Layer8 Phishing melden AddIn

Dokumentation

Version 1.2

Allgeier IT Solutions GmbH
Hans-Bredow-Str. 60
28307 Bremen

Stand: 15. Oktober 2020

Layer8

Mithilfe des Layer8 Phishing melden AddIns haben Ihre Mitarbeiter die Möglichkeit, potentiell gefährliche E-Mails selbstständig zu untersuchen und an eine hinterlegte E-Mail Adresse weiterzuleiten. Dabei werden die für die weitere Untersuchung wichtigen Headerinformationen mit eingefügt.

Da uns IT-Sicherheit und Datenschutz ein wichtiges Anliegen sind, kommuniziert das AddIn mit keinerlei Webdiensten oder Analysetools.

Layer8

Inhaltsverzeichnis

1 Voraussetzungen

1.1 Unterstützte E-Mail Clients

Das Layer8 Phishing melden AddIn wurde für Outlook 2016 und Outlook für Office 365 entwickelt. Das AddIn unterstützt sowohl die 32-Bit, als auch die 64-Bit Version von Office. Bitte wählen Sie für die Installation das entsprechende Installationspaket im Layer8 Webinterface aus.

1.2 Betriebssystem

Als Betriebssystem wird derzeit Windows 10 unterstützt.
Andere Windowsversionen wurden nicht getestet – Feedback ist immer gerne gesehen.

1.3 Verteilung im Unternehmen

Das Installationspaket wird als .msi-Datei zur Verfügung gestellt. Dadurch haben Sie die Möglichkeit, das AddIn durch Gruppenrichtlinien oder andere Software-Verteilungssysteme auszurollen. Ihr definierter Ansprechpartner für potentielle Phishing E-Mails wird beim Herunterladen der .msi-Datei hinzugefügt. Solle sich die E-Mail Adresse des Ansprechpartners ändern, können Sie diese auf der Modulseite ändern und ein neues Installationspaket herunterladen und ausrollen oder die entsprechenden Registry-Schlüssel, wie im Kapitel 2.1 beschrieben, austauschen.

1.3.1 Änderung des Ansprechpartners für Phishingmeldungen

Um die E-Mail Adresse des vordefinierten Kontakts für *Phishing melden* zu ändern haben Sie zwei Möglichkeiten:

- Ändern des Ansprechpartners auf `https://layer8.app`. Danach können Sie das Installationspaket für die entsprechende Office-Version (32 oder 64-Bit) neu herunterladen und auf die Clients verteilen.
- Verteilen von neuen Registry-Einträgen via GPO. Bitte folgen Sie dazu den Anweisungen in Kapitel 2.1.

2 Installation

Für die Konfiguration und Download benötigen Sie einen kostenlosen Account auf `https://layer8.app`.
Es wird nur ein Account pro Unternehmen oder Organisation benötigt.

Sobald Sie Ihren Account per E-Mail bestätigt haben, können Sie in der Menüleiste das AddIn konfigurieren.

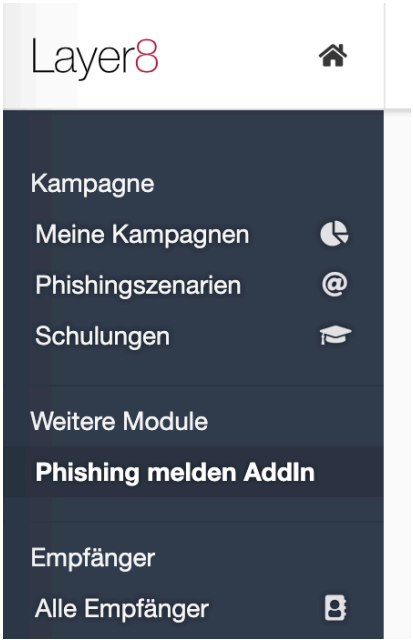

Abbildung 1: Die Einstellungen für das AddIn befinden sich in der Hauptnavigation

Standardmäßig wird als Ansprechpartner für Phishing E-Mails die E-Mail Adresse des aktuellen Accounts verwendet. Sie haben die Möglichkeit, den Ansprechpartner innerhalb der erlaubten Domains zu verändern. Beim Download des Installationspakets wird stets die aktuell hinterlegte E-Mail Adresse verwendet.

2.1 Registry Einträge

2.1.1 Ansprechpartner E-Mail Adresse

Um den Ansprechpartner für potentielle Phishing E-Mails zu ändern, müssen zwei Registry-Schlüssel verändert werden:

- **SettingsEmail** E-Mail Adresse des Ansprechpartners in Base64-Kodierung.
- **SettingsInstallId** Zufällige UUID4[1], welche sich von der aktuell hinterlegten unterscheidet.

Sobald sich die *SettingsInstallId* ändert, wird beim nächsten Start von Outlook der Ansprechpartner für potentielle Phishing E-Mails überschrieben. Falls der Benutzer den Ansprechpartner manuell geändert hat, wird diese Einstellung ebenfalls überschrieben.

2.1.2 Anzeigelabel

Es ist möglich, das Label unter der Symbolgruppe zu verändern. Der Schlüsselwert ist **SettingsLabel** und enhält als Wert den Labelinhalt der Symbolgruppe im AddIn (ohne Base64-Kodierung), z.B. *Layer8 Awareness*. Um das neue Label zu übernehmen, muss sich die die *SettingsInstallId* von der aktuell definierten ID unterscheiden.

2.1.3 Beispiel

Dieser Eintrag nutzt die E-Mail Adresse *kontakt@example.com* mit dem Label *Layer8 Awareness*:

```
SettingsEmail: a29udGFrdEBleGFtcGxlLmNvbQ==
SettingsInstallId: 46f559f0-a088-41bc-9f42-925d91e70c39
SettingsLabel: Layer8 Awareness
```

2.1.4 32-Bit

Registry-Pfad für 32-Bit Installationen von Office:
SOFTWARE\WOW6432Node\Microsoft\Office\Outlook\Addins\Layer8PhishingMeldenAddIn

Ändern Sie folgende Registry-Schlüssel:
SettingsEmail: Base64 kodierte E-Mail Adresse des Ansprechpartners
SettingsInstallId: Zufällige UUID4

2.1.5 64-Bit

Registry-Pfad für 64-Bit Installationen von Office:
SOFTWARE\Microsoft\Office\Outlook\Addins\Layer8PhishingMeldenAddIn

Ändern Sie folgende Registry-Schlüssel:
SettingsEmail: Base64 kodierte E-Mail Adresse des Ansprechpartners
SettingsInstallId: Zufällige UUID4

[1] https://de.wikipedia.org/wiki/Universally_Unique_Identifier

3 Funktionen

3.1 Phishing melden

Die Funktion *Phishing melden* leitet die aktuell ausgewählte E-Mail an die hinterlegte E-Mail-Adresse (beispielsweise Ihrer IT-Abteilung) mitsamt E-Mail-Header weiter. Zusätzlich wird die ursprüngliche Nachricht als .msg-Datei angehängt.

3.2 Links anzeigen

Diese Funktion listet alle Hyperlinks in der ausgewählten E-Mail mit Linktext, Ziel und vollständiger Zieladresse auf.

3.3 Header anzeigen

Die Funktion zeigt mit einem Klick alle E-Mail-Header der ausgewählten E-Mail an.

3.4 Tipps öffnen

Tipps öffnen zeigt nützliche Tipps und Hinweise, wie man potentielle Phishing E-Mails erkennen kann.

3.5 Einstellungen

In den Einstellungen können Ihre Mitarbeiter den Ansprechpartner für potentielle Phishing E-Mails ändern. Bei Verteilung von neuen Registry-Schlüsseln, wie in Kapitel 2.1 beschrieben, wird der Ansprechpartner überschrieben.

4 Changelog

4.1 Version 1.2

- Verbesserte Link-Erkennung in E-Mails
- Zuverlässigkeit und Darstellung von **Links anzeigen** verbessert
- Mehrsprachigkeit: Deutsch und Englisch
  Die Sprache des Add-Ins wird auf Basis der Betriebssystemsprache eingestellt.
- Quarantäne-Ordner für Phishingmails: Nach dem Melden von Phishing kann die ursprüngliche Mail auf Wunsch in einen vom AddIn angelegten Quarantäne-Ordner verschoben werden.
- Ursprüngliche E-Mail wird bei der Phishingmeldung nun zusätzlich als Outlook Mail Message (.msg) angehängt.

4.2 Version 1.1

- Konfigurationsverarbeitung aus Registry verbessert
- Verbessertes UI, größerer **Phishing melden**-Button
- Verbessertes Fensterhandling für **Links anzeigen** und **Header anzeigen**
- Anpassbares Label für Symbolleiste
- Stabilität erhöht
- Links lassen sich nun in **Links anzeigen** kopieren

4.3 Version 1.0

Implementation der wichtigsten Funktionen:

- **Phishing melden**: Aktuelle E-Mail wird mitsamt E-Mail-Headern kopiert und durch die definierte Ansprechpartner E-Mail-Adresse zur weiteren Überprüfung vorausgefüllt.
- **Links anzeigen**: Funktion, um Links alle einer Mail anzeigen zu lassen (Linktext, Hauptdomain, Link URL).
- **Header anzeigen**: Zeigt alle E-Mail-Header der aktuell geöffneten E-Mail an.
- **Tipps anzeigen**: Zeigt Tipps und Hinweise an

5 Kontakt

Das *Layer8 Phishing melden AddIn* befindet sich derzeit in der Beta-Phase. Falls Fehler auftreten sollten, oder Sie weitere Anregungen und Ideen haben, die wir in zukünftigen Versionen anbieten können, freuen wir uns über Ihr Feedback.

Allgeier IT Solutions GmbH
Hans-Bredow-Str. 60
28307 Bremen

Telefon: +49 781 203588 - 00
E-Mail: sales-security-og@allgeier-it.de