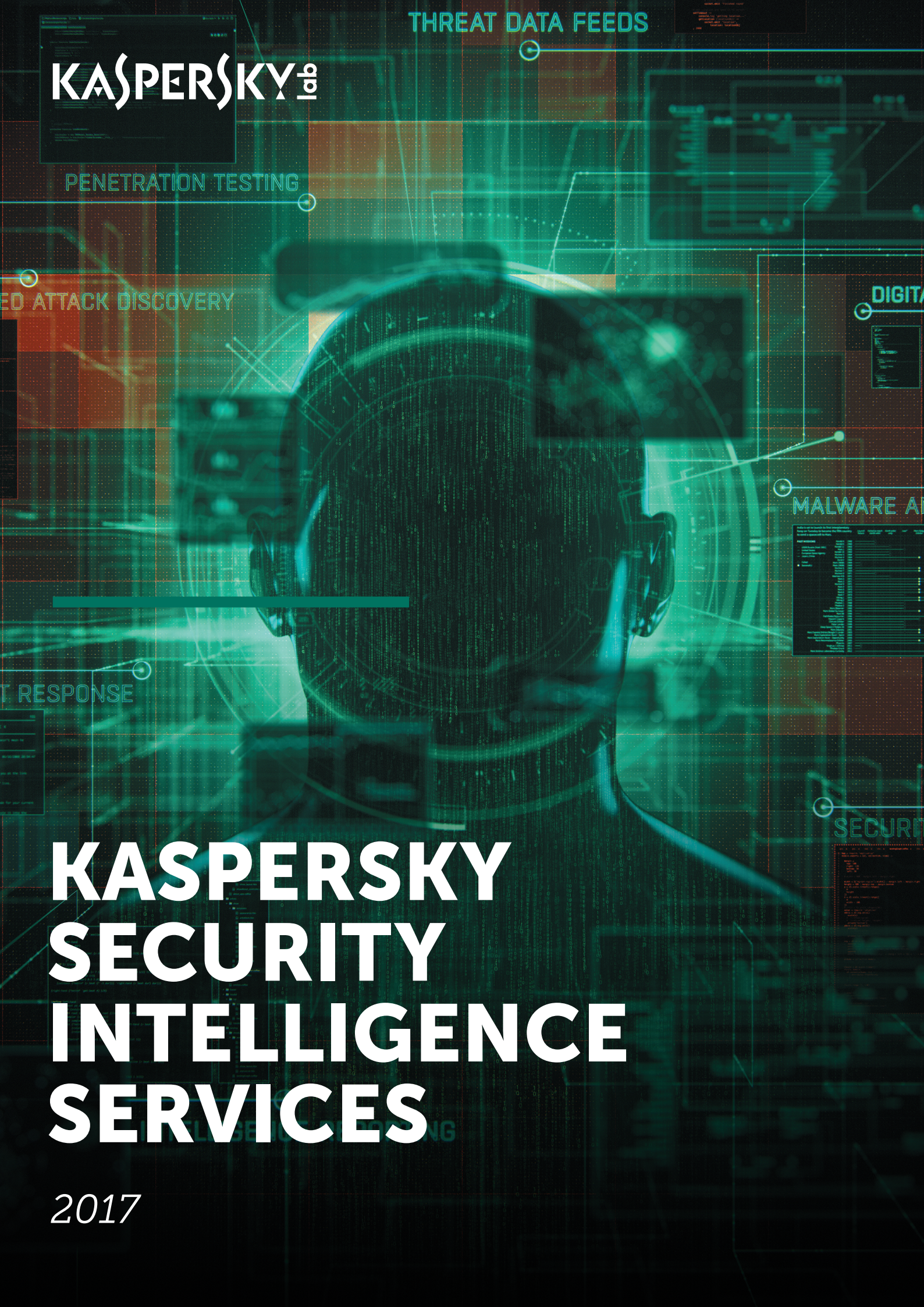


KASPERSKY SECURITY INTELLIGENCE SERVICES

2017

Cyberverbrechen kennen heute keine Grenzen, 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 sicherer 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
Chairman 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.

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 Security Intelligence Services profitieren.

SICHERHEIT MIT EINEM ENTSCHEIDENDEN UNTERSCHIED

Unser Ziel ist es, mit unseren Security Intelligence Services den aktuellen Bedrohungen immer einen Schritt voraus zu sein. Dadurch sind wir in der Lage, einen leistungsstarken Malware-Schutz bereitzustellen.

In unserem Unternehmen steht Technologie auf allen Mitarbeiterebenen im Mittelpunkt – ausgehend von unserem CEO Eugene Kaspersky.

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 und perfektioniert 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.

CYBERSECURITY TRAININGS

Machen Sie sich das Wissen, die Erfahrung und die Erkenntnisse von Kaspersky Lab im Bereich Cybersicherheit im Rahmen dieses innovativen Schulungsprogramms zunutze.

