KASPERSKY lab

SERVIZI DI INTELLIGENCE KASPERSKY PER LA SICUREZZA

2015

Oggi il cybercrimine non conosce confini e le competenze tecniche dei cybercriminali migliorano di giorno in giorno, con il risultato che gli attacchi diventano sempre più sofisticati. La nostra missione è salvare il mondo da tutti i tipi di cyberminacce. Proprio per questo, e per consentire a tutti di navigare in Internet in tutta sicurezza, è essenziale condividere in tempo reale l'intelligence sulle minacce informatiche. Un accesso tempestivo alle informazioni è fondamentale per garantire una protezione efficace di dati e reti.

Eugene Kaspersky
Presidente e CEO, Kaspersky Lab

INTRODUZIONE

Ogni giorno si registrano nuove cyberminacce, che compaiono sotto svariate forme e attraverso molti vettori di attacco differenti.

Non esiste un'unica soluzione in grado di offrire una protezione completa. Tuttavia, anche in un mondo ormai contraddistinto da grandi volumi di dati, sapere da dove proviene il pericolo costituisce già un passo avanti nella lotta contro le minacce più recenti.

È responsabilità dei dirigenti aziendali tutelare le proprie aziende dalle minacce dei nostri giorni e anticipare i pericoli previsti per gli anni a venire. A tale scopo, non è sufficiente solo una protezione operativa efficace contro le minacce conosciute, ma è richiesto un livello di intelligence per la sicurezza strategica che molte poche aziende sono in grado di sviluppare internamente.

Kaspersky Lab sa perfettamente che sono necessarie relazioni durature per garantire prosperità a lungo termine a un'azienda.

Kaspersky Lab è un partner aziendale prezioso, sempre disponibile a condividere informazioni sempre aggiornate con il team dell'azienda attraverso diversi canali. La nostra ampia gamma di metodi di distribuzione permette al Centro operativo di sicurezza/team di sicurezza IT dell'azienda di essere perfettamente attrezzato per proteggere l'organizzazione da qualsiasi tipo di minaccia online.

Anche se un'organizzazione non utilizza i prodotti Kaspersky Lab, potrà comunque beneficiare dei servizi di intelligence per la sicurezza di Kaspersky Lab.

LA SICUREZZA, CON UNA DIFFERENZA

L'intelligence per la sicurezza di livello mondiale è intrinseca nel nostro DNA e ci permette di offrire le più avanzate funzionalità anti-malware sul mercato, influenzando tutte le nostre attività.

È una società basata sulla tecnologia, a partire dal suo CEO, Eugene Kaspersky.

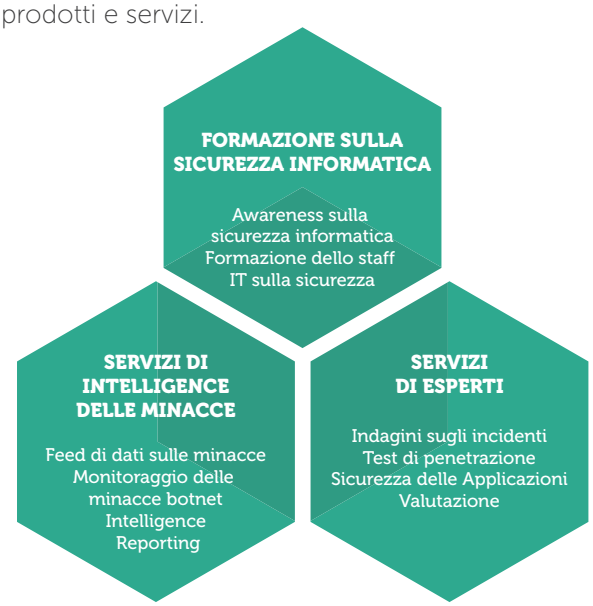
Il nostro Team Ricerca Globale e Analisi (GReAT), un gruppo d'elite di esperti di sicurezza IT, è costantemente impegnato nell'individuare molti dei più pericolosi attacchi mirati e minacce malware al mondo.

Molte tra le più rispettate aziende per la protezione e forze dell'ordine, tra cui INTERPOL, Europol, CERT e la polizia della città di Londra, hanno richiesto attivamente la nostra assistenza.

Kaspersky Lab sviluppa e perfeziona tutte le sue tecnologie di base internamente, pertanto i nostri prodotti e la nostra intelligence sono naturalmente più affidabili ed efficienti.

Gli analisti del settore maggiormente rinomati, tra cui Gartner, Forrester Research e International Data Corporation (IDC), ci qualificano come leader nell'ambito di molte tra le principali categorie di sicurezza IT.

Oltre 130 OEM, inclusi Microsoft, Cisco Meraki, Blue Coat, Juniper Networks, Alcatel Lucent e molti altri, utilizzano le nostre tecnologie all'interno dei loro prodotti e servizi.

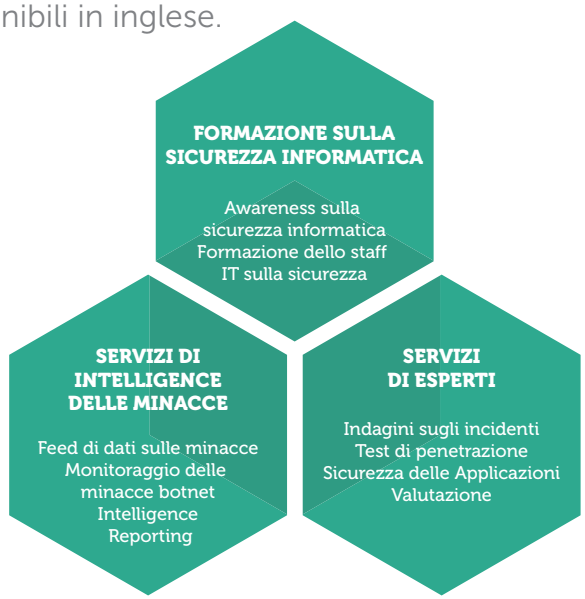


FORMAZIONE SULLA SICUREZZA INFORMATICA

Sfruttate le conoscenze, l'esperienza e l'intelligence di Kaspersky Lab sulla sicurezza informatica con questi innovativi programmi di formazione.

La awareness e la formazione nel campo della sicurezza informatica sono ormai requisiti essenziali per le aziende che devono affrontare un volume crescente di minacce in continua evoluzione. Gli addetti alla sicurezza devono possedere solide competenze sulle tecniche di sicurezza avanzate, componente chiave di un'efficiente gestione aziendale delle minacce e delle strategie di mitigazione. Tutti i dipendenti sono tenuti a possedere conoscenze di base sui pericoli e sulle modalità più sicure per lavorare.

I corsi di formazione sulla sicurezza informatica offerti da Kaspersky Lab sono stati appositamente sviluppati per le aziende alla ricerca di una migliore protezione per la propria infrastruttura e per la proprietà intellettuale a essa correlata. Tutti i corsi di formazione sono disponibili in inglese.



