sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Le Guide pour réduire les cyber-risques humains

Apprenez à renforcer le dispositif de sécurité des employés de votre organisation contre l'erreur humaine et les cybermenaces en constante évolution.

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ

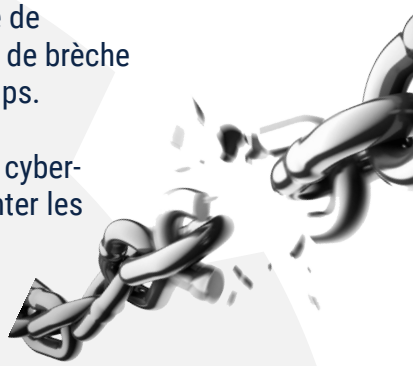
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

www.sinequanon.fr

Transformer les humains de « maillon faible » ...

Les employés ont longtemps été considérés comme le "maillon faible" de la chaîne de cybersécurité d'une entreprise et, l'erreur humaine étant toujours la première cause de brèche des données, ce malheureux trophée a été attribué à juste titre depuis très longtemps.

Même si les organisations consacrent plus de temps et d'argent à la lutte contre le cyber-risque humain, les incidents de sécurité liés aux employés ont continué de tourmenter les entreprises en 2022.



Mais pourquoi ?

Pour faire simple, de nombreuses entreprises n'en font pas assez pour lutter contre les menaces en constante évolution. Les cybercriminels utilisant des techniques plus avancées pour exploiter les humains, la voie traditionnelle de la formation ponctuelle à la sensibilisation à la sécurité ne suffit pas à protéger les entreprises d'aujourd'hui contre la perte d'informations sensibles, les atteintes à la réputation et les répercussions financières.

40%

Selon les estimations de l'ANSSI, en 2022, 40% des sociétés touchées par des cyberattaques sont des TPE/PME.

94%

D'après le Data Breach Investigations Report de l'entreprise Verizon, 94% des logiciels malveillants sont délivrés par e-mail.

73%

73% des entreprises déclarent le phishing comme vecteur d'entrée principal pour les attaques subies selon le baromètre du CESIN en 2022.

... en employés conscients des cyber-risques !

La bonne nouvelle, c'est que la solution de sécurité axée sur l'utilisateur a également évolué ces dernières années grâce à l'introduction de la gestion des risques humains (GRH), offrant un niveau de protection beaucoup plus solide aux entreprises de toutes tailles et de tous secteurs. Dans ce guide, nous verrons pourquoi les employés constituent une menace interne et comment favoriser un comportement humain sûr dans votre entreprise.

Humains, la cause #1 des brèches de cybersécurité

85% des brèches de données impliquent l'élément humain

Verizon 2021
Data Breach Investigations Report

- Les employés négligents sont à l'origine d'environ 62% des incidents de sécurité.
- 60% des entreprises connaissent plus de 20 incidents d'attaques internes par an.
- 82% des responsables informatiques estiment que le risque de menaces internes est plus élevé si leur entreprise adopte une structure de travail hybride permanente.
- 98% des organisations disent se sentir plus ou moins vulnérables aux menaces internes.

Quels sont les principaux types de menaces internes ?

Employés négligents

Les employés négligents - par exemple un employé qui adresse mal un e-mail ou joint accidentellement le mauvais fichier - constituent la menace la plus courante pour votre entreprise et sont responsables de 62% de tous les incidents de sécurité.

Les employés négligents qui subissent une brèche

Les employés négligents disposant d'informations d'identification qui ont été volées - par exemple, un employé dont le nom d'utilisateur et le mot de passe sont exposés sur le Dark Web - sont responsables de 25% de tous les incidents de sécurité.

Employés malveillants

Les employés malveillants - c'est-à-dire les employés ou ex-employés ayant des motivations malveillantes envers l'entreprise, comme un employé mécontent récemment licencié - représentent 13% des incidents.

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Pourquoi les employés constituent-ils une menace interne ?

1

Les humains font des erreurs

Nous faisons tous des erreurs. En fait, 43% des employés déclarent avoir fait une erreur au travail qui a compromis la cybersécurité, comme par exemple le mauvais acheminement d'un email.
Le problème est que ce type de "petites" erreurs peut entraîner l'exposition de données sensibles, que les hackers savent parfaitement exploiter.

2

Les humains sont des proies faciles

La plupart des informations relatives à votre entreprise se trouvent en ligne, notamment celles concernant vos fournisseurs, vos sous-traitants et vos clients. Il est donc facile pour les attaquants d'usurper l'identité de contacts internes et externes, et il suffit qu'une seule personne soit dupée avec succès pour que votre entreprise soit exposée à un risque de brèche grave.

