Services d'évaluation de la sécurité de Kaspersky Lab

www.kaspersky.fr
#truecybersecurity

Services d'évaluation de la sécurité

Services d'évaluation de la sécurité de Kaspersky Lab : services proposés par nos experts internes qui, pour la plupart, font autorité dans leur domaine au niveau mondial et dont les connaissances et l'expérience jouent un rôle essentiel dans notre réputation de leader mondial en matière de veille stratégique.

Chaque infrastructure informatique est unique et les cybermenaces les plus redoutables sont conçues sur mesure pour exploiter les vulnérabilités spécifiques à chaque organisation, c'est pourquoi nos experts proposent également des services sur mesure. Les services décrits dans les pages suivantes font partie de notre boîte à outils professionnelle. Ils pourront être utilisés, en partie ou en totalité, lors de notre collaboration avec vous.

Notre objectif premier est de travailler avec vous individuellement pour vous fournir des conseils spécialisés afin de vous aider à évaluer vos risques, renforcer votre sécurité et atténuer les effets des futures menaces.

Les services d'évaluation de la sécurité comprennent :

- des services de test de pénétration
- des services d'évaluation de la sécurité des applications
- une évaluation de la sécurité des DAB/points de vente
- une évaluation de la sécurité des réseaux de télécommunications

Toutes les entreprises sont confrontées à la difficulté de protéger entièrement leur infrastructure IT contre d'éventuelles cyberattaques, mais cette tâche s'avère d'autant plus compliquée pour les grandes entreprises avec plusieurs milliers de salariés, des centaines de systèmes d'information et plusieurs sites dans le monde entier.

Votre équipe informatique et vos spécialistes en sécurité travaillent d'arrache-pied pour s'assurer que toutes les composantes du réseau sont protégées contre les intrusions tout en restant entièrement disponibles pour les utilisateurs légitimes ; cependant, il suffit d'une seule vulnérabilité pour offrir une porte d'entrée à n'importe quel cybercriminel cherchant à contrôler vos systèmes d'information.

Les tests de pénétration servent de démonstration pratique des scénarios d'attaque possibles, où une personne malintentionnée tenterait de contourner les contrôles de sécurité de votre réseau d'entreprise afin d'obtenir des privilèges élevés dans des systèmes importants.

Le service de test de pénétration de Kaspersky Lab vous permet de mieux comprendre les failles de sécurité de votre infrastructure, en révélant les vulnérabilités, en analysant les conséquences possibles des différents types d'attaques, en évaluant l'efficacité de vos mesures de sécurité actuelles et en proposant des améliorations et des mesures correctives.

Tests de pénétration

Les tests de pénétration de Kaspersky Lab vous aident, vous et votre entreprise, à :

- **Identifier les principales vulnérabilités de votre réseau** pour que vous puissiez décider, en toute connaissance de cause, des points sur lesquels vous devez concentrer votre attention et vos investissements afin de réduire les risques à venir.
- **Éviter les dommages financiers, opérationnels et liés à la réputation causés par les cyberattaques,** en les empêchant de se produire grâce à la détection proactive des vulnérabilités et à leur correction.
- **Respecter les normes gouvernementales, industrielles et internes de l'entreprise** qui imposent ce type d'évaluation de sécurité (par exemple dans le cadre de la norme PCI DSS (paiement sécurisé par carte bancaire)).

Formules et étendue des services

En fonction de vos besoins et de votre infrastructure informatique, vous pouvez faire appel à l'ensemble ou à une partie seulement des services de test de pénétration suivants :

- **Tests de pénétration externe :** évaluation de sécurité effectuée via Internet par un « pirate » n'ayant aucune connaissance préalable de votre système.
- **Tests de pénétration interne :** scénarios basés sur une attaque de l'intérieur, par exemple par un visiteur bénéficiant seulement d'un accès physique à vos bureaux ou par un sous-traitant disposant d'un accès limité aux systèmes.
- **Tests d'ingénierie sociale :** évaluation du niveau de sensibilisation de votre personnel aux questions de sécurité en simulant des attaques d'ingénierie sociale, telles que le phishing, les faux liens malveillants dans les e-mails, les pièces jointes suspectes, etc.
- **Évaluation de la sécurité des réseaux wi-fi :** nos experts effectuent une visite de votre site et analysent les contrôles de sécurité wi-fi.

