KASPERSKY lab

Kaspersky Interactive Protection Simulation

Eine effektive Möglichkeit zur Verbesserung des Cybersicherheitsbewusstseins von führenden Managern und Entscheidungsträgern

www.kaspersky.de
#truecybersecurity

Kaspersky Interactive Protection Simulation

Das „Sicherheitsrisiko Mensch“

Eine der größten Sicherheitsherausforderungen besteht darin, dass verschiedene Rollen im leitenden Management Cybersicherheit aus unterschiedlichen Perspektiven betrachten und verschiedene Prioritäten haben. Dies kann zu einer Art „Bermudadreieck“ für die Entscheidungsfindung führen.

- Die unternehmerische Seite sieht die Sicherheitsmaßnahmen häufig als eine Verkomplizierung/einen Widerspruch zu ihren Geschäftszielen (billiger/schneller/mehr/besser).
- IT-Sicherheitsmanager haben unter Umständen das Gefühl, dass Cybersicherheit als Infrastruktur- und Investitionsproblem ihren Verantwortungsbereich verlässt.
- Manager, die mit der Kostenkontrolle beauftragt sind, erkennen möglicherweise nicht, dass Ausgaben für Cybersicherheit eher zu Einsparungen und Umsätzen führen, als zu weiteren Kosten.

Der Grad der Cybersicherheit ist also von gegenseitigem Verständnis und partnerschaftlicher Zusammenarbeit zwischen diesen drei Bereichen abhängig. Herkömmliche Schulungsformate, darunter Vorlesungen und Übungen mit den Parteien Rot und Blau sind fehleranfällig, langwierig, eher technisch orientiert und ungeeignet für viel beschäftigte Manager. Außerdem schaffen sie keine „gemeinsame Basis“ der Übereinstimmung.

Was ist KIPS?

Kaspersky Interactive Protection Simulation (KIPS) ist ein Übungsszenario, bei dem IT-Sicherheitsteams aus Unternehmen und Behörden in eine simulierte Geschäftsumgebung versetzt werden, in der sie einer Reihe unerwarteter Cyberbedrohungen ausgesetzt werden, während die Teams versuchen, den Gewinn zu maximieren und das Vertrauen der Kunden zu erhalten.

Die Idee besteht darin, durch Auswahl der besten verfügbaren vorausschauenden und reaktionsschnellen Kontrollmöglichkeiten eine Cyberverteidigungsstrategie zu entwickeln. Jede Reaktion der Teams auf die eintretenden Ereignisse verändert den Verlauf des Szenarios und damit den Gewinn bzw. den Verlust des Unternehmens.

Mit einem ausgewogenen Verhältnis von Entwicklungs-, geschäftlichen und Sicherheitsprioritäten sowie den Kosten eines realistischen Cyberangriffs analysiert das Team Daten und trifft strategische Entscheidungen auf Basis unsicherer Informationen und begrenzter Ressourcen. Dieser Realitätsgrad ist beabsichtigt, da alle Szenarien auf realen Ereignissen basieren.

Warum ist die KIPS-Übung effektiv?

KIPS-Training richtet sich an Experten für Geschäftssysteme, IT-Personal und Bereichsleiter. Es soll diese Zielgruppe auf Risiken und Sicherheitsprobleme moderner Computersysteme aufmerksam machen.

Jedes der konkurrierenden Teams aus 4 bis 6 Personen erhält die Aufgabe, ein Unternehmen (Wasseraufbereitungsanlage, Bank usw.) möglichst effizient zu führen. Jedes Unternehmen besteht aus einigen Produktionseinrichtungen und Computern, die diese steuern. Während der Spielrunden generieren die Einrichtungen Umsätze, Gemeinwohl und Geschäftsergebnisse. Die Teams müssen sich jedoch auch mit Cyberangriffen auseinandersetzen, die sich potentiell auf die Unternehmensleistung auswirken.

Zur Verteidigung des jeweiligen Unternehmens müssen die Teams strategische, Management- und technische Entscheidungen treffen und dabei betriebliche Einschränkungen berücksichtigen bzw. ein hohes Umsatzniveau beibehalten.

