KASPERSKY lab

Kaspersky Cybersecurity Services 2017

www.kaspersky.de
#truecybersecurity

Cyberverbrechen nehmen stetig zu, und ihr technisches Potenzial wächst rasant: Jeden Tag sehen wir, wie die Angriffe immer ausgereifter werden. Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um dies zu erreichen und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben werden. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz von Daten und Netzwerken unerlässlich.

Eugene Kaspersky
Gründer und CEO, Kaspersky Lab

Einleitung

Jeden Tag entstehen neue Cyberbedrohungen in den unterschiedlichsten Formen und über viele verschiedene Angriffsvektoren.

Es gibt keine einzelne Lösung, die vollständigen Schutz bietet. Jedoch besteht selbst in unserer Big-Data-Welt ein großer Teil des Kampfes gegen die aktuellen Bedrohungen darin, zu wissen, wo man nach Gefahren suchen soll.

Als Geschäftsführer, CIO, CISO oder CTO liegt es in Ihrer Verantwortung, Ihr Unternehmen vor den heutigen Bedrohungen zu schützen und die Gefahren vorauszuahnen, die in den nächsten Jahren auf Sie zukommen. Dazu ist mehr als nur ein zuverlässiger technologischer Schutz vor bekannten Bedrohungen erforderlich. Sie benötigen strategische Sicherheitsinformationen, für deren Erhebung die wenigsten Unternehmen über genügend interne Ressourcen verfügen.

Wir bei Kaspersky Lab verstehen, dass ein langfristiger Geschäftserfolg auf langfristigen Beziehungen beruht.

Mit Kaspersky Lab an Ihrer Seite erhalten Sie stets in Echtzeit wichtige Informationen über aktuelle Bedrohungen. Unsere breite Auswahl an Bereitstellungsmethoden bereitet Ihr Security Operation Center (SOC)/IT-Sicherheitsteam darauf vor, das Unternehmen vor Online-Bedrohungen zu beschützen.

Selbst wenn Ihr Unternehmen keine Produkte von Kaspersky Lab einsetzt, können Sie dennoch von den Kaspersky Lab Cybersecurity Services profitieren.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Trainings**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Sicherheit mit dem entscheidenden Unterschied

Den aktuellen Bedrohungen mit unseren Security Intelligence Services immer einen Schritt voraus zu sein, ist unser Anspruch. Dadurch sind wir in der Lage, einen leistungsstarken Malware-Schutz auf dem Markt bereitzustellen.

In unserem Unternehmen steht Technologie auf allen Ebenen im Mittelpunkt und bei unserem CEO Eugene Kaspersky an allererster Stelle.

Unser Global Research & Analysis Team (GReAT) besteht aus erfahrenen IT-Sicherheitsexperten, die bei der Erkennung einiger der weltweit gefährlichsten Malware-Bedrohungen und gezielten Angriffe federführend war.

Viele der weltweit anerkanntesten Sicherheitsunternehmen und Vollzugsbehörden, darunter INTERPOL, Europol, CERT und die Polizei Londons, haben uns aktiv um Unterstützung gebeten.

Kaspersky Lab entwickelt alle unternehmenseigenen Kerntechnologien intern, was die Zuverlässigkeit unserer Produkte und Dienstleistungen erhöht, denn alle unsere Technologien greifen nahtlos ineinander.

Die renommiertesten Branchenanalysten, darunter Gartner, Forrester Research und International Data Corporation (IDC), setzen uns in vielen wichtigen IT-Sicherheitskategorien an die Spitzenposition.

Mehr als 130 OEMs nutzen unsere Technologien innerhalb ihrer eigenen Produkte und Services, darunter Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent und mehr.

Kaspersky Threat Intelligence Services

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen verfügen oft nicht über die aktuellen und relevanten Daten, die für einen effektiven Umgang mit den Risiken der IT-Sicherheitsbedrohungen erforderlich sind.

Kaspersky Cybersecurity Services

Kaspersky Threat Intelligence Services

Threat Data Feeds
APT Intelligence Reporting
Tailored Threat Reporting
Kaspersky Threat Lookup
Kaspersky Phishing Tracking
Kaspersky Botnet Tracking

Kaspersky Threat Hunting Services

Kaspersky Security Trainings

Kaspersky Incident Response Services

Kaspersky Security Assessment Services

Die Threat Intelligence Services von Kaspersky Lab geben Ihnen Zugriff auf alle Informationen, die Sie zur Abwehr dieser Bedrohungen benötigen. Sie werden zur Verfügung gestellt von unserem weltweiten Team aus Forschern und Analysten.

Wissen, Erfahrung und umfassende Erkenntnisse über praktisch jeden Aspekt der Cybersicherheit haben Kaspersky Lab zum vertrauenswürdigen Partner renommierter internationaler Strafverfolgungs- und Regierungsbehörden, darunter Interpol und CERTS, gemacht. Auch Sie können dieses Wissen für Ihr Unternehmen nutzen.

Die Threat Intelligence Services von Kaspersky Lab beinhalten:

- Threat Data Feeds
- APT Intelligence Reporting
- Tailored Threat Reporting
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

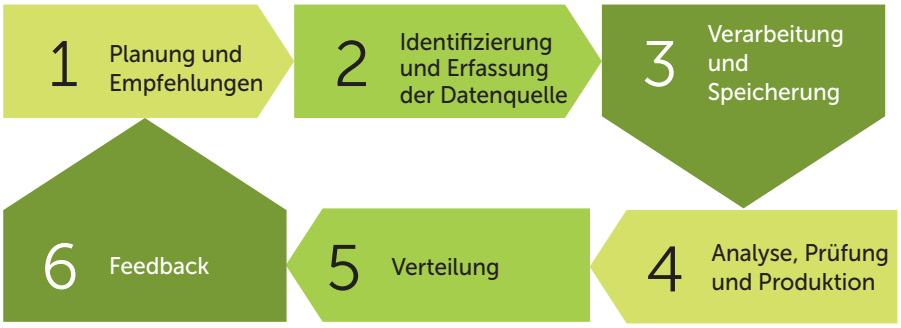
Threat Data Feeds

Andere Sicherheitsanbieter und Unternehmen nutzen Kaspersky Threat Data Feeds, um **eigene Sicherheitslösungen zu entwickeln oder ihr Unternehmen zu schützen**.

Cyberangriffe geschehen jeden Tag. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. **Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger.** Die Angreifer nutzen komplizierte **Kill Chains**, Kampagnen und angepasste **Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um in Systeme einzudringen und Ihre Geschäftsabläufe zu unterbrechen oder Ihre Kunden zu schädigen**.

Kaspersky Lab informiert Ihr Unternehmen bzw. Ihre Kunden **regelmäßig** mit **aktualisierten Threat Data Feeds über Risiken und Auswirkungen** von Cyberbedrohungen. Diese helfen Ihnen, **Bedrohungen effektiver zu bekämpfen** und Ihr Unternehmen **besser vor Angriffen zu schützen**, noch bevor diese eingeleitet werden.

Informationszyklus



Die Data Feeds

Die Feeds umfassen Folgendes:

- IP Reputation Feed – Gruppen von IP-Adressen mit Kontext zu verdächtigen und schädlichen Hosts
- Malicious and Phishing URL Feed – Enthält schädliche bzw. Phishing-Links und -Websites
- Botnet C&C URL Feed – Enthält C&C-Server für Desktop-Botnets sowie zugehörige schädliche Objekte
- Mobile Botnet C&C URL Feed – Enthält C&C-Server für mobile Botnets, um infizierte Geräte zu erkennen, die mit C&C-Servern kommunizieren
- Malicious Hash Feed – Umfasst die gefährlichste am weitesten verbreitete und neu aufkommende Malware
- Mobile Malicious Hash Feed – Unterstützt die Erkennung schädlicher Objekte, die mobile Android- und iOS-Plattformen infizieren
- P-SMS Trojan Feed – Unterstützt die Erkennung von SMS-Trojanern, über die Angreifer SMS-Nachrichten stehlen, löschen oder beantworten und Sondergebühren für mobile Nutzer erheben können
- Whitelisting Data Feed – Versorgt Lösungen und Services von Drittanbietern mit systematischen Informationen zu legitimer Software
- **NEU!!! Kaspersky Transforms for Maltego** – Bietet Maltego-Benutzern eine Reihe von Transformationen, über die sie Zugriff auf Kaspersky Threat Data Feeds erhalten. Mit Kaspersky Transforms for Maltego können Sie URLs, Hashes und IP-Adressen mithilfe der Feeds von Kaspersky Lab überprüfen. Die Transformationen können die Kategorie eines Objekts bestimmen und nützlichen Kontext bereitstellen.

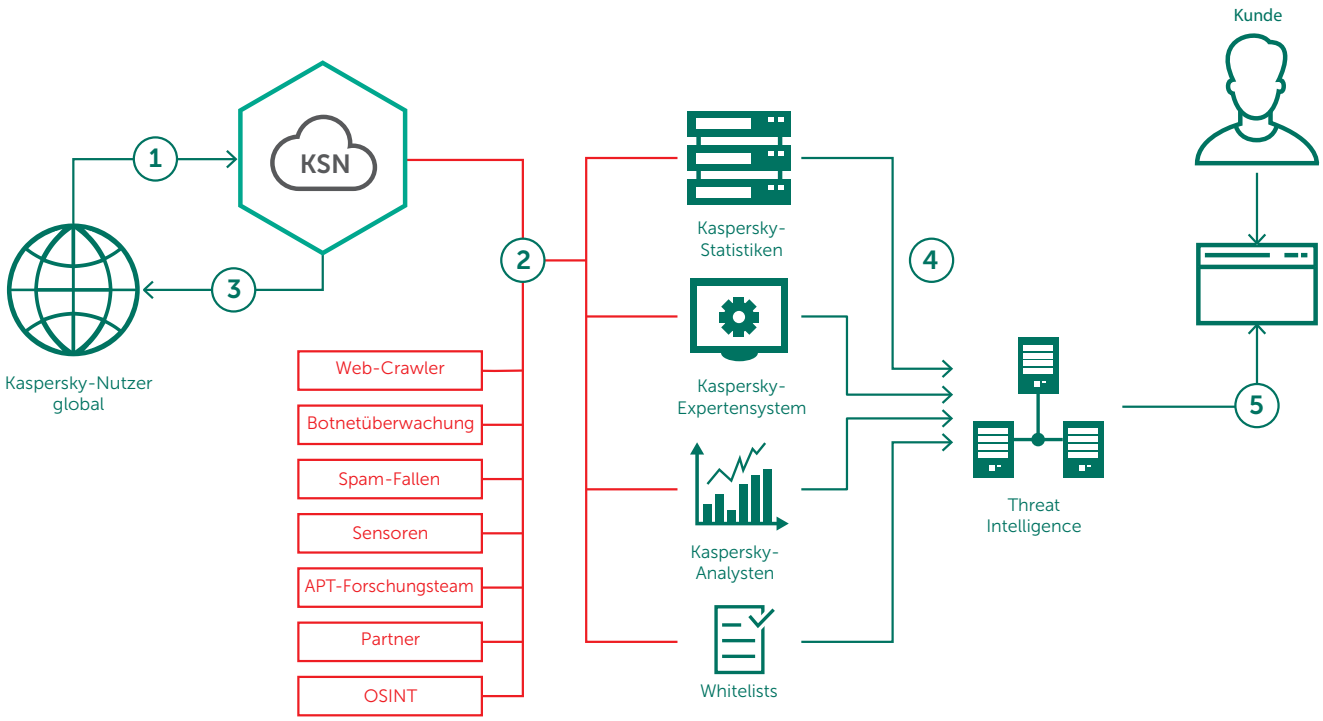
Kontextdaten

Jeder Datensatz in jedem Data Feed wird mit **umfangreichem Kontext** angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gesetzt werden, liefern sie schneller Antworten auf die Fragen **„Wer?“, „Was?“, „Wo?“ und „Wann?“**. Außerdem geben sie Aufschluss über Ihre Gegner, sodass Sie rechtzeitig Entscheidungen treffen und die **richtigen Maßnahmen für Ihr Unternehmen** finden können.

Erfassung und Verarbeitung

Unsere Data Feeds werden aus zusammengeführten, heterogenen und äußerst zuverlässigen Quellen bezogen, darunter das Kaspersky Security Network, unsere eigenen Webcrawler, unser Service zur Botnet-Überwachung (Überwachung von Botnets und ihrer Ziele und Aktivitäten rund um die Uhr, das ganze Jahr) sowie Spam-Fallen, Forschungsteams und Partner.

Dann werden sämtliche zusammengefassten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Expertensysteme von Kaspersky Lab (Sandboxes, heuristische Engines, Multi-Scanner, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Analysten und die Verifizierung anhand von Whitelists.



Kaspersky Threat Data Feeds enthalten sorgfältig geprüfte Daten zu Bedrohungsindikatoren, die in Echtzeit aus realen Datenquellen bezogen werden.