Angesichts einer ständig wachsenden Menge immer ausgeklügelterer Bedrohungen ist die Sensibilisierung und Schulung von Mitarbeitern im Bereich der Cybersicherheit für Unternehmen zu einer unerlässlichen Grundvoraussetzung geworden. Mitarbeiter in der IT-Sicherheit müssen die Sicherheitsverfahren kennen, die eine wichtige Komponente für ein effektives Bedrohungsmanagement und Strategien zur Risikominimierung im Unternehmen bilden. Darüber hinaus sollten alle Mitarbeiter ein allgemeines Verständnis der bestehenden Gefahren haben und mit sicheren Arbeitsmethoden vertraut sein.

Unsere Cybersecurity Trainings wurden speziell für Unternehmen entwickelt, die einen effektiveren Schutz von Infrastruktur und geistigem Eigentum benötigen. Sämtliche Schulungen sind auf Englisch verfügbar (Schulungen zum Cybersicherheitsbewusstsein sind in mehr als zehn Sprachen verfügbar).

DIE KURSE

SENSIBILISIERUNG VON MITARBEITERN AUSSERHALB DER IT	IT-SICHERHEITSSCHULUNG
Alle Mitarbeiter	Einsteiger
SCHULUNGSPLATTFORM FÜR CYBERSECURITY TRAININGS CyberSecurity Awareness	GRUNDLAGEN DER CYBERSICHERHEIT Online-Schulung für grundlegendes IT-Wissen POSITIVE MOTIVATION Effektive Kommunikation zur Cybersicherheit
Bereichsleiter	Fortgeschrittener
CYBERSAFETY MANAGEMENT GAMES „Cybersichere" Geschäftsentscheidungen	DIGITALE FORENSIK Systemverwaltungsfähigkeiten erforderlich MALWARE-ANALYSE UND REVERSE ENGINEERING Programmierungsfähigkeiten erforderlich
Führungskräfte und CISO	Experte
KASPERSKY INTERACTIVE PROTECTION (KIPS) Strategie und Unterstützung für das Unternehmen	ERWEITERTE DIGITALE FORENSIK Fortgeschrittene Systemverwaltungsfähigkeiten erforderlich ERWEITERTE MALWARE-ANALYSE UND REVERSE ENGINEERING Assembler-Fähigkeiten erforderlich
Geschäftsführer	Mitarbeiter für Vorfallsreaktion und Sicherheitsanalysten
ASSESSMENT DER CYBERSICHERHEITSKULTUR Berichte zu Werten und Einstellungen hinsichtlich Cybersicherheit	VORFALLSREAKTION UND YARA

CYBERSICHERHEITS-BEWUSSTSEIN

Interaktive Schulungsprogramme, die den Aufbau einer sicheren Cyberumgebung im Unternehmen ermöglichen. Die auf Planspielen und fundiertem Cybersicherheitswissen basierenden Kaspersky-Produkte zum Sicherheitsbewusstsein sollen jedem Nicht-IT-Mitarbeiter die relevanten Kenntnisse und Motivationen vermitteln.

Über 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Es kostet Unternehmen Millionen, sich von Vorfällen mit Mitarbeiterbeteiligung zu erholen. Leider ist die Effektivität herkömmlicher Schulungsprogramme zur Vermeidung dieser Probleme beschränkt. Sie führen in der Regel nicht zum gewünschten Verhalten und zur gewünschten Motivation.

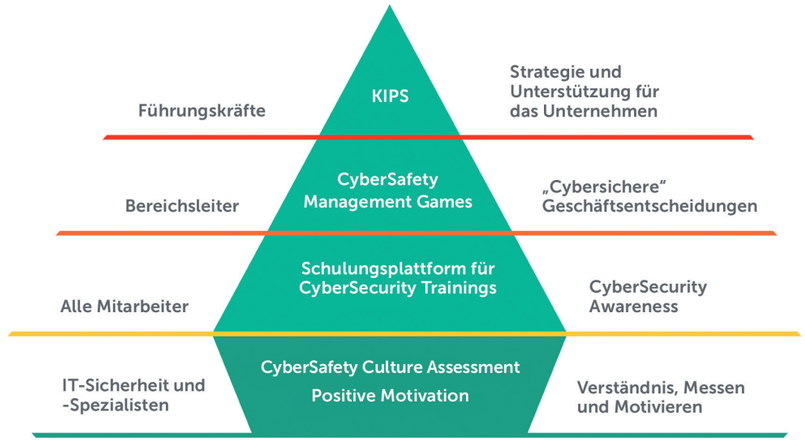
Kaspersky Lab hat eine Reihe von computerbasierten Schulungsprodukten auf den Markt gebracht, die auf modernen Lerntechniken basieren und an sämtliche Unternehmensebenen gerichtet sind. Unser Schulungsprogramm hat sich bereits bewährt – sowohl für unsere Kunden als auch für die Partner von Kaspersky Lab:

- **Entwicklung von Verhaltensweisen statt einer reinen Wissensvermittlung**: Dieser Lernansatz beruht auf Planspielen, Learning by Doing, Gruppendynamik, simulierten Angriffen, Lernpfaden usw. Das Ergebnis sind fest verankerte Verhaltensweisen mit einem langfristigen Effekt auf die Cybersicherheit.
- **Aufbau einer Cybersicherheitskultur** getreu dem Motto: „Cybersicherheit geht jeden an, also auch mich". Dies erzeugt Werte, Gewohnheiten und Einstellungen, die eine selbsttragende Sicherheitskultur bilden.
- **Ein funktionierendes Programm zum Sicherheitsbewusstsein**: Reduzierung der Vorfälle um bis zu 90 %, Senkung der potentiellen finanziellen Verluste durch Cyberrisiken um 50 bis 60 %, Wahrscheinlichkeit von bis zu 93 %, dass das Erlernte im Alltag eingesetzt wird.