3

Les humains enfreignent les règles

Dans toute entreprise, les gens sont en capacité d'enfreindre les règles, que ce soit par malveillance ou par accident.
Mais une grande partie des infractions aux règles vont au-delà du non-respect des politiques de mot de passe et certains employés peuvent aller jusqu'à voler des données d'entreprise et les vendre sur le dark web.

88% L'université de Stanford attribue 88% des brèches de données à l'erreur humaine.

En 2021, les attaques de phishing étaient liées à 36% des brèches, soit une augmentation de 11%.

43% des employés disent avoir fait une erreur au travail qui a compromis la sécurité.

70% des intrusions sont motivées financièrement par la vente d'identifiants sur le dark web.

25% des employés pensent avoir cliqué sur un email de phishing au travail.

45% des employés seraient prêts à vendre des informations à des personnes extérieures à leur organisation.

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

brèche de données liée à l'utilisateur

4 causes principales

Un employé qui manipule mal les informations d'identification

Le comportement des employés en matière de mots de passe joue un rôle important dans les incidents de sécurité. En effet, 61% des brèches impliquent des informations d'identification volées.

En réutilisant le même mot de passe sur plusieurs comptes, une seule brèche par un tiers peut créer un portail de risques humains pour votre entreprise.

La route qui mène à la compromission des informations d'identification

- Un employé s'inscrit à plusieurs services tiers en utilisant la même adresse électronique professionnelle et le même mot de passe.
- Un service tiers subit une brèche de données, exposant les informations d'identification de l'utilisateur.
- Les informations d'identification sont vendues sur le Dark Web, et les hackers peuvent potentiellement les utiliser pour accéder à plusieurs comptes.

À l'intérieur du Dark Web

- Le Dark Web est 500x plus grand que le Web de surface.
- L'activité sur le Dark Web a augmenté de 300% depuis 2017.
- Plus de 22 milliards de fichiers ont été ajoutés au Dark Web en 2020.
- 60% des informations disponibles sur le dark web pourraient potentiellement nuire aux entreprises.

Un employé tombe dans le piège astucieux d'une attaque de phishing

Le moyen le plus fréquent pour un employé de causer une brèche de sécurité est de se laisser prendre au piège d'une attaque de phishing.

Et comme le phishing est plus ciblé et plus sophistiqué que jamais, les employés ont de plus en plus de mal à repérer ces attaques.

Les techniques astucieuses utilisées par les hackers pour piéger vos employés.

- Spear Phishing — Ces attaques hyper-personnalisées visent un individu ou un groupe spécifique, l'attaquant effectuant des recherches préalables sur une cible souvent de haut niveau.
- Business Email Compromise — Si un hacker obtient l'accès à un compte de messagerie légitime, il peut exploiter des "collègues" en se faisant passer pour une personne de confiance via une attaque BEC..
- Domain Spoofing — Un hacker peut falsifier le nom d'affichage et l'adresse de l'expéditeur d'un email pour faire croire qu'il provient de l'intérieur de l'entreprise ou d'un fournisseur de confiance.

Erreur humaine

Une erreur d'un employé, comme une simple faute de frappe, peut sembler minime mais les répercussions peuvent être énormes.

Pour de nombreuses entreprises, une violation liée à une erreur humaine a entraîné des amendes, la perte de la confiance des clients et la perte de l'accès aux données.

Comment le comportement risqué d'un employé peut conduire à un incident de sécurité ?

- Partager, écrire ou réutiliser des mots de passe sur plusieurs comptes.
- Manipuler les données sans précaution, comme saisir le mauvais destinataire d'un email ou joindre le mauvais fichier.
- Manque de sensibilisation aux menaces courantes, telles que les emails de Spear Phishing.
- Ne pas comprendre que la sécurité est la responsabilité de tous les employés, et pas seulement un problème pour le département informatique.

Un manque de chartes et de processus de sécurité

Les chartes de sécurité de l'information permettent de guider le comportement des employés lorsqu'il s'agit de traiter les informations de l'entreprise et de garantir la sécurité des systèmes informatiques.

Sans ces chartes, les employés sont moins susceptibles de savoir à qui ils doivent signaler les attaques de phishing ou qui est autorisé à accéder à quelles données sensibles.

Comment les chartes peuvent-elles contribuer à réduire les risques ?

- Elles protègent les informations critiques de votre organisation en définissant clairement les responsabilités des employés en matière de sécurité.
- Elles empêchent la divulgation, la perturbation, la perte, l'accès, l'utilisation ou la modification non autorisés des actifs d'une organisation.

