Naviguer dans le paysage numérique du secteur agroalimentaire

Opportunités et stratégies pour développer et étendre votre entreprise grâce aux technologies modernes

PRÉSENTÉ PAR:
Ines & Eric Batterton de

My NORDIC Garden
Natural & Sustainable Kitchen Gardens

Réseau Agroalimentaire de l'Est ontarien
Eastern Ontario Agri-Food Network

MODULES

1. INTRODUCTION À LA TRANSFORMATION NUMÉRIQUE DANS L'AGROALIMENTAIRE
2. CRÉER UNE PRÉSENCE NUMÉRIQUE
3. COMMERCE ÉLECTRONIQUE ET VENTES EN LIGNE
4. STRATÉGIES DE MARKETING NUMÉRIQUE
5. ANALYSE DE DONNÉES ET PERSPECTIVES
6. TECHNOLOGIE MOBILE ET APPLICATIONS
7. INTERNET DES OBJETS (IOT) EN AGRICULTURE
8. RÉSEAUTAGE ET COLLABORATION EN LIGNE
9. CYBERSÉCURITÉ ET PROTECTION DES DONNÉES
10. TENDANCES FUTURES ET STRATÉGIES D'ADAPTATION

Cybersécurité et protection des données

- Comprendre les concepts clés de la cybersécurité et de la protection des données
- Identifier les menaces et vulnérabilités courantes dans le secteur agroalimentaire
- Mettre en œuvre les meilleures pratiques pour protéger les données et les systèmes
- Reconnaître l'importance de la conformité

1) Introduction à la cybersécurité

Définition

La cybersécurité est la pratique visant à protéger les systèmes informatiques, les réseaux et les données contre les attaques numériques et les accès non autorisés. Elle implique la mise en œuvre de technologies et de politiques pour sécuriser les informations sensibles contre des menaces telles que les logiciels malveillants et le phishing.

Pertinence pour l'agriculture

La cybersécurité est de plus en plus pertinente pour le secteur agroalimentaire en raison de la dépendance croissante à la technologie dans l'agriculture, la transformation des aliments et la gestion de la chaîne d'approvisionnement. À mesure que les exploitations agricoles adoptent des technologies intelligentes, des dispositifs IoT et l'analyse de données, elles deviennent plus vulnérables aux cybermenaces pouvant perturber les opérations, compromettre les données ou entraîner des problèmes de sécurité alimentaire.

2) Menaces et vulnérabilités cyber courantes

Cybermenaces

Malware

Abréviation de « logiciel malveillant ».
Fait référence à tout logiciel conçu pour nuire, exploiter ou compromettre un système informatique, un réseau ou un appareil.

- Virus
- Vers
- Chevaux de Troie
- Rançongiciels
- Logiciels espions

Ce logiciel peut voler des données, perturber les opérations ou obtenir un accès non autorisé aux systèmes.

2) Menaces et vulnérabilités courantes en cybersécurité

Cybermenaces

Hameçonnage

Le phishing est une technique de cyberattaque qui consiste à tromper les individus pour qu'ils fournissent des informations sensibles, telles que des mots de passe ou des numéros de carte de crédit.
Cela se produit souvent via des courriels, des messages ou des sites web trompeurs semblant légitimes.

- **Hameçonnage par courriel :** l'attaquant envoie un courriel semblant provenir d'une source légitime (banque, service populaire), incitant le destinataire à cliquer sur un lien et à saisir des informations personnelles sur un faux site web.
- **Hameçonnage ciblé (spear phishing) :** attaque ciblée dans laquelle l'escroc personnalise le message pour une personne ou une organisation précise, en utilisant souvent des informations professionnelles afin de le rendre plus crédible.

2) Menaces et vulnérabilités cyber courantes

Cybermenaces

Hameçonnage

- **Smishing :** attaque menée par SMS dans laquelle l'expéditeur trompe le destinataire afin qu'il clique sur un lien ou fournisse des informations personnelles, en prétendant souvent provenir d'une source de confiance.
- **Hameçonnage vocal (vishing) :** appel téléphonique d'une personne se faisant passer pour un représentant d'une organisation, incitant le destinataire à fournir des informations sensibles ou à effectuer un paiement urgent pour résoudre un problème.
- **Hameçonnage par clonage (clone phishing) :** arnaque dans laquelle un courriel légitime que la victime a déjà reçu est reproduit avec des liens ou des pièces jointes malveillants ajoutés, puis envoyé depuis une adresse falsifiée.
- **Hameçonnage sur les réseaux sociaux :** messages ou publications frauduleux sur les plateformes de réseaux sociaux incitant les utilisateurs à cliquer sur des liens ou à fournir des informations personnelles, souvent présentés comme des concours ou des alertes urgentes.

