# Bewertung der Effektivität der untersuchten Antimalware-Lösungen

*Klaus Jochem*

*Unternehmensberatung*

*2021-05-06*

## Warum ist die Bewertung der Effektivität von Lösungen notwendig?

RoSI dient zum Vergleich verschiedener Sicherheitslösungen, die ein Risiko um einen Prozentsatz $S_R$% reduzieren. In diesem Dokument begründe ich „meine Einschätzung" zur Effektivität der untersuchten Antimalware-Lösungen. Die Einschätzung kann durch Anpassung der Werte in Excel-Dokument „Rosi-Vergleich-Lösungen-Public.xlsx" Blatt „Effektivität Security Maßnahmen" leicht angepasst werden.

Ist die Effektivität der Lösung kleiner als $S_R$%, so ist die Lösung nicht geeignet, das Risiko unter die Risikotragfähigkeit der Organisation zu reduzieren. In diesem Fall muss die Lösung von der Betrachtung ausgeschlossen werden. Alternativ kann die Lösung um weitere Funktionen oder eine weitere Lösung ergänzt werden, um die erforderliche Reduktion zu erreichen.

Hier werden die individuellen Lösungen bewertet. Kombinationen von Lösungen werden auf Blatt „Effektivität Security Maßnahmen" bewertet.

| | | Antivirus, Pattern basiert | Application Whitelisting, System-basiert | Application Directory Allow Listing |
|---|---|---|---|---|
| *Malware Typ* | *Label* | *AV.Trad* | *AWL.SYS* | *AWL.DIR* |
| Bekannte Malware, Externe Angriffe | Bekannt, Extern | 85% | 80% | 36% |
| Bekannte Malware, Interne Angriffe[1)] | Bekannt, Intern | 85% | 80% | 36% |
| Neuartige Malware, Externe Angriffe | Neuartig, Extern | 10% | 80% | 36% |
| Neuartige Malware, Interne Angriffe[1)] | Neuartig, Intern | 10% | 80% | 36% |
| Modifizierte 3rd-party Software | 3rd Party | 0% | 0% | 0% |
| *Effektivität* | *Mittelwert* | *38%* | *64%* | *29%* |

*Tabelle 1: Übersicht individuelle Effektivität der untersuchten Lösungen*

1) Angriff erfolgt etwa über kompromittierte Speichermedien.

# Bewertung der Effektivität der untersuchten Antimalware-Lösungen

## Bewertung der Effektivität

*Hinweis*: Eine Grundhärtung ist bei allen betrachteten Lösungen erforderlich. Dazu gehört etwa der Verzicht auf das Arbeiten mit permanenten Admin-Rechten, um das Schadensausmaß zu begrenzen.

### AV.Trad: Antivirus, pattern based

| Label | Effektivität | Bewertung |
|---|---|---|
| Bekannt, Extern | 85% | Malwarepattern-Updates benötigen Zeit zur Installation, da sie auf viele Systeme verteilt werden müssen. Bei der Verteilung treten Fehler auf, die das Sicherheitsniveau des Netzwerkes reduzieren. Zudem sind zur vollen Entfaltung der Wirksamkeit häufig Engine-Updates erforderlich. Ausnahmen vom Scan, Einschränkungen in der Scan-Tiefe bei Archiven usw. reduzieren die Effektivität zusätzlich. |
| Bekannt, Intern | 85% | Siehe „Bekannt, Extern“. |
| Neuartig, Extern | 10% | Bei neuartiger Malware keine Schutzwirkung, da kein Pattern vorhanden ist. Mutationen etc. werden in der Regel erkannt. |
| Neuartig, Intern | 10% | Siehe „Neuartig, Extern“. |
| 3rd Party | 0% | Keine Schutzwirkung, da die Malware als gutartiges Programm getarnt ist. |
| Gesamt | 38% | Mittelwert |

