Adaptive Anomaly Control: Hält Angriffe auf, bevor sie beginnen

Effektiver Schutz, der einfache Blockierungsregeln mit automatischen intelligenten Feineinstellungen kombiniert, die aus Verhaltensanalysen gewonnen werden.

kaspersky BRING ON THE FUTURE

www.kaspersky.de
#truecybersecurity

Adaptive Anomaly Control: Hält Angriffe auf, bevor sie beginnen

Warum Härtung harte Arbeit ist

Entwickler von Endpoint-Protection-Plattformen sind ständig auf der Suche nach neuen Möglichkeiten, Malware, unsichere Links und andere Anzeichen für Angriffe zu erkennen, um moderne Cyberbedrohungen zu bekämpfen. Doch trotz des Einsatzes von komplexen und ressourcenintensiven Technologien (Big Data, maschinelles Lernen), schaffen es Eindringlinge immer noch, diese Schutzsysteme zu umgehen und dabei gravierende Schäden in Unternehmen anzurichten.

Andererseits können viele dieser Bedrohungen, einschließlich APTs, erfolgreich durch einfache signaturlose Methoden zur Prävention abgewehrt werden, die sich nicht auf die Tools der Angreifer, sondern auf die „Hygiene" des angegriffenen Systems konzentrieren. Wenn Sie die Schwachstellen Ihres Systems kennen, können Sie proaktiv Aktionen blockieren, die zu deren Ausnutzung führen könnten. In den letzten Jahren liegt der Schwerpunkt verstärkt auf Methoden zur Reduzierung der Angriffsfläche oder „Härtung", denn:

Alte Schwachstellen sind die Hauptursache für die meisten Angriffe der letzten Zeit. Viele gut dokumentierte Schwachstellen werden monate- oder sogar jahrelang nicht gepatcht, da ihre Behebung zusätzliche technische Arbeiten und die Unterbrechung wichtiger Geschäftsprozesse mit sich bringt. Die effektivste Methode, diese nicht gepatchten Schwachstellen „abzudecken", besteht darin, Ihre Sicherheitsrichtlinien zu härten.

Ein Beispiel: Der massenhafte Ausbruch von Angriffen durch die Cryptolocker WannaCry und ExPetr im Mai und Juni 2017 basierte auf der Ausnutzung der EternalBlue-Schwachstelle im SMB-Protokoll. Der Sicherheitspatch für diese Schwachstelle war bereits zwei Monate davor verfügbar, aber viele Systeme waren noch nicht aktualisiert. Einige Systemadministratoren verhinderten jedoch die Infektion ihrer anfälligen Systeme durch die Implementierung einfacher Einschränkungen: Sie deaktivierten den anfälligen SMB1-Transport und blockierten bestimmte TCP-Ports, die wahrscheinlich Ziel eines Angriffs der Malware werden würden.

Die Vielzahl von Funktionen, über die viele moderne Computersysteme verfügen, hilft Eindringlingen. Softwareanbieter bewerben die „umfangreichen Funktionen" und den „einfachen Zugriff" ihrer Produkte. Wenn diese Produkte wie in der Werbung versprochen als „sofort einsatzbereit" ausgeführt werden, werden ihre vollen, übermäßigen Funktionen für gewöhnlich standardmäßig aktiviert, wobei ihre Sicherheitseinstellungen deaktiviert sind. Sie sehen also, warum Angreifer heute häufig legitime Programme nutzen, statt sich mit spezieller Malware zu beschäftigen, oder Social Engineering anwenden, um legitime Benutzer dazu zu zwingen, selbst schädliche Aktionen durchzuführen.

Nehmen Sie z. B. MS Word-Dokumente. Anfang 1990 wurden diese Dateien als sicher betrachtet, da sie nicht ausführbar waren. Als jedoch Makros aufkamen, wurde es möglich, beispielsweise PowerShell direkt aus dem Dokument auszuführen. Diese „nützliche" Funktion hat zu vielen Malware-Epidemien geführt, darunter Angriffe durch Cryptolocker (PowerWare), Spyware (August Stealer) und APTs, die es auf Finanzinstitute abgesehen haben (Odinaff, Turla). Um diese Angriffe zu verhindern, müssen Sie nicht warten, bis jeder neue Trojaner erkannt wird – deaktivieren Sie einfach die Makros in MS Office-Dokumenten. So einfach ist es.

