Freistaat Thüringen
Thüringer Landesrechenzentrum

Informationssicherheitsmanagement des Freistaats Thüringen

Konzept Mailempfangsregeln zentrales Internet E-Mail Gateway und Exchangeserver CNFT

Version / Datum	1.0	28.01.2021
Dateiname	2735.ISMS.Ko.Mailempfangsregeln_V1.0	
Dokumententyp	Konzept	
Vertraulichkeitsstufe	**TLP GREEN**	
Verantwortlicher	Manuel Wiesner	
Erstellt am	13.12.2018	
Status	**freigegeben**	
Verteiler	TLRZ A1-A3, ISB-Ressorts, ISB-Land	
Dokumentenablage	VIS: 25.14-1073-13086/2018	
Ersteller (Name/Rolle)	TLRZ Wiesner, Manuel / SOC	

Dokumentenfreigabe:

Stufe	Z.S.	Kategorie	Erlassen von	Erlassen für	Fällig am	erledigt	Aufgabe	Vermerk
1	1.1	Unterschrift	Weide, Günter	Sperling, Stefan	16.10.2020	28.01.2021 15:03	Hier wurde offensichtlich der Zeichnungsschritt vergessen, bitte jetzt zeichnen	

Inhaltsverzeichnis

1 Allgemeines ... 3
1.1 Zielsetzung ... 3
1.2 Geltungsbereich ... 3
1.3 Geltungsdauer/ Revision ... 3
2 Einleitung ... 4
3 Betreffmarkierung ... 5
3.1 Beantragung und Auswahl von Schlagworten ... 5
3.2 Bereitstellung der zentralen Schlagwortliste ... 5
3.3 Zeitliche Begrenzung des Blacklist-Eintrags ... 5
3.4 Auswirkungen von Einträgen in der Schlagwortliste ... 5
4 Regelbasierte Nachrichtenmarkierung ... 6
5 Ablehnen unberechtigter Nachrichten hinsichtlich Envelope ... 6
6 Ablehnen unberechtigter Anhänge ... 6
7 Freigaberegelung ... 7
8 Mitgeltende Unterlagen ... 7
9 Änderungsverzeichnis ... 8

1 Allgemeines

1.1 Zielsetzung

Ziel dieses Dokumentes ist es, Regelungen für die Behandlung für eingehende Nachrichten in Verbindung mit dem zentral bereitgestellten Internet E-Mail Gateways aufzustellen, welche als Grundlage zur Gefahrenabwehr durch maliziöse Emailinhalte fungieren.

1.2 Geltungsbereich

Das vorliegende Dokument gilt für den Informationsverbund „Konvergentes Sprach- und Datennetz der Thüringer Landesverwaltung – Corporate Network Freistaat Thüringen (CNFT)“ [3].

1.3 Geltungsdauer/ Revision

Die Dauer dieses Konzepts ist nicht befristet.

Das vorliegende Konzept wird entweder anlassbezogen oder mindestens alle 2 Jahre einer überprüfenden Fortschreibung unterzogen. Das Konzept wird dabei, nach dem KVP durch Mitglieder des ISM-Teams des- Informationsverbundes inhaltlich überprüft und im Bedarfsfall fortgeschrieben. Dieses Konzept unterliegt der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen [2].

2 Einleitung

Das TLRZ verwendet als erste Stufe zur SPAM-Abwehr das „Greylisting"-Verfahren, hierbei wird die erste Nachricht eines Absenders mit einer temporären Fehlermeldung abgewiesen und die Metadaten:

- E-Mail Adresse des Absenders
- E-Mail Adresse des Empfängers
- IP-Adresse des Clients

zur Greylist-Datenbank hinzugefügt. RFC-konform (hier 5321 bzw. 6647) agierende E-Mail-Server werden daraufhin die Nachricht erneut senden. Die wieder übermittelten Metadaten werden daraufhin in die Whitelist übernommen und alle zukünftigen Nachrichten, deren Metadaten zu diesem Tripple passen, werden verzögerungslos übermittelt.

Darüber hinaus konnte aufgrund der gesammelten Erfahrungen festgestellt werden, dass aufgrund der steigenden Vielzahl von Schadcode eine Erkennung infizierter Nachrichten mittels Heuristik oder Mustererkennung nur unzuverlässig und verzögert möglich ist. In der Folge kommt es dazu, dass infizierte Nachrichten zugestellt werden.

