Cyber Attack and Readiness Evaluation : CARE

Êtes-vous réellement prêts à faire face aux cybermenaces ?

Cybersecurity and Privacy

www.pwc.ch/care

pwc

La cybersécurité chez PwC : nous nous concentrons sur les risques

Cyber Attack & Readiness Evaluation : CARE

Outil d'évaluation de votre état de préparation face aux cyber-risques

CARE est un nouveau service développé par PwC afin d'aider nos clients à évaluer leur dispositif de sécurité, c'est-à-dire leur capacité à faire face efficacement aux principales menaces de notre cybermonde.

Comment fonctionne CARE ? Dans un premier temps, nous évaluons, au cours d'un atelier, votre tolérance au risque et les mesures en place pour diminuer votre exposition aux principaux cyber-risques. Nous confrontons ensuite les résultats avec une évaluation technique de votre état de préparation.

S'il s'adresse principalement aux petites et moyennes entreprises, ce service modulaire peut être facilement adapté à toute entreprise, quels que soient sa taille et son secteur d'activité. Notre service est reconnu et apprécié d'un grand nombre d'entreprises, y compris des administrations publiques, des banques et l'industrie du luxe.

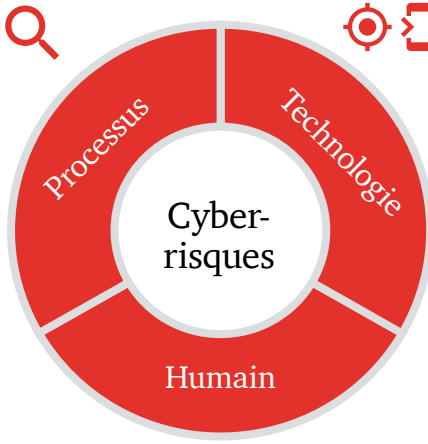
Notre approche modulaire inclut cinq services couvrant les trois dimensions de la cybersécurité :

Les processus sont au centre de toute entreprise.

Notre service :
- Évaluation des cyber-risques

La cybersécurité et la technologie sont étroitement liées.

Nos services :
- Scan de vulnérabilité
- Test d'intrusion (pentest)



Souvent présenté comme le maillon faible de la cybersécurité…

l'humain, s'il est correctement formé, est un élément clé de la résilience.

Notre service :
- Campagne de sensibilisation à l'hameçonnage
- Atelier de sensibilisation aux cyber-risques pour les dirigeants

---

Évaluation des cyber-risques

La démarche

Connaître les risques avant qu'ils ne causent des dégâts

L'objectif de l'évaluation des cyber-risques est d'identifier tout problème potentiel avant qu'il ne survienne. Cela vous permet de planifier des mesures de réduction des risques et de les appliquer au besoin à vos systèmes d'information et/ou vos projets.

Durant cette phase, nous vous soumettons un questionnaire en ligne afin d'évaluer votre exposition aux risques et la maturité de vos contrôles de sécurité. Nous avons basé nos contrôles sur la Norme minimale pour les TIC publiée par l'Office fédéral pour l'approvisionnement économique (OFAE).

Les résultats

Recommandations pragmatiques

- Un rapport contenant une liste exhaustive des cyber-risques critiques et un résumé de votre niveau de maturité actuel
- Pour le périmètre défini, un rapport détaillé au format électronique qui sera préparé spécifiquement pour vous et qui fera l'objet d'une présentation aux différents membres de votre entreprise
- Un plan d'action incluant les activités planifiées pour chaque phase du projet dès la phase initiale de mobilisation

Scan de vulnérabilité

La démarche

Quels sont les points d'entrée les moins bien sécurisés ?

Un scan de vulnérabilité externe est une solution facile à mettre en œuvre afin d'identifier rapidement les failles de votre réseau susceptibles d'être exploitées par des pirates informatiques.

Les résultats

Définition de tâches claires et d'une feuille de route pour votre Département IT

Vous recevrez un rapport complet contenant une liste des vulnérabilités connues découvertes durant l'analyse. Ce rapport fournira également un aperçu des étapes requises pour remédier à ces faiblesses (par exemple les mesures correctives à appliquer).

Test d'intrusion

La démarche

Infiltration !

Alors que le scan de vulnérabilité détecte une faille mais ne l'exploite pas, le test d'intrusion cherche à démontrer l'existence d'une vulnérabilité en l'exploitant. Le test d'intrusion dévoile la profondeur du problème et révèle quels dommages pourraient être causés si une telle vulnérabilité était exploitée.