KIPS ist ein dynamisches Lehrprogramm, das auf praktischem Lernen basiert:

- Unterhaltsam, fesselnd und schnell (2 Stunden)
- Teamwork stärkt die Zusammenarbeit
- Wettbewerb fördert Initiative und Analysekompetenz
- Das Planspiel fördert das Verständnis von Cybersicherheitmaßnahmen

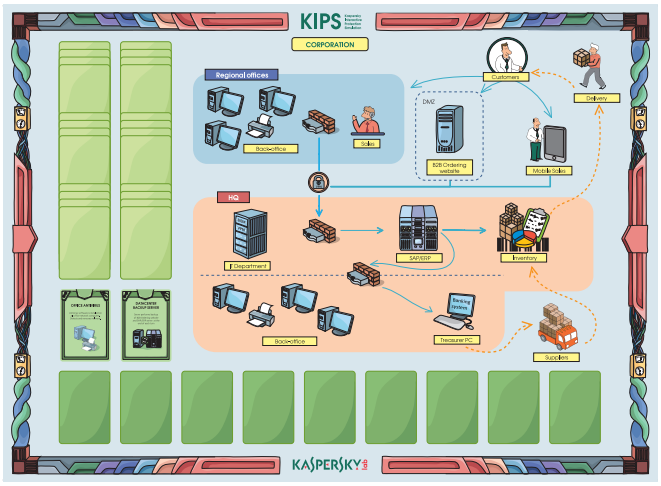
Nach dem KIPS-Spiel müssen die Spieler wichtige, praktisch umsetzbare Schlussfolgerungen für ihren Arbeitsalltag treffen:

- Cyberangriffe schädigen den Umsatz und müssen von allen Abteilungen bekämpft werden, angefangen bei der obersten Managementebene.
- Für den Erfolg der Cybersicherheit ist die Kooperation zwischen IT- Sicherheits- und Business-Mitarbeitern unabdingbar.
- Ein wirksames Sicherheitsbudget ist wesentlich kleiner als der potentielle Umsatzverlust, es sind keine Millioneninvestitionen erforderlich.
- Die Mitarbeiter gewöhnen sich an bestimmte Sicherheitskontrollen und ihre Bedeutung (Audit, Training, Virenschutz usw.).

„Mit dieser Übung wird jedoch klar, dass einige der ersten und grundlegenden strategischen Entscheidungen, die man trifft (darunter Sicherheits-Audits und Trainings, Passwortänderungen und Patch Management) spätere Reaktionen auf Vorfälle erheblich vereinfachen.“

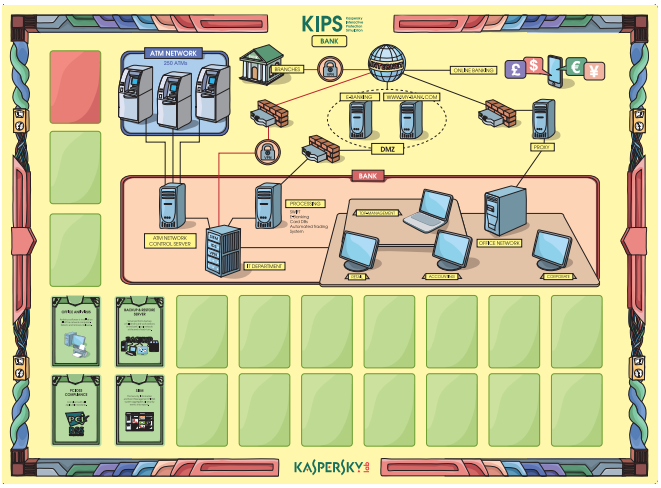
Mark Jenkins · 16. Dezember 2015, ICT Qatar
http://www.digitalqatar.qa/en/2015/12/16/

