prodware

Cyber-sensibilisation

Mieux gérer le risque humain dans votre stratégie de **cybersécurité**

L'HUMAIN AU CŒUR DE LA CYBERSÉCURITÉ

Si la transformation digitale a créé de nouvelles opportunités pour les organisations, elle a aussi augmenté leur surface d'exposition aux risques cyber. Demandes de rançon, vol de données et sabotage sont quelques-uns des dangers qui pèsent aujourd'hui sur elles, quels que soient leur taille et leur secteur d'activité. Et ce, dans un paysage marqué par l'intensification et la diversification des attaques informatiques.

Avec des impacts allant bien au-delà de la perte d'exploitation, les conséquences de telles attaques sont parfois dramatiques. Une entreprise familiale peut ainsi se voir placée en redressement judiciaire après avoir été victime d'un rançongiciel. Un incident de sécurité peut engendrer de nombreux coûts directs liés à l'impact sur le business et à la gestion de la crise mais aussi porter durablement atteinte à l'image d'une organisation, voire entraîner des sanctions juridiques.

Si la mutation des modes de travail avait déjà été amorcée, la crise sanitaire, avec la nécessaire mise en œuvre du travail à distance, a créé de nouveaux défis et révélé des faiblesses dans la sécurité de la plupart des organisations. Elle a aussi confirmé que le comportement des collaborateurs, principales cibles des cybercriminels, pouvaient avoir des répercussions importantes sur la sécurité du Système d'Information.

Aujourd'hui plus que jamais, la cybersécurité est un enjeu stratégique pour les organisations. Et même si celles-ci musclent leur défense en protégeant leur réseau, leurs applications et leurs données à l'aide d'outils informatiques sophistiqués, la réponse aux cybermenaces ne peut être uniquement technologique. Une part importante des incidents de sécurité est due à une erreur humaine. Il est donc primordial de sensibiliser tous les collaborateurs à la cybersécurité.

Acteur international de la transformation digitale des entreprises, Prodware a fait de la cyber-sensibilisation une composante essentielle de son accompagnement en cybersécurité. Partenaires de KnowBe4, leader mondial sur le marché de la formation de sensibilisation à la sécurité, Prodware a mis en œuvre une démarche structurée pour aider les organisations à réduire le risque humain dans leur stratégie de cybersécurité.

SOMMAIRE

Partie 1
L'humain, maillon faible de la cybersécurité ? 3

Pourquoi le facteur humain est-il si important ? 4

À quelles menaces les organisations sont-elles confrontées ? 6

Comment minimiser le risque humain ? 7

Partie 2
L'offre Prodware : assurer la sécurité par la sensibilisation 9

Prodware et la cyber-sensibilisation 10

KNOWBE4, la solution de cyber-sensibilisation de référence 12

Prodware et la méthodologie KNOWBE4 13

Quand la cybersécurité devient une opportunité 14

Partie 1

L'HUMAIN, MAILLON FAIBLE DE LA CYBERSÉCURITÉ ?

