Integrierte Lösung für Endpoint Security

Aufbau einer zuverlässigen Abwehr bei eingeschränkten Ressourcen

kaspersky

Weitere Informationen finden Sie unter kaspersky.de
#bringonthefuture

Einleitung

Unabhängig von Größe, Standort oder Branche ist den meisten Organisationen mittlerweile bewusst, dass in Bezug auf Cyberangriffe die Frage nicht lautet, ob man davon betroffen sein wird, sondern wann. Keiner sollte sich davon ausnehmen.

Aber ob man über die Zeit, die Ressourcen oder (offen gesagt) die Motivation verfügt, um mit der aktuellen Bedrohung und der Sicherheitslandschaft effektiv umzugehen – das steht auf einem ganz anderen Blatt.

Die meisten IT-Sicherheitsanalysten – und es gibt bei Weitem nicht genug von ihnen, um überall präsent zu sein – sind ohnehin schon überarbeitet. Geräte für neue Mitarbeiter einrichten, neue Gesetze und Compliance-Themen studieren, sich über die neuesten Bedrohungen auf dem Laufenden halten – all das will erledigt sein, bevor man sich der eigentlichen Aufgabe widmen kann: dem Schutz des Unternehmens.

Wenn überhaupt, dann genießen nur sehr wenige Sicherheitsexperten den Luxus, sich ununterbrochen mit neuen und exotischen Bedrohungen befassen und darauf reagieren zu können.

Und genau hier kommen die Anbieter von Cybersicherheit mit ihren Produkten und Lösungen ins Spiel. Unsere Aufgabe besteht darin, Ihre Infrastruktur vollständig abzusichern und Ihre Nutzer zu schützen. Gleichzeitig sollte der Aufwand, insbesondere an Ressourcen wie Zeit und Geld, aber auch an teurem und schwer zu erwerbendem Know-how, so gering wie möglich gehalten werden.

Herausforderungen

Sehen wir uns zunächst einmal die Probleme näher an, denen sich die IT und IT-Sicherheitsmanager von heute stellen müssen.

Erhöhte Gefahr eines hochentwickelten oder zielgerichteten Angriffs

Zielgerichtete Angriffe und komplexe Bedrohungen sind ein großes Problem und nehmen ständig zu. Die Tools der Cyberkriminellen sind mittlerweile so günstig und leicht zu haben, dass heutzutage praktisch jeder mit einem Computer einen ausgefeilten Angriff starten kann. Was bedeutet, dass Organisationen, die bislang annehmen konnten, dass sie nicht zur Zielgruppe solch hochentwickelter Bedrohungen gehören, auf schmerzvolle Weise erfahren müssen, dass sich die Dinge geändert haben.

Nichtsdestotrotz bleiben auch Commodity-Bedrohungen ein Problem, schon allein durch die Häufigkeit ihres Auftretens.

Die überwältigende Mehrheit der Cyberbedrohungen verschafft sich entweder über Endpoints Einlass oder sind so programmiert, dass sie einen Angriff von dort auslösen (oder beides).

Daher besteht eine der besten Möglichkeiten, seine Assets zu schützen, im Endpoint-Schutz.

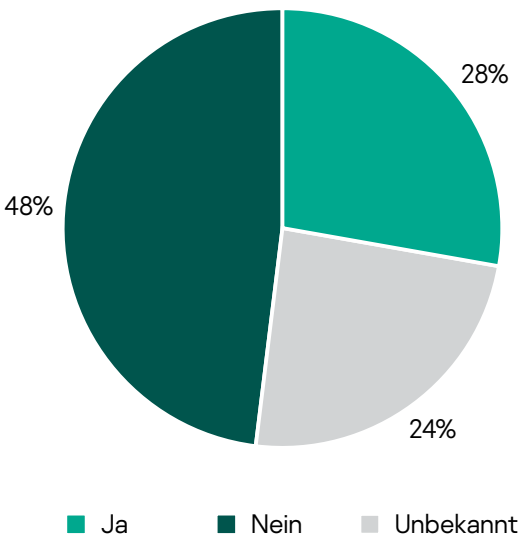
Laut einer Studie des SANS-Instituts[2] sind Hacker bei 28 % der befragten Organisationen über die Endpoints eingedrungen, 24 % wissen nicht, ob es zu einem Sicherheitsvorfall gekommen ist.

91 %[1] der Unternehmen sind innerhalb von 12 Monaten mindestens ein Mal einem Angriff zum Opfer gefallen.

