Solutions de cybersécurité de
Kaspersky Lab pour les entreprises

KASPERSKY lab

Kaspersky Interactive Protection Simulation

Un moyen efficace de sensibiliser les hauts dirigeants et les décideurs à la cybersécurité

www.kaspersky.fr
#truecybersecurity

Kaspersky Interactive Protection Simulation

Le problème du « facteur humain »

L'une des plus grandes difficultés en matière de cybersécurité, c'est de concilier les différents points de vue et priorités des dirigeants. Cette diversité peut en effet entraîner une prise de décisions de type « Triangle des Bermudes » dès qu'il s'agit de la sécurité :

- Les responsables opérationnels peuvent considérer que les mesures de sécurité sont contradictoires avec leurs objectifs (à savoir, des services plus économiques, plus rapides et de meilleure qualité).
- Les responsables de la sécurité IT peuvent avoir le sentiment que l'infrastructure de cybersécurité et les investissements y afférents ne sont pas de leur ressort.
- Les responsables de la maîtrise des coûts peuvent ne pas voir le lien entre les dépenses de cybersécurité et les revenus ni comprendre en quoi celles-ci représentent des économies plus que des coûts.

L'efficacité de la cybersécurité repose sur une compréhension mutuelle et une collaboration entre ces trois catégories de responsables. Cependant, les méthodes de sensibilisation traditionnelles (conférences, exercices rouges/bleus) présentent des lacunes. Elles sont en effet interminables, trop techniques, incompatibles avec les emplois du temps chargés des responsables et dépourvues d'un « langage commun » rationnel.

Qu'est-ce que KIPS ?

Kaspersky Interactive Protection Simulation (KIPS) est un exercice qui place des équipes de sécurité IT d'entreprises ou d'organismes gouvernementaux au sein d'un environnement commercial simulé. Ces équipes devront faire face à une série de cybermenaces inattendues, tout en essayant d'optimiser les bénéfices et d'entretenir la confiance.

L'idée est de construire une stratégie de défense informatique en effectuant des choix parmi les meilleures commandes proactives et réactives disponibles. Chaque réaction des équipes face aux événements modifie la façon dont le scénario se déroule et impacte, en définitive, les bénéfices générés par l'entreprise... de façon positive ou négative.

En équilibrant les priorités en matière d'ingénierie, d'opportunités commerciales et de sécurité face au coût d'une cyberattaque réaliste, les équipes analysent des données et prennent des décisions stratégiques en fonction d'informations incertaines et de ressources limitées. Si cela vous paraît réaliste, c'est le but, chaque scénario étant conçu d'après des événements réels.

En quoi la formation KIPS est-elle efficace ?

La formation KIPS vise les responsables IT et lur responsables hiérarchiques, avec pour but d'accroître leur sensibilisation aux risques et aux problèmes de sécurité posés par l'exploitation de systèmes informatisés modernes.

Chaque équipe se compose de 4 à 6 personnes et a pour mission de gérer une entreprise (station d'épuration, banque, etc.) le plus efficacement possible. Cette entreprise comprend des sites de production et est contrôlée par des ordinateurs. Tout au long du jeu, les sites de production génèrent des revenus et des résultats commerciaux et contribuent au bien-être de la population. Toutefois, les équipes sont confrontées à des cyberattaques susceptibles d'affecter la performance de leur entreprise.

Afin de protéger son entreprise, chaque équipe doit prendre des décisions stratégiques, techniques et de gestion tout en tenant compte des contraintes opérationnelles et en maintenant un niveau élevé de revenus.