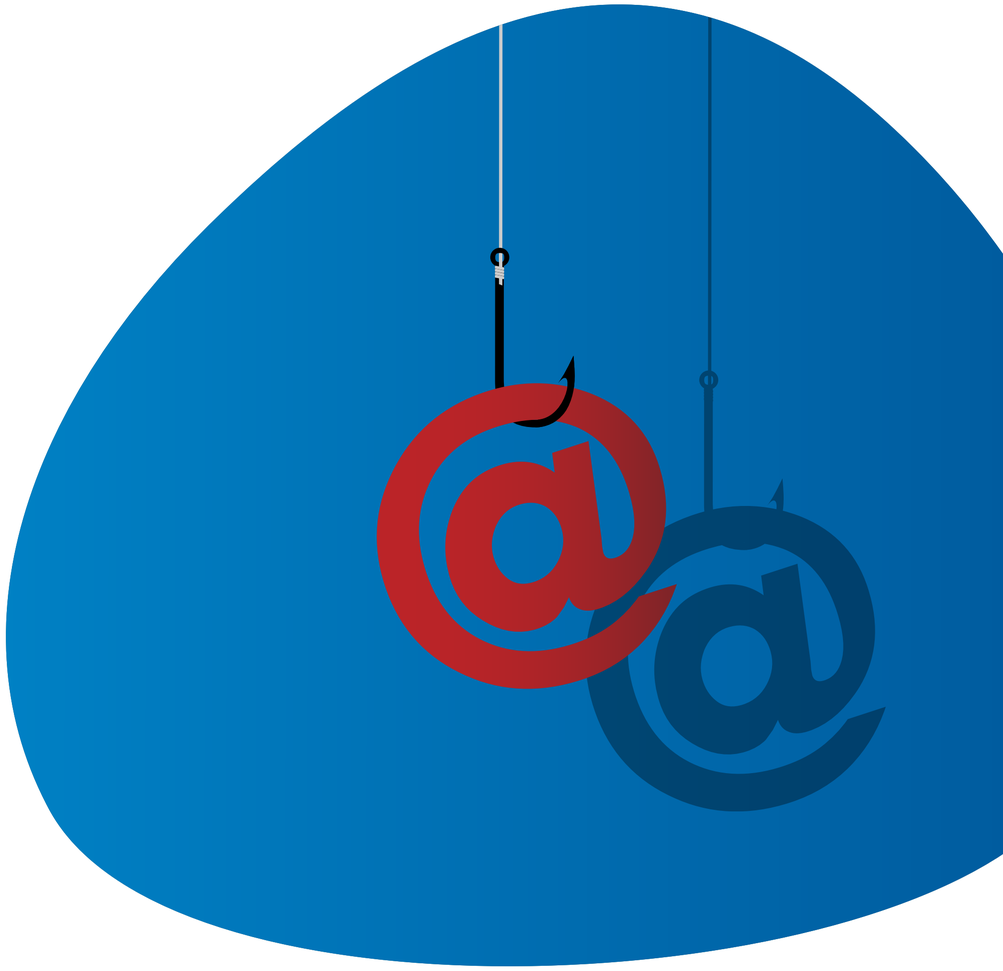
Sommaire

POURQUOI LE FACTEUR HUMAIN EST-IL SI IMPORTANT ?

Divulgation d'informations sensibles sur Internet, négligence ou manque de prudence vis-à-vis des courriels, contournements des règles de sécurité ou utilisation inappropriée des ressources informatiques professionnelles… La très grande majorité des incidents de sécurité est d'origine humaine.

Conscients que le facteur humain est le maillon faible de la sécurité informatique, les pirates se servent désormais des collaborateurs comme porte d'entrée vers les Systèmes d'Information (SI) des organisations, exploitant en priorité des faiblesses psychologiques et organisationnelles plutôt que des vulnérabilités informatiques.

Pour ce faire, ils ont recours à une arme redoutable : l'ingénierie sociale.



L'ingénierie sociale, quèsaco ?

Concept théorisé par le hacker repenti Kevin Mitnick dans son ouvrage L'Art de la supercherie paru en 2002, l'ingénierie sociale — ou piratage psychologique — se définit comme l'art de manipuler sa cible pour la pousser à accomplir une action ou à divulguer des informations personnelles ou confidentielles à des fins d'escroquerie. L'objectif est d'obtenir de l'argent ou un accès au SI d'une entité.

Pour tromper sa victime, « l'ingénieur social » pourra avoir recours à l'usurpation d'identité, se faisant par exemple passer pour un technicien de maintenance informatique ou un collègue. La mise en œuvre d'un processus fiable de contrôle de l'identité, est donc une étape fondamentale pour renforcer la sécurité des SI. Cela consiste à utiliser des mots de passe robustes et des méthodes d'authentification forte, telles que l'authentification à facteurs multiples, le certificat numérique ou la biométrie, pour vérifier l'identité d'une personne et lui autoriser l'accès à des ressources.

Chiffres clés

85%

des violations de données impliquent un élément humain[1].