2) Menaces et vulnérabilités courantes en cybersécurité

Cybermenaces

Rançongiciel

Type de logiciel malveillant qui chiffre les fichiers de la victime ou bloque l'accès à son système, exigeant le paiement d'une rançon pour rétablir l'accès. Il se propage souvent via le phishing, les courriels ou des téléchargements malveillants et peut entraîner des pertes de données importantes ainsi que des dommages financiers.

Identification

- Comportement suspect, fichiers devenant soudainement inaccessibles
- Notes de rançon
- Rechercher des messages contextuels inattendus demandant un paiement
- Ralentissement du système

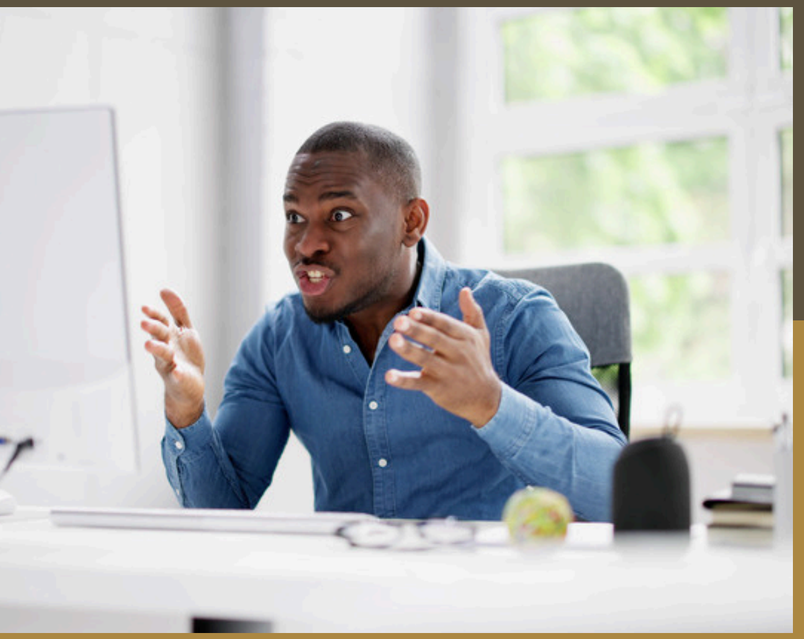
Prévention

- Sauvegardes régulières
- Vigilance face aux courriels
- Logiciels de sécurité
- Mises à jour du système
- Formation des utilisateurs
- Segmentation du réseau

2) Menaces et vulnérabilités courantes en cybersécurité

Cybermenaces

Menaces internes



Fait référence aux risques de sécurité posés par des personnes au sein d'une organisation, telles que les employés, les contractuels ou les partenaires commerciaux, qui ont un accès autorisé aux systèmes et aux données. Ces personnes peuvent provoquer un sabotage intentionnel ou accidentel des opérations.

Les menaces internes peuvent être particulièrement difficiles à détecter et à prévenir en raison du statut de confiance des personnes impliquées.

2) Menaces et vulnérabilités cyber courantes

Vulnérabilités

Points faibles

Identifier les vulnérabilités en cybersécurité et mettre en œuvre des stratégies de prévention est une étape cruciale pour maintenir un environnement sécurisé.

Identification

- Réaliser des audits de sécurité réguliers
- Utiliser des analyseurs de vulnérabilités
- Effectuer des tests d'intrusion
- Vérifier les paramètres de configuration
- Surveiller les journaux et les alertes
- Se tenir informé

Étapes de prévention

- Gestion régulière des correctifs
- Mettre en place des contrôles d'accès stricts, des pare-feu et des systèmes de détection d'intrusion (IDS)
- Mots de passe robustes
- Chiffrement des données
- Sauvegarde des données
- Plan de réponse aux incidents
- Limiter les connexions externes
- Réviser et mettre à jour les politiques de sécurité

3) Meilleures pratiques pour la protection des données

Mots de passe solides

- Mots de passe complexes et uniques

Mises à jour régulières des logiciels

- S'assurer que tous les systèmes et applications sont à jour

Chiffrement des données

- Protéger les données sensibles grâce à des méthodes de chiffrement

Formation des employés

- Former le personnel à reconnaître les menaces et aux bonnes pratiques en ligne

3) Meilleures pratiques pour la protection des données

Antivirus et antimalware

Norton Antivirus, Bitdefender, Kaspersky

Analyse des vulnérabilités

Nessus, OpenVAS, Qualys

Test d'intrusion

Metasploit, Burp Suite, Kali Linux

Informations et événements de sécurité

Splunk, IBM QRadar, LogRhythm

3) Meilleures pratiques pour la protection des données

Pare-feu et sécurité réseau

Palo Alto Networks, Cisco ASA, Fortinet FortiGate

Prévention de la perte de données (DLP)

