



32Guards Sandbox

Version 15

Rechtliche Hinweise

Alle Rechte vorbehalten. Dieses Dokument und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2023 Net at Work GmbH

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

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 11. DEZEMBER 2024 ÜBERARBEITET.

Inhalt

32Guards Sandbox	1
Lizenzierung und Datenschutz	6
Limitierung der Überprüfungen	7
Testbetrieb	8
32Guards Sandbox konfigurieren	8
Möglichkeit 1: Anpassen einer vorhandenen Aktion	8
Möglichkeit 2: Erstellen einer neuen Inhaltsfilteraktion	10
Hilfe und Unterstützung	16

32Guards Sandbox

I Bestmöglicher Schutz mit NoSpamProxy

Die 32Guards Sandbox ist eine Zusatzoption zu NoSpamProxy Protection. Sie bietet Ihnen neben dem Konzept des Content Disarming und des konsequenten Abweisens bei fehlendem Vertrauen zu Absendern eine weitere Schutzkomponente.

Durch den Einsatz der 32Guards Sandbox steigt die Wahrscheinlichkeit der Erkennung neuer Viren deutlich.

I Was ist eine Sandbox?

Eine Sandbox ist ein komplexes System, an das Dateien zur Überprüfung übergeben werden. Anders als bei einem gewöhnlichen Virenschanner 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.

I Herausforderungen

Einige Virentypen können erkennen, ob sie in einer Sandbox oder auf einem „echten“ Computer ausgeführt werden. Man spricht hier von **Hyper-Evasive Malware**. Dies wird beispielsweise durch das Erkennen der oben erwähnten **hooks** ermöglicht. Die Malware versucht also herauszufinden, ob sie beobachtet wird und in was für einer Umgebung sie gerade ausgeführt wird. Dazu greift sie beispielsweise auf den Arbeitsspeicher zu und beobachtet die dann folgende Reaktion.

Fühlt sich die Malware wohl, wartet sie unter Umständen eine Weile, bevor sie ihre eigentliche Aufgabe ausführt, oder sie wartet auf eine Aktion, die nur ein echter Benutzer tätigen würde. Bei einem Word-Dokument könnte eine Malware abwarten, bis Text eingegeben und der „Speichern“-Knopf gedrückt wird. Auch Mausbewegungen werden durch die Malware erkannt und entsprechend positiv bewertet.

All das muss eine gute Sandbox simulieren können. Das bedeutet auch, dass es genau wie bei konventionellen Virenprogrammen das berühmte Hase- und Igel-Spiel gibt: Die Sandbox-Betreiber versuchen, sich bestmöglich zu tarnen, Malware-Hersteller versuchen, sich bestmöglich umzusehen und abzusichern.

Ein weiteres Problem ist der verwendete Dateityp. Sandboxes können in der Regel alle Arten von ausführbaren Dateien, Office-Dokumente, PDF-Dokumente und ZIP-Archive detonieren, kommen aber in einigen Fällen an ihre Grenzen. So wird zum aktuellen Zeitpunkt kaum eine Sandbox eine AutoCAD-Datei detonieren können.

I 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.

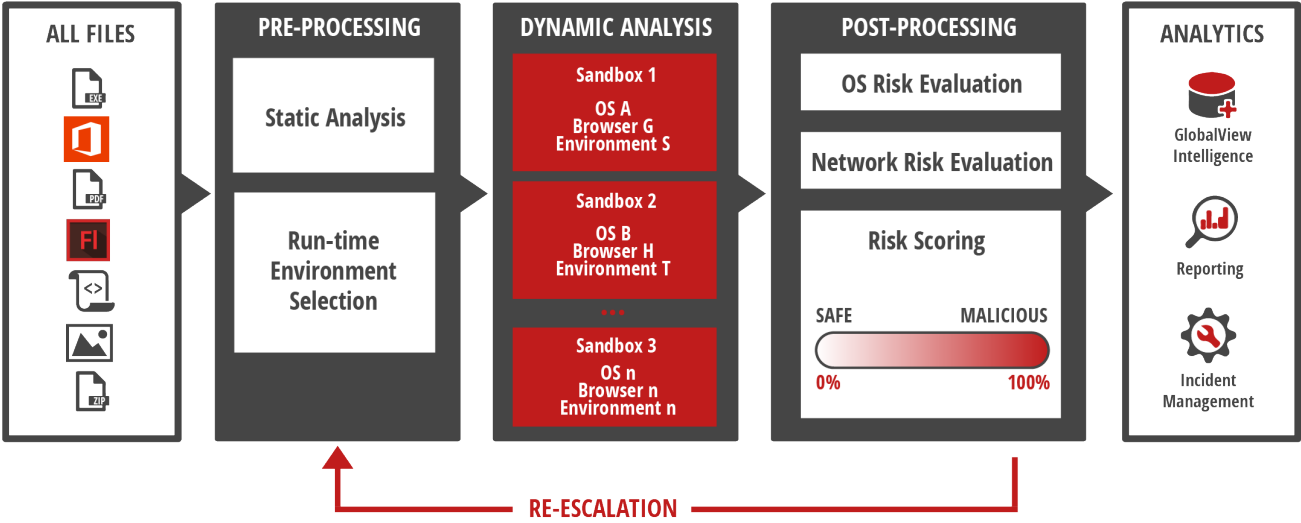
I Vorgehen

Die 32Guards Sandbox analysiert Dateien, URLs und den sogenannten **Command & Control-Verkehr**. Letzterer beschreibt den Datenaustausch zwischen einem infizierten Computer 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 verschlüsselt übertragen und geprüft. 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.