I CORSI

AWARENESS DI TIPO NON INFORMATICO

Dipendenti

- PIATTAFORMA DI FORMAZIONE ONLINE

Line Manager

- GIOCHI SULLA SICUREZZA INFORMATICA

Business Manager

- VALUTAZIONE DELLE CONOSCENZE SULLA SICUREZZA INFORMATICA

FORMAZIONE SULLA SICUREZZA IT

Livello 1: principiante

- ELEMENTI FONDAMENTALI DELLA SICUREZZA DEL CORE
  Conoscenza IT di base
- ELEMENTI PRATICI SULLA SICUREZZA CON LABORATORI
  Conoscenza IT di base

Livello 2: avanzato

- ANALISI FORENSE
  Sono richieste competenze di amministrazione di sistema
- ANALISI DEL MALWARE E REVERSE ENGINEERING
  Sono richieste competenze di programmazione

Livello 3: esperto

- ANALISI FORENSE AVANZATA
  Sono richieste competenze avanzate di amministrazione di sistema
- ANALISI DEL MALWARE AVANZATA E REVERSE ENGINEERING
  Sono richieste competenze sugli assembler

AWARENESS SULLA SICUREZZA INFORMATICA

Moduli di formazione interattivi online e formazione sui giochi per la sicurezza informatica in loco per tutti i dipendenti e i responsabili che utilizzano o gestiscono computer o dispositivi mobili sul lavoro.

La causa di circa l'80% degli incidenti informatici è un errore umano. Le aziende investono grandi somme sui programmi per la awareness sulla sicurezza informatica, ma pochi CISO sono davvero soddisfatti dei risultati. Che cosa non va?

Molti programmi di formazione per la awareness sulla sicurezza informatica sono notevolmente lunghi, tecnici e sostanzialmente negativi. Questa tipologia di corsi non si concentra sui punti di forza dei partecipanti, come i criteri decisionali e le capacità di apprendimento, e, di conseguenza, rende la formazione inefficiente.

Per questo motivo, le aziende sono alla ricerca di approcci di assistenza più evoluti dal punto di vista comportamentale (come lo sviluppo di una cultura aziendale) che offrano un ritorno quantificabile e proficuo sull'investimento nella awareness sulla sicurezza.

I corsi per la awareness sulla sicurezza informatica di Kaspersky Lab servono per:

- Modificare il comportamento, stimolando l'impegno dell'individuo a lavorare al sicuro, costruendo un ambiente aziendale in cui "Tutti sono attenti alla sicurezza informatica. Quindi, mi impegno anche io".
- Condividere un approccio motivazionale, tramite tecniche di apprendimento con giochi, simulazione di attacchi e formazione dettagliata sulle competenze interattive per la sicurezza informatica.

COME FUNZIONA

Completo e chiaro	I corsi di formazione coprono un'ampia gamma di problematiche sulla sicurezza: dalle modalità di perdita di dati agli attacchi malware su Internet, fino al networking sicuro, tramite una serie di esercizi pratici e semplici. Utilizziamo tecniche di apprendimento che aumentano il coinvolgimento durante il processo: esercitazioni e discussioni di gruppo, moduli interattivi, vignette e risorse di gamification.
Motivazione continua	Creiamo momenti di apprendimento tramite giochi e competizioni, rinforzando tali momenti di formazione per tutto il corso dell'anno con esercizi di simulazione di attacchi online, campagne di valutazione e formazione.
Cambiamento dei principi	Insegniamo ai partecipanti che è l'essere umano, e non la macchina, l'obiettivo principale della criminalità informatica. Dimostriamo come, lavorando in modo più scrupoloso, sia possibile evitare di diventare vittime, esponendo se stessi e l'ambiente di lavoro agli attacchi.
Creazione di una cultura sulla sicurezza informatica dell'azienda	Formiamo la dirigenza perché diventi garante della sicurezza: una cultura in cui la sicurezza informatica sia naturale viene veicolata meglio tramite l'impegno e l'esempio dei dirigenti senza l'imposizione del reparto informatico.
Approccio positivo e collaborativo	Dimostriamo in che modo le pratiche di sicurezza influiscano positivamente sull'efficienza dell'azienda e promuovano una collaborazione più efficace con altri dipartimenti interni, tra cui il team per la sicurezza informatica.
Misurabile	Forniamo strumenti per la misurazione delle abilità dei dipendenti, oltre a valutazioni a livello aziendale per l'analisi del comportamento dello staff in materia di sicurezza informatica nel lavoro di tutti i giorni.

FORMAZIONE DELLO STAFF IT SULLA SICUREZZA

I corsi offrono un ampio curriculum su argomenti e tecniche di sicurezza informatica e valutazioni dal livello base a esperto. Tutti i corsi sono impartiti in classe, su richiesta del cliente, o presso un ufficio locale o regionale di Kaspersky Lab, se disponibile.

I corsi prevedono sia lezioni teoriche che laboratori pratici. Al termine di ogni corso, i partecipanti potranno sostenere una valutazione per attestare le loro conoscenze.

PRINCIPIANTE, AVANZATO O ESPERTO?

Il programma tratta tutti gli argomenti, dalle nozioni base sulla sicurezza all'analisi forense avanzata e del malware, consentendo alle aziende di migliorare le loro conoscenze sulla sicurezza informatica in tre aree principali:

- Competenze fondamentali sull'argomento
- Analisi forense e risposta agli incidenti
- Analisi del malware e reverse engineering

VANTAGGI DEL SERVIZIO

LIVELLO 1 – Elementi fondamentali della sicurezza del core
Fornire ad amministratori e responsabili IT la conoscenza di base delle misure pratiche più recenti in materia di sicurezza IT da un leader del settore.

LIVELLO 1 – Elementi pratici sulla sicurezza
Acquisire comprensione dettagliata della sicurezza tramite esercizi pratici con appositi strumenti moderni.

LIVELLI 2-3 – Analisi forense
Migliorare le competenze del team interno di analisi forense e risposta agli incidenti.

LIVELLI 2-3 – Analisi del malware e reverse engineering
Migliorare le competenze del team interno di analisi del malware e reverse engineering.

ESPERIENZA PRATICA

Il prodotto di un leader nel settore della sicurezza, messo a punto grazie alla collaborazione di esperti provenienti da tutto il mondo che partecipano attraverso la propria esperienza al rilevamento e alla prevenzione della criminalità informatica.