Die verwendete soziale Komponente im Rahmen von beobachteten Spam-Kampagnen beschränkt sich aber auf wenige Varianten, so dass eine Markierung der Nachrichten mittels Schlagworten zur Sensibilisierung der Mitarbeiter beiträgt und daraus resultierend das Risiko einer Infektion sinkt. (Betreffmarkierung)

Weiterhin sollen Nachrichten, welche von außerhalb des CNFT abgesendet werden und eine Anlage enthalten mittels automatisierten Systems zusätzlich mit einem Hinweis gekennzeichnet werden, welcher den Empfänger auf eine potentielle Gefahr im Anhang der Email hinweist. (Regelbasierte Nachrichtenmarkierung)

Um den Angriffsvektor weiter zu verringern sollen Nachrichten, welche einen CNFT-internen Absender mittels sogenanntem Envelope vorgeben, tatsächlich aber von nicht zum CNFT gehörenden Absender versendet werden, direkt am E-Mail Gateway mittels Reject abgelehnt werden. (Ablehnen unberechtigter Nachrichten)

Darüber hinaus sollen Nachrichten mit Anhängen überholter Dateitypen und –endungen oder ausführbarer Anhänge (z.B. *.exe oder in Officedokumente eingebettete Macros) am Emailgateway abgelehnt werden. Der Empfänger wird mittels automatischer Systemnachricht darüber informiert. (Ablehnen unberechtigter Anhänge)

3 Betreffmarkierung

3.1 Beantragung und Auswahl von Schlagworten

Die statische Aufnahme von Schlagwörtern für die Betreffmarkierung kann von dem für IT-Aufgaben zuständigen Strukturleiter einer Behörde oder Einrichtung, hilfsweise dem ISB beim TLRZ beantragt werden. Das Ansinnen ist hinreichend zu begründen, mindestens sind die Schlagworte zu nennen und die Quelle, die belegt, dass die Nachrichten mit besagten Schlagworten zeitweilig hauptsächlich bösartig sind.
Der Behördenleiter ist laut IT-Grundschutz immer für die Informationssicherheit verantwortlich und muss abschließend den Antrag unterzeichnen. Bei obersten Landesbehörden gilt die Ausnahme, dass der zuständige Abteilungsleiter abschließend zeichnen kann. Die Beantragung soll formlos elektronisch an das Servicecenter (support@servicecenter.thueringen.de) gesendet werden
Das Servicecenter des TLRZ leitet entsprechende Anträge in die Queue „CERT-TLRZ“ weiter. Änderungen in der Schlagwortliste werden als Change Request behandelt und müssen wegen der Auswirkung auf die gesamte Landesverwaltung vom Thüringen CERT bewertet und freigegeben werden.

3.2 Bereitstellung der zentralen Schlagwortliste

Nach Freigabe des Change Request Blacklist veranlasst das Thüringen CERT den Eintrag der Veränderungen in die zentrale Schlagwortliste [5]. Die Schlagwortlisten der zentralen Internet E-Mail Gateways des TLRZ werde periodisch mit der zentralen Schlagwortliste [5] abgeglichen.

3.3 Zeitliche Begrenzung des Blacklist-Eintrags

Die Wirksamkeit eines Schlagwortlist-Eintrags ist auf 1 Monat begrenzt. In Ausnahmefällen, für die eine gesonderte Begründung im Antrag beizufügen ist, kann die Laufzeit auf 3 Monate festgelegt werden. Nach Verstreichen dieser Frist werden die Einträge gelöscht. Zur längeren Aufrechterhaltung von Einträgen müssen diese durch die beantragende Stelle vor Fristablauf erneuert werden.

3.4 Auswirkungen von Einträgen in der Schlagwortliste

Einträge in der Schlagwortliste wirken immer systemweit, eine Einschränkung für einzelne Ressorts oder Einrichtungen und Behörden ist nicht möglich. Sie führen nicht dazu, dass Mails nicht zugestellt werden, sondern stellen lediglich eine vorbeugende Maßnahme zur Sensibilisierung dar.
Ein Eintrag in die Schlagwortliste stellt kein Sicherheitsrisiko dar, ist jedoch zur Vermeidung von Fehlalarmen sorgsam abzuwägen. Aus diesem Grund hat eine Information der Nutzer über die Vorgehensweise zu erfolgen. Dieses Konzept ist deshalb den ISB der Dienststellen mit der Maßgabe der Information der Beschäftigten zur Kenntnis zu geben.

4 Regelbasierte Nachrichtenmarkierung

Nachrichten, welche von einem Absender außerhalb des CNFT-Verbundes versendet werden und die Anlagen enthalten, sollen mittels Hinweis am Anfang der Email markiert werden, so dass der Empfänger zusätzlich hinsichtlich potentiell schadhafter Anhänge sensibilisiert wird.