Le jeu KIPS est un programme de sensibilisation dynamique basé sur « l'apprentissage par la pratique » :

- Amusant, attrayant et rapide (2 heures)
- Le travail d'équipe renforce la coopération
- La compétition favorise l'initiative et l'analyse
- L'expérience de jeu développe la connaissance des mesures de cybersécurité

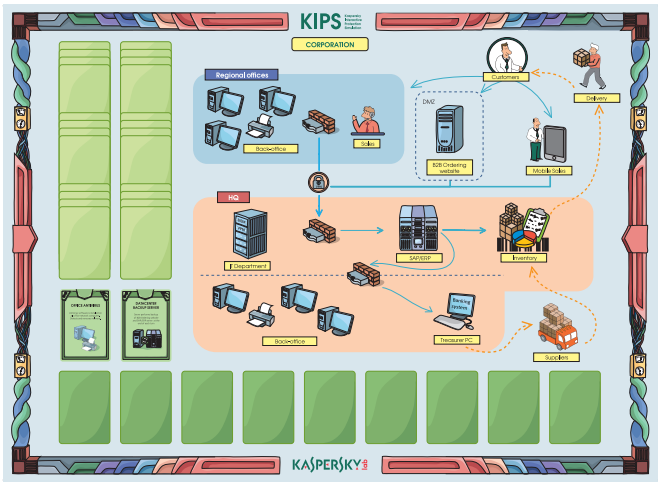
À l'issue du jeu KIPS, les participants parviennent à des conclusions importantes et utiles pour leur travail quotidien :

- Les cyberattaques affectent les revenus et doivent être contrées au niveau de la direction.
- Les services IT et opérationnel doivent impérativement collaborer pour garantir une cybersécurité efficace.
- Un budget de sécurité suffisant coûtera toujours beaucoup moins cher que d'éventuelles pertes de revenus et ne se chiffre pas forcément en millions.
- Les gens s'accoutument aux contrôles de sécurité particuliers et ont conscience de leur importance (audits, formations, antivirus, etc.).

« Parmi les tendances qui se dégagent de l'exercice, on constate que les premières décisions de sécurité, et parmi les plus simples, que vous pouvez prendre, comme les audits de sécurité et la formation, ou les changements de mots de passe et la gestion des correctifs, vous aideront énormément à réagir efficacement aux incidents qui pourraient survenir à l'avenir. »

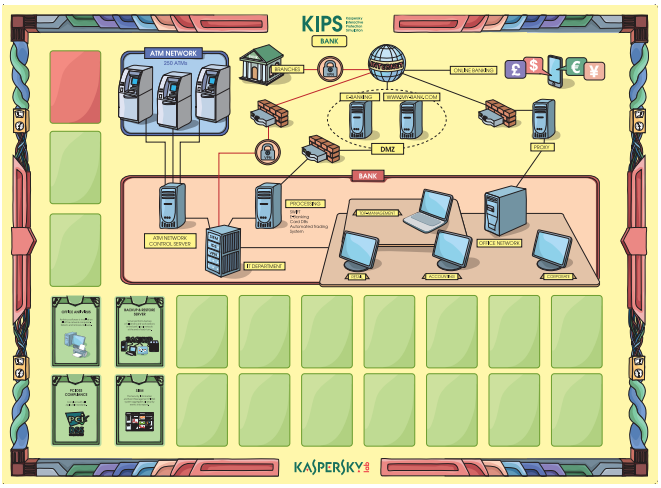
Mark Jenkins · 16 décembre 2015 ICT Qatar
www.digitalqatar.qa/en/2015/12/16/let-the- cyber-games-commence

Entreprise



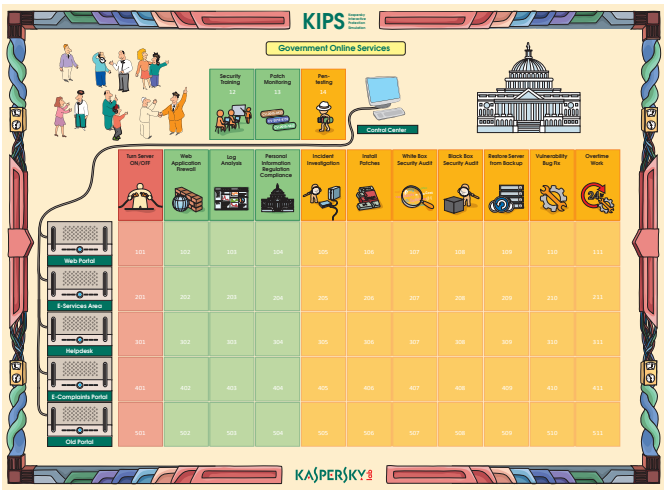
Protéger l'entreprise contre les ransomwares, les menaces persistantes avancées (Advanced Persistent Threats ou « APT »), les failles de sécurité liées à l'automatisation