Symantec DLP, Forcepoint DLP, Digital Guardian

Gestion des identités et des accès (IAM)

Okta, Microsoft Azure Active Directory, Ping Identity

Renseignement sur les menaces

Recorded Future, ThreatConnect, Anomali

Conformité et gestion des risques

RSA Archer, ServiceNow GRC, LogicManager

4) Règlementations sur la protection des données

LPRPDE (Loi sur la protection des renseignements personnels et les documents électroniques)

- Adoptée en 2000, elle s'applique aux organisations du secteur privé à travers le Canada.
- Elle régit la façon dont les organisations recueillent, utilisent et divulguent les renseignements personnels dans le cadre de leurs activités commerciales.

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

5) Construire une culture de cybersécurité

Promotion de Sensibilisation

- Encourager une culture de sécurité au sein de l'organisation

Plans de réponse aux incidents

- Élaborer et communiquer un plan de réponse aux incidents cybernétiques

Amélioration continue

- Revoir et mettre à jour régulièrement les mesures de cybersécurité

6) En conclusion

La cybersécurité et la protection des données sont essentielles pour préserver l'intégrité et la confidentialité des informations dans le secteur agroalimentaire.
En comprenant les menaces, en appliquant les meilleures pratiques et en assurant la conformité, les producteurs agroalimentaires peuvent mieux protéger leurs organisations et renforcer la confiance de leurs parties prenantes.

7) Exercices d’engagement actif

Recherche

Trouver une étude de cas d’un incident de cybersécurité dans le secteur agroalimentaire et l’examiner.
Exemple: https://agriculture.canada.ca/sites/default/files/documents/2024-09/cyber-security-infographic-en.pdf

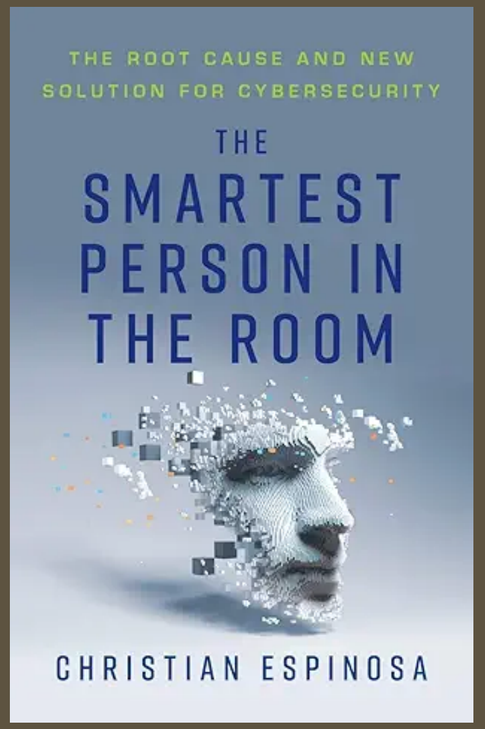
Exercice d’identification des menaces

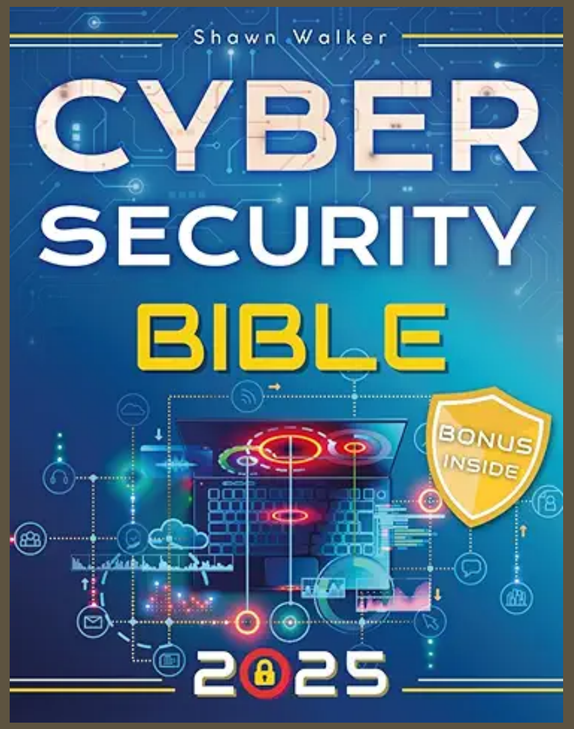
Identifier les menaces potentielles en cybersécurité pertinentes pour votre exploitation (agroalimentaire)

