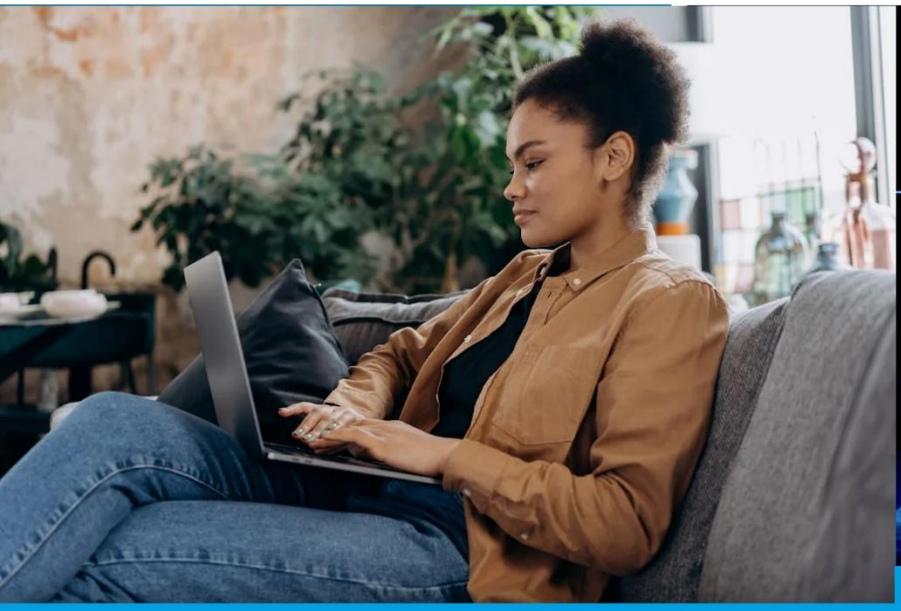
Aaron Siller



Microsoft Defender for Office 365

Dein Guide zur sicheren Konfiguration

- E-Mail Schutz: Safe-Links & Safe-Attachments
- Anti-Threat Richtlinien richtig konfigurieren
- Angriffssimulationen anwenden

siller.consulting
INTELLIGENCE FOR IT

Über den Autor

Aaron Siller

Als ich 2014 als IT-Dienstleister startete, stand ich vor denselben Herausforderungen, mit denen heute viele meiner Kunden zu mir kommen: Komplexe Microsoft-Systeme, ständig neue Security-Anforderungen und nie genug Zeit, um alles richtig zu konfigurieren.

Was als klassische IT-Beratung begann, entwickelte sich schnell zu einer klaren Mission: **Microsoft 365 Umgebungen sicherer machen, ohne dass Admins dafür Wochenenden opfern müssen.**

Heute werde ich von führenden Instituten wie der Heise Academy und Golem Karrierewelt als Trainer für Microsoft 365 Security eingesetzt. Meine Expertise bestätigt sich in der Zusammenarbeit mit Unternehmen vom handwerklichen Mittelstand bis hin zu internationalen Konzernen. Schau Dir gerne meine Referenzen auf meiner Website an.

E-MAIL aaron@siller.consulting

WEBSITE siller.consulting

LINKEDIN Aaron-Siller

YOUTUBE Aaron-Siller-YT

Inhaltsverzeichnis

Microsoft Defender für Office 365

Was ist Microsoft Defender für Office 365?

Microsoft Defender für Office 365 ist eine Sammlung von Funktionen, die über den Standardumfang hinaus zusätzlichen Schutz bieten – etwa im Vergleich zu dem, was Exchange Online Protection bereitstellt. Es verbessert den „Standard"-Scanvorgang und erweitert den Schutz über Exchange Online hinaus durch Funktionen wie Safe Links, Safe Attachments, Safe Documents, Anti-Phishing, Mailbox Intelligence und den Attack Simulator. Insgesamt lässt sich sagen, dass Microsoft Defender für Office 365 die Sicherheit in verschiedenen Phasen der Cybersicherheit gemäß dem NIST-Rahmenwerk verbessert:

- **Mehr Erkenntnisse (Identify)**: Angetrieben durch Informationen von Microsoft Defender für Office 365 bieten die verschiedenen Dashboards und Berichte wertvolle Einblicke in deiner Sicherheitslage und relevnten Bedrohungen in deiner Umgebung.
- **Besserer Schutz**: Durch zusätzliche Richtlinien, die die Schutzfunktionen integrierter Sicherheitslösungen wie Exchange Online Protection ergänzen.
- **Schnellere Erkennung und Reaktion**: Mithilfe von Funktionen wie Automated Investigation & Response (AIR) sowie der Integration mit Microsoft 365 Defender für die erweiterte Suche usw.

Wenn du Microsoft Defender für Office 365 entweder als separates Add-On oder als Teil bestimmter Lizenzpakete wie Microsoft 365 E5 oder des Microsoft 365 E5 Security Bundles erwirbst, stehen in verschiedenen Verwaltungsportalen sowie in PowerShell zusätzliche Optionen zur Verfügung. Mit einer P2-Lizenz können Sie zudem Microsoft 365 Defender nutzen, um die volle Leistungsfähigkeit von Microsoft Defender für Office 365 auszuschöpfen.

Wie bereits kurz erwähnt, beschränkt sich der von Microsoft Defender für Office 365 bereitgestellte Schutz nicht nur auf E-Mails. Einige Richtlinien und Funktionen lassen sich auch auf SharePoint, OneDrive for Business und Microsoft Teams anwenden. In diesem Abschnitt befassen wir uns zunächst mit den globalen Einstellungen von Microsoft Defender für Office 365, bevor wir auf spezifische Funktionen sowie ein Tool eingehen, mit dem sich Ihre Konfiguration anhand von Best Practices überprüfen lässt.

Microsoft Defender für Office 365 Lizenzierung

Microsoft Defender für Office 365 verfügt – ähnlich wie Exchange Online Protection – über eigene Lizenzen. Anders als bei Postfachlizenzen wird Microsoft Defender für Office 365 in vielen Fällen als Add-On betrachtet. Es stehen zwei „Pläne" zur Verfügung: Plan 1 (P1) und Plan 2 (P2).

Jeder dieser Pläne enthält die folgenden Funktionen:

- Safe Attachments
- Safe Attachments in Teams
- Safe Links
- Safe Documents

Plan 2 bietet darüber hinaus zusätzliche Funktionen wie:

- Threat Explorer
- Automated Incident & Response (AIR)
- Attack Simulator

Die Lizenzen für Microsoft Defender für Office 365 können entweder als Add-On oder als Bestandteil eines Lizenzpakets erworben werden. Da sich Lizenzmodelle häufig ändern und teils auf spezifischen Vereinbarungen zwischen Ihrer Organisation und Microsoft beruhen, verzichten wir an dieser Stelle auf detaillierte Angaben zur Lizenzierung. Allgemeine Informationen dazu findest du in Kapitel 1.

Microsoft Defender für Office 365 Dashboard

Microsoft stellt verschiedene Dashboards zur Verfügung, die Administratoren einen schnellen Überblick über den Status von Funktionen und relevante Informationen bieten. Microsoft Defender für Office 365 bildet hier keine Ausnahme und ist vollständig in das Microsoft 365 Defender-Portal integriert.

Spezifische Informationen zu Microsoft Defender für Office 365 findest du im Abschnitt „E-Mail & Zusammenarbeit“ des Portals. Von dort aus kannst du auf verschiedene Funktionen wie den Threat Explorer, Richtlinien, Quarantäne und mehr zugreifen. Alle Funktionen und Möglichkeiten werden im weiteren Verlauf dieses Kapitels behandelt.

Safe Links

Hast du eine E-Mail mit einem Link zu einem neuen Produkt erhalten oder ein Angebot für kostenloses Produkt? Vielleicht hat dir ein Freund einen Link zu einem YouTube-Video oder einer Witzeseite geschickt? Fragst du dich smanchmal, ob diese Links wirklich harmlos sind oder möglicherweise bösartige Absichten verbergen? Tatsächlich habe ich beim Schreiben dieses Kapitels ein Test-Postfach ohne spezielle Filterung eingerichtet und mehrere solcher bösartigen E-Mails erhalten. Abbildung 6-1 zeigt eine davon, inklusive des Links, wie er in Outlook dargestellt wird.

Abbildung 6-1: Bösartige E-Mail mit bösartigem Link, auf den eine ahnungslose Person klicken soll.

Beachte den Link in der Mitte. Sieht sicher aus, oder? Ist er aber nicht. Wenn du darauf klickst, wirst du auf eine bösartige Website weitergeleitet. Manche dieser Zielseiten sind gefährlicher als andere. Diese Methode ist weit verbreitet und zielt darauf ab, dich dazu zu bringen, eine bestimmte Seite zu öffnen, die anschließend versucht, zusätzliche Schadsoftware herunterzuladen oder schädliche Skripte auf deinem System auszuführen.

Ohne zusätzlichen Schutz könntest du auf den Link klicken und damit nicht nur dein System gefährden, sondern im schlimmsten Fall auch die Sicherheit deiner gesamten Umgebung kompromittieren. Was kannst du also tun, um dich davor zu schützen? In einem traditionelleren Ansatz setzen Unternehmen ein Secure Web Gateway (SWG) ein – auch als Forward-Proxy oder Proxy-Server bekannt. Dieses (virtuelle) Gerät oder dieser Dienst wirkt als eine Art Durchgangsstation für den Internetverkehr. Während der Datenverkehr hindurchfließt, wird er überprüft und – falls etwas Verdächtiges erkannt wird – blockiert. Dieser Ansatz ist sinnvoll, bringt aber eine Herausforderung mit sich: Er funktioniert nur zuverlässig, wenn der gesamte Datenverkehr tatsächlich über das SWG geleitet wird. Doch was ist, wenn das nicht möglich ist? Wenn plötzlich alle Benutzer im Homeoffice arbeiten und du deren Internetzugriffe nicht mehr zentral kontrollieren kannst? Oder wenn dein zentraler Standort nicht über genügend Bandbreite verfügt? Safe Links ist ein Teil der Antwort auf diese Herausforderungen.

Safe Links schützt dich in Office 365, indem verhindert wird, dass du auf bösartige Links zugreifst oder sie weiterleitest. Zum Zeitpunkt des Schreibens ist Safe Links vor allem für E-Mail-Nachrichten in Exchange Online verfügbar, wird aber künftig auch für andere Dienste wie Microsoft Teams bereitgestellt.

Wie funktioniert Safe Links?

Abbildung 6-2 zeigt, wie Safe Links verarbeitet werden. Wenn eine E-Mail mit einem oder mehreren Links in Exchange Online Protection eingeht, wird jeder dieser Links zunächst mit einer Datenbank bekannter bösartiger Websites abgeglichen. Wird eine Übereinstimmung gefunden, wird die Nachricht blockiert. Abhängig von deiner Safe-Links-Richtlinie (dazu später mehr) werden die URLs auch aktiv analysiert. Dabei navigiert eine Prüf-Engine zur Zielseite und prüft, ob sie sich verdächtig verhält – etwa durch das Ausführen schädlicher Skripte oder das

Initiieren eines Downloads. Wird nichts Verdächtiges festgestellt, wird die URL umgeschrieben, sodass sie über die Safe-Links-Infrastruktur von Microsoft läuft.

Eine solche umgeschriebene URL sieht dann zum Beispiel so aus:

https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2Fqtex0l&data=04%7C01%7C%7C78997604e9574b2393a808d878ce1a9e%7Ca4bfde4e50d6437aaf37d62d3a9c53cf%7C1%7C0%7C637392173893897317%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=tE7Gxc10QeMwrxNTsxGovojtUBbhsmmOfYLiboxFBks%3D&re served=0

Einschränkungen: Natürlich hat auch Safe Links seine Grenzen. Es bietet keinen bietet keinen vollständigen Schutz vor allen bösartigen Websites. Die Lösung funktioniert nur dann, wenn die ursprüngliche URL auch tatsächlich umgeschrieben werden kann. Außerdem ist es möglich, dass Nutzer trotzdem auf die Webseite zugreifen – selbst wenn sie als verdächtig eingestuft wurde. In manchen Fällen können sie den Schutz auch bewusst umgehen, indem sie direct zur Original-URL navigieren. Verlasse dich deshalb nicht ausschließlich auf Safe Links – zusätzlicher Schutz bleibt weiterhin notwendig.

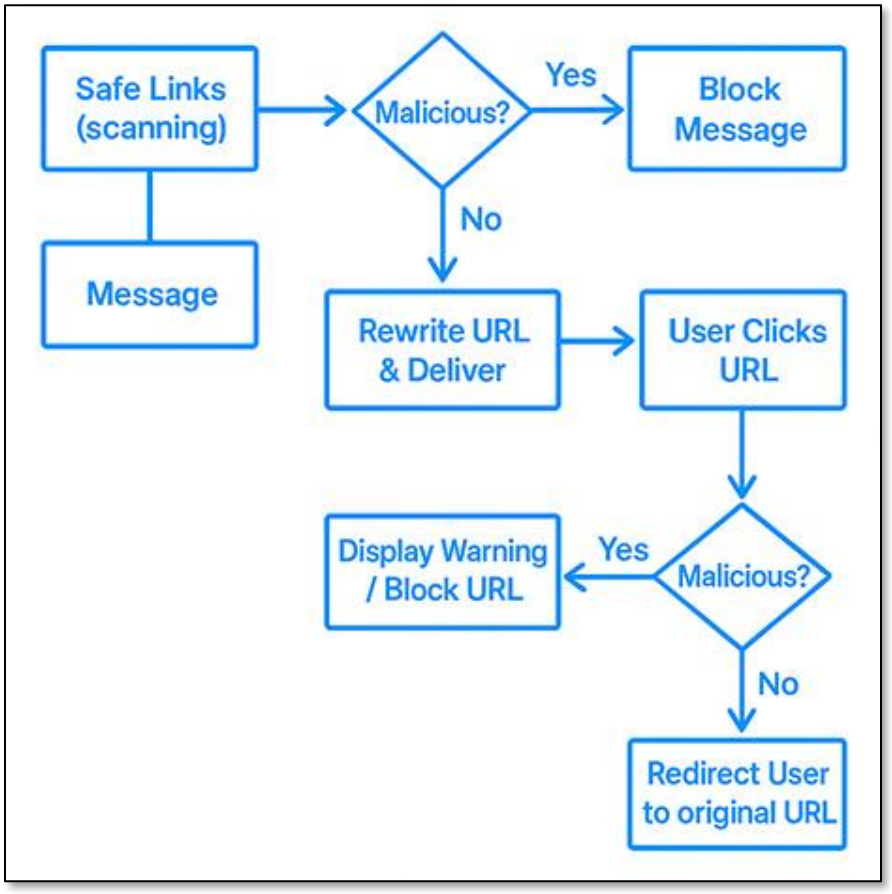


Abbildung 6-2: Safe Links Ablaufdiagramm

Konfigurieren von Safe Links

Wie einige andere Funktionen in Microsoft Defender für Office 365 kannst du Safe Links zentral im Microsoft 365 Defender-Portal konfigurieren. Standardmäßig gibt es keine Safe Links-Richtlinie – du musst also zunächst eine eigene Richtlinie erstellen, bevor Safe Links für deine Benutzer aktiv ist. Öffne dafür die Microsoft Defender-Konsole und wechsle im Bereich „**E-Mail und Zusammenarbeit**“ zu „**Richtlinien und Regeln**“. Wähle dort „**Bedrohungsrichtlinien**“ und anschließend „Safe Links“.

