08.12.2015 – 10:00 Uhr

PwC : Des cyberattaques grandeur nature

Zurich (ots) -

PwC lance en Suisse l'atelier interactif « Game of Threats[TM] - simulation de cyberattaques ». Cela consiste pour des cadres à tester, par des simulations réalistes, leur capacité de réaction à des cyberattaques soudaines.

GoT, ce sigle, pour une fois, ne désigne pas la célèbre série « Game of Thrones » mais l'atelier interactif « Game of Threats[TM] - simulation de cyberattaques » que vient de créer PwC et dans lequel des cadres responsables ressentent à fleur de peau, en quelque sorte, comment fonctionnent des cyberattaques.

Une approche duale : piratage et défense

Game of Threats[TM] simule des scénarios réalistes de cyberattaques, tant du point de vue de l'entreprise cible que de celui de l'assaillant. Ainsi, les participants à l'atelier sont d'abord répartis en deux groupes: l'entreprise et le pirate. Les acteurs censés défendre l'entreprise testent dans l'urgence leur capacité de réaction face à des cyberattaques soudaines. Les assaillants, une fois n'est pas coutume, changent de camp et, mués en pirates, exploitent les failles de sécurité de l'entreprise. Les rôles sont intervertis en cours d'atelier.

« Game of Threats[TM] teste aussi les compétences décisionnelles des cadres en leur proposant une approche quasi-réaliste », résume Jan Schreuder, responsable de la cybersécurité chez PwC Suisse. « En cours de jeu, les acteurs doivent traiter quantité d'informations en un minimum de temps, puis investir dans les bonnes décisions avec des ressources limitées. C'est cette pression qui confère son aspect extrêmement réaliste à la confrontation avec la cyberattaque. »

Sensibilisation aux menaces cybernétiques

L'atelier a pour but non seulement de tester la capacité de réaction des cadres mais encore de les sensibiliser aux menaces cybernétiques. En ce sens, les participants apprennent à assimiler les étapes suivantes dans la préparation la mieux adaptée aux attaques :

- identification des cybercriminels ainsi que de leurs méthodes et stratégies préférées ;
- évocation des mesures de sécurité personnelles à prendre face à des cyberattaques ;
- perception claire des conséquences financières, prudentielles et, surtout, dommageables en termes de réputation, d'une cyberattaque ;
- compréhension claire des éventuelles mesures préventives à prendre et des infrastructures à mettre en place ;
- compréhension claire des éventuelles mesures d'assainissement à prendre après une attaque ;
- perception claire des tendances et de la terminologie dans le domaine de la cybersécurité.

Contact:

Jan Schreuder
Responsable Cyber Security, PwC Suisse
http://ch.linkedin.com/in/janschreuder1
jan.schreuder@ch.pwc.com

Claudia Sauter
Head of PR & Communications, PwC Suisse
http://ch.linkedin.com/in/claudiasauter
claudia.sauter@ch.pwc.com