NetSpy Dokumentation

# Liste der Basis-Funktionalitäten von NetSpy

|  |  |
| --- | --- |
| Aufgabe | Erledigt |
| Alle Emails in einem bestimmten Verzeichnis nach Suchwörtern durchsuchen | x |
| Suchwörter aus einer Blacklist lesen | x |
| Einstufung „verdächtig“ nach bestimmter Anzahl von Treffern innerhalb einer Email | x |
| Quarantäneordner für „verdächtige“ Emails einrichtigen und „verdächtige“ Emails dahin verschieben | x |
| Für jeden Suchlauf eine Logdatei mit Infos über „verdächtige“ Emails schreiben. Die Logdatei sollte pro Email folgende Informationen enthalten (Absender, Empfänger, Sendedatum, Betreff, gefundene Suchwörter mit Angabe der Trefferzahl pro Suchwort) | TODO |
| Groß- und Kleinschreibung ignorieren | x |
| ASCII-Code ersetzen (Umlaute / Sonderzeichen) | x |
| Suchwörter in zusammengesetzten Wörtern erkennen (Teilstrings) | x |

# Lösungsweg für Basis-Funktionalitäten von NetSpy

|  |  |
| --- | --- |
| Aufgabe | Lösung |
| Alle Emails in einem bestimmten Verzeichnis nach Suchwörtern durchsuchen | **EmailHandler** holt sich die Blacklist **via FileManager** undführt **Blacklist-Scan** durch. |
| Suchwörter aus einer Blacklist lesen | **FileManager** liest Blacklistdatei aus und gibt String-Liste mit „verdächtigen“ Wörtern zurück. |
| Einstufung „verdächtig“ nach bestimmter Anzahl von Treffern innerhalb einer Email | **EmailHandler** enhält Sicherheitsstufen-Konfiguration: Bei insgesamt 10 Treffern z. B. wird eine Email erst als „verdächtig“ markiert. **EmailHandler** setzt ein **Email-Objekt** auf „verdächtig“. |
| Quarantäneordner für „verdächtige“ Emails einrichtigen und „verdächtige“ Emails dahin verschieben | **FileManager** erstellt und verschiebt Dateien und Ordner. |
| Für jeden Suchlauf eine Logdatei mit Infos über „verdächtige“ Emails schreiben. Die Logdatei sollte pro Email folgende Informationen enthalten (Absender, Empfänger, Sendedatum, Betreff, gefundene Suchwörter mit Angabe der Trefferzahl pro Suchwort) | **FileManager** erstellt Logdatei und schreibt dort hinein. **LogManager** gibt **Schreibauftrag** an **FileManager** mittels eines **ScanResult-Objektes** weiter. |
| Groß- und Kleinschreibung ignorieren | **Achtung:** Erst nach ASCII-Code Ersetzung .toLowerCase() anwenden |
| ASCII-Code ersetzen (Umlaute / Sonderzeichen) | **Achtung:** Vor dem Speichern des Mail-Inhalts in ein Email-Objekt! |
| Suchwörter in zusammengesetzten Wörtern erkennen (Teilstrings) | **Beispiel:** „K O K S“, „ Bom be“ |

# Liste der Optionalen Funktionalitäten von NetSpy

|  |  |
| --- | --- |
| Aufgabe | Erledigt |
| Zeilenumbruch, Leerstellen ignorieren |  |
| Suchbegriffen unterschiedliche Prioritäten zuordnen |  |
| Berücksichtigung von Jokerzeichen im Suchwort |  |
| Automatisch nach ähnlichen Wörtern suchen (regular expressions) |  |
| Blacklist dynamisch aus der Anwendung heraus verwalten (löschen, ändern, hinzufügen) |  |
| Whitelist für Email-Adressen (Absender, Empfänger) verwenden |  |
| Whitelist für Email-Adressen dynamisch aus der Anwendung heraus verwalten |  |
| Option für Suche als ganzes Wort oder als Teilstring zur Verfügung stellen |  |
| HTML-Teil bei der Suche ignorieren | x |

# Lösungsweg der Optionalen Funktionalitäten von NetSpy

|  |  |
| --- | --- |
| Aufgabe | Lösung |
| Zeilenumbruch, Leerstellen ignorieren | Ersetze Leerzeichen und Zeilenumbrüche (backslash r backslash n) vor dem Blacklist-Scan |
| Suchbegriffen unterschiedliche Prioritäten zuordnen | Klasse Blacklist enthält eine Map mit Suchwort (String) und Priorität (Integer/String) |
| Berücksichtigung von Jokerzeichen im Suchwort | O = 0; e = 3; \*#\_+$ und andere |
| Automatisch nach ähnlichen Wörtern suchen (regular expressions) | Bombe, bombig, bombastisch, bombenhaft |
| Blacklist dynamisch aus der Anwendung heraus verwalten (löschen, ändern, hinzufügen) | Erstellung eines Menüs mit Blacklist-Option |
| Whitelist für Email-Adressen (Absender, Empfänger) verwenden | Ähnlich zu der Blacklist: whitelist.txt. Enthält Email den Absender, so soll Email-Objekt nicht verdächtig gesetzt werden |
| Whitelist für Email-Adressen dynamisch aus der Anwendung heraus verwalten | Siehe Blacklist dynamisch aus der Anwendung heraus verwalten |
| Option für Suche als ganzes Wort oder als Teilstring zur Verfügung stellen | Zum Verständnis: Wenn nur nach „bombe“ gesucht werden soll, so ist „bombenanschlag“ legitim |
| HTML-Teil bei der Suche ignorieren | Beende auslesen der Datei, sobald „Content-Type: text/html“ in einer Zeile auftaucht. |