Globale Einstellungen / Eingebaute Schutzrichtlinie

Zunächst kannst du einige globale Einstellungen vornehmen. Klicke dazu auf „**Globale Einstellungen**“, um die Auswahlleiste zu öffnen. Dort kannst du unter anderem Folgendes konfigurieren:

- Blockieren der folgenden URLs: Du kannst bestimmte URLs sperren, sodass Benutzer keinen Zugriff darauf haben.

Beachte, dass einige der Optionen, die in früheren Kapiteln dieses Buchs beschrieben wurden, inzwischen zugunsten der integrierten Schutzrichtlinie entfernt wurden, die mittlerweile in allen Mandanten verfügbar ist. Diese eingebaute Richtlinie gilt für Benutzer, für die keine eigene Richtlinie festgelegt wurde. Die Einstellungen werden von Microsoft verwaltet und lassen sich nicht anpassen. Am einfachsten kannst du sie über einen PowerShell-One-Liner im Exchange Online PowerShell-Modul einsehen:

```
Get-SafeLinksPolicy 'Built-In Protection Policy' | Fl

EnableSafeLinksForEmail       : True
EnableSafeLinksForTeams       : True
EnableSafeLinksForOffice      : True
TrackClicks                   : True
AllowClickThrough             : True
ScanUrls                      : True
EnableForInternalSenders      : False
DeliverMessageAfterScan       : True
DisableUrlRewrite             : True DoNotRewriteUrls             :
{}
AdminDisplayName              :
CustomNotificationText        :
LocalizedNotificationTextList : {}
EnableOrganizationBranding    : False
```

```
RecommendedPolicyType          : Custom
IsBuiltInProtection            : True
```

- **EnableSafeLinksFor [E-Mail/Teams/Office]**: Aktiviert SafeLinks für diese Workloads in Microsoft 365.
- **Track Clicks**: Klicks auf bäsartige Links werden protokolliert
- **AllowClickThrough**: Wenn aktiviert, können Benutzer auch dann auf einen Link klicken, wenn er als bösartig erkannt wurde.
- **ScanURLs**: URLs werden aktiv gescannt, wenn diese Option auf "True" gesetzt ist.
- **Enable For Internal Senders**: Links von internen Benutzer werden nicht gescannt gesendet werden, werden nicht gescannt.
- **DeliverMessageAfterScan**: E-Mails werden erst gescanntund dann zugestellt.
- **DisableURLRewrite**: URLs werden nicht umgeschrieben, was z.B. für interne Websites sinnvoll sein kann.
- **EnableOrganizationBranding**: Deaktiviert SafeLinks für deine Organisation.

Tracking: Beachte, dass das Tracking von Link-Klicks aus Datenschutzsicht heikel sein kann. Je nach lokalen Vorschriften darfst du diese Aktivität nur unter bestimmten Voraussetzungen erfassen – zum Beispiel mit entsprechenden Schutzmaßnahmen oder klarer Kommunikation gegenüber deinen Benutzern. Trotzdem ist diese Funktion extrem hilfreich für die Analyse von Vorfällen. Du kannst damit sehr schnell herausfinden, wer sonst noch auf einen Link geklickt hat, der später als bösartig eingestuft wurde!

Erstellen einer Safe Links-Richtlinie

Abbildung 6-3 zeigt dir die verschiedenen Einstellungen, die du beim Erstellen einer neuen Safe Links-Richtlinie vornehmen kannst. Mit einer eigenen Richtlinie kannst du ein individuelles Safe Links-Erlebnis schaffen, das über den Funktionsumfang der eingebauten Schutzrichtlinie hinausgeht.

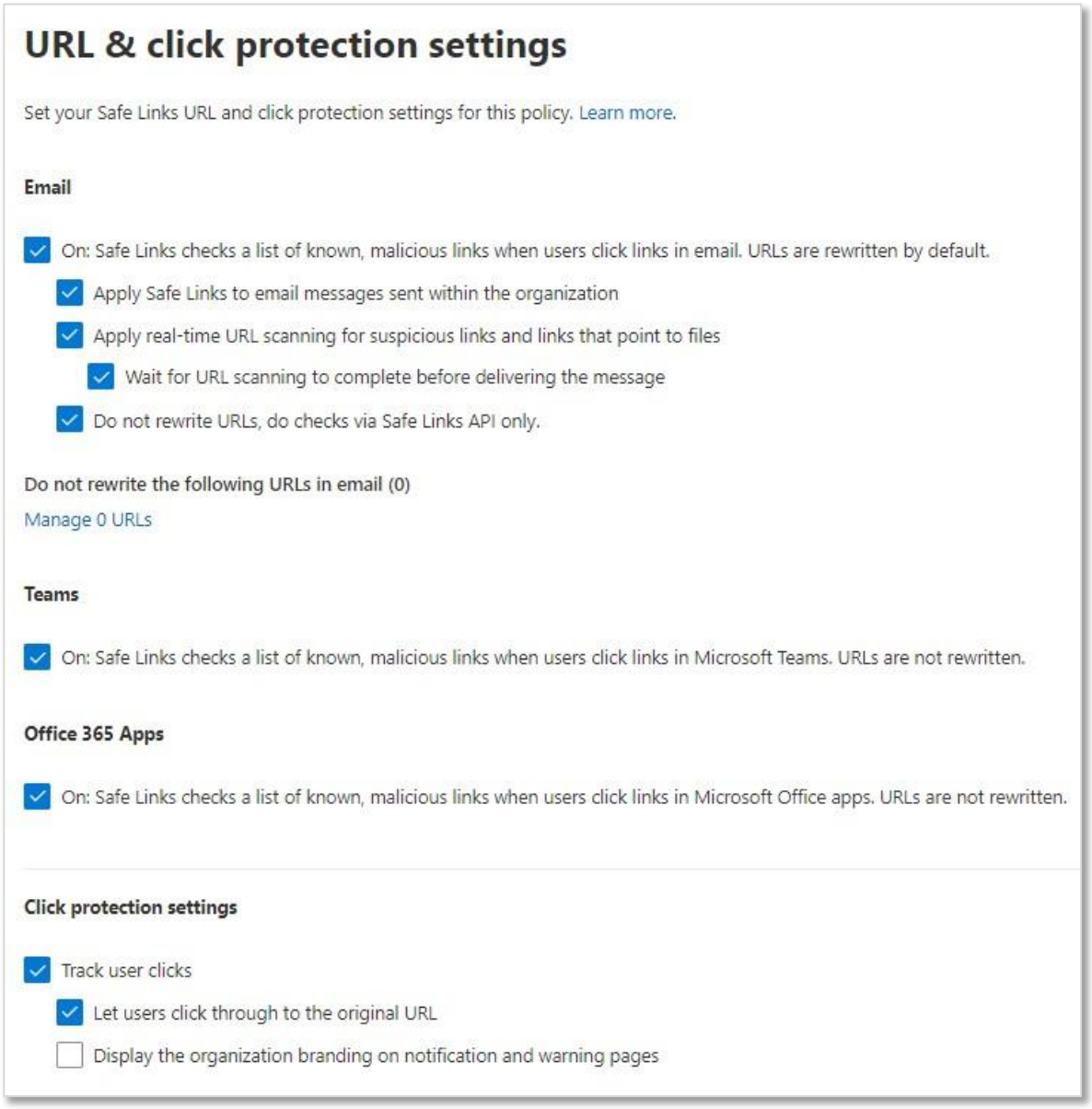


Abbildung 6-3: Erstellen einer Safe Links-Richtlinie

In der Abbildung siehst du, dass es vier konfigurierbare Bereiche für Safe Links gibt: E-Mail, Teams, Office 365-Apps und Click Protection Settings.

Um eine neue Richtlinie zu erstellen, klickst du auf **Erstellen**. Dann wird der Assistent "Safe Links-Richtlinie erstellen" auf der rechten Seite eingeblendet. Innerhalb der Richtlinie kannst du folgende Einstellungen vornehmen:

- **Aktionen für bekannte, bösartige URLs in (E-Mail-)Nachrichten**: Hier legst du fest, ob Links umgeschrieben werden sollen.

- Ob Safe Links Nachrichten, die **innerhalb der Organisation** gesendet werden, ebenfalls umschreiben soll.
- Echtzeit-Scannen von Links, die auf **Dateien** verweisen.
- **URL-Scan-Abschluss vor der Zustellung**: Du kannst festlegen, ob E-Mails erst nach abgeschlosseneme URL-Scan zugestellt werden. Wenn du die Zustellung nicht verzögerst und Benutzer bereits auf einen Link klicken, während die Remote-Webseite noch geprüft wird, erscheint eine Info, dass der Scan noch nicht bageschlossen ist und sie es später erneut versuchen sollen.
- **Bestimmte Links** aus dem Umschreibungsprozess **ausschließen** – ideal für vertrauenswürdige interen URLs wie Intranet- oder SharePoint.
- Aktionen für bekannte, bösartige URLs in **Microsoft Teams:** Bestimme, ob Safe Links für Microsoft Teams aktiviert wird.
- Aktionen für bekannte, bösartige URLs in **Microsoft 365-Apps:** Aktiviere Safe Links für diese Apps.
- Ob Klicks **verfolgt** werden sollen.
- Ob Benutzern trotzdem **auf die ursprüngliche URL zugriefen dürfen**, nachdem sie als potenziell gefährlich erkannt wurde. Die Best-Practice ist, das nicht zu erlauben, um sie nicht unnötig zu gefährden.
- Ob das **Organisationsbranding** auf Benachrichtigungs- und Warnseiten angezeigt werden soll.

Im letzten Schritt des Assistenten legst du den Geltungsbereich fest, also für welche Benutzer oder Gruppen die Richtlinie gilt. Der Anwendungsbereich entspricht dem von Exchange Online Protection, den du bereits in Kapitel 4 kennengelernt hast.

Verwendung von PowerShell zum Erstellen einer neuen Safe Links-Richtlinie

Auch wenn du Richtlinien direkt im Security Center erstellen und ändern kannst, lassen sich Safe Links-Richtlinien ebenfalls per PowerShell konfigurieren. Hier ein Beispiel für einen One-Liner, mit dem du das, was du über die Weboberfläche gemacht hast, in PowerShell umsetzen kannst:

```
New-SafeLinksPolicy -Name ‘Safe Links Policy - Damian' -IsEnabled $True -
EnableSafeLinksForTeams $True -ScanUrls $True -DeliverMessageAfterScan $True EnableForInternalSenders $True -AdminDisplayName 'Apply a policy just to Damian for testing.'
```

Du musst dabei noch einen zusätzlichen Schritt durchführen – nämlich den Geltungsbereich der Richtlinie mit dem Cmdlet New-SafeLinksRule neu erstellen:

```
New-SafeLinksRule -Name ‘Safe Links Rule - Damian' -SafeLinksPolicy
'Safe Links Policy - Damian' -RecipientDomainIs M365securitybook.com -
ExceptIfSentTo damian@m365securitybook.com
```

Denk daran, dass Richtlinie und Regel immer paarweise verwendet werden, wenn du Safe Links gezielt auf bestimmte Benutzergruppen oder Domänen anwenden willst.

Berichterstellung

Wenn Klicks blockiert, durchgeleitet oder anderweitig verarbeitet werden, findest du diese Informationen im Bericht „URL-Bedrohungsschutz“ unter „E-Mail & Zusammenarbeit“. Du solltest diese Berichte regelmäßig prüfen – sie sind im Abschnitt „E-Mail & Zusammenarbeit Berichte“ im Security Admin Center verfügbar.