1 von 10[1] Organisationen waren über denselben Zeitraum einem zielgerichteten Angriff ausgesetzt (oder sind sich zumindest dessen bewusst).

30 %[1] der Organisationen haben noch immer keinen umfassenden Malware-Schutz implementiert

Störungsraten bei Endpoints



1 Kaspersky-Bericht zu globalen IT-Risiken, Kaspersky, 2019

2 2019 SANS-Erhebung zu Next-Generation Endpoint Risks and Protections, The SANS Institute, 2019

3 Studie zu Mitarbeitern in der Cybersicherheit, (ISC)² 2019,

4 Official Annual Cybersecurity Jobs Report, Cybersecurity Ventures, 2019

Der menschliche Faktor

Unglücklicherweise ist die verletzlichste Komponente in der Infrastruktur einer Organisation mit den meisten unserer Endpoints verbunden: die Nutzer. Sie greifen regelmäßig auf Unternehmensdaten zu, sei es remote oder über private Endgeräte. Viele von ihnen sind mit dem Internet groß geworden und haben im Laufe der Zeit schlechte Angewohnheiten und ein übermäßiges Selbstvertrauen entwickelt. Und auch sie müssen, wie alles andere auch, abgesichert werden.

So gehört auch das Erkennen und Verhindern von unsicherem Verhalten in den heutigen komplexen IT-Umgebungen zu den Aufgaben der stark beanspruchten Sicherheitsfachleute.

Und auch IT-Fachleute können Fehler machen – schließlich sind wir alle nur Menschen – wenn es zum Beispiel aufgrund unregelmäßig installierter Sicherheitspatches zu Angriffen über Schwachstellen an Dienst- oder Privatgeräten kommt.

(Fehlende) Ressourcen

In 2 von 3[3] Organisationen besteht ein Mangel an qualifizierten Mitarbeitern im Bereich der Informationssicherheit.

Man geht davon aus, dass bis 2021 **3,5 Millionen**[4] Arbeitsplätze in der Cybersicherheit nicht besetzt werden können.

Die IT-Spezialisten haben also offensichtlich viel zu tun.

Selbst in kleinen Organisationen gibt es eine ständig steigende Zahl an Sicherheitsvorfällen, die täglich analysiert und behoben werden müssen, was nur schwerlich effizient und zeitnah geschehen kann. Cyberkriminelle wissen, dass Unternehmen damit ein Problem haben und nutzen diesen Umstand schamlos aus.

Und selbst für die Glücklichen, die über ein solides Finanzpolster verfügen, besteht ein weltweiter Mangel an Cybersicherheitsexperten. Dieses Problem ist nicht neu, und wenn man sich die Ausbildungszahlen in diesem Bereich ansieht, dann wird sich daran auch so bald nichts ändern.

Sicherheitsexperten unter diesen Umständen bei Laune und bei der Stange, d. h. im Unternehmen zu halten, ist eine echte Herausforderung. Burnout ist ein großes Thema, vor allem wenn sich Ihr hoch qualifiziertes und für teures Geld geschultes Team den ganzen Tag an einem Berg von Banalitäten abarbeitet.

Und dann ist da natürlich noch das Problem mit den finanziellen Ressourcen. Und mit der Prozessorleistung. Und was man sonst noch so braucht, um optimale Sicherheit zu gewährleisten, ohne Verarbeitungsgeschwindigkeiten, Mitarbeiterproduktivität, Nutzerzufriedenheit und Budgets zu beeinträchtigen.

Die Lösung

Wie lautet also die Antwort?

Effektiver Schutz

Zuallererst hängt alles von einem **effektiven Endpoint-Schutz** und einer starken EEP (Endpoint Protection Platform) ab – so einfach ist das. Bedrohungen auf Endpoint-Ebene abzuwenden, bevor sie Warnmeldungen auslösen, entlastet die Ressourcen, mindert das Risiko eines erfolgreichen Angriffs und sorgt für einen reibungslosen und sicheren Geschäftsbetrieb. Das gilt sowohl für Commodity-Angriffe, die die meiste Zeit verschlingen, als auch für komplexere und sogar zielgerichtete Angriffe, die sehr wahrscheinlich erfolgreich verlaufen und den größten Schaden anrichten.