DESCRIZIONE DEL PROGRAMMA

ARGOMENTI	Durata	Competenze acquisite
LIVELLO 1 – ELEMENTI FONDAMENTALI DELLA SICUREZZA DEL CORE		
• Panoramica delle cyberminacce e del mercato "underground" • Spam e phishing, sicurezza delle e-mail • Tecnologie per la protezione dalle frodi • Exploit, minacce mobili e APT • Elementi fondamentali delle indagini mediante strumenti Web pubblici • Protezione del luogo di lavoro	2 giorni	• Riconoscere gli incidenti di sicurezza e adottare misure per risolverli • Ridurre il carico di lavoro dei reparti di sicurezza delle informazioni • Aumentare il livello di sicurezza dell'ambiente di lavoro di ogni dipendente tramite strumenti aggiuntivi • Eseguire semplici indagini • Analizzare le mail di phishing • Riconoscere i siti Web falsi o infetti

ARGOMENTI	Durata	Competenze acquisite
LIVELLO 1 – ELEMENTI PRATICI SULLA SICUREZZA		
• Nozioni di base sulla sicurezza • Intelligence open-source • Sicurezza della rete aziendale • Sicurezza delle applicazioni e prevenzione degli exploit • Attacchi DDoS e minacce alle operazioni bancarie • Sicurezza della LAN wireless e della rete mobile globale • Minacce alle operazioni bancarie e ai dispositivi mobili • Risposta agli incidenti di sicurezza negli ambienti virtuali e cloud	5 giorni	• Eseguire indagini di base tramite risorse pubbliche, motori di ricerca specializzati e social network • Creare un perimetro di rete protetto • Competenze di base sui test di penetrazione • Ispezionare il traffico per i diversi tipi di attacco • Garantire la protezione per lo sviluppo di software • Individuare code injection dannosi • Eseguire analisi del malware e forensi di base
LIVELLO 2 – ANALISI FORENSE GENERALE		
• Introduzione all'analisi forense • Acquisizione di prove e risposta live • Elementi interni del Registro di sistema di Windows • Analisi degli elementi di Windows • Analisi dei browser • Analisi delle e-mail	5 giorni	• Creare un laboratorio di analisi forense • Raccogliere prove digitali e gestirle correttamente • Ricostruire un incidente e utilizzare indicatori orari • Individuare tracce di intrusione negli elementi del sistema operativo Windows • Trovare e analizzare la cronologia dei browser e delle e-mail • Essere in grado di adottare gli strumenti di analisi forense
LIVELLO 2 – ANALISI GENERALE DEL MALWARE E REVERSE ENGINEERING		
• Obiettivi e tecniche di analisi del malware e reverse engineering • Elementi interni di Windows, file eseguibili, assembler x86 • Tecniche di analisi statica di base (estrazione di stringhe, analisi delle importazioni, punti di ingresso PE immediati, decompressione automatica, ecc.) • Tecniche di analisi dinamica di base (debugging, strumenti di monitoraggio, intercettazione del traffico, ecc.) • Analisi dei file .NET, Visual Basic, Win64 • Tecniche di analisi basate su script e non PE (file batch, Autoit, Python, Jscript, JavaScript, VBS)	5 giorni	• Creare un ambiente protetto per l'analisi del malware: implementazione di strumenti di sandbox e di tutti gli strumenti necessari • Comprendere i principi dell'esecuzione dei programmi di Windows • Decomprimere, eseguire il debugging e analizzare oggetti dannosi e identificarne le funzioni • Rilevare siti dannosi attraverso l'analisi del malware basata su script • Condurre un'analisi del malware immediata
LIVELLO 3 – ANALISI FORENSE AVANZATA		
• Analisi di Windows approfondita • Recupero dei dati • Analisi di rete e cloud • Analisi della memoria • Analisi della tempistica • Esempi pratici per l'analisi di attacchi mirati nel mondo reale	5 giorni	• Essere in grado di eseguire un'analisi approfondita del file system • Essere in grado di recuperare file eliminati • Essere in grado di analizzare il traffico di rete • Rivelare attività dannose da immagini della memoria • Ricostruire la tempistica dell'incidente
LIVELLO 3 – ANALISI AVANZATA DEL MALWARE E REVERSE ENGINEERING		
• Obiettivi e tecniche di analisi del malware e reverse engineering • Tecniche di analisi statica e dinamica avanzate • (decompressione manuale) • Tecniche di deoffuscamento • Analisi di rootkit e bootkit • Analisi degli exploit (.pdf, .doc, .swf, ecc.) • Analisi del malware non Windows (Android, Linux, Mac OS)	5 giorni	• Utilizzare le best practice più comuni di reverse engineering • Riconoscere le tecniche di anti-reverse engineering (offuscamento, anti-debugging) • Applicare l'analisi del malware avanzata per rootkit/bootkit • Analizzare il codice della shell degli exploit, incorporato in diversi tipi di file • Analizzare il malware non Windows

SERVIZI DI THREAT INTELLIGENCE

Monitorare, analizzare, interpretare e ridurre le minacce alla sicurezza IT in continua evoluzione è un impegno di enorme portata. Le aziende in tutti i settori lamentano la mancanza dei dati rilevanti e aggiornati di cui hanno bisogno per poter gestire i rischi associati alle minacce alla sicurezza IT.

I servizi di Threat Intelligence per la sicurezza di Kaspersky Lab vi forniscono accesso alle informazioni che vi servono per bloccare le minacce, fornite dal nostro team composto dai migliori ricercatori e analisti del mondo.

Le conoscenze, l'esperienza e le informazioni approfondite di Kaspersky Lab su ogni aspetto della sicurezza informatica ne hanno fatto il partner di fiducia delle più importanti agenzie governative e forze dell'ordine, comprese Interpol e CERT. Potete sfruttare queste informazioni nella vostra organizzazione oggi stesso.

I servizi di Threat Intelligence di Kaspersky Lab includono:

- Feed di dati sulle minacce
- Monitoraggio delle minacce botnet
- Report sull'intelligence degli APT

FEED DI DATI SULLE MINACCE

Rinforzate le soluzioni di difesa della rete, con sistemi SIEM, firewall, IPS/IDS, Anti-APT e tecnologie sandbox/di simulazione, eseguendo aggiornamenti in modo regolare, ricavando dati comprensivi e consultando approfondimenti sulle minacce informatiche e sugli attacchi mirati.

Le famiglie di malware e le varianti sono aumentate in maniera esponenziale negli ultimi anni: Kaspersky Lab rileva attualmente circa 325.000 nuovi campioni di malware ogni giorno. Per difendere gli endpoint da queste minacce, la maggior parte delle aziende implementa misure di protezione classiche come le soluzioni anti-malware o i sistemi di prevenzione delle intrusioni o di rilevamento delle minacce. In un ambiente in rapida evoluzione in cui la sicurezza informatica cerca sempre di essere un passo avanti rispetto al cybercrimine, queste soluzioni classiche devono essere supportate da un'intelligence sempre aggiornata sulle minacce informatiche.

I feed di dati sulle minacce di Kaspersky Lab sono pensati espressamente per l'integrazione con i sistemi SIEM (Security Information and Event Management) esistenti, garantendo un grado di protezione aggiuntivo. L'integrazione dei feed di dati sulle minacce rende possibile, ad esempio, correlare i registri che arrivano al sistema SIEM da diversi dispositivi di rete con i feed degli URL di Kaspersky Lab. È inclusa una connessione con il sistema SIEM HP ArcSight. Sono inoltre disponibili i connettori per Splunk e QRadar.

