**ATP: Livetest gegen Datendiebstahl- und Verschlüsselungs-Malware**

**Bei privaten Nutzern sind oft alle Urlaubsfotos und weitere Erinnerungen verloren – bei Unternehmen steht teils die ganze Existenz auf dem Spiel. Wenn Infostealer oder Ransomware zuschlagen, landen Daten in fremden Händen oder sind professionell hochgradig verschlüsselt. Diese Szenarien sollte eine gute Schutz-Software für private Anwender und Unternehmen verhindern. Aber gelingt das wirklich? Der Advanced Threat Protection – kurz ATP-Test gibt klare Antworten. Denn in diesem Live-Test spielen die Tester 10 sehr gefährliche Angreifer auf die Systeme und beobachten Schritt für Schritt, was passiert. Im aktuellen Test mit 16 Schutzpaketen steckt alles drin: von der perfekten Abwehr bis hin zu Verschlüsselung und Datendiebstahl.**

Wenn ein Infostealer oder eine Ransomware angreift, läuft das Szenario zu Beginn immer recht ähnlich ab. Meist kommt eine Phishing-E-Mail mit einem Angreifer im Gepäck. Kaum auf dem Windows-System gelandet, fallen nach Meinung vieler gleich die Würfel: Der Angriff wird von der Schutz-Software erkannt oder nicht. Aber das stimmt so nicht ganz. Denn auch wenn eine Abwehr-Software im ersten Schritt versagt, heißt das nicht, dass alles verloren ist. Eine gute Security-Software besteht nicht nur aus einer Erkennungs-Engine, sondern hat viele weitere Module, die sich in Sachen Schutz unterstützen und oft in perfekter Zusammenarbeit eine Malware in weiteren Angriffsschritten abwehren.

Das dies funktionieren kann, zeigt der Advanced Threat Protection-Test – kurz ATP-Test. Er verfolgt in 10 Live-Szenarien Schritt für Schritt, wie 5 Exemplare Ransomware und 5 Infostealer die Windows-Test-Systeme angreifen. Dabei ist die Erkennung, dass die Malware auf dem System landet oder ausgeführt wird, nur der erste Abwehrschritt. Interessant ist, wenn weitere Module trotz einer Nichterkennung die Malware in späteren Schritten aufhalten und zu guter Letzt abwehren. Manchmal bleibt ein vernachlässigbarer Schaden, etwa eine übrige Text- oder Bilddatei. Allerdings gibt es auch Fälle, bei denen der Abwehrkampf bis zuletzt tobt und einzelne Daten gestohlen oder verschlüsselt werden. Aber auch das ist im Ernstfall noch ein annehmbares Ergebnis im Vergleich zu einem Totalverlust.

**16 Security-Lösungen im ATP-TEST**

Dem Test stellen sich 8 Pakete für private Anwender und 8 Endpoint-Lösungen für Unternehmen. Alle Produkte wurden im März und April 2025 unter Windows 10 Professional untersucht.

Die Pakete für Anwender kommen von Avast, AVG, Avira, F-Secure, Kaspersky, McAfee, Microsoft und Norton. Die Endpoint-Lösungen von Acronis, Avast, Kaspersky (mit 2 Versionen), Microsoft, Microworld, Trellix und WithSecure.

In der Tabelle ist jeder Lösung ein Schutz-Score zugewiesen – maximal 35 Punkte sind möglich. Jede komplett abgewehrte Ransomware bringt bis zu 3 Punkte, Infostealer bis zu 4 Punkte. Bei den jeweils 5 Varianten pro Angriffstyp kann es in den insgesamt 10 Szenarien auch halbe Punktzahlen geben.

Den Ablauf der Abwehraktionen beschreibt das Labor in einer Matrix nach dem MITRE ATT&CK-Standard. Wenn ein Produkt den Angreifer nicht sofort erkennt, können weitere Abwehraktionen greifen und so den Angriff stoppen. Der Test zeigt genau, bei welchem Schritt das der Fall ist – oder auch nicht.

**Neueste Angriffstechniken im Einsatz**

Im aktuellen März-April-ATP-Test kommt eine besondere Angriffstechnik zum Einsatz, die alle Malware-Exemplare in den 10 Szenarien im Labor ausnutzen:

**MSBuild (Microsoft Build Engine):** Das vertrauenswürdige Windows-Tool gehört zum .NET Framework und Visual Studio. Mit seiner Hilfe lassen sich aus Projektdateien (.proj, .csproj usw.) ausführbare Anwendungen erstellen (kompilieren).

Angreifer fügen allerdings gefährlichen Code in eine Projektdatei ein und bieten diese zum Kompilieren durch den Anwender an. Bei diesem Vorgang wird der gefährliche Code als dateilose Malware im Arbeitsspeicher ausgeführt und kann so Schutzmaßnahmen umgehen, da MSBuild als vertrauenswürdige Anwendung gilt.

**ATP: So gut sind die Privatanwender-Produkte**

Im März-April-ATP-Test gibt es bei den Produkten für private Anwender einige negative Überraschungen. Von den 8 untersuchten Paketen liefern nur 3 Produkte eine lückenlose Abwehr in allen 10 Szenarien und erhalten so die maximalen 35 Punkte: Kaspersky, McAfee und Microsoft.