Vous pouvez appliquer nos tests de pénétration à n'importe quelle partie de votre infrastructure informatique, mais nous vous recommandons fortement de tester l'ensemble du réseau ou ses principales composantes, car les tests donnent toujours des résultats plus probants lorsque nos experts travaillent dans les mêmes conditions qu'un intrus potentiel.

Résultats des tests de pénétration

Le service de test de pénétration est conçu pour révéler les failles de sécurité susceptibles d'être exploitées pour accéder sans autorisation aux composantes essentielles d'un réseau. Les failles potentielles concernent notamment les aspects suivants :

- Une architecture réseau vulnérable, une protection insuffisante du réseau
- Des vulnérabilités permettant d'intercepter et de rediriger le trafic du réseau
- Des niveaux d'authentification et d'autorisation insuffisants dans différents services
- Des données d'identification utilisateur à faible sécurité
- Des défauts de configuration, notamment des privilèges excessifs accordés aux utilisateurs
- Des vulnérabilités provenant d'erreurs dans le code d'application (injection de code, traversée de chemin, vulnérabilités côté client, etc.)
- Des vulnérabilités causées par l'utilisation de matériel et de logiciels obsolètes ne bénéficiant pas des dernières mises à jour de sécurité
- La divulgation d'informations

Les résultats sont présentés dans un rapport final, qui comprend des informations techniques détaillées sur le déroulement du test, les résultats, les vulnérabilités révélées et les mesures correctives préconisées, le tout accompagné d'un résumé analytique décrivant les résultats du test et illustrant les vecteurs d'attaque. Sur demande, nous pouvons également fournir des vidéos et des présentations destinées à votre équipe technique ou à la direction.

Que vous développiez vos applications d'entreprise en interne ou les achetiez à des tiers, vous savez qu'une seule erreur de codage peut créer une vulnérabilité qui vous expose aux attaques et entraîne des dommages financiers considérables tout en portant sérieusement atteinte à votre réputation. De nouvelles vulnérabilités peuvent également apparaître pendant le cycle de vie d'une application, lors de la mise à jour de logiciels, au cours d'une configuration de composants non sécurisée ou encore suite à l'apparition de nouvelles méthodes d'attaque.

Les services d'évaluation de la sécurité des applications de Kaspersky Lab permettent d'identifier les vulnérabilités de toutes sortes d'applications : solutions Cloud, systèmes ERP, services bancaires en ligne et autres applications professionnelles spécialisées ou encore applications mobiles et embarquées sur différentes plates-formes (iOS, Android et autres).

Avantages du service

Les services d'évaluation de la sécurité des applications de Kaspersky Lab aident les propriétaires et les développeurs d'applications à :

- **Éviter les dommages financiers, opérationnels et liés à la réputation** en détectant et corrigeant proactivement les vulnérabilités exploitées dans les attaques contre les applications.
- **Réduire les coûts des mesures correctives** en repérant les vulnérabilités des applications encore au stade de développement et de test, avant leur entrée dans l'environnement utilisateur, où leur correction peut entraîner des perturbations et des frais considérables.
- **Favoriser un cycle de développement de systèmes sécurisé** (S-SDLC) permettant de créer et de maintenir des applications fiables.
- **Se conformer aux normes gouvernementales, industrielles et internes de l'entreprise** en matière de sécurité des applications, telles que les normes PCI DSS ou HIPAA

