Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2015)
Heft: 2

Artikel: Red Teaming : Interview avec Uri
Autor: Uri / Garcia, Yves
DOI: https://doi.org/10.5169/seals-781255

Cyber

Red Teaming : Interview avec Uri

Uri

Propos receuillis par Yves Garcia, Rédacteur adjoint RMS+

Pourriez-vous vous présenter ?

J'ai commencé ma carrière en tant que pentester[1]. *En raison de certaines circonstances, j'ai choisi de rejoindre l'armée où j'ai passé du temps dans une unité combattante. Lorsque j'ai finalement quitté l'armée, j'ai réalisé que j'avais l'opportunité de combiner ce que j'avais appris au cours de mes années en tant que* pentester *avec l'intensité du* stress *lié au monde du combat urbain. Donc aujourd'hui, je combine les différents aspects du* Red Teaming *(numérique, physique et social) afin d'appréhender la sécurité de manière plus approfondie.*

Qu'est-ce qu'un / le *Red Team/ing* ?

Pour faire simple, un Red Team *est un groupe de professionnels hautement qualifiés qui défient en permanence les plans, mesures défensives et concepts de sécurité d'une organisation en simulant un adversaire. En d'autres termes : il s'agit d'un groupe de personnes hautement qualifiées qui agissent comme des attaquants.* Red Teaming *est l'art de penser comme un adversaire. Tout cela permet une meilleure compréhension de quelles sont les vulnérabilités et aide à comprendre ce que vos adversaires potentiels pourraient faire.*

D'où cela vient-il ?

Historiquement, un Red Team, *ou équipe rouge, était un groupe de militaires jouant le rôle de l'adversaire, le rôle de l'ennemi, de l'équipe adverse par opposition aux équipes amies, ou équipes bleues. Avec le temps, la mission et les capacités des* Red Teams *ont évolué et ils se transformèrent en une force chargée de contester la posture de sécurité des bases militaires, des avant-postes et d'autres « cibles ». Pensez «* Red Cell. *»*

Le *Red Teaming* est utilisé dans divers environnements critiques. Qui d'autre que les communautés militaires et celles du renseignement pourrait en bénéficier ?

A la fin des années 1980 et au début des années 1990, les sociétés de manière générale ainsi que les entreprises high-tech *en particulier ont cherché un moyen de tester leur sécurité afin de voir si elles étaient vulnérables aux attaques auxquelles elles n'auraient pas pensé. Les premiers* Red Teams *civils étaient pour la plupart des professionnels de l'information et/ou de la sécurité informatique mélangés avec des experts de la sécurité physique qui se concentraient principalement sur les possibilités que la technologie d'alors permettait. Les procédures des organisations étaient revues mais ce n'était pas l'objet de l'exercice des* Red Teams.
Aujourd'hui, les Red Teams *ont évolué et sont une force importante dans le monde de la sécurité. Les gouvernements comme les organisations privées utilisent des* Red Teams, *non seulement pour tester l'état actuel de leur sécurité physique et digitale mais aussi afin de défier en permanence les plans, mesures défensives, concepts et politiques de sécurité.*
Essentiellement, tout le monde peut bénéficier du red teaming.

Que je sois une agence de marketing ou une unité de forces spéciales, y a-t-il des conditions générales afin d'utiliser efficacement le *Red Teaming* ?

Tout dépe*nd de l'équipe et de son chef. Une bonne équipe doit être petite et fluide. Avoir une bonne équipe solide avec des membres qui viennent d'horizons différents et un leader qui comprend le projet et ses besoins est la clé. De petites équipes, comme dans les forces spéciales à travers le monde, peuvent s'adapter plus rapidement à la réalité sur le terrain.*

1 NdlR : Un pentester est une personne en charge de surveiller la sécurité d'un système informatique pour éviter qu'il ne soit piraté. Le mot vient de l'anglais «*pentest*» qui est la contraction de «*penetration test*», soit test d'intrusion. http://www.linternaute.com/dictionnaire/fr/definition/pentester/

Qu'en est-il du *Red Teaming* et de la cyber-défense/attaque? Je vois deux côtés: la pénétration physique et la pénétration digitale. Sont-ils deux côtés de la même médaille ou pas nécessairement?

*Comme je le vois, ils font partie d'un tout. J'ai l'habitude de parler de mondes différents: digital (*cyber*), physique et social. Attaquez n'importe lequel d'entre eux séparément et peut-être que cela marchera. Attaquez-les ensemble et vous allez certainement faire une différence.*

U.

Soldat des opérations spéciales de la Marine U.S. dans la province d'Helmand, Afghanistan, 2013. Photo © USN.