Service-Highlights

- Data Feeds mit vielen **False Positives** sind wertlos. Deshalb werden die Feeds vor ihrer Veröffentlichung umfassend getestet und gefiltert, um zu gewährleisten, dass nur überprüfte Daten bereitgestellt werden.
- Die Data Feeds werden automatisch in Echtzeit generiert – basierend auf den weltweit vom Kaspersky Security Network erfassten Daten, die einen Einblick in einen signifikanten Anteil des gesamten Internetdatenverkehrs und alle möglichen Datentypen von Millionen von Endbenutzern in mehr als 213 Ländern gewähren. So werden **hohe Erkennungsraten** garantiert.
- Sämtliche Feeds werden über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die **dauerhafte Verfügbarkeit** gewährleistet.
- Die Feeds ermöglichen die **umgehende Erkennung von URLs**, die für Phishing, Malware, Exploits, Botnets und andere schädliche Inhalte genutzt werden.
- **Malware** in allen Arten von Datenverkehr (Web, E-Mail, P2P, IM usw.) sowie gezielte mobile Malware kann **sofort erkannt** und identifiziert werden.
- Einfache **Verteilungsformate** (**JSON, CSV, OpenIoC, STIX**) über **HTTPS** oder Ad-hoc-Bereitstellungsmechanismen ermöglichen die einfache Integration der Daten in Sicherheitslösungen.
- Hunderte von Experten, darunter **Sicherheitsanalysten** aus der ganzen Welt, weltweit anerkannte **Sicherheitsexperten aus unserem GReAT-Team und führenden Forschungs- und Entwicklungsteams**, tragen gemeinsam zur Bereitstellung dieser Feeds bei. Sicherheitsbeauftragte erhalten kritische, aus zuverlässigen Daten generierte Informationen und Benachrichtigungen, ohne Gefahr zu laufen, von unnötigen Anzeigen und Warnungen überflutet zu werden.
- **Einfache Implementierung**. Dank ergänzender Dokumentation, Beispielen, einem persönlichen technischen Account Manager sowie dem technischen Support von Kaspersky Lab geht die Integration schnell und einfach vonstatten.

Vorteile

- **Verstärken Sie Ihre Lösungen zur Netzwerkverteidigung**, einschließlich SIEMs, Firewalls, IPS/IDS, Sicherheits-Proxys, DNS-Lösungen und APT-Abwehr, mit regelmäßig aktualisierten Gefährdungsindikatoren (Indicators of Compromise, IOCs) und praktisch umsetzbarem Kontext. So erhalten Sie Einblicke in Cyberangriffe und können den Zweck, die Funktionen und die Ziele der Angreifer ermitteln. Führende SIEM-Systeme (einschließlich HP ArcSight, IBM QRadar, Splunk usw.) werden vollständig unterstützt.
- Entwickeln oder verbessern Sie den **Malware-Schutz für Geräte am Netzwerkrand** (wie z. B. Router, Gateways und UTM-Appliances).
- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Fähigkeiten**, indem Sie Ihren Sicherheits- bzw. SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe gezielter Angriffe bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill-Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Stellen Sie Unternehmensnutzern Bedrohungsinformationen bereit**. Nutzen Sie Informationen aus erster Hand zu aufkommender Malware und anderen Bedrohungen, um **Ihre Verteidigung präventiv zu stärken und Vorfälle zu vermeiden**.
- **Helfen Sie bei der Abwehr gezielter Angriffe**. Verstärken Sie Ihre Sicherheitsstellung durch taktische und strategische Bedrohungsinformationen, indem Sie Verteidigungsstrategien an die spezifischen Bedrohungen anpassen, mit denen Ihr Unternehmen konfrontiert ist.
- Nutzen Sie Bedrohungsinformationen, um **schädliche Inhalte zu erkennen, die in Ihren Netzwerken und Rechenzentren gehostet werden**.
- **Verhindern Sie die Extraktion vertraulicher Assets und geistigen Eigentums** über infizierte Geräte an Personen außerhalb des Unternehmens. Dank der schnellen Erkennung infizierter Assets vermeiden Sie den Verlust von Wettbewerbsvorteilen und Geschäftschancen und schützen den Ruf Ihrer Marke.
- Durchsuchen Sie Gefährdungsindikatoren, wie z. B. C&C-Protokolle, IP-Adressen, schädliche URLs oder Datei-Hashes mit von Experten validiertem Bedrohungskontext. Dieser ermöglicht es Ihnen, Angriffe zu priorisieren, vereinfacht Entscheidungen zu IT-Ausgaben und -Ressourcenverteilung und **unterstützt Sie dabei, sich auf die Abwehr der Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen**.
- Nutzen Sie unsere Expertise und praktisch umsetzbaren Kontextinformationen, um **den Schutz Ihrer Produkte und Services zu verbessern**, wie z. B. Inhaltsfilterung, Blockierung von Spam/Phishing usw.
- **Erweitern Sie als MSSP Ihr Geschäft**, indem Sie Ihren Kunden branchenführende Bedrohungsinformationen als Premiumservice bieten. **Als CERT** können Sie Ihre Fähigkeiten rund um die Erkennung und Identifizierung von Bedrohungen verbessern und erweitern.

Kaspersky APT Intelligence Reporting bietet Ihnen Folgendes:

- **Exklusiver Zugriff** auf die technischen Details hochmoderner Bedrohungen noch während der Untersuchung und vor der Veröffentlichung.
- **Einblicke in nicht öffentliche APTs**. Nicht alle hochkarätigen Bedrohungen werden öffentlich bekannt gemacht. Einige von ihnen werden aufgrund der Angriffsziele, der Vertraulichkeit der Daten, der Art und Weise, auf die die Schwachstellen geschlossen werden, oder der zugehörigen Strafverfolgungsmaßnahmen nie veröffentlicht. Aber die Details werden unseren Kunden mitgeteilt.
- **Detaillierte** technische Daten, darunter eine umfangreiche Liste von Gefährdungsindikatoren (Indicators of Compromise, IOCs), die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere Yara-Regeln.
- **Kontinuierliche Überwachung von APT-Kampagnen.** Zugriff auf praktisch nutzbare Informationen noch während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur).
- **Inhalte für unterschiedliche Zielgruppen.** Jeder der Berichte enthält Zusammenfassungen, die sich an C-Level-Mitarbeiter richten und einfach verständliche Informationen zum entsprechenden APT enthalten. Der Zusammenfassung folgt eine ausführliche technische Beschreibung des APT mit zugehörigen IOCs und Yara-Regeln. So erhalten Sicherheitsforscher, Malware-Analysten, Sicherheitstechniker, Netzwerkanalysten und APT-Experten praktisch umsetzbare Informationen für überragenden Schutz vor entsprechenden Bedrohungen.
- **Nachträgliche Analyse.** Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit.
- **APT Intelligence Portal.** Alle Berichte, einschließlich der aktuellen IOCs, können über das APT Intelligence Portal heruntergeladen werden, um unseren Kunden eine nahtlose Benutzererfahrung zu bieten. Auch eine API ist verfügbar.

Hinweis – Einschränkung von Abonnenten

Aufgrund der Tatsache, dass einige der in den Berichten enthaltenen Informationen äußerst vertraulich und spezifisch sind, können wir diese Services nur vertrauenswürdigen staatlichen sowie börsennotierten bzw. privat geführten Unternehmen zur Verfügung stellen.

APT Intelligence Reporting

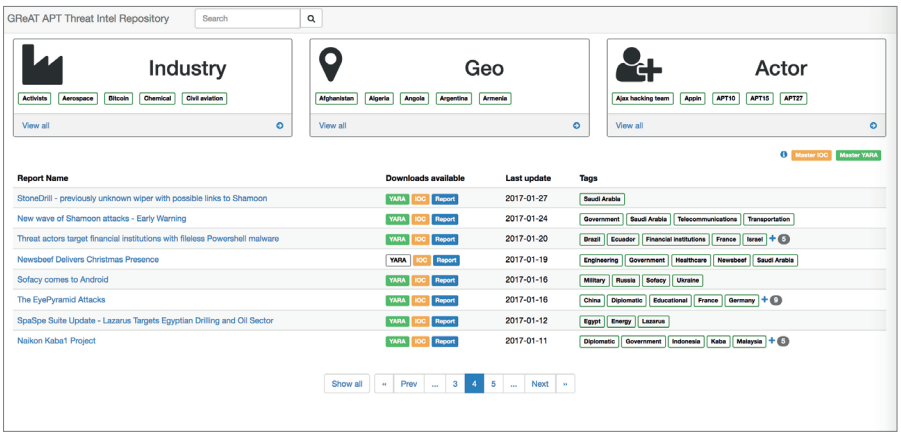
Verbessern Sie Wahrnehmung und Wissen über hochkarätige Cyberspionagekampagnen durch umfassende, praxisorientierte Berichte von Kaspersky Lab.

Mit den Informationen in diesen Berichten können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, indem Sie Angriffe über bekannte Vektoren abblocken, den durch hoch entwickelte Angriffe angerichteten Schaden reduzieren und Ihre Sicherheitsstrategie oder die Ihrer Kunden erweitern.

Kaspersky Lab hat einige der bedeutendsten APT-Angriffe aller Zeiten entdeckt. Nicht alle neu entdeckten APTs werden jedoch umgehend gemeldet – viele von ihnen werden sogar nie veröffentlicht.

Als Abonnent von Kaspersky APT Intelligence Reporting erhalten Sie exklusiven Zugang zu unseren Forschungsergebnissen und Entdeckungen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser aufgedeckt wird – inklusive aller Bedrohungen, die nie veröffentlicht werden. 2016 haben wir mehr als 100 Berichte erstellt.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie zudem über Änderungen in der Taktik von Cyberkriminellen auf dem Laufenden. Außerdem erhalten Sie Zugriff auf unsere vollständige Datenbank mit APT-Berichten – eine weitere effektive Recherche- und Analysequelle, die Sie zur Verteidigung Ihres Unternehmens nutzen können.



Tailored Threat Reporting

Kundenspezifisches Threat Reporting

Was wäre die beste Methode, einen Angriff gegen Ihr Unternehmen vorzutragen? Welche Routen und welche Informationen kann ein Angreifer nutzen, der es speziell auf Sie abgesehen hat? Hat es bereits einen Angriff gegeben, oder sind Sie derzeit einer Bedrohung ausgesetzt?

Unsere kundenspezifischen Berichte zu Bedrohungen beantworten diese und weitere Fragen. Unsere Experten erstellen dazu ein umfassendes Bild Ihrer aktuellen Gefährdungslage, zeigen Schwachstellen auf, die mit großer Wahrscheinlichkeit genutzt werden, und weisen ggf. bereits stattgefundene bzw. geplante Angriffe nach.

Dank dieser einzigartigen Einblicke können Sie Ihre Verteidigungsstrategie auf die Bereiche konzentrieren, die als Hauptziele der Cyberkriminellen erkannt wurden. Auf diese Weise handeln Sie schnell und präzise und minimieren das Risiko eines erfolgreichen Angriffs.

Unsere Berichte, die mithilfe von frei zugänglichen Informationsquellen (OSINT), einer tiefgreifenden Analyse mithilfe von Expertensystemen und Datenbanken von Kaspersky Lab sowie unserer Erkenntnisse über kriminelle Untergrundnetzwerke zusammengestellt werden, decken die folgenden Bereiche ab:

- **Identifizierung von Angriffsvektoren:** Identifizierung und Statusanalyse von extern verfügbaren, wichtigen Komponenten Ihres Netzwerks, z. B. Bankautomaten,

Videoüberwachung und andere Systeme, die Mobiltechnologien nutzen, Mitarbeiterprofile in Sozialen Netzwerken und E-Mail-Konten von Mitarbeitern, die potentielle Angriffsziele darstellen.

- **Tracking-Analyse von Malware und Cyberattacken**: Identifizierung, Überwachung und Analyse von aktiven oder inaktiven, gegen Ihr Unternehmen gerichteten Malware-Proben, aller früheren oder aktuellen Botnet-Aktivitäten und aller verdächtigen netzwerkbasierten Aktivitäten.
- **Angriffe auf Dritte**: Beweise für Bedrohungen und Botnet-Aktivitäten, die sich speziell gegen Ihre Kunden, Partner und Abonnenten richten, deren infizierte Systeme dann für Angriffe auf Ihr Unternehmen genutzt werden könnten.
- **Informationslecks:** Durch diskrete Überwachung von Online-Foren und Communitys können wir herausfinden, ob es Angriffspläne gegen Ihr Unternehmen gibt, z. B. ob ein illoyaler Mitarbeiter mit Informationen handelt.
- **Aktueller Angriffsstatus**: APT-Attacken können jahrelang unentdeckt bleiben. Wenn wir einen aktuellen Angriff auf Ihre Infrastruktur entdecken, beraten wir Sie hinsichtlich einer effektiven Beseitigung.

