Comment sélectionner un fournisseur de tests d'intrusion

Introduction

Les tests d'intrusion constituent une part importante de la capacité de gestion des menaces et des vulnérabilités d'une équipe en charge de la sécurité. De nombreux responsables de la gestion du risque et de la sécurité s'appuient sur les tests d'intrusion comme mécanisme de vérification indépendant pour évaluer leurs contrôles et l'environnement informatique de leur entreprise.

Les résultats de ces tests sont utilisés à plusieurs fins, comme l'indiquent les clients de Gartner ; par exemple :

 pour contribuer à l'élaboration de programmes d'amélioration de la gestion du risque et de la sécurité (si le responsable est nouveau dans l'entreprise, par exemple) ;
 pour valider l'efficacité des capacités et contrôles de sécurité (à l'aide d'un exercice en équipe rouge, par exemple) ;
 dans le cadre des activités continues de gestion des vulnérabilités et des menaces (par exemple, évaluation des plates-formes et des applications prenant en charge de nouvelles initiatives cruciales).

Pour certaines entreprises, ces tests sont obligatoires, par exemple pour répondre aux impératifs de la norme de sécurité des données de l'industrie des cartes de paiement.

D'autres entreprises peuvent avoir besoin de tests d'intrusion afin de se conformer à une norme spécifique de gestion de la sécurité des informations, comme les normes de l'Institut national des normes et de la technologie (NIST) ou du Center for Internet Security (CIS).

Les tests d'intrusion peuvent englober un large éventail d'activités et de résultats. Les clients de Gartner qui utilisent des tests d'intrusion se concentrent généralement sur des tests de réseaux externes et internes, ainsi que sur des applications web internes cruciales et externes.

Plus récemment, les tests des réseaux sans fil sont devenus plus courants, parfois pour répondre à des impératifs réglementaires tels que la norme de sécurité des données de l'industrie des cartes de paiement , de même que des tests physiques, en fonction du secteur vertical de l'entreprise (par exemple, les services publics ou la vente au détail). Des tests portant spécifiquement sur l'hameçonnage et l'ingénierie sociale sont quelquefois réalisés.

Les tests avec équipe rouge gagnent en visibilité sur le marché, ce qui ne fait que semer la confusion chez les acheteurs.

Pourquoi cette confusion ? Parce que les tests avec équipe rouge semblent très similaires à ce qui peut être commercialisé en tant que test d'intrusion de réseau « avancé », mais aussi parce que certains fournisseurs adoptent ce terme pour se différencier sur le marché.
La réalité est que le principe de l'équipe rouge est similaire, mais néanmoins différent des tests

traditionnels d'intrusion du réseau. Certains fournisseurs proposent légitimement l'un ou l'autre ou les deux types de tests, tandis que d'autres ne font en réalité que des tests d'intrusion du réseau et abusent de l'utilisation du terme « équipe rouge ».

Gartner définit les tests d'intrusion comme « allant au-delà de l'analyse des vulnérabilités pour utiliser des scénarios d'attaque à multiples étapes et vecteurs, qui d'abord trouvent les vulnérabilités et ensuite tentent de les exploiter pour pénétrer plus en profondeur dans l'infrastructure de l'entreprise » .

Le principe de l'équipe rouge peut se décliner en plusieurs styles qui incluent des tests d'intrusion plus avancés à une extrémité du spectre jusqu'à un exercice de jeu de guerre où les attaques contre une entreprise et ses défenses de sécurité par des adversaires sont émulées par les testeurs. Les caractéristiques qui différencient ces tests incluent des durées d'engagement plus longues (des semaines au lieu de jours), moins de limites autour de vecteurs d'attaque particuliers (apps web, hameçonnage, hameçonnage vocal, physique), les armes utilisées (nouveau code malveillant exploitant une faille de sécurité ou programmes malveillants et implants personnalisés) et un effort accru pour éviter la détection. Cela peut inclure des tests d'intrusion de type boîte noire et boîte grise. Ces caractéristiques se reflètent également dans le prix, car ces tests imposent un surcoût en raison de la durée de l'engagement, de la préparation requise et de l'expertise employée.