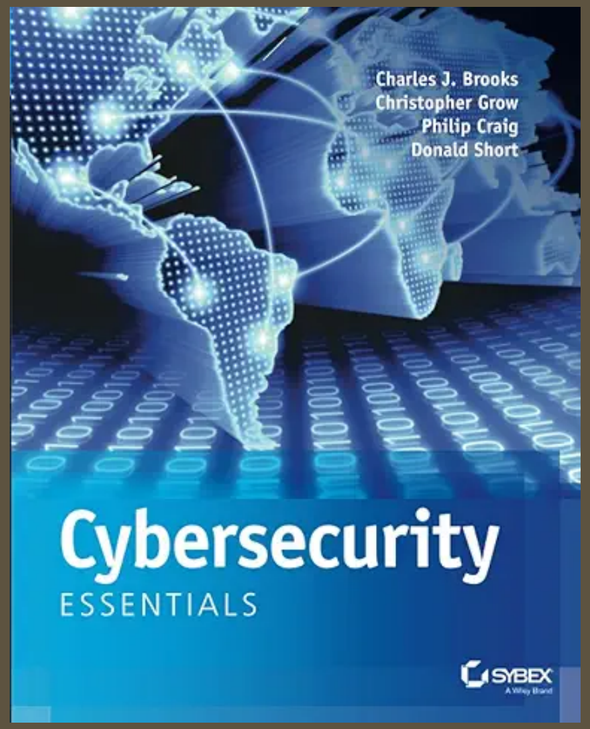
Révision

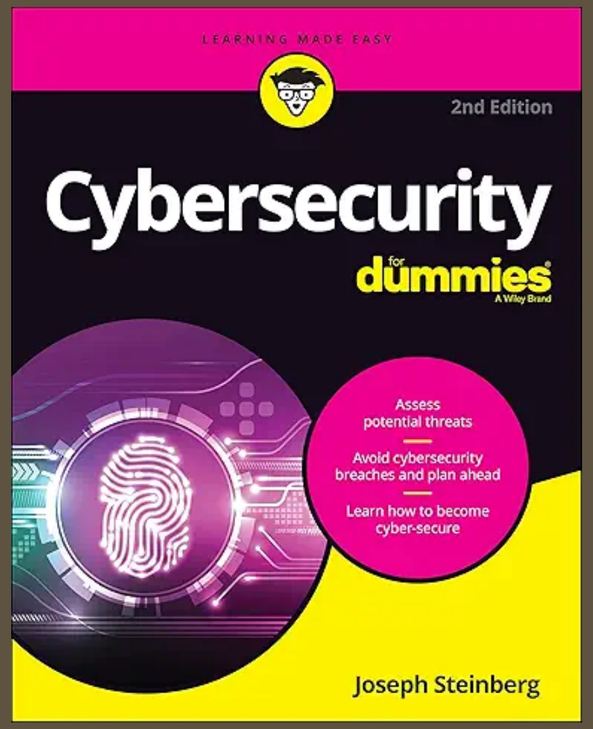
Revue des politiques : examinez les politiques sur votre site web et analysez leur conformité avec les réglementations officielles.

RESSOURCES


THE ROOT CAUSE AND NEW SOLUTION FOR CYBERSECURITY
THE SMARTEST PERSON IN THE ROOM
CHRISTIAN ESPINOSA


Shawn Walker
CYBER SECURITY BIBLE
BONUS INSIDE
2025


Charles J. Brooks
Christopher Grow
Philip Craig
Donald Short
Cybersecurity
ESSENTIALS
SYBEX


LEARNING MADE EASY
2nd Edition
Cybersecurity
for dummies
Assess potential threats
Avoid cybersecurity breaches and plan ahead
Learn how to become cyber-secure
Joseph Steinberg

MERCI

CRÉATEURS DE COURS :
Ines & Eric Batterton de

My NORDIC Garden
Natural & Sustainable Kitchen Gardens

RENDU POSSIBLE GRÂCE AU RÉSEAU AGROALIMENTAIRE DE L'EST ONTARIEN

Réseau Agroalimentaire de l'Est ontarien
Eastern Ontario Agri-Food Network