Schneller Einstieg – Einfache Anwendung – Keine Ressourcen erforderlich

Nachdem Sie die Parameter und Ihre bevorzugten Datenformate festgelegt haben, ist keine zusätzliche Infrastruktur erforderlich, um mit der Nutzung dieses Services von Kaspersky Lab zu beginnen.

Kaspersky Tailored Threat Reporting hat keine Auswirkungen auf die Integrität und Verfügbarkeit von Ressourcen, einschließlich Netzwerkressourcen.

Der Service kann als einmaliges Projekt oder regelmäßig in Form eines Abonnements (z. B. vierteljährlich) in Anspruch genommen werden.

Länderspezifisches Threat Reporting

Die Cybersicherheit eines Landes umfasst den Schutz aller wichtigen Institutionen und Unternehmen. Hochentwickelte, anhaltende Bedrohungen (Advanced Persistent Threats, APT), die auf staatliche Behörden abzielen, können die nationale Sicherheit bedrohen. Mögliche Cyberattacken gegen Unternehmen in den Bereichen Produktion, Transport und Telekommunikation sowie im Bankensektor und anderen wichtigen Branchen können den Staat empfindlich treffen, beispielsweise in Form von finanziellen Verlusten, Produktionsunfällen, Störungen in der Netzwerkkommunikation und Unzufriedenheit in der Bevölkerung.

Mit einem Überblick über die aktuelle Gefährdungslage und aktuelle Trends in Bezug auf Malware und Hackerangriffe, die gegen Ihr Land gerichtet sind, können Sie Ihre Verteidigungsstrategie auf Bereiche konzentrieren, die als Hauptziele für Cyberkriminelle dienen. So können Sie Eindringlinge schnell und präzise bekämpfen und das Risiko erfolgreicher Angriffe verringern.

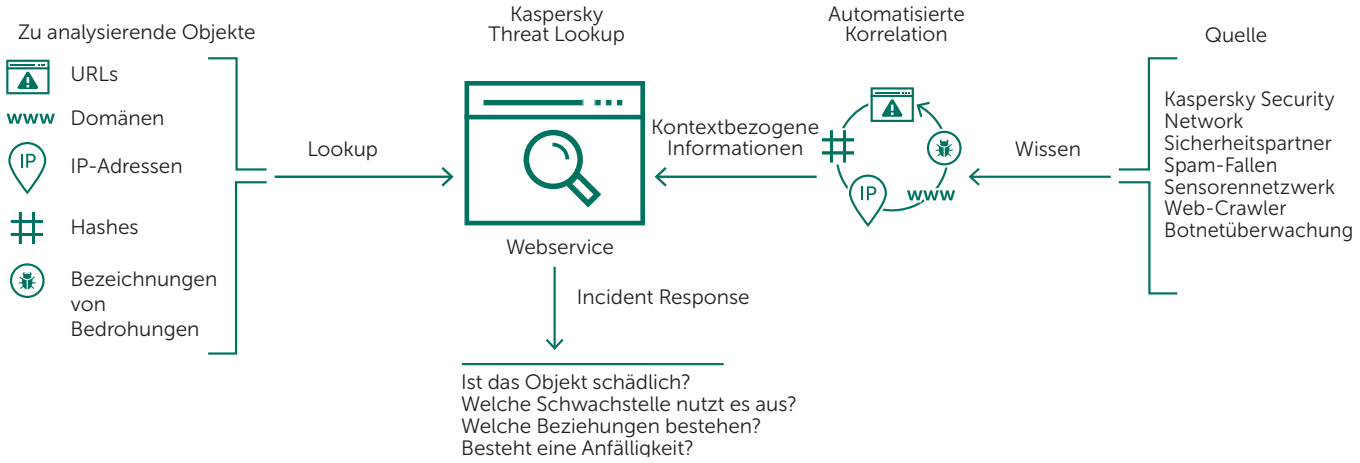
Unsere länderspezifischen Berichte, die mithilfe von frei zugänglichen Informationsquellen (OSINT), einer gründlichen Analyse mithilfe von Expertensystemen und Datenbanken von Kaspersky Lab sowie unseren Erkenntnissen über kriminelle Untergrundnetzwerke zusammengestellt werden, decken die folgenden Bereiche ab:

- **Identifizierung von Bedrohungsvektoren**: Identifizierung und Statusanalyse extern verfügbarer, wichtiger nationaler IT-Ressourcen, einschließlich anfälliger staatlicher Programme, Telekommunikationsanlagen, Komponenten von Industriesteuerungen (wie SCADA, PLCs usw.), Geldautomaten usw.
- **Tracking-Analyse von Malware und Cyberattacken**: Identifizierung und Analyse von APT-Kampagnen, aktiven oder inaktiven Malware-Proben, früheren oder aktuellen Botnet-Aktivitäten und anderen nennenswerten Bedrohungen, die auf Ihr Land abzielen, basierend auf den Daten aus unseren einzigartigen internen Überwachungsressourcen.
- **Informationslecks**: Durch diskrete Überwachung von Untergrundnetzen und Online-Communitys können wir ermitteln, ob Hacker Angriffspläne gegen bestimmte Unternehmen erörtern. Außerdem decken wir stark gefährdete Konten auf, die ein Risiko für geschädigte Unternehmen und Institutionen darstellen können (z. B. Konten von Mitarbeitern von Regierungsbehörden, die beim Ashley Madison-Angriff auftauchten und für Erpressungen genutzt werden könnten).

Kaspersky Threat Intelligence Reporting hat keine Auswirkungen auf die Integrität und Verfügbarkeit der untersuchten Netzwerkressourcen. Der Service basiert auf nicht invasiven Netzwerkanalysemethoden sowie auf der Analyse von Informationen aus frei zugänglichen Quellen und aus Ressourcen mit beschränktem Zugriff.

Zum Schluss erhalten Sie einen Bericht mit einer Beschreibung nennenswerter Bedrohungen für Branchen und Institutionen des Landes sowie zusätzliche Informationen zu detaillierten technischen Analyseergebnissen. Die Berichte werden in verschlüsselten E-Mails versendet.

Threat Lookup



Service-Highlights

- **Zuverlässige Sicherheitsinformationen**: Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Produkte von Kaspersky Lab zählen zu den führenden bei Anti-Malware-Tests[1]. Die hohen Erkennungsraten mit Fehlalarmquoten, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.
- **Aufspüren von Bedrohungen**: Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Erkennen und beenden Sie Angriffe so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.
- **Sandbox-Analyse**[2] Dabei werden unbekannte Bedrohungen durch die Ausführung von verdächtigen Objekten in einer abgesicherten Umgebung erkannt sowie das gesamte Bedrohungsverhalten mitsamt der Artefakte in leicht verständlichen Berichten überprüft.
- **Breites Spektrum an Exportformaten**: Exportieren Sie die IOCs oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV, um alle Vorteile der Bedrohungsinformationen zu nutzen, betriebliche Workflows zu automatisieren oder die Integration in bestehende Sicherheitskontrollen, wie z. B. SIEMs, zu ermöglichen.
- **Benutzerfreundliche Web-Oberfläche oder RESTful-API**: Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über ein einfaches RESTful-API zugreifen.

1 http://www.kaspersky.de/top3

2 Die Funktion soll in der ersten Jahreshälfte 2017 eingeführt werden.

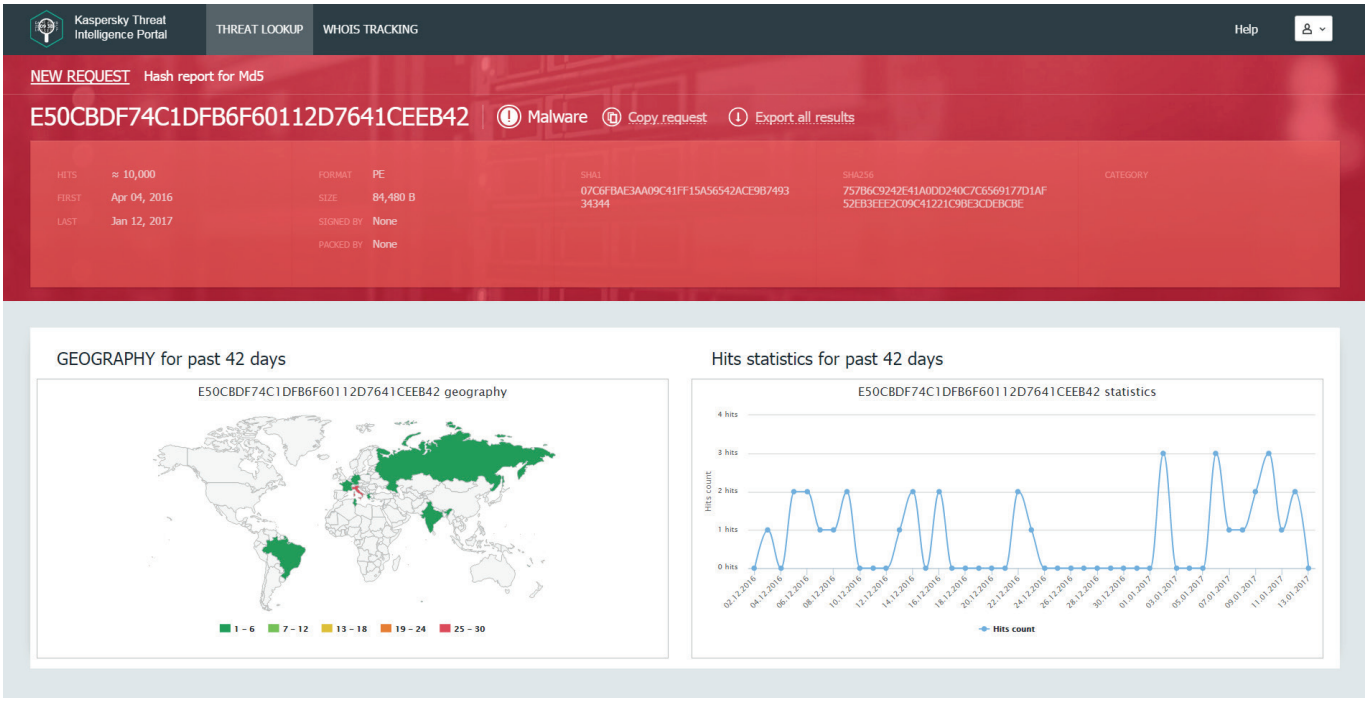
Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt heute kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die für ihre Angriffe zunehmend Ressourcen aus dem Dark Web einsetzen. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains" und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihre Kunden zu schädigen.

Kaspersky Threat Lookup bietet unser gesamtes Wissen über Cyberbedrohungen und ihre Interdependenzen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die aktuellen Bedrohungsinformationen zu URLs, Domänen, IP-Adressen, Datei-Hashes, Bedrohungsbezeichnungen, Statistik- und Verhaltensdaten, WHOIS-/DNS-Daten, Dateiattribute, Geolokalisierungsdaten, Download-Ketten, Zeitstempel usw. ab. Hieraus ergibt sich ein umfassender Überblick über neue und aufkommende Bedrohungen, der Ihnen hilft, die Verteidigung und Vorfallsreaktion Ihres Unternehmens zu verbessern.

Die von Kaspersky Threat Lookup bereitgestellten Bedrohungsinformationen werden in Echtzeit über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die kontinuierliche Verfügbarkeit und ein gleichbleibendes Leistungsniveau gewährleistet. Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT-Team und führenden Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung wertvoller, realer Bedrohungsdaten bei.

Hauptvorteile

- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen**, indem Sie Ihren Sicherheits-/SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe von gezielten Angriffen bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill-Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Führen Sie anhand hochzuverlässiger Bedrohungskontexte detaillierte Suchen innerhalb der Bedrohungsindikatoren aus**, z. B. in IP-Adressen, URLs, Domänen oder Datei-Hashes, um Angriffe zu priorisieren, Entscheidungen über Personal- und Ressourcenzuteilungen zu verbessern und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.
- **Wehren Sie gezielte Angriffe ab**. Verbessern Sie mithilfe taktischer und strategischer Bedrohungsinformationen Ihre Sicherheitsinfrastruktur, indem Sie die richtigen Verteidigungsstrategien einsetzen.



Jetzt können Sie ...

- über eine webbasierte Benutzeroberfläche oder das RESTful-API nach Bedrohungsindikatoren suchen.
- nachvollziehen, warum ein Objekt als schädlich eingestuft wird.
- überprüfen, ob ein entdecktes Objekt weit verbreitet ist oder isoliert vorkommt.
- zusätzliche Details überprüfen, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu entdecken.

Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl von Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.

Kenne deine Feinde und deine Freunde. Erkennen Sie nachgewiesen unschädliche Dateien, URLs und IP-Adressen, und beschleunigen Sie den Untersuchungsvorgang. Wenn jede Sekunde zählt, sollten Sie keine Zeit mit der Analyse von vertrauenswürdigen Objekten verlieren.

Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um dies zu erreichen und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben und verwendet werden können. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz Ihrer Daten und Netzwerke unerlässlich. Jetzt können Sie mit Kaspersky Threat Lookup effizienter und einfacher denn je auf diese Daten zugreifen.

Jede Benachrichtigung von Kaspersky Phishing Tracking wird per HTTPS bereitgestellt und beinhaltet Folgendes:

- Screenshot der Phishing-URL
- HTML-Code der Phishing-URL
- JSON-Datei, die folgende Felder
- enthält:
  - Phishing-URL
  - Name der Marke, auf die die Phishing-URL abzielt
  - Zeitstempel der ersten Entdeckung
  - Zeitstempel der letzten Entdeckung
  - Beliebtheit der Phishing-URL
  - Geostandort der Benutzer, die von der Phishing-URL betroffen sind
  - Art der gestohlenen Daten (Kreditkartendaten, Anmeldedaten für Banking, E-Mail oder soziale Netzwerke, persönliche Informationen usw.)
  - Angriffstyp (angedrohte Kontosperrung, Datei-Download, Aufforderung, persönliche Daten zu aktualisieren, usw.)
  - Aufgelöste IP-Adresse der Phishing-URL
  - WHOIS-Daten
  - und vieles mehr.

Phishing Tracking

Phishing – insbesondere gezieltes Spear-Phishing – stellt aktuell eine der gefährlichsten und effektivsten Methoden für Onlinebetrug dar. Gefälschte Webseiten erfassen Anmeldedaten und Passwörter, um die Online-Identitäten der Opfer zu übernehmen, um ihnen so Geld zu stehlen oder über ihre E-Mail- oder Social-Media-Konten Spam und Malware zu verbreiten. Diese Methode ist eine leistungsstarke Waffe im Arsenal von Cyberkriminellen, und die Häufigkeit und Vielfalt der Angriffe nimmt immer weiter zu.

Und es trifft nicht nur Finanzinstitute. Jeder – vom Onlinehändler über den Internetanbieter bis hin zur Regierungsbehörde – läuft Gefahr, Opfer von Spear-Phishing zu werden. Durch perfekt kopierte Fälschungen Ihrer Webseite samt vollständiger Corporate Identity oder durch Nachrichten, die direkt von eigenen Führungskräften zu stammen scheinen, werden Nutzer leicht in die Irre geführt und davon überzeugt, vertrauliche Daten preiszugeben – und so sich und dem gesamten Unternehmen großen Schaden zuzufügen.

Ein einziger erfolgreicher Phishing-Angriff kann verheerende Auswirkungen auf das angegriffene Unternehmen haben. Neben direkten Verlusten entstehen auch indirekte Kosten, wie z. B. die Bereinigung kompromittierter Webseiten und Konten. Und zu guter Letzt schädigen erfolgreiche Angriffe den Ruf den des Unternehmens. Ein solcher Verlust des Kundenvertrauens in Ihre Onlineservices kann zum jahrelangen Verlust von Kunden und Glaubwürdigkeit führen. Cyberkriminalität kennt heutzutage keine Grenzen mehr, und die technischen Möglichkeiten entwickeln sich rapide weiter: Wir erleben immer komplexere Angriffe, bei denen Cyberkriminelle Dark-Web-Ressourcen nutzen, um ihre Opfer anzugreifen. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains“ und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihre Kunden zu schädigen.

Unsere Lösung – Kaspersky Phishing Tracking Service

Dieser Service verfolgt aktiv das Auftreten von Phishing-Websites, benachrichtigt Sie in Echtzeit und stellt präzise und ausführliche laufende Daten zu Phishing- oder betrügerischen Aktivitäten bereit, die für Ihr Unternehmen relevant sind. Diese Daten umfassen die injizierte Malware und die Phishing-URLs, die Anmeldedaten, vertrauliche Informationen, Finanzdaten und persönliche Informationen von Ihren Benutzern stehlen. Der Service überwacht darüber hinaus die spezifischen Top-Level-Domänen (TLD) oder sogar ganze Regionen hinsichtlich des Auftretens von Phishing-Sites.

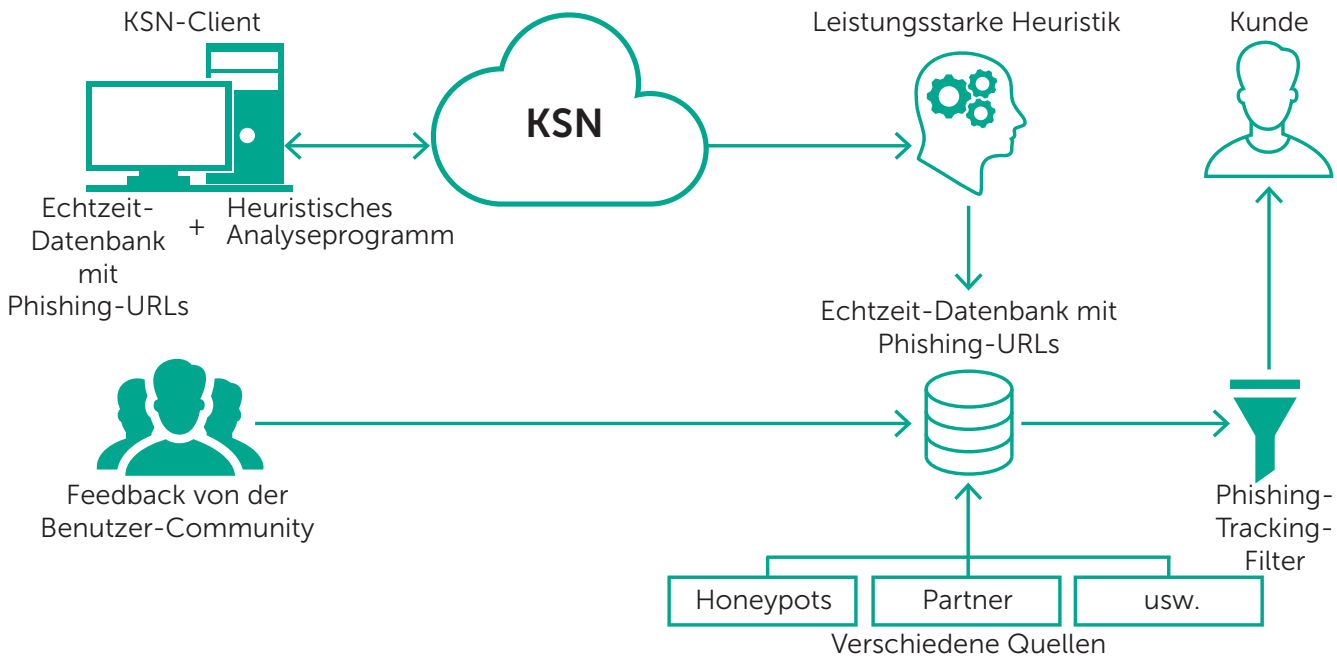
Im Rahmen des Service erhalten Sie E-Mail-Benachrichtigungen zu bestätigten Phishing-Bedrohungen gegen Ihre Marke, Ihren Unternehmensnamen oder Ihre Handelsmarken. Jede Benachrichtigung bietet tief gehende Informationen, hohe Präzision und zuverlässige Informationen zu den immer komplexeren Phishing-Angriffen. So können Sie schnell auf Phishing-Angriffe sowie dynamisch generierte Phishing-Domänen und -URLs reagieren. Neben einer Liste mit Phishing-Sites erhalten Sie zusätzliche Informationen, damit Sie umgehend spezifische Maßnahmen gegen jede beliebige Phishing-Attacke ergreifen können.

Mithilfe dieser frühzeitig bereitgestellten, professionell überprüften Informationen können Sie schnell und präzise reagieren, um die Auswirkungen von Phishing-Aktivitäten in Ihrem Unternehmen und unter Ihren Benutzern einzudämmen und sich optimal so vor Betrug zu schützen.

Quellen der Bedrohungsinformationen

Kaspersky Phishing Tracking nutzt Daten aus heterogenen und äußerst zuverlässigen Informationsquellen, einschließlich Kaspersky Security Network (KSN), leistungsstarker heuristischer Engines, E-Mail-Honeypots, Webcrawler, Spam-Fallen, Forschungsteams, Partner und Verlaufsdaten zu schädlichen Objekten, die wir in den letzten 20 Jahren erfasst haben. Die aggregierten Daten werden dann in Echtzeit überprüft und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Kaspersky-Expertensysteme (Sandboxes, heuristische Engines, Multi-Scanner, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Inhaltsanalysten und Verifizierungstools anhand von Whitelists.

Die Kombination der weltweiten Abdeckung des Kaspersky Security Networks, der Erkennungstechnologien von Kaspersky Lab sowie einer Vielzahl von Tests und Filtern gewährleistet maximale Erkennungsraten für jeden Phishing-Angriff und jede Bedrohung – und das ohne Fehlalarme, wie unabhängige Tests zeigen*.



Frühzeitige Warnung vor Phishing-Angriffen

Nutzen Sie den Kaspersky Phishing Tracking Service, und Sie erhalten den entscheidenden Vorteil gegenüber Angreifern. Durch die frühzeitige Warnung zu Phishing-Attacken – ob geplant oder im Gange –, die es auf Ihre Marken, Onlineservices und Kunden abgesehen haben, können Sie Ihre Ressourcen schützen und die Risiken pragmatischer, präziser und kosteneffizienter abwehren.

Einen Schritt voraus

Kritische Informationen werden in Echtzeit sowie über regelmäßige Berichte zu schädlichen Aktivitäten bereitgestellt, die Informationen zu geplanten und aktuell laufenden Angriffen enthalten. So sind Sie den Cyberkriminellen endlich einen Schritt voraus.

Verbesserung des Benutzererlebnisses

Sobald Sie die Phishing-Angreifer kennen und verstehen, können Sie den Schutz entsprechend planen: von der Blockierung veralteter Software bis hin zur Einführung SMS-basierter Autorisierung – damit sich Ihre Onlinekunden geschützt und sicher fühlen.

Minimierung der Auswirkungen

Wenn die URLs von Phishing-Webseiten bekannt sind, können die Internetanbieter benachrichtigt werden, die entsprechende Sites hosten. So wird ein weiterer Diebstahl persönlicher Daten durch die Site verhindert, und der Angriff wird im Keim erstickt.

Immer bestens informiert

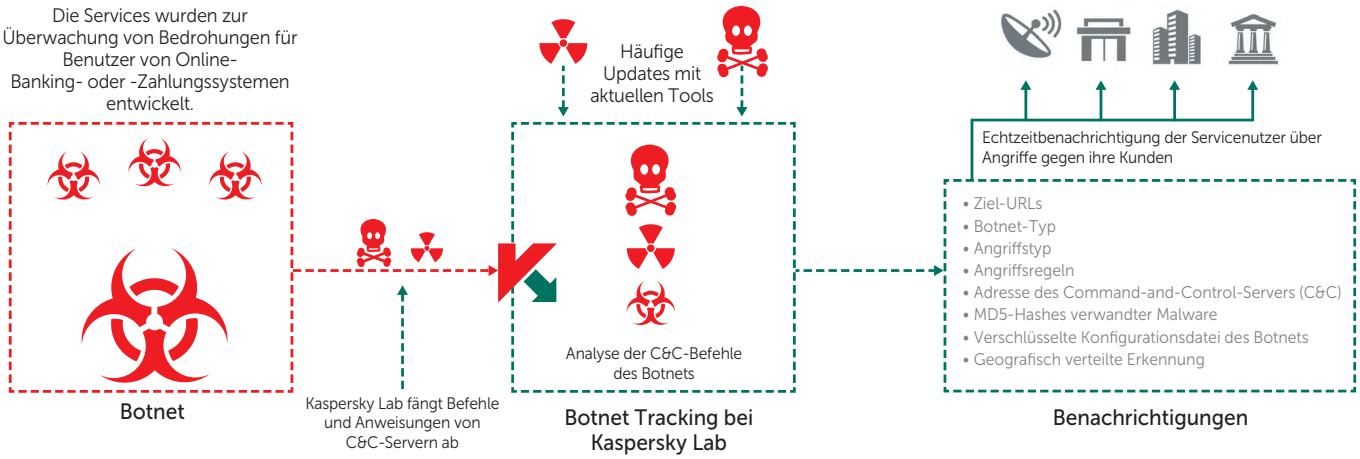
Dieser Fluss relevanter, präziser und ausführlicher Informationen ohne False Positives oder sonstigen unnötigen Aufwand bietet neue Einblicke, mit deren Hilfe Sie heute und in Zukunft die perfekte Sicherheitsstrategie finden. So schützen Sie sich und Ihr Unternehmen vor Onlinebetrug.

AV comparatives Approved 2016 Anti-Phishing

* Testberichte von AV-Comparatives sind auf Anfrage verfügbar.

