noSpamproxy®

Version 13

Informationen zum NoSpamProxy Sandbox-Service

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

Dieses Dokument wurde zuletzt am 06. März 2019 überarbeitet.

Inhalt

Über den NoSpamProxy Sandbox-Service

Bestmöglicher Schutz mit NoSpamProxy®

Der NoSpamProxy® Sandbox-Service ist eine Zusatzoption zu NoSpamProxy® Protection. Er bietet Ihnen neben dem Konzept des Content Disarming und des konsequenten Abweisens bei fehlendem Vertrauen zu Absendern eine weitere Schutzkomponente.

Durch den Einsatz des NoSpamProxy® Sandbox-Service steigt die Wahrscheinlichkeit der Erkennung neuer Viren deutlich. Dies ist möglich, weil der NoSpamProxy® Sandbox-Service Dateien nicht nur in einer einzelnen Sandbox, sondern in einem Sandbox-Array überprüft.

Was ist eine Sandbox?

Eine Sandbox ist ein komplexes System, an das Dateien zur Überprüfung übergeben werden. Anders als bei einem gewöhnlichen Virenscanner wird nicht nur geprüft, ob die Datei bereits als Virus bekannt ist oder nicht. Eine Sandbox führt die Datei aus und beobachtet diese. Man spricht hier von „detonieren“.

Zu diesem Zweck wird ein virtueller Computer installiert und hochgefahren. Anschließend wird die zu überprüfende Datei in diesen virtuellen Computer kopiert und detoniert. Nun beginnt die wichtigste Aufgabe der Sandbox: Sie muss beobachten, was in dem Computer passiert. Aus dem beobachteten Verhalten kann die Sandbox dann Rückschlüsse auf den Malware-Gehalt der Datei ziehen.

Funktionsweise

Prinzip

Die Sandbox analysiert zunächst den Dateityp. In Abhängigkeit vom erkannten Typ provisioniert sie dann mehrere virtuelle Computer, auf denen jeweils unterschiedliche Betriebssysteme und unterschiedliche Applikationsversionen installiert sind - beispielsweise Windows 7 oder 10 und Word 2010 oder Word 2016.

Die Datei wird in jeden virtuellen Computer kopiert und dort detoniert. Das wird gemacht, weil sich Malware in vielen Fällen auf bestimmte Versionen spezialisiert hat oder in unterschiedlichen Versionen unterschiedliches Verhalten zeigt. Im Regelfall werden aber nicht mehr als drei oder vier unterschiedliche Umgebungen eingesetzt, da der Rechenaufwand zu hoch wäre. Darüber hinaus gibt es hierbei Herausforderungen im Hinblick auf die Microsoft-Lizenzierung.

Damit die Sandbox den virtuellen Computer beobachten kann, schlägt sie sogenannte *hooks* ein. Man kann sich das wie ein Mikrofon oder eine Überwachungskamera vorstellen, die in einem Raum installiert werden. Mit Hilfe der *hooks* kann die Sandbox erkennen, was auf der Festplatte des virtuellen Computers geschrieben und gelesen wird. Sie erkennt auch, ob und welche Netzwerkverbindungen wohin aufgebaut werden, welche Änderungen an der Registry oder der Startumgebung vorgenommen werden und vieles mehr.

Wenn beispielsweise beim Öffnen einer Word-Datei Änderungen an der Registry vorgenommen werden oder Dateien von einer Internet-Adresse heruntergeladen werden, ist die Wahrscheinlichkeit hoch, dass es sich um Malware handelt. Wichtig ist hierbei, dass das Ergebnis immer eine Wahrscheinlichkeit ausdrückt. Wenn eine URL aufgerufen wird, die bereits als schlecht bekannt ist, ist die Wahrscheinlichkeit sehr hoch.

Vorgehen

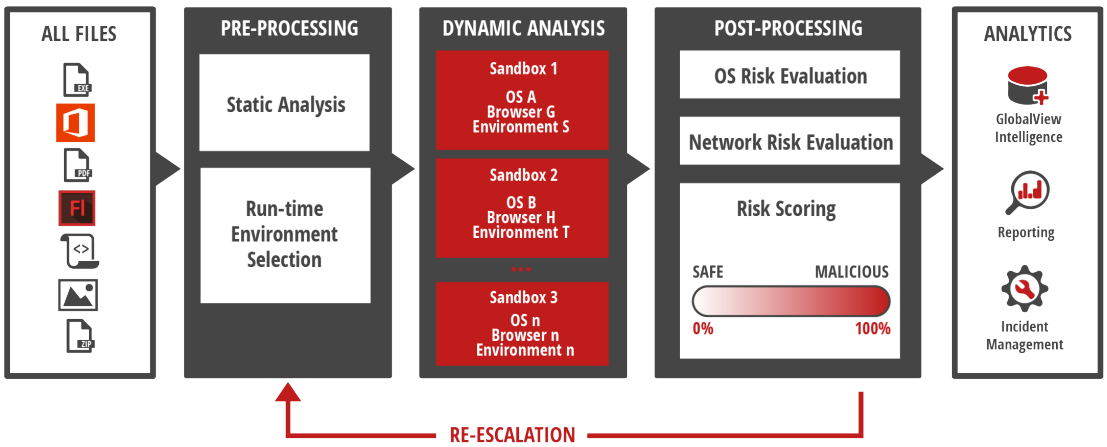
Der NoSpamProxy® Sandbox-Service analysiert Dateien, URLs und den sogenannten *Command & Control-Verkehr*. Letzterer beschreibt den Datenaustausch zwischen einem infizierten Computzer und seinem „Meister“ im Netz, von dem er neue Befehle bekommt.