### AWL.SYS: Application Whitelisting, System-basiert

| Label | Effektivität | Bewertung |
|---|---|---|
| Bekannt, Extern | 80% | Sehr hohe Effektivität, da alles, was nicht zum Zeitpunkt der Erzeugung der Whitelist bekannt ist, blockiert wird, unabhängig von Kontext (User- und System-Kontext) und der Benutzerinteraktion. Einschränkung der Effektivität durch Ausnahmen oder bewusster Deaktivierung aufgrund von Einschränkungen der Benutzererfahrung.<br>Kritische Einschränkung durch Updates: Wird über einen Update Malware verbreitet, so wird diese in die Whitelist aufgenommen, kann also ausgeführt werden. Deshalb sollte eine Application-Whitelisting-Lösungen (AWL) immer durch Antivirus-Lösungen, Virenschleusen, oder Firewalls mit IDS/IPS ergänzt werden. |
| Bekannt, Intern | 80% | Siehe „Bekannt, Extern“. |
| Neuartig, Extern | 80% | Siehe „Bekannt, Extern“. Siehe *Hinweis 1*, unten. |
| Neuartig, Intern | 80% | Siehe „Bekannt, Extern“. Siehe *Hinweis 1*, unten. |
| 3rd Party | 0% | Keine Schutzwirkung, da die Malware aus einer vertrauenswürdigen Quelle stammt. Auch signatur-basierte Verfahren sind wirkungslos, da das Schadprogramm im ungünstigsten Fall die gültige Signatur des Lieferanten erhält. Prominentes Beispiel: SolarWinds. |
| Gesamt | 64% | Mittelwert |

# Bewertung der Effektivität der untersuchten Antimalware-Lösungen

*Hinweis 1*: Application-Whitelisting-Lösungen (AWL) blockieren Malware erst bei der Ausführung. Dieses Verhalten ist ungewohnt, denn Anwender und IT-Security-Spezialisten sind seit 30 Jahren darauf eingestellt, dass Malware-behaftete Objekte bei jeder Aktion (Lesen, Schreiben, Attribute ändern) identifiziert und blockiert werden. Kritisch ist dieses Verhalten, wenn keine Antimalware-Lösung installiert ist. Beim Kopieren eines Malware-behafteten Objektes auf ein externes Speichermedium erfolgt keine Überprüfung bzw. Warnung. Wird das Speichermedium in einer Umgebung weiterverarbeitet, die nicht mit einer AWL geschützt ist, so kann das Zielnetzwerk kompromittiert werden. Dieser Effekt wird hier nicht berücksichtigt.

## AWL.DIR: Application Directory Allow Listing

| Label | Effektivität | Bewertung |
|---|---|---|
| Bekannt, Extern | 36% | Malware, die im User-Kontext ins System gelangt, wird blockiert. Dazu gehören etwa Drive-by-Downloads aus dem Internet, PuA (Potentially unwanted Applications), als Office-Dokumente getarnte Schadprogramme (1- und 2-stufige Dropper-Malware), etc.<br>Schadprogramme, die im Systemkontext in den Computer gelangen, werden in der Regel nicht blockiert. Dazu gehören etwa WannaCry oder NotPetya.<br>Ca. 36% der in der NIST NVD gelisteten Schwachstellen (Zeitraum 2016-2020, CVSS V3) benötigen zur Ausnutzung eine Benutzerinteraktion (UI:R). Daher eine Effektivität von 36% angenommen. |
| Bekannt, Intern | 36% | Siehe „Bekannt, Extern“. |
| Neuartig, Extern | 36% | Siehe „Bekannt, Extern“. |
| Neuartig, Intern | 36% | Siehe „Bekannt, Extern“. |
| 3rd Party | 0% | Keine Schutzwirkung, da die Malware aus einer vertrauenswürdigen Quelle stammt und in Systemverzeichnissen installiert ist. Auch signatur-basierte Verfahren sind wirkungslos, da das Schadprogramm im ungünstigsten Fall die gültige Signatur des Lieferanten erhält.<br>Prominentes Beispiel: SolarWinds. |
| Gesamt | 29% | Mittelwert |