À propos de l'approche adoptée par Kaspersky Lab pour les tests de pénétration

Les tests de pénétration simulent de véritables cyberattaques, mais restent étroitement contrôlés ; ils sont effectués par les experts en sécurité de Kaspersky Lab en préservant entièrement la confidentialité, l'intégrité et la disponibilité de vos systèmes et dans le plus strict respect des normes internationales et des bonnes pratiques, telles que :

- La norme en matière d'exécution des tests de pénétration (PTES)
- Les publications spéciales 800-115 du NIST - Guide technique des tests et des évaluations de la sécurité des informations
- Le Manuel méthodologique des tests de sécurité open source (OSSTMM)
- Le Cadre d'évaluation de la sécurité des systèmes d'information (ISSAF)
- La classification des menaces établie par le consortium WASC (Web Application Security Consortium)
- Le Guide des tests du projet OWASP (Open Web Application Security Project)
- Le système de notation des vulnérabilités CVSS (Common Vulnerability Scoring System)

L'équipe du projet est composée de professionnels expérimentés bénéficiant de connaissances pratiques approfondies et actuelles dans ce domaine ; ce sont des conseillers en sécurité reconnus par les plus grandes entreprises du secteur, dont Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens et SAP.

Formules des services

En fonction du type de service d'évaluation de sécurité, des spécificités de vos systèmes et de vos habitudes de travail, nous pouvons procéder à l'évaluation de votre sécurité à distance ou sur place. La plupart des services peuvent être réalisés à distance et les tests de pénétration interne peuvent même être effectués via un réseau VPN, tandis que d'autres, tels que l'évaluation de sécurité des réseaux wi-fi, exigent une présence sur place.

Évaluation de la sécurité des applications

Grâce à leurs connaissances pratiques et à leur expérience en matière de bonnes pratiques internationales, nos experts détectent les failles de sécurité pouvant exposer votre organisation à différentes menaces, dont :

- le détournement de données confidentielles
- l'infiltration et la modification de données et de systèmes
- le lancement d'attaques par déni de service
- l'implication dans des activités frauduleuses

En suivant nos recommandations, vous pouvez corriger les vulnérabilités identifiées dans les applications et empêcher ainsi ces attaques.

Formules et étendue des services

Parmi les applications pouvant être évaluées figurent les sites Internet officiels et les applications métiers, classiques ou basées dans le Cloud, y compris les applications mobiles et embarquées.

Adaptés à vos besoins et aux spécificités des applications, les services peuvent comprendre :

- **Le test de la boîte noire :** simule une attaque externe
- **Le test de la boîte grise :** simule l'attaque par des utilisateurs légitimes présentant différents profils
- **Le test de la boîte blanche** : procède à une analyse avec un accès complet à l'application, y compris aux codes sources ; cette approche est la plus efficace pour révéler de nombreuses vulnérabilités
- **L'évaluation de l'efficacité du pare-feu d'application :** les applications sont testées avec le pare-feu activé et désactivé de façon à repérer des vulnérabilités et à vérifier si les failles éventuelles sont bloquées

Résultats

Vulnérabilités pouvant être identifiées par les services d'évaluation de la sécurité des applications de Kaspersky Lab :

- Failles dans l'authentification et l'autorisation, y compris l'authentification multi-facteurs
- Injection de code (injection SQL, OS Command, etc.)
- Vulnérabilités logiques à l'origine de fraudes
- Vulnérabilités côté client (script intersite, falsification de requête intersite, etc.)
- Utilisation d'un chiffrement insuffisant
- Vulnérabilités dans les communications client-serveur
- Transfert ou stockage de données non sécurisées, par exemple avec un masquage insuffisant du numéro de compte principal dans les systèmes de paiement
- Défauts de configuration, y compris ceux à l'origine d'attaques de gestion de session
- Divulgation d'informations sensibles
- Autres vulnérabilités d'applications Web les exposant aux menaces énumérées dans la classification des menaces v2.0 du WASC et dans la liste des 10 menaces les plus importantes d'après l'OWASP

Les résultats sont présentés dans un rapport final, qui inclut des informations techniques détaillées sur le déroulement du test, les résultats, les vulnérabilités révélées et les mesures correctives préconisées, le tout accompagné d'un résumé analytique expliquant les implications en matière de gestion. Sur demande, nous pouvons également fournir à votre équipe technique ou à la direction des vidéos et des présentations.