FUNKTIONSWEISE

Die Schulung deckt ein breites Spektrum an Sicherheitsthemen ab: von Datenlecks und Ransomware über internetbasierte Malware-Angriffe bis hin zu sicheren Sozialen Netzwerken und mobiler Sicherheit.

Dauerhaftes Lernen führt zur kontinuierlichen Festigung von Wissen und fördert die Motivation im gesamten Unternehmen.



Unterschiedliche Schulungen für unterschiedliche Unternehmensebenen und -funktionen schaffen eine Cybersicherheitskultur der Zusammenarbeit, die von jedem Einzelnen gelebt und von der Führungsebene gefördert wird.

Über Analyse- und Reporting-Tools werden die Fähigkeiten und der Lernfortschritt sowie die Effektivität des Schulungsprogramms auf den einzelnen Unternehmensebenen gemessen.

SCHULUNGEN FÜR MITARBEITER IN DER IT-SICHERHEIT

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.

EINSTEIGER, FORTGESCHRITTENER ODER EXPERTE?

Das Programm deckt alles von den Sicherheitsgrundlagen bis zur erweiterten digitalen Forensik und Malware-Analyse ab. So helfen wir Unternehmen, ihr Wissen über Cybersicherheit in drei Hauptbereichen zu erweitern:

- Grundwissen zum Thema
- Digitale Forensik und Vorfallsreaktion
- Malware-Analyse und Reverse Engineering

SERVICEVORTEILE

Grundlagen der Cybersicherheit
Vermittelt IT- und Sicherheitsadministratoren sowie Führungskräften ein grundlegendes Verständnis aktueller Modelle der praktischen IT-Sicherheit.

Digitale Forensik
Verbessert das Fachwissen Ihres internen Teams für digitale Forensik und Vorfallsreaktion.

Malware-Analyse und Reverse Engineering
Verbessert das Fachwissen Ihres internen Teams für Malware-Analyse und Reverse Engineering.

Vorfallsreaktion
Verbessert das Fachwissen Ihres internen Vorfallsreaktionsteams.

Yara
Verbessert die Fähigkeiten Ihres Vorfallsreaktionsteams bis zu einer Stufe, auf der es Bedrohungen findet, die sonst niemand findet.

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
GRUNDLAGEN DER CYBERSICHERHEIT		
• Übersicht über Cyberbedrohungen und den Untergrundmarkt • Spam und Phishing, E-Mail-Sicherheit • Technologien zum Betrugsschutz • Exploits, mobile und hochentwickelte, hartnäckige Bedrohungen • Grundlagen der Untersuchung mit öffentlichen Webtools • Sicherung Ihres Arbeitsplatzes	ATC/ Online	• Erkennung und Behebung von Sicherheitsvorfällen • Reduzierung der Belastung für die Informationssicherheitsabteilungen • Erhöhung der IT-Sicherheit für den Arbeitsplatz jedes einzelnen Mitarbeiters durch zusätzliche Tools • Ausführung von grundlegenden Untersuchungen • Analyse von Phishing-E-Mails • Erkennung von infizierten oder gefälschten Webseiten
ALLGEMEINE DIGITALE FORENSIK		
• 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
ALLGEMEINE MALWARE-ANALYSE UND REVERSE ENGINEERING		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Windows-Interna, ausführbare Dateien, x86-Assembler • Grundlegende statische Analysetechniken (Extrahierung von Zeichenfolgen, Importanalyse, 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
ERWEITERTE DIGITALE FORENSIK		
• 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 UND 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
VORFALLSREAKTION		
• 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-SCHULUNG		
• 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

THREAT INTELLGENCE SERVICES

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen sind für den effektiven Umgang mit IT-Sicherheitsbedrohungen auf aktuelle und relevante Daten angewiesen.

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 angesehener 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:

- Machine-Readable Threat Intelligence
- Botnet Tracking
- Intelligence Reporting
- Tailored Reporting
- Kaspersky Threat Lookup
- Kaspersky Managed Protection

MACHINE-READABLE THREAT INTELLIGENCE

Verstärken Sie Ihre Netzwerksicherheitslösungen, darunter SIEM-Systeme, Firewalls, IPS/IDS, Anti-APT und Sandbox-/Simulationsverfahren, durch umfassende, laufend aktualisierte Daten, die Ihnen wichtige Einblicke in Cyberbedrohungen und gezielte Angriffe liefern.

Die unterschiedlichen Familien und Varianten von Malware sind in den letzten Jahren exponentiell gewachsen. Derzeit erkennt Kaspersky Lab jeden Tag fast 310.000 einzigartige neue Malware-Proben. Zur Verteidigung ihrer Endpoints vor dieser Art von Bedrohung setzen die meisten Unternehmen herkömmliche Schutzmaßnahmen wie Anti-Malware-Lösungen, Intrusion Prevention und Threat Detection ein. In einer sich schnell ändernden Umgebung, in der Cybersicherheit stets versucht, dem Cyberverbrechen einen Schritt voraus zu sein, müssen diese klassischen Lösungen mit auf die Minute aktuellen Bedrohungsinformationen verstärkt werden.