75%

des organisations ont fait face à des attaques par hameçonnage en 2020[2].

66%

ont subi des formes d' hameçonnage ciblé[2].

64%

ont subi des attaques d'hameçonnage par téléphone[2].

80%

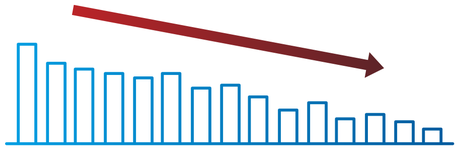
des professionnels de la sécurité ont été confrontés à une intensification des menaces de sécurité depuis le passage au télétravail[3].

62%

affirment que les campagnes de phishing sont celles qui se sont le plus accrues pendant la crise du Covid-19[3].

1 entreprise sur 5

déclare avoir subi au moins une attaque par ransomware en 2020[4].



4,24 M$

Coût total moyen d'une violation de données[5].

1. *Verizon 2021 Data Breach Investigations Report (DBIR)*
2. *Proofpoint 2021 State of the Phish Report*
3. Microsoft New Future of Work Report
4. *Sondage OpinionWay pour le CESIN*
5. *IBM Cost of a Data Breach Report 2021*

À QUELLES MENACES LES ORGANISATIONS SONT-ELLES CONFRONTÉES ?

Les attaques d'ingénierie sociale englobent tout un arsenal de techniques avec des conséquences, immédiates et à retardement, parfois dévastatrices.

Exemples d'attaques :

Rançongiciel (ransomware) : logiciel malveillant prenant des données en otage — en les chiffrant — dans le but d'extorquer de l'argent.

Hameçonnage (phishing) : technique visant à obtenir des informations personnelles ou confidentielles en se faisant passer pour un tiers de confiance et en diffusant un courriel frauduleux à un grand nombre de personnes.

Vishing : hameçonnage par téléphone

Harponnage (spear phishing) : hameçonnage ciblé

Arnaque au président : escroquerie exploitant la technique du prétexte (création d'un scénario) pour gagner la confiance d'un employé et le pousser à effectuer un virement.
Le cybercriminel se fait généralement passer pour le dirigeant de la société ou pour un fournisseur.

Attaque de point d'eau : technique ciblant une organisation ou un secteur d'activité spécifique, qui consiste à piéger un site Web légitime pour infecter les appareils des internautes qui le visitent.

Exemples d'impacts :

- Interruption des activités
- Perte de données
- Perte de propriété intellectuelle
- Perte de confiance des clients et des partenaires
- Dépréciation financière
- Augmentation du coût des assurances
- Sanctions réglementaires
- Honoraires d'avocat et frais de justice
- Amendes
- Coûts de mise en conformité réglementaire - notamment au RGPD - et de sécurisation post-incident

Spear phishing : l'ingénierie sociale à l'œuvre

Le harponnage illustre parfaitement l'utilisation du facteur humain pour percer les défenses d'une organisation.
À la différence du phishing, cette attaque est ciblée. Elle repose généralement sur une usurpation de l'identité de l'expéditeur d'un message personnalisé, envoyé à un nombre limité de personnes, dans le but d'infiltrer un SI. Le plus souvent, le destinataire reçoit un courriel qui l'invite à ouvrir une pièce jointe piégée ou à cliquer sur un lien malveillant (phase de contamination). Une fois la première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du SI de l'organisation ciblée (phase d'infiltration). L'attaquant cherche ensuite à obtenir des droits d'administrateur (« escalade de privilèges ») pour pouvoir s'implanter sur les postes et serveurs où sont stockées les informations convoitées. On parle aussi de « propagation latérale ». Il s'efforcera dès lors de voler des données le plus discrètement possible (phase d'exfiltration).

Source : ANSSI

COMMENT MINIMISER LE RISQUE HUMAIN ?

Chaque individu peut potentiellement constituer une « faille de sécurité ». Quelles mesures mettre en œuvre pour se prémunir des risques ?