Bevor eine Datei von NoSpamProxy® in die Sandbox hochgeladen wird, erstellt NoSpamProxy® einen Hashwert und fragt die Sandbox, ob sie den Hash bereits kennt.

Ist der Hash bekannt, wird zudem abgefragt, ob der Hash gut oder böse ist. Man spricht hier von Level 1 (Hashabfrage) und Level 2 (File-Upload).

Die zu prüfenden Dateien werden in unterschiedlichen Sandboxen geprüft, die sowohl auf Basis von virtuellen als auch von physikalischen Computern arbeiten. Deshalb spricht man auch von einem Sandbox-Array. Um den Prüfprozess so effizient wie möglich zu gestalten, wird anhand des Dateityps ein erwartetes Verhalten vorhergesagt (static analysis) und eine auf diese Vorhersage optimierte Umgebung hochgefahren (dynamic analysis). Erst, wenn das erwartete Verhalten nicht eintritt, werden weitere virtuelle Computer provisioniert (post-processing).

Sobald eine Datei oder eine URL als schlecht erkannt wird, wird ein Fingerabdruck des jeweiligen Objekts erstellt und dem Netzwerk unseres Technologiepartners Cyren zur Verfügung gestellt.



Quelle: Cyren

Lizenzierung und Datenschutz

Der NoSpamProxy® Sandbox-Service muss zusätzlich lizenziert werden. Die Lizenz richtet sich nach der Anzahl der Anwender, die durch NoSpamProxy® Protection lizenziert sind. NoSpamProxy® Protection ist die Grundvoraussetzung für die Nutzung des Sandbox-Service. Für den Service wird ein eigener Lizenzschlüssel erstellt, der in die bestehende Lizenz integriert wird.

NoSpamProxy® bietet den Sandbox-Service für den deutschen Markt in einem Rechenzentrum in Deutschland an. Der Dienst wird von unserem langjährigen Technologiepartner Cyren betrieben. Alle NoSpamProxy®-Installationen kommunizieren automatisch mit diesem Rechenzentrum. Keine Datei wird in einem Rechenzentrum außerhalb der Bundesrepublik Deutschland geprüft.

Testbetrieb

Für einen Testbetrieb des Sandbox-Service ist ein entsprechender Lizenzschlüssel erforderlich, der beim Vertriebsteam von NoSpamProxy® erhältlich ist.

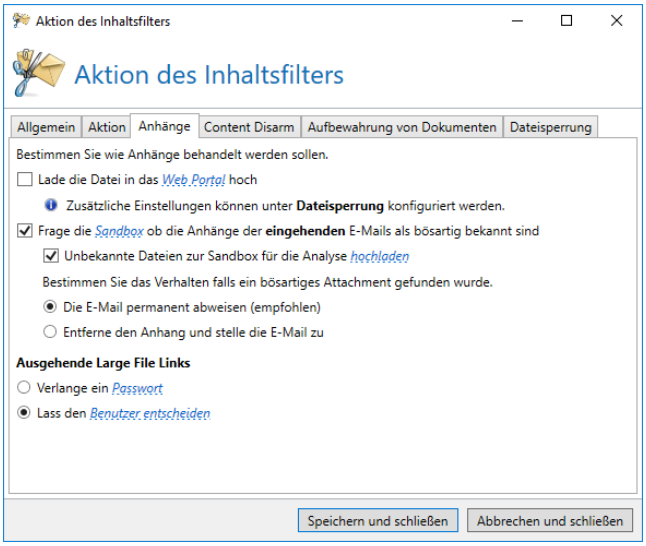
Standardmäßig ist der Testzeitraum auf 30 Tage begrenzt. Die Lizenzanpassung nach dem Kauf erfolgt durch Cyren, die die Testlizenz dann in eine reguläre Lizenz umwandeln.