Cette évaluation consiste en une analyse complète de vos DAB et/ou terminaux de points de vente. Elle permet de repérer les éventuelles vulnérabilités que les criminels pourraient exploiter pour leurs activités frauduleuses, par exemple : un retrait ou des transactions non autorisé(es), la récupération des données de cartes de paiement de vos clients ou encore une attaque par déni de service. Ce service mettra en évidence la moindre vulnérabilité dans l'infrastructure de vos DAB/terminaux PDV susceptible d'être exploitée pour différents types d'attaques pointera les conséquences possibles, évaluera l'efficacité de vos mesures de sécurité actuelles et vous aidera à établir un plan d'action pour corriger les failles et renforcer votre protection.

À propos de l'approche adoptée par Kaspersky Lab pour évaluer la sécurité des applications

La sécurité des applications est évaluée par les experts en sécurité de Kaspersky Lab aussi bien manuellement qu'avec des outils automatisés dans le respect le plus total de la confidentialité, de l'intégrité et de la disponibilité de vos systèmes et conformément aux normes internationales et aux bonnes pratiques, telles que :

- la classification des menaces établie par le consortium WASC (Web Application Security Consortium)
- le Guide de tests du projet OWASP (Open Web Application Security Project)
- le Guide de tests de la sécurité mobile d'OWASP
- d'autres normes, en fonction du secteur d'activité et de la localisation de votre entreprise

L'équipe du projet est composée de professionnels expérimentés bénéficiant de connaissances pratiques actuelles et approfondies dans le domaine, notamment concernant différentes plates-formes, langages de programmation, infrastructures, vulnérabilités et méthodes d'attaque. Ils interviennent dans les plus grandes conférences internationales et sont consultés pour des questions de sécurité par les principaux fournisseurs d'applications et de services Cloud, tels qu'Oracle, Google, Facebook, Apple et PayPal.

Formules des services

En fonction du type de service d'évaluation de sécurité, des spécificités des systèmes concernés et de vos exigences en matière de conditions de travail, nous pouvons fournir nos services d'évaluation de sécurité à distance ou sur place. La plupart de ces services peuvent être réalisés à distance.

Évaluation de la sécurité des DAB/ TERMINAUX DE POINTS DE VENTE

Les DAB et les terminaux de points de vente ne sont plus seulement vulnérables aux attaques physiques (par ex., cambriolage de distributeur ou piratage et clonage de carte). Suite à l'évolution des mesures de protection prises par les fournisseurs de DAB/terminaux de point de vente, les criminels passent eux aussi à la vitesse supérieure et leurs attaques sont de plus en plus sophistiquées. Les pirates informatiques exploitent les vulnérabilités des applications et de l'infrastructure des DAB/terminaux de point de vente afin de créer des programmes malveillants sur mesure. Les services d'évaluation de la sécurité des DAB/terminaux de points de vente de Kaspersky Lab vous aident à identifier les failles de sécurité de vos DAB et/ou terminaux de points de vente et à limiter le risque qu'ils soient compromis.