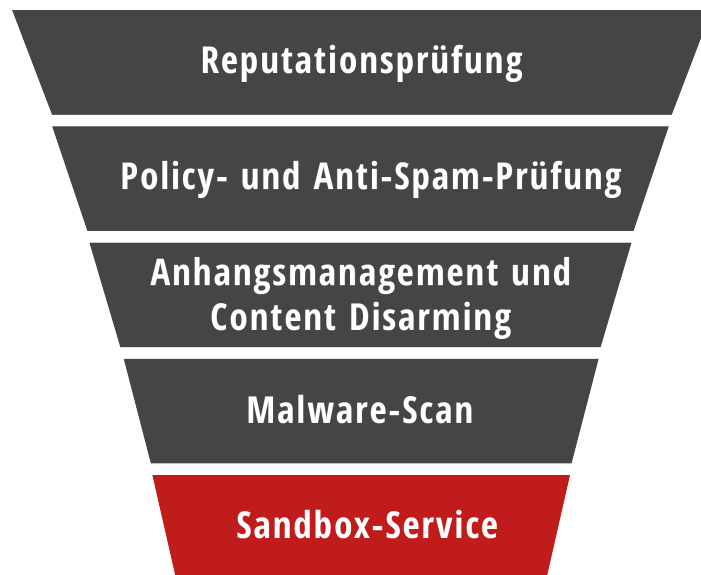
Quelle: Cyren

Lizenzierung und Datenschutz

Die 32Guards Sandbox 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 der 32Guards Sandbox. Für die Sandbox wird ein eigener Lizenzschlüssel erstellt, der in die bestehende Lizenz integriert wird.

Limitierung der Überprüfungen

Die Anzahl der vollständigen Analysen durch die 32Guards Sandbox ist wegen des hohen Ressourcenbedarfs 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 unseren Kunden, die Filter in NoSpamProxy® so zu konfigurieren, dass eine Überprüfung durch die 32Guards Sandbox nur erfolgt, falls E-Mails durch vorgelagerte Filterstufen nicht schon vorher abgelehnt wurden.



Überblick über die Filterstufen in NoSpamProxy

Testbetrieb

Für einen Testbetrieb der 32Guards Sandbox ist ein entsprechender Lizenzschlüssel erforderlich, der beim Vertriebsteam von NoSpamProxy® erhältlich ist.

Standardmäßig ist der Testzeitraum auf 30 Tage begrenzt.

32Guards Sandbox konfigurieren



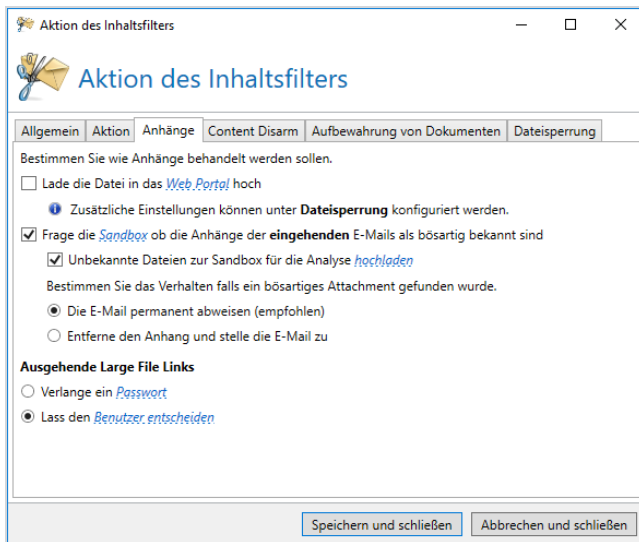
Diese Funktion ist verfügbar, wenn Sie die **32Guards Sandbox** lizenziert haben.

Möglichkeit 1: Anpassen einer vorhandenen Aktion


Möglichkeit 1: 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 böse bekannt sind**.

 Ist diese Option aktiviert, gleicht NoSpamProxy die Hashwerte von Anhängen mit bereits in der Sandbox-Datenbank vorhandenen Hashwerten ab. Das Abfragen der Hashwerte wird uneingeschränkt und ohne Abzug von gekauften Lizenzen durchgeführt.

