Die Lösung für Ihre aktuellen und zukünftigen IT-Sicherheitsanforderungen

Ein stufenweises Cybersicherheitskonzept

kaspersky

Der Aufbau einer Sicherheitsgrundlage für Ihr Unternehmen durch die Auswahl des richtigen Produkts oder Services ist der erste Schritt. Der Schlüssel für den langfristigen Erfolg liegt aber in der Entwicklung einer zukunftsorientierten Cybersicherheitsstrategie.

Das Enterprise Portfolio von Kaspersky ist auf die Sicherheitsanforderungen heutiger Unternehmen abgestimmt und bietet Organisationen mit unterschiedlichem technischen Reifegrad einen stufenweisen Ansatz. Dieser Ansatz umfasst unterschiedliche Schutzebenen von allen Arten von Cyberbedrohungen. Selbst äußerst komplexe Angriffe werden erkannt, die Reaktion auf Vorfälle erfolgt schnell und angemessen und zukünftige Bedrohungen können verhindert werden.

Expertise zur Abwehr unterschiedlicher Bedrohungsarten

Da IT-Umgebungen an Größe und Komplexität zunehmen, sehen sich Unternehmen mit immer raffinierter werdenden Bedrohungen konfrontiert, die Sie dazu veranlassen, ihr Cybersicherheits-Know-how ständig weiterzuentwickeln, um einen effektiven Schutz zu gewährleisten.

Unsere Erfahrung und kontinuierliche Bedrohungsanalyse ermöglicht es uns, alle verfügbaren Bedrohungen in Kategorien zu unterteilen. Der Großteil der Bedrohungen befindet sich im unteren Teil der Pyramide. Es handelt sich um generische Bedrohungen, die lediglich einen grundlegenden Abwehrmechanismus sowie eine vorhandene IT-Sicherheitspraktik erfordern. Wenn man in der Pyramide weiter nach oben geht, stößt man auf fortschrittlichere Bedrohungen, die den Präventivschutz umgehen, indem sie bekannte Taktiken, Techniken und Vorgehensweisen (TTPs) verwenden. Bedrohungsakteure in dieser Kategorie könnten sich zum Beispiel raffinierte Tools, die ihre besser ausgestatteten „Kollegen“ entwickelt haben, aneignen und diese weiterverwenden. Die meisten Sicherheitsverletzungen fallen in diese Kategorie. Und zu guter Letzt befinden sich ganz oben in der Pyramide Advanced Persistent Threats (APTs) und Angriffe, die unbekannte TTPs nutzen. Bedrohungsakteure auf dieser Ebene verfügen über unbegrenzte Ressourcen für die Entwicklung raffinierter Tools und Methoden, die ausgesuchte Ziele ins Visier nehmen.

