaques.

Toutefois, ce n'est pas suffisant : il est essentiel de sensibiliser et former tous les salariés à la cybersécurité. Ce sont eux la première source de défense de l'entreprise, eux qui peuvent signaler le moindre événement éveillant leurs soupçons.

Former les salariés, quel que soit leur poste, à la cybersécurité est un sujet de gouvernance que doivent s'approprier les managers des entreprises du commerce. Objectif : accompagner les collaborateurs dans leur montée en compétences sur la sécurité numérique.

La cybersécurité est l'affaire de tous : chaque usager peut être le maillon faible de la chaîne de sécurité d'une entreprise.

L'offre de formation cybersécurité à disposition

489

formations identifiées en cybersécurité

105

établissements identifiés (organismes de formation (spécialisés ou généralistes), écoles d'ingénieurs, universités)

80%

des formations à destination des experts IT

50%

des certifications de niveau 7 (Bac + 5)

Cette offre de formation regroupe une majorité de formations courtes. La moitié des formations dispensées sont d'une durée inférieure à 4 jours.

FOCUS GRANDS MAGASINS ET MAGASINS POPULAIRES

Retrouvez un focus sur l'offre de formation accessible aux Grands Magasins et Magasins Populaires sur la page https://alliancecommerce.org/nos-publications/

Commerce et Cybersécurité : Mettre en place les **bonnes pratiques**

La formation n'est pas le seul outil mobilisable par les entreprises du commerce pour informer leurs salariés sur la cybersécurité. Elles peuvent :

- **réaliser des campagnes de sensibilisation** grâce à différents canaux de communication : affiches, vidéos en ligne, mailings…,
- **transmettre les bonnes pratiques** en matière de cybersécurité.

Prévention des cybermenaces

10 BONNES PRATIQUES GÉNÉRIQUES ET SIMPLES À TRANSMETTRE AUX SALARIÉS

Ces bonnes pratiques permettent de diminuer l'exposition aux cybermenaces :

1

Appliquer de manière régulière et systématique les mises à jour de sécurité depuis les sites officiels

2

Utiliser des mots de passe différents et complexes pour chaque site et application

3

Effectuer régulièrement des sauvegardes des données sauf si la procédure a été automatisée

4

Ne jamais communiquer d'informations sensibles par messagerie ou téléphone (données bancaires, mots de passe…)

5

Ne jamais communiquer d'éléments d'accès administrateurs et d'authentification à un tiers non identifié

6

Ne pas ouvrir les courriels, pièces jointes et les liens provenant d'expéditeurs inconnus ou d'un expéditeur connu dont la structure du message est inhabituelle ou vide (message infecté)

7

En cas de lien douteux, positionner le curseur de la souris sur le lien (sans cliquer) : l'adresse vers laquelle pointe le lien s'affiche pour vérification

8

Ne pas échanger de données confidentielles sur des réseaux wi-fi publics ou inconnus

9

Eviter les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons

10

En cas de soupçon de cybermenaces (cf. page 3), contacter son supérieur hiérarchique ou un responsable IT.

FOCUS GRANDS MAGASINS ET MAGASINS POPULAIRES

Retrouvez un focus sur les bonnes pratiques destinées aux salariés des Grands Magasins et Magasins Populaires sur la page https://alliancecommerce.org/nos-publications/

MINISTÈRE
DU TRAVAIL,
DE L'EMPLOI
ET DE L'INSERTION
Liberté
Égalité
Fraternité

Observatoire
prospectif du commerce

Observatoire prospectif du commerce
251, boulevard Pereire - 75852 Paris cedex 17
Tél. : 01 55 37 41 51
E-mail : observatoire@lopcommerce.com - www.lopcommerce.com

CIF COMMUNICATION - 8578 - Illustrations : Stories.Freepik.com/Amico Style - Février 2021.