Die machine-readable Threat Intelligence, also die computerlesbaren Informationen zu Bedrohungen, von Kaspersky Lab bietet Data Feeds mit Bedrohungsinformationen sowie Tools zur Integration in weltweit anerkannte SIEM-Plattformen (darunter IBM QRadar, HP ArcSight und Splunk). Diese Kombination ermöglicht Unternehmen einen einzigartigen Einblick in ihre Bedrohungslandschaft und liefert Security Operations Centern Gefährdungsindikatoren, sogenannte Indicators of Compromise, zur schnellstmöglichen Identifizierung und Abwehr einer Vielzahl von Cyberangriffen.

NUTZUNGSSZENARIEN/SERVICEVORTEILE

Data Feeds von Kaspersky Lab:

- Verbessern Sie Ihre SIEM-Lösung durch Daten zu schädlichen URLs aus Feeds von Kaspersky Lab. Das SIEM-System wird anhand von Protokollen, die von den unterschiedlichen Netzwerkgeräten (Benutzer-PCs, Netzwerkproxys, Firewalls, andere Server) an das SIEM-System gesendet werden, über Malware-, Phishing-und Botnet C&C-URLs informiert.
- Versorgen primäre Netzwerksicherheitslösungen wie Firewalls, IPS/IDS, SIEM-Lösungen, Anti-APT, Sandbox-/Simulationsverfahren, UTM-Appliances usw. mit laufend aktualisierten Bedrohungsdaten
- Verbessern Sie Ihre forensischen Fähigkeiten, indem Sie Ihren Sicherheitsteams aussagekräftige Informationen über Bedrohungen und Einblicke in die Strategie von gezielten Angriffen zur Verfügung stellen
- Fördern Sie die Forschung. Informationen über schädliche URLs und MD5-Hashes (SHA1 und SHA256) von schädlichen Dateien sind ein wertvoller Beitrag für die Bedrohungsforschung.

Kaspersky Lab stellt fünf Arten von Data Feeds mit Bedrohungsinformationen bereit:

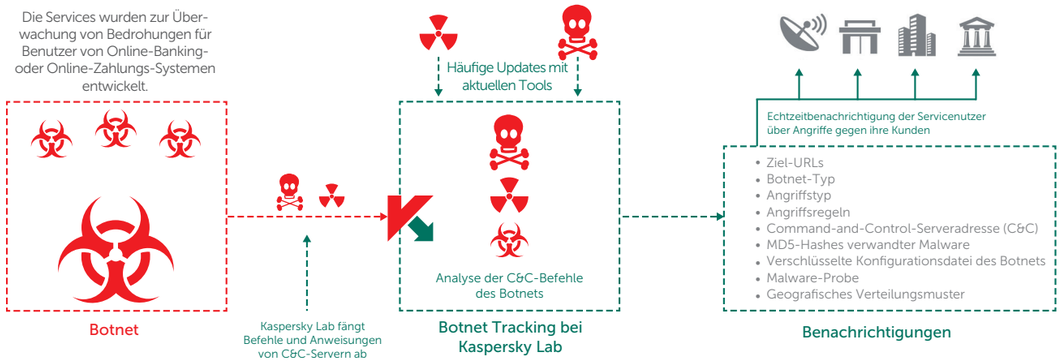
1. Malicious URLs und Masks
2. MD5-Hashes (SHA1 und SHA256) von schädlichen Objektdatenbanken
3. Mobile Threat Feeds
4. MD5-Hashes (SHA1 und SHA256) von legitimen Objektdatenbanken
5. Schädliche IP-Adressen

FEED-BESCHREIBUNG

IP Reputation Feed – Mehrere IP-Adressen einschließlich des Kontexts zu verdächtigen und schädlichen Hosts.
Malicious URLs – Ein Datensatz mit URLs, der die schädlichsten Links und Webseiten beinhaltet. Es stehen maskierte und nicht maskierte Datensätze zur Verfügung.
Phishing URLs – Ein Datensatz mit URLs, die von Kaspersky Lab als Phishing-Webseiten identifiziert wurden. Es stehen maskierte und nicht maskierte Datensätze zur Verfügung.
Botnet C&C URLs – Ein Datensatz von Command-and-Control-Server-URLs (C&C) und verwandten schädlichen Objekten.
Malicious Hash Feeds – einschließlich der gefährlichsten, am weitesten verbreiteten und neu aufkommenden Malware.
Mobile Malware Hashes – Ein Datensatz von Datei-Hashfunktionen zur Erkennung schädlicher Objekte, die mobile Plattformen infizieren.
P-SMS Trojan Feed – Ein Datensatz mit Trojaner-Hashwerten mitsamt dem zugehörigen Kontext für die Erkennung von SMS-Trojanern, die hohe Mobilfunkkosten generieren und es dem Angreifer ermöglichen, SMS-Nachrichten zu entwenden, zu löschen oder auf sie zu antworten.
Mobile Botnet C&C URLs – Ein Datensatz mit URLs, inklusive Kontext zu C&C-Servern für mobile Botnets.
Whitelisting Data Feed – Mehrere Datei-Hashes, die systematisches Wissen zu legitimer Software enthalten.