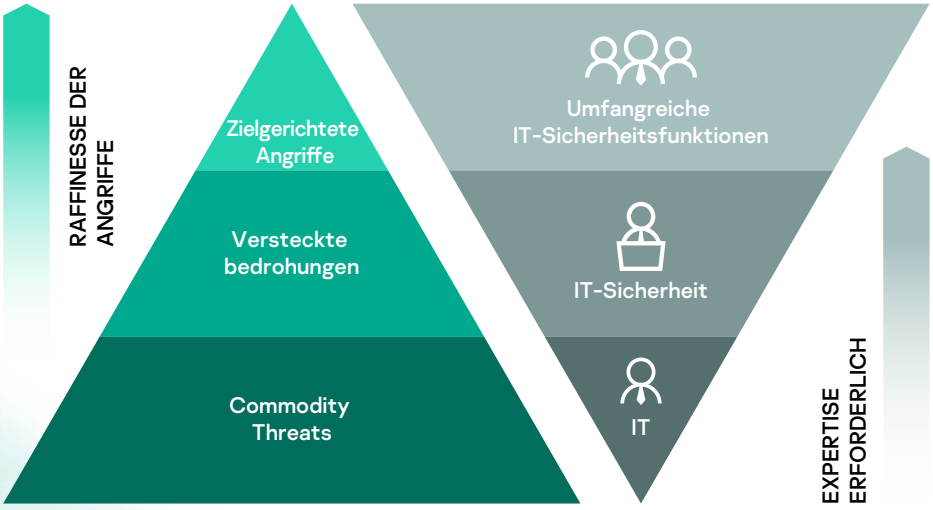


Abbildung 1. Expertise zur Abwehr unterschiedlicher Bedrohungsarten

Um ein erfolgreiches Geschäftswachstum voranzutreiben und die Wettbewerbsfähigkeit zu sichern, verlassen sich Unternehmen zunehmend auf Informationstechnologien. Der fortschreitende digitale Wandel vergrößert die potentielle Angriffsoberfläche, da die Systeme stark miteinander verbunden sind. Da IT-Umgebungen an Größe und Komplexität zunehmen, sehen sich Unternehmen mit immer raffinierter werdenden Bedrohungen konfrontiert, die sie dazu veranlassen, ihr Cybersicherheits-Know-how ständig weiterzuentwickeln, um einen effektiven Schutz zu gewährleisten.

Ein stufenweises Cybersicherheitskonzept

In Abstimmung mit den Bedrohungen und den Abweichungen hinsichtlich der Cybersicherheitskapazitäten unserer Kunden, haben wir eine Markteinführungsstrategie für unsere Produkte und Services umgesetzt, mit der Unternehmen automatisch 90 % der Bedrohungen verhindern können – und mit der sie dann systematisch und methodisch neue und fortschrittliche Kapazitäten hinzufügen können, um die raffinierten Bedrohungen, mit denen sie sich im Laufe der Weiterentwicklung ihres Geschäfts konfrontiert sehen, abzuwenden.

Unter Berücksichtigung der steigenden Anzahl und Komplexität der Bedrohungen, des Reifegrads der IT-Sicherheit, der Cybersicherheitskapazitäten sowie der vorhandenen Budgets, kristallisiert sich eine deutliche Notwendigkeit für den Aufbau einer umfassenden und anpassungsfähigen Sicherheitsstrategie heraus.

In Stufe 1 bieten wir all unsere führenden Präventivprodukte zusammen mit Premium-Support und professionellen Services an, um zu gewährleisten, dass die Kunden die maximalen Vorteile unserer Technologien ausschöpfen können. In Stufe 2 – weiter oben in der Pyramide – besteht eine zunehmende Notwendigkeit, den Bedrohungen zu begegnen, die die vorhandenen Präventivmechanismen umgehen. Um einen ressourcenschonenden Schutz vor fortschrittlichen und versteckten Bedrohungen zu unterstützen, bieten wir eine Cloud-fähige Lösung an, die die kundeneigenen, grundlegenden Cybersicherheitskapazitäten mit Managed Detection, Priorisierung und Anleitung zur Abwehr ergänzt. Abgerundet wird diese Lösung durch ein automatisiertes Toolkit, das den Sicherheitsexperten bei der effizienteren Ermittlung und Analyse sowie Reaktion auf die gefährlicheren, versteckten Bedrohungen hilft. Unternehmen in Stufe 3 haben eine größere Wahrscheinlichkeit einer tatsächlichen APT ausgesetzt zu sein und benötigen effektivere Abwehrmechanismen gegen unbekannte TTPs. Um die Anforderungen erfahrener IT-Sicherheitsteams zu erfüllen, bietet Kaspersky eine innovative und ausgewogene Kombination an Technologien und Services an, die die Herausforderungen der raffiniertesten Bedrohungen und zielgerichteten Angriffe von heute bewältigt.

Kaspersky Managed Detection and Response kann sofort als reife IT-Sicherheitseinrichtung bereitgestellt werden, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss. Gleichzeitig ermöglicht es die Auslagerung der Auswahlprozesse für Vorfälle an Kaspersky, damit erfahrene IT-Sicherheitsteams sich auf die Lösung der vorgelegten kritischen Fälle konzentrieren können.