Unternehmen



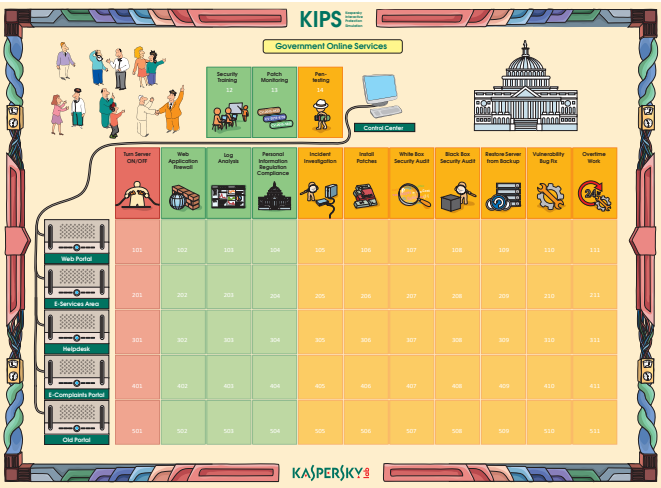
Schutz des Unternehmens vor Ransomware, APTs und Fehlern in der Automatisierungssicherheit

Bank



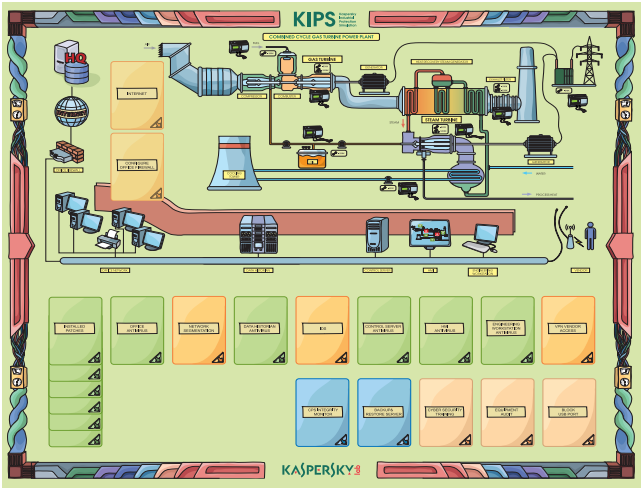
Schutz von Finanzinstitutionen vor neuen, übergeordneten APTs wie Tyukpin und Carbanak

Behördliche Online-Services



Schutz öffentlicher Webserver vor Angriffen und Exploits

Kraftwerk



Schutz industrieller Steuerungssysteme und wichtiger Infrastrukturen

KIPS-Szenarien für Unternehmen aus allen Branchen

Lerninhalte des KIPS-Trainings:

- Die reale Rolle der Cybersicherheit in den Bereichen Geschäftskontinuität und Rentabilität
- Neue Herausforderungen und Bedrohungen
- Typische Fehler von Unternehmen bei der Einrichtung von Cybersicherheit
- Zusammenarbeit zwischen Unternehmens- und Sicherheitsteams zur Aufrechterhaltung eines stabilen Betriebs des Unternehmens und der Widerstandsfähigkeit gegenüber Cyberbedrohungen

Das Unternehmen wird Ziel eines Cyberangriffs, und die Teilnehmer erleben die Auswirkungen auf Produktion und Umsätze. Sie müssen verschiedene Unternehmens- und IT-Strategien und -Lösungen einsetzen, um die Auswirkungen der Attacke zu minimieren und weiterhin erfolgreich zu sein.

Jedes Szenario konzentriert sich auf die jeweiligen Bedrohungsvektoren. Auf diese Weise lassen sich die typischen Fehler beim Aufbau der Cybersicherheit ermitteln und analysieren und Reaktionsverfahren je Industriezweig entwickeln.

Zitate und Referenzen zum KIPS-Planspiel

KIPS (Kaspersky Industrial Protection-Simulation) war ein echter Augenöffner und sollte für alle Sicherheitsprofis zur Pflichtveranstaltung werden.

Warwick Ashford, Computer Weekly

Wir bei CERN betreiben eine große Anzahl von IT- und Entwicklungssystemen, mit denen Tausende von Menschen arbeiten. Aus Sicht der Cybersicherheit sind die Erweiterung des Bewusstseins und das Engagement für Cybersicherheit ebenso wichtig wie die technischen Steuerungen. Das Training von Kaspersky Lab hat sich als spannend, aufschlussreich und effizient erwiesen.

Stefan Luders, CERN CISO

Es war wirklich sehr aufschlussreich, und zahlreiche Teilnehmer haben gefragt, ob sie dieses Planspiel auch in ihrem Unternehmen anwenden können.

Joe Weiss PE, CISM, CRISC, ISA Fellow

Wir müssen ein Netzwerk aus Personen aufbauen, das auf Zusammenschluss und Kooperation basiert. KIPS ist hierfür der perfekte Einstieg.