Avantages du service

Les services d'évaluation de la sécurité des DAB/terminaux de points de vente de Kaspersky Lab permettent aux fournisseurs et aux établissements financiers :

- **De comprendre les vulnérabilités** de leurs DAB et/ou terminaux de points de vente et d'optimiser les processus de sécurité correspondants.
- **D'éviter les dommages financiers, opérationnels et liés à la réputation** qui peuvent être occasionnés par une attaque, en détectant et corrigeant de manière proactive les vulnérabilités susceptibles d'être exploitées par les criminels.
- **De se conformer aux normes gouvernementales, industrielles et internes de l'entreprise** qui imposent des évaluations de sécurité, (par exemple la norme PCI DSS (paiement sécurisé par carte bancaire)).

Étendue des services

Ce service inclut une analyse complète des DAB/terminaux de points de vente, notamment un « fuzzing » et des démonstrations d'attaques dans un environnement de test. Cette analyse peut porter sur un seul DAB et/ou terminal de point de vente, ou bien sur tout un réseau. Nous vous recommandons, aux fins de cette évaluation, de choisir le type de DAB et/ou de terminal PDV le plus utilisé au sein de votre entreprise, ou le plus critique (par exemple un appareil qui a déjà fait l'objet d'incidents) dans sa configuration classique.

Résultats de l'évaluation de la sécurité des DAB/TERMINAUX PDV

Les services d'évaluation de la sécurité des DAB/points de vente doivent permettre d'identifier un certain nombre de vulnérabilités, parmi lesquelles :

- Une architecture réseau vulnérable et une protection insuffisante du réseau.
- Des vulnérabilités permettant à un cybercriminel de contourner le mode kiosque et d'obtenir un accès non autorisé au système d'exploitation.
- Des vulnérabilités dans les logiciels de sécurité tiers permettant aux éventuels cybercriminels de contourner les contrôles de sécurité.
- Une protection insuffisante des appareils d'entrée/sortie (lecteurs de cartes, distributeurs, etc.), ainsi que des vulnérabilités dans les communications desdits appareils, susceptibles de favoriser l'interception et la modification des données transférées.
- Des vulnérabilités provenant d'erreurs dans le code de l'application ou causées par l'utilisation de matériels et de logiciels obsolètes (dépassement de la mémoire tampon, injection de code, etc.).
- La divulgation d'informations.

Au terme de l'évaluation, vous recevrez un rapport contenant des informations techniques détaillées sur le déroulement du test, les résultats, les vulnérabilités révélées et les mesures correctives préconisées, avec un résumé analytique décrivant nos conclusions au vu des résultats du test et illustrant les différents vecteurs d'attaque. Sur demande, nous pouvons également fournir à votre équipe technique ou à la direction des présentations et des vidéos de démonstration d'attaques.

Résultats

Au terme de chaque évaluation de sécurité, vous recevrez un rapport contenant des informations techniques et détaillées sur les failles de sécurité de vos réseaux de télécommunications, ainsi que nos conclusions quant à l'efficacité de vos contrôles de sécurité. Vous pourrez utiliser ces résultats pour renforcer la sécurité de vos réseaux et, ce faisant, limiter les risques en termes financiers, opérationnels et de réputation associés aux menaces sur la sécurité des informations.

Le rapport contiendra les éléments suivants :

- Des conclusions détaillées sur le niveau de sécurité actuel de vos réseaux de télécommunications
- Une description de la méthodologie et du processus appliqués par le service
- Une description détaillée des vulnérabilités détectées, y compris leur degré de gravité et de complexité, leurs répercussions éventuelles sur le système et les preuves de leur existence (dans la mesure du possible)
- Des recommandations pour éliminer ces vulnérabilités (modification de la configuration, mises à jour, modification des codes sources ou mise en place de contrôles de compensation lorsqu'il est impossible d'éliminer une vulnérabilité)

Approche adoptée par Kaspersky Lab pour évaluer la sécurité des DAB/TERMINAUX DE POINTS DE VENTE

Nos experts vont non seulement rechercher et identifier les défauts de configuration et les vulnérabilités des logiciels obsolètes, mais aussi examiner en détail la logique qui sous-tend les processus de vos DAB et/ou terminaux PDV et réaliser une recherche dans le but de repérer les nouvelles vulnérabilités de type « zero-day » au niveau des composants. S'ils découvrent des vulnérabilités susceptibles d'être exploitées par un criminel (et conduisant, par exemple, à un retrait non autorisé), nos experts pourront vous fournir une démonstration des scénarios d'attaque possibles au moyen d'outils ou d'appareils d'automatisation spécialement conçus à cet effet.