Der automatisch einzufügende Text enthält folgende Informationen:
„*Diese E-Mail erreichte Sie von einem Absender außerhalb der Infrastruktur der Thüringer Landesverwaltung. Bitte klicken Sie auf keine Links und öffnen Sie keine Anhänge, falls Sie den Absender nicht kennen und nicht abschätzen können, ob der Inhalt sicher ist!*“

Dieser Hinweis wird automatisch mittels Transportregel durch die Exchangeserver des CNFT hinzugefügt werden, ohne die Nachricht manuell öffnen zu müssen. Diese automatische Verarbeitung durch Technik mittels definierter Regeln stellt die Unversehrtheit der Nachricht sowie das Briefgeheimnis sicher.

5 Ablehnen unberechtigter Nachrichten hinsichtlich Envelope

Nachrichten, welche nicht dazu berechtigt sind, mittels „Envelope“ (Absenderdomain, Absendername) einen CNFT-internen Absender anzugeben werden automatisiert am E-Mailgateway des CNFT geprüft und bei Regelverstoß durch das E-Mail Gateway mittels „Reject“ abgelehnt. Der Absender erhält gemäß RFC eine entsprechende Systemnachricht, der eigentliche Nachrichtenempfänger wird RFC-konform nicht über den Vorgang informiert. Die Prüfung des Envelope erfolgt hierbei automatisiert auf Codierungen im ASCII als auch im UniCode-Format. Die Unterscheidung erfolgt hierbei über festgelegte Behördenkürzel , die in Anhang Behördenkürzel [5] aufgelistet sind . Weiterhin werden legitimen Ausnahmen (MailWhitelist) im selben Dokument zentral durch das CERT gepflegt.

6 Ablehnen unberechtigter Anhänge

Nachrichten, welche einen Anhang beinhalten werden automatisch durch das Emailgateway auf Art- und Güte der/des angehängten Dokumentes oder Dokumente überprüft. Wird dabei ein laut Blacklist unberechtigter Anhang vom System erkannt, wird die Nachricht automatisch vom System abgewiesen. Der Absender erhält gemäß RFC eine entsprechende Systemnachricht, der eigentliche Nachrichtenempfänger wird RFC-konform nicht über den Vorgang informiert. Die Auflistung abzulehnender Dateitypen befindet sich im Anhang Fileextension [5].

7 Ausnahmeregelung

Eine Abweichung von den vorgenannten Festlegungen ist in der Dokumentation des entsprechenden Veränderungsvorgangs (Change) zu begründen, vom zuständigen Informationssicherheitsbeauftragten zu befürworten und vom zuständigen Vorgesetzten gemäß CAB zu genehmigen.

8 Freigaberegelung

Das vorliegende Dokument tritt am Tag nach der Bekanntgabe/Veröffentlichung in Kraft.

9 Mitgeltende Unterlagen

[1] Leitlinie zur Informationssicherheit
Dokument: 1010.ISMS.RL_Leitlinie_Informationssicherheit

[2] Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
Dokument: 1030.ISMS.RL_Dokumentenlenkung

[3] Definition Untersuchungsgegenstand
Dokument: 0002.ISMS_Index_Definition_Untersuchungsgegenstand

[4] Abkürzungsverzeichnis
Dokument: 0030.ISMS.Index_Abkürzungen

[5] Mailempfangsregelwerk
Dokument: 2735.ISMS.Index.Mailempfangsregelwerk.xlsx
Schlagwortliste: *2735.ISMS.Index.Mailempfangsregelwerk!Schlagworte*
Behördenkürzel: *2735.ISMS.Index.Mailempfangsregelwerk! Behördenkürzel*
Mail Ausnahmen: *2735.ISMS.Index.Mailempfangsregelwerk! MailWhitelist*
abzulehnender Dateitypen: *2735.ISMS.Index.Mailempfangsregelwerk!FileExtensions*

10 Änderungsverzeichnis

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
28.01.2021	1.0		Freigabe	St. Sperling
19.01.2012	0.6		Aktualisierung auf neue Vorlage	M.Frühauf
18.01.2021	0.5		Review + redaktionelle Änderungen	St. Sperling
12.01.2021	0.4.1	7	Redaktionelle Änderung	G. Weide
12.01.2021	0.4		Ergänzung Enevelope Reject	M. Wiesner
16.01.2019	0.3	-	Review	St. Sperling
07.01.2019	0.2		Änderungen eingearbeitet	M. Wiesner
13.12.2018	0.1	Erstellt	Dokument erstellt	M. Wiesner