BOTNET TRACKING

Hochwertige Überwachungs- und Benachrichtigungsservices zur Identifizierung von Botnets, die Ihre Kunden und Ihren Ruf 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 anzugreifenden Unternehmens zugreift, und startet dann den Angriff.
- **Botnet-Typ** – Bestimmen Sie präzise den Malware-Typ, der von Cyberkriminellen eingesetzt wird, um die Transaktionen Ihrer Kunden zu manipulieren. Beispiele: Zeus, SpyEye oder Citadel.
- **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-Hash-Werte der Malware** – Kaspersky Lab stellt Ihnen den zur Malware-Verifizierung verwendeten Hash-Wert zur Verfügung.
- **Verschlüsselte Konfigurationsdatei des Botnets** – Ermittlung der vollständigen Liste der betroffenen URLs.
- **Malware-Probe** – Für weiteres Reverse Engineering und eine digitale forensische Analyse des Botnet-Angriffs.
- **Geografisches Verteilungsmuster (10 Hauptländer)** – Statistische Daten zur weltweiten Verteilung der Malware-Proben.

LEISTUNGEN

Benachrichtigung per E-Mail oder im JSON-Format

- Verschlüsselte Konfigurationsdatei des Botnets
- Zugehörige Malware-Probe (bei Bedarf)
- Geografisches Muster der weltweiten Verteilung der Malware-Proben

Benachrichtigung per E-Mail

- Ziel-URL (Angabe der URL, unter der das Bot-Programm Benutzer angreift)
- Botnet-Typ (z. B. Zeus, SpyEye, Citadel, Kins usw.)
- Angriffstyp
- Angriffsregeln, u. a.: Injektion von Webdaten, URL, Bildschirm, Videoaufzeichnung usw.
- C&C-Adresse
- MD5-Hashes verwandter Malware

INTELLIGENCE REPORTING

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

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

APT Intelligence Reporting

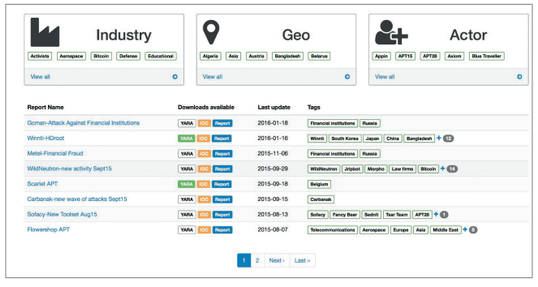
Nicht alle neu entdeckten APTs werden umgehend gemeldet, und viele von ihnen werden nie öffentlich gemacht. Dank unserer umfassenden und praktisch nutzbaren Berichte bleiben Sie stets über APTs auf dem Laufenden.

Als Abonnent des Kaspersky APT Intelligence Reportings haben 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 all jener Bedrohungen, die nie veröffentlicht werden.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie auch über Änderungen in der Taktik von Cyberkriminellen und Cyberterroristen 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.

KASPERSKY LAB 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, Proben und Tools, darunter eine umfangreiche Liste von Gefährdungsindikatoren (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).
- **Nachträgliche Analyse**. Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit.
- **APT Intelligence Portal**. Alle Berichte, einschließlich der aktuellen Gefährdungsindikatoren (IOCs = Indicators of Compromise), können über das APT Intelligence Portal heruntergeladen werden, um unseren Kunden eine nahtlose Benutzererfahrung zu bieten.



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.

TAILORED THREAT REPORTING

Kundenspezifische Berichte zu Bedrohungen

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 ausgewiesen 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 (für kundenspezifische Berichte) und Ihre bevorzugten Datenformate festgelegt haben, ist keine zusätzliche Infrastruktur erforderlich, um mit der Nutzung dieses Kaspersky-Service zu beginnen.

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

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 der Herstellungs-, Transport- und Telekommunikationsbranche 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 von extern verfügbaren, wichtigen IT-Ressourcen des Landes, 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.

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

SO NUTZEN SIE DEN SERVICE FÜR LÄNDERSPEZIFISCHE BERICHTE ZU BEDROHUNGEN

Wenn Sie sich für länderspezifische Berichte zu Bedrohungen von Kaspersky Lab interessieren, wenden Sie sich bitte an den Vertreter von Kaspersky Lab in Ihrer Region, oder schreiben Sie eine E-Mail an intelligence@kaspersky.com. Sie erhalten daraufhin ein Angebot über Berichte zu Bedrohungen für Ihr Land, in dem der gewünschte Leistungsumfang, die Servicebedingungen und die gewünschte Laufzeit aufgeführt sind.