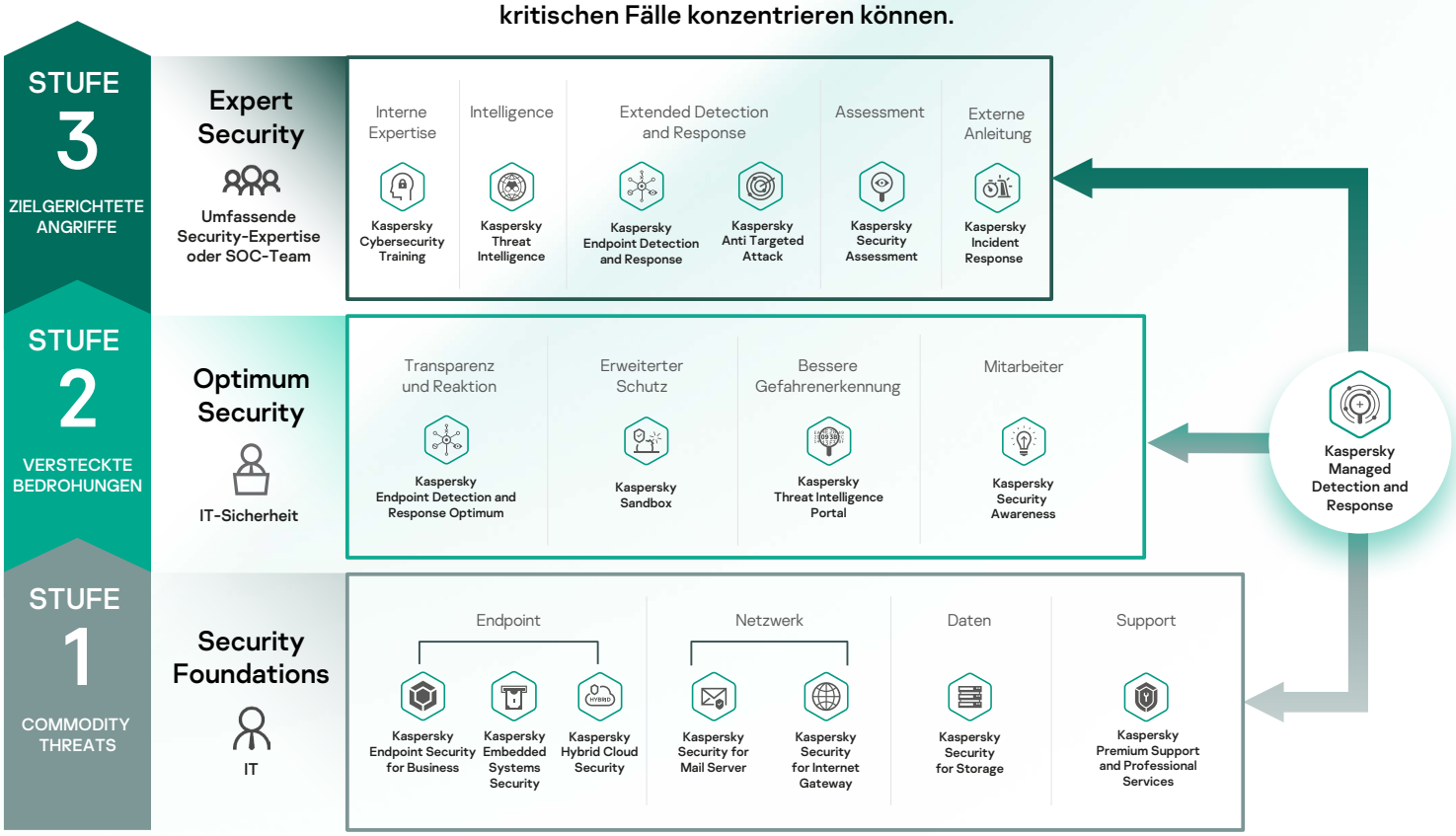


Abbildung 2. Ein stufenweises Cybersicherheitskonzept

Security Foundations

Automatisches Blockieren der maximal möglichen Anzahl von Bedrohungen

Security Foundations ist eine grundlegende Stufe für Unternehmen aller Größen und Infrastruktur-Komplexität zum Aufbau einer integrierten Strategie zum Schutz vor komplexen Bedrohungen. Es bietet eine automatische Multi-Vektor-Prävention einer großen Anzahl möglicher Vorfälle aufgrund von Commodity Threats. Diese Stufe ist für gewöhnlich ausreichend für kleinere Unternehmen mit IT-Teams.