Une bonne hygiène informatique

À l'échelle individuelle, les utilisateurs doivent appliquer plusieurs bonnes pratiques : employer des mots de passe robustes et maintenir leur confidentialité, effectuer régulièrement des mises à jour, faire preuve de prudence dans la diffusion de ses informations personnelles ou lors de l'ouverture de courriels…
Il est également recommandé de proscrire les pratiques de Shadow IT : emploi de terminaux et de logiciels non autorisés par le service informatique.
Ces règles élémentaires constituent ce que l'on appelle « l'hygiène informatique » : autant de bonnes habitudes à prendre pour améliorer sa posture individuelle et donc la sécurité collective de l'organisation.

Sensibiliser, former, évaluer

Les organisations peuvent limiter la portée des attaques grâce à des solutions techniques, comme les antivirus, les EDR et les filtres anti-phishing, répondant aux menaces connues. Toutefois, la technologie à elle seule ne suffit pas à les protéger complètement contre les cyberattaques. Elles doivent absolument compléter leur démarche par des actions de sensibilisation aux risques cyber et de formation de leurs collaborateurs.

Plus que de simples campagnes de communication ponctuelles, ces mesures visent à apporter aux utilisateurs le savoir et les compétences nécessaires pour leur permettre d'identifier les attaques et de se prémunir contre elles. S'inscrivant généralement dans un temps moyen à long, elles comportent des tests d'hameçonnage et autres exercices pratiques pour stimuler et évaluer en permanence l'assimilation des connaissances. Dans le cas précis de l'ingénierie sociale, il s'agira par exemple de faire un tour d'horizon des dernières techniques de phishing et de s'entraîner à réagir en réalisant des simulations de vishing dans lesquelles un attaquant usurpe le numéro appelant.

Ce type de programmes permet non seulement de réduire les risques de systèmes compromis, mais aussi de créer une culture de sécurité de l'information au sein comme à l'extérieur de l'organisation.

Transition

Les usages et les comportements des collaborateurs ont des répercussions importantes sur le niveau de sécurité de leur organisation. Il est donc indispensable de les inclure dans la politique de sécurité des SI, de leur fournir les connaissances et les compétences nécessaires en cybersécurité
et de renforcer leur implication dans la protection du SI et des données de la société. Ce type d'actions peut toutefois s'avérer difficile à mettre en place d'autant que les équipes informatiques ne disposent pas toujours de l'expertise et de l'expérience nécessaires leur permettant de mettre
sur pied un programme de sensibilisation efficace et attractif. Heureusement, des solutions ont été spécialement pensées pour les organisations.