CASI DI UTILIZZO/VANTAGGI DEL SERVIZIO

Feed di dati sulle minacce di Kaspersky Lab:

- Rinforzate la soluzione SIEM sfruttando i dati sugli URL nocivi. Il sistema SIEM riceve le notifiche relative a URL malware, URL di phishing e URL dei server di comando e controllo delle botnet dai registri che arrivano al sistema SIEM da diversi dispositivi di rete (PC degli utenti, proxy di rete, firewall o altri server).
- Potenziate le soluzioni principali per la difesa della rete, tra cui firewall, IPS/IDS, sistemi SIEM, Anti-APT, tecnologie sandbox/di simulazione, dispositivi UTM e così via, aggiornando in modo regolare la threat intelligence.
- Migliorate le capacità di analisi forense fornendo al team di sicurezza informazioni importanti sulle minacce e approfondimenti sulle intenzioni che si celano dietro agli attacchi mirati.
- Supportate la ricerca. Le informazioni su URL e hash MD5 dannosi contenuti nei file nocivi costituiscono un contributo prezioso per i progetti di ricerca sulle minacce.

Kaspersky Lab offre tre tipi di feed di dati sulle minacce:

1. URL nocivi e maschere
2. Database di hash MD5 di oggetti dannosi
3. Feed sulle minacce dei dispositivi mobili

DESCRIZIONE DEI FEED

URL nocivi: un set di URL relativi ai siti Web e ai collegamenti più dannosi. Sono disponibili record mascherati e non mascherati.
URL di phishing: un set di URL identificati da Kaspersky Lab come siti di phishing. Sono disponibili record mascherati e non mascherati.
URL dei server di comando e controllo delle botnet: un set di URL dei server di comando e controllo (C&C) delle botnet e oggetti dannosi correlati.
Hash del malware (ITW): un set di hash dei file e relativi verdetti, che coprono il malware più nocivo e diffuso tramite l'intelligence di KSN.
Hash del malware (UDS): un set di hash dei file rilevati dalle tecnologie cloud di Kaspersky (UDS - Urgent Detection System) sulla base delle statistiche e dei metadati di un file (senza disporre dell'oggetto stesso). Questa operazione consente di identificare nuovi ed emergenti oggetti pericolosi (Zero-day) non rilevati con altri metodi.
Hash del malware mobile: un set di hash dei file per il rilevamento di oggetti pericolosi che infettano le piattaforme mobili.
Feed su Trojan P-SMS: un set di hash Trojan con relativo contesto per il rilevamento di Trojan SMS che generano sovrapprezzi per gli utenti di dispositivi mobili, nonché l'attivazione di un autore di attacchi che ruba, elimina e risponde ai messaggi SMS.
URL dei server di comando e controllo delle botnet mobili: un set di URL contestuali che coprono i server di comando e controllo (C&C) delle botnet mobili.

MONITORAGGIO DELLE MINACCE BOTNET

Servizi avanzati di monitoraggio e notifica per identificare le botnet che minacciano i vostri clienti e la vostra reputazione.

Molti attacchi alle reti sono organizzati mediante botnet. Questi attacchi possono essere rivolti agli utenti privati di Internet, ma spesso le minacce di questo tipo sono indirizzate contro i clienti online di specifiche aziende.

La soluzione avanzata di Kaspersky Lab tiene traccia delle attività delle botnet e fornisce notifiche rapide (entro 20 minuti) delle minacce associate agli utenti di singoli sistemi bancari e di pagamento online. Queste informazioni possono essere utilizzate per avvertire e informare i clienti, fornitori di servizi di sicurezza e forze dell'ordine locali delle minacce in corso. Proteggete oggi stesso la reputazione e i clienti della vostra organizzazione con il servizio di monitoraggio delle minacce botnet di Kaspersky Lab.

CASI DI UTILIZZO/VANTAGGI DEL SERVIZIO

- Grazie agli avvisi proattivi relativi alle minacce provenienti dalle botnet che prendono di mira gli utenti online, l'azienda potrà rimanere sempre un passo avanti rispetto ai nuovi attacchi.
- La possibilità di identificare un elenco degli URL dei server di comando e controllo delle botnet che prendono di mira gli utenti online consente di bloccarli inviando richieste ai CERT o alle forze dell'ordine.
- Migliorate il vostro online banking e i sistemi di pagamento comprendendo la natura dell'attacco.
- Insegnate ai vostri utenti online a riconoscere ed evitare le tecniche di attacco di social engineering.

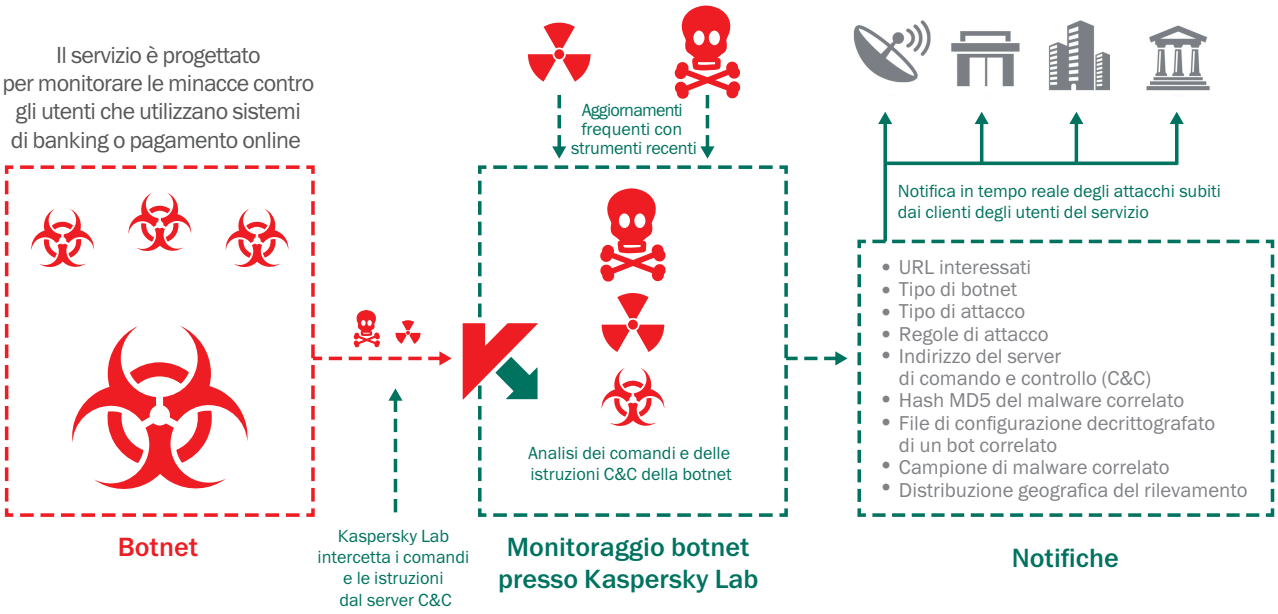
AZIONE IMMEDIATA CON RISULTATI IN TEMPO REALE