Botnet Tracking

Zuverlässige Überwachungs- und Benachrichtigungsservices zur Identifizierung von Botnets, die Ihren Ruf und Ihre Kunden schädigen könnten.



Nutzungsszenarien/Servicevorteile

- Mit proaktiven Benachrichtigungen zu Bedrohungen durch Botnets, die es auf Ihre Online-Benutzer abgesehen haben, sind Sie dem Angriff immer einen Schritt voraus.
- Durch die Identifizierung einer Liste von Botnet-Command & Control-Server-URLs, die auf Ihre Online-Benutzer ausgerichtet sind, können Sie diese über Anforderungen an CERTs oder Strafverfolgungsbehörden blockieren.
- Verbessern Sie Ihr Online-Banking/Ihre Zahlungssysteme, indem Sie die Art des Angriffs verstehen.
- Schulen Sie Ihre Online-Benutzer, damit sie die bei Angriffen verwendeten Social-Engineering-Techniken erkennen und nicht darauf hereinfallen.

Bleiben sie dank Echtzeitinformationen handlungsfähig:

Zum Umfang dieses Service gehören personalisierte Benachrichtigungen mit Informationen zu übereinstimmenden Markennamen, die durch die Analyse von Schlüsselwörtern in den von Kaspersky Lab überwachten Botnets ermittelt wurden. Die Benachrichtigungen können Ihnen per E-Mail oder RSS im HTML- oder JSON-Format bereitgestellt werden. Sie erhalten u. a. folgende Informationen:

- **Ziel-URL(s)** – Bot-Malware wartet so lange ab, bis ein Benutzer auf die URLs des zu attackierenden Unternehmens zugreift, und startet dann den Angriff.
- **Botnet-Typ** – Bestimmen Sie präzise den Malware-Typ, der eingesetzt wird, um die Transaktionen Ihrer Kunden zu gefährden. Beispiele: Zeus, SpyEye oder Citadel usw.
- **Angriffstyp** – Verrät Ihnen, zu welchem Zweck die Malware eingesetzt wird, z. B. Injektion von Webdaten, Bildschirmlöschung, Videoaufzeichnung oder Weiterleitung an Phishing-URLs.
- **Angriffsregeln** – Verrät Ihnen, welche unterschiedlichen Regeln für die Injektion von Webcodes verwendet werden, z. B. HTML-Anfragen (GET/POST), Webseitendaten vor und nach der Injektion.
- **Command-and-Control-Serveradressen (C&C)** – Gibt Ihnen die Möglichkeit, dem Internetdienstanbieter den betreffenden Server zu melden, damit die Bedrohung rascher entschärft werden kann.
- **MD5-Hashwerte der Malware** – Kaspersky Lab stellt Ihnen den zur Malware-Verifizierung verwendeten Hashwert zur Verfügung.
- **Verschlüsselte Konfigurationsdatei des Botnets** – Vollständige Liste der betroffenen URLs.
- **Geografisches Verteilungsmuster (10 Hauptländer)** – Statistische Daten zur weltweiten Verteilung der Malware-Proben.

Kaspersky Threat Threat Hunting Services

Sicherheitsteams in allen Branchen arbeiten hart daran, Systeme aufzubauen, die umfassenden Schutz vor sich immer schneller entwickelnden Cyberbedrohungen bieten. Die meisten dieser Systeme nutzen jedoch einen reaktiven Benachrichtigungsansatz bei Vorfällen der Cybersicherheit: Sie warnen erst, nachdem ein Vorfall bereits eingetreten ist. Neueste Forschungen zeigen jedoch, dass ein Großteil der Sicherheitsvorfälle unerkannt bleibt. Diese Bedrohungen bleiben unter dem Radar und sorgen so dafür, dass Unternehmen sich zu Unrecht sicher fühlen. Unternehmen sind sich jedoch zunehmend bewusst, dass Bedrohungen, die zwar unerkannt, aber aktiv in ihren eigenen Infrastrukturen lauern, aktiv gejagt werden müssen. Kaspersky Threat Hunting Services unterstützen Sie bei der Entdeckung hoch entwickelter Bedrohungen in Ihrem Unternehmen. Hierfür setzen hoch qualifizierte und erfahrene Sicherheitsexperten präventive Techniken zur Bedrohungserkennung ein.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
  - Kaspersky Managed Protection
  - Targeted Attack Discovery
- **Kaspersky Security Trainings**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Servicevorteile

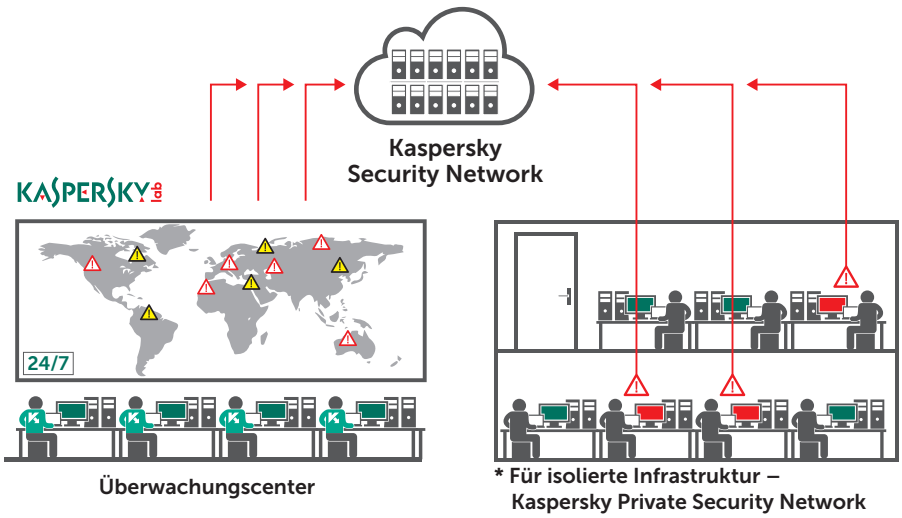
- Schnellere und effektivere Abwehr dank schneller und effizienter Erkennung
- Keine Zeitverschwendung durch Fehlalarme dank der klaren und umgehenden Identifizierung und Klassifizierung sämtlicher verdächtiger Aktivitäten
- Geringere Gesamtkosten für die Sicherheit Keine Einstellung und Schulung verschiedener interner Experten
- Die Gewissheit, dass Sie bestens vor den komplexesten und innovativsten Bedrohungen abseits von Malware geschützt sind
- Erkenntnisse zu Angreifern, ihrer Motivation, ihren Methoden und Tools und dem potenziellen Schaden, den sie anrichten können – zur Entwicklung einer fundierten und effektiven Verteidigungsstrategie

Kaspersky Managed Protection

Kaspersky Managed Protection bietet Benutzern von Kaspersky Endpoint Security und Kaspersky Anti Targeted Attack Platform einen vollständig verwalteten Service, der eine einzigartige Kombination aus Technologien zur Erkennung und Vermeidung gezielter Angriffe bietet. Der Service umfasst die Überwachung durch Kaspersky-Experten rund um die Uhr und die kontinuierliche Analyse von Bedrohungsinformationen, um die Echtzeiterkennung bekannter und neuer Kampagnen für Cyberspionage und Cyberkriminalität zu erkennen, die auf wichtige Informationssysteme abzielen.

Service-Highlights

- Dauerhaft hohes Maß an Schutz vor gezielten Angriffen und Malware inklusive Rund-um-die-Uhr-Überwachung und -Support von Ihrem persönlichen Kaspersky-Expertenteam sowie stets aktuelle Bedrohungsinformationen.
- Rechtzeitige und präzise Erkennung von Nicht-Malware-Angriffen, Angriffen mit bisher unbekannten Hilfsmitteln und Angriffen, die Zero-Day-Schwachstellen ausnutzen
- Umgehender Schutz vor sämtlichen unbekannten Bedrohungen durch automatische Updates der Virendatenbank
- Rückwirkende Analyse von Vorfällen und Bedrohungsermittlung, einschließlich der von den Angreifern gegen Ihr Unternehmen eingesetzten Methoden und Technologien
- Integrierter Ansatz – das Kaspersky-Portfolio beinhaltet sämtliche Technologien und Services, die Sie für die Implementierung eines vollständigen Zyklus für den Schutz vor gezielten Angriffen benötigen: Vorbereitung, Erkennung/Untersuchung, Datenanalyse, automatisierter Schutz



Der Service im Detail

Die Erkennung gezielter Angriffe von Kaspersky Lab umfasst die folgenden Aktivitäten:

Sammlung und Analyse von Bedrohungsinformationen. Ziel ist es, eine Momentaufnahme Ihrer Angriffsfläche zu erstellen. Dabei werden die Bedrohungen durch Cyberkriminalität und Cyberspionage sowie Angriffe ermittelt, die Ihre Ressourcen aktiv oder potenziell schädigen. Zu diesem Zweck tauchen wir in interne und externe Informationsquellen ein, darunter Untergrund-Communities von Betrügern, und überwachen Ihre Umgebung mithilfe von internen Überwachungssystemen von Kaspersky Lab. Die Analyse der erfassten Daten ermöglicht uns das Aufspüren von Schwachstellen in Ihrer Infrastruktur, die Cyberkriminelle ausnutzen könnten, sowie von gefährdeten Konten.

Datenerfassung am Standort und frühe Vorfallsreaktion. Neben den Aktivitäten zur Informationsbeschaffung in unseren eigenen Laboren kommen Experten von Kaspersky Lab vor Ort, um Netzwerk- und Systemartefakte sowie verfügbare SIEM-Informationen zu erfassen. Wir führen ggf. auch ein Vulnerability Assessment durch, um die kritischsten Sicherheitslücken zu erkennen, und sofort darauf zu reagieren. Hat ein Vorfall bereits stattgefunden, sammeln wir Beweise für weitere Untersuchungen. In diesem Stadium geben wir Ihnen vorläufige Empfehlungen für kurzfristige Abhilfemaßnahmen an die Hand.

Datenanalyse. Zurück im Labor werden die erfassten Netzwerk- und Systemartefakte mithilfe der Wissensdatenbank von Kaspersky Lab analysiert, die IOCs, C&C-Blacklists (Command-and-Control-Serveradressen), Sandboxing-Technologien usw. enthält, um genau zu verstehen, was in Ihrem System passiert. Wird in diesem Stadium zum Beispiel eine neue Malware gefunden, stehen wir Ihnen mit Rat und Tat sowie Tools (z. B. YARA-Tools) zur Seite, um sie sofort zu identifizieren. Wir halten Sie stets auf dem Laufenden und greifen bei Bedarf per Fernzugriff auf Ihre Systeme zu.

Berichterstellung. Abschließend erstellen wir unseren formellen Bericht, der die erkannten gezielten Angriffe sowie unsere Empfehlungen für weitere Abhilfemaßnahmen enthält.

Targeted Attack Discovery

Kaspersky-Experten bieten den Targeted Attack Discovery-Service an, um die Sicherheit Ihres Betriebsvermögens zu gewährleisten.

Mithilfe der Ergebnisse der Targeted Attack Discovery können Sie aktuelle Aktivitäten rund um Cyberkriminalität und -spionage identifizieren, die Gründe für den Angriff sowie die Quellen der Vorfälle verstehen und effektiv Gegenmaßnahmen planen, die Sie künftig vor ähnlichen Angriffen schützen. Wenn Sie befürchten, dass Angriffe auf Ihre Branche abzielen, und Ihnen verdächtiges Verhalten in Ihren eigenen Systemen auffällt, oder wenn Sie proaktiv vorbeugen wollen ist unser Service „Targeted Attack Discovery" genau das Richtige für Sie, denn sie klärt Sie über Folgendes auf:

- Ob, wie und von wem Sie derzeit angegriffen werden
- Wie sich dieser Angriff auf Ihre Systeme auswirkt, und wie Sie sich wehren können
- Wie Sie zukünftige Angriffe vermeiden

Beschreibung des Service

Unsere global anerkannten, unabhängigen Experten decken aktive Vorfälle, anhaltende Bedrohungen (Advanced Persistent Threats, APT), Aktivitäten der Cyberspionage und Cyberkriminalität in Ihrem Netzwerk auf und analysieren diese. Unsere Experten unterstützen Sie dabei, schädliche Aktivitäten aufzudecken, die möglichen Quellen zu erkennen und die effektivsten Beseitigungsmaßnahmen zu planen.