Die Reduzierung der Angriffsfläche kann also eine sehr effektive und kostengünstige Präventionsmethode sein. Im täglichen Gebrauch können jedoch Nachteile auftreten.

Allgemeine Einschränkungen ignorieren spezifische Szenarien, wodurch legitime Benutzer belastet werden. Stellen Sie sich vor, Sie würden Ihr System durch die Anwendung allgemeiner Blockierungsregeln wie Default Deny härten, nur um zu festzustellen, dass die Finanzabteilung MS Word-Dokumente mit Makros benötigt und die Marketingabteilung Bannerwerbung auf Websites prüfen muss. Mit Ihrer allgemeinen Blockierung von Makros und Adobe Flash würden Sie ihnen das Leben sehr schwer machen. Wenn eine Blockierungsregel nicht an verschiedene Szenarien angepasst werden kann, kann sie in der Praxis möglicherweise nicht angewendet werden.

Die manuelle Feineinstellung erfordert viel Arbeit von Experten. Einige Anbieter bieten bereits Härtungslösungen an, die eine subtilere Konfiguration von Blockierungsregeln ermöglichen. Jedoch wenden selbst erfahrene Administratoren diese Tools wahrscheinlich nicht vollständig an, da die manuelle Anpassung jeder Regel für viele verschiedene Gruppen und Programme sehr viel Zeit in Anspruch nehmen würde. Hinzu kommt, dass neue Bedrohungen und Änderungen der Infrastruktur erfordern, dass diese Sicherheitsrichtlinien regelmäßig überarbeitet werden, wodurch die Systemhärtung noch arbeitsintensiver wird.

Was ist die Adaptive Anomaly Control?

Die Adaptive Anomaly Control (AAC) ist ein intelligentes Tool zur automatisierten Reduzierung von Angriffsflächen, das die Ausnutzung von Schwachstellen oder übermäßigen Funktionen in einem durch die Kaspersky Endpoint Security-Lösung (KES) geschützten System verhindert. Wichtige Funktionen:

(1) Umfassende effektive Kontrollregeln, die von Experten von Kaspersky erstellt wurden, und auf Daten basieren, die über Techniken des maschinellen Lernens ermittelt werden. Mithilfe von Algorithmen zur Verhaltensanalyse werden neue potentielle Heuristiken verdächtiger Aktionen im System gefunden. Diese Aktionen können jedoch in bestimmten Fällen legitim sein, sodass eine allgemeine Blockierung nicht angewendet werden kann. Die Definition und Feststellung solcher Ausnahmen mithilfe von Experten kann diese potentielle Heuristik in voll funktionsfähige Härtungsregeln umwandeln.

Ein typisches Beispiel für verdächtiges Verhalten ist der Start eines Programms durch einen Systemprozess: beispielsweise Windows Session Manager, Local Security Authority Process oder Windows Start-Up Application. Es gibt Situationen, in denen dies eine legitime Aktion ist, z. B. beim Starten des Windows-Betriebssystems. Die Aufgabe der Experten besteht darin, diese Bedingungen zu identifizieren und dann eine Kontrollregel zu erstellen, die die Ausführung von Programmen durch einen Systemprozess blockiert – jedoch mit entsprechenden Ausnahmen, die den ordnungsgemäßen Betrieb des Betriebssystems ermöglichen.

(2) Automatisierte Anpassung (Smart-Modus), die auf der Analyse der Benutzeraktivität basiert. Dadurch wird die Notwendigkeit einer manuellen Konfiguration von Kontrollregeln deutlich reduziert. Zunächst arbeitet das AAC-Modul im Lernmodus und erfasst statistische Daten zu Kontrollregeln, die über einen bestimmten Zeitraum ausgelöst wurden. So wird ein Modell der normalen Aktivität für einen Benutzer oder eine Gruppe erstellt (legitimes Szenario). Daraufhin aktiviert das System im Präventionsmodus nur die Regeln, die ungewöhnliche Aktionen für dieses Gruppen- oder Benutzerszenario blockieren. Sollte sich aus irgendeinem Grund ein normales Aktivitätsmuster ändern, kann das AAC-Modul zurück in den Lernmodus versetzt werden, um ein neues Szenario zu erstellen.