La sélection d'un fournisseur de tests d'intrusion peut être un défi colossal en raison du grand nombre d'entreprises offrant ces services. Une recherche sur Google de « tests de pénétration » révèle des centaines de prestataires de services qui varient à bien des égards, comme la taille de l'entreprise (et des effectifs), l'emplacement géographique, les années d'expérience et la réputation.

Ainsi, les prestataires peuvent aussi bien être de grands cabinets de conseil ayant des bureaux partout dans le monde que des prestataires régionaux de services de sécurité personnalisés, ou encore des individus travaillant à domicile. L'expérience des testeurs varie entre des vétérans qui ont effectué des centaines de tests d'intrusion et des individus récemment agréés qui ont décidé de lancer une activité de tests de pénétration.

Il est important de noter qu'une plus grande taille ou reconnaissance de la marque mondiale n'équivaut pas nécessairement à de meilleurs résultats lorsqu'il s'agit de tests de pénétration.

De plus, le nombre d'années d'expérience n'est pas forcément un bon indicateur pour les technologies émergentes (telles que les environnements de cloud computing) ou les cas d'utilisation pour lesquels une expertise de niche est requise (par exemple, les tests d'environnements SCADA ou de systèmes de contrôles industriels).
L'expérience du testeur est par conséquent un facteur clé.

De nouvelles approches des tests d'intrusion sont également apparues sur le marché.

Pour les tests d'intrusion de type boîte noire, les options en crowdsourcing se sont développées sur le marché. Ces tests sont dispensés par des fournisseurs qui agissent au titre du prestataire de tests d'intrusion sous contrat et qui soumettent le travail à des testeurs agréés une fois que l'acheteur a enregistré le type de test requis.
Les plates-formes de ces fournisseurs visent à optimiser le temps des testeurs d'intrusion en

automatisant une grande partie des activités de gestion de projet et de collecte d'informations, ce qui laisse aux testeurs plus de temps pour réaliser les tests ; elles offrent en outre aux acheteurs un plus grand vivier de testeurs. Elles peuvent également raccourcir le temps qu'il faut à un acheteur pour identifier et planifier un test, ce qui est devenu un aspect problématique pour les acheteurs de tests de pénétration.
Le délai nécessaire pour planifier un test auprès des prestataires de tests d'intrusion peut en effet atteindre au minimum 10 jours ouvrables. Dans certains cas, il est même impossible de planifier un test avant plusieurs semaines, selon le degré d'occupation du prestataire au moment où le test est requis.

Des outils de simulation d'attaque et de violation de la sécurité et des outils de tests d'intrusion automatisés sont disponibles.

Les outils de simulation d'attaque et de violation de la sécurité visent à fournir une surveillance en temps réel et une évaluation de la surface d'attaque de l'environnement informatique d'une entreprise. Ces outils mettent en évidence les ressources présentant le risque le plus fort qui pourraient être compromises par un attaquant et ensuite exploitées pour se déplacer latéralement au sein du réseau d'une entreprise. Il existe aussi des outils qui tentent d'automatiser entièrement un testeur humain d'intrusion en utilisant une boîte à outils et un ensemble de techniques et de tactiques d'attaque pour effectuer un test d'intrusion du réseau.

Pour tester les applications web et mobiles, il existe désormais des programmes de primes aux bugs (à la fois privés ou fermés et ouverts aux modèles publics). Les primes aux bugs sont différentes dans le sens où vous, le client, ne payez que pour les problèmes ou vulnérabilités confirmés qui sont trouvés, et non pour les heures passées sur une cible.
Cette prestation s'effectue également selon un modèle de crowdsourcing, si bien qu'au lieu d'un seul consultant, il peut y avoir des douzaines de personnes qui travaillent sur votre cible de test.

Analyse

Avant de commencer le processus de sélection d'un fournisseur, vous devez comprendre les types, la portée et les objectifs des tests de pénétration.

Une fois que l'équipe chargée de la sécurité et les principales parties prenantes se sont mises d'accord sur les objectifs et la portée du test d'intrusion et les ont documentés, les impératifs et les limites doivent être définis, acceptés et documentés. Ceux-ci précisent comment un fournisseur doit procéder pour atteindre les objectifs du test dans le respect de la portée convenue.

Les impératifs doivent être établis à partir de la portée et des objectifs, conjointement avec la contribution des parties prenantes concernées, notamment les responsables d'applications d'entreprise et de l'infrastructure informatique. De plus, les dirigeants en dehors du département informatique doivent signifier leur tolérance au risque concernant leurs opérations, en lien avec la portée et les objectifs de l'exercice, car les tests pourraient avoir une incidence négative sur les opérations.

Voici des exemples de questions auxquelles vous devez répondre lorsque vous définissez vos

impératifs et les limites du test (notez que plusieurs de ces questions se recoupent, alors considérez la liste dans son ensemble).

 Quels types de ressources (appareils, hôtes et applications) sont explicitement dans la portée et lesquels sont hors limites pour le fournisseur de tests ? Sont-ils en permanence hors limites ou seulement certains jours ou à certaines heures ? Les ressources qui sont hors limites varient généralement selon le type de test. Les évaluations légères et ciblées (tests de boîte blanche et de boîte grise) spécifient généralement les ressources hors limites, tandis que les tests d'intrusion standard (tests de boîte noire) et les exercices avec équipe rouge en auront peu, voire aucune. Si le style avec équipe rouge est préféré, l'objectif est-il ou pas d'être furtif et non détectable par l'équipe bleue ?

 Y a-t-il des restrictions sur la période de fonctionnement ? Par exemple, si un test d'intrusion standard doit être effectué, voulez-vous qu'il ait lieu uniquement les jours ouvrables et pendant les heures de bureau, de sorte que, si une exploitation provoque la défaillance d'une application ou d'un serveur, le personnel informatique soit disponible pour rétablir les opérations normales ? Y a-t-il des périodes d'interruption normales imposées par l'entreprise (par exemple, pendant les périodes de vacances pour les détaillants) pendant lesquelles les tests ne doivent pas avoir lieu ?

 Selon le type de test de pénétration, quel niveau de risque quant à la disponibilité et l'intégrité des ressources concernées par le test votre entreprise est-elle prête à accepter lorsque le testeur utilise des codes malveillants réels exploitant une faille de sécurité ? Si un test d'intrusion standard doit être effectué, votre entreprise acceptera-t-elle l'utilisation de codes malveillants réels pour atteindre les objectifs du test ? Il est en outre important de vérifier auprès du fournisseur de quelle façon il applique et surveille les limites pendant les tests.

 Le testeur devra-t-il se trouver physiquement dans vos locaux ou le télétravail sera-t-il acceptable ? Comment l'accès (physique et à distance) sera-t-il accordé, surveillé et révoqué à la fin du test ? Le fournisseur doit-il déployer ses propres ressources, comme une machine virtuelle ou un ordinateur portable physique sur votre réseau pour faciliter les tests d'intrusion internes ? Habituellement, le type de test détermine l'emplacement du testeur. Un test d'intrusion contre un système ou une application spécifique peut nécessiter un accès intégral à votre réseau interne. Cela ne sera pas forcément le cas pour la simulation d'une attaque provenant de l'extérieur du périmètre réseau de votre entreprise.

 Quels environnements les testeurs sont-ils censés utiliser ? Par exemple, les environnements de développement ou de tests uniquement, ou bien tous les environnements, y compris de production ? Le type de test d'intrusion utilisé peut orienter le choix de l'environnement. Par exemple, un test de boîte grise contre une nouvelle plate-forme et une nouvelle application qui ne sont pas encore exposées à l'extérieur peut être réalisé sur des versions de préproduction.

 Quel est le plan de signalement progressif ? Il n'est pas toujours approprié de s'en remettre aux communications par messagerie électronique et aux réunions ; vous avez besoin d'un plan détaillé de communication et de signalement progressif. Les deux parties doivent s'entendre sur une politique « sans hypothèses », par exemple, si un système ne répond plus, si une vulnérabilité importante est découverte ou s'il y a la preuve d'une violation de la sécurité. Les communications doivent être faites en temps opportun et être précises dans leurs détails (par exemple, ce qui s'est

produit, ce qui a été identifié, la gravité du problème, si une violation est active ou s'il y a indication d'une activité passée et quels artefacts témoignent d'une violation).