Dies erfolgt auf folgende Weise:

- Analysieren von Quellen für Bedrohungsinformationen zur Erfassung Ihrer speziellen Gefährdungslage
- Durchführen umfassender Scans Ihrer IT-Infrastruktur und Daten (z. B. Protokolldateien) zur Aufdeckung von Gefährdungsanzeichen
- Analyse aktueller Netzwerkverbindungen zur Erkennung verdächtiger Aktivitäten
- Aufdecken möglicher Angriffsquellen und anderer potenziell gefährdeter Systeme

Die Ergebnisse

Sie erhalten die Ergebnisse in Form eines detaillierten Berichts mit folgenden Angaben:

Unsere allgemeinen Feststellungen: Bestätigung der Existenz oder Abwesenheit von Gefährdungshinweisen in Ihrem Netzwerk

Tief greifende Analyse der erfassten Bedrohungsinformationen und der gefundenen Gefährdungsindikatoren

Genaue Beschreibung der ausgenutzten Schwachstellen, möglichen Angriffsziele und betroffenen Netzwerkkomponenten

Empfehlung von Abhilfemaßnahmen, einschließlich möglicher Schritte zur Verringerung der Folgen des Vorfalls und zum Schutz Ihrer Ressourcen vor ähnlichen Angriffen in der Zukunft

Zusätzliche Services

Unsere Experten unterstützen Sie auch dabei, die Symptome eines Vorfalls zu analysieren, tief greifende digitale Analysen für bestimmte Systemen durchzuführen, Malware-Binärdateien zu identifizieren (falls vorhanden) und Malware-Analysen durchzuführen. Die Ergebnisse dieses optionalen Service werden zusammen mit weiteren empfohlenen Abhilfemaßnahmen in einem separaten Bericht aufgeführt.

Auf Wunsch integrieren wir zudem die **Kaspersky Anti Targeted Attack (KATA) Platform** in Ihrem Netzwerk – dauerhaft oder als „Proof of Concept". Diese Plattform vereint die neuesten Technologien und globalen Analysen, die gezielte Angriffe in Ihrem System erkennen, sofort darauf reagieren und Angriffe auf allen Stufen des Lebenszyklus bekämpfen.

Kaspersky Security Trainings

Sicherheitsschulungen sind angesichts der zunehmenden Bedrohungslage für Unternehmen unerlässlich. Sicherheitsmitarbeiter müssen in den erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente des effektiven Bedrohungsmanagements und der Strategien zur Risikominimierung im Unternehmen bilden.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Trainings**
  - Digital Forensics
  - Malware-Analyse und Reverse-Engineering
  - Advanced Digital Forensics
  - Advanced Malware Analysis and Reverse Engineering
  - Incident Response
  - Yara
  - KATA Administration
  - KATA Security Analyst
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Diese Kurse umfassen eine breite Auswahl von Cybersicherheitsthemen und -techniken mit Assessments von der Einsteiger- bis zur Expertenebene. Alle Kurse werden am Kundenstandort oder ggf. in einer lokalen oder regionalen Niederlassung von Kaspersky Lab angeboten.

Die Kurse umfassen sowohl theoretische Lektionen als auch praktische Übungen. Nach Abschluss jedes Kurses können die Teilnehmer ihr Wissen in einem Test prüfen.

Servicevorteile

Digital Forensics und Advanced Digital Forensics

Vertieft das Fachwissen Ihres internen Teams für digitale Forensik und Vorfallsreaktion. Teilnehmer dieses Kurses können Erfahrungslücken schließen und ihre praktischen Fertigkeiten bei der Suche nach digitalen Spuren von Cyberkriminalität sowie bei der Analyse verschiedener Datentypen zur Ermittlung des zeitlichen Ablaufs und der Quellen des Angriffs entwickeln und verbessern. Nach Abschluss dieses Kurses können Teilnehmer Computervorfälle erfolgreich untersuchen und die Sicherheit des Unternehmens verbessern.

Malware-Analyse und Reverse Engineering und Erweiterte Malware-Analyse und Reverse Engineering

Die Reverse-Engineering-Schulung wurde entwickelt, um Teams für Vorfallsreaktionen (Incident Responses) bei der Untersuchung schädlicher Aktivitäten zu unterstützen. Dieser Kurs richtet sich an Mitarbeiter der IT-Abteilung und Systemadministratoren. Die Teilnehmer erfahren, wie sie Schadsoftware analysieren, IOCs erfassen, Signaturen zur Erkennung von Malware auf infizierten Geräten schreiben und infizierte/verschlüsselte Dateien und Dokumente wiederherstellen.

Incident Response

Der Kurs führt Ihr internes Team durch sämtliche Phasen der Vorfallsreaktion und stattet sie mit dem umfassenden Wissen aus, das für eine erfolgreiche Wiederherstellung nach Vorfällen erforderlich ist.

Yara

In diesem Kurs erfahren Sie, wie Sie effektive Yara-Regeln schreiben, testen und so verbessern können, dass sie Bedrohungen finden, die bisher unbekannt blieben.

KATA Administration

Die Schulung „KATA Administration“ umfasst sämtliches Know-how zur Planung, Installation und Konfiguration der Lösung, mit dem Sie die Bedrohungserkennung optimieren können.

KATA Security Analyst

Der Schulungskurs beinhaltet eine Reihe praktischer Übungen, die auf tatsächlichen Bedrohungsszenarien basieren, und vermittelt das Wissen, das Sie für die Überwachung, Interpretation und Reaktion auf KATA-Warnungen benötigen.

Praktische Erfahrung

Von einem der führenden Sicherheitsanbieter, gemeinsames Arbeiten und Lernen zusammen mit unseren globalen Experten, die die Teilnehmer durch ihre eigene Erfahrung im alltäglichen Kampf gegen die Cyberkriminalität inspirieren.

Programmbeschreibung

Themen	Dauer	Erlernte Fertigkeiten
Digital Forensics		
• Einführung in die digitale Forensik • Live-Reaktion und Erfassung von Beweisen • Details der Windows-Registrierung • Windows-Artefaktanalyse • Browser-Forensik • E-Mail-Analyse	5 Tage	• Aufbau eines digitalen Forensiklabors • Sammeln von digitalen Beweisen und entsprechende Nutzung • Rekonstruieren eines Vorfalls und Verwenden von Zeitstempeln • Analyse von Eindringspuren anhand von Windows-Artefakten • Finden und Analysieren von Browser- und E-Mail-Verlauf • Anwenden der Tools und Instrumente der digitalen Forensik
Malware-Analyse und Reverse Engineering		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Windows-Interna, ausführbare Dateien, x86-Assembler • Grundlegende Analysetechniken (String-Extraktion, Import-Analyse, • PE-Zugangspunkte auf einen Blick, automatisches Entpacken usw.) • Grundlegende dynamische Analysetechniken (Debugging, Überwachungstools, Abfangen von Datenverkehr usw.) • .NET, Visual Basic, Win64-Dateianalyse • Skript- und Nicht-PE-Analysetechniken (Batch-Dateien, Autoit, Python, Jscript, JavaScript, VBS)	5 Tage	• Aufbau einer sicheren Umgebung für Malware-Analyse: Bereitstellung der Sandbox und aller benötigten Tools • Verstehen der Prinzipien der Windows-Programmausführung • Entpacken, Debugging und Analyse von schädlichen Objekten und Identifizierung ihrer Funktionen • Erkennen von schädlichen Webseiten über die skriptbasierte Malware-Analyse • Durchführung von Malware-Expressanalysen
Advanced Digital Forensics		
• Umfassende Windows-Forensik • Datenwiederherstellung • Netzwerk- und Cloud-Forensik • Speicherforensik • Timeline-Analyse • Forensikübung eines realen gezielten Angriffs	5 Tage	• Durchführen einer umfassenden Dateisystemanalyse • Wiederherstellung gelöschter Dateien • Analyse des Netzwerkdatenverkehrs • Erkennung von schädlichen Aktivitäten in Speicherauszügen • Rekonstruieren des Vorfallablaufs
Erweiterte Malware-Analyse Reverse Engineering		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Erweiterte statische Analyseverfahren (statische Analyse von Shellcode, Analysieren von PE-Headern, TEB (Thread Environment Block, Datenstruktur in Windows NT), PEB (Process Environment Block, Datenstruktur in Windows NT), Ladefunktionen durch verschiedene Hash-Algorithmen) • Erweiterte dynamische Analysetechniken (PE-Struktur, manuelles und erweitertes Entpacken, Entpacken von schädlichen Packprogrammen, die die ausführbare Datei in verschlüsselter Form speichern) • APT Reverse Engineering (einschließlich APT-Angriffsszenario, angefangen bei Phishing-E-Mails bis hin zur möglichst tiefgreifenden Analyse) • Protokollanalyse (Analyse von verschlüsselten C2-Kommunikationsprotokollen, Entschlüsseln von Datenverkehr) • Analyse von Rootkits und Bootkits (Debuggen des Bootsektors mithilfe von Ida und VMWare, Kernel-Debugging mit zwei virtuellen Maschinen, Analyse von Rootkit-Proben)	5 Tage	• Befolgen von Best Practices im Bereich Reverse Engineering sowie Erkennung von Anti-Reverse-Engineering-Tricks (versteckte Bedrohungen, Anti-Debugging) • Anwendung erweiterter Malware-Analysen für die Zerlegung von Rootkits/Bootkits • Analyse von in verschiedene Dateitypen eingebettetem Exploit-Shellcode und Nicht-Windows-Malware

Programmbeschreibung

Themen	Dauer	Erlernte Fertigkeiten
Incident Response		
• Einführung in die Vorfallsreaktion • Erkennung und primäre Analyse • Digitale Analyse • Erstellen von Erkennungsregeln (YARA, Snort, Bro)	5 Tage	• Abgrenzung von APTs von anderen Bedrohungen • Verstehen der verschiedenen Angreifertechniken und des Aufbaus gezielter Angriffe • Anwenden bestimmter Überwachungs- und Erkennungsmethoden • Einhaltung des Workflows für die Vorfallsreaktion • Rekonstruktion der Vorfallschronologie und -logik • Erstellen von Erkennungsregeln und Reporting
Yara		
• Kurze Einführung in die Yara-Syntax • Tipps und Tricks zur Erstellung schneller und effektiver Regeln • Yara-Generatoren • Testen von Yara-Regeln auf Fehlalarme (False-Positives) • Aufspüren neuer, unentdeckter Proben auf VT • Verwenden externer Module innerhalb von Yara zum effektiven Aufspüren von Bedrohungen • Suche nach Anomalien • Zahlreiche (!) Beispiele aus dem echten Leben • Übungen zur Vertiefung der Yara-Kenntnisse	2 Tage	• Erstellen effektiver Yara-Regeln • Testen von Yara-Regeln • Verbessern der Regeln, bis sie Bedrohungen finden, die sonst niemand findet
KATA Administration		
• Allgemeine Szenarien der Lösungsbereitstellung und Serverstandorte • Größenüberlegungen • Lizenzmodell • Sandbox-Server • Zentraler Node • Sensor • Integration in Infrastruktur • Installation von Endpoint-Sensor • Hinzufügung einer Lizenz und Aktualisierung der Datenbanken • Algorithmus für Lösungsbetrieb	1 Tag	• Entwurf des Implementierungsplans für die Kundenumgebung • Installation und Einrichtung aller KATA-Komponenten • Verwaltung und Überwachung der Lösung
KATA Security Analyst		
• Interpretation der KATA-Warnungen • Erklärung der Erkennungs- und Analysetechnologien • Erklärung der Bewertung und Risiko-Engines	1 Tag	• Verstehen der Bewertung und ihrer Verwendung durch Risiko-Engines • Überwachung, Interpretation und Reaktion auf KATA-Warnungen

Kaspersky Incident Response Services

Obwohl Ihre IT- und Sicherheitsfachleute ihr Bestes geben, um sicherzustellen, dass jede der Netzwerkkomponenten gut geschützt ist und jederzeit für legitime Benutzer verfügbar bleibt, kann eine einzige Schwachstelle zum Einfallstor für Kriminelle werden, die den Zugriff auf Ihre Informationssysteme wollen. Niemand ist immun. Egal, wie effektiv Ihre Sicherheitskontrollen sind – Sie können schnell zum Opfer werden.

IT-Sicherheitsvorfälle zu vermeiden wird immer schwieriger. Doch selbst wenn es nicht immer möglich ist, einen Angriff zu stoppen, bevor er Ihren Sicherheitsperimeter überwindet, sind wir in der Lage, den entstehenden Schaden zu beschränken und eine weitere Ausbreitung des Angriffs zu verhindern.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Trainings**
- **Kaspersky Incident Response Services**
  Incident Response
  Malware-Analyse
  Digital Forensics
- **Kaspersky Security Assessment Services**

Das wichtigste Ziel der Vorfallsreaktion ist die Reduzierung der Auswirkungen einer Sicherheitsverletzung oder eines Angriffs auf Ihre IT-Umgebung. Der Service deckt den gesamten Vorfallsuntersuchungszyklus ab – von der Erfassung von Beweisen vor Ort über die Identifizierung zusätzlicher Gefährdungsindikatoren und der Vorbereitung eines Abhilfemaßnahmenplans bis hin zur vollständigen Beseitigung der Bedrohung aus Ihrem Unternehmen.

