PRESSEINFORMATION

FKIE-Forscher entdecken Methode zur Täuschung von Sandboxen

In vielen Unternehmen kommen als Teil des IT-Sicherheitskonzeptes sogenannte Sandboxen zum Einsatz: Ihre Aufgabe ist es, die Sicherheit im Unternehmensnetzwerk zu erhöhen und eine Art sichere Testumgebung zur Analyse anzubieten. Doch das Ziel der Sandboxen wird nicht immer erreicht: Wissenschaftler vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE haben eine Methode entdeckt, die das Konzept der Sandbox aushebelt.

Anders als bei klassischen Anti-Viren-Lösungen wird bei den Sandboxen eine verdächtige Datei nicht beim Nutzer, sondern auf der Sandbox als dediziertem Testsystem in einer möglichst realistischen Umgebung ausgeführt. Gleichzeitig werden deren Aktionen überwacht. Ziel dieser Methode ist, dass die Sandbox bislang unbekannte Schadsoftware bzw. Malware an ihrem Verhalten erkennt. Darüber hinaus setzen IT-Spezialisten Sandboxen im Rahmen ihrer eigenen Analysen von Malware ein.

Um zu vermeiden, dass ihre Malware erkannt wird, haben die Autoren von Schadsoftware bereits früh begonnen, Gegenmaßnahmen zu implementieren, die eine Analyse deutlich erschweren oder sogar verhindern – man spricht von »Sandbox Evasion«. Meist führt die Schadsoftware dazu zunächst verschiedene Checks aus, um festzustellen, ob sie in einer abgesicherten Sandbox läuft. Werden solche Indizien gefunden, bricht sie die weitere Ausführung ihres Schadecodes ab und wird daraufhin nicht erkannt.

Wissenschaftler am Fraunhofer FKIE haben nun eine neue Form der »Sandbox Evasion« entdeckt: Hierbei führt die Malware zunächst eine »Fake-Aktion« durch. Während diese Fake-Aktion von der Sandbox protokolliert wird, wird die Aktion unbemerkt verändert, sodass die Sandbox eine gutartige statt der bösartigen Aktion protokolliert.

In einer Studie, die vom Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) unterstützt wurde, hat das Fraunhofer FKIE acht Sandbox-Lösungen auf die Reaktion der neuen Form der »Sandbox Evasion« getestet. Unabhängig von der angewandten Sandbox-Technik (usermode-, kernelmode-, hypervisor- oder emulationsbasiert) konnte diese Art der Evasion durchgeführt werden. Von den acht getesteten Sandbox-Lösungen waren vier anfällig, eine weitere partiell anfällig. Bei den übrigen drei Sandbox-Lösungen funktioniert die Evasion nicht und die bösartigen Aktionen wurden von der Sandbox protokolliert.

Redaktion
Silke Wiesemann | silke.wiesemann@fkie.fraunhofer.de | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Fraunhoferstraße 20, 53343 Wachtberg-Werthhoven | www.fkie.fraunhofer.de | Telefon +49 228 9435-103

Die betroffenen Hersteller der Sandboxen wurden über diese Methode zur Täuschung ihrer Systeme informiert. Die Ergebnisse der Studie wurden in einem Bericht dokumentiert, der die technischen Details zu den Schwachstellen erläutert. Gleichzeitig hat das Fraunhofer FKIE ein Tool zum Checken sowie einige anonymisierte Analyse-Reports anfälliger Sandboxen bereitgestellt.

Ansprechpartner

Dr. Elmar Padilla, Abteilungsleiter »Cyber Analysis & Defense« | elmar.padilla@fkie.fraunhofer.de |
Viviane Zwanger, Abteilung »Cyber Analysis & Defense« | viviane.zwanger@fkie.fraunhofer.de |
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Wachtberg |
www.fkie.fraunhofer.de | Telefon: + 49 228 50212-595

Das **Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE** ist in seinem Kern auf die Unterstützung staatlicher Institutionen im Bereich der Äußeren und Inneren Sicherheit ausgerichtet. Herausragende Bedeutung hat die strategische Kooperation mit dem Verteidigungsministerium, dem Bundesamt für Sicherheit in der Informationstechnik und der Bundespolizei. Im Bereich der Wirtschaft fokussiert FKIE auf Sicherheit an Flughäfen und im Luftverkehr, bei Maritimen Systemen und in der IT-Branche. Mit seinen etwa 410 Mitarbeitern an den Standorten Bonn und Wachtberg ist das FKIE ein führendes Institut für anwendungsorientierte Forschung und praxisnahe Innovation in der Informations- und Kommunikationstechnologie sowie im Bereich der menschengerechten Gestaltung von Technik.