Banque



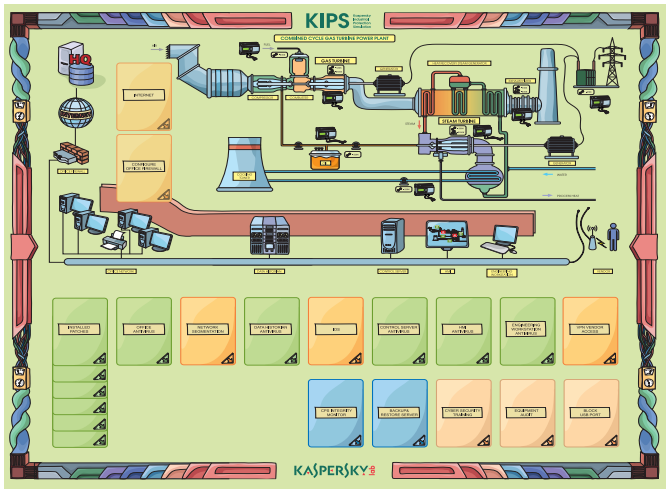
Protéger les établissements financiers contre les nouvelles APT à haut risque telles que Tyukpin et Carbanak

Services administratifs en ligne



Protéger les serveurs Web publics contre les attaques et les failles

Centrale électrique



Protéger les infrastructures critiques et les systèmes de contrôle industriels

Scénarios KIPS destinés aux entreprises de tous secteurs

Grâce à la formation KIPS, les participants sont mieux à même de saisir :

- le véritable rôle de la cybersécurité dans la continuité et la rentabilité de l'entreprise ;
- les nouvelles difficultés et menaces en passe d'émerger ;
- les erreurs typiquement commises par les entreprises dans leur stratégie de cybersécurité ;
- comment les équipes de sécurité et opérationnelle peuvent collaborer pour contribuer à maintenir la stabilité des activités de l'entreprise et une protection durable face aux cybermenaces.

Témoins d'une cyberattaque affectant la production et les revenus de leur entreprise, les participants apprennent à mettre en œuvre diverses stratégies et solutions opérationnelles et IT afin d'en minimiser l'impact et de gagner davantage d'argent.

Chacun de ces scénarios se concentre sur des vecteurs de menaces respectifs et permet la découverte et l'analyse des erreurs typiques commises lors de la mise en place de mesures de cybersécurité et de procédures de réponse aux incidents dans le secteur correspondant.

Citations et références relatives au jeu KIPS

La formation Kaspersky Industrial Protection Simulation a été particulièrement instructive et devrait être obligatoire pour tous les professionnels de la sécurité.

Warwick Ashford, Computer Weekly

Le CERN possède des quantités de systèmes IT et d'ingénierie qui mobilisent des milliers de personnes. C'est pourquoi il est tout aussi essentiel de mettre en place des contrôles techniques que de sensibiliser nos employés à la cybersécurité et de les inciter à s'en soucier. La formation de Kaspersky Lab s'est révélée stimulante, brillante et efficace.

Stefan Luders, responsable de la sécurité des systèmes d'information au CERN

Cette formation a été extrêmement enrichissante et bon nombre de participants ont demandé à pouvoir l'utiliser dans leur entreprise.

Joe Weiss, PE, CISM, CRISC, membre de l'ISA

Rien de tel que cette formation KIPS pour entamer la construction d'un réseau axé sur l'affiliation et la collaboration.

