Brochure de la solution

SOPHOS

SERVICES DE CONSEIL SOPHOS

Tests de pénétration

Valider les défenses de sécurité à l'aide de méthodes d'attaque simulées en conditions réelles

Identifiez les vulnérabilités et validez les défenses de sécurité en vous appuyant sur une expertise indépendante, une expérience et des stratégies conçues sur mesure pour améliorer votre posture de sécurité, réduire les risques, faciliter la mise en conformité et améliorer votre efficacité opérationnelle.

Renforcer de manière proactive les défenses et la posture de sécurité

L'accès non autorisé aux ressources de l'entreprise, l'exploitation des vulnérabilités existantes et émergentes, l'utilisation de configurations incorrectes et le contournement des politiques de sécurité insuffisantes sont autant de menaces sérieuses pour la sécurité. Pouvoir vérifier que les applications, les réseaux et les systèmes ne sont pas exposés à un risque de sécurité est essentiel pour pallier ces vulnérabilités avant qu'elles ne puissent être exploitées par des attaquants. Si les analyses et l'évaluation des vulnérabilités sont un moyen « léger » d'identifier les failles et vulnérabilités de votre réseau, des tests et validations plus approfondis sont nécessaires pour montrer comment un attaquant pourrait s'introduire dans votre environnement et utiliser ces systèmes comme une rampe de lancement d'attaques plus profondes au sein du réseau.

Services Sophos de tests de pénétration

Les tests de pénétration, ou « pentests », permettent d'identifier et de mettre en évidence les failles de sécurité, et de répondre à la question : « Un attaquant pourrait-il s'introduire dans mon réseau ? » Ces tests simulent des cyberattaques réelles pour identifier les vulnérabilités des systèmes, des réseaux et des applications. Les testeurs expérimentés (hackers éthiques) tentent d'exploiter les vulnérabilités pour montrer ce qu'un attaquant pourrait réaliser.

Il existe deux grands types de tests de pénétration :

- **Test d'intrusion externe :** il se limite aux systèmes accessibles depuis Internet : sites Web, VPN, services publics, etc. Il simule une tentative d'intrusion dans votre périmètre depuis l'extérieur.
- **Test d'intrusion interne :** il simule une menace interne ou un attaquant qui s'est déjà introduit, en se concentrant sur les systèmes, les applications et les données au sein du réseau interne.

Sophos Approche chaque test de pénétration de manière unique, car il doit être adapté aux besoins spécifiques de chaque organisation. Notre méthodologie axée sur les objectifs est mise en œuvre par les meilleurs testeurs de sécurité de l'industrie. Ils qui s'appuient sur nos tactiques et renseignements propriétaires fournis par Sophos X-Ops, notre groupe dédié au renseignement sur les menaces, qui comprend la Counter Threat Unit (CTU), réputée pour ses renseignements et ses recherches sur les menaces persistantes avancées (APT) et les attaquants soutenus par des États.

Avantages

- Gagnez en assurance en testant les contrôles de sécurité internes et externes, y compris les protections relatives aux systèmes et aux ressources de grande valeur.
- Atteignez des objectifs de test spécifiques grâce à un modèle de menace et à un contexte adaptés à votre environnement unique.
- Obtenez un plan d'action réalisable pour remédier à la situation.
- Assurez la mise en conformité réglementaire, y compris : PCI DSS, HIPAA, RGPD, NIS, ISO 27001, SOC 2.
- Obtenez des informations techniques par Sophos X-Ops, notre groupe dédié aux renseignements sur les menaces.
- Déterminez votre risque réel de compromission.

Simuler des attaques sophistiquées pour tester vos défenses

En effectuant régulièrement des tests de pénétration, les organisations ne cherchent pas seulement à se conformer aux réglementations du secteur, mais aussi à gérer de manière proactive le paysage des menaces de cybersécurité de plus en plus complexe et en constante évolution. En effectuant des tests de pénétration à intervalles réguliers, les organisations gardent une longueur d'avance sur les attaquants qui adaptent continuellement leurs techniques pour exploiter de nouvelles vulnérabilités. Des tests réguliers permettent également d'identifier les failles introduites par des changements apportés à l'infrastructure, aux applications ou aux intégrations tierces. En outre, ces tests offrent aux organisations une compréhension réaliste de leur exposition aux risques, ainsi que des stratégies de remédiation applicables et un moyen mesurable de suivre les améliorations apportées à la sécurité au fil du temps.

Les avantages des tests de pénétration :

- **Réduction proactive des risques :** les entreprises qui effectuent régulièrement des tests de pénétration voient une réduction de 50 % des incidents de sécurité et de 30 % du coût lié à la gestion des incidents de sécurité.[1]
- **Aide à la conformité :** les cadres réglementaires, tels que PCI DSS, HIPAA et ISO 27001 requièrent souvent des tests de pénétration. Pour 73 % des entreprises, la conformité est un facteur déterminant dans la conduite de tests de pénétration.[2]
- **Réduction des coûts :** le coût moyen d'une violation de données se chiffre à 4,45 millions de dollars[3], bien que de nombreuses vulnérabilités peuvent être corrigées pour une infime partie de ce coût grâce aux tests de pénétration.
- **Confiance des clients :** 65 % des consommateurs déclarent être plus enclins à faire confiance à une entreprise qui témoigne de solides pratiques en matière de cybersécurité.[4]

Mettre à l'épreuve votre personnel

Avec l'intelligence artificielle, les attaques de phishing sont de plus en plus sophistiquées et convaincantes, et de plus en plus difficiles à détecter. Contrairement aux emails de phishing traditionnels truffés d'erreurs grammaticales et de contenu vague, le phishing assisté par IA peut générer des messages personnalisés, contextuellement pertinents et taillés sur mesure pour des individus ou des entreprises spécifiques. De ce fait, les équipes de sécurité comme les utilisateurs doivent désormais apprendre à identifier les attaques de phishing et à s'en défendre, ce qui est loin d'être simple… D'où la nécessité d'une formation continue.

Notre programme de tests de pénétration peut être combiné à des simulations d'attaques de phishing afin d'évaluer la capacité de vos employés à repérer les tentatives de phishing et à y répondre.

Fonctionnalités du service

- Règles d'engagement sur mesure, y compris l'examen des systèmes cibles pour les données critiques de l'entreprise.
- Rapports finaux contenant des conclusions détaillées et un résumé.
- Possibilités de test sur place et à distance.
- Possibilité de sélectionner un test de pénétration externe, un test de pénétration interne et une session de simulation d'attaque de phishing, afin de créer un scénario de menace mixte adapté à votre cas d'usage spécifique.
- Opération manuelle pilotée par les testeurs, qui inclut le recours à des tactiques utilisées par de véritables attaquants.
- Méthodologie orientée sur les objectifs qui garantit que les systèmes sont testés dans le contexte plus large de leur environnement.

Ce qui est inclus dans le rapport

Résumé : destiné aux parties prenantes non techniques (direction, auditeurs, conseil d'administration et d'autres parties importantes).

Conclusions détaillées : rédigées pour que le personnel technique fournisse des conclusions et des recommandations approfondies.

Méthodologie de la mission : définit la portée de la mission et les activités de test qui ont été réalisées.

Descriptif : décrit la séquence d'actions entreprises par les testeurs pour atteindre les objectifs de la mission, pour aider à comprendre les menaces mixtes ou les phases dépendantes.

Recommandations : présente les résultats détaillés, des liens vers des pages Web pour approfondir le sujet et des recommandations pour remédier aux problèmes ou réduire les risques. Les testeurs fournissent des preuves de leurs constatations, le cas échéant, et, si possible, suffisamment d'informations pour reproduire les constatations à l'aide d'outils accessibles au public.

Résultats du phishing (le cas échéant) : détaille les attaques de phishing utilisées et leur taux de réussite.

Autres services de tests de cybersécurité

Aucune évaluation ou technique isolée ne saurait fournir une image exhaustive de la posture de sécurité d'une entreprise. Chaque test a ses propres objectifs et ses propres niveaux de risque acceptables. Sophos peut travailler avec vous pour déterminer quelle combinaison d'évaluations et de techniques utiliser pour évaluer votre posture de sécurité et vos contrôles.

En savoir plus:
sophos.fr/advisory-services

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2025-06-05 BRFR (MP)

SOPHOS