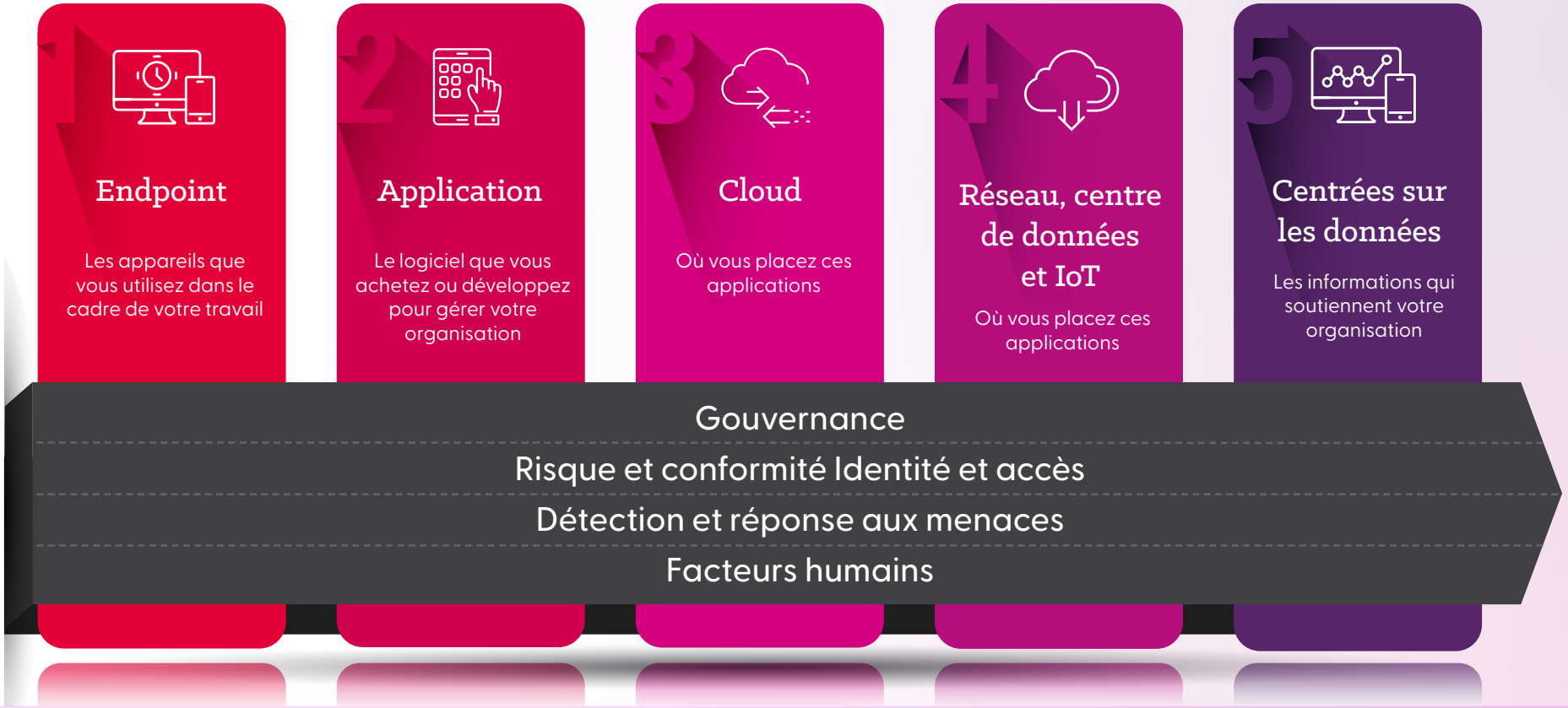
Insight Guide sur les facteurs humains dans la sécurité

Insight

Introduction

Chez Insight, nous reconnaissons l'importance d'une approche holistique de la sécurité. Les agresseurs chercheront votre point faible, pas votre point fort. Nous disposons d'une expertise technique dans les cinq domaines de la technologie (Endpoints, Applications, Cloud, Network, Centre de données et IOT, et données centrées), mais en tant qu'intégrateur de solutions de premier plan, nous pensons que vous devez également prêter une attention particulière aux interactions entre ces domaines de la technologie (gouvernance, risque et conformité, identité et accès, détection et réponse aux menaces, et facteurs humains). Les lacunes où les domaines technologiques se connectent sont souvent là où une valeur ajoutée peut être obtenue, contribuant à améliorer votre posture de sécurité globale de manière rentable.