Der von uns empfohlene Ansatz sieht eine Kombination aus **mehrschichtigem Endpoint-Schutz** vor – ein starker Basisschutz gegen Commodity-Bedrohungen, sowie eine Reihe von vielschichtigen Abwehrmechanismen gegen die neuesten, komplexeren Bedrohungen.

Darüber hinaus darf man nicht vergessen, dass einige Bedrohungen speziell darauf ausgelegt sind, EPPs zu umgehen, und für diese braucht man andere Erkennungsmethoden, wie die **automatisierte Sandbox**.

Die nächste wichtige Sicherheitsschicht ist EDR (Endpoint Detection and Response). EPP bietet erste Identifizierungs- und Schutzfunktionen, währen EDR für Sichtbarkeit und weiterführende Analysen sorgt, damit Sie sehen können, wo ein Angriff begonnen hat und in welchem Stadium er sich jetzt befindet. Neben der Erkennung umfasst EDR auch mehrere Abwehroptionen, damit die erkannte Bedrohung schnell und effizient eingedämmt werden kann.

EDR kann seine Wirkung aber nur zusammen mit einem starken Basisschutz entfalten. Je mehr Vorfälle gleich zu Beginn von der EPP-Lösung abgefangen werden, desto mehr Kapazitäten bleiben der EDR-Lösung, um sich auf die wenigen verbleibenden Fälle zu konzentrieren.

Menschliches Verhalten

Aus Sicht der Nutzer lässt sich der menschliche Faktor am besten dadurch ausschalten, dass man mithilfe von **Programm-, Internet- und Gerätekontrollen** dem Menschen gar nicht erst die Gelegenheit bietet, Fehler zu machen. Effektive Kontrollen wirken dabei keineswegs als Beschränkung für die Geschäftstätigkeit, sondern können die Produktivität sogar noch steigern, indem Zeit fressende und potentiell gefährliche Unterhaltungsseiten im Internet und den sozialen Medien blockiert werden.

Aber auch hier kommt es entscheidend darauf an, die Nutzer aufzuklären. Die richtige **Schulung zum Thema Cybersicherheit** kann sich wesentlich auf das Mitarbeiterverhalten auswirken, eine neue Unternehmenskultur schaffen und die Risiken für den Betrieb deutlich eindämmen. Und letztendlich kann sich auch die Arbeitslast für die IT-Abteilung spürbar verringern.

Rendite für Ihre Investition

Schlussendlich muss jeder Ansatz in Bezug auf die Kapitalrendite finanziell tragfähig sein, sowohl heute als auch in der Zukunft, in Umgebungen mit begrenzten Ressourcen, zu denen auch begrenztes Expertenwissen zählen könnte.

Automatisierung und Verschlankung

Angesichts der rasant steigenden Anzahl der Bedrohungen und dem Mangel an Sicherheitsexperten, die sie bearbeiten könnten, nimmt die **Automatisierung von Sicherheitstasks** einen immer höheren Stellenwert ein. Damit gewinnen Ihre Sicherheitsexperten wertvolle Zeit, in der sie ihre Fähigkeit im Umgang mit den Vorfällen einsetzen können, für die menschlicher Eingriff und Fachwissen unabdingbar sind (was sie gleichzeitig zufriedener und motivierter macht).

Mit der Automatisierung von Aufgaben lässt sich auch der menschliche Faktor ausschalten, indem beispielsweise Sicherheitsupdates automatisch priorisiert und implementiert werden, was wesentlich effektiver ist, als darauf zu hoffen, dass ein Mitarbeiter die Zeit findet, diese kritische, aber wenig erfüllende Aufgabe zu erledigen.

Vereinfachte Bereitstellung und eine zentralisierte, schlanke **Verwaltungskonsole** sparen ebenfalls Zeit und Ressourcen. Zwischen Konsolen hin- und herzuschalten und nach den jeweils passenden Befehlen zu suchen, ist nicht nur zeitaufwändig und frustrierend, sondern birgt die Gefahr von Fehlern und Versäumnissen.

Hinweis zum mehrstufigen Schutz

Wie bereits ausgeführt, muss jede Lösung, die vor allen möglichen Cyberbedrohungen einschließlich hochentwickelten und zielgerichteten Angriffen schützen soll, aus mehreren Stufen bestehen.

Die Lösung muss in erster Linie einen **robusten Endpoint-Basisschutz** einschließlich Endpoint-Kontrollen (mit Funktionen zur Internet-, Programm- und Geräteblockierung und -beschränkung) sowie eine starke Anti-Malware-Engine enthalten. Außerdem sollten vorzugsweise ein automatisiertes Patch Management und Funktionen für das Vulnerability Assessment vorhanden sein, um IT-Mitarbeitern die Zeit und den Aufwand für derartige Routinearbeiten zu ersparen.

