KASPERSKY lab

LASSEN SIE SICH NICHT ERPRESSEN! SCHÜTZEN SIE IHR UNTERNEHMEN NOCH HEUTE.

WARUM SOLLTEN SIE SICH BEIM SCHUTZ VOR RANSOMWARE FÜR KASPERSKY LAB ENTSCHEIDEN?

DAS PROBLEM

2016 war das Jahr der Ransomware-Revolution. Die Angriffe ereigneten sich weltweit und wurden im Hinblick auf Daten, Geräte, Unternehmen und einzelne Benutzer noch rigoroser durchgeführt.

Außerdem richteten sich 2016 Cryptomalware-Angriffe verstärkt gegen Unternehmen, wodurch sie zu den 3 größten IT-Sicherheitsproblemen für KMUs zählten.

DAS JAHR 2016 IN ZAHLEN

20% DER UNTERNEHMEN WELTWEIT **verzeichneten einen IT-Sicherheitsvorfall infolge eines Ransomware-Angriffs.***

42% DER KLEINEN UND MITTELSTÄNDISCHEN UNTERNEHMEN **wurden in den letzten 12 Monaten Opfer von Ransomware-Angriffen.**

DIE HÄUFIGKEIT, MIT DER UNTERNEHMEN durch Ransomware angegriffen wurden: alle **40 Sekunden**

DIE DURCHSCHNITTLICHEN KOSTEN für Schäden, die durch einen einzigen Cryptomalware-Angriff auf KMUs entstanden: **99.000 $**

67% DER UNGEFÄHRE ANTEIL VON KMUs, die einen vollständigen oder teilweisen Verlust von Unternehmensdaten aufgrund von Cryptomalware verzeichneten.

1 von 5 KMUs, DIE DER LÖSEGELDFORERUNG NACHKAMEN, erhielten ihre Daten niemals zurück.

62 NEUE RANSOMWARE-ARTEN wurden entdeckt.

1.445.434 BENUTZER-PCs wurden von Cryptors ins Visier genommen.

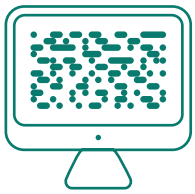
**Umfrage zu IT-Sicherheitsrisiken 2016*

DIE LÖSUNG

Seit 2014 sind Produkte von Kaspersky Lab mit Funktionen zum Schutz vor Cryptomalware ausgestattet. Und unsere Technologie wurde erheblich ausgeweitet, um dieser sich ständig wandelnden Bedrohungslage zu begegnen.

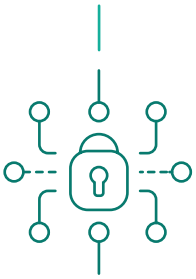
MEHRSTUFIGER SCHUTZ VON KASPERSKY LAB

Die Sicherheitslösungen von Kaspersky Lab bieten einen mehrstufigen Schutz vor Cryptomalware, sowohl im Hinblick auf Infrastrukturelemente als auch auf Technologien, die verwendet werden, um Ransomware abzuwehren.



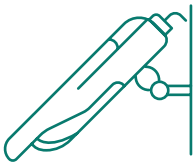
Die zuverlässige Erkennung von Malware und der Schutz vor bekannten, unbekannten sowie hochentwickelten Bedrohungen wird durch eine Kombination aus präzisen Erkennungstechnologien sichergestellt, die auf Blacklisting und proaktiven, maschinellen Lernfunktionen basieren. Sie alle nutzen die globalen Big-Data-Verarbeitungsfunktionen des Kaspersky Security Networks (KSN).

Sicherheitskontrollen (u. a. für Geräte, Web und Programmstarts) ermöglichen es Ihnen, die Nutzung von unerwünschten Geräten und Webseiten sowie den Start unbefugter bzw. nicht vertrauenswürdiger Programme zu beschränken. Dadurch wird die Gefahr von Malware-Angriffen, einschließlich Cryptors, minimiert.



Die Application Privilege Control kann so konfiguriert werden, dass Programme auf bestimmte Ressourcen, einschließlich System- und Benutzerdateien, nur beschränkt zugreifen können. Das bedeutet, dass Ransomware diese nicht verschlüsseln kann, da keine Schreibberechtigung gewährt wird.

Der automatische Exploit-Schutz sorgt stets dafür, dass Malware keine Schwachstellen innerhalb des Betriebssystems oder bei häufig angegriffenen Programmen ausnutzen kann.



Der System Watcher überwacht Programmprozesse und vergleicht deren Verhalten mit bekannten, gefährlichen Aktivitätsmustern. Dadurch können von schädlichen Programmen durchgeführte Aktionen erkannt und blockiert werden. Der System Watcher verwendet Verhaltensanalysen zur Identifizierung von verdächtigen und unbekannten (Zero-Day)-Aktivitäten. Anhand der gesammelten Informationen kann Kaspersky Endpoint Security die von Malware durchgeführten Aktionen rückgängig machen; u. a. kann es Dateien, die zuvor von Cryptomalware verschlüsselt wurden, automatisch wiederherstellen.

Die serverbasierten Anti-Cryptor-Funktionen von Kaspersky Lab kommen zum Einsatz, wenn ein Verschlüsselungsversuch von einer infizierten Workstation (über das lokale Netzwerk) erkannt wird. Wenn ein Cryptor versucht, Dateien auf gemeinsam genutzten Ressourcen, z. B. Unternehmensservern, zu verschlüsseln, blockiert die Anti-Cryptor-Komponente den Zugriff über die infizierte Workstation auf die gemeinsam genutzte Ressource und stoppt den Verschlüsselungsprozess.

Das Vulnerability Assessment und Patch Management in Kaspersky Endpoint Security for Business tragen zu einer noch größeren Sicherheit bei, indem der Prozess zur Reduzierung von Software-Schwachstellen automatisiert wird.
Dadurch werden mögliche Penetrationen bzw. erfolgreiche Angriffe sämtlicher Malware-Arten auf Ihr IT-Netzwerk minimiert.

ZUVERLÄSSIGER SCHUTZ VOR RANSOMWARE

DURCH KUNDEN-DEPLOYMENTS BESTÄTIGT

COLLEZIONE, eine der führenden Modemarken in der Türkei, nutzt Kaspersky Endpoint Security for Business – Advanced.

"... Wir waren insbesondere davon beeindruckt, dass der Ransomware-Schutz all unsere Tests bestanden hat", erinnert sich Gökhan Zengin, IT-Manager von Collezione.

JJW HOTELS, ein vielfach ausgezeichnetes Gastronomie-, Hotel- und Freizeitunternehmen, nutzt Kaspersky Endpoint Security for Business – Select.

„Seitdem die Lösung von Kaspersky Lab installiert ist, haben wir keine Probleme mehr mit Ransomware oder anderen Angriffen", sagt Tiago Reis, Group IT Infrastructure Manager, MBI International.

KONTAKTIEREN SIE UNS NOCH HEUTE, UND SCHÜTZEN SIE IHR UNTERNEHMEN

Anti-Ransomware-Tool von Kaspersky Lab:
go.kaspersky.com/anti-ransomware-tool

Webseite von Kaspersky Lab:
kaspersky.de

Kaspersky Lab – B2B-Blog
business.kaspersky.com