Norton erkennt 9 Angreifer, wobei aber ein Infostealer trotzdem sein Werk vollrichten kann. Das macht 3,5 Punkte Abzug. Die 10. Malware, eine Ransomware, wird nicht bemerkt – weitere 3 Punkte Verlust. Norton erhält für den Schutz-Score noch 28,5 Punkte.

Für die Pakete von Avast, AVG, Avira und F-Secure war es ein harter Test. Alle Pakete erkennen nur 8 von 10 Angreifern. Die Produkte lassen je einen Infostealer und eine Ransomware ohne Gegenwehr passieren. Interessanterweise sind es in allen Fällen die gleichen Malware-Samples. Jedes Produkt verliert so insgesamt 7 Punkte und alle verzeichnen am Ende 28 von 35 Punkten in ihrem Schutz-Score.

Die untersuchten Produkte verdienen alle das AV-TEST-Zertifikat „Advanced Certified“, da 75 Prozent der maximalen 35 Punkte (26,5 Punkte) erreicht werden.

**ATP: So gut sind die Unternehmens-Produkte**

Die Lösungen für Unternehmen schließen den Test zwar wesentlich besser ab als die Privatprodukte, aber auch nicht ohne Probleme. Die 5 Produkte von Acronis, Kaspersky (beide Versionen), Microsoft und Microworld beenden den Test fehlerfrei und verbuchen die vollen 35 Punkte für ihren Schutz-Score.

Das Endpoint-Paket von WithSecure registriert zwar ebenfalls alle 10 Angreifer, hat aber im Nachgang Probleme. Den bereits identifizierten Infostealer stoppt es erst in weiteren Schritten. Das kostet einen Punkt und es bleiben 3 von 4 Punkten. Auch bei einer Ransomware gibt es ein Problem und den Verlust weiterer Punkte. Auch hier wird der Angreifer erkannt, aber nicht gleich gestoppt. Das Produkt von WithSecure schafft das erst in späteren Schritten. In der Abrechnung bleiben damit für den Schutz-Score von WithSecure 33 von 35 Punkten.

Die Endpoint-Lösung von Trellix spürt 9 von 10 Angreifern auf. Während ein Infostealer unerkannt sein Werk verrichten kann, wird eine Ransomware entdeckt, aber nicht weiter aufgehalten. Am Ende ist das Testsystem verschlüsselt. Für Trellix bleiben so 28,5 von 35 Punkten.

Die Business-Lösung von Avast wehrt 8 von 10 Angreifern ohne Einschränkungen ab. Bei einem Infostealer und einer Ransomware muss die Lösung passen und die Angreifer übernehmen ungestört die Testsysteme. Es bleiben 28 von 35 Punkten für den Schutz-Score.

Alle geprüften Lösungen erfüllen die Vorgaben für das Test-Zertifikat „Advanced Approved Endpoint Protection“, da sie 75 Prozent der 35 Punkte (26,5 Punkte) als Schutz-Score erreichen. Lediglich Acronis erhält das Zertifikat nicht, denn dieses bleibt Produkten vorbehalten, [die auch im regulären Monatstest zertifiziert sind und dort die Kriterien erfüllen](https://www.av-test.org/de/antivirus/unternehmen-windows-client/).

**Fazit: Harter ATP-Test hinterlässt Spuren**

Bei den Produkten für Endanwender lassen sich teils herbe Punktverluste in der Tabelle ablesen. Dass es dennoch fehlerfrei in Sachen Sicherheit geht, beweisen die Pakete von Kaspersky, McAfee und Microsoft. Sie schließen den Test mit Bestwerten ab: 10 erkannte und abgewehrte Angreifer und 35 Punkte im Schutz-Score.

Das Ergebnis bei den Unternehmensprodukten ist deutlich besser, aber weit entfernt von perfekt. Acronis, die beiden Kaspersky-Versionen, Microsoft und Microworld arbeiten völlig fehlerfrei und verdienen so die maximalen 35 Punkte für den Schutz-Score.

Einige Produkte bemerken zwar die Angreifer im jeweiligen Szenario, verhindern aber erst in weiteren Schritten das desaströse Werk der Malware. Umgekehrt gelingt die Abwehr manchmal nicht, obwohl die Schadsoftware bereits identifiziert ist.

Dennoch beweisen viele der geprüften Produkte, dass die Entwicklerteams der Security-Unternehmen einen guten Job machen und den Angreifern weiterhin einen entscheidenden Schritt voraus sind.

Ein Bild, das Text, Screenshot, Software, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Security-Pakete für Privatanwender im ATP-Test**

Im aktuellen Advanced Threat Protection-Test unter Windows 10 sind nicht alle Security-Lösungen den Angreifern gewachsen

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Endpoint-Lösungen im ATP-Test**

Bei den Schutzlösungen für Unternehmen halten 5 der 8 untersuchten Lösungen in allen 10 Szenarien den Angriffen stand

**Die 10 Testszenarien**

Alle Angriffsszenarien sind dokumentiert nach dem Standard der MITRE ATT&CK-Datenbank. Die einzelnen Unterpunkte, z.B. „T1566.001,“ stehen in der MITRE-Datenbank für „Techniques“ unter „Phishing: Spearphishing Attachment“. Jeder Testschritt ist so unter Fachleuten definiert und lässt sich nachvollziehen. Zusätzlich sind alle Angriffstechniken erklärt und wie dabei die Malware zum Zuge kommt.