Aber aus hochentwickelter Malware ergeben sich noch zusätzliche Herausforderungen, für die weitere Sicherheitsstufen erforderlich sind. Die Malware könnte speziell dafür konzipiert sein, selbst ausgefeilte Endpoint-Schutzmechanismen zu umgehen, indem sie als Schläfer im Verborgenen wartet, bis sich eine geeignete Gelegenheit ergibt. Als Gegenmaßnahme wird die Malware in einer sicheren, kontrollierten Umgebung dazu verleitet, sich zu erkennen zu geben und aktiv zu werden. An diesem Punkt kommt die **Sandbox** ins Spiel – eine, die vor allem Bedrohungen nicht nur hochautomatisiert erkennen, sondern auch darauf reagieren kann.

Komplexes Verhalten an Endpoints zu erkennen, ist auch die **Hauptaufgabe von EDR.** Wie EPP, sollte auch EDR idealerweise aus einer Kombination von Automatisierung, Tools und Sichtbarkeit bestehen, um menschliche Eingriffe bei Bedarf zu unterstützen. Der Sicherheitsbeauftragte muss in der Lage sein, Vorfälle einer Ursachenanalyse zu unterziehen und auf Bedrohungen zeitnah zu reagieren, sei es manuell oder mithilfe von automatisierten Abwehroptionen.

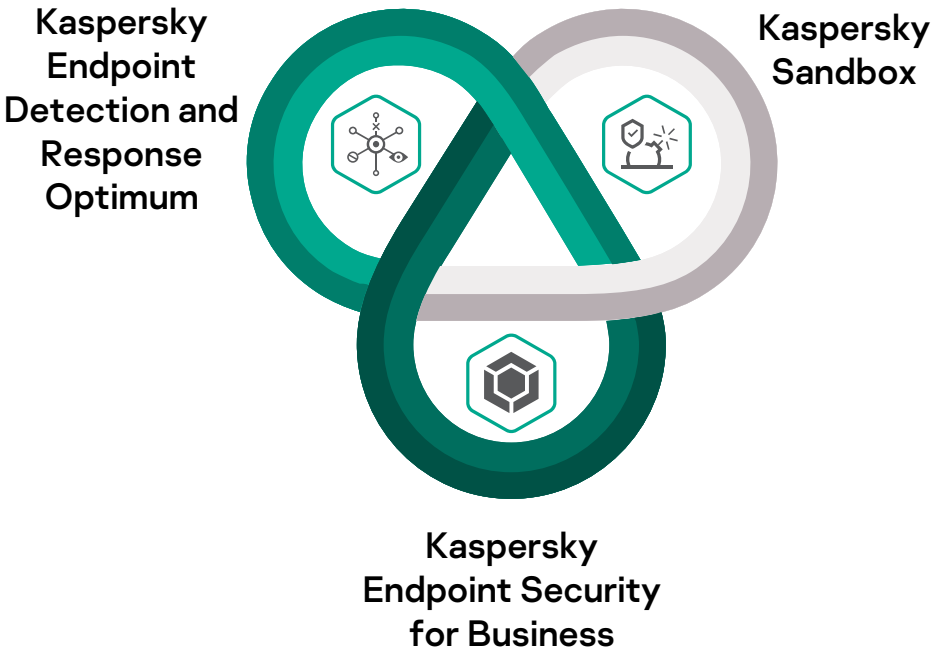
Mit den kombinierten Technologien von EPP, Sandbox und EDR wird Commodity-Malware schnell und effizient bekämpft, die Möglichkeiten für menschliche Fehler werden eingeschränkt und das Risiko eines erfolgreichen hochentwickelten oder zielgerichteten Angriffs wird gemindert, indem auch auf neue, unbekannte und Zero-Day-Bedrohungen reagiert wird.

Und weil all das in einer einzigen Lösung vereint ist, gibt es keine Lücken zwischen unterschiedlichen Tools, die Hacker und Angreifer ausnutzen könnten.

Lösung von Kaspersky

Alle oben genannten Probleme sind in der Integrated Endpoint Security-Lösung von Kaspersky optimal gelöst, einer hochautomatisierten integrierten Lösung aus Endpoint-Schutz und -Kontrollen, einer automatisierten Sandbox und EDR. Alle drei Komponenten arbeiten gemeinsam auf Basis einer starken EPP-Plattform Im Folgenden sollen die einzelnen Komponenten noch etwas detaillierter vorgestellt werden, denn sie bieten weit mehr als nur die Lösung der oben beschriebenen Probleme.

Starker Endpoint-Basisschutz



Kaspersky Endpoint Security for Business basiert auf einer häufig getesteten und vielfach ausgezeichneten Anti-Malware-Engine und hat sich als sehr robuste EPP-Plattform am Markt bewährt (einschließlich Schutz gegen Ransomware und dateilose Angriffe).

Zu den Endpoint-Schutzschichten von Kaspersky Endpoint Security for Business gehören:

- Unsere vielfach ausgezeichnete Anti-Malware-Engine, unterstützt durch maschinelles Lernen
- Erkennung von Ransomware
- Verhaltenserkennung mit automatischem Rollback zum Identifizieren und Blockieren von hochentwickelten Bedrohungen wie dateiloser Malware und Adminkonten-Übernahmen sowie um bereits vorgenommene Änderungen wieder zurückzunehmen
- Exploit Prevention
- Abwehr von mobilen Bedrohungen und EMM-Integration
- Host-basierte Angriffsüberwachung (HIPS)
- Firewall plus Verwaltung der nativen Firewall
- Automatisierte Bedrohungsanalyse (Kaspersky Security Network)
- Verschlüsselung – einschließlich in das Betriebssystem integriertes Verschlüsselungsmanagement
- Security Policy Advisor – zur Überwachung von Änderungen an optimierten Sicherheitseinstellungen
- Vulnerability Assessment und Patch Management
- Installation von Betriebssystemen und Drittanbietersoftware
- Integration von SIEM-Systemen

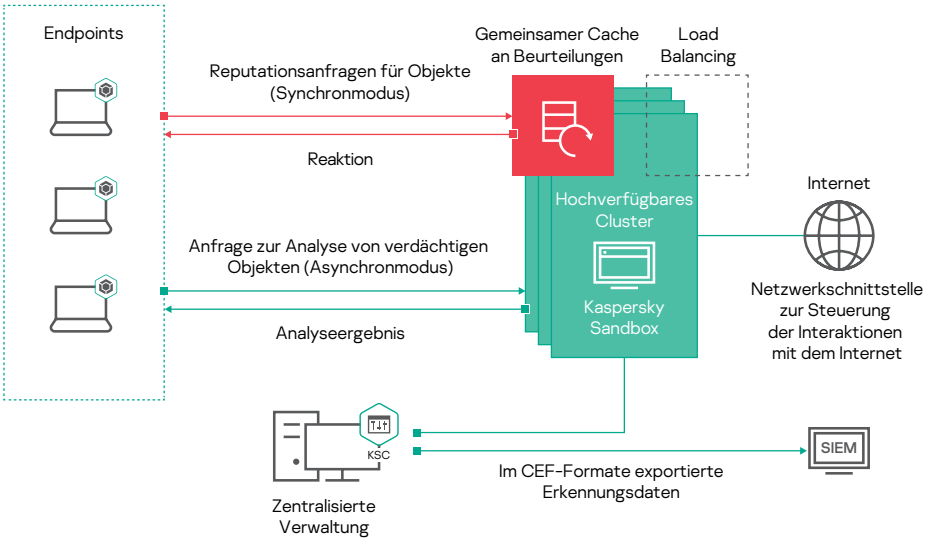
Systemhärtung und Abschwächung menschlicher Fehler werden über Kontrollen erreicht, wie:

- Programmkontrolle mit Kategorie-basiertem Whitelisting
- Adaptive Anomaly Control zum Überwachen und Blockieren von verdächtigen Aktionen, die für die Computer in einem Unternehmenswerk untypisch sind
- Gerätekontrolle – Kontrolle und Blockierung beim Plug-in externer Geräte
- Webkontrolle – blockiert oder beschränkt den Zugriff auf möglicherweise gefährliche, Zeit verschwendende oder unangemessene Seiten

Weitere Informationen zu Kaspersky Endpoint Security for Business finden Sie auf unserer Webseite.

Automatisierte Sandbox

Kaspersky Sandbox erkennt und reagiert automatisch auf Bedrohungen, die den Endpoint-Schutz umgehen, ohne dass ein menschlicher Eingriff erforderlich ist.



Kaspersky Sandbox-Workflow

Die gescannten Objekte werden vom Sandbox-Servercluster auf einer isolierten virtuellen Maschine ausgeführt, die eine Workstation simuliert. Die Komponente erhält eine Anfrage zur Dateianalyse von einem Kaspersky Endpoint Security for Business-Agent, der auf dem Gerät des Endbenutzers installiert ist. Daraufhin wird das Objekt in die Warteschlange eines der Server im Cluster verschoben. Wenn Datei zur Verarbeitung gesendet wird, führt Kaspersky Sandbox sie aus und protokolliert alle Aktionen der Datei. Daraufhin analysiert die Komponente die gewonnenen Daten auf verdächtige und schädliche Aktivitäten und gibt das Ergebnis an den Kaspersky Endpoint Security for Business-Agent zurück, der den Scan angefordert hat. Darüber hinaus wird das Ergebnis der Dateiprüfung an einen gemeinsamen Speicher gesendet, über den auch andere Hosts schnell Informationen zum gescannten Objekt abrufen können, ohne es erneut analysieren zu müssen. Diese Vorgehensweise reduziert die Auslastung der Sandbox-Server und verbessert die Reaktionszeit bei neuen Bedrohungen.

Nachdem eine Datei als schädlich erkannt wurde, kann ihr Gefährdungsindikator von der Kaspersky Endpoint Security for Business-Engine dazu verwendet werden, eine automatische Maßnahme einzuleiten, um die Datei von allen anderen Computern im Netzwerk zu löschen.

Folgende Techniken kommen in der Kaspersky Sandbox zum Einsatz:

- Überwachung der Interaktion mit Internetressourcen
- Laden von Modulen
- Synchrone und asynchrone Scan-Modi
- Anti-Umgehungs-Techniken
- Anwendung unterschiedlicher Emulationsmodi
- Modellierung von Benutzeraktionen
- Automatische IoC-Generierung und Infrastrukturscans
- Automatische Prävention

Weitere Informationen zur Kaspersky Sandbox finden Sie auf unserer Webseite.

Optimierte EDR

Das neue Kaspersky Endpoint Detection and Response Optimum ergänzt Kaspersky Endpoint Security for Business und bietet umfassende Transparenz und die Möglichkeit, Ursachenanalysen durchzuführen. So erhalten Sie einen vollständigen Überblick über den Status Ihrer Unternehmensabwehr von hoch entwickelten Bedrohungen.

Ihr IT-Sicherheitsexperte erhält die nötigen Informationen, die für eine effektive Untersuchung und eine schnelle, genaue Reaktion auf Vorfälle erforderlich sind. Und das noch bevor Schäden auftreten.

Als Teil unserer integrierten Endpoint-Sicherheitslösung ermöglicht Kaspersky Endpoint Detection and Response Optimum Ursachenanalysen hinsichtlich der folgenden Punkte:

- Bildliche Übersicht über den Ausbreitungspfad eines Angriffs, aus der ersichtlich ist, wie sich die Bedrohung auf dem Endpoint entwickelt hat
- Informationen zur Datei wie Metadaten, Dateiursprung, Modifizierungsdaten, digitale Signatur etc.
- Informationen zu Host und Benutzer
- Informationen zur Erkennung
- Prozessinjektion
- Abgelegte Dateien
- Änderungen am Registrierungsschlüssel
- Verbindungen

Nachdem eine Bedrohung erkannt wurde, stehen mehrere automatisierte, per einfachem Mausklick zu aktivierende Abwehroptionen zur Verfügung, wie zum Beispiel:

- Trennen des Hosts
- Start eines Scanvorgangs am Host
- Entfernen der (in Quarantäne gestellten) Datei
- Prozess beenden
- Prozess an der Ausführung hindern

Mit Funktionen wie dem Import bzw. dem Generieren von Gefährdungsindikatoren (IoCs) und anschließendem Scanning dieser IoCs mit voreingestellten Abwehroptionen lässt sich die Bedrohung weiter untersuchen.

Weitere Informationen zu Kaspersky Endpoint Detection and Response Optimum finden Sie auf unserer Webseite.

Kaspersky Endpoint Detection and Response Optimum ist sowohl als lokale als auch als Cloud-basierte Version erhältlich.

Verwaltung und Administration

Alle Komponenten unserer Lösung sind firmeninterne Entwicklungen. Sie werden über eine einzelne Konsole bereitgestellt und nutzen in den unterschiedlichen Bereichen denselben Endpoint-Agent. Daher läuft die tägliche Verwaltung zentralisiert, unmittelbar und effizient ab.

Sicherheitsbewusstsein

- **52 %** der Unternehmen sehen Mitarbeiter als größte Bedrohung für die Cybersicherheit[6]
- **60 %** der Mitarbeiter haben vertrauliche Daten auf ihren Dienstgeräten (z. B. Finanzdaten, E-Mail-Datenbanken etc.)
- **30 %** der Mitarbeiter räumen ein, dass sie die Anmeldedaten ihrer dienstlichen Computer an Kollegen weitergeben[8]

Die computerbasierten Schulungsprodukte von Kaspersky vermitteln mithilfe bewährter Schulungsmethoden und -technologien Fachwissen im Bereich Cybersicherheit. Das Konzept fördert ein optimales Anwenderverhalten und gewährleistet Cybersicherheit in allen Unternehmensbereichen.

Kaspersky Security Awareness sorgt für eine Kultur des sicheren Verhaltens im Cyberspace:

- Nutzer erfahren, wann sie Administratoren über Anzeichen einer potentiellen Bedrohung benachrichtigen sollen.
- Es kommt zu weniger Nutzerfehlern aufgrund von Unwissenheit oder Naivität.
- Es müssen weniger Sicherheitswarnungen von Administratoren überprüft werden.

Sie können den Lernfortschritt Ihrer Mitarbeiter über ein benutzerfreundliches Dashboard mitverfolgen, wo Sie neben einer Datenverfolgung in Echtzeit auch Trends und Vorhersagen zusammen mit Empfehlungen einsehen können, wie Sie Ihre Resultate noch weiter verbessern können.

Weitere Informationen zu Kaspersky Security Awareness finden Sie auf unserer Webseite.

Laut einer Forrester-Studie besteht eine der Hauptforderungen der befragten Unternehmen darin, dass die Bereitstellung von Sicherheitslösungen mit möglichst geringen Unterbrechungen für die Nutzer einhergehen sollten. Diese Forderung ist eines der Grundprinzipien der Integrated Endpoint Security

6 The Cost of a Data Breach, Kaspersky, 2018

* Es gibt gewisse Einschränkungen bezüglich der Auswahl an Funktionen, die über die Cloud-Konsole verwaltet werden können. Eine vollständige Aufstellung finden Sie in der Onlinehilfe.

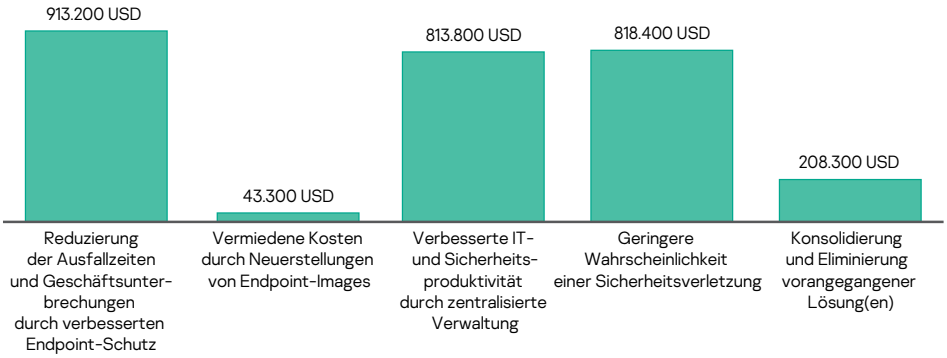
Ihr ROI

Wie bei jeder Lösung sind die Kosten ebenso wichtig wie die Vorteile, die sie bietet. Weiter unten finden Sie ein Beispiel dafür, wie die Kapitalrendite für Kaspersky-Lösungen aussieht. Die Angaben basieren auf einer Forrester-Studie[7], in deren Rahmen eine Kaspersky-Sicherheitslösung auf der Grundlage von Kaspersky Endpoint Security for Business und Kaspersky Endpoint Detection and Responce untersucht wurde.