Daniel P. Bagge, Národní centrum kybernetické bezpečnosti, Tschechische Republik.

Empfehlungen zur Vorbereitung einer KIPS-Sitzung

Zeitplan: Planen Sie KIPS als separate Veranstaltung oder Sitzung im Rahmen einer Veranstaltung/einer Konferenz/eines Seminars (in diesem Fall ist der optimale Zeitpunkt für KIPS der Abend des ersten Tages).

Gruppe: 20 bis 100 Personen, aufgeteilt in Teams von 3 bis 4 Personen. Idealerweise umfasst jedes Team eine Mischung aus Management-, Technik-, CISO/IT-Sicherheitsmitarbeitern:

- Optimal ist mindestens ein Mitglied aus jeder Rolle/Funktion.
- Teams können Personen aus demselben Unternehmen/derselben Abteilung umfassen.
- Diese Personen können einander kennen oder auch nicht.

Spielaufbau: Das Planspiel dauert zwei Stunden. Der Raum muss dem Moderatorenteam von Kaspersky Lab zwei Stunden vor Beginn für die Vorbereitung und den Spielaufbau überlassen werden.

Raum: Planen Sie ~3 m²/Person, keine Säulen, Standardform

Audio-visuelle Geräte: Projektor (6–8 Lumen), Leinwand, Audiosystem (Lautsprecher, Fernsteuerung, Mikrofone).

WLAN mit Internetzugang (Zugriff auf Spiele-Server für Spiele zur Cybersicherheit) ab 4 MB/s.

1 iPad pro Team (4 Personen) mit WLAN-Unterstützung (vorzugsweise iPad mit Retina) oder ein anderes Tablet.

Möblierung: Tische für vier Teilnehmer (rechteckig, nicht kleiner als 75 x 180 cm bzw. rund mit einem Durchmesser von mindestens 1,5 m), die Teilnehmer sitzen in Vierergruppen an den Tischen. Tisch/Stuhl für den Kursleiter, ausreichend Stühle für die Teilnehmer an den Tischen.

Referenzen und Fallstudie

Seit der Einführung im Jahr 2013 wurde KIPS bereits von 5000 Industrie-Sicherheitsexperten in 20 Ländern durchgespielt.

- KIPS wurde in Englisch, Russisch, Deutsch, Französisch, Japanisch, Spanisch und Portugiesisch übersetzt.
- KIPS wurde von Regierungsbehörden wie ICTQatar, CyberSecurity Malaysia, der tschechischen NSA und dem Netherlands Cyber Security Centrum eingesetzt, um das Bewusstsein in kritischen Infrastrukturen zu stärken und dazu Hunderte von Experten aus wichtigen nationalen Infrastrukturunternehmen zu schulen.
- KIPS wird in Unternehmen wie BASF (weltweit führendes Chemieunternehmen), CERN (Large Hadron Collider), Mitsubishi, Yokogawa, RusHydro, Panasonic und ISA (International Society of Automation) eingesetzt, um eigene Ingenieure, Entwickler und Kundenbetreuer darin zu schulen, Cybersicherheit in industriellen Automatisierungsumgebungen ernst zu nehmen und sich dafür einzusetzen.
- KIPS wurde von führenden Bildungseinrichtungen lizenziert, darunter vom SANS Institute, wo es weltweit für Studenten im Bereich Cybersicherheit eingesetzt wird.
- KIPS wurde auch von Sicherheitsserviceanbietern und Herstellern lizenziert, darunter von Mitsubishi-Hitachi Power Systems, um Endkunden aus wichtigen Infrastruktursektoren zu schulen.

Leistungen

Jedes KIPS-Training umfasst Folgendes:

- 2-stündiges KIPS-Planspiel (Briefing, Spiel, Nachbesprechung und Diskussion), 1 Szenario
- Bis zu 100 Teilnehmer
- Die Durchführung wird von einem zertifizierten KIPS-Trainer von Kaspersky Lab oder von einem autorisierten Trainingspartner geleitet.