Il servizio fornisce una sottoscrizione a notifiche personalizzate contenenti informazioni sui brand corrispondenti grazie all'intercettazione delle parole chiave nelle botnet monitorate da Kaspersky Lab. Le notifiche possono essere inviate tramite e-mail o RSS in formato HTML o JSON. Le notifiche includono:

- **URL sotto attacco:** il malware delle botnet è progettato in modo da attendere che l'utente acceda a uno o più URL dell'organizzazione presa di mira e avviare l'attacco.
- **Tipo di botnet:** consente di comprendere esattamente quale minaccia malware stia utilizzando il cybercriminale a danno delle transazioni dei vostri clienti. Tra gli esempi vi sono Zeus, SpyEye e Citadel.
- **Tipo di attacco:** identifica l'attività per cui i cybercriminali stanno utilizzando il malware, ad esempio Web data injection, registrazione dello schermo, acquisizione video o inoltro a URL di phishing.
- **Regole di attacco:** indicano quali regole di Web code injection vengono utilizzate, come richieste HTML (GET/POST), dati della pagina Web prima dell'immissione, dati della pagina Web dopo l'immissione.
- **Indirizzo del server di comando e controllo (C&C):** consente di notificare il provider di servizi Internet del server identificato per poter neutralizzare più rapidamente la minaccia.
- **Hash MD5 del malware correlato:** Kaspersky Lab fornisce il valore hash che viene utilizzato per la verifica del malware.
- **File di configurazione decrittografato di un bot correlato,** che identifica l'elenco completo degli URL sotto attacco.
- **Campione del malware correlato,** per un'ulteriore analisi forense e reverse engineering dell'attacco botnet.
- **Distribuzione geografica del rilevamento (primi 10 paesi):** dati statistici sui campioni di malware correlati in tutto il mondo.

MONITORAGGIO DELLE MINACCE BOTNET: ARCHITETTURA

DEL SERVER C&C



La soluzione di Kaspersky Lab è disponibile in versione Standard o Premium e offre una vasta gamma di condizioni per l'utilizzo del servizio e URL monitorati. Contattate Kaspersky Lab o il vostro partner/rivenditore per determinare il pacchetto più adeguato alle esigenze della vostra organizzazione.

LIVELLI DI SOTTOSCRIZIONE E RISULTATI FINALI

Standard	Premium	Notifica in formato e-mail o JSON	10 URL monitorati
		• File di configurazione decrittografato di un bot correlato • Campione di malware correlato (su richiesta) • Distribuzione geografica del rilevamento per i campioni di malware correlato	
		Notifica in formato e-mail	5 URL monitorati
		• URL sotto attacco (identificazione degli URL in cui il programma bot prende di mira gli utenti) • Tipo di botnet (ad es., Zeus, SpyEye, Citadel, Kins, ecc.) • Tipo di attacco • Regole di attacco, tra cui: Web data injection, URL, registrazione dello schermo, acquisizione video, ecc. • Indirizzo C&C • Hash MD5 del malware correlato	

REPORT DI INTELLIGENCE

Aumentate la conoscenza e la awareness sulle campagne di cyberspionaggio ad alto profilo con i funzionali e dettagliati report di Kaspersky Lab.

Sfruttando le informazioni e gli strumenti forniti dai report, sarete in grado di rispondere rapidamente alle nuove minacce e alle vulnerabilità emergenti, bloccando gli attacchi provenienti da vettori noti, riducendo i danni causati dagli attacchi avanzati e migliorando la strategia di sicurezza della vostra azienda o dei vostri clienti.

Report sull'intelligence degli APT

Non tutti i nuovi APT (Advanced Persistent Threat) vengono segnalati tempestivamente. La nascita di molti di essi, anzi, non viene mai divulgata. Scegliete di essere i primi a conoscere i nuovi APT con i nostri report dettagliati che forniscono informazioni applicabili.

Agli abbonati al servizio di Report sull'intelligence degli APT forniamo un utile e costante accesso alle nostre indagini e ai relativi risultati, che comprendono dati tecnici completi in un'ampia gamma di formati su ogni nuovo APT scoperto, comprese le minacce che non saranno mai rese pubbliche.

I nostri esperti, i più stimati e competenti del settore nella scoperta di nuovi APT, vi comunicheranno tempestivamente eventuali cambiamenti rilevati nelle strategie dei gruppi cybercriminali e cyberterroristi. Potrete inoltre usufruire di accesso completo al database dei report sugli APT di Kaspersky Lab, un altro potente strumento di ricerca e analisi che apporta valore aggiunto all'esercito per la sicurezza aziendale.

IL REPORT SULL'INTELLIGENCE DEGLI APT DI KASPERSKY FORNISCE:

- **Accesso esclusivo** a descrizioni tecniche sulle minacce più recenti durante le continue indagini, prima della comunicazione pubblica.
- **Approfondimenti sugli APT non pubblici**. Non tutte le minacce ad alto profilo vengono comunicate pubblicamente. Alcune di esse, a causa delle vittime che vengono colpite, della sensibilità dei dati, della natura delle vulnerabilità relative ai processi di recupero o della relativa attività di applicazione dei criteri, non vengono rese pubbliche. Tuttavia, i nostri clienti ne verranno sempre a conoscenza.
- **Dati tecnici** dettagliati a supporto, campioni e strumenti, tra cui un elenco esteso di Indicatori di compromissione (IOC), disponibile in formati standard quali openIOC o STIX, e accesso alle nostre norme Yara.
- **Monitoraggio continuo delle campagne APT**. Accesso a informazioni di intelligence applicabili durante le indagini (informazioni sulla distribuzione degli APT, sugli IOC e sull'infrastruttura di comando e controllo).
- **Analisi retrospettive**. **Durante il periodo di validità dell'abbonamento, forniamo** accesso all'archivio dei report privati.

NOTA: RISERVATO AGLI ABBONATI

A causa della natura specifica e sensibile di alcune delle informazioni contenute nei report forniti tramite questo servizio, siamo costretti a riservare gli abbonamenti solo a enti governativi, istituzioni pubbliche e aziende private.

REPORT DI INTELLIGENCE

Report specifico sulla Threat Intelligence di un cliente

Qual è il miglior modo per attaccare la vostra organizzazione? Quale percorso e quali informazioni sono disponibili ai cybercriminali che intendono attaccare la vostra azienda? Avete già subito un attacco o siete sotto minaccia?

Il report specifico sulla Threat Intelligence di un cliente offerto da Kaspersky risponde a queste e a molte altre esigenze. I nostri esperti creano un quadro completo sullo stato dell'attacco in corso, identificando i punti deboli da migliorare e rilevando le prove degli attacchi del passato, di quelli in corso, nonché di quelli pianificati per il futuro.