KASPERSKY THREAT LOOKUP

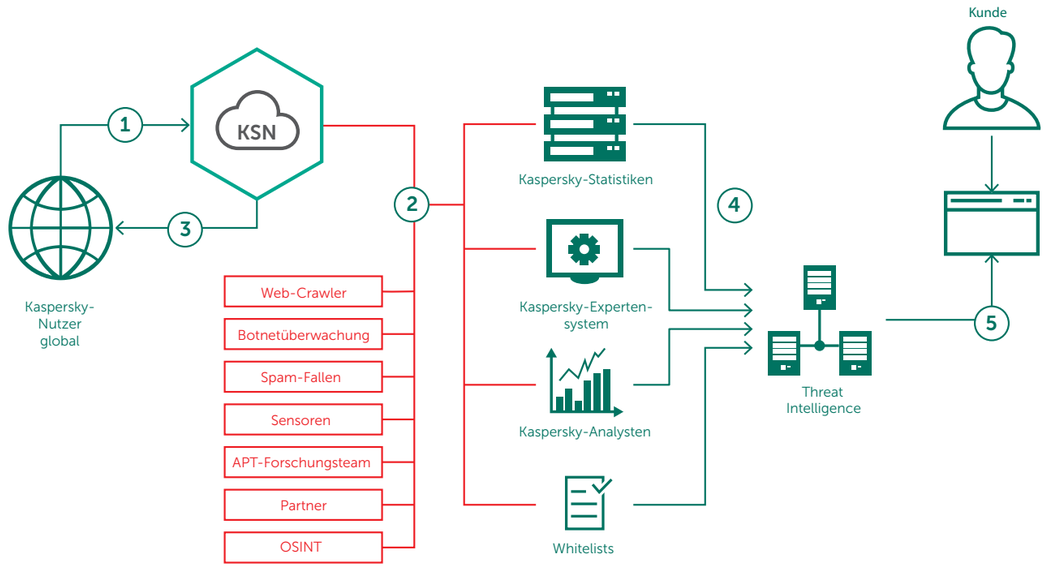
Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt heute kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die Ressourcen aus dem Dark Web für den Angriff auf ihre Ziele einsetzen. Cyberbedrohungen werden immer häufiger, 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 Ihnen unmittelbar verlässliche Informationen über Cyberbedrohungen, legitime Objekte, deren gegenseitigen Abhängigkeiten und Indikatoren sowie praktisch umsetzbare Kontextinformationen, anhand derer sich Ihr Unternehmen und Ihre Kunden über die damit verbundenen Risiken und Folgen ein Bild machen können. Dies ermöglicht eine effektivere Reaktion auf Bedrohungen und die Einleitung von Verteidigungsmaßnahmen noch vor dem Angriff.

Kaspersky Threat Lookup bietet unser gesamtes Wissen über Cyberbedrohungen und ihre Abhängigkeiten 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, Bezeichnungen von Bedrohungen, Statistik- und Verhaltensdaten, WHOIS/DNS-Einträge usw. ab. Hieraus ergibt sich ein umfassender Überblick über neue und aufkommende Bedrohungen, der Ihnen hilft, die Verteidigung und Vorfallsreaktion Ihres Unternehmens zu verbessern.

FUNKTIONEN

- **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 unvergleichliche Zuverlässigkeit unserer Sicherheitsinformationen.
- **Hohe Echtzeitrate:** Unsere Bedrohungsinformationen werden automatisch in Echtzeit generiert, und zwar basierend auf den weltweit von 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. Hierdurch entstehen umfassender Schutz und hohe Genauigkeit.
- **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.
- **Umfassende Daten**: Die Bedrohungsinformationen von Kaspersky Threat Lookup decken eine große Bandbreite unterschiedlicher Datentypen ab, darunter Hash-Werte, URLs, IPs, whois-Einträge, pDNS, GeoIP, Dateiattribute, Statistiken und Verhaltensmuster, Downloadketten, Zeitstempel usw. Dank dieser Informationen erhalten Sie einen Überblick über die Bedrohungslage, mit der Sie konfrontiert sind.
- **Kontinuierliche Verfügbarkeit**: Unsere Bedrohungsinformationen werden durch eine hochgradig fehlertolerante Infrastruktur generiert und überwacht, die eine kontinuierliche Verfügbarkeit und ein gleichbleibendes Leistungsniveau sicherstellt.
- **Kontinuierliche Überprüfung durch Sicherheitsexperten**: Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT-Team und führende Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung von wertvollen und praxisnahen Bedrohungsinformationen bei.
- **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 Gefährdungsindikatoren (IOCs = Indicators of Compromise) oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV, um alle Vorzüge von Bedrohungsinformationen nutzen zu können, betriebliche Workflows zu automatisieren oder eine Integration in bestehenden Sicherheitskontrollen, z. B. SIEMs, zu ermöglichen.



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

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

- **Benutzerfreundliche Web-Oberfläche oder RESTful-API**: Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über eine einfache RESTful-API zugreifen.

HAUPTVORTEILE

- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Fähigkeiten**, 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.

QUELLEN FÜR UNSERE THREAT INTELLIGENCE

Unsere Bedrohungsinformationen (Threat Intelligence) werden aus heterogenen und höchst zuverlässigen Quellen wie dem Kaspersky Security Network (KSN) und unseren eigenen Web-Crawlern, unserem Botnet Monitoring Service (ununterbrochene Überwachung von Botnets sowie ihrer Ziele und Aktivitäten), Spam-Fallen, Forschungsteams, Partnern sowie anhand anderer historischer Daten zusammengestellt, die Kaspersky Lab in den vergangenen zwei Jahrzehnten erfasst hat. Dann werden sämtliche aggregierten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Kaspersky-Expertensysteme (Sandboxes, heuristische Engines, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Analysten und die Verifizierung anhand von Whitelists.