Beispielsweise ist das Vorhandensein von JavaScript im Archiv ein Indikator für einen gefährlichen E-Mail-Anhang: Mitarbeiter der Finanzabteilung müssen solche Archive niemals legitim austauschen. Unter Entwicklern wiederum sind solche Situationen alltäglich. Wenn die Adaptive Anomaly Control diese unterschiedlichen Szenarien also erkennt, blockiert sie die Anhänge mit aktivem Inhalt für eine Benutzergruppe (Finanzabteilung), aber nicht für eine andere Gruppe (Entwickler).

(3) Feineinstellung. Neben dem automatischen Modus kann der Systemadministrator die Aktivierung von Blockierungsregeln steuern und individuelle Ausnahmen erstellen, wenn das zu blockierende Verhalten Teil einer legitimen Aktivität bestimmter Benutzer, Programme oder Geräte sein könnte.

So ist eine Regel, die die Ausführung von Dateien mit doppelter Erweiterung (z. B. img18.jpg.exe) blockiert, in 99 % aller Fälle richtig. In manchen Systemen werden die doppelten Dateierweiterungen jedoch auf legitime Weise verwendet (update.txt.cmd). In diesem Fall kann der Administrator einfach eine Ausnahme dafür hinzufügen.

(4) Zusammenspiel mehrerer Werkzeuge. Das Adaptive Anomaly Control-Modul reduziert nicht nur die Angriffsfläche und das Bedrohungsrisiko, einschließlich Zero-Day-Bedrohungen, sondern verbessert auch die kollaborative Leistung der Kaspersky Endpoint Security als Teil einer mehrschichtigen Sicherheitsplattform. Die Auslösung einer bestimmten AAC-Regel kann als Signal zur näheren Untersuchung eines verdächtigen Objekts durch andere Schutzmodule oder Experten dienen.