Les résultats

Observations et recommandations

Nous délivrons un rapport pragmatique listant nos observations et recommandations, y compris les « quick wins ». Le rapport décrit la méthodologie utilisée durant l'exercice d'intrusion, les hypothèses retenues et l'impact de l'attaque sur l'activité de l'entreprise.

Campagne de sensibilisation à l'hameçonnage

La démarche

Défier le « maillon faible »

L'hameçonnage est une méthode très répandue chez les pirates informatiques pour mettre un premier pied dans le réseau d'une entreprise. Son taux de réussite est élevé car il s'attaque au maillon le plus faible de la chaîne de sécurité : le comportement des utilisateurs ! Notre campagne de sensibilisation simule une attaque d'hameçonnage par l'envoi d'un courriel vraisemblable à un groupe défini de personnes en leur demandant d'effectuer une action particulière (par exemple cliquer sur un lien ou ouvrir une pièce-jointe). Cette action pourrait compromettre le poste de la victime ou l'inciter à divulguer des informations confidentielles.

Les résultats

Un rapport détaillant comment moins se faire hameçonner

Chaque action effectuée par le groupe test sera enregistrée et répertoriée dans un rapport.

Ce dernier décrira les actions de vos employés (par exemple nombre de personnes ayant cliqué sur le lien, ouvert la pièce-jointe et fourni leurs identifiants). Vous pourrez ainsi jauger leur niveau de sensibilisation et/ou estimer les effets de précédents efforts de sensibilisation.

Atelier de sensibilisation aux cyber-risques pour les dirigeants

La démarche

Sensibilisation des dirigeants

Devant l'évolution rapide de la nature des cyber-risques, les dirigeants d'entreprises et les cadres doivent être régulièrement tenus au courant des dernières technologies et des principaux développements en matière de cyber-risques.

Notre session Game of Threats™ les aidera à comprendre, tester et simuler une attaque réaliste à l'aide de notre outil interactif.

Les résultats

Rapport de sensibilisation

Vous recevrez une présentation résumant les points principaux des observations faites lors des activités pratiques.

Notre approche modulaire

Nous avons conçu un service adaptable et évolutif afin que nos services correspondent au mieux à vos besoins et à la taille de votre entreprise. Le niveau d'évaluation technique et humaine dont vous aurez besoin dépendra de la profondeur d'analyse requise, de votre expérience et de vos connaissances de la cybersécurité. Construisons ensemble ce qu'il vous faut !

	Processus	Technologie	Humain
Basique	Évaluation des cyber-risques > Questionnaire en ligne > Atelier avec nos experts en cybersécurité	Évaluation de la sécurité des applications Web (Black box) > Évaluation d'une petite application web/e-commerce dédiée	Simulation d'hameçonnage « cliquez et téléchargez » > Jusqu'à 50 employés
Avancé	Évaluation des cyber-risques > Questionnaire en ligne > Plusieurs ateliers avec nos experts en cybersécurité, y compris des ateliers avec vos fournisseurs dans le domaine de l'informatique/sécurité informatique.	Évaluation de la sécurité des applications Web (Grey box) > Évaluation d'une application de taille moyenne telle qu'un système e-banking ou de traitement de paiements ou un CRM/ERP de taille moyenne	Simulation d'hameçonnage « cliquez et téléchargez » > Jusqu'à 100 employés
Étendu	Évaluation des cyber-risques > Questionnaire en ligne > Atelier avec nos experts cybersécurité > Test des contrôles de sécurité basés sur la Norme minimale pour les TIC	Évaluation de la sécurité des applications Web (White box) > Grand site Web avec des systèmes CRM complexes ou des applications Web basées sur SAP/Oracle/ Microsoft	Simulation d'hameçonnage « cliquez et téléchargez » > Jusqu'à 250 employés Atelier de sensibilisation aux cyber-risques pour les dirigeants > Game of Threats™

Contacts

Contactez-nous pour dresser un premier état des lieux. Nous trouverons comment vous aider à cerner vos besoins et à évaluer vos risques afin de mieux vous y préparer.

Yan Borboën
Partner
Cybersecurity and Privacy
+41 58 792 84 59
yan.borboen@pwc.ch

Urs Küderli
Partner
Cybersecurity and Privacy
+41 58 792 42 21
urs.kuederli@pwc.ch

Benoit de Jocas
Senior Manager
Cybersecurity and Privacy
+41 58 792 96 10
benoit.de.jocas@pwc.ch