Exemples de chartes

- Charte d'utilisation acceptable
- Charte de données confidentielles
- Charte d'utilisation de l'email
- Charte de réponse aux incidents
- Charte de sécurité du réseaux
- Charte liée aux mots de passe
- Charte de sécurité physique

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Instaurer une culture de la sécurité

Une "culture de la sécurité" vise à encourager tous les employés à penser et à aborder la sécurité à travers les mêmes valeurs, en encourageant les gens à adopter les comportements souhaités pour assurer la sécurité du personnel, des clients et des fournisseurs.
La construction de cette culture nécessite un certain nombre de facteurs, dont la cohérence, le temps et les efforts. Voici quelques-uns des éléments essentiels à la création d'une équipe sensibilisée à la sécurité.

Obtenir le soutien de la direction

Le soutien de la direction est crucial pour le succès de toute initiative de gestion des risques humains.
Il ne s'agit pas seulement d'un courriel adressé à tous par le PDG, mais de l'équipe dirigeante qui démontre son soutien total à cette initiative en communiquant régulièrement avec le personnel, en affectant le budget nécessaire et en créant des rôles professionnels spécifiques.

La cohérence et l'engagement sont essentiels

La clé de la création et du maintien d'une équipe sensibilisée à la sécurité réside dans une formation cohérente et à long terme des utilisateurs, comme l'a souligné un rapport de Keepnet Labs, dans lequel il a été prouvé qu'une formation cohérente à la sensibilisation à la sécurité réduisait la sensibilité des employés au phishing de 60% à 10% au cours des 12 premiers mois.

Le temps, et non le budget, est le facteur bloquant à combattre

Selon le rapport SANS 2021 "Managing Human Cyber Risk", 75% des professionnels de la sécurité consacrent moins de la moitié de leur temps à la sensibilisation à la sécurité, même si une plus grande implication dans la formation est corrélée à une augmentation des changements de comportement positifs.

Sécurité : une responsabilité commune

Les employés doivent comprendre que la cybersécurité est la responsabilité de chacun d'entre eux, et pas seulement du service informatique.
Les employés ont plus que jamais accès aux ordinateurs et aux ressources en ligne et sont largement considérés comme le plus grand risque pour une entreprise.

Aller au-delà de la formation à la sensibilisation à la sécurité

La formation à la sensibilisation à la sécurité est un excellent moyen de réduire le cyber-risque humain, 80% des organisations constatent une réduction de la vulnérabilité lorsqu'elles forment leur personnel.
Pour que votre équipe soit vraiment résiliente face à l'évolution des menaces, des politiques doivent être mises en œuvre et des évaluations pratiques, telles que des simulations de phishing, doivent avoir lieu régulièrement.

L'alignement stratégique est crucial

SANS indique également que les dirigeants doivent réaliser des investissements stratégiques à long terme dans les ressources humaines, tout comme ils le feraient pour d'autres efforts de sécurité tels que la gestion des vulnérabilités, la réponse aux incidents ou les centres d'opérations de sécurité, afin de gérer efficacement le risque humain.

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Gestion des Risques Humains
Mise en œuvre de la GRH

La Gestion des Risques Humains (GRH) permet aux entreprises d'évaluer, de réduire et de surveiller la posture de sécurité de leurs employés face à l'évolution des cybermenaces et des erreurs humaines.

Ces menaces devenant de plus en plus complexes et sophistiquées, la gestion des risques humains offre une solution complète pour favoriser un comportement humain sûr, plutôt que de s'en remettre uniquement à la formation des utilisateurs dans l'espoir qu'ils retiennent quelque chose.

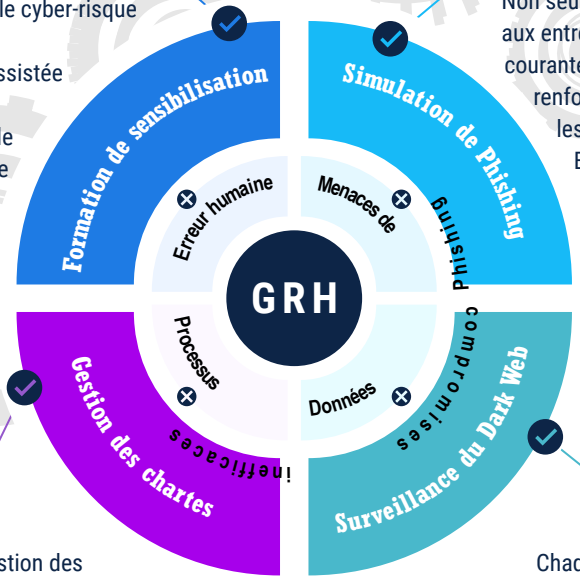
4 éléments clés

Favoriser un comportement sûr des utilisateurs

La formation à la sensibilisation à la sécurité est l'une des approches les plus efficaces pour réduire le cyber-risque humain.
Dispensées par le biais d'une formation assistée par ordinateur, ces sessions doivent être régulières, courtes et couvrir une variété de sujets essentiels en matière de sécurité de l'information et de conformité.