Daniel P. Bagge, Národní centrum kybernetické bezpečnosti, République tchèque

Recommandations relatives à la préparation des sessions de formation KIPS

Agenda : programmez la formation KIPS à part ou bien dans le cadre d'un événement / d'une conférence / d'un séminaire (dans ce second cas, organisez-la le soir du premier jour).

Groupe : entre 20 et 100 personnes réparties en équipes de 3 ou 4. Dans l'idéal, chaque équipe doit se composer de dirigeants, d'ingénieurs et de responsables de la sécurité des systèmes d'information ou de la sécurité IT :

- il est préférable que chaque équipe comporte au moins un membre de chacun de ces postes ;
- il n'est pas obligatoire que les membres d'une équipe appartiennent à la même entreprise / au même service ;
- il n'est pas obligatoire que les membres d'une équipe se connaissent.

Installation : le jeu dure 2 heures, mais la salle doit être mise à disposition de l'équipe de formation de Kaspersky Lab 2 heures avant le début du jeu afin qu'elle puisse tout préparer et installer.

Salle : comptez environ 3 m²/personne et choisissez une salle d'une forme standard sans colonnes.

Équipement audiovisuel : projecteur (6-8 lumens), écran, système audio (haut-parleurs, télécommande, microphones).

Wi-Fi avec accès Internet (accès au serveur de jeu KIPS), à partir de 4 Mbit/s.

1 iPad par équipe (4 personnes) avec une connexion Wi-Fi (et un affichage Retina idéalement) ou d'autres tablettes.

Mobilier : tables de participants pour 4 personnes (rectangulaires ne mesurant pas moins de 75 x 180 cm, ou rondes d'un diamètre de 1,5 m au maximum). Les participants doivent pouvoir s'asseoir en groupes de 4 à chaque table. Tables pour les co-formateurs. Chaises en fonction du nombre de participants.

Références et études de cas

Depuis son introduction en 2013, le jeu KIPS a conquis 5 000 professionnels de la sécurité industrielle dans une vingtaine de pays.

- Le jeu KIPS a été traduit en anglais, en russe, en allemand, en français, en japonais, en espagnol et en portugais.
- Il a été utilisé par des agences gouvernementales (ictQATAR, CyberSecurity Malaysia, l'Autorité de sécurité tchèque, le Nationaal Cyber Security Centrum aux Pays-Bas) afin de renforcer la sensibilisation aux infrastructures critiques et de former des centaines d'experts issus d'entreprises nationales en charge de telles infrastructures.
- Il est utilisé par des entreprises telles que BASF (premier fabricant mondial de produits chimiques), le CERN (à l'origine du Grand collisionneur de hadrons), Mitsubishi, Yokogawa, RusHydro, Panasonic ou encore l'ISA (International Society of Automation), qui s'en servent pour enseigner à leurs propres ingénieurs, développeurs et employés au contact de la clientèle comment préserver la cybersécurité dans les environnements d'automatisation industrielle.
- Des établissements d'enseignement faisant autorité ont acheté la licence, notamment le SANS Institute, qui l'utilise dans ses programmes de formation à la cybersécurité à travers le monde.
- Des fournisseurs de services de sécurité (dont Mitsubishi Hitachi Power Systems) ont acheté la licence afin de l'utiliser pour former les clients finaux des différents secteurs d'infrastructures critiques.

Éléments livrables

Chaque formation KIPS :

- dure 2 heures (briefing, jeu, débriefing et discussion) et s'articule autour d'un scénario ;
- peut accueillir jusqu'à 100 participants ;
- est dispensée par un formateur professionnel de Kaspersky Lab certifié KIPS ou par un partenaire autorisé.

Kaspersky Lab fournit :

- le descriptif de la formation KIPS à intégrer aux invitations ;
- les supports (tapis de jeu, cartes) à utiliser pendant la session, ainsi que le logiciel KIPS ;
- l'équipe chargée d'animer le jeu.

