Cyberdéfense : l'humain au cœur de l'efficacité opérationnelle

Mettre à l'épreuve son dispositif de défense est indispensable pour progresser

Par **Vincent RIOU**
Directeur associé Cybersécurité, CEIS

Mais comment se fait-il que les meilleures technologies de détection et de prévention des attaques, combinées avec les meilleures sources de Threat Intelligence, le tout utilisé par une équipe de lutte informatique défensive dédiée échouent encore et encore à stopper des attaques avancées ? Comment se fait-il que nous assistions à une explosion des vols de données massifs alors que les budgets cyber ne cessent d'augmenter ? La réponse est simple. Dans un contexte de cyberguerre totalement asymétrique, le défenseur sera mis en échec si, après avoir arrêté des milliers d'attaques, il n'en laisse passer ne serait-ce qu'une seule. À l'inverse, l'attaquant, après avoir été bloqué des centaines de fois, sera gagnant pour une seule attaque réussie. Le jeu est totalement déséquilibré.

Dès lors, faut-il encore et encore augmenter son budget cyber et accumuler dans son réseau les « boîtes magiques » tant vantées par le marketing des éditeurs ? Le nombre de sociétés ayant subi une attaque majeure malgré des millions d'euros dépensés en outils de sécurité divers montre qu'il ne suffit pas de dépenser plus pour limiter son risque. Il faut dépenser mieux. Pour vous en convaincre, engagez une équipe de *Red Team* et observez par où ils rentrent dans vos réseaux (certainement pas par la grande porte blindée !), comment ils bougent latéralement, comment ils effacent leurs traces, comment ils leurrent vos *cyber magic tools* achetés à grands frais, le tout sans se faire une seule fois détecter par le SOC[(1)]… Pendant ces tests *Red Team*, les outils du SOC reçoivent des dizaines d'alertes, voire des centaines. Le problème est que ce sont principalement des faux positifs, ou des leurres sciemment orchestrés par l'attaquant pour faire « sonner » le SOC et occuper l'attention des équipes en dehors des zones privilégiées par l'attaquant. Ces faux positifs créent dans les équipes du SOC une fatigue latente et une baisse d'attention et de motivation, qui conduisent inexorablement à l'inefficacité d'un dispositif censé traiter des attaques « avancées ».

Dès lors, posons-nous la question. Avant de réinvestir dans de nouveaux outils miracles, n'est-il pas grand temps d'apprendre à utiliser à pleine capacité les moyens dont nous disposons déjà ? L'importance de l'entraînement et de la préparation des troupes, de la connaissance de ses forces et de ses faiblesses, l'anticipation des stratégies de l'ennemi, la dissimulation, le leurrage… Tout est dans *L'Art de la guerre.* Ouvrage toujours cité, rarement appliqué…

Se mettre à l'épreuve pour progresser

Plus qu'en suivant des principes normatifs génériques, il faut appréhender sa cybersécurité du point de vue de l'attaquant : *Red Team,* entraînement opérationnel, exercice de crise. Cela demande du courage à une organisation de se mettre à l'épreuve, mais c'est la clé du succès.

(1) *Security Operation Center* ou Centre d'Opérations de Sécurité.

Les conséquences d'une attaque informatique réussie sont dramatiques : image écornée, pertes financières, rançonnage, vol de données, arrêt d'une exploitation, voire danger majeur pour les populations, si l'attaque vise une infrastructure sensible. Cette tribune n'a pas vocation à égrener les chiffres, ils sont connus. Elle s'attellera à ouvrir une piste fondamentale pour circonscrire le phénomène : la mise à l'épreuve et l'entraînement.

À un premier niveau, des opérations de sensibilisation en entreprise permettent aux employés, quelles que soient leurs compétences techniques, de connaître les fondamentaux des comportements à adopter. C'est ce que l'ANSSI appelle l'« hygiène informatique ». À l'image des règles de sécurité sanitaire, un entraînement régulier s'impose, afin de créer des automatismes. Ainsi, il conviendrait de créer de manière récurrente des exercices de crise cyber touchant une large part des employés, afin de les sensibiliser aux risques. Un employé averti en vaut deux, et le coût du montage de tels exercices est largement amorti par la diminution du risque induit par les bons réflexes créés à tous les niveaux de l'entreprise.

L'entraînement des professionnels de la cybersécurité d'une entreprise ou société de service spécialisée doit, lui, aller bien plus loin. Afin d'acquérir et de conserver les réflexes indispensables à ces métiers, les professionnels doivent se former, puis s'entraîner en permanence. Dans un parallèle avec la sécurité physique, on n'imagine pas le GIGN ou le RAID partir en mission sans un entraînement préalable d'une intensité telle qu'elle amène ses personnels à agir de manière réflexe, avec une extrême efficience une fois sur le terrain. Ils évaluent l'ensemble des comportements possibles de l'attaquant et préparent la contre-offensive en fonction. Confrontées à une attaque de grande ampleur, les équipes de réponse aux incidents informatiques doivent, elles aussi, être préparées. Plus que des fiches réflexes, il faut des actes réflexes.

Formation *vs* entraînement

On distingue la formation de l'entraînement par le caractère immersif de ce dernier. La formation va permettre de développer des compétences théoriques selon une démarche pédagogique adaptée. L'entraînement, quant à lui, consiste à effectuer une mise en situation dont le niveau de difficulté sera corrélé au niveau de compétence du professionnel. Là où la formation permet de connaître les techniques de base composant la boîte à outils du cyber-défenseur, l'entraînement permet de les maîtriser par la mise en pratique, afin d'augmenter la qualité et la vitesse d'exécution et de diminuer le stress en situation réelle. C'est l'entraînement qui permet d'acquérir les réflexes vitaux en cas d'agression et d'augmenter son efficacité.

« Plus je m'entraîne et plus j'ai de la chance », disait Arnold Palmer. En effet, l'efficacité opérationnelle ne dépend pas seulement de la somme de connaissances amassée souvent de manière trop théorique. Elle résulte, au contraire, de mécanismes réflexes qui ne peuvent s'acquérir que par la pratique intensive. Le vocabulaire et les modes d'actions de la cyberdéfense s'apparentent beaucoup aux sports de combat : attaque, défense, parades, feintes, anticipation, réflexes, endurance… Un parallèle également évident avec le monde militaire, où nos soldats doivent maîtriser armement, tactiques et modes opératoires sur le bout des doigts avant de partir en opération. Ceci est d'autant plus vrai que les moyens de cyberdéfense, évoluant au rythme des nouvelles techniques d'attaque et des avancées technologiques, deviennent de plus en plus complexes et donc difficiles à maîtriser, ce qui renforce le besoin d'un entraînement régulier.

On peut, dès lors, faire le lien avec les qualités nécessaires à un compétiteur sportif, ces qualités devant s'acquérir par un entraînement régulier :

- Le relâchement : conserver son sang-froid est indispensable quand l'attaque survient. Toute crispation est synonyme d'une baisse d'efficacité. Le relâchement permet de diminuer la

pression et le stress, permettant un état d'esprit propice à la diminution du temps de réaction et à l'augmentation de la qualité des réponses aux attaques.

- Des techniques adaptées : souplesse, vivacité, adaptation au contexte. La réponse à incident nécessite une palette de techniques large, qu'il faut acquérir préalablement à la survenue d'un incident important. Celle-ci doit être la plus exhaustive possible. D'où la nécessité d'une mise à jour de ses capacités de défense régulière par des entraînements et des stages ciblés, en environnement simulé.
- La diminution du temps de réaction : outre l'expérience du terrain, seul un entraînement réaliste permet de diminuer ce temps de réaction, crucial pour la qualité d'une réponse à une attaque et la limitation des dégâts induits. Au-delà des connaissances théoriques, la mise en pratique répétée permet d'automatiser la réaction, jusqu'à arriver à des actions « réflexes ».
- La multiplication des oppositions : un boxeur ne progressera plus s'il s'entraîne constamment avec le même partenaire. Au contraire, sa courbe de progression sera maximale s'il varie les entraînements (sac de frappe, musculation, cibles mobiles, partenaires différents, travail de vitesse…). Il en va de même en cyberdéfense. Il faut se confronter à des attaques larges et variées, dans des contextes opérationnels différents, avec des outils différents, pour aiguiser ses sens et optimiser une réaction qui se veut avant tout humaine, même si elle est fortement soutenue par la technologie.
- La focalisation de son attention : en opération, lorsqu'une attaque survient, il est essentiel de pouvoir faire abstraction des stimuli parasites, de gérer son effort, et de bien réagir aux commandements de la chaîne de décision. Cela ne s'acquiert pas en théorie, mais bien par la pratique.

À ces qualités personnelles, il convient de rajouter les qualités collectives, car la cyberdéfense est un travail d'équipe. Chaque acteur de la chaîne de défense a un rôle particulier et complémentaire. On peut faire le parallèle avec les qualités d'une équipe de rugby ou de football. Les qualités individuelles s'additionnent alors par la mise en œuvre de stratégies collectives, par la solidarité et l'entraide, l'optimisation de la chaîne de décision, l'initiative au service du collectif, la qualité du reporting, le respect des rôles et des règles…

Pour être efficaces, ces entraînements collectifs et individuels doivent être réguliers. En effet, les menaces informatiques sont en constante évolution, et un « expert » du domaine ne le reste jamais longtemps s'il se repose sur ses acquis. De nouvelles techniques d'attaques sont perpétuellement développées dans le monde cybercriminel. Il faut donc en permanence se préparer pour limiter l'effet de surprise et les dégâts induits par les attaques. Le rôle de la *Cyber Threat Intelligence* est alors mis en avant, à raison. Encore ne faut-il pas se contenter d'intégrer les tactiques et procédures d'attaque constatées par le passé, mais anticiper comment elles pourraient être adaptées par l'ennemi.

La formation et l'entraînement s'adaptent ainsi au niveau et aux besoins requis, de la sensibilisation à l'entraînement intensif, des « gestes qui sauvent » en cas d'agression, à l'entraînement d'un « cyberdéfenseur » professionnel.

Une entreprise peut décider de mettre en place un processus de formation et d'entraînement interne, basé sur les compétences à sa disposition, ou choisir de faire appel à un centre professionnel de formation et d'entraînement à la cyberdéfense, à l'image de *bluecyforce* en France, qui dispose de moyens très importants d'immersion dans le réalisme d'une cyber-crise et de méthodes pédagogiques adaptées.

En effet, bien s'entraîner impose de disposer de moyens importants pour renforcer le réalisme de l'immersion. On ne progresse efficacement que par l'action. Reprenons notre parallèle sportif. Pour améliorer ses performances, le boxeur amateur va s'inscrire dans une salle, où il trouvera

l'ensemble du matériel adapté à sa pratique : rings, sacs de frappe, poire de vitesse, partenaires d'entraînement, professeurs… Les cours seront adaptés à son niveau, le faisant progresser d'étape en étape, par la confrontation avec des adversaires de plus en plus forts. Le tout dans une ambiance ludique et agréable, mêlant challenge physique, mise sous pression puis détente, afin d'améliorer autant le mental que le physique.

Il en va de même pour la formation et l'entraînement à la cyberdéfense.

Le ring et tous les accessoires d'entraînement ? Un environnement fermé et contrôlé, intégrant de larges topologies réseaux, des flux de données réalistes et des systèmes d'information simulés, permettant de mener des attaques de tous niveaux d'intensité, en toute sécurité, sans risque de propagation incontrôlée.

Les partenaires d'entraînement ? Une *Red Team,* hackers éthiques professionnels et expérimentés, dont le niveau des attaques s'adaptera au niveau des stagiaires, afin de ne pas les « noyer sous les coups » mais, au contraire, de les faire progresser.

Les poings, les gants, les yeux, les muscles du boxeur ? L'ensemble de moyens techniques de la chaîne de lutte informatique défensive : WAF, SIEM, EDR, firewalls, sondes de détection, outils de forensique… Autant de moyens qu'il ne faut pas se contenter d'implémenter dans leur environnement informatique, mais bien de maîtriser dans un contexte d'ensemble cohérent.

À tout cela s'ajoute un paramètre essentiel de l'entraînement : la « ludification ». Sous forme de jeux, l'entraînement doit aboutir à une implication totale, à la provocation d'une montée de stress qu'il faudra apprendre à contrôler, à des enjeux forts qu'il faudra défendre. La qualité des scénarios proposés est donc partie intégrante de la pédagogie, tout comme la complémentarité des profils des « entraîneurs » des futurs champions de la cyberdéfense.

Leurrer l'ennemi : la cybersécurité déceptive

L'épreuve des équipes de défense face à une *Red Team* aguerrie nous amène naturellement à définir de nouvelles stratégies de réponse. Comment combattre un ennemi furtif, agile, qui s'adapte, qui n'a à suivre aucun carcan légal ou règlementaire ? Les actions contre-offensives étant interdites dans notre législation, il faut piéger l'ennemi. C'est le concept de Cybersécurité déceptive. Leurrage, dissimulation, déception… autant de stratégies de contre-mesures bien connues du monde de la Guerre électronique, qu'il nous faut nous réapproprier dans le cyberespace, afin de ne pas laisser l'attaquant serein par une posture de défense passive, uniquement basée sur la détection et la remédiation des incidents. Pour le moment, nos entreprises les plus matures se croient à l'abri derrière de hautes murailles, tandis que l'ennemi apprend à voler…

L'entraînement des équipes opérationnelles, les exercices de crise et la confrontation à une équipe *Red Team* sont de véritables épreuves du feu. Elles seules sont en mesure de qualifier l'efficacité réelle d'une stratégie de cybersécurité, tout en faisant progresser l'ensemble de la chaîne de défense.

Se confronter, se réadapter, ne pas se contenter de suivre les normes, ne pas faire confiance aux seuls outils de cybersécurité pour se défense. À tous niveaux, l'humain est au cœur de l'efficacité opérationnelle.