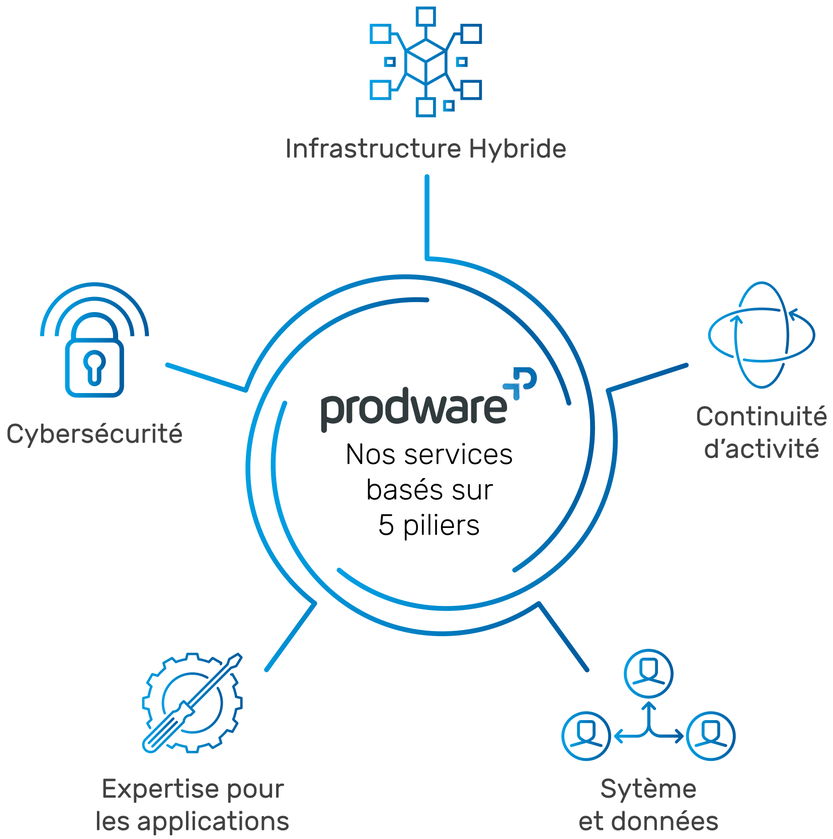
Partie 2

L'OFFRE PRODWARE : ASSURER LA SÉCURITÉ PAR LA SENSIBILISATION

Sommaire

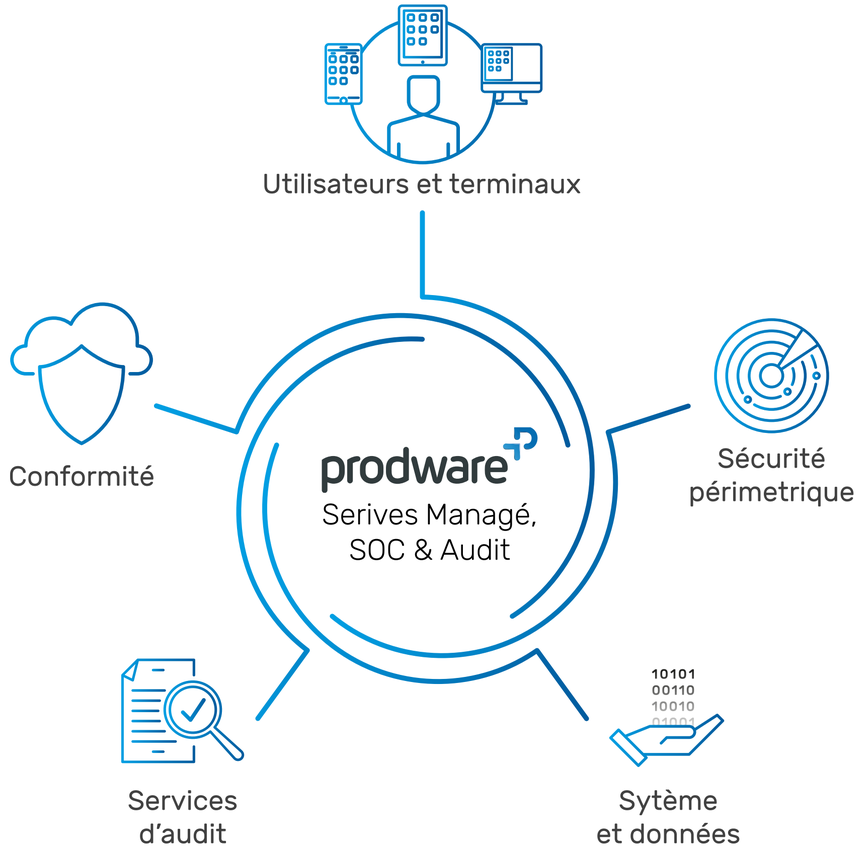
PRODWARE ET LA CYBER-SENSIBILISATION

Grâce à son large éventail de solutions et de services, Prodware répond à l'ensemble des enjeux autour de l'Infrastructure, du Cloud et de la Collaboration digitale.



Une approche de la cybersécurité orientée client

Conscient que la maîtrise du risque informatique nécessite une démarche globale, l'approche de Prodware en matière de cybersécurité repose sur cinq piliers, dont des services de cyber-sensibilisation au sein de la dimension « Utilisateurs et Terminaux ».