Unternehmen können diese Stufe nicht überspringen und direkt zur Implementierung fortschrittlicher Schutz- und Reaktionstechnologien übergehen. Denn bei einem Großteil dieser Technologien ist ein menschlicher Eingriff nötig, der natürlich teuer ist und entsprechendes Fachwissen erfordert. So werden teure IT-Sicherheitsexperten mit Warnmeldungen überhäuft, ohne dass die meisten Bedrohungen überhaupt verhindert werden. Und statt proaktives Hunting nach verborgenen Bedrohungen zu betreiben und Vorfälle zu lösen, verschwenden die IT-Sicherheitsexperten Zeit damit, tausende Warnmeldungen zu sortieren und diese zu priorisieren, wodurch die meisten unbeachtet bleiben.

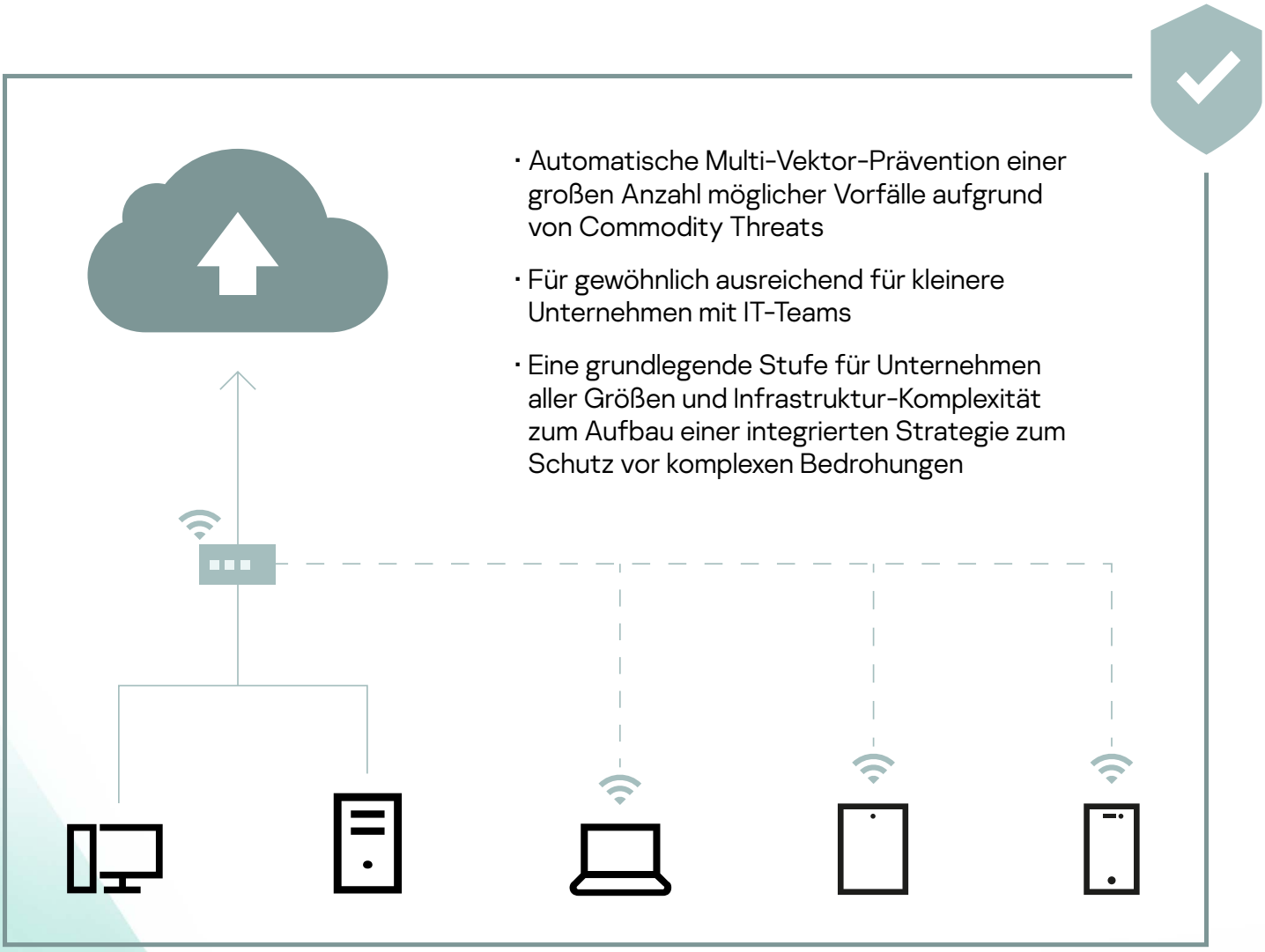


Abbildung 3. Die wichtigsten Eigenschaften von Stufe 1

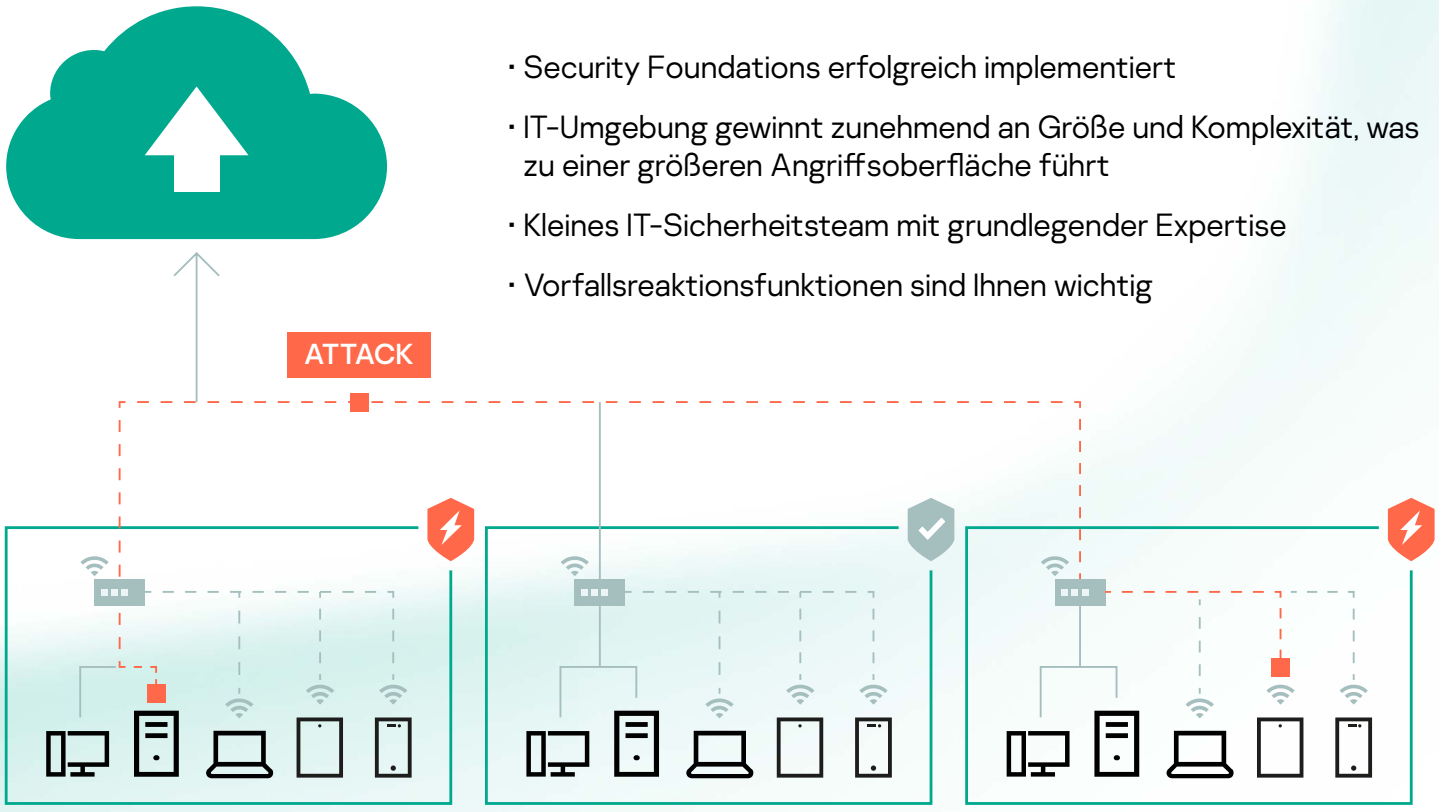
Optimum Security

Schwerpunkt auf erweiterter Erkennung und schneller Reaktion auf nicht durch Präventivschutz erkannte Bedrohungen.