Le client gère :

- la salle, les iPad[1], l'équipement audiovisuel, l'accès Internet ;
- l'envoi des invitations et les inscriptions des participants.

Possibilité d'une « formation pour les formateurs »

Si un client souhaite utiliser la formation KIPS pour former un plus grand nombre d'employés, de responsables et d'experts à travers divers services ou sites, il peut acheter la licence correspondante, former des formateurs internes et organiser des sessions de formation KIPS à son propre rythme et selon ses propres besoins.

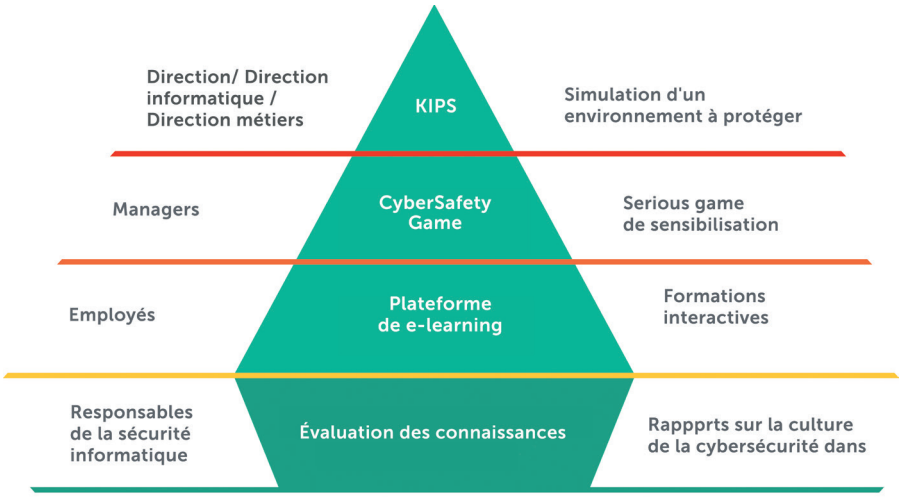
Cette licence est disponible auprès de Kaspersky Lab et comprend :

- le droit d'utiliser en interne le programme de formation KIPS ;
- des supports de formation et le droit de les utiliser/reproduire ;
- des identifiants de connexion au serveur du logiciel KIPS ;
- un guide et une formation destinés aux formateurs pour que les responsables du programme sachent comment dispenser la formation KIPS ;
- un service de maintenance et d'assistance (mises à jour et assistance pour le logiciel KIPS et le contenu de formation) ;
- des options de personnalisation du scénario KIPS (moyennant un supplément).

[1] Kaspersky Lab peut fournir des iPad moyennant un supplément d'environ 100 $ par appareil.

Produits pédagogiques Kaspersky Security Awareness

La formation Kaspersky Interactive Protection Simulation (KIPS) fait partie de la gamme Kaspersky Security Awareness, laquelle s'appuie sur une méthode prônant une culture de la cybersécurité, grâce à un ensemble de formations de sensibilisation axées sur le jeu, pour tous les niveaux de l'entreprise, et gérées par les équipes de sécurité et RH.



Une approche complète, mais simple

- Un large éventail de questions de sécurité couvert
- Des environnements familiers
- Un processus de formation axé sur la participation
- Des exercices pratiques
- Des explications compréhensibles par les néophytes

Avantages commerciaux

pas moins de

93 %

de chances de voir les employés utiliser leurs connaissances au quotidien

jusqu'à

90 %

d'incidents en moins

50-60 %

de baisse des dépenses liées aux risques de cybersécurité

Multipl. par 30

du retour sur investissement en sensibilisation à la sécurité

www.kaspersky.fr

Solutions de sécurité Kaspersky Lab
pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness :
https://www.kaspersky.fr/enterprise-security/security-awareness
Démonstration du produit : **www.kaspersky.com/demo-sa**