Réussir votre programme de cyber-sensibilisation avec Prodware

« Les cybermenaces actuelles obligent les Directions des Systèmes d'Information (DSI) à repenser les protections en place, les améliorer en permanence et s'adapter à l'évolution des risques en tenant compte des nouveaux usages des utilisateurs. La protection du réseau d'entreprise, ainsi que des données et applications hébergées dans le Cloud, ne suffisent pas. La protection des points de terminaison, déjà clé, devient vitale dans un contexte de recours massif au télétravail où chaque terminal est un point d'entrée potentiel pour les pirates, même les moins expérimentés.

Dans cet environnement, l'approche doit être globale et inclure des mesures techniques, le tout en tenant compte du risque humain et ce, à l'échelle de toute l'entreprise. Tout le monde est concerné, à tous les niveaux.

La DSI, la Direction des Ressources Humaines et la Direction Générale doivent ainsi travailler de concert afin de fédérer l'ensemble des métiers et engager pleinement tous les collaborateurs dans des plans de sensibilisation et de formation inclusifs, en veillant à ce que même les populations les moins technophiles puissent appréhender les risques cyber. Pour s'assurer que ces actions soient à la fois acceptées et comprises par l'ensemble des publics, il est crucial qu'elles soient correctement pensées et déployées. »

Cyrille Duvivier, Directeur Infrastructure, Cloud et Digital chez Prodware

En partenariat avec KnowBe4, leader mondial de la formation et de la sensibilisation à la sécurité, l'offre de Prodware aide les organisations à mettre en place puis à piloter simplement une politique efficace de cyber-sensibilisation.

KNOWBE4,
LA SOLUTION DE CYBER-SENSIBILISATION DE RÉFÉRENCE

KnowBe4 est une plateforme Cloud qui procure un programme complet de formation sur la sensibilisation à la cybersécurité ainsi que des outils complémentaires. Cette solution met à la disposition des organisations tous les outils nécessaires pour réduire les risques Cyber liés à l'ingénierie sociale et aux mauvais comportements informatiques.

Analyser, entraîner, tester

À partir d'une simulation d'attaque puis d'une enquête auprès des utilisateurs d'une organisation, KnowBe4 évalue la maturité des collaborateurs en matière de sécurité puis restitue le niveau global de « culture sécurité ».

KnowBe4 donne ensuite accès à une vaste bibliothèque de contenus de formation, comprenant notamment des modules interactifs, des vidéos, des jeux, des enquêtes et des newsletters. Ces contenus précis, interactifs et régulièrement renouvelés ont été pensés pour que les collaborateurs comprennent les mécanismes d'attaques d'ingénierie sociale et le fonctionnement des logiciels malveillants, assimilant ainsi les bonnes pratiques.

Les connaissances et réflexes des utilisateurs peuvent être régulièrement testés à l'aide de simulations de phishing (email) et de vishing (voix) automatisées. Ces simulations peuvent s'effectuer à partir de modèles éprouvés proposés par KnowBe4, de modèles communautaires « créés par des admins, pour des admins », ou de modèles spécifiques conçus par le DSI de l'organisation.

« Le choix de la solution Knowbe4 s'est fait naturellement en raison de la qualité des contenus proposés, d'une expérience utilisateur adaptée à différents publics, d'une interface ergonomique, de la présence d'éléments de gamification et du caractère multilingue de la plateforme. Ce dernier point est essentiel pour former les collaborateurs sur l'ensemble des filiales en s'assurant que les risques et les mesures de protection soient pleinement compris. »

DSI dans une ESN internationale

PRODWARE ET LA MÉTHODOLOGIE KNOWBE4

Fort de plus de trente ans d'expérience au service de la performance des entreprises et d'une double expertise sur les Infrastructures et les Applications métier, Prodware aide les organisations à mettre en place les solutions informatiques les plus performantes du marché.

Pour répondre à leurs besoins en cyber-sensibilisation, Prodware a élaboré une démarche structurée qui garantit un déploiement efficace et simple de la solution KnowBe4. Celle-ci permet d'évaluer les connaissances des collaborateurs, d'adapter en continu le plan de formation, et d'améliorer la cyber-résilience des organisations.