Le modèle de sécurité holistique d'Insight



Que sont les facteurs humains et pourquoi sont-ils importants ?

Même si l'infrastructure, les outils et les contrôles de sécurité sont constamment améliorés et font l'objet d'investissements, des violations se produisent toujours, et il n'est pas facile de les identifier et de les résoudre. Il existe de nombreux contrôles de sécurité spécialisés pour différents types de menaces, des attaques sur les terminaux aux attaques sur les chaînes d'approvisionnement, mais lorsque vous examinez comment ces attaques se sont réellement produites, les trois principales raisons sont les suivantes :

- **Mots de passe –** aun mot de passe non sécurisé a été déchiffré, un mot de passe par défaut a été laissé inchangé ou le même mot de passe a été utilisé sur plusieurs sites.s.
- **Phishing –** un utilisateur a été induit en erreur pour divulguer ses identifiants, visiter un site Internet compromis ou ouvrir une pièce jointe hostile.
- **Patching –** une vulnérabilité connue n'a pas été corrigée et a été exploitée par un malware, ou certains logiciels risqués ont été installés par un utilisateur compromis.

Les équipes informatiques peuvent utiliser la technologie pour réduire le risque de violations, mais les utilisateurs finaux joueront toujours un rôle dans le support de la sécurité d'une organisation. Équipes IT :se concentrent souvent sur la technologie, et parfois sur le processus, et oublient l'aspect humain, alors que c'est lui qui peut déterminer l'échec ou la réussite d'un projet.

Processus : les politiques écrites expliquant ce que les utilisateurs doivent ou ne doivent pas faire prennent de nombreuses formes, telles que les politiques de sécurité de l'information, les contrats de travail, les manuels des collaborateurs, les politiques d'utilisation acceptable ou les plans d'intervention en cas d'incident.

Technologie : les outils, systèmes et contrôles qui fournissent des directives et des restrictions sur ce que les utilisateurs peuvent faire doivent être suffisamment stricts pour restreindre les activités à risque évident, mais suffisamment permissifs pour permettre une certaine flexibilité et ne pas perturber les processus commerciaux.

Personnes : lorsqu'il n'y a pas de processus documenté ou que les personnes ne le connaissent pas, elles doivent utiliser leur propre jugement. Ou lorsqu'une technologie ne parvient pas à prévenir une nouvelle menace, les personnes sont souvent la première et la dernière ligne de défense, en s'appuyant uniquement sur leurs compétences et leurs formations.