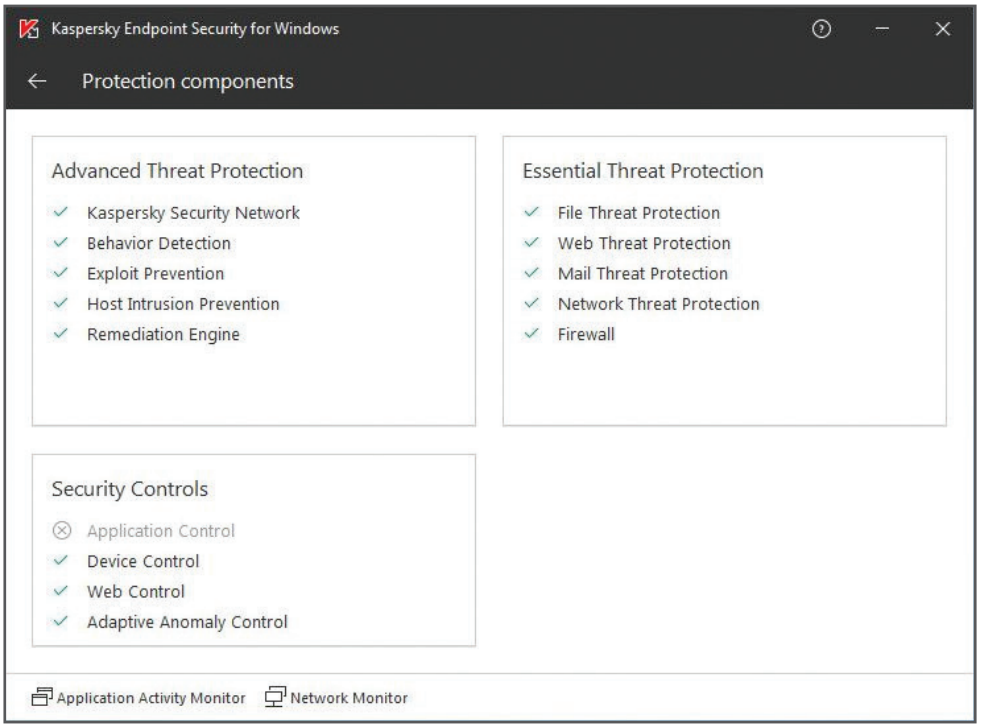
Im Detail: Adaptive Kontrollregeln

Die Kontrollregeln der Adaptive Anomaly Control werden von Kaspersky-Experten mithilfe von Verhaltensanalyse-Algorithmen erstellt. Neue Regeln werden regelmäßig über die Datenbank-Updates der Kaspersky Endpoint Security zur AAC-Datenbank hinzugefügt. Die Regeln werden in der Datenbank in Gruppen wie „Ungewöhnliche Programmaktivität", „Verwendung von WMI" oder „Aktivität von Script Engines und Frameworks" gesammelt. Die folgende Tabelle enthält einige grundlegende Kontrollregeln einer aktuellen Version von KES:

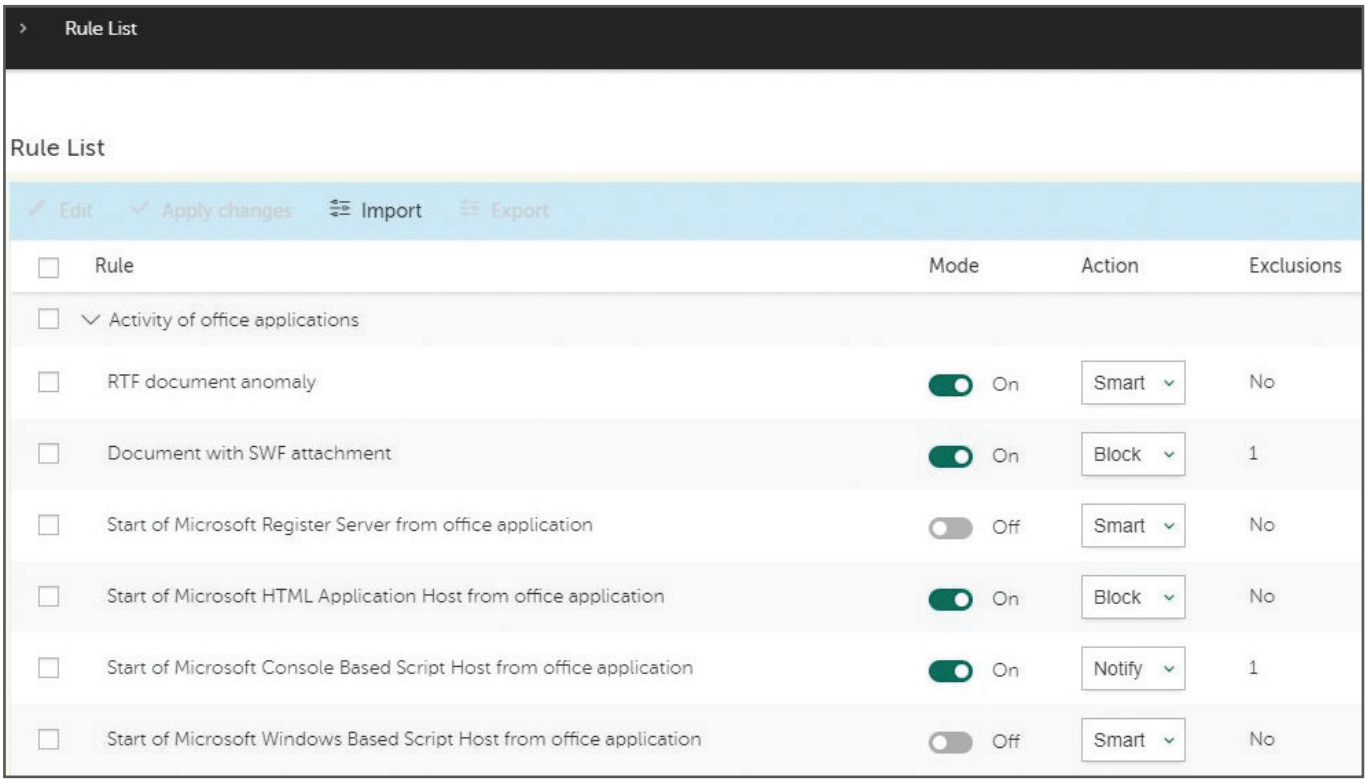
Regelname	Zu blockierende Aktion
Anomalie in RTF-Dokument	Öffnen eines RTF-Dokuments, das für das RTF-Format typische Anomalien enthält, durch das Programm Microsoft Word
Dokument mit SWF-Anhang	Öffnen eines Dokuments mit einem SWF-Anhang, der Code enthält, durch ein Office-Programm
Start des Microsoft Register Servers aus einem Office-Programm	Starten des Microsoft Register Servers durch ein Office-Programm
Start des Microsoft HTML Application Hosts aus einem Office-Programm	Starten des Microsoft HTML Application Hosts aus einem Office-Programm
Start des Microsoft Console Based Script Hosts aus einem Office-Programm	Starten des Microsoft Console Based Script Hosts aus einem Office-Programm
Start des Microsoft Windows Based Script Hosts aus einem Office-Programm	Starten des Microsoft Windows Based Script Hosts aus einem Office-Programm
Start des Microsoft Windows Command Processors aus einem Office-Programm	Starten des Microsoft Windows Command Processors aus einem Office-Programm
Start von Microsoft PowerShell aus einem Office-Programm	Starten von Windows PowerShell aus einem Office-Programm
Start einer eingebetteten Datei aus einem Office-Programm	Ausführen einer in ein Office-Dokument eingebetteten ausführbaren Datei
Start des Microsoft HTML Application Host aus WMI	Ausführen von Windows PowerShell aus Windows Management Instrumentation (WMI)
Start von Microsoft PowerShell aus WMI	Ausführen von Windows PowerShell aus Windows Management Instrumentation (WMI)
PowerShell führt externen Code aus	Ausführen von externem (heruntergeladenen) Code durch PowerShell-Skripts
PowerShell-Skript führt unbekannten dynamischen Code aus	Ausführen von unbekanntem dynamischem Code (bei Ausführung generiert) durch PowerShell-Skript
PowerShell führt verschleierten Code aus	Ausführen von verschleiertem Code durch PowerShell-Skript
PowerShell ruft native API auf	Aufrufen der nativen API (Programmierschnittstelle) durch PowerShell-Skript
Für den Ordner ungewöhnliche Datei	Ausführen des Programms und/oder Skripts aus einem Standard- oder Systemverzeichnis, das solche ausführbaren Dateien in der Standardkonfiguration nicht enthält
Systemdatei in einem Nicht-Systemordner	Ausführen des Programms mit dem Namen eines Systemprozesses (z. B. explorer.exe) aus einem Nicht-Systemverzeichnis
Nicht vertrauenswürdiges Programm mit einem systemähnlichen Namen	Ausführen eines nicht vertrauenswürdigen Programms mit einem Namen, der dem Namen eines Systemprozesses ähnelt (z. B. explorer. exe)