Dies erfolgt auf folgende Weise:

- Identifizierung angegriffener Ressourcen
- Isolierung der Bedrohung
- Verhinderung einer weiteren Ausbreitung des Angriffs
- Suchen und Erfassen von Beweisen
- Analyse der Beweise und Rekonstruktion der Chronologie und Logik des Vorfalls
- Analyse der für den Angriff verwendeten Malware (falls diese gefunden wird)
- Aufdecken der Angriffsquellen und anderer potentiell gefährdeter Systeme (falls möglich)
- Durchführung toolgestützter Scans Ihrer IT-Infrastruktur zur Aufdeckung möglicher Gefährdungshinweise
- Analyse ausgehender Verbindungen zu externen Ressourcen (z. B. mögliche Befehls- und Controll-Server) zur Aufspürung von verdächtigem Verhalten
- Beseitigung der Bedrohung
- Empfehlung weiterer möglicher Abhilfemaßnahmen

Je nachdem, ob Sie ein internes Incident Response-Team haben oder nicht, können Sie unsere Experten damit beauftragen, eine vollständige Untersuchung durchzuführen, um angegriffene Computer zu identifizieren und zu isolieren und eine Ausbreitung der Bedrohung zu verhindern, oder um eine Malware-Analyse oder digitale Forensik durchführen zu lassen.

Die Incident Response Services von Kaspersky Lab werden von erfahrenen Experten auf dem Gebiet der Analyse von Cyberbedrohungen sowie von Ermittlern erbracht. Wir setzen unser gesamtes Wissen und unsere globale Erfahrung in den Bereichen digitale Forensik und Malware-Analyse für die Behebung Ihres Sicherheitsvorfalls ein.

Malware-Analyse

Die Malware-Analyse liefert ein vollständiges Bild des Verhaltens und der Ziele bestimmter Malware-Dateien, die es auf Ihr Unternehmen abgesehen haben. Die Experten von Kaspersky Lab führen eine detaillierte Analyse der von Ihrem Unternehmen bereitgestellten Malware-Probe durch und erstellen einen detaillierten Bericht, der Folgendes enthält:

- **Eigenschaften der Malware-Probe:** Eine kurze Beschreibung der Probe und eine Einschätzung zur Malware-Klassifizierung.

- **Detaillierte Beschreibung der Malware:** Eine umfassende Analyse der Funktionen der Malware-Probe, des Verhaltens und der Ziele der Bedrohung (inkl. IOCs), um Ihnen die erforderlichen Informationen zur Neutralisierung ihrer Aktivitäten zu liefern.

- **Beseitigung:** In dem Bericht werden Schritte zur vollständigen Sicherung Ihres Unternehmens vor dieser Art von Bedrohung vorgeschlagen.

Digital Forensics

Die digitale Forensik kann eine Malware-Analyse umfassen, wie oben gezeigt, falls Malware während der Untersuchung gefunden wurde. Unsere Experten bei Kaspersky Lab setzen die Beweise zusammen, um genau zu verstehen, was vor sich geht, darunter Festplatten-Images, Speicherauszüge und Netzwerk-Traces. Das Ergebnis ist eine detaillierte Aufklärung des Vorfalls. Sie als Kunde leiten diesen Vorgang ein, indem Sie Beweise sammeln und einen Abriss des Vorfalls bereitstellen. Daraufhin analysieren die Experten von Kaspersky Lab die Vorfallssymptome, identifizieren den Malware-Binärcode (falls vorhanden) und führen die Malware-Analyse durch, um einen detaillierten Bericht inklusive empfohlener Korrekturmaßnahmen bereitzustellen.

Bereitstellungsoptionen

Die Incident Response Services von Kaspersky Lab sind verfügbar:

- als Abonnement
- als Reaktion auf einen einzelnen Vorfall

Beide Optionen werden nach Aufwand unserer Experten für die Aufklärung eines Vorfalls berechnet. Dies wird vor der Unterzeichnung des Vertrags mit Ihnen verhandelt. Sie können die gewünschte Anzahl an Stunden, die wir aufwenden sollen, festlegen, oder Sie folgen den Empfehlungen unserer Experten, die sich nach Ihrem speziellen Vorfall und Ihren individuellen Anforderungen richten.

Kaspersky Security Assessment Services

Bei den Security Assessment Services von Kaspersky Lab handelt es sich um die Services unserer internen Experten. Viele von ihnen sind internationale Autoritäten auf ihrem Gebiet und von fundamentaler Bedeutung für die Entwicklung unserer Security Intelligence.

Da keine zwei IT-Infrastrukturen exakt gleich und die gefährlichsten Cyberbedrohungen individuell auf die Schwachstellen von Unternehmen zugeschnitten sind, sind auch unsere Expertenservices ein maßgeschneidertes Angebot. Die auf den folgenden Seiten beschriebenen Services sind Teil unseres professionellen Toolkits – sie kommen während der Zusammenarbeit mit Ihnen selektiv bzw. teilweise oder vollständig zum Einsatz.

Unser vorrangiges Ziel besteht darin, individuell als Berater für Sie tätig zu werden, Ihr Risiko zu bewerten, Ihre Sicherheitsmaßnahmen zu verschärfen und Sie vor zukünftigen Bedrohungen zu schützen.

Security Assessment Services beinhalten Folgendes:

- Penetration Testing
- Application Security Assessment
- ATM/POS Security Assessment
- Telecommunication Networks Security Assessment

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Trainings**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**
  - Penetration Testing
  - Assessment der Programmsicherheit
  - ATM/POS Security Assessment
  - Telecommunication Networks Security Assessment

Penetration Testing

Sicherzustellen, dass die IT-Infrastruktur umfassend vor potenziellen Cyberattacken geschützt ist, ist für jedes Unternehmen eine ständige Herausforderung – insbesondere jedoch für Großunternehmen mit Tausenden von Mitarbeitern, Hunderten von Informationssystemen und einer Vielzahl von Standorten weltweit.

Ein Penetrationstest ist eine praktische Demonstration möglicher Angriffsszenarien, in denen versucht wird, die Sicherheitskontrollen Ihres Unternehmensnetzwerks zu umgehen, um Zugriff auf wichtige Systeme zu erlangen.

Unsere Penetrationstests vermitteln Ihnen ein genaues Verständnis der Sicherheitslücken in Ihrer Infrastruktur, indem wir die möglichen Konsequenzen unterschiedlicher Angriffsarten analysieren, die Effektivität Ihrer aktuellen Sicherheitsmaßnahmen bewerten und Abhilfe- und Verbesserungsmaßnahmen vorschlagen.

Dank unserer Penetrationstests können Sie:

- **Schwachpunkte in Ihrem Netzwerk identifizieren,** um eine fundierte Entscheidung darüber zu treffen, wie finanzielle Mittel am besten einzusetzen sind, um das Risiko in Zukunft zu verringern.
- **Finanzielle und betriebliche Verluste sowie Rufschädigungen durch Cyberangriffe vermeiden,** indem Sie diese durch frühzeitige Erkennung und Schließen von Schwachstellen verhindern.
- **Behördliche Auflagen und Branchen- bzw. unternehmensinterne Normen erfüllen,** die diese Art von Sicherheitsprüfung vorschreiben (z. B. der Datensicherungsstandard für Kreditkartentransaktionen, PCI-DSS).

Ergebnisse der Penetrationstests

Penetrationstests sollen Sicherheitslücken aufdecken, die ausgenutzt werden könnten, um Zugriff auf wichtige Netzwerkkomponenten zu erlangen. Dies beinhaltet u. a.:

- Anfällige Netzwerkarchitektur, unzureichender Netzwerkschutz
- Schwachstellen, die das Abfangen und Umleiten des Netzwerkverkehrs ermöglichen
- Unzureichende Authentifizierungs- und Autorisierungsmechanismen von unterschiedlichen Diensten
- Schwache Benutzeranmeldedaten
- Konfigurationsfehler inklusive zu umfangreicher Benutzerberechtigungen
- Schwachstellen durch Fehler im Programmcode (Code-Injektionen, Manipulation von Pfadangaben, Schwachstellen auf Clientseite usw.)
- Schwachstellen durch veraltete Hardware und Software ohne aktuelle Sicherheitsupdates
- Bereitstellung der Ergebnisse

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst, einschließlich detaillierter technischer Informationen zum Testvorgang, Ergebnissen, den entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie einer Kurzübersicht über die Testergebnisse und die möglichen Angriffsvektoren. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

Serviceumfang und Optionen

Abhängig von Ihren Anforderungen und der bestehenden IT-Infrastruktur können Sie beliebige oder alle der folgenden Services in Anspruch nehmen:

- **Externer Penetrationstest:** Über das Internet vorgenommene Sicherheitsprüfung durch einen „Angreifer" ohne Vorkenntnisse über Ihr System.

- **Interner Penetrationstest:** Szenarien mit einem internen Angreifer, z. B. einem Besucher, der nur physischen Zugang zu Ihren Büroräumen hat, oder einem Dienstleister, der nur eingeschränkten Zugriff auf Ihre Systeme hat.

- **Social-Engineering-Test:** Assessment des Sicherheitsbewusstseins Ihrer Mitarbeiter durch Simulation von Social-Engineering-Angriffen, z. B. Phishing, schädliche Links in E-Mails, verdächtige Anhänge usw.

- **WLAN-Sicherheitsassessments:** Unsere Experten besuchen Ihren Standort und analysieren Ihre WLAN-Sicherheitskontrollen.

Welche Teile Ihrer IT-Infrastruktur Sie testen lassen, bleibt Ihnen überlassen, wir empfehlen jedoch, entweder das gesamte Netzwerk oder zumindest die größten Segmente einzubeziehen, da die Testergebnisse aussagekräftiger sind, wenn unsere Experten unter denselben Bedingungen arbeiten wie potentielle Eindringlinge.

Informationen zur Vorgehensweise von Kaspersky Lab bei Penetrationstests

Obwohl bei Penetrationstests echte Hacker-Angriffe simuliert werden, werden diese Tests streng kontrolliert. Sie werden von Kaspersky-Sicherheitsexperten unter vollständiger Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme ausgeführt und halten sich streng an internationale Normen und Best Practices, darunter:

- Ausführungsnorm für Penetrationstests (PTES)
- NIST Special Publications 800-115 „Technical Guide to Information Security Testing and Assessment"
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Experten mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, die als Sicherheitsberater von Branchenführern wie Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens und SAP anerkannt sind.

Bereitstellungsoptionen

Je nach Art des gewünschten Sicherheitsassessments und ihrer speziellen Systembedingungen und Arbeitsabläufe können die Services entweder remote oder am Standort geleistet werden. Die meisten Services lassen sich per Fernzugriff ausführen, und selbst die internen Penetrationstests können per VPN-Zugriff durchgeführt werden. Einige Services (z. B. WLAN-Sicherheits-Assessments) können jedoch nur vor Ort ausgeführt werden.

Application Security Assessment

Egal, ob Sie Ihre Unternehmensanwendungen intern entwickeln oder diese extern einkaufen, Sie wissen, dass ein einziger Fehler im Code zu einer Schwachstelle führen kann, die bei Angriffen erhebliche finanzielle Verluste und Imageschäden nach sich ziehen könnten. Während des Programmlebenszyklus können außerdem weitere Schwachstellen hinzukommen, etwa durch Softwareupdates oder eine unsichere Komponentenkonfiguration bzw. durch neue Angriffsmethoden.

Unsere Application Security Assessments decken Schwachstellen in beliebigen Anwendungstypen auf, von umfangreichen Cloud-basierten Lösungen, ERP-Systemen,

Online-Banking und anderen speziellen Geschäftsanwendungen bis hin zu integrierten und mobilen Anwendungen auf unterschiedlichen Plattformen (iOS, Android und andere).

Dank einer Kombination aus Praxiswissen und Erfahrung mit international anerkannten Best Practices entdecken unsere Experten Sicherheitslücken, die Ihr Unternehmen anfällig für unterschiedliche Angriffstypen machen könnten, u. a.:

- Abschöpfen vertraulicher Daten
- Infiltration und Manipulation von Daten und Systemen
- DoS-Attacken
- Betrügerische Aktivitäten

Auf Grundlage unserer Empfehlungen lassen sich die in den Programmen entdeckten Schwachstellen beheben und die aufgeführten Angriffstypen vermeiden.

Servicevorteile

Die Application Security Assessments von Kaspersky Lab bieten den Programmeigentümern und -entwicklern folgende Vorteile:

- **Keine finanziellen und betrieblichen Verluste sowie Imageschäden** durch frühzeitige Erkennung und Behebung von Schwachstellen, die für Angriffe genutzt werden könnten
- **Keine Korrekturkosten,** da Programmschwachstellen noch während der Entwicklung identifiziert werden, bevor sie die Produktionsumgebung erreichen, wo die Behebung meist mit erheblichen Störungen und Kosten verbunden ist.
- **Unterstützung des Secure Software Development Lifecycle** (S-SDLC) für Entwicklung und Betrieb sicherer Softwareprogramme.
- **Einhaltung von Verordnungen sowie von Branchen- und internationalen Unternehmensstandards** zur Programmsicherheit, z. B. PCI DSS oder HIPAA

Serviceumfang und Optionen

Zu den getesteten Programmen gehören u. a. offizielle Webseiten und Unternehmensprogramme (herkömmlich oder Cloud-basiert), darunter auch integrierte oder mobile Programme.