L'évaluation de la sécurité des DAB/terminaux PDV implique la simulation de cyberattaques en vue de mesurer concrètement l'efficacité de votre défense, mais sachez que cette méthode est parfaitement sûre et non invasive. Ce service est fourni par les experts en sécurité de Kaspersky Lab qui s'attacheront à préserver la confidentialité, l'intégrité et la disponibilité de vos systèmes, dans le plus strict respect des normes internationales et des bonnes pratiques. Si nous découvrons une nouvelle vulnérabilité dans le DAB/terminaux PDV d'un client, nous nous engageons à appliquer une politique d'information responsable, c'est-à-dire à avertir le fournisseur et à lui recommander des correctifs.

Kaspersky Lab fournit ses services d'évaluation de la sécurité des DAB/terminaux de points de vente conformément aux normes internationales et aux bonnes pratiques ci-dessous :

- Les normes sectorielles relatives aux cartes de paiement {{La norme sur la sécurité des données {{ La norme sur la sécurité des données des applications de paiement {{ La norme sur la sécurité des transactions nécessitant la saisie d'un code PIN
- Le Manuel méthodologique des tests de sécurité open source (OSSTMM)
- Le Cadre d'évaluation de la sécurité des systèmes d'information (ISSAF)
- Le système de notation des vulnérabilités CVSS (Common Vulnerability Scoring System)
- D'autres normes applicables, selon les besoins, à des modèles d'activité et des zones géographiques spécifiques

L'équipe de projet est composée de professionnels de la sécurité très expérimentés bénéficiant de connaissances pratiques approfondies dans un domaine qu'ils ne cessent de parfaire. Régulièrement, ceux-ci conseillent les fournisseurs de DAB/points de vente en matière de sécurité et présentent les résultats de leurs recherches dans le cadre de conférences phares sur la sécurité des informations (comme la conférence Black Hat).

Évaluation de la sécurité des réseaux de télécommunications

Présentation des services

L'infrastructure informatique d'une entreprise de télécommunications est constituée d'un certain nombre de réseaux interconnectés reposant sur diverses fonctionnalités et technologies. En règle générale, elle comprend un réseau d'entreprise incluant des éléments de gestion, un réseau radio central (GSM/UMTS/LTE) fournissant un accès Internet haut débit aux abonnés, des canaux dédiés à grande vitesse de type « trunk », ainsi que des services d'hébergement et de Cloud. Chaque composante de cette infrastructure est essentielle à l'entreprise et doit être parfaitement protégée contre les cyberattaques pour réduire les risques en termes financiers, opérationnels et de réputation. Vous pouvez atteindre cet objectif grâce aux services d'évaluation de la sécurité des réseaux de télécommunications de Kaspersky Lab qui, après avoir identifié les vulnérabilités de vos systèmes, les éliminent ou les corrigent en instaurant des contrôles.

En ce qui concerne la sécurité des réseaux de télécommunications, Kaspersky Lab propose les services d'évaluation suivants :

- Test de pénétration de l'infrastructure informatique
- Évaluation de la sécurité au niveau de la configuration de l'infrastructure informatique
- Évaluation de la sécurité des réseaux GSM/UMTS/LTE
- Évaluation de la sécurité des applications (fournissant divers services : IPTV, portail client libre-service, etc.)
- Évaluation de la sécurité du service voix sur IP (VoIP)
- Évaluation de la sécurité des équipements de télécommunications

Solutions de cybersécurité de
Kaspersky Lab pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr