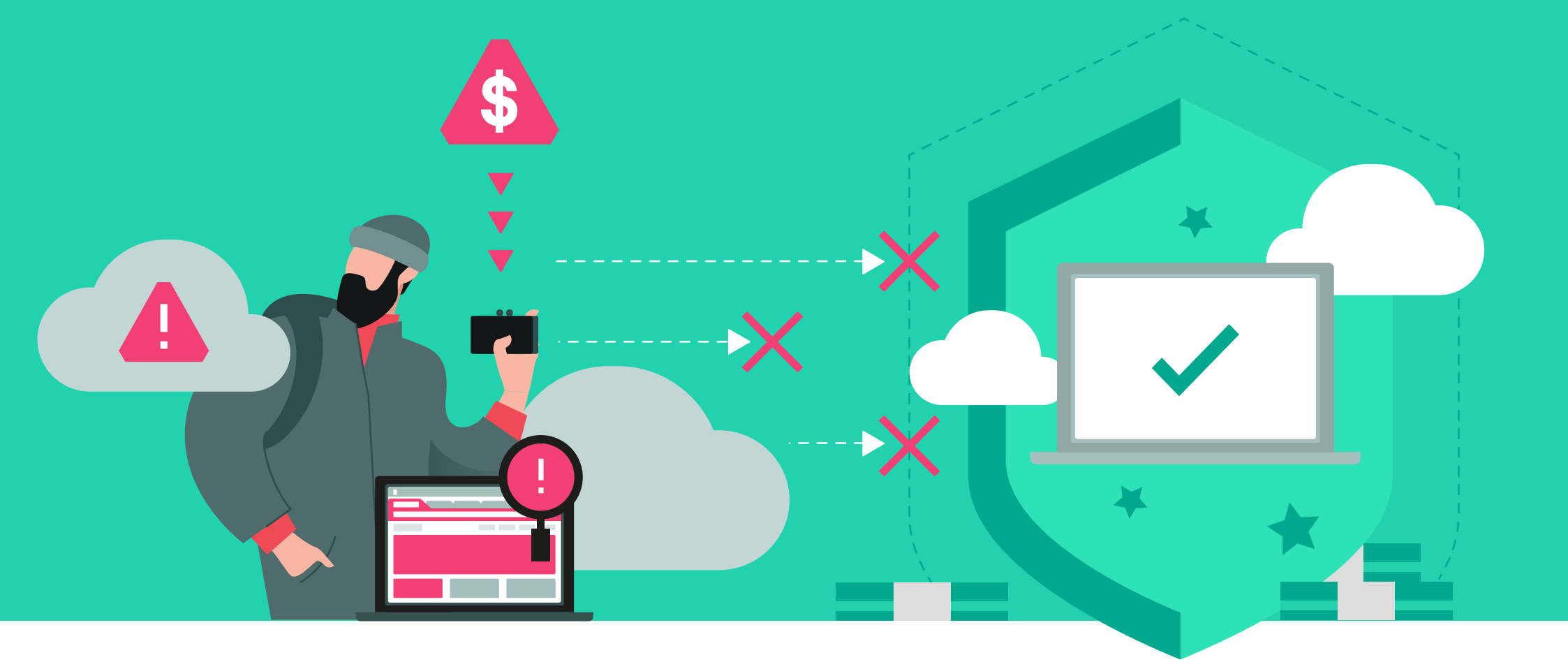


Warum Schutz von Kaspersky vor Ransomware?

kaspersky

Das Problem

Ransomware im Jahr 2020 ist eine Bedrohung, die sich stetig weiterentwickelt. Ransomware-Angriffe sind gefährlicher geworden, gehen gezielter bestimmte Unternehmensbereiche und Branchen an und erpressen immer höhere Lösegeldzahlungen. Die Kosten für disruptive Geschäftsunterbrechungen sind in die Höhe geschnellt und auch die Zahl der neuen Ransomware-Arten von undefinierten Akteuren steigt stetig an, was Ransomware zu einem der größten Problem für die IT-Sicherheit macht.

Die Lösung

Endpoint-Schutz von Kaspersky ist speziell auf die Herausforderungen in 2020 und darüber hinaus zugeschnitten. Die branchenführende Lösung umfasst Tools zum Schutz gegen Ransomware und Krypto-Malware, sichert Cloud-Umgebungen, virtuelle und physische Endpoints sowie geteilte Netzwerke und versetzt betroffene Dateien wieder in den ursprünglichen Zustand vor der Verschlüsselung.

Das Jahr 2020 in Zahlen

40 Mrd. USD

GESCHÄTZTE WELTWEITE KOSTEN

für Ransomware-Forderungen und Geschäftsunterbrechungen in 2020 [1]

23x

HÖHERE KOSTEN FÜR GESCHÄFTSUNTERBRECHUNGEN

als die durchschnittliche Lösegeldforderung (laut Studie) [2]

141.000 USD

DURCHSCHNITTLICHE KOSTEN FÜR RANSOMWARE-STILLSTAND

im Jahr 2019 (200 % höher als noch 2018) [3]

[1] Ransomware-Lösegeldforderungen: 170 Mill USD Worldwide Forecast in 2020, Bericht

[2] „Global State of the Channel Ransomware Report 2019" von Datto

[3] Help Net Security: 1 von 5 KMUs ist einem Ransomware-Angriff zum Opfer gefallen

62,4%

BUSINESSES VICTIMISED BY RANSOMWARE

according to 2019 global IT decision makers' survey [4]

30%

OF RANSOMWARE TARGETS IN PAST YEAR

are business users [5]

20%

SMBs FELL VICTIM

to a ransomware attack in 2019, according to survey [9]

[4] Statista: Anteil der Organisationen, die zwischen 2017 und 2019 weltweiten Ransomware-Angriffen zum Opfer gefallen sind.

[5] Einer von drei Ransomware-Angriffe zielt auf Unternehmensnutzer ab: Kaspersky und INTERPOL fordern am „Anti-Ransomware Day" Backups und Schutz

[9] „Global State of the Channel Ransomware Report 2019" von Datto

21%

WANNACRY IM VERGANGENEN JAHR

% aller erkannten Ransomware-Angriffe [6]

22

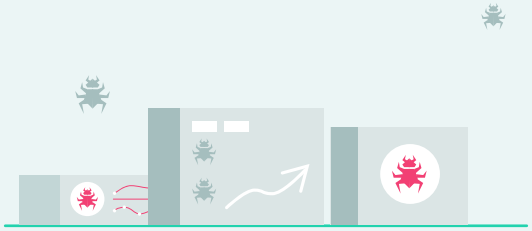
NEUE RANSOMWARE-ARTEN

wurden entdeckt.
+ 46.156 Änderungen durch Enkrypter [7]

49%

DER IM ERSTEN QUARTAL 2020 ERKANNTEN RANSOMWARE-ANGRIFFE

sind Krypto-Ransomware [8]



[6] Einer von drei Ransomware-Angriffe zielt auf Unternehmensnutzer ab: Kaspersky und INTERPOL fordern am „Anti-Ransomware Day" Backups und Schutz

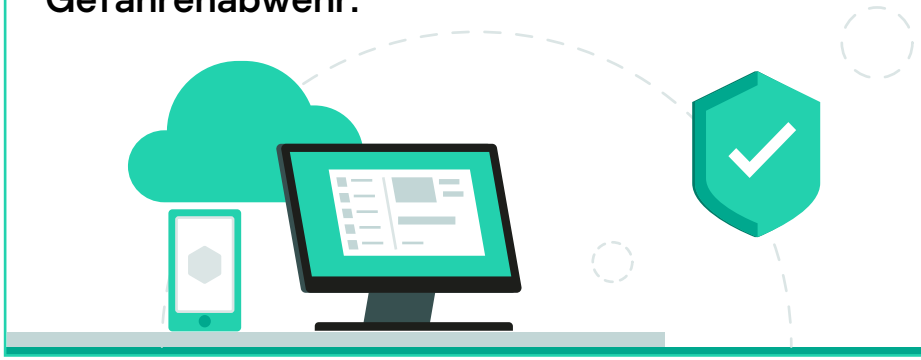
[7] Kaspersky Security Bulletin 2019. Statistiken

[8] KSN Report: Ransomware 2018-2020

Cybersicherheitslösungen von Kaspersky bieten mithilfe hochentwickelter mehrstufiger Technologien bewährten Schutz gegen Ransomware sowohl in der Bereitstellungs- als auch der Ausführungsphase.

Automatische EDR

Kaspersky Endpoint Detection and Response bietet umfassende Netzwerktransparenz und hochentwickelte Schutzmechanismen. Mit automatisierten Tasks werden Ransomware und andere komplexe Bedrohungen erkannt, priorisiert, untersucht und neutralisiert. EDR umfasst alle „Schwergewichte“ unter den Erkennungstools (Sandbox, Deep Learning-Modelle, Ereigniskorrelation) sowie Expertentools für die Vorfallsuntersuchung, vorausschauendes Threat Hunting und Gefahrenabwehr.

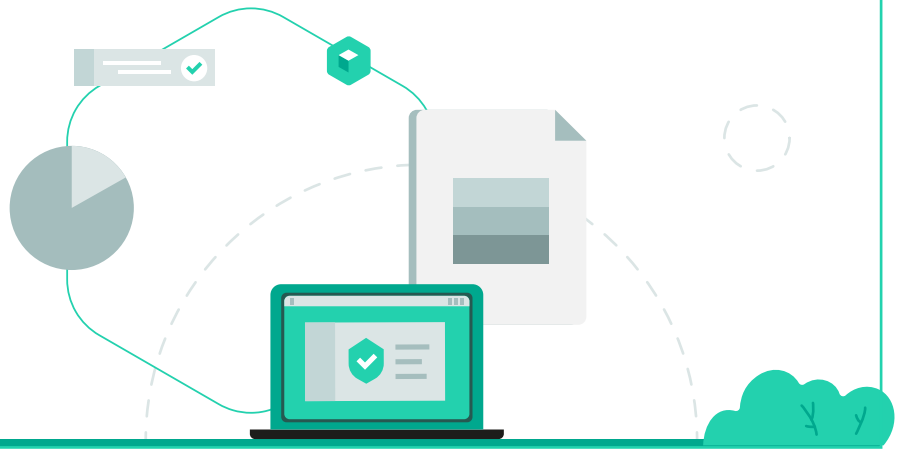


Exploit Prevention

Kaspersky Exploit Prevention hindert Malware (einschließlich Ransomware) an der Ausnutzung von Software-Schwachstellen. Ausgelöst durch verdächtige Aktionen analysiert die Komponente das Verhalten auf schädliche Muster. Malware wird mit speziellen Signaturen versehen, damit schädliche Dateien noch vor dem Öffnen erkannt werden. Vorausschauender Schutz ermöglicht Malware-Erkennung und -Blockierung, sobald eine Datei geöffnet wird.

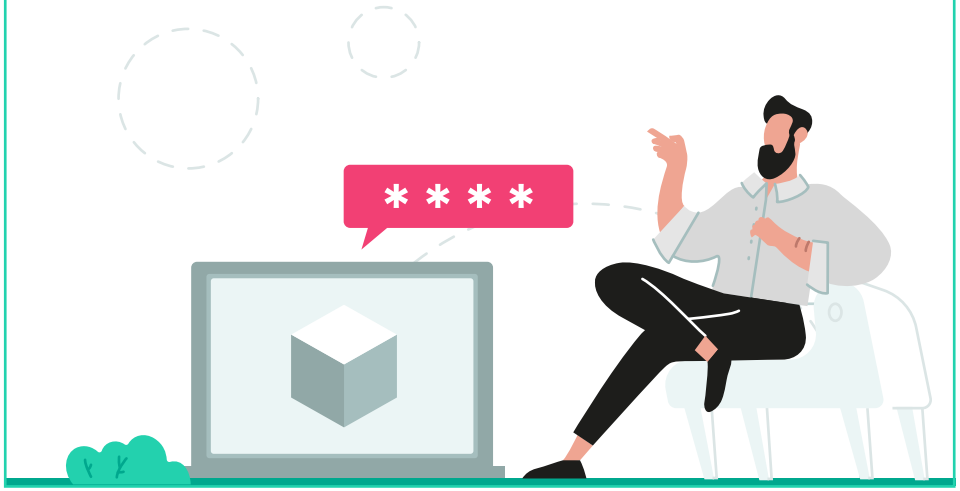
Verhaltenserkennung mithilfe von maschinellem Lernen (mit automatischer Wiederherstellung des Ausgangszustandes)

Dank maschinellem Lernen erkennen Kaspersky-Technologien bislang unbekannte Malware-Bedrohungen (einschließlich Ransomware), indem sie aus großen relevanten Datenmengen der Threat Intelligence „lernen“ und entsprechende effektive Erkennungsmodelle entwickeln – vor Ort, aber auch im Rahmen einer Bedrohungsanalyse im Labor und unter Einsatz mehrerer Sicherheitsschichten. Das Anti-Ransomware-Tool von Kaspersky versucht automatisch eindringende Programme unschädlich zu machen (zum Beispiel durch Wiederherstellen veränderter Dateien und der System-Registry).



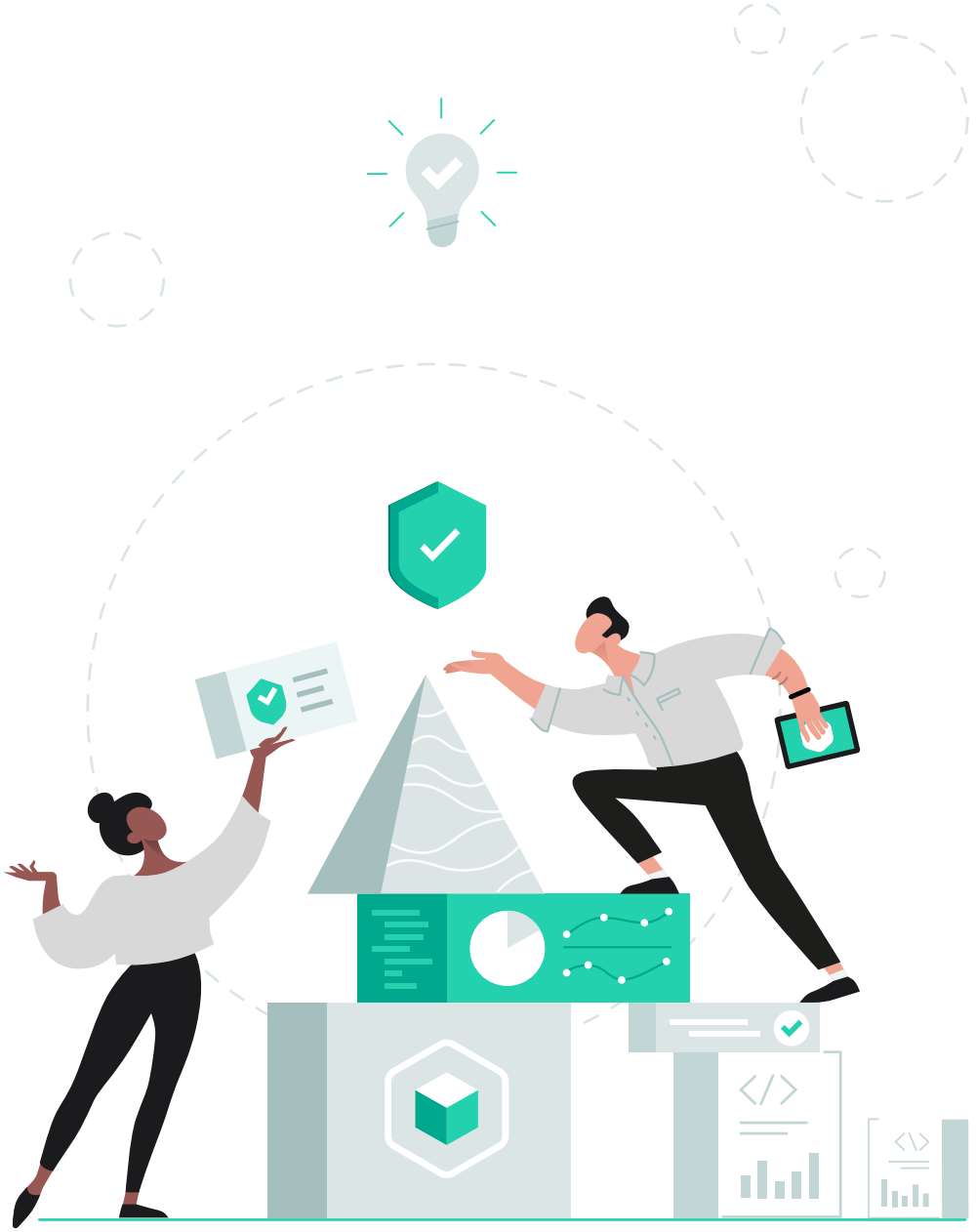
Encryption Management

Ransomware ist eine Malware, die die Dateien ihrer Opfer verschlüsselt. Mit dem Encryption Management von Kaspersky werden alle gemanagten Geräte unter Windows und macOS verschlüsselt, so dass kein unbefugter Benutzer auf gespeicherte Daten zugreifen kann. Mit einer Full-Disk-Verschlüsselung werden Datenlecks bei Verlust eines Geräts verhindert. File-Level-Verschlüsselung schützt Dateien, die in nicht vertrauenswürdige Kanäle übertragen werden, und Crypto Disk speichert Nutzerdaten in verschlüsselter Form in einer separaten Datei



Vulnerability Assessment und Patch Management

Kaspersky Vulnerability Assessment und Patch Management verhindern, dass Malware einschließlich Ransomware erst kürzlich erkannte und noch nicht gepatchte Schwachstellen in Betriebssystemen und gängigen Programmen ausnutzen kann. Gefährdete Software an jedem Endpoint wird dank automatisiertem Vulnerability Assessment erkannt, Patches, Programme und Updates können selbsttätig von einer zentralen, integrierten Verwaltungskonsole aus installiert werden.



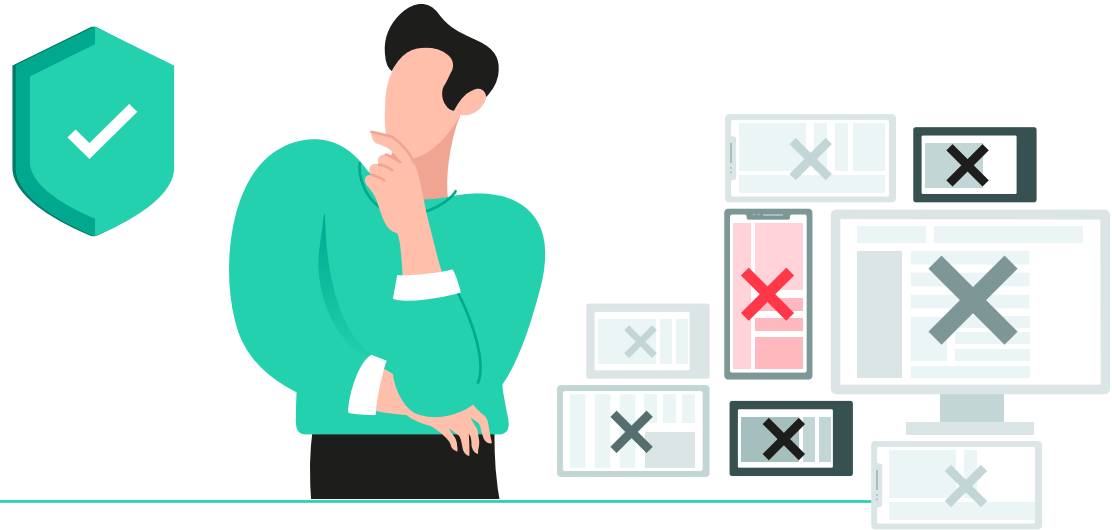
Auch wenn die absolute Zahl der Ransomware-Angriffe in den letzten 12 Monaten zurückgegangen ist, sind die negativen Auswirkungen eines erfolgreichen Ransomware-Angriffs auf Organisationen aufgrund der Kombination aus teurem Stillstand, Reputiationsschaden und Lösegeldzahlungen beträchtlich in die Höhe geschnellt. Ransomware bleibt eine der am meisten gefürchteten Cyberbedrohungen, mit denen Organisationen jeglicher Größe und Branche konfrontiert sind.

So schützen Sie Ihre Geräte vor Ransomware

- [x] Erstellen Sie regelmäßig Datenbackups, um im Notfall jederzeit darauf zurückgreifen zu können.
- [x] Nutzen Sie Tools, die Schwachstellen automatisch erkennen sowie Patches selbsttätig herunterladen und installieren können.
- [x] Halten Sie Software und Betriebssysteme auf allen Geräten grundsätzlich auf dem neuesten Stand.
- [x] Bleiben Sie stets wachsam gegenüber Phishing-Angriffen, gefälschten Nachrichten und Links sowie potentiell schädlichen Dateien.
- [x] Schulen Sie Ihre Mitarbeiter. Schulungsangebote wie die Kaspersky Automated Security Awareness Platform können hier helfen.
- [x] Installieren Sie hochwertige, mehrstufige Cybersicherheit wie Kaspersky Endpoint Security for Business bzw. Kaspersky Security Cloud für persönliche Geräte, um sich gegen Dateien-verschlüsselnde Malware zu schützen und Änderungen von Schadprogrammen zurückzunehmen.

Was tun, wenn Daten von Ransomware befallen sind

- [x] Trennen Sie die Internetverbindung.
- [x] Gehen Sie grundsätzlich nicht auf Lösegeldforderungen ein. Ein Drittel der Opfer erhält trotz Zahlung keinen Zugang zu seinen Daten.
- [x] Holen Sie sich technische Hilfe, um die Daten wiederherzustellen.
- [x] Wenden Sie sich an No More Ransom, eine Initiative gegen Lösegeldzahlungen, wo Sie Ressourcen wie z. B. mehr als 100 kostenlose Entschlüsselungstools finden.



Schützen Sie Ihre Geräte wirksam vor Ransomware

Installieren Sie das KOSTENLOSE Kaspersky Anti-Ransomware Tool und nutzen Sie moderne Funktionen wie Cloud-gestützte Verhaltenserkennung, um Ransomware und Krypto-Malware zu scannen und sofort unschädlich zu machen. Unser Tool erfüllt die Anforderungen der DSGVO und ist mit den meisten Sicherheitsprogrammen kompatibel.

Kaspersky Anti-Ransomware Tool ist nicht das einzige Kaspersky-Produkt mit hervorragenden Testergebnissen. Cybersicherheitslösungen von Kaspersky haben sich immer wieder in unabhängigen Tests bewährt:

DER WELTWEIT AM HÄUFIGSTEN GETESTETE UND VIELFACH AUSGEZEICHNETE SCHUTZ

86
TEILNAHMEN AN TESTS/BEWERTUNGEN

64
ERSTE PLÄTZE

81%
TOP-3-PLÄTZE

Lernen Sie die Vorteile der modernen Technologien von Kaspersky kennen und genießen Sie umfassenden Schutz mit Kaspersky Endpoint Security for Business Standortunabhängige Remote-Sicherheitsverwaltung für mehrere Endpoints, mobile Geräte und File-Server.

kaspersky