Kick off

- Enjeux
- Équipes projet IT et RH
- Planning
- Plan de communication
- Appui Direction

Intégration technique

- Setup console KB4 et Single Sign on
- Paramétrage serveurs KB4
- Import des utilisateurs et groupes

Campagne de Phishing (1 semaine)

- Péparation de l'attaque fictive
- Évaluation des résultats

Evaluation Cyber (2 semaines)

- Enquête d'évaluation du niveau Cyber des utilisateurs
- Analyse des résultats par groupe

Campagne de formation Cyber

- Définition du plan de formation annuel par groupe, basé sur le résultat de l'analyse

Sprints

Pilotage et amélioration de la maturité Cyber

- Ajustement des contenus, gamification
- Évaluation continue et enquête anuelle
- Campagnes de hameçonnage régulières
- Support des managers/Sponsors

Accompagnement

Au-delà de la mise en œuvre KnowBe4, Prodware accompagne les équipes IT et RH chaque mois, trimestre ou semestre pour piloter, analyser et adapter le plan de formation Cyber.

« La mise en place de la solution KnowBe4 (cadrage/analyse/évaluation/1ère formation) peut être réalisée en moins d'un mois. À raison d'une formation par mois, complétée par la diffusion de contenus additionnels et ponctuée de tests d'hameçonnage, le programme est supposé durer environ un an. Les premiers résultats concrets sont visibles dès le premier mois : plus vigilants, les utilisateurs signalent plus souvent les courriels suspects. Dans un premier temps, le nombre de faux-positif va très certainement augmenter, mais c'est une bonne chose ! »

RSSI dans une entreprise de l'agro-alimentaire

QUAND LA CYBERSÉCURITÉ DEVIENT UNE OPPORTUNITÉ

La cybersécurité est un prérequis majeur de toute transformation digitale

Sur la base de notre expérience, nous sommes persuadés que les démarches de cybersécurité doivent être appréhendées non pas comme une contrainte, mais comme une opportunité. Correctement mises en œuvre, elles sécurisent l'organisation tout en communiquant des messages positifs aux employés, clients et partenaires.

Dans cette optique, la cyber-sensibilisation donne les bons réflexes aux collaborateurs tant sur le plan professionnel que personnel. En complément de la protection opérationnelle du SI qu'elle procure, elle véhicule un message responsable de maîtrise des risques et d'esprit de corps dont toute l'organisation bénéficie.

De manière générale, la cybersécurité constitue un élément fort de différenciation. De même que la gestion éthique des données personnelles peut améliorer l'image de marque d'une organisation, une stratégie de cybersécurité sérieuse et transparente peut faire rayonner une marque sur son marché et renforcer la confiance de ses clients et partenaires.

La cyber-sensibilisation est également un formidable levier « d'empowerment », qui donne aux collaborateurs les moyens de se protéger contre une menace ubiquitaire. Elle les rend plus responsables, autonomes et actifs, elle leur permet de devenir une partie intégrante du système de défense de leur organisation. En somme, de faire partie de la solution et non plus du problème.

Faire du facteur humain un atout dans une stratégie de cybersécurité, c'est là tout l'enjeu d'une campagne de cyber-sensibilisation. Affronter efficacement la Cybercriminalité et la faire reculer, c'est possible, à condition bien sûr d'être accompagné par un partenaire expérimenté.

NOS POINTS FORTS

- Leader en **zone EMEA** sur les solutions de gestion Microsoft
- Présence à la fois **nationale** et **internationale**
- **Méthodologie** éprouvée, compétences **multi produits**
- **Forte expertise** sectorielle et métier
- **Equipes** dédiées, **investissements** en R&D

POUR EN SAVOIR PLUS...

CONTACTEZ-NOUS

Découvrez nos services et rencontrez nos experts dans nos 42 agences répartis dans 12 pays

Prodware France
45, quai de la Seine, 75019 PARIS
France infos@prodware.fr