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.

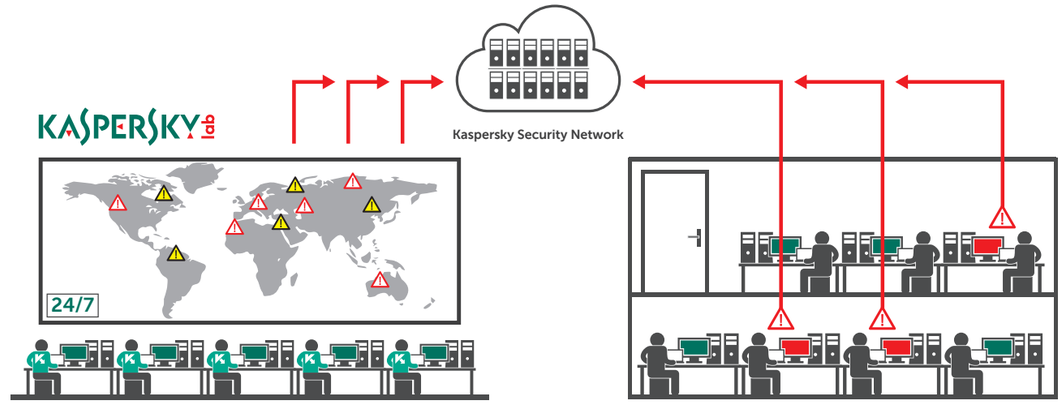
Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl von Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.

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.

KASPERSKY MANAGED PROTECTION

Der Kaspersky Managed Protection-Service bietet Kunden von Kaspersky Security for Business und Kaspersky Anti Targeted Attack Platform eine leistungsstarke Kombination erweiterter technischer Maßnahmen zur Erkennung und Vermeidung gezielter Angriffe. Der Service umfasst die Überwachung durch Kaspersky-Experten rund um die Uhr und die kontinuierliche Analyse von Bedrohungsinformationen (Cyber Threat Intelligence), um die Echtzeiterkennung von bekannten und neuen Kampagnen zur Cyberspionage und Cyberkriminalität zu erkennen, die auf wichtige Informationssysteme abzielen.



SERVICE-HIGHLIGHTS

- Hoher Schutz vor gezielten Angriffen und Malware mit Support durch Kaspersky-Analysten rund um die Uhr
- Erkenntnisse zu Angreifern, ihrer Motivation, ihren Methoden und Tools und dem potentiellen Schaden, den sie anrichten können, zur Entwicklung einer fundierten, effektiven Verteidigungsstrategie
- Erkennung von Nicht-Malware-Angriffen, Angriffen mit bisher unbekannten Hilfsmitteln und Angriffen, die Zero-Day-Schwachstellen ausnutzen
- Rückblickende Analyse von Vorfällen und aufgespürten Bedrohungen
- Senkung der allgemeinen Sicherheitskosten bei gleichzeitiger Verbesserung der Qualität der Schutzmaßnahmen. Dies ist ein Expertenservice eines der weltweit führenden Anbieter von Angriffsanalysen, der auch die Analyse der von den Angreifern eingesetzten Methoden und Technologien umfasst. Es ist sehr viel wirtschaftlicher, diese wertvollen Informationen von einem externen Serviceanbieter zu beziehen, als hochspezialisierte Experten zu beschäftigen.
- Integrierter Ansatz: Unser umfassendes Angebot an integrierten Kaspersky Security for Business-Lösungen hält für jeden Kunden die richtigen Technologien und Services bereit, um eine umfassende Verteidigungsstrategie zum Schutz des Unternehmens vor gezielten Angriffen aufzubauen: Vorbereitung – Erkennung – Untersuchung – Datenanalyse – automatisierter Schutz.

SERVICEVORTEILE

- Schnelle Erkennung von Vorfällen
- Sammlung einer ausreichenden Menge von Informationen zur Einteilung der Vorfälle in Fehlalarme und korrekt erkannte Bedrohungen
- Ermittlung, wie häufig die erfassten Artefakte auftreten, und Bestimmung, wie einzigartig der Angriff ist
- Initiierung der Reaktion auf einen Informationssicherheitsvorfall
- Initiierung notwendiger Updates der Viren-Datenbank zur Verhinderung einer Ausbreitung der Bedrohungen

EXPERT SERVICES

Wie der Name schon sagt, werden die Expertenservices von unseren Inhouse-Experten bei Kaspersky Lab bereitgestellt. Viele von ihnen sind internationale Autoritäten auf ihrem Gebiet, deren Fachwissen und Erfahrung von fundamentaler Bedeutung für unsere weltweit führende Stellung auf dem Gebiet der Security Intelligence sind.

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.

Zu den Expertenservices gehören:

- Penetrationstests
- Application Security Assessment
- ATM/POS Security Assessment
- Telecommunication Networks Security Assessment

PENETRATIONSTESTS

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

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.

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).

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.

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 wie zu umfangreiche 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.

