

IMMERSION DANS LE JEU GAME OF THREATS

QUAND LES ENTREPRISES PEUVENT JOUER AUX PIRATES

Et si votre société était cyber-attaquée? Qu'advierait-il de vos données, de vos ressources et de vos dossiers parfois confidentiels? Comment éviter ces agressions informatiques et comment les contrer si elles surviennent? PwC a imaginé un «serious game» qui sensibilise aux menaces du cyber-piratage.

Voilà une façon originale de prendre conscience des risques qui menacent la protection de vos données. Ce jeu immerge complètement les participants dans le monde des petits génies de l'informatique. *Trends-Tendances* a joué le jeu, sans arme ni bagage. *Welcome to the Game of Threats!*

Servir et protéger

Le cabinet PwC est connu pour les prestations de consultance qu'il propose aux entreprises publiques et privées dans 157 pays à travers le monde. En se spé-

cialisant dans les services de conseils, de fiscalité et d'audit, le géant américain peut compter entre autres Pepsi et la Deutsche Bank parmi ses clients. Pour maintenir la qualité de leurs services, les équipes de PwC mettent à jour, entre autres, plusieurs défis à relever. La «cyber-sécurité» en fait partie. Selon les spécialistes de PwC, 65% de la criminalité économique en Belgique est informatique et deux tiers des compagnies sont attaquées avec succès. Plus surprenant encore: le plus grand danger pour les sociétés vient de la crédulité de leurs employés. Sans s'en rendre compte, ils auront tendance

à ouvrir un e-mail ou à cliquer sur un lien qui constitue en réalité une menace pour tout le système informatique de leur compagnie. Dès lors, le cabinet de conseil a choisi d'aller au-delà de la prévention traditionnelle et a mis sur pied Game of Threats. Un véritable jeu interactif et éducatif destiné aux postes à responsabilités des sociétés.

Dans la peau d'un pirate informatique

Avant de démarrer la partie, les joueurs (entre quatre et 14) sont invités à former deux équipes. Certains représentent une

compagnie fictive, les autres deviennent les «hackers». Parmi eux, plusieurs profils sont possibles: Etats, organismes de crime organisé, *hacktivistes* (tels que les Anonymous) ou traîtres en interne. Selon le profil d'attaquants choisi, les «cartes» disponibles varient et les ressources financières diffèrent. Une fois les rôles distribués, les équipes prennent possession de leur tablette et la bataille peut commencer. L'objectif? Rendre l'adversaire inoffensif.

Dès que le coup de feu est lancé, les équipes sélectionnent tour à tour une carte virtuelle parmi celles proposées sur leur tablette. Chaque carte aura un impact sur l'adversaire et sur les ressources de l'équipe. Par exemple, dans le cas où les apprentis pirates choisissent de lancer une attaque DoS (*Denial of service*), qui rend un service indisponible au sein de l'entreprise fictive, cette dernière pourra choisir de réagir en investissant dans une infrastructure de sécurité plus solide ou en analysant l'ensemble de son réseau. Plusieurs possibilités, d'attaque ou de réponse, sont présentées aux joueurs, selon la situation. Dès qu'un choix de carte est validé par une équipe, son impact est affiché en temps réel sur un grand écran, visible par tous. Cette mise à jour en continu permet aux deux équipes d'évaluer laquelle d'entre elles est en position de force.

Avant de démarrer la partie, les joueurs (entre quatre et 14) sont invités à former deux équipes...

...Certains représentent une compagnie fictive, les autres deviennent les «hackers». Parmi eux, plusieurs profils sont possibles: Etats, organismes de crime organisé, «hacktivistes» ou traîtres en interne.

Game of Threats est configuré de telle manière qu'il récompense les bonnes décisions des deux parties et pénalise les choix qui ne sont pas optimaux. Enfin, pour défendre ses intérêts, chaque camp doit réagir dans un laps de temps imparti. Lorsque nous avons participé, PwC avait prévu 90 secondes par tour.

Nous y étions!

Avant tout, nous pouvons le confirmer: Game of Threats est bel et bien un jeu! L'esprit de compétition prend très vite le dessus, exacerbé par le chronomètre qui tourne. Avec toute cette pression, on se sent véritablement responsable du cyber-avenir de l'univers (au moins) et on s'investit très vite dans la partie. Cependant, là où le temps qui file nous permet de garder un bon rythme, il peut aussi être handicapant pour ceux qui ne sont pas de petits génies de l'informatique. Certaines cartes virtuelles d'attaque ou de défense portent des noms savants pour désigner des outils techniques qu'on maîtrise encore moins bien qu'on ne les connaît. Cette carence en informations nous pousse alors à faire des choix guidés par l'instinct, donc pas toujours pertinents.

Un animateur de chez PwC est cependant présent aux côtés de chaque équipe.

Il a le droit de les conseiller rapidement, mais pas d'influencer concrètement ses choix. En somme, il est rassurant mais ne suffit pas à faire des joueurs des informaticiens hors pair.

Game of Threats est amusant et instructif, ça éveille les compétiteurs et ça sensibilise plutôt bien sur les dangers des cyber-attaques. On prend conscience de l'utilité d'un bon équipement de défense. Objectif principal atteint pour PwC, donc. Pour le reste, une rapide formation préliminaire sur les grandes lignes informatiques semble nécessaire pour pouvoir profiter pleinement de l'expérience.

Un workshop de trois heures

PwC a évidemment plus d'un tour dans son sac et organise des séances d'information dans le programme de ces *workshops*. Avant la session de jeu, l'entreprise de conseils prévoit une heure d'introduction théorique sur la cyber-sécurité dans le monde des affaires. Durant cette même heure, un médiateur de PwC explique le système de jeu et son objectif éducatif, en présentant les différentes étapes des deux équipes. Les joueurs sont ainsi un minimum armés pour affronter le cyber-combat.

A la fin du jeu, les animateurs de PwC discutent avec les participants pour évaluer leurs décisions stratégiques. Un graphique s'affiche alors sur l'écran principal, relatant les différentes étapes de la partie. Quelles décisions ont été bonnes, lesquelles ont affaibli l'équipe et en quoi les différents camps ont plus ou moins bien réagi. Ce feedback permet d'avoir un regard critique sur les stratégies, les actions et les opportunités manquées des deux équipes. Une jolie manière d'apprendre de ses erreurs. La piraterie, sans rhum ni moussaillon, n'a qu'à bien se tenir!

© LUCIE HERMANT



INFORMATIONS PRATIQUES

Game of Threats est destiné aux «C-level» (celui des cadres supérieurs) des entreprises. PwC étant une entreprise de conseils mais pas de produits, l'objectif reste bien de sensibiliser les utilisateurs aux risques des cyber-attaques, sans promouvoir de solutions ou de produits commerciaux. Pour un budget d'environ 6.000 euros, PwC propose trois heures d'activité qui comprennent l'introduction, le jeu et une courte formation des choses essentielles à retenir. Comparable à du *team building*, le *serious game* permet également d'analyser le comportement de ses collègues ou employés en situation de stress. Très populaire aux Etats-Unis, Game of Threats est proposé partout en Europe.