Mit der zunehmenden Größe und Komplexität von IT-Umgebungen, die die Geschäftsentwicklung und das Wachstum unterstützen, vergrößern Unternehmen auch ihre potentielle Angriffsfläche. Sie werden zu attraktiveren Zielen für Cyberkriminelle und sind einem höheren Risiko für hochentwickelte Bedrohungen ausgesetzt, die die automatischen Präventivmechanismen umgehen.

Da die potenzielle Angriffsfläche immer größer wird, darf die Bedeutung der Implementierung zumindest grundlegender Verfahren zur Reaktion auf Vorfälle nicht unterschätzt werden. Diese Unternehmen beginnen für gewöhnlich mit der Entwicklung einer noch wenig ausgereiften IT-Sicherheitsfunktion in ihrer IT-Abteilung. Kleine IT-Sicherheitsteams benötigen Instrumente für die automatische Erkennung fortschrittlicher Bedrohungen und eine zentralisierte Reaktion als Grundlage für eine weitere Reifung ihrer Funktion. Mitarbeiterschulungen sind unerlässlich, um das Sicherheitsbewusstsein im ganzen Unternehmen zu erhöhen und alle Mitarbeiter zu motivieren, auch dann auf Cyberbedrohungen und die jeweiligen Abwehrmaßnahmen zu achten, wenn sie dies nicht als Teil ihrer eigentlichen Aufgaben sehen.