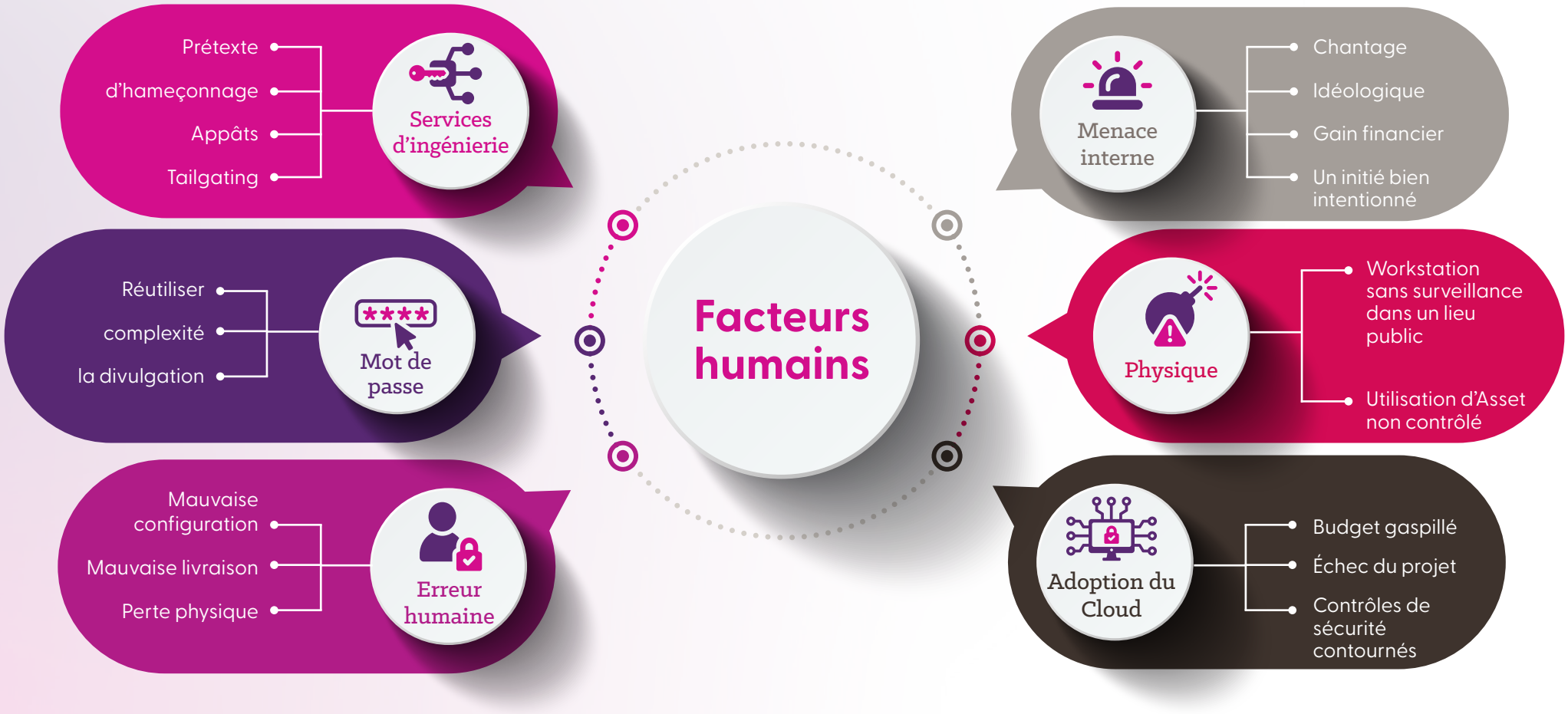
D'ici 2027, 50 % des responsables de la sécurité de l'information (RSSI) des grandes entreprises auront adopté des pratiques de conception de la sécurité centrées sur l'humain pour minimiser la cybersécurité. et de maximiser l'adoption du contrôle.

- Gartner identifie les principales tendances en matière de cybersécurité pour 2023.

L'écart de compétences

Étant donné que le manque de cybercompétences persiste comme un obstacle pour les organisations, il peut être nécessaire de transférer des personnes d'autres parties de l'entreprise vers des rôles axés sur la sécurité et de les équiper des compétences dont elles ont besoin. La formation et l'accompagnement sur le terrain ont leurs limites lorsque les compétences à enseigner sont rares dans l'organisation. Pour les ressources plus qualifiées, la formation est souvent considérée comme essentielle pour maintenir les experts techniques qui veulent mettre à jour leurs compétences.

Les facteurs humains peuvent avoir un impact sur presque tous les aspects de votre stratégie de sécurité.



L’importance des personas

Vous devez adapter vos facteurs humains dans la stratégie de sécurité aux différents types d’utilisateurs, ou personas, de votre organisation. Une approche générique ne sera pas très efficace – les personnes doivent être responsabilisées par rapport à leur rôle actuel et comprendre comment elles peuvent contribuer personnellement à la sécurité de l’organisation.

Voici un exemple de la manière dont vous pouvez catégoriser les types d’utilisateurs dans une organisation type, mais chaque organisation est différente.

Utilisateur final

- Différents niveaux de compétences informatiques, certains n’ont que des connaissances très basiques
- Le multilinguisme est susceptible d’être une exigence dans les organisations mondiales
- Les sujets peuvent être liés au phishing, au RGPD, à la sécurité physique, etc.