Supportate da informazioni così dettagliate, le aziende potranno concentrare la strategia di difesa sulle aree maggiormente inclini a subire attacchi dai cybercriminali, adottando misure rapide e precise per respingere gli intrusi e ridurre al minimo il rischio che gli attacchi possano provocare danni.

Sviluppati con sistemi di intelligence open-source (OSINT), sistemi e database di analisi dettagliata di Kaspersky Lab e con la nostra esperienza sulle reti "underground" dei cybercriminali, i report coprono aree quali:

- **Identificazione dei vettori della minaccia:** identificazione e analisi dello stato dei componenti critici disponibili esternamente, tra cui ATM, sistemi di videosorveglianza e altri sistemi che utilizzano tecnologie mobili, i profili dei dipendenti sui social network e gli account e-mail del personale, potenziali obiettivi di un attacco.
- **Analisi sul monitoraggio del malware e dell'attacco informatico:** identificazione, monitoraggio e analisi di un potenziale malware attivo o disattivo indirizzato sulla vostra organizzazione, delle attività di botnet passate o in corso e di eventuali attività sospette sulla rete.
- **Attacchi di terzi:** prova dell'attività di botnet o di minaccia indirizzata in modo particolare sui vostri clienti, partner e abbonati, i cui sistemi infetti potrebbero essere utilizzati per un attacco diretto alla vostra azienda.
- **Perdita delle informazioni:** tramite il monitoraggio discreto delle community e dei forum online "underground", siamo in grado di scoprire se gli hacker stanno pianificando un attacco alla vostra azienda o, ad esempio, se un dipendente disonesto sta divulgando informazioni.
- **Stato dell'attacco in corso:** gli attacchi APT possono continuare per anni, senza essere rilevati. Se rileviamo un attacco in corso sulla vostra infrastruttura, vi forniamo la consulenza per consentirvi di risolvere in modo efficiente il problema.

AVVIO RAPIDO – SEMPLICITÀ D'USO – NESSUNA RISORSA NECESSARIA

Una volta stabiliti i parametri e il formato dei dati preferiti (per i report specifici sui clienti), non è necessaria alcuna infrastruttura aggiuntiva per iniziare a usare il servizio di Kaspersky Lab.

Il report sulla Threat Intelligence di Kaspersky non compromette l'integrità e la disponibilità delle risorse, comprese quelle di rete.

SERVIZI DEGLI ESPERTI

I servizi degli esperti di Kaspersky Lab offrono la consulenza dei nostri esperti interni, molti dei quali autorità di livello mondiale per il settore e professionisti indipendenti, le cui competenze ed esperienza sono di cruciale importanza per la nostra reputazione come leader mondiali nel settore dell'intelligence per la sicurezza.

Dal momento che non esistono infrastrutture IT uguali e che le minacce informatiche più potenti sono appositamente ideate per sfruttare le vulnerabilità specifiche delle singole aziende, anche il servizio dei nostri esperti è su misura della vostra azienda. I servizi descritti nelle pagine che seguono fanno parte del nostro kit professionale: alcuni o tutti i servizi, in parte o completamente, possono essere applicati durante la collaborazione con la vostra azienda.

Il nostro obiettivo primario è di collaborare con voi e con la vostra azienda in qualità di consulenti esperti, per aiutarvi a valutare il rischio, a rinforzare la sicurezza e a ridurre al minimo il rischio di future minacce.

I servizi degli esperti comprendono:

- Indagini sugli incidenti
- Test di penetrazione
- Valutazione della sicurezza delle applicazioni

INDAGINI SUGLI INCIDENTI

Analisi forense | Analisi del malware

Supporto personalizzato per le indagini sugli incidenti in grado di aiutare l'organizzazione a identificare e risolvere i problemi di sicurezza IT.

I cyberattacchi stanno diventando un pericolo sempre più presente per le reti aziendali. Personalizzati in modo da sfruttare le vulnerabilità specifiche dell'obiettivo prescelto dai cybercriminali, questi attacchi sono spesso progettati con l'intento di sottrarre o distruggere informazioni riservate o proprietà intellettuali, minare i processi operativi, danneggiare gli impianti industriali o rubare denaro.

Proteggere un'azienda da questi attacchi sofisticati e ben pianificati è diventato sempre più complicato. Può risultare addirittura difficile stabilire con certezza se un'organizzazione è effettivamente sotto attacco.

I servizi di indagine sugli incidenti di Kaspersky Lab possono aiutare le aziende a realizzare le proprie strategie di difesa fornendo un'analisi approfondita delle minacce e la necessaria consulenza sulle misure appropriate da adottare per la risoluzione dell'incidente.

VANTAGGI DEL SERVIZIO

I servizi di indagine di Kaspersky Lab aiutano i clienti a risolvere i problemi di sicurezza live e a comprendere il comportamento del malware e le sue conseguenze, fornendo indicazioni dettagliate su come risolverli. Questo approccio aiuta indirettamente le aziende a:

- Ridurre i costi legati alla risoluzione dei problemi derivanti da una cyberinfezione
- Arrestare la perdita di informazioni riservate che potrebbero essere sottratte dai PC infetti
- Ridurre i rischi per la reputazione causati dal danneggiamento dei processi operativi correlato all'infezione
- Ripristinare il normale funzionamento dei PC danneggiati dall'infezione

Le indagini di Kaspersky Lab sono condotte da analisti esperti con competenze pratiche in analisi forense e del malware. Al termine dell'indagine, viene fornito un report dettagliato con i risultati completi dell'indagine sulla cyberminaccia e le misure di correzione proposte.

ANALISI FORENSE

L'analisi forense è un servizio di indagine mirato a fornire un'immagine dettagliata di un incidente. Questo tipo di analisi può includere anche l'analisi del malware, in caso di rilevamento di un malware durante l'indagine. Gli esperti di Kaspersky Lab mettono assieme le prove per comprendere esattamente quello che sta succedendo, avvalendosi dell'uso di immagini del disco rigido, dati estratti dalla memoria e tracce sulla rete. Il risultato è una spiegazione dettagliata dell'incidente.

Il cliente avvia il processo raccogliendo le prove e definendo il contesto dell'incidente. Gli esperti di Kaspersky Lab analizzano i sintomi dell'incidente, identificano l'eventuale malware binario e conducono l'analisi del malware per fornire un report dettagliato comprensivo delle necessarie misure di correzione.

ANALISI DEL MALWARE

L'analisi del malware offre una spiegazione completa del comportamento e degli obiettivi degli specifici file di malware che prendono di mira un'organizzazione.

Gli esperti di Kaspersky Lab conducono un'analisi approfondita del campione di malware fornito dall'organizzazione, creando un report dettagliato che include:

- **Proprietà del campione:** una breve descrizione del campione e il verdetto sulla classificazione del malware.
- **Descrizione dettagliata del malware:** un'analisi approfondita delle funzioni, del comportamento e degli obiettivi della minaccia nel campione del malware, inclusi gli indicatori di compromissione, che fornirà le informazioni necessarie a neutralizzarne le attività.
- **Scenario di correzione:** il report suggerirà le misure necessarie per proteggere completamente l'organizzazione da questo tipo di minaccia.