Adaptive Anomaly Control in der Kaspersky Endpoint Security-Oberfläche

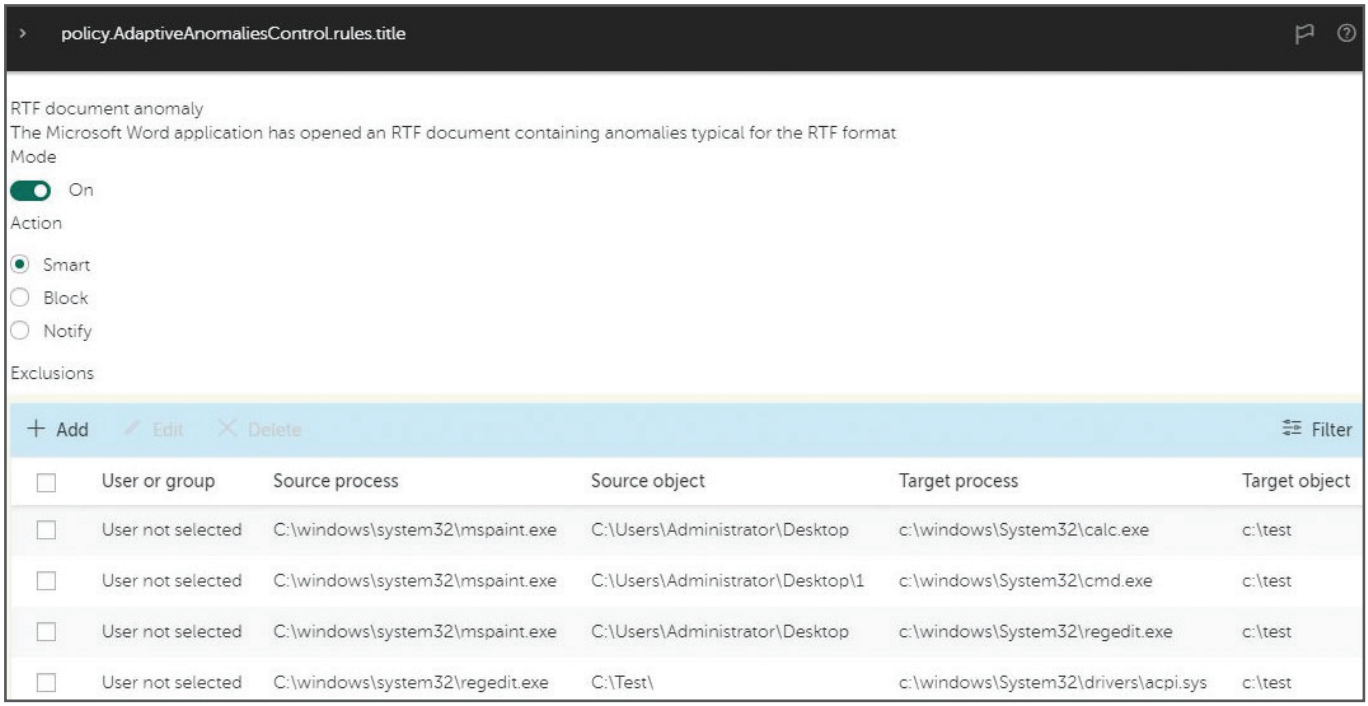
Die AAC-Moduleinstellungen finden Sie im Sicherheitskontrollenmenü:



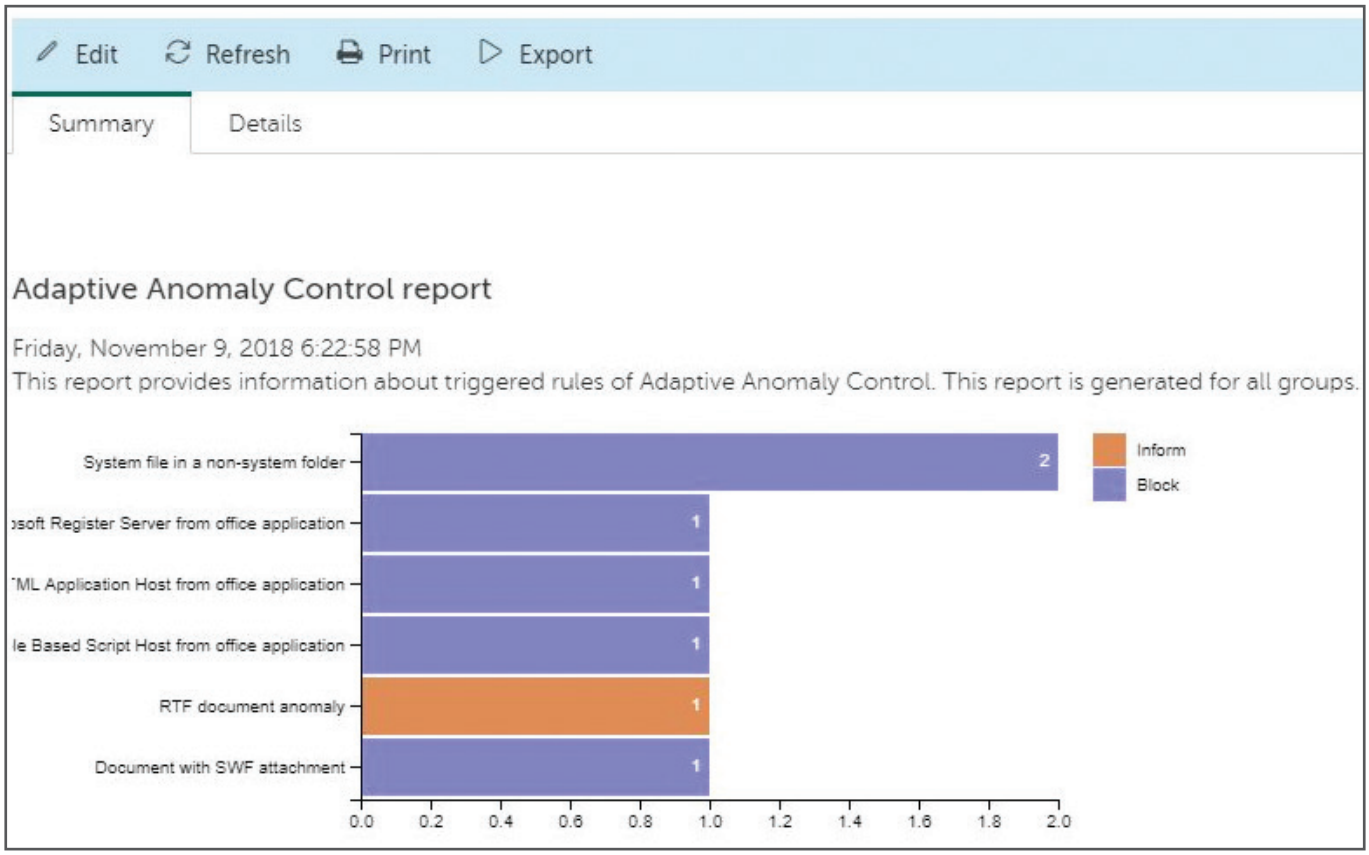
Unten sehen Sie eine Liste der angewendeten AAC-Regeln mit den Parametern „Status“ (Mode), „Aktion“ (Action) und „Ausnahme“ (Exclusion):



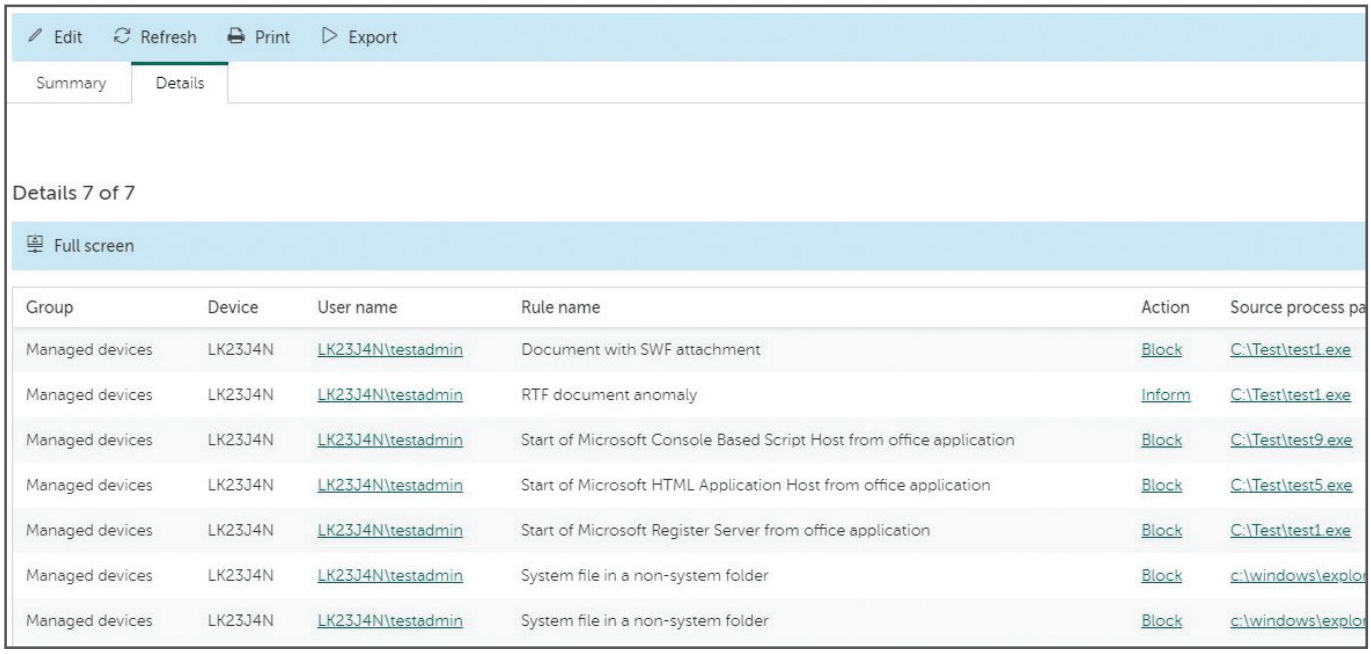
Feineinstellung einer bestimmten AAC-Regel – wählen Sie „Aktion“ (Action) aus und legen Sie hier eine Liste der „Ausnahmen“ (Exclusion) fest:



Hier können Sie die am häufigsten ausgelösten AAC-Regeln für alle Benutzergruppen anzeigen:



Das detaillierte Protokoll der Adaptive Anomaly Control-Regeln, die auf verschiedene Benutzergruppen angewendet werden:



Group	Device	User name	Rule name	Action	Source process pa
Managed devices	LK23J4N	LK23J4N\testadmin	Document with SWF attachment	Block	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	RTF document anomaly	Inform	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft Console Based Script Host from office application	Block	C:\Test\test9.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft HTML Application Host from office application	Block	C:\Test\test5.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft Register Server from office application	Block	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	System file in a non-system folder	Block	c:\windows\explor
Managed devices	LK23J4N	LK23J4N\testadmin	System file in a non-system folder	Block	c:\windows\explor

Zusammenfassung

Die Reduzierung der Angriffsfläche ist eine sehr effektive und vergleichsweise kostengünstige Methode, um Ihre Systeme vor einer Vielzahl von Bedrohungen, sowohl bekannten als auch völlig neuen, zu schützen. Eine allgemeine Härtung kann jedoch auch ein zu grobes Instrument sein. Die Adaptive Anomaly Control ermöglicht die Feineinstellung dieses Instruments durch die Anwendung von Techniken des maschinellen Lernens. So wird der manuelle Arbeitsaufwand von Systemadministratoren und Sicherheitsexperten minimiert und sichergestellt, dass jeder Benutzer geschützt ist, ohne dass einem Benutzer Unannehmlichkeiten entstehen. Mit dieser Technologie können Sie die Systemhärtung bis auf die Ebene einzelner Benutzer anpassen oder maßgeschneiderte Zugriffsregeln auf die verschiedenen Bereiche Ihres Unternehmens anwenden, um deren unterschiedliche Anforderungen zu berücksichtigen. Diese intelligente, automatisierte Feineinstellung der Blockierungsregeln fügt dem Technologiestack von Kaspersky Endpoint Security eine weitere Schutzebene hinzu, die Ihnen in einer gefährlichen und unberechenbaren Cyberwelt eine leistungsstarke Abwehr bietet.

Cyber Threats News: **https://de.securelist.com**
IT Security News: **https://www.kaspersky.de/blog/b2b/**
IT-Sicherheit für wachsende Unternehmen: **kaspersky.de/business**
IT-Sicherheit für Unternehmen: **kaspersky.de/enterprise**

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Weitere Informationen finden Sie unter kaspersky.de/transparency.

Getestet.
Transparent
Unabhängig.