Développement

- Généralement techniquement avancé, mais peut ne pas être au courant des techniques de codage sécurisé
- Nécessite probablement une formation de niche, en utilisant le même langage de programmation que le développeur
- La ludification et l’apprentissage pratique sont susceptibles d’avoir un meilleur impact que l’apprentissage non interactif

Administrateur IT

- Les utilisateurs à la pointe de la technologie veulent pouvoir développer encore davantage leurs compétences existantes et être mis au défi
- La gamification et la concurrence peuvent aider à stimuler l’adoption
- Comme un pilote, des compétences pratiques dans un environnement de simulateur sur-utilisé peuvent aider à réagir à des situations de sécurité réellement stressantes

Directeurs généraux

- Concentrez-vous sur les activités d’apprentissage de groupe pour tester les processus de prise de décision, les rôles et les définitions de responsabilités
- Axé sur l’entreprise
- Peut impliquer de nombreux rôles différents pour tester la dynamique de l’équipe

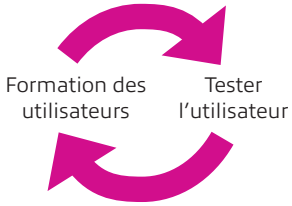
Comment Insight peut vous aider

Sensibilisation à la sécurité des utilisateurs finaux managés

Dans l'environnement numérique actuel, où la plupart des opérations commerciales sont effectuées en ligne, il est vital que les utilisateurs finaux soient conscients de la sécurité. Les organisations doivent s'assurer que leurs collaborateurs connaissent les dangers possibles des cyberattaques et la manière dont ils peuvent les réduire. Cela implique d'enseigner aux collaborateurs comment suivre les bonnes pratiques de management des mots de passe, les habitudes de navigation sécurisées et comment repérer et signaler les e-mails douteux.

Les attaques par hameçonnage sont l'un des plus grands risques pour la cybersécurité d'une entreprise. Ces attaques tentent de tromper les gens en leur donnant des informations personnelles telles que des noms d'utilisateur, des mots de passe ou des informations financièresd'informations. Les simulations de phishing sont un moyen utile d'enseigner aux collaborateurs comment se protéger contre ces attaques. En créant de faux e-mails de phishing qui ressemblent à de vrais e-mails, les collaborateurs peuvent apprendre à repérer et à signaler les messages douteux.

Nous travaillons avec KnowBe4, un expert en formation de sensibilisation à la sécurité pour les utilisateurs finaux, qui fournit une plateforme complète comprenant des modules de formation, des simulations de phishing et d'autres outils qui enseignent aux collaborateurs les dernières menaces et comment les éviter. La plateforme utilise des méthodes engageantes, telles que des vidéos, des quiz et des jeux interactifs, pour contacter les collaborateurs et rendre l'expérience de formation plus amusante.



Leur méthodologie est basée sur un cycle de formation et de tests - pas une fois par an, mais régulièrement en petits morceaux afin de renforcer la formation et de pouvoir mesurer les améliorations. La formation peut ensuite être ciblée dans les bonnes quantités, sur les bonnes personnes.

Nous proposons une solution complète de bout en bout qui exploite la plateforme KnowBe4 pour fournir une formation efficace à la sensibilisation à la sécurité à nos clients/clientes. Nos services managés incluent une surveillance et des rapports continus, ce qui nous permet d'identifier les domaines où une formation supplémentaire peut être nécessaire et de fournir un retour d'information opportun à nos clients/clientes. Les organisations peuvent ensuite se concentrer sur leurs activités commerciales de base, tandis que nous nous occupons de leurs besoins en formation de sensibilisation à la sécurité, ce qui les aide à se protéger contre les cybermenaces.

Plateforme de résilience des cyber-équipes

Une plateforme SaaS conçue pour exercer, établir des références, améliorer les compétences et prouver en permanence la cyberrésilience des équipes d'une organisation.

Pour les particuliers :

Un environnement d'apprentissage attrayant et ludique qui couvre l'ensemble du spectre de la formation technique pratique pour l'entreprise.

- Cyberprofessionnels offensives et défensives
- Développeurs et experts en sécurité des applications
- Professionnels de la sécurité Cloud et des infrastructures

Pour les équipes :

Réagir aux menaces liées à la sécurité nécessite un effort d'équipe, des techniciens aux cadres. Nous contactons des équipes de l'ensemble de votre organisation pour améliorer leurs compétences en matière de prise de décision et de réponse technique aux crises afin de répondre de manière adaptable et efficace aux cyber-risques.

- Équipes dirigeante
- Equipes de gestion de crise
- Équipes cybertechniques

Pour l'organisation :

Exercices de développement des compétences qui stimulent le changement de comportement transformationnel dans toute l'organisation.