OPZIONI DI DISTRIBUZIONE

I servizi di indagine di Kaspersky Lab sono disponibili:

- tramite abbonamento, per un numero concordato di incidenti
- in risposta a un singolo incidente

SERVIZIO DI TEST DI PENETRAZIONE

Garantire la completa protezione dell'infrastruttura IT dai potenziali attacchi informatici rappresenta un impegno costante per qualsiasi organizzazione. Tuttavia, per le aziende di grandi dimensioni, con migliaia di dipendenti, centinaia di sistemi informatici e numerose sedi in tutto il mondo, la sfida è ancora più dura.

Mentre gli specialisti IT e i responsabili della sicurezza lavorano duro per garantire che tutti i componenti della rete siano al contempo protetti dalle intrusioni e completamente disponibili per gli utenti legittimi, una sola vulnerabilità può rappresentare una "porta aperta" per qualsiasi intento di cybercriminalità, che consente agli intrusi di ottenere il controllo sui sistemi informatici aziendali.

I test di penetrazione offrono una dimostrazione pratica dei potenziali scenari di attacco nel momento in cui un agente pericoloso tenta di superare i controlli di sicurezza della rete aziendale per ottenere privilegi elevati sui sistemi importanti.

Il servizio di test di penetrazione di Kaspersky Lab fornisce una awareness più profonda sui difetti del sistema di sicurezza dell'infrastruttura aziendale, portando alla luce le vulnerabilità, analizzando le possibili conseguenze delle diverse forme di attacco, valutando l'efficienza delle misure di protezione in uso e consigliando azioni correttive e miglioramenti.

I test di penetrazione di Kaspersky Lab aiutano voi e la vostra organizzazione a:

- **Identificare i punti più deboli della rete,** per consentirvi di realizzare decisioni informate sui punti in cui concentrare l'attenzione e il budget, al fine di ridurre al minimo i rischi per il futuro.
- **Evitare perdite finanziarie, operative e della reputazione, conseguenza degli attacchi informatici,** prevenendo il verificarsi di questi attacchi tramite il rilevamento attivo e la correzione delle vulnerabilità.
- **Rispettare gli standard governativi, settoriali o aziendali** che richiedono questa forma di valutazione della sicurezza (ad esempio lo standard PCI DSSP (Payment Card Industry Data Security Standard)).

SCOPO E OPZIONI DEL SERVIZIO

A seconda delle esigenze e in base all'infrastruttura IT, potete scegliere di applicare uno o una serie dei seguenti servizi di test di penetrazione:

- **Test di penetrazione esterno:** valutazione del sistema di sicurezza condotta su Internet tramite un "aggressore" che non conosce nello specifico i sistemi in uso.
- **Test di penetrazione interno:** scenari basati su un aggressore interno, come un visitatore con accesso fisico agli uffici aziendali o un fornitore esterno con accesso limitato ai sistemi.
- **Test sul social engineering:** valutazione della awareness sulla sicurezza da parte del personale, tramite la simulazione di attacchi social, quali phishing, link pseudo-nocivi contenuti nelle e-mail, allegati sospetti e altro ancora.
- **Valutazione della sicurezza delle reti wireless:** i nostri esperti visiteranno il sito della vostra azienda per analizzare i controlli di sicurezza Wi-Fi.

Tra gli obiettivi del test di penetrazione, potete includere qualsiasi parte dell'infrastruttura IT. Tuttavia, consigliamo di analizzare l'intera rete o i segmenti più ampi, dal momento che i risultati del test sono sempre più attendibili quando i nostri esperti lavorano, come i potenziali aggressori, nelle stesse condizioni.

RISULTATI DEI TEST DI PENETRAZIONE

Il servizio di test di penetrazione è ideato per portare alla luce i limiti del sistema di sicurezza che potrebbero essere sfruttati per ottenere accesso non autorizzato ai componenti importanti della rete. Tra i difetti, si ricordano:

- Architettura di rete vulnerabile, protezione di rete non sufficiente
- Vulnerabilità che causano intercettazione e reindirizzamento del traffico della rete
- Autenticazione e autorizzazioni non sufficienti per i diversi servizi
- Credenziali utente deboli
- Difetti di configurazione, tra cui privilegi utente eccessivi
- Vulnerabilità causate da errori nel codice dell'applicazione (code injection, attraversamento percorso, vulnerabilità lato cliente e così via)
- Vulnerabilità causate dall'uso di versioni hardware e software obsolete privi dei più recenti aggiornamenti della sicurezza
- Divulgazione di informazioni

I risultati vengono forniti in un report finale che comprende informazioni tecniche dettagliate sulla procedura del test, i risultati, le vulnerabilità rilevate e consigli sulle correzioni, insieme a un riepilogo per la dirigenza in cui vengono evidenziati i risultati del test e i vettori di attacco. Se necessario, siamo inoltre in grado di fornire video e presentazioni per lo staff tecnico o per la dirigenza.

INFORMAZIONI SULL'APPROCCIO DI KASPERSKY LAB VERSO I TEST DI PENETRAZIONE

Mentre i test di penetrazione simulano veri e propri attacchi da parte di hacker, questi test vengono controllati rigidamente ed eseguiti dagli esperti di sicurezza di Kaspersky Lab con grande attenzione verso la riservatezza dei sistemi aziendali, nonché in stretta conformità con gli standard e le best practice internazionali tra cui:

- PTES (Penetration Testing Execution Standard)
- NIST Special Publications 800-115, Technical Guide to Information Security Testing and Assessment
- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- Classificazione delle minacce del WASC (Web Application Security Consortium)
- Guida ai test dell'OWASP (Open Web Application Security Project)
- CVSS (Common Vulnerability Scoring System)

I membri del team del progetto sono professionisti esperti con competenze pratiche dettagliate e aggiornate sul campo, riconosciuti come consulenti di sicurezza da aziende leader del settore quali Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens e SAP.

OPZIONI DI DISTRIBUZIONE:

A seconda del tipo di servizio di valutazione del sistema di sicurezza, delle specifiche tecniche dei sistemi aziendali e delle pratiche di lavoro, i servizi di valutazione possono essere offerti da remoto o in loco. La maggior parte dei servizi può essere fornita da remoto e i test di penetrazione interni possono essere eseguiti tramite accesso VPN, mentre alcuni servizi (come ad esempio la valutazione della sicurezza delle reti wireless) richiede la presenza in loco.