Kaspersky Lab bietet:

- KIPS-Beschreibung für Einladungen
- KIPS-Materialien (Spielfelder, Karten) für die KIPS-Sitzung und KIPS-Software
- Moderatorenteam für die Durchführung des Spiels

Der Kunde ist verantwortlich für:

- Raum, iPads[1], audio-visuelle Geräte, Internetzugang
- Einladung und Registrierung der Teilnehmer

Train-The-Trainer verfügbar

Wenn der Kunde eine größere Anzahl von Mitarbeitern, Managern und Experten aus mehreren Abteilungen oder Standorten mit KIPS schulen möchte, kann es sinnvoll sein, die Lizenz für KIPS-Schulungen zu erwerben, interne Trainer zu schulen und KIPS-Sitzungen nach den Vorgaben des Kunden am Kundenstandort durchzuführen.

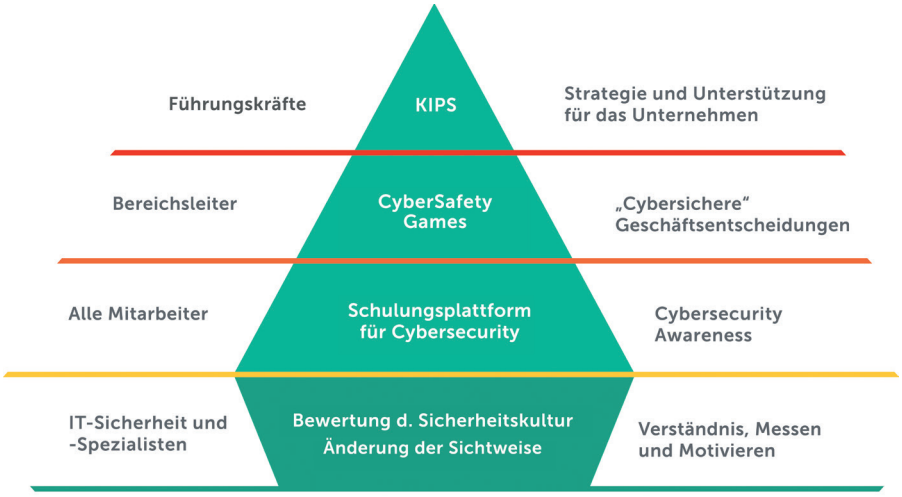
Eine solche Lizenz ist bei Kaspersky Lab erhältlich und umfasst Folgendes:

- Das Recht zur internen Nutzung des KIPS-Trainingsprogramms
- Schulungsmaterialien und das Recht zu deren Nutzung/Reproduktion
- Anmeldedaten/Passwort für KIPS-Softwareserver
- Trainerleitfaden, Schulung und Training für Programmleiter hinsichtlich der Durchführung eines KIPS-Trainings
- Wartung und Support (Updates und Support für KIPS-Software und Trainingsinhalte)
- Optionale Anpassung des KIPS-Szenarios (gegen zusätzliche Gebühr)

[1] Kaspersky Lab kann gegen Gebühr iPads bereitstellen (ca. 100 US-Dollar pro iPad).

Kaspersky-Schulungsprodukte für Sicherheitsbewusstsein

Die KIPS-Schulung ist ein Teil des Portfolios von Kaspersky Lab zum Thema Sicherheitsbewusstsein, das auf CyberSafety Culture-Methoden beruht. Cyber Safety Culture-Entwicklung durch verschiedene Trainings mit Spielcharakter für alle Ebenen der Unternehmensstruktur, verwaltet durch Sicherheits- und Personalteams.



Umfassend, aber einfach und verständlich

- Zahlreiche Sicherheitsaspekte
- Vertraute Umgebungen
- Fesselnder Schulungsprozess
- Praktische Übungen
- Sprache geeignet für Nicht-IT-Mitarbeiter

Geschäftsvorteile

ganze
93 %
Wahrscheinlichkeit der Anwendung des Wissens in der täglichen Arbeit

bis
90 %
weniger Vorfälle

50–60 %
geringeres monetäres Cyberrisiko

mehr als
30-fache
Rendite für Investition in Sensibilisierung

www.kaspersky.de

Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Kaspersky Security Awareness: **https://www.kaspersky.de/enterprise-security/security-awareness**
Produktdemo: **https://www.kaspersky.de/enterprise-security/cybersecurity-awareness/demo/**