 Quel degré d'indépendance êtes-vous prêt à donner au fournisseur de tests ? Il est crucial de comprendre ce point. L'autorisez-vous à utiliser des techniques d'ingénierie sociale (par exemple, le hameçonnage de messages électroniques et d'appels téléphoniques) ? Accorderez-vous un accès physique pour atteindre les objectifs du test ? Plus vous donnez d'autonomie à un prestataire, plus le risque est élevé, mais plus les résultats sont susceptibles d'être précis.

Une fois que vous avez documenté vos objectifs, votre portée, vos impératifs et vos limites, dressez une liste restreinte de fournisseurs de tests de pénétration. La taille des prestataires varie entre des consultants individuels et des cabinets de conseil internationaux.

Pour identifier des fournisseurs potentiels auxquels recourir, les sources ne manquent pas : recommandations de pairs, relations existantes avec des prestataires de services informatiques et des cabinets de conseil, fournisseurs expérimentés dans des réglementations spécifiques telles que la norme de sécurité des données de l'industrie des cartes de paiement, ou encore fournisseurs associés à des programmes de certification et d'accréditation afférents tels que CREST et Tigerscheme. Une fois que vous avez une liste restreinte de fournisseurs, il est recommandé de lancer un appel d'offres.

En introduction de l'appel d'offres, les objectifs, la portée et les limites du test doivent être stipulés. Il est également important d'être très précis et de fournir suffisamment de détails pour qu'un fournisseur puisse déterminer s'il peut atteindre vos objectifs et opérer dans le cadre de vos limites. Certains consultants et cabinets sont susceptibles de refuser un engagement en fonction de ces facteurs. Par exemple, certains cabinets ne veulent effectuer que des tests d'intrusion standard à distance et ne disposent pas des ressources nécessaires pour réaliser des tests sur site.

Votre objectif est d'émettre un appel d'offres qui permette, dans la mesure du possible, une comparaison cohérente des points forts et des points faibles des fournisseurs. Donnez-leur une certaine latitude pour expliquer leur différenciation, mais formulez les questions de sorte à obtenir des réponses claires.

Appel d'offres : quatre parties fondamentales

Votre appel d'offres doit comporter quatre parties fondamentales, qui sont décrites plus en détail ci-après :

1. les détails de votre entreprise, les informations de base pertinentes, les moteurs de l'engagement, ainsi que la portée et les objectifs du test d'intrusion ;

2. les impératifs et limites (ou « garde-fous ») pertinents ;

3. les questions spécifiques auxquelles les fournisseurs doivent répondre dans leur réponse à l'appel d'offres ;

4. les informations et questions standard sur l'appel d'offres, notamment le format de la réponse à

l'appel d'offres, les coordonnées de contact, les renseignements commerciaux, les références de clients et la date d'échéance pour les réponses.

La première partie doit inclure de brèves informations de base sur votre entreprise et les moteurs de l'engagement. Soyez aussi précis que possible dans le cadre de ce que votre entreprise peut accepter de partager à l'extérieur. Il s'agit d'un élément important du document qui est souvent négligé lors de l'élaboration de l'appel d'offres.

La deuxième partie doit comporter une description des objectifs et de la portée de l'engagement. Une fois ceux-ci énoncés, les limites de l'engagement doivent être décrites. Ensuite, fournissez une liste numérotée de vos impératifs spécifiques, comme le télétravail ou la présence physique et les heures de test autorisées (par exemple, entre 18 h et 6 h). Documentez clairement les méthodes de communication. De plus, il est nécessaire d'être très clair sur les impératifs susceptibles de limiter la capacité d'un testeur à respecter ses méthodologies et pratiques (par exemple, lorsque les impératifs dictent les outils ou l'hôte à utiliser pour effectuer les tests).