SERVIZI DI VALUTAZIONE DELLA SICUREZZA DELLE APPLICAZIONI

Sia che sviluppiate internamente le applicazioni aziendali, sia che le acquistiate da fornitori terzi, sapete che un solo errore di codifica può generare vulnerabilità che espongono l'azienda ad attacchi informatici, con conseguenti notevoli danni finanziari e alla reputazione. Inoltre, durante il ciclo di vita dell'applicazione possono generarsi nuove vulnerabilità, tramite aggiornamenti software o configurazioni non sicure dei componenti, o, addirittura, potrebbero emergere dai nuovi metodi di attacco.

I servizi di valutazione della sicurezza delle applicazioni offerti da Kaspersky Lab rivelano le vulnerabilità di applicazioni di qualsiasi tipo, dalle grandi soluzioni basate su cloud, ai sistemi ERP, alle applicazioni di online banking o altre applicazioni specifiche dell'azienda, fino alle applicazioni mobili o integrate su diverse piattaforme (iOS, Android e altre).

Grazie alla combinazione di esperienza e competenze pratiche, unite alle best practice internazionali, i nostri esperti rilevano i limiti dei sistemi di sicurezza che possono esporre l'organizzazione a minacce quali:

- Deviazione dei dati riservati
- Infiltrazione e modifica di dati e sistemi
- Avvio di attacchi DOS (Denial-of-Service)
- Avvio di attività fraudolente

Seguendo i nostri consigli, le vulnerabilità rilevate nelle applicazioni possono essere corrette, prevenendo gli attacchi.

VANTAGGI DEL SERVIZIO

I servizi di valutazione della sicurezza delle applicazioni offerti da Kaspersky Lab aiutano i proprietari e gli sviluppatori delle applicazioni a:

- **Evitare perdite finanziarie, operative e della reputazione**, rilevando attivamente e correggendo le vulnerabilità che vengono utilizzate per portare a termine gli attacchi alle applicazioni.
- **Risparmiare sui costi di correzione** monitorando le vulnerabilità nelle applicazioni anche durante le fasi di sviluppo e valutazione, prima che raggiungano l'ambiente degli utenti, in cui la correzione potrebbe comportare interruzioni e spese considerevoli.
- **Supportare un ciclo di vita di sviluppo software sicuro** (S-SDLC) al fine di creare e continuare a lavorare con applicazioni sicure.
- **Rispettare gli standard governativi, settoriali o aziendali** in materia di sicurezza delle applicazioni, quali gli standard PCI DSS o HIPAA.

SCOPO E OPZIONI DEL SERVIZIO

La valutazione può essere eseguita sul sito Web e sulle applicazioni ufficiali dell'azienda, standard o basate su cloud, applicazioni mobili o integrate.

I servizi vengono realizzati in base alle esigenze aziendali e alle specifiche delle applicazioni, e potrebbero includere:

- **Test della scatola nera:** simulazione di un attacco esterno.
- **Test della scatola grigia:** simulazione di utenti ammessi con una gamma di profili.
- **Test della scatola bianca:** analisi con accesso completo all'applicazione e ai codici sorgente della stessa; questo approccio risulta il più efficiente in termini numero di vulnerabilità rilevate.
- **Valutazione dell'efficienza del firewall dell'applicazione:** le applicazioni vengono verificate con protezione firewall attiva e disattivata, al fine di rilevare le vulnerabilità e verificare il blocco di potenziali exploit.

RISULTATI

Le vulnerabilità che possono essere identificate dai servizi di valutazione della sicurezza delle applicazioni offerti da Kaspersky Lab comprendono:

- Difetti nell'autenticazione e nelle autorizzazioni, nonché nell'autenticazione a più fattori
- Code injection (SQL Injection, OS Commanding, ecc.)
- Vulnerabilità nella logica che comportano frodi
- Vulnerabilità lato cliente (Script cross-site, Cross-Site Request Forgery, ecc.)
- Uso di crittografia debole
- Vulnerabilità nelle comunicazioni client-server
- Archiviazione o trasferimento dati non sicuri, come ad esempio la mancanza di una maschera PAN nei sistemi di pagamento
- Difetti di configurazione, tra cui difetti che comportano attacchi alla sessione
- Divulgazione di informazioni riservate
- Altre vulnerabilità dell'applicazione Web che causano le minacce elencate nella Classifica delle minacce WASC v2.0 e quelle riportate nella lista OWASP Top Ten.

I risultati vengono forniti in un report finale che comprende informazioni tecniche dettagliate sulla procedura di valutazione, i risultati, le vulnerabilità rilevate e consigli sulle correzioni, insieme a un riepilogo in cui vengono evidenziate le implicazioni a livello dirigenziale. Se necessario, siamo inoltre in grado di fornire video e presentazioni per lo staff tecnico o per la dirigenza.

INFORMAZIONI SULL'APPROCCIO DI KASPERSKY LAB VERSO LA VALUTAZIONE DELLA SICUREZZA DELLE APPLICAZIONI

Le valutazioni sulla sicurezza delle applicazioni vengono eseguite dagli esperti di sicurezza di Kaspersky Lab manualmente o tramite strumenti automatizzati, con grande attenzione verso la riservatezza, l'integrità e la disponibilità dei sistemi aziendali, nonché in stretta conformità con gli standard e le best practice internazionali tra cui:

- Classificazione delle minacce del WASC (Web Application Security Consortium)
- Guida ai test dell'OWASP (Open Web Application Security Project)
- Guida ai test per la sicurezza mobile OWASP
- Altri standard, a seconda della tipologia e della sede dell'azienda.

I membri del team del progetto sono professionisti esperti con competenze pratiche dettagliate e aggiornate sul campo, su diverse piattaforme, su linguaggi di programmazione, framework, vulnerabilità e metodi di attacco differenti. I nostri consulenti partecipano come esperti alle conferenze internazionali del settore e offrono servizi di consulenza sulla sicurezza ai principali fornitori di applicazioni e servizi basati su cloud, tra cui Oracle, Google, Apple, Facebook e PayPal.

OPZIONI DI DISTRIBUZIONE:

A seconda del tipo di servizio di valutazione del sistema di sicurezza, delle specifiche dei sistemi oggetto di verifica e dei requisiti aziendali per le condizioni di lavoro, i servizi di valutazione possono essere offerti da remoto o in loco. La maggior parte dei servizi può essere eseguita da remoto.


Twitter.com/
KasperskyLabIT


Facebook.com/
Kasperskylabitalia


Youtube.com/
Kasperskyitalia

Kaspersky Lab, Mosca, Russia
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

Trovate il partner più vicino:
ww.kaspersky.it/buyoffline

Per ulteriori informazioni sui prodotti e servizi offerti nel presente catalogo o per ricevere informazioni sull'applicabilità di questi servizi alla sicurezza della vostra azienda, vi invitiamo a contattarci tramite e-mail all'indirizzo intelligence@kaspersky.com

I termini e le condizioni applicabili possono variare a seconda dell'area geografica, ma non dipendono da: scopo del lavoro, tempistiche, disponibilità locale dei servizi, lingua di lavoro, costi.

Catalogo sui servizi di intelligence per la sicurezza, agosto 2015 GL

KASPERSKY lab