ÜBER UNSERE VORGEHENSWEISE 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 Profis 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 erledigt werden. Einige Services (z. B. WLAN-Sicherheitsassessments) 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 der Grundlage unserer Empfehlungen lassen sich die in den Programmen entdeckten Schwachstellen beheben und die entsprechenden Angriffe 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 das Programm 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

ERGEBNISSE

Zu den durch die Assessmentservices 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 Angriffen 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.

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

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 Ihrer ATM-/POS-Infrastruktur 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 und Maßnahmen zur Verbesserung Ihrer 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 Geräteverbund erfolgen. Sie sollten für das Assessment entweder den Geldautomaten-/Kassensystemtyp verwenden, 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.

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)
  - Datensicherheitsstandard
  - 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).

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.

TELECOMMUNICATION NETWORKS SECURITY ASSESSMENT SERVICES

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, Selfservice-Portale für Kunden usw.)
- VoIP Security Assessment
- Telecommunication Equipment Security Assessment Services

SERVICEERGEBNISSE

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, Änderung des Quellcodes oder Implementierung kompensierender Kontrollen, wenn die Schwachstelle nicht entfernt werden kann

INCIDENT DETECTION UND 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 ein Opfer werden.

Die Incident Detection und Response Services sind darauf ausgelegt, herauszufinden, ob Sie derzeit angegriffen werden und warum. Außerdem spüren sie mögliche Angriffsquellen auf, um einen Aktionsplan zur Abwehr aufzustellen und Ihnen zu helfen, ähnliche Angriffe in der Zukunft zu vermeiden.

Gemeinsam mit den Experten von Kaspersky Lab lösen Sie Sicherheitsprobleme und erlangen ein Verständnis für das Verhalten von Malware und die entsprechenden Folgen. Ferner erhalten Sie Unterstützung bei der Beseitigung:

- **Erkennung gezielter Angriffe**
- **Vorfallsreaktion**
- **Malware-Analyse**
- **Digitale Forensik**

Targeted Attack Discovery

Wenn Sie befürchten, dass Angriffe auf Ihre Branche abzielen, und Ihnen verdächtiges Verhalten in Ihren eigenen Systemen auffällt, oder wenn Ihr Unternehmen einfach die Vorteile einer regelmäßigen vorbeugenden Inspektion erkennt, 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 potentiell 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

Tiefgreifende Analyse von erfassten Daten mit Bedrohungsinformationen und der gefundenen Gefährdungsindikatoren (IOCs = Indicators of Compromise)

Genaue Beschreibung der ausgenutzten Schwachstellen, möglicher Angriffsziele und der betroffenen Netzwerkkomponenten.

Empfehlung von Abhilfemaßnahmen: mögliche Schritte zur Verringerung der Folgen des aufgedeckten Vorfalls und Schutz Ihrer Ressourcen vor ähnlichen Angriffen in der Zukunft.

DER SERVICE IM DETAIL

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

Sammlung und Analyse von Bedrohungsinformationen. Das Ziel ist, eine Momentaufnahme Ihrer Angriffsfläche zu erstellen. Dabei werden die Bedrohungen durch Cyberkriminalität und Cyberspionage sowie Angriffe ermittelt, die Ihre Ressourcen aktiv oder potentiell schädigen. Zu diesem Zweck tauchen wir in interne und externe Informationsquellen ein, darunter Untergrund-Communitys 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 Labors kommen Experten von Kaspersky Lab vor Ort, um Netzwerk- und Systemartefakte sowie verfügbare SIEM-Informationen zu erfassen. Wir führen ggf. auch ein Vulnerablility 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.

WEITERE DIENSTLEISTUNGEN

Unsere Experten unterstützen Sie auch dabei, die Symptome eines Vorfalls zu analysieren, tiefgreifende digitale Analysen für bestimmte Systemen durchzuführen, eine Malware-Binärdatei 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 stellen wir zudem die **Kaspersky Anti Targeted Attack (KATA) Platform** in Ihrem Netzwerk bereit, und zwar dauerhaft oder zu Beweiszwecken. 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.

Vorfallsreaktion (Incident Response)

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.

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 Vorfallsreaktionsteam 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 eine Malware-Analyse oder digitale Forensik durchzuführen.

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*: Der Bericht schlägt Schritte zur vollständigen Sicherung Ihres Unternehmens vor dieser Bedrohung vor.

DIGITALE FORENSIK

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 Vorfallsreaktionsservices 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.

ANMERKUNGEN

ANMERKUNGEN


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab GmbH,
Ingolstadt, Deutschland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.securelist.com

Informationen zu Partnern in
Ihrer Nähe finden Sie hier:
www.kaspersky.de/buyoffline

Wenn Sie mehr über die hier vorgestellten Produkte oder Services erfahren oder mit uns darüber sprechen möchten, wie sich die Services für die Sicherheit Ihres Unternehmens einsetzen lassen, wenden Sie sich per E-Mail unter intelligence@kaspersky.com an uns.

Beachten Sie bitte, dass die allgemeinen Geschäftsbedingungen je nach Gebiet unterschiedlich ausfallen können. Dies betrifft insbesondere den Leistungsumfang, Fristen, die Verfügbarkeit von Vor-Ort-Services, die Sprache, in der die Leistung erbracht wird, und die Kosten.

Katalog für Security Intelligence Services, August 2017 GL

KASPERSKY lab