Il est également important de définir une date d'achèvement prévue pour l'engagement, à laquelle le testeur doit remettre au plus tard un rapport final et des recommandations. Même si les attaquants ont un temps quasiment infini, un test d'intrusion doit être limité dans le temps, car les entreprises n'ont pas des budgets illimités. Si l'engagement est susceptible d'inclure de nouveaux tests, indiquez clairement le nombre de tests supplémentaires requis, ainsi que les critères de décision et d'autorisation s'y rapportant.

La troisième partie doit comporter des questions visant à cerner les capacités des fournisseurs et à faciliter leur comparaison. Vous trouverez ci-après des suggestions de questions.

Les paragraphes commençant par « Remarque » fournissent des explications supplémentaires sur la question ou la demande et doivent être supprimés si vous reprenez textuellement les questions du présent document.
Nous recommandons également que les questions portant sur le personnel, la méthodologie des tests, la gestion de l'engagement et les rapports soient obligatoires : les réponses à ces questions seront essentielles pendant la phase de comparaison et de sélection finale.

À qui allez-vous attribuer cet engagement ? Quelles sont les compétences, l'expérience et les qualifications des testeurs qui seront désignés ? Quel est le nombre moyen d'années d'expérience par testeur ? Veuillez fournir des biographies en compléments.

Remarque : les tests d'intrusion standard et ciblés sont principalement pilotés par les attributs du testeur, et non par les outils et méthodes utilisés. Il est important de passer en revue les capacités des collaborateurs qui sont employés par le fournisseur comme facteurs de différenciation. Le fournisseur doit être en mesure de comprendre les impératifs du test (si ce n'est pas le cas, il doit vous demander des éclaircissements) et de savoir qui il va désigner.

Recherchez des testeurs qui ont plusieurs années d'expérience et, éventuellement, des certifications reconnues telles que celles de CREST, du programme de certification mondiale en assurance de l'information (GIAC) et d'Offensive Security. Pour les engagements portant sur des tests d'intrusion standard, il vaut la peine de passer quelques minutes à chercher en ligne pour voir si les collaborateurs du fournisseur sont des membres visibles de la communauté de la sécurité

des informations.
Par exemple, font-ils des présentations lors de conférences et publient-ils des exploitations de failles ? Sont-ils crédités pour avoir découvert des vulnérabilités ? Tiennent-ils un blog sur leurs recherches ? Si un fournisseur n'indique pas à ce stade qui il affectera à votre engagement, assurezvous de lui demander une liste finale du personnel, avec la possibilité d'approuver toute substitution avant de signer un accord.

Comment validez-vous vos collaborateurs ? Faites-vous appel à des ressources à l'extérieur du pays ?
Remarque : les fournisseurs doivent vérifier régulièrement les antécédents du personnel qui effectue les tests de pénétration. Toutefois, la nature et la régularité de ces contrôles varient selon les pays, car les lois diffèrent. Déterminez si le recours à des ressources à l'extérieur de votre pays crée des problèmes de conformité aux politiques ou de responsabilité pour votre entreprise.

Combien de tests manuels, par opposition aux tests automatisés, effectuez-vous habituellement ?
Remarque : les tests initiaux utilisent généralement des outils automatisés pour cartographier un réseau et recueillir des informations détaillées sur les cibles potentielles, mais, selon la portée et les limites du test, un bon fournisseur peut se fier davantage à des tests manuels. La quantité de tests manuels est susceptible d'influer sur la durée et le coût de l'engagement, de sorte que les différences de coûts entre les fournisseurs peuvent s'expliquer notamment en comprenant les proportions relatives des tests manuels et automatisés.

Décrivez vos expériences et donnez des exemples de vos engagements, incluant des objectifs similaires.

Décrivez vos expériences avec des entreprises et des environnements informatiques de taille similaire.