Aktivieren des Sandbox-Service in NoSpamProxy

Um den NoSpamProxy® Sandbox-Service in NoSpamProxy® zu aktivieren, haben Sie zwei Möglichkeiten:

Anpassen einer vorhandenen Aktion

1. Gehen Sie zu **Konfiguration/Inhaltsfilter/Aktionen des Inhaltsfilters**.
2. Öffnen Sie eine vorhandene Aktion für eingehende E-Mails.
3. Wechseln Sie zur Registerkarte **Anhänge**.



4. Setzen Sie das Häkchen neben **Frage die Sandbox, ob die Anhänge der eingehenden E-Mails als bösartig bekannt sind**.
5. *Optional* Setzen Sie das Häkchen neben **Unbekannte Dateien zur Sandbox für die Analyse hochladen**.

> **HINWEIS:** Ist diese Option aktiviert, werden der Sandbox unbekannte Dateien zur Analyse in die Sandbox hochgeladen.

6. Wählen Sie entweder **Die E-Mail permanent abweisen (empfohlen)** oder **Entferne den Anhang und stelle die E-Mail** zu.

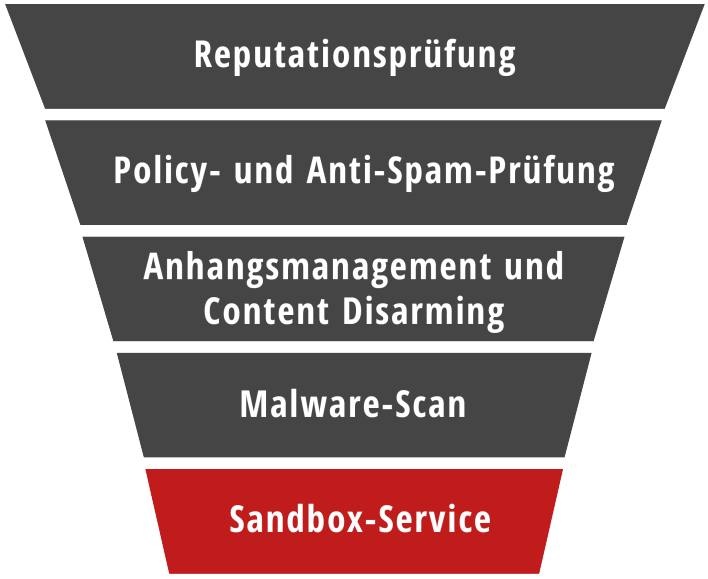
> **HINWEIS:** Der Sandbox-Service ist nur auswählbar, wenn Sie auf der Registerkarte **Aktion** die Option **Erlaube den Anhang** gewählt haben.

Erstellen einer neuen Aktion

1. Gehen Sie zu **Konfiguration/Inhaltsfilter/Aktionen des Inhaltsfilters**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie im Dialogfenster **Allgemein** einen Namen für die neue Aktion ein und wählen Sie **SMTP-E-Mails** aus.
4. Wählen Sie im Dialogfenster **Aktion** die Option **Erlaube den Anhang** aus.
5. Nehmen Sie die Einstellungen für die Sandbox vor, wie oben für die Registerkarte **Anhänge** beschrieben.
6. Nehmen Sie alle weiteren Einstellungen für die neue Aktion wie gewünscht vor.
7. Klicken Sie **Fertigstellen**.

Die angepasste oder neu erstellte Aktion müssen Sie nun per Inhaltsfiltereintrag auslösen.

HINWEIS: Die Anzahl der vollständigen Analysen durch den Sandbox-Service ist pro Anwender und Monat auf 20 limitiert. Die Abrechnung erfolgt nicht anwenderbasiert. Ein Beispiel: Bei 100 Anwendern können insgesamt 2000 vollständige Analysen durchgeführt werden, unabhängig davon, wie viele Analysen die einzelnen Anwender durchführen. Wir empfehlen Ihnen, die Filter in NoSpamProxy® so zu konfigurieren, dass eine Überprüfung durch den Sandbox-Service nur erfolgt, falls E-Mails durch vorgelagerte Filterstufen nicht schon vorher abgelehnt wurden. Bei Überschreiten des Limits können zusätzliche Kosten anfallen.



Überblick über die Filterstufen in NoSpamProxy

Hilfe und Unterstützung

Wir freuen uns, dass Sie sich für NoSpamProxy® entschieden haben!

Bei Fragen zu NoSpamProxy® oder diesem Dokument stehen Ihnen folgende Ressourcen zur Verfügung:

KNOWLEDGE BASE

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

WEBSITE

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

BLOG

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy-Managementkonsole angezeigt.

NOSPAMPROXY-SUPPORT

Unser Support-Team erreichen Sie

- per Telefon unter **+49 5251304-636**
- per E-Mail unter **support@nospamproxy.de**.

Wir wünschen Ihnen viel Erfolg und Spaß mit NoSpamProxy®.