Réduire considérablement la vulnérabilité au phishing

Non seulement les simulations de phishing permettent aux entreprises d'évaluer leur vulnérabilité aux attaques courantes, mais elles offrent également la possibilité de renforcer la formation des utilisateurs et de mesurer les progrès de chacun.
Elles devraient être effectuées régulièrement afin de tester les nouvelles attaques, tout en évaluant le niveau de risque des nouveaux employés.



Améliorer les processus de sécurité

La mise en œuvre d'un processus de gestion des chartes aide le personnel à comprendre et à assumer ses responsabilités, ce qui renforce la protection des informations commerciales et des systèmes informatiques.
Les chartes doivent aborder un certain nombre de domaines clés (voir les exemples à la page suivante) et doivent être mises à jour et signées par le personnel au moins une fois par an afin de maintenir les processus à jour.

Atténuer les menaces extérieures

Chaque année, des millions de noms d'utilisateur, de mots de passe et de données de paiement sont déversés sur le Dark Web. La surveillance permanente du Dark Web permet d'alerter les entreprises lorsque les données des employés sont compromises.
La détection de ces menaces précoces peut permettre d'éviter une attaque ciblée - et une brèche potentielle des données - plus tard.

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Maximiser le succès, les **bonnes pratiques**

Apprenez quels sont les ingrédients clés d'une approche réussie de la Gestion des Risques Humains.

1. **Rendre la formation courte et attrayante**
   Utiliser des cours de formation vidéo courts pour impliquer le personnel
2. **Aborder l'essentiel**
   Aborder les principaux sujets liés à la sécurité
3. **Former les équipes régulièrement**
   Une formation régulière et récurrente permet de bien retenir les informations
4. **Éviter le jargon technique**
   De nombreux employés ne comprennent pas les termes techniques
5. **Reproduire les menaces de phishing**
   Simulations de phishing en s'inspirant des attaques les plus récentes.
6. **Chartes informatiques**
   Assurez-vous que votre bibliothèque de chartes comprend les éléments essentiels
7. **Mesurer l'impact**
   Suivez les performances de la formation et les simulations dans le temps.

Thèmes de formation clés pour vos collaborateurs

- Attaques de phishing
- Mots de passe & Authentification Télétravail
- Utilisation d'Internet et des emails
- Sécurité physique
- Ingénierie sociale
- Appareils connectés
- Wi-Fi public

Les escroqueries par phishing les plus courantes à tester sur vos collaborateurs

- Nouvelle demande de Microsoft Teams
- Alerte Covid-19
- Mot de passe Microsoft 365
- Facture à payer
- Remboursement d'impôts
- Carte-cadeau d'Amazon
- Messagerie bloquée

Chartes de sécurité essentielles à mettre en œuvre dans votre entreprise

- Charte d'utilisation acceptable
- Charte de données confidentielles
- Charte d'utilisation de l'email
- Charte de réponse aux incidents
- Charte de sécurité du réseaux
- Charte liée aux mots de passe
- Charte de sécurité physique

sine qua non .fr

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Commencez dès aujoud'hui !

Réduisez le cyber-risque humain.

Faites la lumière sur les zones de risque humain actuelles de votre entreprise et commencez à mettre en place un personnel sensibilisé à la sécurité grâce à notre service de GRH entièrement géré.

Nous savons que le temps, le budget et le fait de ne pas savoir par où commencer sont souvent les principaux obstacles au lancement d'un nouveau processus interne.

C'est pourquoi **nous avons lancé un service de gestion des risques humains** à faible coût et entièrement géré, qui est rapide à lancer, non perturbateur et qui couvre tous les éléments clés pour favoriser un comportement sûr des utilisateurs, notamment :

- Programmes de formation à la sensibilisation à la sécurité attrayants et concis
- Des évaluations régulières de phishing
- Surveillance continue du Dark Web
- Une mise en œuvre essentielle des chartes traçables
- Notation permanente des risques humains et rapports réguliers

Contactez-nous

Adoptez une attitude proactive et commencez à vous attaquer au cyber-risque humain avant qu'une brèche de données liée à un utilisateur ne se produise.

sine qua non .fr
Sine Qua Non
13 rue Chaligny - 75012 Paris
Tél. 01 40 38 22 13 - www.sinequanon.fr

Avantages

- Renforcer la résistance des utilisateurs aux attaques de phishing
- Réduire les incidents de sécurité liés aux utilisateurs
- Démontrer la conformité aux normes clés telles que ISO 27001et RGPD
- Comprendre la posture de sécurité des employés de votre entreprise grâce à un score de risque humain
- Analyser en profondeur le risque humain permanent grâce à des rapports sur la formation, le phishing et les chartes
- Configuration simple, déploiement rapide et rappels automatisés de formation des équipes