Vorteile für Unternehmen laut risikobereinigtem aktuellen Wert (Present Value – PV) der Forrester-Studie:

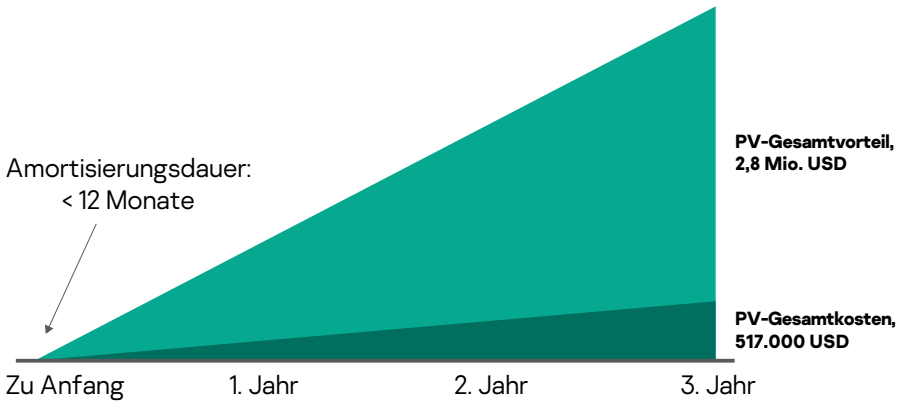
- **Fast 1,0 Million USD:** Auswirkung auf den Umsatz wegen verbesserter Betriebszeiten am Endpoint aufgrund von weniger Geschäftsunterbrechungen
- **Mehr als 40.000 USD:** Durch weniger Sicherheitsvorfälle eingesparte IT-Workloads durch weniger Neuerstellungen von Endpoint-Images
- **Mehr als 800.000 USD:** Einsparungen dank vereinfachter Verwaltung von mehreren Sicherheitslösungen durch eine zentralisierte Verwaltungskonsole
- **Mehr als 800.000 USD:** Geringere Gefahr einer wesentlichen Sicherheitsverletzung führt zu erheblicher Steigerung der allgemeinen Sicherheitsstellung
- **Mehr als 200.000 USD:** Kosteneinsparungen nach dem Umstieg auf Kaspersky

Vorteile (über drei Jahre)



Anhand von Gesprächen mit Bestandskunden und der nachfolgenden Finanzanalyse ergab die Studie, dass eine Organisation im Laufe von drei Jahren gegenüber den Kosten von 500.000 USD einen finanziellen Vorteil von 2,8 Millionen USD erwirtschaftete, was einem aktuellen Nettoüberschuss von 2,3 Millionen USD und ein ROI von 441 % entspricht.

Finanzübersicht



7 The Total Economic Impact™ von Kaspersky-Sicherheitslösungen, eine bei Forrester Consulting in Auftrag gegebene Studie vom Januar 2020

8 „Sorting out a Digital Clutter", Kaspersky, 2019.

Zusammenfassung

Der Schutz von Endpoints ist unabdingbar, um Ihre Organisation in der heutigen Bedrohungslandschaft abzusichern. Und die beste Möglichkeit, Ihre Endpoints zu schützen, ist eine mehrstufige Lösung mit unterschiedlichen Techniken zur hochautomatisierten Erkennung und Abwehr von Bedrohungen, während menschliche Eingriffe den komplizierteren Aufgaben und wichtigen Entscheidungen vorbehalten sind.

Die Integrated Endpoint Security-Lösung von Kaspersky wurde speziell konzipiert, um dem Bedürfnis von Organisationen nach Schutz gegen Commodity-Bedrohungen, hochentwickelte und komplexe Bedrohungen sowie menschliche Fehler gerecht zu werden. All das wird erreicht durch:

- Implementierung einer **mehrstufigen, integrierten Schutz-, Erkennungs- und** Abwehrstrategie
- **Automatisierung** von Abwehrmechanismen, um die Zeit und den Aufwand für Reaktionen auf zielgerichtete und hochentwickelte Angriffe zu reduzieren
- Erkennungsraten **auf höchstem Niveau**
- Einrichtung **einer sicheren Cyberkultur mithilfe von Kontrollen und der Schärfung des Sicherheitsbewusstseins**
- Sicherstellung **einer erheblichen Rendite auf Ihre Investition**

All das bedeutet, dass Sie ein Höchstmaß an Sicherheit selbst gegen hochkomplexe Cyberbedrohungen genießen können, ohne wertvolle Ressourcen zu binden.

Weitere Informationen dazu, wie Integrated Endpoint Security Ihnen helfen kann, Ihre Organisation gegen komplexe Angriffe zu schützen, ohne Ihre Ressourcen allzu sehr zu beanspruchen, finden Sie auf unserer **Webseite**.

www.kaspersky.de