Vos rapports sont-ils rédigés par les testeurs eux-mêmes ou par des rédacteurs dédiés ? Utilisez-vous un modèle standard ou le format des rapports est-il propre à chaque engagement ? Le rapport contient-il un résumé, une description technique détaillée des constatations, des conseils en matière de mesures correctives et une liste des méthodologies et des outils utilisés et des tests effectués ? Les résultats sont-ils contextualisés dans une approche basée sur le risque, y compris le niveau de complexité requis pour corriger une vulnérabilité ? Des enregistrements sont-ils mis à disposition pour démontrer comment une exploitation a été réalisée ? Donnez des exemples de rapports concernant des engagements similaires.

Remarque : cela fait partie des questions les plus importantes à poser. Il est en outre essentiel que le fournisseur produise des rapports concrets (avec des détails expurgés, si nécessaire). Le rapport final sera le produit que vous recevrez et sur lequel vous vous appuierez pour déterminer si l'engagement a atteint ses objectifs.

Comment allez-vous gérer l'engagement ? Comment allez-vous communiquer les mises à jour de l'état et les constatations au client au cours de l'engagement ?
Remarque : il est important de gérer l'engagement comme un projet. La tenue de réunions

régulières, voire quotidiennes, au cours de l'engagement pour traiter les problèmes ou les constatations urgentes et de réunions hebdomadaires pour évaluer les progrès contribuera à la réussite de l'opération.

Signez-vous des accords de confidentialité ? Comment stockez-vous en toute sécurité les données des clients afin d'éviter toute divulgation non autorisée ? Quelles sont les périodes de conservation des données brutes et des rapports ? Qui est autorisé à consulter les résultats, aussi bien chez le fournisseur que le client ?
Remarque : le fournisseur collectera des informations sur vos ressources informatiques, en particulier les hôtes, les appareils de sécurité, les réseaux et les applications. Plus important encore, il enregistrera les vulnérabilités et les points faibles. Il est de la plus haute importance que le fournisseur accepte de garder confidentielles toutes les informations, qu'il dispose de processus et d'outils en place pour protéger vos informations et qu'il les détruise après une période donnée. Les fournisseurs doivent offrir cette protection à leurs clients.

Fournissez deux ou trois références de clients concernant des engagements ayant une portée et des objectifs similaires.
Remarque : les clients qui fournissent des références ne doivent pas nécessairement être des clients de référence officiels auxquels vous pouvez parler, mais leurs références doivent vous permettre de confirmer que le fournisseur a réalisé un travail similaire avec des clients de taille similaire dans la même industrie ou une industrie semblable. Si vous pouvez parler aux clients qui fournissent des références, saisissez cette opportunité.

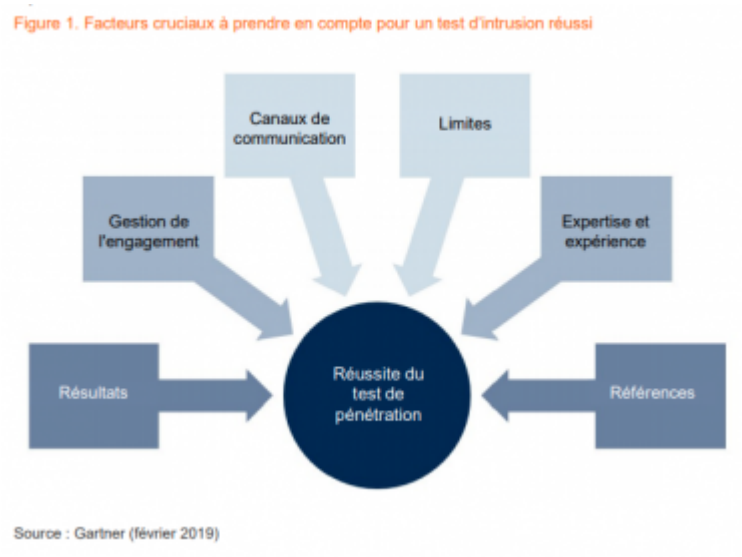
Quel est le coût estimé de cet engagement ? Veuillez fournir une ventilation des coûts totaux par jour et par heure (entre les ressources s'il existe des taux différents pour différentes compétences, par exemple pour les testeurs ou les chefs de projets). Si l'engagement dure plus longtemps que prévu, comment les ordres de modification sont-ils traités et quel est le tarif pour le temps d'engagement supplémentaire (par jour et par heure) ?

La dernière partie du processus consiste à envoyer l'appel d'offres, ainsi que les documents d'achats standard de votre entreprise, à une sélection gérable de fournisseurs potentiels (pas trop nombreux, mais suffisamment pour que l'analyse des réponses à l'appel d'offres soit possible sans trop de difficultés).

Les clients de Gartner qui font appel à des services de tests d'intrusion choisiront entre trois et cinq fournisseurs pour leur liste restreinte. Sachez que, même après avoir choisi un fournisseur, certaines entreprises conservent une réserve d'autres fournisseurs, en fonction de leurs atouts et de leurs spécialisations (par exemple, les tests d'applications web et la simulation d'attaques). Selon le type de test, elles pourront faire appel aux services de ces autres fournisseurs si leur fournisseur principal n'est pas en mesure d'effectuer un test dans les délais requis, ou bien pour obtenir des perspectives différentes.

L'étape suivante consiste à analyser les réponses des fournisseurs à l'appel d'offres.
Concentrez vous sur les facteurs de sélection cruciaux pour obtenir un test d'intrusion réussi (voir la figure 1). Examinez ensuite leurs réponses aux autres questions, car elles ajouteront du contexte aux réponses cruciales.

Figure 1. Facteurs cruciaux à prendre en compte pour un test d'intrusion réussi



Résultats

Passez en revue les exemples de rapports et tout autre document supplémentaire. Demandez-vous quels fournisseurs ont transmis des rapports prédéfinis, plutôt que des rapports qui sont plus orientés sur votre engagement. Le contenu des rapports est-il suffisamment détaillé ? Les informations fournies sont-elles utiles ? Sont-elles suffisamment détaillées pour aider à classer par ordre de priorité la correction des points faibles, aussi bien immédiatement qu'à long terme ? Avez-vous la possibilité d'influer sur le format du rapport ou de sortie du fournisseur, ou bien devez-vous accepter sa version par défaut ? Quels fournisseurs sont prêts à travailler selon vos besoins et dans le respect de vos limites ?

Gestion de l'engagement et canaux de communication

Considérez également de quelle façon l'engagement sera géré. Existe-t-il une ressource dédiée à la gestion du projet pour soutenir les testeurs, ou bien les testeurs sont-ils également chargés de gérer l'engagement ? Les canaux et la cadence de communication sont-ils adaptés à la complexité de l'engagement ? Par exemple, si les testeurs causent un impact présumé sur votre environnement ou s'ils trouvent la preuve d'une violation active ou passée, les deux parties

sauront-elles comment et à qui le signaler ? Il s'agit là d'éléments cruciaux qui doivent être documentés dans la réponse du fournisseur et/ou l'énoncé des travaux.

Expertise et expérience

Il n'est pas recommandé de sélectionner un fournisseur uniquement en fonction du coût. L'adage « vous en avez pour votre argent » s'applique également au choix d'un fournisseur de tests de pénétration.

Concentrez-vous d'abord sur la qualité de la réponse et du travail du fournisseur, ainsi que sur sa capacité à atteindre les objectifs, puis comparez les prix. Lorsque vous comparez les prix, portez une attention particulière au nombre de jours alloués à l'évaluation, à la gestion du projet et à la génération de rapports. Les différences dans le nombre de jours alloués à ces activités expliquent souvent pourquoi les prix des fournisseurs divergent considérablement. Si le nombre de jours que les fournisseurs prévoient pour mener à bien l'engagement varie considérablement d'un fournisseur à l'autre, discutez-en avec eux.

Prenez conscience que le temps consacré à l'évaluation est crucial ; une durée d'engagement sensiblement plus courte peut indiquer un test moins approfondi. Par exemple, une plus grande part d'automatisation peut être utilisée pour tenter de découvrir plus de vulnérabilités afin de démontrer la valeur au client, alors même que ces vulnérabilités peuvent être de faible valeur et cacher le fait que des vulnérabilités plus importantes n'ont pas été découvertes.