FORMATION GÉRÉE DE SENSIBILISATION À LA CYBERSÉCURITÉ

La mise en place d'un programme de sensibilisation va bien au-delà d'un simple achat de produit. Il est primordial d'instaurer une stratégie cohérente avec votre entreprise et le niveau de maturité en cybersécurité de vos ressources.

La principale porte d'entrée des cybercriminels est indéniablement les collaborateurs/employés de votre entreprise. Ils sont la première ligne de défense de votre entreprise, il est donc nécessaire de les former et de les sensibiliser régulièrement.

Notre offre de sensibilisation est un service clé en main proposé par des experts certifiés en sécurité et qui s'échelonne sur 12 mois. Cette offre comprend une évaluation de vos ressources à l'aide de questionnaires adaptés, vidéos de formation et de trois campagnes de phising réparties durant l'année.

ESTIMATION DU SERVICE GÉRÉ SUR 12 MOIS :

Très petite entreprise	Petite à moyenne entreprise	Moyenne à grande entreprise
5 jours	**7 jours**	**Variable**

Une phase de qualification et d'introduction doit être effectuée afin de garantir les livrables et la durée réelle.

CE QUE L'OFFRE INCLUT:

- → Analyse pour une bonne compréhension de vos enjeux d'affaires.
- → Plan de communication pour une sensibilisation adaptée.
- → Questionnaires adaptés et basés par groupe segmenté pour établir la maturité des usagers.
- → Plan de formation adapté en fonction des comportements et des réponses aux questionnaires de vos usagers.
- → Trois campagnes de phishing réparties sur 12 mois.
- → Rapport sur les questionnaires et campagnes pour mesurer la progression.

PRÉREQUIS POUR L'OFFRE:

- → Solution de sensibilisation à la cybersécurité de NOVIPRO
- → Disponibilité d'un interlocuteur (Responsable TI ou RH)

Vos usagers savent-ils reconnaitre les dangers et les cyberattaques?

LES ÉTAPES DE LA FORMATION GÉRÉE DE SENSIBILISATION À LA CYBERSÉCURITÉ

SEMAINES 1 À 4

- → Analyser votre entreprise pour déterminer le type de questions et de campagnes de phishing à réaliser.
- → Déterminer si des regroupements sont appropriés.
- → Rédiger un premier plan de communication interne en collaboration avec le client. Celui-ci devra le transmettre à l'interne.
- → Présentation des différents contenus de communication à personnaliser et afficher à l'interne.
- → Transmettre le questionnaire aux usagers pour évaluer leurs niveaux de connaissance.

APRÈS 1, 5 ET 10 MOIS

Une campagne de phising interne contrôlée est déployée afin d'évaluer le progrès et d'optimiser la formation aux employés:

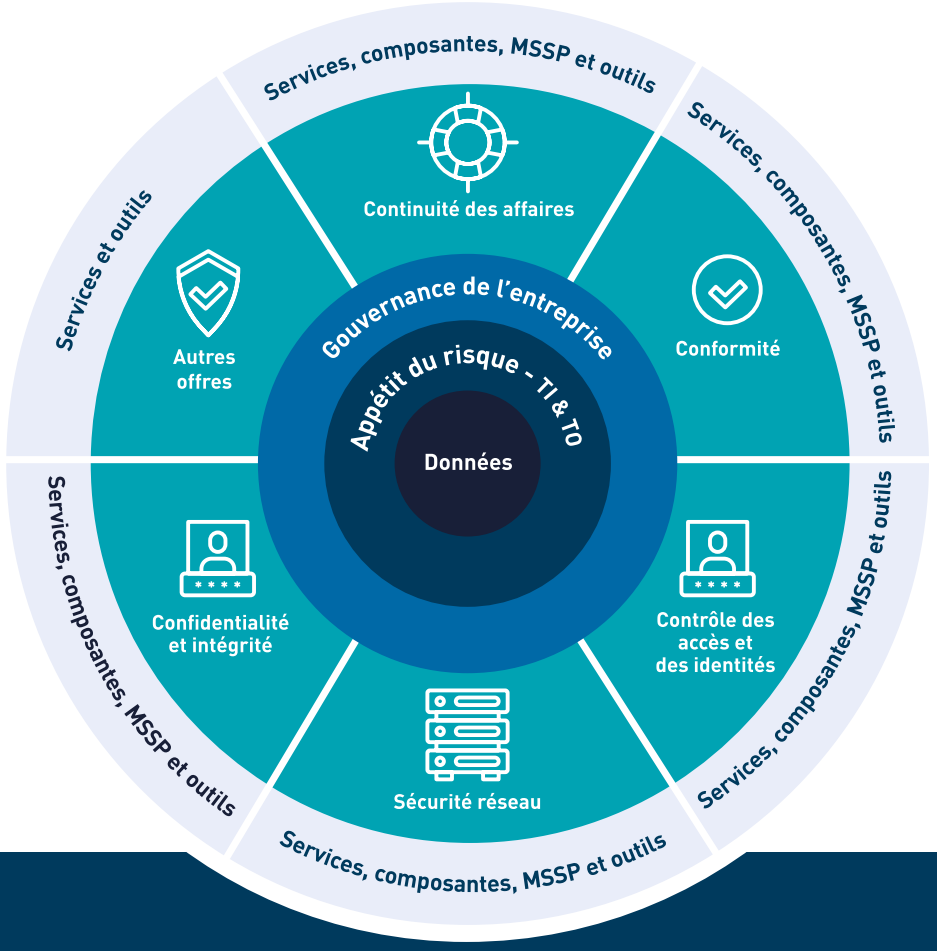
- → Simulation d'attaques de phishing sur une durée de 5 jours.
- → Analyses des résultats des questionnaires et de la simulation.
- → Présentation des résultats.
- → Création d'un plan de formation basée sur les résultats.

LIVRABLES

- Sensibilisation à l'échelle de votre organisation
- Évaluation des connaissances
- Matériel et vidéo de formation adapté
- Trois simulations d'attaques de phishing
- Analyses et rapports

L'ÉCOSYSTÈME DE L'OFFRE SÉCURITÉ DE NOVIPRO

NOVIPRO met l'expertise de son équipe sécurité à votre service afin d'assurer la protection de votre entreprise. De la gestion des politiques et procédures à l'élaboration d'un plan de continuité des affaires en passant par tous les aspects et composantes liés à la sécurité, NOVIPRO est en mesure de répondre à l'ensemble de vos besoins.



DES EXPERTS DE HAUT NIVEAU

L'équipe d'experts de NOVIPRO est composée de CISO, conseillers, analystes et spécialistes techniques. NOVIPRO respecte les recommandations du Disaster Recovery Institute International (DRI), des méthodologies Zero Trust de Forrester (ZTX), ISO 27001 et Cobit qui encouragent les meilleures pratiques pour évaluer et gérer les risques informatiques et assurer la continuité des affaires.

PLANIFIEZ UNE RENCONTRE

NOVIPRO | NOVIPRO.COM