- Cadres supérieurs
- Collaborateurs de première ligne
- Cibles à haut risque des cyberattaques

Tous ces éléments sont accessibles depuis n'importe quel endroit à l'aide d'un simple navigateur Web, et peuvent donc même être utilisés par des personnes extérieures aux organisations, par exemple dans le cadre d'un Recruitment Assessment pré-embauche.

En tant qu'entreprise, vous pourrez :

- Prouver en permanence la capacité de cybersécurité
- Améliorer la rapidité et la qualité de la réponse.
- Améliorer le recrutement et le développement de carrière.
- Réduire les vulnérabilités du Cloud et des applications.
- Réduire les coûts de cybersécurité.

Management de l'adoption et du changement

L'adoption et le management du changement jouent un rôle crucial dans le support des facteurs humains en matière de cybersécurité en veillant à ce que les mesures, politiques et technologies de sécurité soient efficacement adoptées et intégrées dans la culture et les pratiques d'une organisation. Les facteurs humains, tels que le comportement, la sensibilisation et les habitudes des utilisateurs, sont souvent les maillons les plus faibles de la cybersécurité, car ils peuvent être exploités par des acteurs malveillants.

Voici comment l'adoption et le management du changement d'Insight peuvent être bénéfiques pour traiter ces facteurs humains :

Sensibilisation et formation des collaborateurs : L'adoption et le management du changement impliquent de sensibiliser les utilisateurs aux menaces de cybersécurité, aux meilleures pratiques et à l'importance de la sécurité. En fournissant une formation et une communication claire, les utilisateurs sont plus conscients des risques potentiels et sont en mesure de prendre des décisions éclairées qui améliorent la sécurité.

Changement de comportement : Le management du changement vise à modifier le comportement des utilisateurs conformément aux pratiques de sécurité souhaitées. En établissant de nouvelles routines et habitudes, les utilisateurs peuvent être encouragés à adopter des comportements sécurisés, tels que la mise à jour régulière des mots de passe, la prudence face aux e-mails d'hameçonnage et le signalement d'activités suspectes.

Changement culturel : L'adoption réussie et les initiatives de management du changement favorisent une culture de la sécurité au sein de l'organisation. Lorsque la cybersécurité est ancrée dans la culture organisationnelle, les collaborateurs sont plus susceptibles de donner la priorité à la sécurité dans leurs activités quotidiennes, ce qui conduit à un environnement global plus sûr. Réduction de la résistance : Les gens résistent souvent aux changements, en particulier lorsqu'ils perturbent leurs routines habituelles. Des stratégies efficaces de management du changement anticipent et traitent cette résistance, contribuant à atténuer les revers contre les mesures de sécurité et facilitant une adoption plus fluide des nouvelles pratiques.

Conception centrée sur l'utilisateur : Les processus d'adoption et de management du changement impliquent de comprendre les besoins des utilisateurs et d'adapter les solutions de sécurité pour répondre à ces besoins. Cette approche centrée sur l'utilisateur augmente la probabilité d'acceptation et réduit les frictions lors de l'adoption de mesures de sécurité.

Amélioration continue : L'adoption et le management du changement sont des processus continus qui impliquent de recueillir des commentaires et d'ajuster les stratégies en fonction des expériences du monde réel. Cela permet aux entreprises d'affiner leurs pratiques de sécurité en réponse à l'évolution des menaces et des besoins des utilisateurs.

Canaux de communication : Une communication efficace est essentielle pour favoriser la confiance et la transparence dans les initiatives de cybersécurité. L'adoption et le changement. le management fournit des moyens de dialogue ouvert entre les équipes de sécurité et les utilisateurs, en s'assurant que les préoccupations et les malentendus sont traités

Atténuer les menaces internes : En favorisant un sentiment d'appartenance et de loyauté parmi les collaborateurs, l'adoption et le management du changement peuvent aider à réduire la probabilité de menaces internes, lorsque les collaborateurs compromettent intentionnellement ou non la sécurité.

Encourager la responsabilité : Les processus de management du changement mettent l'accent sur la responsabilité individuelle et collective de la sécurité. Lorsque les utilisateurs se sentent responsables de leurs actions, ils sont plus susceptibles de respecter les protocoles de sécurité et de signaler rapidement les incidents potentiels.

