Schutz vor noch unbekannten Viren

Das Katz- und Mausspiel zwischen Virenschreibern und Virenjägern dauert nun schon über 20 Jahre an. Taucht ein neuer Schädling auf, wird die Virensignatur identifiziert und neutralisiert. Dieses definitionsbasierte Schutzmodell steht vor dem Problem, nur reagieren zu können. Mit F-Secure DeepGuard, ein Host-basiertes Intrusion Prevention System (HIPS), gibt es nun eine neue Waffe im Kampf gegen das Eindringen von noch unbekannter Malware.

Wie wirkungsvoll Antivirensoftware vor Computerschädlingen schützen kann, hängt tatsächlich fast völlig von der Aufmerksamkeit der Benutzer ab. Wenn die Benutzer Infizierungen nicht erkennen – zum Beispiel, weil die Malware Rootkits und ähnliche Techniken nutzen, um so lange wie möglich unentdeckt zu bleiben – erhalten die Virenschutzlabore keine Virenmuster und die Bereitstellung eines Gegenmittels wird behindert. Auch der richtige Zeitpunkt ist entscheidend. Je mehr Zeit zwischen dem Auftreten von Malware und dem Eingang des Virenmusters im Labor vergeht, desto grösser wird die Menge der infizierten Computer sein. Antivirensoftware ist daher unfähig, Schutz vor neuen und unbekannten Bedrohungen zu bieten.

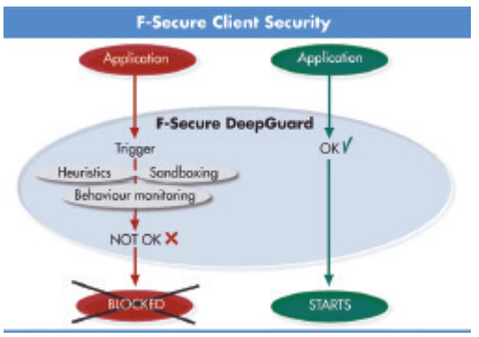
F-Secure DeepGuard – Die perfekte Ergänzung zu Antivirensoftware

HIPS stellt heutzutage eine notwendige Ergänzung zu Antivirensoftware dar und spiegelt eine moderne Entwicklung im Schutz gegen Malware wider. Im Laufe der Entwicklung der Antivirensoftware haben sich kriminelle Virenautoren angepasst und greifen nun verstärkt gezielt an. Es gibt beispielsweise viele verschiedene Hintertüren oder Bots, die dazu dienen, in ein System einzudringen. Einige dieser Malware-Varianten werden nur an eine einzige Organisation oder manchmal sogar nur an einen einzigen Benutzer gesendet. In diesen Fällen werden häufig Social-Engineering-Tricks angewandt (z.B. gezielte E-Mails mit individuellem Inhalt), die die Wahrscheinlichkeit erhöhen, dass die Malware installiert wird.

Antivirensoftware und HIPS ergänzen sich perfekt und bieten so zuverlässigen Schutz gegen bekannte und neue Malware. HIPS ist ein Behaviour Blocker und fungiert im Endeffekt als Firewall zwischen dem Betriebssystem und Anwendungen. Wenn also eine Anwendung andere Schutzmassnahmen durchdringt und versucht, dem Computer potenziellen Schaden zuzufügen, reagiert HIPS und isoliert das Problem.

Der letzte Schutzwall

F-Secure DeepGuard kombiniert HIPS mit moderner Heuristik. Als letzter Schutzwall verhindert diese innovative Technologie Beeinträchtigungen des Systems und wehrt Eindringlinge ab, selbst wenn die Malware nicht von der Antivirensoftware erkannt wird. Wenn eine Anwendung eine potenziell gefährliche Aktion ausführt, wird sie zunächst überprüft. Vertrauenswürdige Anwendungen können fortfahren, sind sie nicht vertrauenswürdig, werden sie blockiert und der Anwender alarmiert.
DeepGuard wird immer gestartet, wenn der Computer hochgefahren wird, und beginnt,



die Betriebssystemprozesse zu kontrollieren. Jede Anwendung muss diese Überwachung durchlaufen und benötigt die Zulassung von DeepGuard oder die des Benutzers, um auf das Betriebssystem zugreifen und die gewünschten Aktionen ausführen zu können. Die neuartige Schutztechnologie überwacht vor allem die Teile des Betriebssystems genau, die von bösartigen Programmen für gefährliche Aktionen verwendet werden könnten.

Schlägt F-Secure DeepGuard an, überprüft eine moderne künstliche Intelligenz, ob das betroffene Programm bösartig ist und handelt dementsprechend. Jede Entscheidung wird gespeichert. Dies minimiert die Anzahl der Analysevorgänge, die die Technologie durchführen muss, und bringt Transparenz für den Anwender mit sich.

Wenn zu einer Anwendung noch keine Entscheidung des Benutzers vorliegt und DeepGuard das Programm nicht erkennt, analysiert die künstliche Intelligenz zuerst das Zielprogramm und untersucht es auf Anomalien und Zeichen für gefährliche Absichten. Mit Hilfe eines Sandbox-basierten heuristischen Antivirenmoduls wird zusätzlich ein Scan ausgeführt, um das Zielprogramm nach der Gefährdungsstufe in eine von vier Kategorien einzuordnen:

- Malware – Eindeutig bösartig. Der Anwender erhält eine Antivirenwarnung.
- Rot – Programme, die eindeutig versuchen, gefährliche Aktionen auszuführen, werden blockiert.
- Gelb – Programme, die nicht eindeutig bösartig sind, benötigen eine einmalige Eingabe durch den Benutzer, um die Vorgehensweise festzulegen.
- Grün – Alle legitimen Programme, die automatisch Aktionen durchführen dürfen.

Die leistungsstarke künstliche Intelligenz und das fortschrittliche heuristische Modul ermöglichen es F-Secure DeepGuard, den Benutzer wirkungsvoll vor unbekannter und undefinierter Malware sowie gegen jegliche Eindringversuche der Hacker zu schützen.

Mika Ståhlberg