Wirkungsvoller Schutz für Ihre Endgeräte. Endpoint Exploit Prevention.

Angriffe abwehren, bevor etwas passiert

Anstatt zu versuchen Millionen Einzelangriffe zu identifizieren, oder schädliches Verhalten aufzuspüren, konzentriert sich Exploit Prevention auf die Kerntechniken, die jeder Angreifer nacheinander ausführen muss, um den entsprechenden Endpoint zu kapern.

Durch den Aufbau einer Reihe von „Fallen“ zur Abwehr dieser Techniken ist die Lösung in der Lage, den Angriff sofort abzuwehren, bevor eine schädliche Aktivität erfolgreich ausgeführt werden kann.

Malware-Angriffe und Exploits aktiv verhinden

Sowohl bekannte als auch hochentwickelte, gezielte Angriffe, vor denen herkömmliche Sicherheitslösungen keinen Schutz bieten, werden durch eine Endpoint Security Lösung proaktiv abgewehrt.

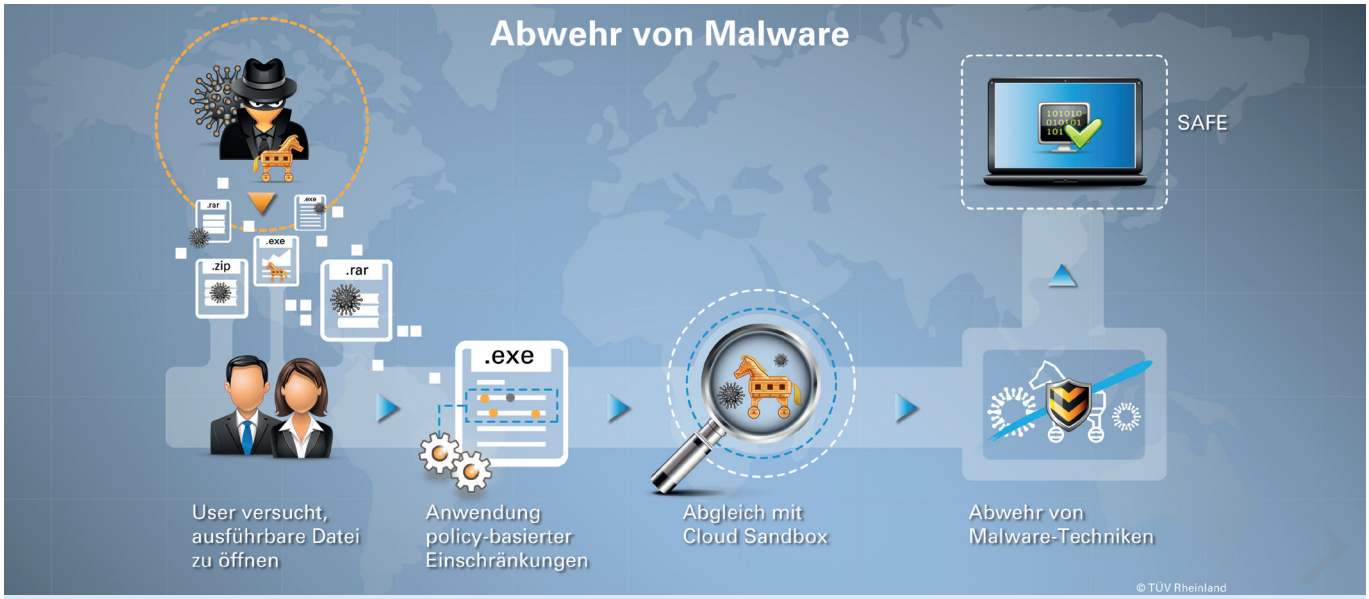
Hierbei kommen hochskalierbare, leichte Agenten mit einem neuen Ansatz zur Angriffsabwehr zum Einsatz. Somit sind keinerlei Vorabkenntnisse über die Bedrohung selbst erforderlich.

Wie werden Exploits verhindert?

Aufgrund des kettenartigen Aufbaus eines Exploits muss mindestens eine der Techniken in der Kette abgewehrt werden, um den gesamten Angriff zu verhindern.

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.



Abwehr von Malware:

Schädliche ausführbare Dateien (Malware) werden oftmals als gutartige Dateien getarnt oder sind in diesen eingebettet. Diese Dateien können den Computer beschädigen, indem sie versuchen, die Kontrolle zu übernehmen, sensible Informationen zu sammeln oder den normalen Betrieb des Systems stören. Mittels der „Fallen“ in unserer Endpoint Security Lösung wird die Malware aktiv abgewehrt.

Ihre Vorteile auf einen Blick:

- Angriffe auf Ihr System werden abgewehrt, bevor schädliche Aktivitäten erfolgreich ausgeführt werden können.
- Umfassender Schutz vor „herkömmlichen“ Angriffen sowie hochentwickelten, gezielten Attacken (Advanced Persistent Threats).
- Die Lösung schützt ungepatchte Systeme, erfordert keine Hardware und wird auf allen Plattformen unterstützt, auf denen Microsoft Windows läuft: Desktops, Server, Industriesteuerungen, Terminals, VDI, VMs, eingebettete Systeme etc.
- Die eingesetzten Agenten benötigen nur minimale Ressourcen – die Abwehrmaßnahmen im Hintergrund beeinträchtigen den Benutzer daher nicht.

Unsere Leistungen und Services:

- Umfassender Konfigurationssupport: Wir definieren gemeinsam mit Ihnen Ihren individuellen Schutzbedarf und konfigurieren Ihre Endpoint Security Lösung entsprechend.
- Anbindung an bestehende IT-Sicherheitssysteme. Wir prüfen die Möglichkeiten und unterstützen Sie bei der Integration in bereits vorhandene IT-Sicherheitssysteme.
- Schnelle Eingreiftruppe: Auf Wunsch kombinieren wir Ihre Endpoint Security Lösung mit unserem CSIRT (Computer Security Incident Response Team). Im Falle eines Cyber Angriffs stehen Ihnen unsere Experten bei der Analyse und Bekämpfung somit schnellstmöglich zur Seite.
- Profitieren Sie von Expertenwissen und jahrelanger Praxiserfahrung!

Gerne unterstützen wir Sie von der Beratung bis zur Implementierung einer effektiven Endpoint Security Lösung. Fragen Sie uns!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com