5. Optional Setzen Sie das Häkchen neben **Unbekannte Dateien zur Sandbox für die Analyse hochladen**.



Ist diese Option aktiviert, werden der Sandbox unbekannte Dateien zur Analyse in diese hochgeladen. Der Upload von Dateien ist auf 20 Dateien pro Benutzer und Monat beschränkt. Siehe [32Guards Sandbox konfigurieren](#).

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.

■ Möglichkeit 2: Erstellen einer neuen Inhaltsfilteraktion

Möglichkeit 2: Erstellen einer neuen Inhaltsfilteraktion

Das Erstellen einer neuen Inhaltsfilteraktion ist vor allem dann sinnvoll, wenn Sie die Prüfung durch die Sandbox auf einzelne Dateitypen einschränken wollen.

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.

Unterstützte Dateitypen

Allgemein

- Ausführbare Dateien
 - Ausführbare Datei für Windows
- Microsoft Office
 - Microsoft Excel (alle)
 - Microsoft PowerPoint (alle)
 - Microsoft Word (alle)
- Text
 - HTML
 - PDF-Dokument
 - PDF-Dokument mit URLs

- Rich Text Format
- Rich Text Format mit OLE-Objekten
- Skripte
 - .js
 - .vbs
 - .ps1
- Archive und komprimierte Dateien
 - 7Zip-komprimierte Datei
 - ACE-komprimierte
 - AR-komprimierte Datei
 - ARJ-komprimierte Datei
 - BZIP2-komprimierte Datei
 - GZIP-komprimierte Datei
 - RAR-komprimierte Datei
 - TAR-komprimierte Datei
 - Windows-Installer-Datei
 - ZIP-komprimierte Datei
 - *.alz
 - *.cab
 - *.z
 - *.zoo



HINWEIS:

Wir empfehlen dringend, bei der Inhaltsfilterung auf einen Allowlisting-Ansatz zu setzen. Diese Empfehlung betrifft insbesondere die Benutzung der 32Guards Sandbox.

Ein Beispiel zur Veranschaulichung: Auch wenn eine „Ausführbare Datei für Windows“ von der Sandbox unterstützt wird, stellt sich die Frage, ob man diesen potenziell gefährlichen Dateityp überhaupt für das eigene Unternehmen erlauben will. Es ist in diesem Fall sinnvoller, diesen Dateityp generell abzulehnen und sich so auch den Upload zur Sandbox zu sparen.

Falls eine Datei von der 32Guards Sandbox als unverdächtig eingestuft werden sollte, wird die jeweilige E-Mail zugestellt.

Zustellverzögerung

Wenn eine Datei zur Sandbox hochgeladen wird, wird die E-Mail im ersten Schritt nicht angenommen sondern temporär abgewiesen, sodass der absendende E-Mail-Server diese noch einmal zustellt. Die temporäre Abweisung wird hier angewandt, da die Analyse eine gewisse Zeit in Anspruch nimmt, diese aber beim erneuten Zustellversuch nach etwa fünf Minuten abgeschlossen sein sollte.

Dies bedeutet für die Zustellung eine Zustellverzögerung, die entsprechend beachtet werden muss. Somit empfehlen wir Ihnen, genau zu prüfen, welche Dateien wirklich zur Sandbox gesendet werden sollen. Beachten Sie die folgende Option, falls zeitkritische Prozesse oder Postfächer im Unternehmen existieren:

- Ist eine Sandbox-Hashabfrage an Stelle einer vollständigen Analyse (Sandbox-Upload) ausreichend?
- Es besteht im Inhaltsfilter die Möglichkeit, unterschiedliche Aktionen zu erstellen, um für „Vertrauenswürdige E-Mails“ und „Nicht vertrauenswürdige E-Mails“ unterschiedliche Aktionen zu konfigurieren. Hier können Sie zwischen einem Sandbox-Upload und einer Sandbox-Hashabfrage unterscheiden.
- Office-Dokumente können gegebenenfalls durch Content Disarm and Reconstruction (CDR) in ein sicheres PDF-Dokument umgewandelt werden. Siehe [Hinweise zu Content Disarm and Reconstruction \(CDR\)](#).

Weitere Informationen



HINWEIS: Die Anzahl der vollständigen Analysen (Sandbox-Upload) durch die 32Guards Sandbox 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 die 32Guards Sandbox nur erfolgt, falls E-Mails durch vorgelagerte Filterstufen nicht schon vorher abgelehnt wurden. Bei Überschreiten des Limits können zusätzliche Kosten anfallen.



TIP: Um die Prüfung durch die 32Guards Sandbox auf einzelne Dateitypen einzuschränken, sollte eine zusätzliche Inhaltsfilteraktion erstellt werden, die nur auf bestimmte Dateitypen angewendet wird.

Hilfe und Unterstützung

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.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

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 des NoSpamProxy Command Center angezeigt.

YouTube

In unserem [YouTube-Kanal](#) finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter [+49 5251304-636](tel:+495251304636)
- per E-Mail unter support@nospamproxy.de.