Aufbauend auf Security Foundations ermöglicht es Optimum Security Unternehmen mit IT-Umgebungen, die an Größe und Komplexität zunehmen, Commodity Threats und Bedrohungen, die die bestehenden Präventivmechanismen umgehen, abzuwenden. Eine ressourcenschonende Lösung ist ideal für kleine IT-Sicherheitsteams mit grundlegender Expertise. In dieser Stufe können Kunden ihre eigenen Erkennungs- und Reaktionskapazitäten optimieren, während Sie rund um die Uhr von Managed Protection profitieren. Gleichzeitig hilft ein Portfolio an computerbasierten, spielerischen Schulungsprodukten dabei das Sicherheitsbewusstsein der Mitarbeiter zu schärfen und sie zu motivieren, sichere Praktiken anzuwenden.



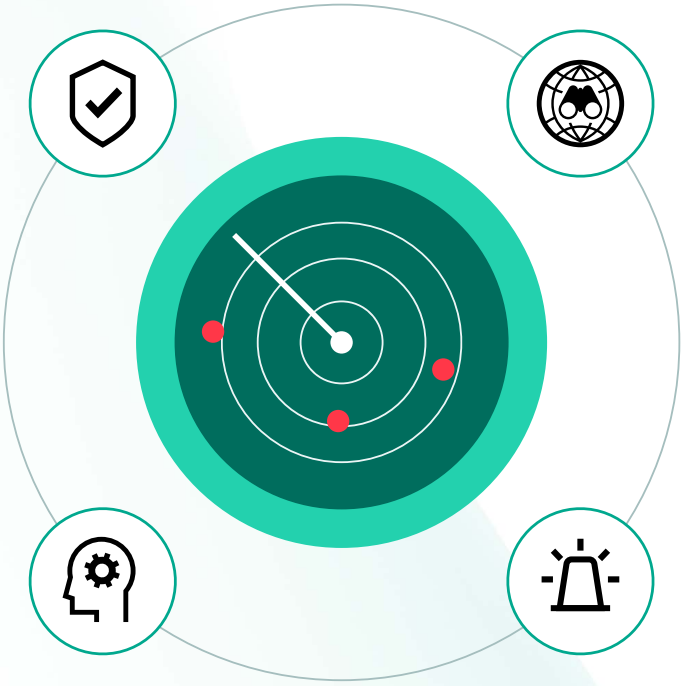
- Security Foundations erfolgreich implementiert
- IT-Umgebung gewinnt zunehmend an Größe und Komplexität, was zu einer größeren Angriffsoberfläche führt
- Kleines IT-Sicherheitsteam mit grundlegender Expertise
- Vorfallsreaktionsfunktionen sind Ihnen wichtig