S'adapter aux nouvelles technologies : Le paysage de la cybersécurité évolue rapidement, avec l'émergence fréquente de nouvelles technologies. L'adoption et le management du changement aident les utilisateurs à s'adapter à ces changements en fournissant une formation et un support, garantissant l'utilisation sécurisée des nouvelles technologies dès le départ.

Conclusion

Les personnes représentent le plus grand risque de sécurité pour une organisation et doivent être formées régulièrement et efficacement pour devenir des gardiens efficaces de la sécurité de votre organisation. Une personne bien formée peut être la dernière ligne de défense contre une violation qui a échappé à vos contrôles techniques et basés sur les processus.

Une formation annuelle traditionnelle de sensibilisation à la sécurité est quelque chose que personne n'attend – et si une organisation consacre aussi peu d'efforts à la sécurité qu'à composer une vidéo et une poignée de questions, il n'est pas surprenant que les employés adoptent la même approche en matière de sécurité. Réfléchissez à quelques-unes des meilleures pratiques suivantes lors de la définition de vos facteurs humains dans la stratégie de sécurité.

Méthodes et techniques de formation :

- Utiliser la gamification et la concurrence pour augmenter le désir de participation des individus.
- Les interventions de formation doivent être régulières et brèves – pensez à 10 minutes par semaine plutôt qu'à une heure par an pour une formation générale de sensibilisation à la sécurité.
- Utilisez les tests pour vous assurer, au niveau organisationnel, que vos objectifs de maturité sont atteints et pour fournir un retour d'information instantané aux participants sur le fait qu'ils apprennent le matériel.
- Pensez à la fois à l'autonomisation individuelle très ciblée axée sur les compétences techniques et aux exercices en équipe pour tester les processus et les compétences de travail en équipe.

Communication et engagement :

- Parler aux gens dans leur langue locale et dans le bon ton peut être aussi important que le contenu.

Gestion des incidents :

- Votre stratégie doit prendre en compte tous les profils, de l'utilisateur informatique occasionnel à l'administrateur de sécurité le plus technique de votre organisation. Ils ont tous un rôle à jouer dans le maintien de la sécurité.

Inclusion dans la sensibilisation à la sécurité :

- Your strategy should consider all personas, from the occasional IT user to the most technical security administrator in your organisation. They all have their part to play in maintaining security.

L'aspect humain de la stratégie de sécurité d'une organisation n'est pas seulement une formalité ; c'est un facteur essentiel qui peut faire la différence entre être sécurisé et être exposé. Comme nous l'avons montré, de l'utilisation de méthodes de formation modernes à l'assurance de la diversité, il est vital de créer une approche globale qui reconnaisse l'importance de l'humain. En nous concentrant sur l'apprentissage continu, une communication efficace, un management solide des incidents et en incluant tous les rôles au sein d'une organisation, nous construisons la base d'une posture de sécurité résiliente. À mesure que la technologie évolue et que les menaces deviennent plus avancées, c'est la personne bien formée, consciente et engagée qui constituera une barrière solide contre les violations possibles. L'adoption et le management du changement garantissent que les actions, les politiques et les technologies de sécurité sont parfaitement intégrées dans la culture et les pratiques quotidiennes d'une organisation. Il change la perspective de la simple prise de conscience au changement de comportement pratique, créant une culture de la sécurité proactive. Ce changement entraîne moins d'opposition, soutient l'amélioration continue et renforce la responsabilité des collaborateurs. À mesure que le paysage de la cybersécurité évolue, il devient crucial de suivre le rythme des nouvelles technologies. Le management du changement veille à ce que les organisations s'adaptent et s'épanouissent au milieu de ces changements en utilisant de nouveaux outils de manière sûre et efficace.

Étapes suivantes

En comprenant votre risque organisationnel, en choisissant les bonnes technologies et plateformes pour le parcours d'apprentissage et en les intégrant dans vos processus commerciaux, Insight peut vous aider à créer et à mettre en œuvre un facteur humain cohérent dans la stratégie de cybersécurité. Nous pouvons également suivre et améliorer l'adoption au fur et à mesure que le déploiement progresse. Contactez nos consultants en sécurité ou nos experts en adoption et en management du changement pour plus d'informations.

- **fr.insight.com**
- **0130672500**