Die Tests werden an Ihre Bedürfnisse und die Besonderheiten der zu testenden Software angepasst. Zu den Services gehören u. a.:

- **Black-Box-Tests** zur Simulation eines externen Angreifers
- **Grey-Box-Tests** zur Simulation von autorisierten Benutzern mit verschiedenen Profilen
- **White-Box-Tests** zur Analyse mit umfassendem Zugriff auf die Anwendung, einschließlich des Quellcodes. Dieser Ansatz ist am effektivsten, wenn es darum geht, möglichst viele Schwachstellen zu entdecken.
- **Application Firewall Effectiveness Assessment:** Programme werden mit und ohne Firewall-Schutz getestet, um Schachstellen zu finden und festzustellen, ob potentielle Exploits geblockt werden

Unsere Vorgehensweise beim Application Security Assessment

Das Application Security Assessment wird von unseren Experten sowohl manuell als auch mithilfe automatisierter Tools ausgeführt. Hierbei kommt dem Schutz von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme sowie der strengen Einhaltung u. a. der folgenden internationalen Normen und Best Practices besondere Bedeutung zu:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Weitere Standards, abhängig von der Branche und dem Standort Ihres Unternehmens

Ergebnisse

Zu den durch die Assessment-Services von Kaspersky Lab ermittelten Schwachstellen gehören:

- Fehler bei Authentifizierung und Autorisierung, inklusive Multifaktor-Authentifizierung
- Code-Injektion (SQL-Injektion, OS-Commanding usw.)
- Logische Schwachstellen, die Betrugsversuche begünstigen
- Schwachstellen auf Clientseite (Cross-Site-Scripting, Cross-Site Request Forgery usw.)
- Schwache Kryptografie
- Schwachstellen in Client-Server-Verbindungen
- Unsicheres Speichern und Übertragen von Daten, z. B. fehlende PAN-Maskierung in Bezahlsystemen
- Konfigurationsfehler, z. B. Fehler, die zu Attacken auf Sitzungen führen
- Offenlegung vertraulicher Informationen
- Weitere Schwachstellen, die zu den im Bericht „WASC Threat Classification v2.0" und in den „OWASP Top Ten" aufgeführten Bedrohungen führen können.

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst, einschließlich detaillierter technischer Informationen zu Testvorgang, Ergebnissen, entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie einer Kurzübersicht, in der mögliche Folgen für die Geschäftsführung beschrieben werden. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Profis mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, inklusive der verschiedenen Plattformen, Programmiersprachen, Frameworks, Schwachstellen und Angriffsmethoden. Sie treten als Redner bei wichtigen internationalen Konferenzen auf und arbeiten als Sicherheitsberater für führende Software- und Cloud-Service-Anbieter, darunter Oracle, Google, Apple, Facebook und PayPal.

Bereitstellungsoptionen

Je nach Art des gewünschten Sicherheitsassessments und ihrer speziellen Systembedingungen und Anforderungen an die Arbeitsbedingungen können die Services entweder remote oder am Standort geleistet werden. Die meisten der Services lassen sich remote ausführen.

ATM/POS Security Assessment

Geldautomaten und Kassensysteme sind nicht mehr allein physischen Angriffen wie Aufbrechen oder Kartenbetrug ausgesetzt. Mit zunehmender Ausgereiftheit der Schutzmaßnahmen für Geldautomaten/Kassensysteme von Banken und Herstellern werden auch die Angriffe auf diese Geräte immer raffinierter. Hacker nutzen die Schwachstellen von Geldautomaten/Kassensystemen und -Anwendungen aus und entwickeln Malware, die speziell auf diese Geräte zugeschnitten ist. ATM/POS Security Assessments von Kaspersky Lab unterstützen Sie bei der Erkennung von Sicherheitsfehlern in Ihren Geldautomaten/Kassensystemen und somit bei der Abwehr von Angriffen.

ATM/POS Security Assessments umfassen die eingehende Analyse Ihrer Geldautomaten und/oder Kassensysteme. Mithilfe dieser Analyse werden Schwachstellen erkannt, die Angreifer für Aktivitäten wie unberechtigtes Abheben von Geld, unberechtigte Transaktionen, Abfangen der Zahlungskarteninformationen oder Initiieren eines DoS-Angriffs nutzen. Dieser Service deckt sämtliche Schwachstellen in der Infrastruktur Ihrer Geldautomaten und Kassensysteme auf, die Angreifer auf verschiedene Arten ausnutzen können. Darüber hinaus erhalten Sie einen Überblick über die möglichen Folgen eines Angriffs, die Effektivität Ihrer vorhandenen Sicherheitsmaßnahmen sowie Empfehlungen zur Verbesserung der Sicherheit.

Servicevorteile

ATM/POS Security Assessments von Kaspersky Lab ermöglichen Herstellern und Finanzinstituten Folgendes:

- **Erkennen der Schwachstellen** in ihren Geldautomaten/Kassensysteme und Verbessern der entsprechenden Sicherheitsverfahren
- **Vermeiden der durch einen Angriff möglichen finanziellen und betrieblichen Verluste sowie von Rufschädigungen** durch schnelle Erkennung und Behebung der Schwachstellen, die von Angreifern ausgenutzt werden könnten.
- **Einhalten behördlichen, Branchen- oder Unternehmensstandards,** die die Durchführung von Sicherheitsassessments wie PCI DSS (Payment Card Industry Data Security Standard) vorschreiben.

Serviceumfang

Der Service beinhaltet umfassende Analysen von Geldautomaten/Kassensystemen, einschließlich Fuzzing und Demonstration von Angriffen in Testumgebungen. Dies kann auf einem einzelnen Geldautomaten/Kassensystem oder in einem Netzwerk mit mehreren Geräten erfolgen. Sie sollten für das Assessment entweder den Geldautomaten-/Kassensystemtyp, den Sie auch am häufigsten in Ihrem Unternehmen einsetzen, oder den am meisten gefährdeten Gerätetyp (der z. B. bereits Opfer eines Angriffs wurde) mit typischen Konfigurationen verwenden.

Ergebnisse der ATM/POS Security Assessments

Die ATM/POS Security Assessments identifizieren eine Reihe von Schwachstellen, darunter:

- Schwachstellen in Netzwerkarchitekturen und unzureichender Netzwerkschutz
- Schwachstellen, die es Angreifern ermöglichen, den Kiosk-Modus zu verlassen und unberechtigten Zugriff auf das Betriebssystem zu erlangen
- Schwachstellen in Sicherheitssoftware von Drittanbietern, die potentiellen Angreifern die Umgehung von Sicherheitskontrollen ermöglichen
- Unzureichender Schutz von Eingabe- und Ausgabegeräten (Kartenlesegerät, Automaten usw.), einschließlich Schwachstellen in der Gerätekommunikation, die das Abfangen und Modifizieren der übertragenen Daten ermöglichen
- Schwachstellen, die durch Fehler im Programmcode oder veraltete Hardware- und Softwareversionen (Buffer Overflows, Codeinjektionen usw.) entstehen
- Offenlegung von Informationen

Nach Abschluss des Assessments erhalten Sie einen Bericht, der detaillierte technische Informationen zum Test, die Ergebnisse, die Schwachstellen und unsere Empfehlungen sowie unsere Schlussfolgerungen basierend auf den Testergebnissen enthält. Außerdem werden die verschiedenen Angriffsvektoren dargestellt. Auf Anfrage können auch Videos zur Demonstration eines Angriffs und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

Unsere Vorgehensweise beim ATM/POS Security Assessment

Bei der Analyse suchen unsere Experten nicht nur nach Konfigurationsfehlern und Schwachstellen in veralteten Softwareversionen, sondern führen auch eine umfangreiche Analyse der zugrunde liegenden Logik eines Geldautomaten/Kassensystems durch. Die Sicherheitsanalyse hat das Ziel, neue Schwachstellen (Zero-Day) auf Komponentenebene zu finden. Wenn wir Schwachstellen finden, die ein Angreifer ausnutzen könnte (z. B. in Form einer unberechtigten Barabhebung), können unsere Experten mögliche Angriffsszenarien mithilfe von speziell entwickelten Automatisierungstools oder -geräten nachstellen.

Unsere ATM/POS Security Assessments sind absolut sicher und nicht invasiv, auch wenn sie die Simulation des Angriffsverhaltens eines echten Hackers beinhalten, um die Effektivität Ihrer Verteidigungsstrategie in der Praxis zu beurteilen. Der Service wird von erfahrenen Kaspersky-Sicherheitsexperten erbracht. Hierbei kommt der Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme sowie der strengen Einhaltung von internationalen Normen und Best Practices besondere Bedeutung zu. Wenn wir eine neue Schwachstelle in einem Geldautomaten/Kassensystem eines Kunden finden, benachrichtigen wir den Hersteller unter Einhaltung einer verantwortungsvollen Informationspolitik und stehen ihm bei der Behebung des Fehlers beratend zur Seite.

Kaspersky Lab bietet ATM/POS Security Assessments gemäß den folgenden internationalen Standards und Best Practices an:

- PCI-Standards (Payment Card Industry)
  - Data Security Standard
  - Payment Application Data Security Standard
  - PIN Transaction Security
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Common Vulnerability Scoring System (CVSS)
- Weitere geltende Standards für bestimmte Geschäftsmodelle und geografische Regionen, sofern erforderlich.

Die Mitglieder des Projektteams sind Experten für praktische Sicherheit und verfügen über langjährige Außendiensterfahrung. Zudem bilden sie sich stets weiter, beraten regelmäßig Hersteller von Geldautomaten/Kassensystemen und präsentieren die Ergebnisse unserer Forschungen im Bereich Geldautomaten-/Kassensystemsicherheit auf wichtigen IT-Sicherheitskonferenzen (wie Black Hat).

Telecommunication Networks Security Assessment

Serviceüberblick

Die IT-Landschaft eines Telekommunikationsunternehmens beinhaltet eine Reihe von verbundenen Netzwerken, die auf verschiedenen Funktionen und Technologien basieren. Dazu zählen in der Regel ein Unternehmensnetzwerk mit Verwaltungselementen, ein Hauptfunknetz (GSM/UMTS/LTE) für den Breitbandinternetzugriff für Abonnenten, dedizierte Hochgeschwindigkeits-Trunk-Verbindungen sowie Hosting- und Cloud-Services. Jede Komponente dieser Infrastruktur ist wichtig für das Unternehmen und muss angemessen vor Hackerangriffen geschützt werden, um finanzielle und betriebliche Risiken sowie Rufschädigungen zu vermeiden. Die Telecommunication Networks Security Assessment Services ermöglichen Ihnen eine Risikominderung durch das Aufspüren von Schwachstellen in Ihren Systemen, die dann entweder entfernt oder deren Auswirkungen durch die Einführung von Kontrollmechanismen behoben werden.

Kaspersky Lab bietet die folgenden Telecommunication Networks Security Assessment Services:

- Penetrationstests für IT-Infrastrukturen
- IT Infrastructure Configuration Security Assessment
- Sicherheitsassessments für GSM-/UMTS-/LTE-Netze
- Application Security Assessment (für Programme mit verschiedenen Services: IP-TV, Self-Service-Portale für Kunden usw.)

- VoIP Security Assessment
- Telecommunication Equipment Security Assessment Services

Service-Ergebnisse

Nach Abschluss eines Sicherheitsassessments erhalten Sie einen technischen und allgemeinen Überblick über die Sicherheitsfehler in Ihren Telekommunikationsnetzen sowie eine Auflistung unserer Schlussfolgerungen über die Effektivität Ihrer Sicherheitskontrollen. Diese Ergebnisse können Sie nutzen, um die Sicherheit Ihres Netzwerks zu erhöhen und finanzielle und betriebliche Risiken sowie Rufschädigungen im Zusammenhang mit den IT-Sicherheitsbedrohungen zu verhindern.

Der Bericht enthält die folgenden Informationen:

- Allgemeine Schlussfolgerungen zum aktuellen Sicherheitsstatus Ihrer Telekommunikationsnetze
- Beschreibung der Servicemethode und -prozesse
- Genaue Beschreibung der erkannten Schwachstellen, darunter Schweregrad, Komplexität der Ausnutzung, mögliche Auswirkungen für das anfällige System, Nachweis über die Existenz der Schwachstelle (wo möglich)
- Empfehlungen zur Beseitigung der Schwachstelle, einschließlich Konfigurationsänderungen, Updates, Änderungen des Quellcodes oder der Implementierung ausgleichender Kontrollen, wenn die Schwachstelle nicht entfernt werden kann

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten:
https://www.kaspersky.de/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.de

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.