Abbildung 4. Die wichtigsten Eigenschaften von Stufe 2

Vorbereitung auf komplexe, APT-ähnliche Angriffe.

Expert Security

Die Einführung manueller Thread Hunting-Praktiken und fortschrittlicher Anwendungsfälle für die Bedrohungsanalyse und das zeitgleiche Vorhandensein eines vollständig ausgerüsteten Teams mit tiefgreifender Expertise in bestimmten Themengebieten, wie digitale Forensik und Malware-Analyse, wird in Stufe 3 für Unternehmen von unternehmenskritischer Bedeutung sein. Durch die schnelle bedarfsgerechte Ergänzung ihrer vorhanden Kapazitäten mit spezifischen Kompetenzen werden sie vom Aufbau vertrauenswürdiger Beziehungen mit einem hochqualifizierten Partner profitieren. Kaspersky Expert Security bietet eine erweiterte Extended Detection and Response-Plattform gepaart mit nie da gewesener Unterstützung durch Experten, Assessment, Bedrohungsanalyse und Kompetenzschulungen. Zusammen werden so die durchgängigen Sicherheitsanforderungen jedes Unternehmens mit einer ausgereiften IT-Sicherheitsfunktion erfüllt, um die komplexen Bedrohungen, APT-ähnlichen und zielgerichteten Angriffe abzuwenden.



- IT-Umgebungen werden immer komplexer und verteilter
- IT-Sicherheitsteam ist erfahren oder ein Security Operations Center wurde eingerichtet
- abnehmende Risikobereitschaft wegen höherer zu erwartender Kosten durch Sicherheitsvorfälle und Datenschutzverletzungen,
- Sorge um Einhaltung gesetzlicher Vorschriften.

Abbildung 5. Die wichtigsten Eigenschaften von Stufe 3

Warum Kaspersky?

Wir möchten eine sicherere Welt schaffen, in der Technologien uns das Leben erleichtern. Wir glauben an eine Zukunft, in der Technologie unser Leben verbessert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen Möglichkeiten, die sie mit sich bringen, nutzen können.

Wir sind ein globales Unternehmen mit einem globalen Ansatz und konzentrieren uns auf internationale Märkte. Wir sind in 200 Ländern und Gebieten tätig und betreiben 34 Niederlassungen in mehr als 30 Ländern. Unser Team besteht aus mehr als 4.000 hochqualifizierten Fachkräften.

Innovationen sind die Antriebskraft hinter unserem Anspruch, stets effektiven, praktisch umsetzbaren und leicht zugänglichen Schutz zu bieten. Mit umfassender Threat Intelligence und fundierter Sicherheitsexpertise entwickeln wir innovative Sicherheitslösungen und -services zum Schutz von Unternehmen, kritischen Infrastrukturen, Regierungen und Verbrauchern auf der ganzen Welt. Unser umfassendes Sicherheitsportfolio beinhaltet führende Schutz-, Erkennungs- und Sicherheitslösungen sowie -services zur Verteidigung vor raffinierten und immer neuen Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 250.000 Unternehmenskunden werden von den Technologien von Kaspersky geschützt.

www.kaspersky.de