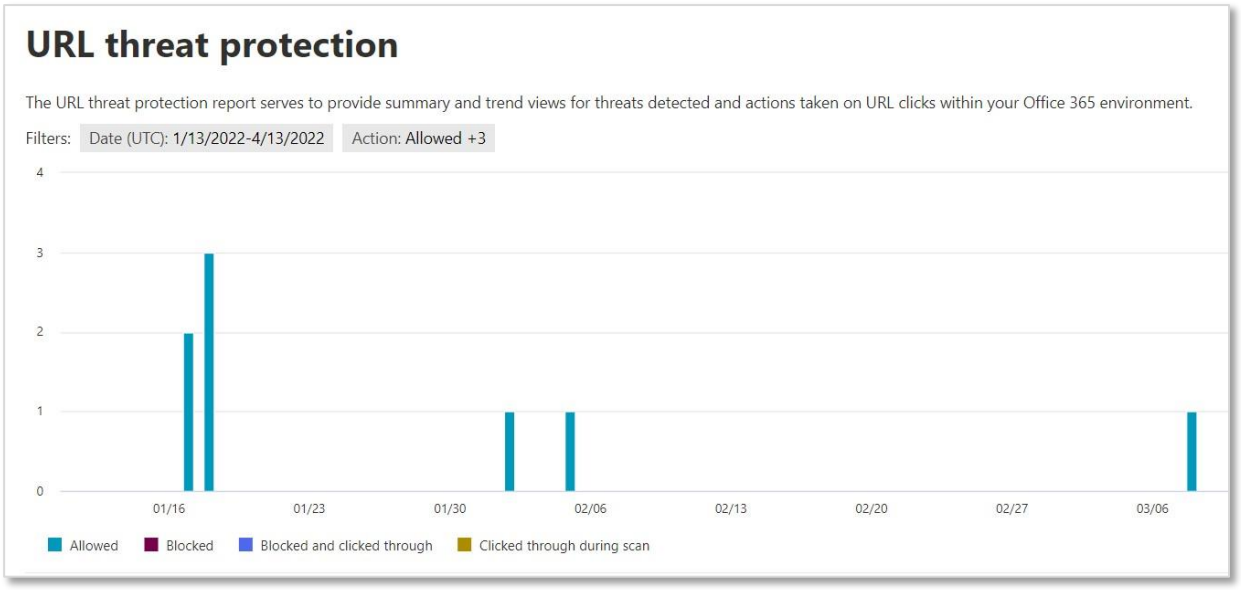


Abbildung 6-4: URL-Bedrohungsschutzbericht

Neue Aktionen wurden inzwischen in der GA-Version für alle Mandanten freigeschaltet: „Vom Mandantenadministrator zugelassen“, „Vom Mandantenadministrator blockiert“, „Ausstehender Scan“ sowie „Vom Mandantenadministrator blockiert und durchgeklickt“. Beim Filtern nach Anwendungen stehen dir neue Optionen zur Verfügung. Dafür klickst du zuerst auf die Schaltfläche „Daten anzeigen nach…“ unter dem Diagramm.

WICHTIG: Priority Accounts können jetzt als separates Tag verwendet werden - anstelle der Standardeinstellung „Alle“. Entferne dazu einfach das Tag „Alle" und füge stattdessen das Tag „Priority Account" hinzu.

Sobald du dies ausgewählt hast, kannst du deine Filteroptionen festlegen. Diese enthalten nun die Kategorien E-Mail-Client, Office-Dokument und Teams.

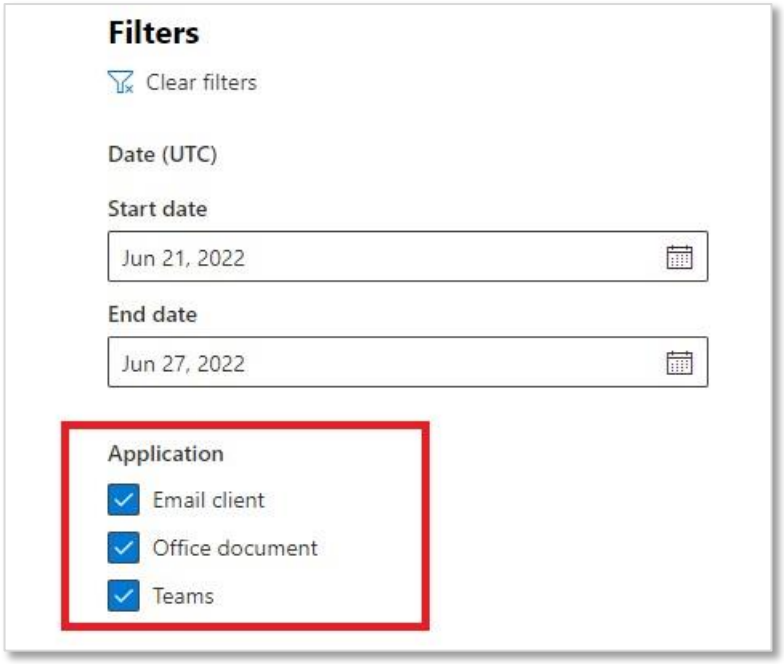


Figure 6-5: Applikationsfiltertypen.

Benutzererfahrung

Wenn für einen Benutzer eine Safe Links-Richtlinie gilt und er eine E-Mail erhält, werden alle Links hinter einer langen URL verschleiert, die ATP als Teil seiner Verarbeitung generiert. Wäre der Link wirklich bösartig, könntest du ihn nicht öffnen. In Abbildung 6-6 siehst du einen Originallink („Original URL“). In der Leiste darunter befindet sich die umgeschriebene URL, wie sie von Safe Links generiert wurde.

Abbildung 6-6: Echter Link und der 'Safe Link'.

Wenn eine Website als potenziell gefährlich eingestuft wird, wird der Benutzer daran gehindert, sie zu besuchen. Beachte, dass in diesem Beispiel auch ein Link mit der Aufschrift „Trotzdem fortfahren“ vorhanden ist. Dieser Link wird nur angezeigt, wenn Deine Richtlinie Benutzern erlaubt, trotzdem auf die ursprüngliche URL zu klicken.

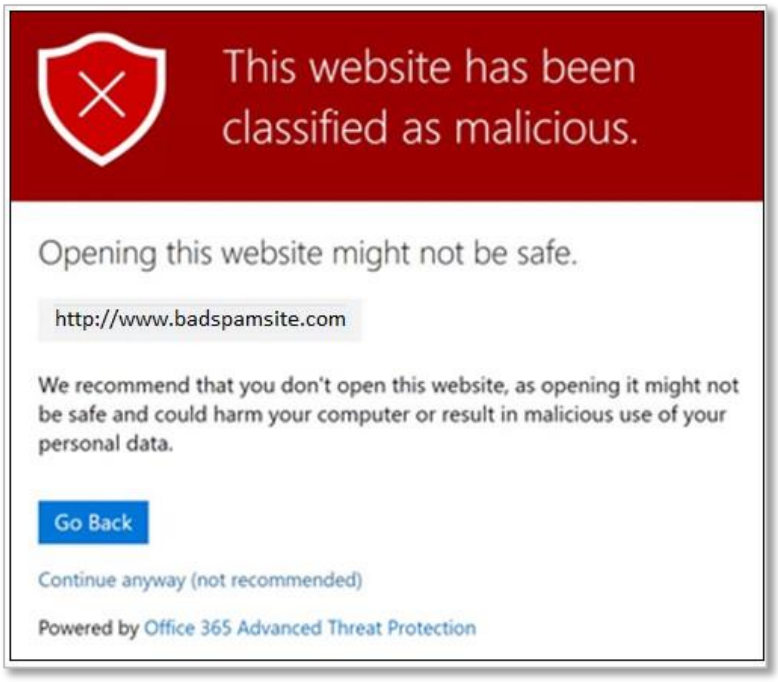


Abbildung 6-7: Wenn ein Link bösartig ist und blockiert wird, würdest du stattdessen dies sehen.

Browserunabhängig: Das Blockieren bösartiger Websites ist browserunabhängig. Es hängt nicht von clientseitigen Komponenten ab, sondern basiert auf der regulären Weiterleitung des Webverkehrs. Daher spielt es keine Rolle, ob die Benutzer Microsofts eigene Browser oder einen Browser von Drittanbietern wie Google Chrome oder Mozilla Firefox verwenden.

Safe Attachments

Fast so lange wie es E-Mails gibt, werden Anhänge zwischen Personen verschickt. Diese Anhänge können Berichte, Rechnungen, Dokumentationen oder viele andere Dateitypen sein – darunter PDFs, Word-Dokumente, Excel-Dateien und mehr. Leider nutzen Angreifer diesen Weg auch, um beispielsweise falsche Rechnungen oder ZIP-Dateien mit ausführbaren Inhalten zu versenden. Zusätzlich musst du dich auch mit Makros oder Skripten in Dateien beschäftigen, die schädlichen Code auf dem System ausführen könnten. Daher besteht seit jeher die Notwendigkeit, Benutzer und ihre Postfächer vor bösartigen Anhängen zu schützen.

Safe Attachments nimmt einen Anhang und analysiert ihn in einer virtuellen Umgebung – einer sogenannten Sandbox –, um festzustellen, ob die Datei bösartig ist. Wenn sie unbedenklich ist,

wird sie sicher an das Postfach des Endbenutzers zugestellt. Bei Anhängen, die als bösartig erkannt werden, kannst du konfigurieren, ob sie verworfen oder an einen anderen Ort zugestellt werden sollen. Je nach Konfiguration von Safe Attachments kann die Nachricht auch zugestellt werden, während der Anhang im Hintergrund gescannt wird.

Safe Attachments ist nicht nur für E-Mails in Exchange Online verfügbar, sondern auch für Teams, SharePoint Online und OneDrive for Business. Safe Documents lässt sich ebenfalls in den Safe Attachments-Richtlinien sowie in den globalen Defender-Einstellungen konfigurieren und wird im Anschluss an diesen Abschnitt behandelt.

Konfigurieren von Safe Attachments

Die Konfiguration von Safe Attachments erfolgt ausschließlich im Microsoft 365 Defender-Portal. Öffne dazu das Microsoft 365 Defender-Portal und navigiere im Abschnitt **E-Mail und Zusammenarbeit** zu **Richtlinien und Regeln**. Wähle dort **Bedrohungsrichtlinien** und schließlich **Safe Attachments**.

Globale Einstellungen

Klicke auf „Globale Einstellungen“. Es wird eine Seitenleiste eingeblendet, in der Du konfigurieren kannst, ob Safe Attachments für SharePoint, OneDrive und Teams aktiviert werden soll. Die Aktivierung dieser Einstellung verhindert, dass Benutzer Dateien öffnen, die als bösartig eingestuft wurden – auch wenn sie spontan in SharePoint, OneDrive oder die Registerkarte „Dateien“ in Teams hochgeladen werden.

Zweitens kannst du Safe Documents konfigurieren. Weitere Details zu diesem Thema folgen später in diesem Kapitel.

Erstellen einer neuen Safe Attachment-Richtlinie

Beim Erstellen einer neuen Safe Attachments-Richtlinie kannst du unter anderem die folgenden Einstellungen festlegen:

- **Safe Attachment Malware Response**: Wenn ein Anhang Malware enthält, must du entscheiden, wie mit der Nachricht umgegangen werden soll. Es stehen fünf Optionen zur Verfügung - Aus, Überwachen, Blockieren, Ersetzen oder Dynamische Zustellung. Standardmäßig ist **Aus** aktiviert, wwodurch keine Überprüfung durch die Safe Attachments-Engine erfolgt. **Überwachen** eignet sich, wenn du lediglich protokollieren möchtest, was erkannt wird, ohne Maßnahmen zu ergreifen. **Dynamische Zustellung** – nur verfügbar für Postfächern in Exchange Online - stellt die nachricht zunächst ohne Anhang zu. Wird der anhang als ungefählrich eingestuft, wird er nachgeliefert.

Andernflass bleibt der Anhang zurückgehalten. **Blockieren** verhindert die Zustellung der gesamten Nachricht, wenn der Anhang Malwre enthält.

- **Quarantänerichtlinie**: Hier jkannst du eine Quarantänerichtlinie für E-Mails festlegen, die durch die Safe Attachment-Richtlinie blockiert wurden.
- **Anhang bei Erkennung umleiten**: Wenn ein bösartiger Anhang blockiert, überwacht oder ersetzt wurde, kann er zur Analyse oder Information an ein anderes Postfach weitergeleitet werden.

Schließlich musst du – wie bei allen anderen Richtlinien – den Geltungsbereich der neuen Richtlinie festlegen. Dies erfolgt auf ähnliche Weise wie bei Safe Links oder den anderen Exchange Online Protection-Richtlinien.

Erstellen einer neuen Safe Attachment-Richtlinie mit PowerShell

Wie bei Safe Links kannst du auch mit PowerShell eine geeignete Safe Attachment-Richtlinie und -Regel konfigurieren. Es gibt einige Einstellungen – wie auch bei Safe Links –, die du mit PowerShell nicht konfigurieren kannst. Wenn du beispielsweise eine Richtlinie erstellen möchtest, die für eine Domäne gilt, dynamische Zustellung durchführt, Einstellungen für Timeouts und Fehler anwendet, aber keine Umleitung vornimmst, wenn der Anhang entfernt wird, kannst du dies wie folgt tun. Zunächst erstellst du eine neue Richtlinie.

```
New-SafeAttachmentPolicy -Name ‘Safe Attachments – Practical PowerShell’ –
AdminDisplayName ‘Protect the M365securitybook.com domain – Safe Attachments’
-Action DynamicDelivery -ActionOnError $True
```

Als Nächstes weist du der Richtlinie einen Geltungsbereich zu, indem du eine neue Regel erstellst.

```
New-SafeAttachmentRule -Name `Safe Attachment Rule - M365securitybook.com' -
Comments
`Safe Attachment Rule for the M365securitybook.com domain.' -
RecipientDomainIs
`M365securitybook.com' -SafeAttachmentPolicy 'Safe Attachments - Practical
PowerShell'
```

Manchmal treten beim Erstellen von Richtlinien unbeabsichtigte Folgen auf. Daher siehst du möglicherweise Warnungen wie diese, wenn du Safe Attachments über PowerShell konfigurierst.

```
WARNING: Dynamic Email Delivery is for O365 hosted mailboxes only. If this action is chosen for a recipient with a
non-hosted mailbox, then a Replace action will be taken for that recipient.
```

Sowie:

```
WARNING: The 'Enable redirect' option should be selected when 'Apply the above selection if malware scanning for
attachments times out or error occurs' is selected. Not enabling redirect could result in loss of messages.
```

Die erste Warnung besagt, dass die dynamische Zustellung nur für gehostete Postfächer verwendet werden sollte. Es ist jedoch gut zu wissen, dass bösartiger Inhalt vor der Zustellung ersetzt wird, wenn ein Postfach nicht von Exchange Online gehostet wird. Die zweite Warnung zeigt dir, dass du eine Postfach- oder Empfängeradresse angeben musst, wenn du eine Aktion für Elemente festlegst, die eine Zeitüberschreitung oder einen Fehler verursachen. Mit der konfigurierten Safe Attachments-Funktion wird eine E-Mail-Nachricht von einem externen Absender verarbeitet.

Integrierte Richtlinien! Integrierte Richtlinien folgen Microsofts Secure by Default-Modell. Theoretisch bist du durch eine integrierte Richtlinie von Microsoft auch dann geschützt, wenn du keine eigene Safe Attachments-Richtlinie erstellt hast. Beachte, dass du Benutzer bei Bedarf von der Standardrichtlinie ausschließen kannst.

Benutzererfahrung

Die Benutzererfahrung variiert je nach Plattform. Abbildung 6-8 zeigt, wie das in SharePoint Online und OneDrive for Business aussehen kann. Der rote Schild weist darauf hin, dass eine Datei als bösartig erkannt wurde.

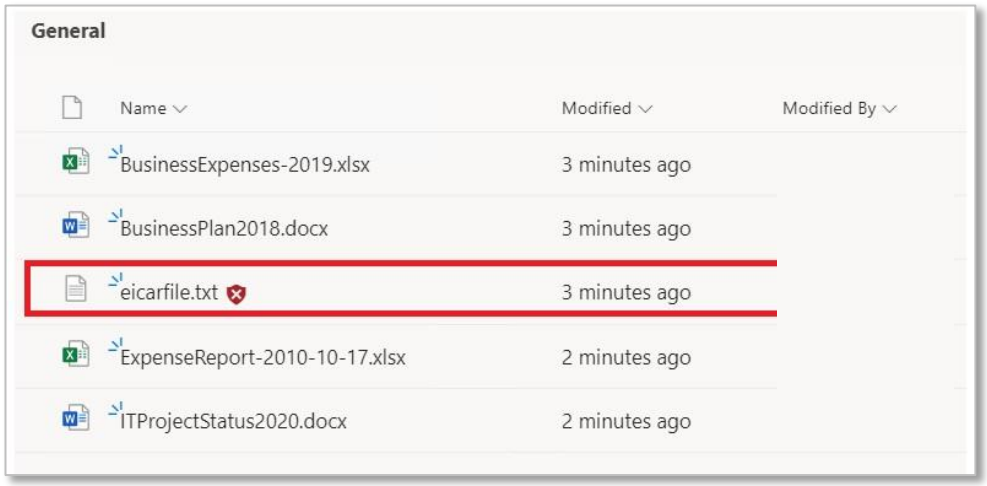


Abbildung 6-8: Benutzererfahrung mit Safe Attachment in SharePoint Online.

Wenn jemand versucht, auf eine infizierte Datei zuzugreifen, sie herunterzuladen oder zu öffnen, wird er mit einer entsprechenden Warnmeldung konfrontiert:

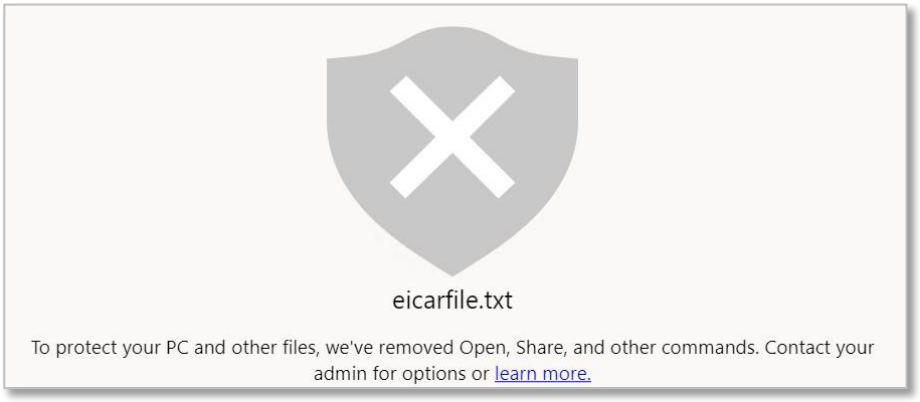


Abbildung 6-9: Safe Attachment-Warnung in SharePoint Online

Standardmäßig können Benutzer potenziell bösartige Dateien wie im obigen Beispiel trotzdem herunterladen. Glücklicherweise kannst du dieses Verhalten als SharePoint-Administrator ändern und verhindern, dass solche Dateien heruntergeladen werden. Dazu musst du einen bestimmten Befehl in SharePoint Online ausführen. Beachte, dass es sich hierbei um eine mandantenweite Einstellung handelt, die für alle gilt – auch für Administratoren, die die Datei vielleicht zur weiteren Analyse benötigen.

```
Set-SPOTenant -DisallowInfectedFileDownload $true
```

Hintergrund-Scannen: Das Scannen beginnt im Hintergrund, sobald eine Datei hochgeladen wird. Nach Abschluss des Scans greift das beschrieben Szenario und verhindert, dass sich infizierte Dateien weiter verbreiten. Die empfohlene Maßnahme bei einer erkannten Bedrohung ist das vollständige Entfernen der Datei. Beachte, dass das Scannen etwas Zeit in Anspruch nehmen kann, sodass eine leichte Verzögerung zwischen dem Hochladen und der Blockierung auftreten kann.

Safe Documents

Safe Documents ist Teil der Microsoft Defender für Office 365 Suite und standardmäßig deaktiviert. Diese Funktion ist sowohl in den globalen Microsoft Defender-Einstellungen als auch in den Safe Attachment-Richtlinien konfigurierbar. Safe Documents verwendet Microsoft Defender for Endpoint, um alle Dokumente zu analysieren. Um diese Funktion zu nutzen, musst du für Microsoft 365 E5 oder Microsoft 365 E5 Security lizenziert sein – sie ist nicht in der regulären Office 365 E5 enthalten. Das macht sie zu einer Premiumfunktion über die Basislizenz von Microsoft Defender hinaus.

Wie funktioniert Safe Documents

Safe Documents wird in Verbindung mit Microsoft Defender für Endpunkt verwendet. Über die Cloud-Infrastruktur von Defender für Endpunkt werden Dokumente analysiert und ein Urteil an den Client zurückgesendet, um zu bestimmen, was mit der Datei geschehen soll. Wenn die Funktion aktiviert ist, wirst du feststellen, dass Dokumente standardmäßig in einer geschützten Ansicht geöffnet werden. Um mit der Datei zu interagieren oder sie zu bearbeiten, musst du zuerst auf „**Bearbeitung aktivieren**“ klicken.

Abbildung 6-10: Geschützte Ansicht in einem Dokument.

Die geschützte Ansicht soll dich vor Dokumenten schützen, die möglicherweise bösartigen Inhalt von extern enthalten. Natürlich werden nicht alle Dokumente auf diese Weise gesendet, aber die geschützte Ansicht dient als Sicherheitsmaßnahme für den Fall, dass ein Dokument zu schädlichen Zwecken versendet wurde. In diesem Modus ist die Bearbeitung deaktiviert, Add-Ins in Anwendungen wie Word oder Excel funktionieren möglicherweise nicht vollständig, und auch Makros sowie weitere Inhalte bleiben deaktiviert, solange das Dokument im geschützten Modus geöffnet ist.

Wenn du auf „Bearbeitung aktivieren“ klickst, wird das Dokument freigegeben. Makros werden aktiviert, Add-Ins sollten wieder funktionieren und du kannst das Dokument anschließend bearbeiten und drucken.

Wenn ein Dokument in die geschützte Ansicht versetzt wird, können Fehler auftreten oder Probleme entstehen, die dich daran hindern, es zu öffnen. Die Überprüfung kann fehlschlagen oder beeinträchtigt sein, wenn das Dokument größer als 60 MB ist. Wenn festgestellt wird, dass eine Datei bösartigen Inhalt enthält, erscheint oben im Dokument eine rote Leiste und die Bearbeitung wird blockiert. Es gibt eine Übersteuerungsfunktion, die in den globalen Microsoft Defender für Office 365-Einstellungen steuerbar ist. Sie erlaubt dir, die Bearbeitung auch dann zu aktivieren, wenn bösartiger Inhalt erkannt wurde.

Konfigurieren von Safe Documents

Wie in Abbildung 6-11 dargestellt, wird Safe Documents als Teil der globalen Safe Attachments-Einstellungen aktiviert. Du kannst festlegen, ob die Funktion aktiviert werden soll und ob du trotz einer Warnung wegen bösartigen Inhalts durch die geschützte Ansicht klicken darfst – zum

Beispiel bei einem infizierten Makro. Aus nachvollziehbaren Gründen solltest du diese Option nur in Ausnahmefällen aktivieren.

Abbildung 6-11: Aktivieren von Safe Documents.

Alternativ kannst du Safe Documents auch über Exchange Online PowerShell aktivieren. Wenn du die Bearbeitung von potenziell bösartigen Dokumenten per PowerShell erlauben willst, kannst du den entsprechenden Befehl ausführen.

```
Set-AtpPolicyForO365 -AllowSafeDocsOpen $True
```

Um sicherzustellen, dass bösartige Dokumente blockiert werden, verwende den folgenden Befehl:

```
Set-AtpPolicyForO365 -AllowSafeDocsOpen $False
```

Anti-Phishing

In Kapitel 5 haben wir bereits einige der integrierten Anti-Phishing-Funktionen von Exchange Online Protection behandelt. Zur Erinnerung: Phishing ist eine ausgeklügelte Methode, bei der Angreifer versuchen, deine Benutzerbasis mithilfe von Social Engineering dazu zu bringen, sensible Informationen preiszugeben. Das können Anmeldedaten sein, Zugänge zu internen Systemen oder jedes andere Ziel, das ein Angreifer im Visier hat.

Es gibt drei bekannte Arten von Phishing-Angriffen:

- **Reguläres Phishing**: Der häufigste Angriff, bei dem ein bösartige Akteur versucht, den Empfänger – meist zufällig ausgewählte Personen innerhalb einer Organisation - dazu zu

bringen, eine bestimmte Aktion auszuführen und zusätzliche Informationen wie Benutzernamen und Passwort usw. anzugeben.

- **Spear Phishing**: Ein gezielter Angriff, bei dem eine Person für Social Engineering ausgewählt wird. Der Angreifer hat dabei oft bereits konkrete Inforamtionen über die Zielperson, um glaubwürdiger aufzutreten.
- **Whaling**: Ein gezielter Angriff auf Führungskräfte eines Unternehmens. Dabei werden subtile Methoden verwendet, die etwa steuerbezogene Inhalte, Anfragen zur sozialen Absicherung oder Aufforderungen zu Geldtransfers enthalten können.

Wie funktioniert der Anti-Phishing-Schutz?

Microsoft hat seine Anti-Phishing-Funktion so konzipiert, dass sie beim Erkennen dieser Bedrohungen hilft, indem sie auffällige Merkmale von Phishing-E-Mails identifiziert. Eingehende Nachrichten werden mithilfe maschinellen Lernens analysiert. Dabei prüft das System, ob Anzeichen für eine Phishing-Mail vorliegen. In Kombination mit der Funktion „Mailbox Intelligence“ kann eine E-Mail als legitim eingestuft werden, wenn bereits eine Beziehung zwischen dem Absender und dem Empfänger besteht und keine Auffälligkeiten erkennbar sind. Stammt die E-Mail hingegen von einer unbekannten Adresse, wird sie besonders genau untersucht. Maschinelles Lernen hilft dabei, die Absicht der Nachricht zu entschlüsseln. Wenn die Mail als Phishing erkannt wird, erfolgt die Verarbeitung nach der Anti-Phishing-Richtlinie, die dem jeweiligen Postfach zugewiesen ist.

Konfigurieren von Anti-Phishing

Anti-Phishing-Richtlinien kannst du in der Microsoft Defender-Konsole konfigurieren. Wie geht das?

Navigiere dazu im Microsoft 365 Defender-Portals zum Bereich E-Mail und Zusammenarbeit und öffne dort den Abschnitt „Richtlinien und Regeln“. Wähle anschließend „Bedrohungsrichtlinien“ und schließlich „Anti-Phishing“. So gelangst du zur Konfigurationsseite. In einer neuen Umgebung sind zunächst keine benutzerdefinierten Anti-Phishing-Richtlinien vorhanden. Standardmäßig gibt es keine, was zu erwarten ist. Du kannst dir aber über eine Schaltfläche die Standardrichtlinie anzeigen lassen, wie in der zugehörigen Abbildung dargestellt.

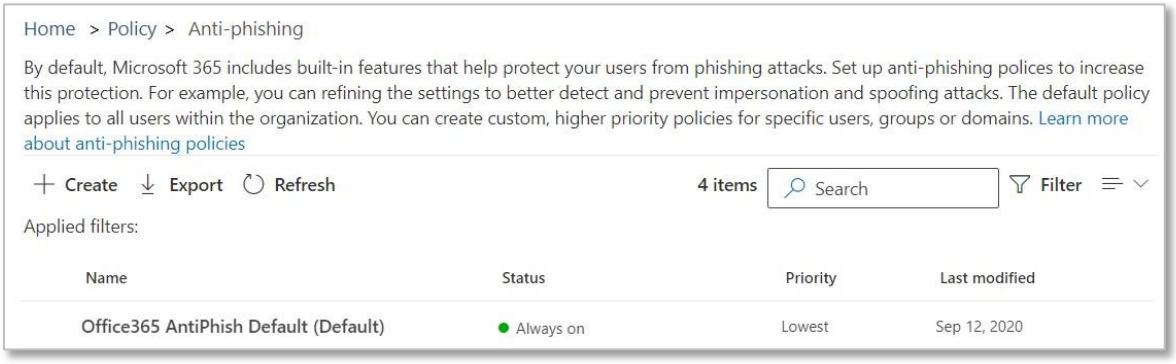


Abbildung 6-12: Überprüfen der integrierten Anti-Phishing-Richtlinie

Wenn du die Standard-Anti-Phishing-Richtlinie überprüfst, fällt auf, dass – obwohl es sich um eine Standardrichtlinie handelt – keine Benutzer in der Richtlinie definiert sind. Die logische Schlussfolgerung könnte sein, dass niemand durch die Standard-AntiPhish-Richtlinie geschützt ist. Das stimmt jedoch nicht. In Wirklichkeit sind alle Benutzer von der Standardrichtlinie erfasst.

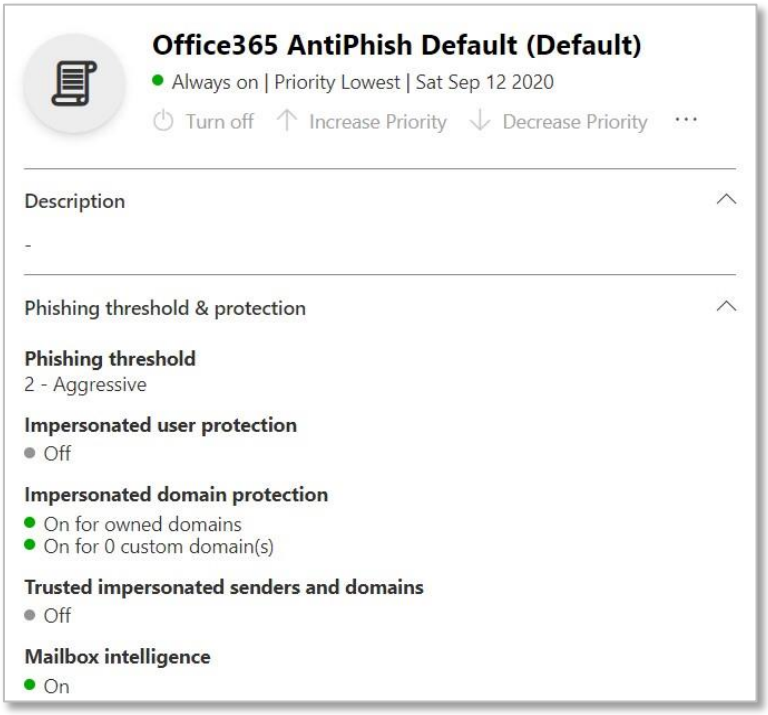


Abbildung 6-13: Einstellungen für die Standardrichtlinie.

Das bedeutet, dass diese Standardrichtlinie mit Einstellungen vorhanden ist, die für alle Benutzer gelten. Die empfohlene Vorgehensweise besteht darin, die Richtlinie an deine Umgebung anzupassen und dann separate, benutzerdefinierte Richtlinien für besonders schützenswerte Ziele wie Führungskräfte oder andere leitende Angestellte deines

Unternehmens zu erstellen. Du solltest dir die verfügbaren Optionen genau ansehen, um besser zu verstehen, ob die Standardrichtlinie aktualisiert werden sollte oder nicht.

Um eine neue Richtlinie zu erstellen, klickst du auf **„+ Erstellen**“. Im Gegensatz zu den meisten anderen Richtlinien ist das Erstellen einer Anti-Phishing-Richtlinie ein zweistufiger Prozess. Zuerst legst du die Richtlinie an, die nur ein Platzhalter für die Einstellungen ist. Dafür gibst du einen Namen, eine Beschreibung und einen Geltungsbereich an. Der Geltungsbereich funktioniert genau wie bei anderen Richtlinien.

Im zweiten Schritt bearbeitest du die soeben erstellte Richtlinie, indem du sie auswählst und dann den oder die Abschnitte auswählst, die du anpassen möchtest.

Identitätswechsel

In diesem Abschnitt konfigurierst du Einstellungen, die einen relevanten Schutz gegen Identitätswechselangriffe bieten.

Dabei handelt es sich um den Versuch eines Angreifers, sich als jemand anderes innerhalb der Organisation auszugeben.

- **Zu schützende Benutzer**: Sollte eine Liste mit besonders gefährdeten Zielen innerhalb deiner Organisation sein. Entgegen der landläufigen Meinung handelt es sich hierbei nicht um die Benutzer, für die die Richtlinie gilt. Stattdessen enthält diese Liste die Namen von Personen, die anfälliger für Identitätswechsel-Angriffe sind - etwa Führungskräfte der C-Ebene oder andere leitenden Personen, die durch einen Identitätswechsel dazu gebracht werden könnten, bestimmte Aufgaben auszuführen, wie zum Beispiel eine Überweisung. Du kannst auch externe Adressen von Partnerunternehmen hinzufügen, um dich besser vor eingehenden Identitätswechselversuchen zu schützen.
- Wie bei der vorherigen Option gibt es auch bei den **zu schützenden Domänen** oft Verwirrung. Hier steuerst du, ob Nachrichten, die deine eigenen Domains zu imitieren scheinen, besonders überprüft werden sollen. Wenn dein Unternehmen beispielsweise Eventbrite heißt, könnten Angreifer versuchen, den Namen Eventbrlte zu fälschen. Da in vielen Schriftarten i und l sehr ähnlich aussehen, kkann dies den Eindruck erwecken, dass die Nachricht aus deiner internen Domäne stammt. Es wird empfohlen, alle deine Domänen automatisch zu schützen.
- **Aktion(en)**: Bei den Aktionen für Benutzeridentitätswechsel, Domänenidentitätswechsel und Mailbox Intelligence solltest du gemäß den Best Practices die Option „In Quarantäne verschieben“ wählen. Auch wenn das Verschieben in den Junk-E-Mail-Ordner technisch möglich ist, solltest du Benutzer vorher gut informieren, wie sie mit diesen E-Mails umgehen sollen. Andernfalls könnten gefährliche Nachrichten direct zugänglich sein, was zu schlechten Ergebnissen führen kann.

Sicherheitstipps & Indikatoren: Alle fünf Sicherheitstipps – Erster Kontakt, Benutzeridentitätswechsel, Domänenidentitätswechsel, Ungewöhnliche Zeichen, Nicht authentifizierte Absender und das „via“-Tag – solltest du aktivieren. Diese Tipps geben den Benutzern visuelle Hinweise darauf, dass mit der E-Mail etwas nicht stimmt. So können sie die Nachrichten mit der nötigen Vorsicht prüfen. Diese Funktion wird leicht übersehen, kann aber wie in Abbildung 6-13 aufgerufen werden.

Mailbox Intelligence: Mailbox Intelligence und der zugehörige Schutz sollten ebenfalls aktiviert sein. Mailbox Intelligence analysiert mithilfe künstlicher Intelligenz, mit wem ein Benutzer häufig kommuniziert. Basierend auf diesen Informationen lassen sich besser Entscheidungen darüber treffen, ob eine E-Mail als Phishing eingestuft werden sollte. Der Schutzmechanismus nutzt diese Erkenntnisse, um Identitätswechselversuche zu erkennen. Du kannst gezielte Aktionen festlegen – die empfohlene Vorgehensweise ist auch hier, verdächtige Nachrichten in Quarantäne zu stellen.

Führungskräfte sind die Schlimmsten! Sei vorsichtig, wenn du diese Richtlinien konfigurierst. Wenn du deine Führungskräfte in den Abschnitt *Zu schützende Benutzer* aufnimmst, werden eingehende Nachrichten von Personen mit dem gleichen oder einem ähnlichen Namen genau unter die Lupe genommen. Wir haben mehr als einmal erlebt, dass sich eine Führungskraft nicht mehr von ihrer privaten Adressen aus selbst erreichen konnte (z.B. John.Smith@gmail.com). Auch wenn klar ist, warum das ein Risiko darstellt, nimmt die Führungskraft es möglicherweise nicht so wahr, da du damit eine völlig legitime Aktion verhinderst. Das Hinzufügen dieser Adressen zur Positivliste ist nicht unbedingt ratsam, da du keine Kontrolle über die Sicherheit ihres persönlichen Postfachs hast.

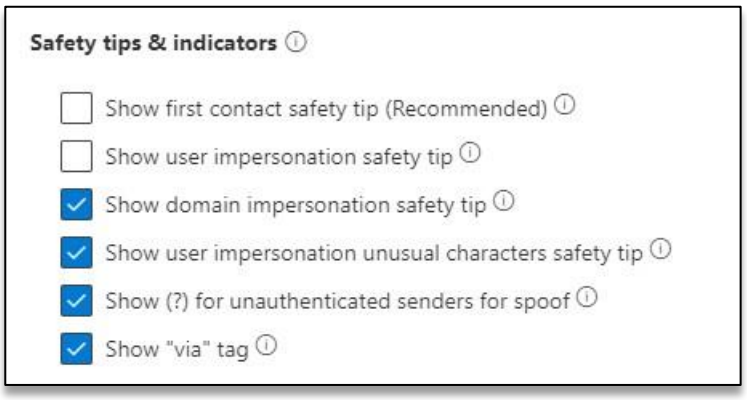


Abbildung 6-14: Anzeigen der Einstellungen für Sicherheitstipps in einer Anti-Phishing-Richtlinie.

Anti-Phishing-Richtlinien beinhalten jetzt auch eine DMARC-Option, mit der du steuern kannst, wie E-Mails entsprechend dem „p=-Wert“ einer Domäne behandelt werden. Standardmäßig ordnet Microsoft p=quarantine der Quarantäne-Aktion zu, während p=reject bedeutet, dass die Nachricht abgelehnt wird. Es gibt zwar weitere Optionen für den Umgang mit solchen

Nachrichten, aber die Empfehlung lautet, entweder Quarantäne oder Ablehnung zu konfigurieren.

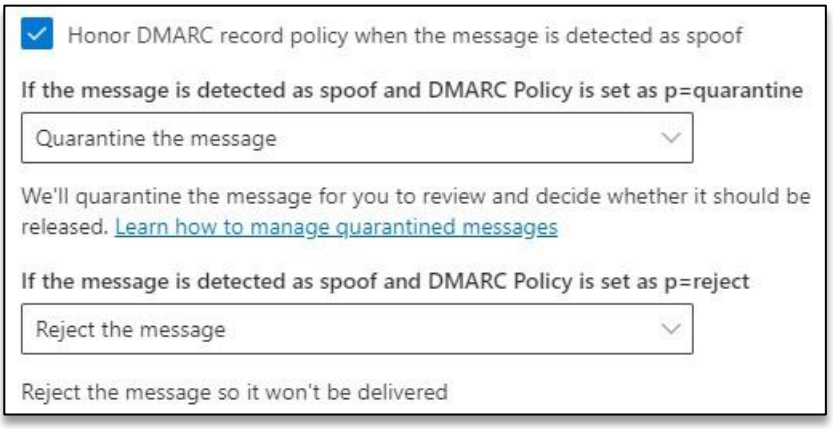


Abbildung 6-15: DMARC-Nachrichtenaktionen für Quarantäne und Ablehnung (Standardeinstellungen).

Spoof

In den Spoof-Intelligence-Einstellungen kannst du drei Funktionen anpassen.

- **Spoof Intelligence aktivieren**: Die Aktivierung von Spoof Intelligence ist standardmäßig eingeschaltet und sollte so belassen werden. Diese Funktion prüft, ob eine E-Mail zu geschäftlichen Zwecken – etwa von einem Drittanbieter, einem internen Dienst oder einem Benutzer, der im Namen einer anderen Person sendet – gespooft wurde. Spoof Intelligence nutzt dabei auch DNS-Einträge wie SPF, DMARC und DKIM. Beachte, dass Absender, die über sichere Outlook-Seiten verwendet werden, unter Umständen die Spoof-Intelligence-Überprüfung umgehen können.
- **Funktion für nicht authentifizierte Absender aktivieren**: Die Funktion erkennt, ob die Authentifizierung einer Nachricht fehlschlägt – etwa wenn SPF, DMARC oder DKIM nicht übereinstimmen. In dem Fall wird die E-Mail möglicherweise als Spoofing eingestuft. Als Aktion solltest du dann nicht den Junk-E-Mail-Ordner verwenden, sondern stattdessen „Nachricht unter Quarantäne stellen“ wählen, da dies einen besseren Schutz bietet.
- **Aktion**: Wenn eine E-Mail als Spoofing eingestuft wird, ist dies die Aktion, die für die E-Mail-Nachricht ausgeführt wird. Die Standardeinstellung besteht darin, die Nachricht in den Junk-E-Mail-Ordner eines Benutzers zu senden. Stattdessen wird empfohlen, diese Einstellung auf "Nachricht unter Quarantäne stellen" zu ändern.

Erweiterte Einstellungen

Die erweiterten Phishing-Schwellenwerte bestimmen, wie aggressiv Microsoft Defender für Office 365 Phishing-E-Mails erkennen soll. Standardmäßig ist der Wert auf 1 gesetzt, was einer normalen Verarbeitung entspricht. Du kannst diesen Wert auf 2 oder 3 erhöhen, um

aggressiver gegen Phishing-E-Mails vorzugehen. Bei Wert 2 werden Nachrichten mit hoher Phishing-Konfidenz als „Sehr hoch“ eingestuft. Bei Wert 3 wird auch mittlere Konfidenz als „Sehr hoch“ betrachtet. Wert 4 ist die aggressivste Einstellung: Jede Nachricht mit niedriger, mittlerer oder hoher Phishing-Konfidenz wird als „Sehr hoch“ eingestuft. Dabei musst du aber mit deutlich mehr falsch positiven Ergebnissen rechnen. Verwende diese Option also nur nach sorgfältiger Abwägung – sie sollte kein Bestandteil der Standardrichtlinie sein.

Neben der Erstellung und Verwaltung der Richtlinien im Microsoft 365 Defender-Portal kannst du sie auch per PowerShell bearbeiten – einschließlich Hinzufügen, Entfernen und Anpassen bestehender Richtlinien. Um die Befehle nutzen zu können, musst du dich zuerst mit Exchange Online PowerShell verbinden.

Konfigurieren von Anti-Phishing über PowerShell

Zusätzlich zur Erstellung und Verwaltung der Richtlinien im Microsoft 365 Defender-Portal kannst du Richtlinien bis hin zum Hinzufügen, Entfernen und Bearbeiten vorhandener Richtlinien auch mit PowerShell verwalten. Nachfolgend findest du einige schnelle Beispiele, wie du das tun kannst. Um die Befehle zu verwenden, stelle zunächst eine Verbindung zu Exchange Online PowerShell her.

Auflisten aller Richtlinien und Regeln (nach Name):

```
Get-AntiPhishPolicy | ft Name Get-
AntiPhishRule | ft Name
```

Erstellen einer neuen Richtlinie:

```
New-AntiPhishPolicy -Name 'Executive Anti-Phishing Protection' -AdminDisplayName
'This policy is designed to protect Executives from Phishing, Spear Phishing and
Whaling attacks.' -EnableOrganizationDomainsProtection $True -
TargetedUserProtectionAction Quarantine -MailboxIntelligenceProtectionAction
Quarantine -TargetedDomainProtectionAction Quarantine -PhishThresholdLevel 3 -
EnableSimilarUsersSafetyTips $True -EnableSimilarDomainsSafetyTips $True
EnableUnusualCharactersSafetyTips $True -EnableMailboxIntelligence $True -
EnableMailboxIntelligenceProtection $True -EnableSpoofIntelligence $True
EnableUnauthenticatedSender $True
```

Erstellen einer entsprechenden Regel:

```
New-AntiPhishRule -Name ‘Executive Anti-Phishing Protection’ -AntiPhishPolicy
‘Executive Anti-Phishing Protection’ -SentToMemberOf Executives@m365securitybook.com
```

Ändern einer Richtlinieneinstellung:

```
Set-AntiPhishPolicy 'Executive Anti-Phishing Protection' -AuthenticationFailAction
Quarantine
```

Vollständiges Entfernen einer Richtlinie:

```
Remove-AntiPhishPolicy 'Executive Anti-Phishing Protection' Remove-
AntiPhishRule 'Executive Anti-Phishing Protection'
```

Unterstützung des Endbenutzers

Auch wenn Microsoft über eine sehr gute Erkennungstechnologie verfügt, ist kein System zu 100 % zuverlässig. Deshalb beginnt Microsoft, Endbenutzer aktiv zu schulen, damit sie Phishing-Angriffe selbst besser erkennen. Dafür gibt es derzeit zwei Maßnahmen:

- **Attack Simulator**: Dies ermöglicht es Administratoren, simulierte Phishing-Angriffe auf Benutzer durchzuführen. Deren Verhalten kann beobachtet werden, und falls jemand auf eine Simulation hereinfällt, erhält er eine Erklärung, was passiert ist und wie man so etwas in Zukunft vermeiden kann. Auf den Simulator gehen wir später in diesem Kapitel noch genauer ein.
- **Endbenutzer-Schulung**: Dies ist eine geplante Funktion, die Benutzern direkt weiterhilft, verschiedene Angriffsarten zu verstehen. Microsoft arbeitet hierfür mit Terranova Security zusammen. Weitere Informationen zur Veröffentlichung findest du auf der folgenden Seite: https://www.microsoft.com/security/blog/2020/08/25/detect-mitigate-phishing-risks-microsoft-security

Advanced Delivery

Advanced Delivery wurde mit zwei Zwecken entwickelt. Erstens als „Phishing Simulation Override“ für Organisationen, die Phishing-Simulationslösungen von Drittanbietern einsetzen. Zweitens für ein Security Operations-Postfach, in dem ungefilterte E-Mails analysiert werden können. Beide Anwendungsfälle benötigen Ausnahmen auf verschiedenen Scan-Ebenen innerhalb von Exchange Online, damit die E-Mails ihr Ziel erreichen – sei es ein Benutzerpostfach für Tests oder ein spezielles SecOps-Postfach. Um Advanced Delivery zu verwenden, brauchst du eine Defender for Office 365 Plan 1 oder Plan 2 Lizenz.

Filterausnahmen

Advanced Delivery ermöglicht es, dass E-Mails die unten genannten Funktionen in Microsofts Scan-Engines umgehen können, wenn sie in das Zielpostfach zugestellt werden:

- Exchange Online Protection und Microsoft Defender für Office 365 Filter

- Zero-hour Auto Purge (ZAP)
- Standardwarnungen werden nicht ausgelöst
- Automated Incident Response (AIR) und Clustering

Bei Phishing-Simulationen, die von Drittanbietern durchgeführt werden, gelten folgende Ausnahmen:

- Eine gemeldete Nachricht erscheint im Bereich "Übermittlungen" von Defender für Office 365 als simulierte Bedrohung, und es wird keine Warnung oder AIR generiert. Das gilt sowohl für von Administratoren übermittelte Nachrichten als auch für von Benutzern übermittelte Nachrichten.
- Wenn eine URL in der Phish Sim Override angegeben wurd, löst diese URL keine Safe Links-Aktionen aus.
- Safe Attachments versucht auch nicht, Anhänge zu detonieren.

Einschränkungen: Du kannst den Malware-Filter oder ZAP für Malware nicht umgehen. Dies sollte zwar keine Auswirkungen auf eine Phishing-Simulation haben, ist aber wichtig zu wissen - besonders dann, wenn du eigenen Simulationen durchführst oder die Funktion für andere Zwecke (nutzen oder missbrauchen möchtest.

Phishing Simulation Override

Zuvor hast du bereits gesehen, wie Microsoft Phishing-E-Mails filtert und welche Mechanismen zur Verfügung stehen. Die Aktivierung verschiedener Schutzmethoden ist ein guter erster Schritt für jede Organisation. Trotzdem solltest du auch deine Endbenutzer schulen – für den Fall, dass bösartige E-Mails doch einmal durch Microsofts Filtermechanismen ins Postfach gelangen. Die Schulung kann über Microsofts eigenes Attack Simulation Training erfolgen, das in diesem Kapitel behandelt wird. Alternativ kannst du auch auf Schulungen oder Lösungen von Drittanbietern setzen. Wenn du Microsofts eigene Lösung nutzt, brauchst du die Funktion Phish Simulation Override nicht – denn diese Trainingsmails werden ohnehin nicht gefiltert, sondern direkt an das Benutzerpostfach zugestellt.

Benutzerübermittlungen: Wenn ein Benutzer einen Bericht über eine Phishing-E-Mail einreicht und diese Teil einer Simulation ist, wird kein Vorfall generiert (z. B. "E-Mail von Benutzer als Malware oder Phishing gemeldet"), was für Support-Teams von Vorteil ist.

Bei Drittanbietern war es bisher üblich, dass technische Artikel oder Wissensdatenbanken bereitgestellt wurden, die dich dazu auffordern, Exchange Online-Transportregeln oder andere Ausnahmen zu konfigurieren. Die Funktion Phish Sim Override vereinfacht diesen Prozess. Sie ermöglicht es, bestimmte Anbieter zu definieren, deren Simulationen die Filterung umgehen dürfen, damit die Trainings-E-Mail wie vorgesehen beim Benutzer ankommt.

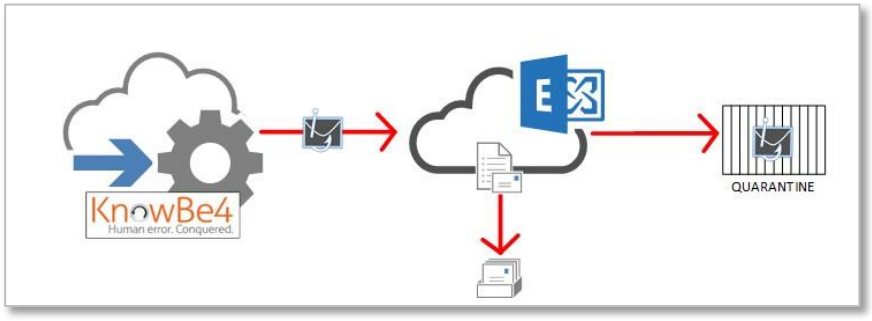


Abbildung 6-16: Phishing-E-Mails von KnowBe4 werden anstelle des Postfachs des vorgesehenen Benutzers in eine Quarantäne geleitet.

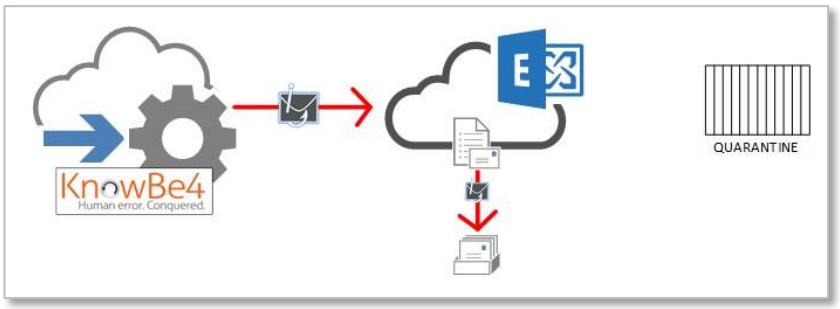


Abbildung 6-17: Mit aktivierter Phish Sim Override wird die E-Mail nun zur Simulationstestung an den Benutzer zugestellt.

Konfigurieren von Phishing Simulation Overrides

Um diese Funktion zu nutzen, gehst du ins **Security Center** > **E-Mail & Zusammenarbeit** > **Richtlinien** > **Bedrohungsrichtlinien** > **Advanced Delivery**. In einer neuen Umgebung wird dir dort zunächst eine leere Konfiguration angezeigt:

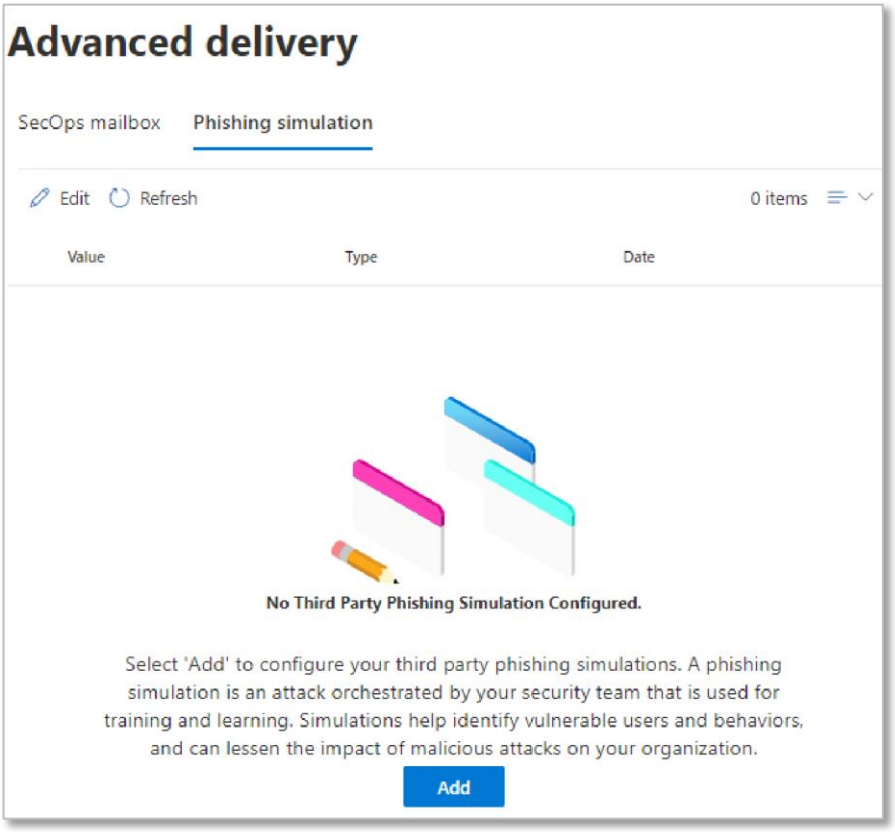


*Abbildung 6-18: Um eine neue Override für eine Simulation eines Drittanbieters zu erstellen, musst du auf den Button **Bearbeiten** oder den blauen Button unten klicken.*

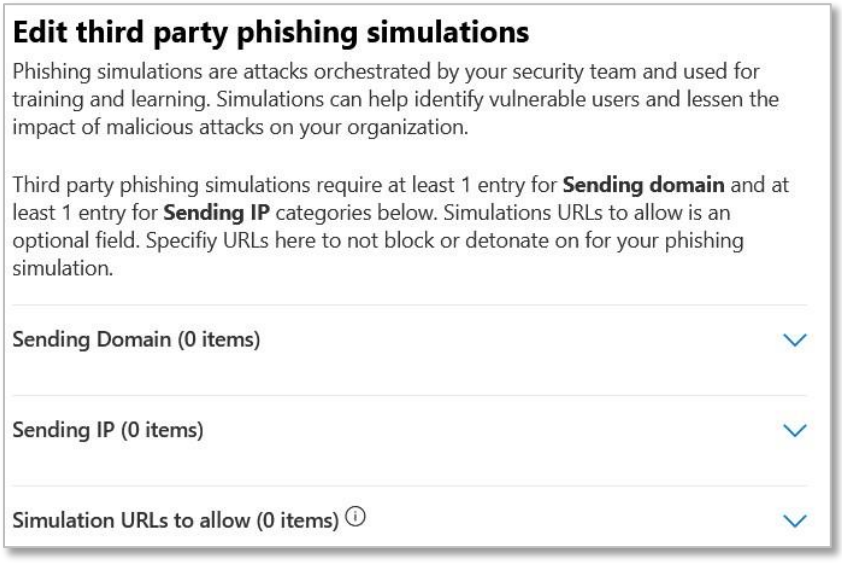


Abbildung 6-19: Konfigurationsoptionen für die Phishing Simulation Override.

- **Absenderdomäne**: Dieser Wert sollte mit der Domäne des Drittanbieters übereinstimmen und in den Headern der vom Drittanbieter gesendeten simulierten Phishing-E-Mail erscheinen.
- **Absender-IP**: IP-Adressen der E-Mail-Server des Drittanbieters, die zum Versenden dieser simulierten E-Mails verwendet werden.
- **Zuzulassende Simulations-URLs**: Wenn es spezielle URLs gibt, die in das Training einbezogen werden, kannst du diese angeben, um Phish-Sim-E-Mails besser zu identifizieren.

Hinweis: Microsoft hat die Handhabung von URLs in Phishing-Sim-E-Mails geändert, und Administratoren müssen diese nicht mehr angeben, da sie automatisch zugelassen werden.

PowerShell

Zusätzlich zur GUI kannst du auch PowerShell-Cmdlets verwenden, um die Einstellungen für Phish Simulation Override zu konfigurieren und zu verwalten. Die Cmdlets stehen zur Verfügung, nachdem du eine Verbindung zur Security and Compliance Center PowerShell hergestellt hast.

```
Connect-IPPSSession
```

Um die verfügbaren Cmdlets abzurufen, gib Folgendes ein:

```
Get-Command *-PhishSim*
```

Zum Zeitpunkt des Schreibens sind die folgenden Cmdlets verfügbar:

```
Get-PhishSimOverridePolicy Get-PhishSimOverrideRule
New-PhishSimOverridePolicy
New-PhishSimOverrideRule
Remove-PhishSimOverridePolicy
Remove-PhishSimOverrideRule
Set-PhishSimOverridePolicy Set-PhishSimOverrideRule
```

Der erste Schritt besteht darin, eine Phish Sim Override-Richtlinie zu erstellen:

```
New-PhishSimOverridePolicy -Name 'KnowBe4PhishOverridePolicy'
```

Hinweis: Beachten Sie, dass der für Richtlinie und Regel angegebene Name ohne Warnung vollständig ignoriert wird. In einem Mandanten kann nur eine Richtlinie und eine Regel erstellt werden.

Nach dem Erstellen der Richtlinie muss der Richtlinie eine Regel hinzugefügt werden:

```
New-PhishSimOverrideRule -Name 'KnowBe4PhishOverridePolicy' -Policy
'KnowBe4PhishOverrideRule' -SenderDomainIs BigBox.Com, MediumBox.Com -SenderIpRanges
147.160.167.0/26, 23.21.109.197,23.21.109.212
```

Die Phish Sim Override-Funktion ist nur für Organisationen wirklich nützlich, die einen Phish-Sim-Anbieter von Drittanbietern nutzen und deshalb Exchange Online-Transportregeln umgehen müssen. Wenn du so einen Anbieter verwendest, solltest du diese Funktion nutzen. Wenn du Microsofts proprietäre Lösung verwendest oder keine Simulationen oder Tools von Drittanbietern einsetzt, solltest du diese Funktion nicht verwenden.

Missbrauch vermeiden: Ich kann nachvollziehen, dass manche Leute in Erwägung ziehen könnten, diese Funktion zu nutzen, um die Filterung für andere Szenarien als Angriffssimulationen zu umgehen. Und obwohl das theoretisch möglich ist, solltest du es wahrscheinlich nicht tun. Es gibt andere Möglichkeiten, (einige) Filterfunktionen zu umgehen. Zum Beispiel mithilfe von Transportregeln usw.

Bedrohungsschutzstatus und Außerkraftsetzungen

Wenn E-Mails von diesen Overrides verarbeitet werden, kannst du sie im Bedrohungsschutzstatusbericht im Security Admin Center sehen, der sich hier befindet. Wenn du die Ergebnisse nach Systemüberschreibungen filterst und nach „Phishing Simulation“ sortierst, solltest du eine Ausgabe wie diese erhalten:

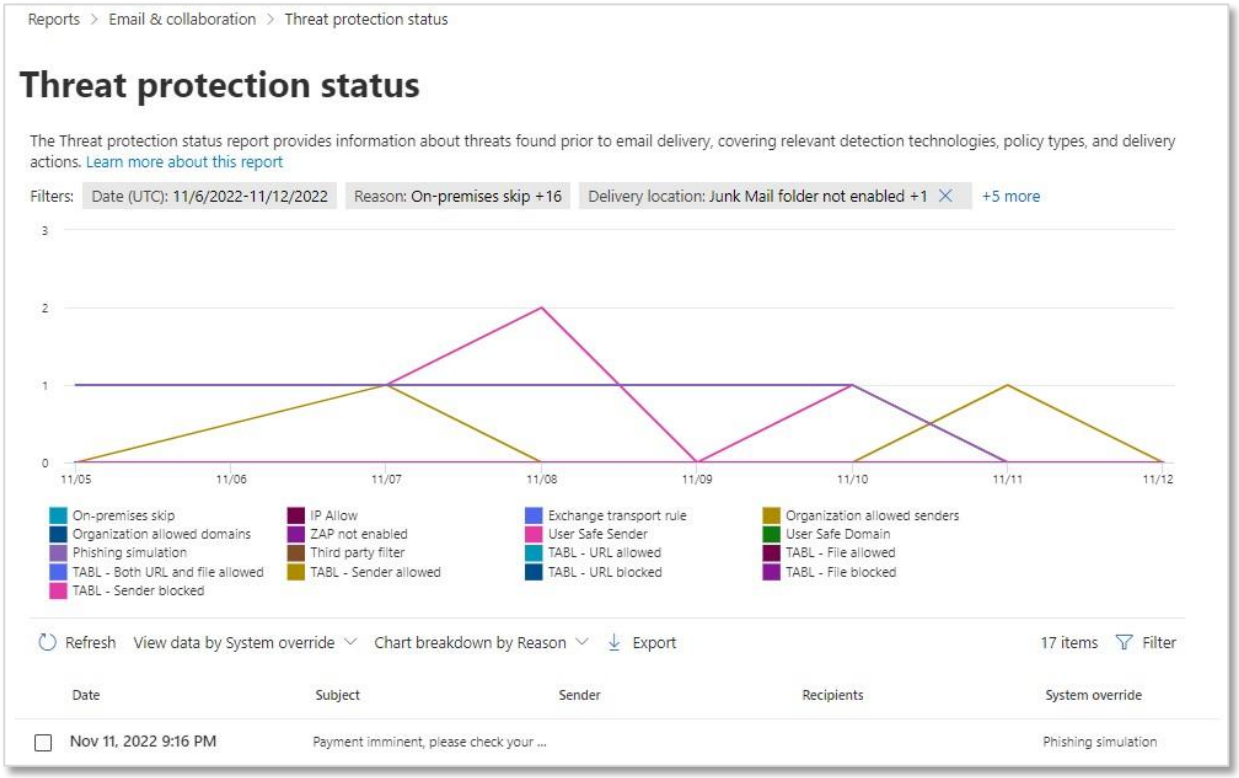


Abbildung 6-20: Bedrohungsschutzstatusbericht

Dieser Bericht ist nützlich, um aufzudecken, woher diese Phishing-Simulations-E-Mails stammen (überprüfe die IP-Adressen, um sie einem konfigurierten Dienst zuzuordnen), aber auch, wer der Zielempfänger war. Jede Nachricht kann erweitert werden, und weitere Details können auch einem Administrator angezeigt werden, der diese E-Mails untersucht.

Änderung für die Standardsicherheit

Mit den neuen Optionen für Phish Simulation Exception und SecOps Mailbox hat Microsoft nun die Sicherheitskompromisse der Exchange-Transportregeln (ETRs) im Visier, die Kunden in Exchange Online einbauen. Microsoft gibt an, dass 60 % der E-Mails, die die Überprüfung umgehen, über ETRs erfolgen und eine Sicherheitslücke darstellen, die so weit wie möglich kontrolliert und geschlossen werden muss. Du solltest daher mit einer Verhaltensänderung rechnen, wenn es darum geht, wie ETRs zwischen dieser Version und einem zukünftigen Update in der Praxis funktionieren.

Wie bei früheren Änderungen sind ETRs nun Teil der Liste von Funktionen, die nicht verwendet werden können, um Malware und Phishing-E-Mails mit hoher Konfidenz zuzulassen.

Du musst keine eigene Richtlinie aktivieren, da es sich um eine „standardmäßig aktivierte“ Funktion handelt. Die Regeln funktionieren größtenteils wie bisher, aber es landen

wahrscheinlich mehr Elemente in der System-Quarantäne, wenn sie wirklich bösartig sind. Du solltest also darauf vorbereitet sein, die Quarantäne häufiger zu prüfen, falls E-Mails dort fälschlicherweise landen.

SecOps-Postfach

Zusätzlich zur Phish Simulation Override enthält Advanced Delivery auch eine Funktion, bei der ein dediziertes Postfach von einem internen Team zur Analyse ungefilterter E-Mails verwendet werden kann, die von der Organisation empfangen werden. Dies ist nützlich für weitere Analysen, die Sammlung von Bedrohungsinformationen oder einfach nur zu Testzwecken.

Konfigurieren des SecOps-Postfachs

Die Konfiguration des SecOps-Postfachs erfolgt ebenfalls in der Advanced-Delivery-Funktion im Security Center, aber auf einer separaten Registerkarte:

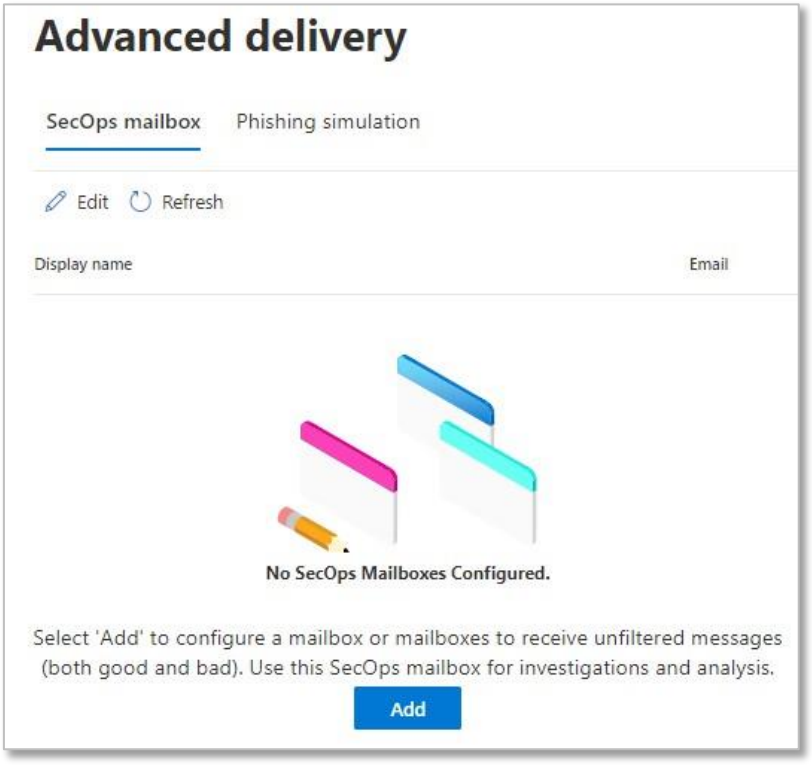


Abbildung 6-21: SecOps-Postfachkonfiguration in einem neuen Mandanten.

Die Konfiguration des SecOps-Postfachs erfolgt ebenfalls in der Advanced-Delivery-Funktion im Security Center, aber auf einer separaten Registerkarte. Wenn du auf „Bearbeiten“ klickst (oder auf „Hinzufügen“ unten in der Mitte des Bildschirms), erscheint ein kleines Popup-Fenster, in das du ein zuvor erstelltes SecOps-Postfach eingeben kannst. Sobald du Zeichen in das

Eingabefeld eintippst, sucht das System nach passenden Postfächern und zeigt dir „Vorgeschlagene Kontakte“ an. Je nach Größe deiner Umgebung sind das oft bereits die richtigen. Wenn du den richtigen Postfacheintrag auswählst, kannst du das speichern:

Abbildung 6-22: Hinzufügen eines einzelnen Postfachs mithilfe von vorgeschlagenen Kontakten, beachte, dass bei Bedarf mehr als ein Postfach ausgewählt werden kann, wenn mehrere Personen Nachrichten überprüfen müssen.

PowerShell

Eine Reihe von Cmdlets zum Erstellen, Auflisten, Ändern und Entfernen von SecOps-Außerkraftsetzungen sind im Security and Compliance Center PowerShell-Modul enthalten:

```
Get-SecOpsOverridePolicy Get-SecOpsOverrideRule
New-SecOpsOverridePolicy
New-SecOpsOverrideRule
Remove-SecOpsOverridePolicy
Remove-SecOpsOverrideRule
Set-SecOpsOverridePolicy Set-SecOpsOverrideRule
```

Zunächst must du, wenn du kein vorgefertigtes SecOps-Postfach hast, ein SecOps-Postfach erstellen, um ungefilterte E-Mails zu untersuchen:

```
New-Mailbox -Shared -Name 'SecurityTeam' -DisplayName 'Security Team' -Alias
SecurityTeam
```

Sobald es ein SecOps-Postfach gibt, das für die Richtlinien verwendet werden kann, kannst du die erforderliche Richtlinie und Regel mit PowerShell erstellen:

```
New-SecOpsOverridePolicy -Name SecTeamSecOpsOverridePolicy -SentTo
SecurityTeam@m365securitybook
New-SecOpsOverrideRule -Name SecOpsOverrideRule -Policy SecOpsOverridePolicy
```

HINWEIS: Der für die Cmdlets für Richtlinie und Regel verwendete Name wird ebenfalls ohne Warnung ignoriert. Derselbe Hinweis gilt für die Tatsache, dass nur eine Richtlinie und eine Regel erstellt werden können. Du kannst in der SecOps Override-Richtlinie trotzdem mehr als ein SecOps-Postfach angeben.

Verwenden von Get-Cmdlets zur Überprüfung unserer Einstellungen:

```
Get-SecOpsOverridePolicy
Get-SecOpsOverridePolicy
```

Die Erstellung und Verwaltung eines SecOps-Postfachs ist sinnvoll, wenn Personen dem Prozess der Überprüfung dieses Postfachs gewidmet werden können. Nicht jeder sollte mit dieser Aufgabe betraut werden, und die Verantwortlichen für die Pflege dieses Postfachs sollten sich des Inhalts sowie der Regeln und Verfahren für den Umgang mit den darin enthaltenen Nachrichten für Untersuchungen und erforderliche Maßnahmen bewusst sein. Wenn dieses Kriterium erfüllt ist, sollte das Postfach und die Funktion dem Mandanten zur Verfügung gestellt werden. Andernfalls kannst du dich heute auf Microsofts bereits leistungsstarke Untersuchungs- und Reaktionsfunktionen in Defender für Office 365 verlassen.

Threat Trackers

In einer Welt, in der Angriffe auf deine Cyber-Umgebung nie weit entfernt sind und viele Bedrohungsakteure mitmischen, ist es nicht nur wichtig, informiert zu bleiben, was um dich herum geschieht, sondern auch zu verstehen, welche Bedrohungen für dich relevanter sind als andere. Threat Trackers ist eine hilfreiche Funktion, die Administratoren einen Einblick in die für Office 365 und ihren Mandanten relevanten Bedrohungen bietet. Diese Funktion erfordert eine Microsoft Defender für Office 365 Plan 2-Lizenz. Um auf Threat Trackers zuzugreifen, öffnest du das Microsoft 365 Defender-Portal und navigierst zu Threat Tracker, das jetzt in einer aktualisierten Form vorliegt. In der oberen rechten Ecke befindet sich ein Umschalter, mit dem du zwischen der alten und der neuen Version wechseln kannst. In den folgenden Abbildungen siehst du das neuere Portal sowie das ursprüngliche Portal, das weiterhin zur Verwendung zur Verfügung steht.

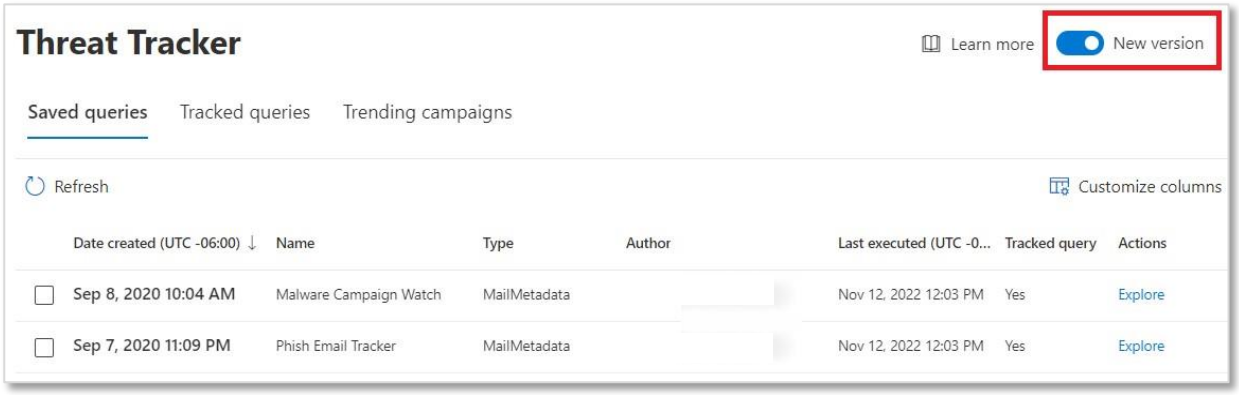


Abbildung 6-23: Neues Threat Tracker-Portal.

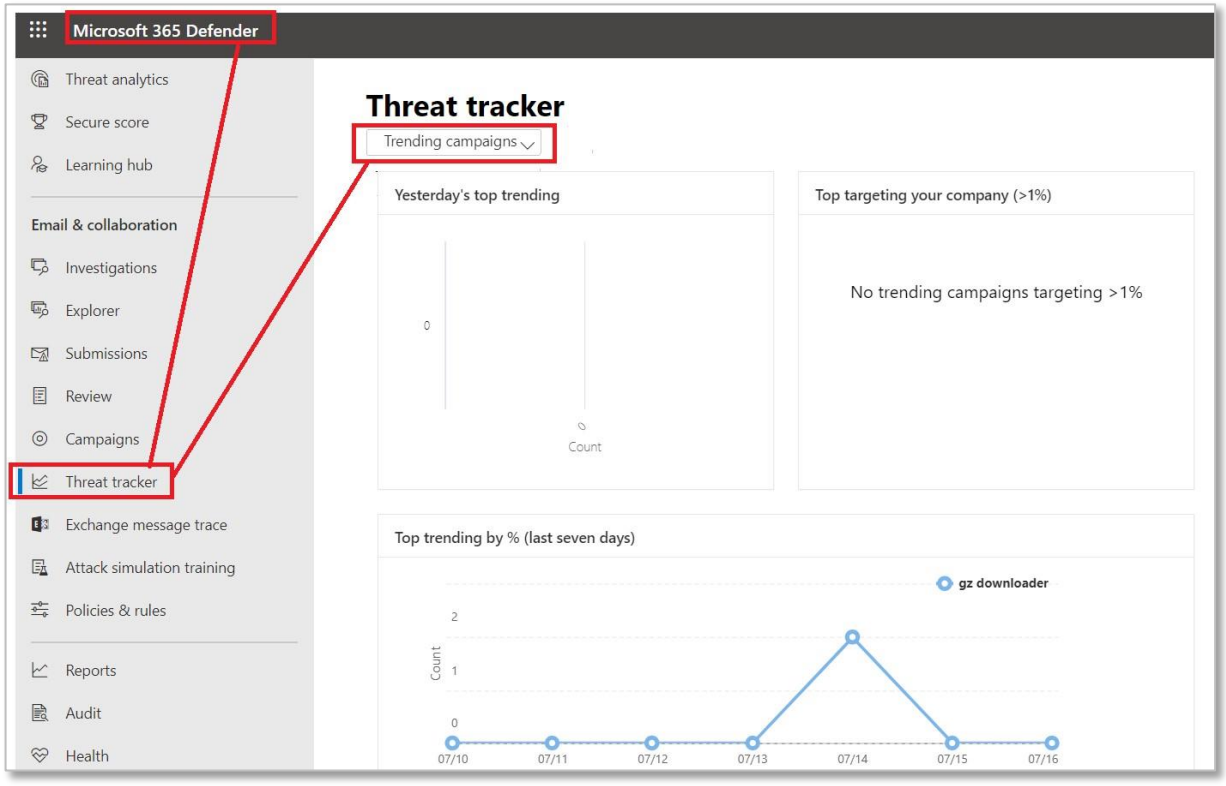


Abbildung 6-24: Ursprüngliches Threat Tracker-Portal.

Microsoft stellt diese Oberfläche zur Verfügung, damit die Administratoren eines Mandanten über Kampagnen und Bedrohungen informiert sind, die Microsoft verfolgt. Im alten Portal werden vier Optionen angeboten, im neueren Portal sind es nur noch drei.

Bemerkenswerte Kampagnen

Bemerkenswerte Kampagnen ist eine vorgefertigte Kampagnenverfolgung, die Microsoft auf Grundlage großer weltweiter Kampagnen erstellt hat. Diese werden so erstellt, dass du dich ebenfalls bewerten und schützen kannst, wobei Statistiken über ihre Auswirkungen bereitgestellt werden.

Die Option Bemerkenswerte Kampagnen wird nur dann ausgefüllt, wenn Microsoft Kampagnen bekannt machen möchte, die große Malware-Angriffe enthalten und über die ein Mandantenadministrator informiert sein sollte. Andernfalls bleibt diese Ansicht leer und enthält keine Daten – was auch zum Zeitpunkt des Schreibens dieses Kapitels der Fall war. Frühere Beispiele für bemerkenswerte Kampagnen sind Petya oder WannaCry.

Trend-Kampagnen

Diese Kampagnen basieren auf tatsächlichen Angriffen, die auf deinen Mandanten abzielen. Da in Trend-Kampagnen echte Daten für einen Mandanten angezeigt werden, kannst du möglicherweise Ergebnisse sehen oder auch nicht. Wenn keine Angriffe stattfinden, bleibt auch dieser Abschnitt leer.

Als Beispiel für eine leere Ansicht wird unten gezeigt, dass zu diesem Zeitpunkt keine aktuellen Trends vorliegen. Du kannst sehen, dass mehrere Angriffskampagnen in dieser Oberfläche verfolgt wurden. Die Kampagne wurde gestoppt, wie du anhand der Trenddaten (oben rechts) sowie der Zeile unten erkennen kannst, in der angegeben ist, dass sie global gestoppt wurde.

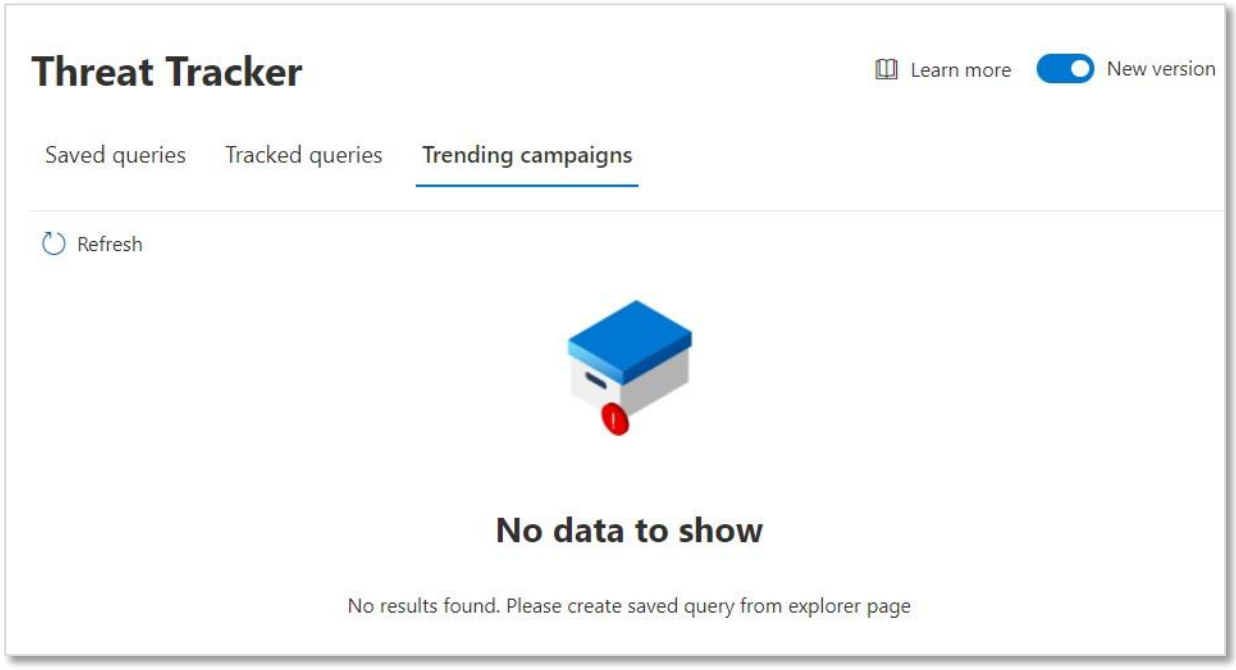


Abbildung 6-25: Trendende Kampagnen.

Tracked und Saved Queries

Die Tracked Queries enthalten Abfragen, die ein Administrator auf Basis seiner eigenen Daten aus der Funktion Threat Explorer erstellt hat, die später noch erläutert wird. Wenn diese Abfrage verfolgt wird, erscheint sie jetzt in der Ansicht Threat Trackers.

Beachte, dass die Daten nach der Aktivierung nicht sofort angezeigt werden. Es kann etwas dauern, bis sie eingehen, aber schließlich werden sie wie in Abbildung 6-24 dargestellt sichtbar:

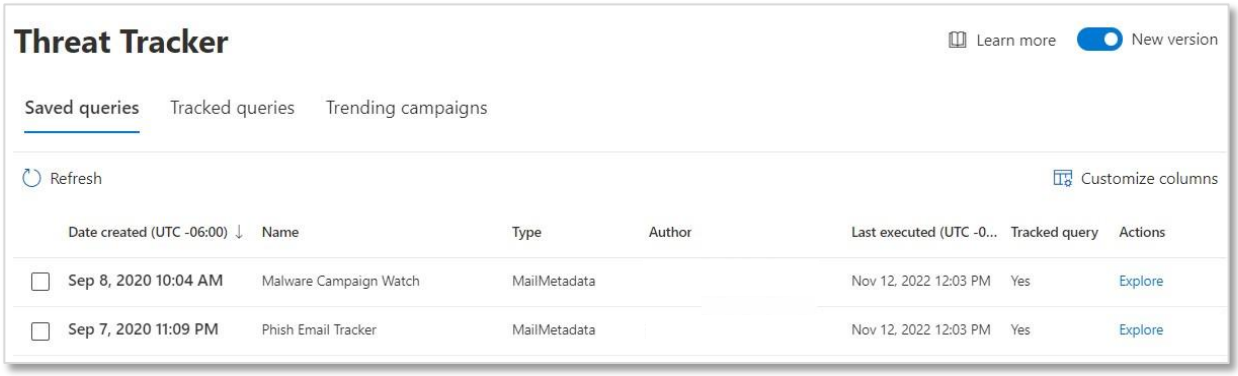


Abbildung 6-26: Überprüfen des Threat Trackers

Wenn du unter Aktionen neben der gespeicherten Abfrage auf „**Untersuchen**“ klickst, öffnet sich die Registerkarte **Explorer** mit der geladenen gespeicherten Abfrage. Wenn eine

gespeicherte Abfrage auch verfolgt wird, steht dir die gleiche Aktion „**Untersuchen**“ für diese Abfrage zur Verfügung. Dieselben Abfragen kannst du auch entfernen, wenn sie nicht mehr benötigt werden. Ein wichtiger Punkt dabei ist, dass die Explorer-Ansicht für diese Berichte auf die letzten 30 Tage beschränkt ist. Jede Abfrage, die älter ist – egal ob gespeichert oder verfolgt – hat einen leeren Datensatz und sollte zu diesem Zeitpunkt entfernt werden.

Abbildung 6-27: Explorer-Daten aus einer gespeicherten Abfrage.

Eine gespeicherte oder verfolgte Abfrage kannst du nach ihrer Erstellung auch ändern. Diese Änderungen beschränken sich auf die Datumsangaben der Abfrage (also den Bereich oder relative Daten) sowie darauf, ob die Abfrage weiterhin verfolgt werden soll. Verfolgte Abfragen sind hilfreich, wenn du bestimmte Ereignistypen regelmäßig überwachen möchtest. Beachte, dass die Berichte bei ihren Tracking-Möglichkeiten begrenzt sind. Außerdem kann es laut Microsoft bis zu einer Woche dauern, bis die Daten korrekt sind. Wenn du also eine Änderung an einem Tracker vornimmst, kann es bis zu einer Woche dauern, bis die Daten für diesen Tracker wieder genau sind.

Threat Explorer

Das Threat-Explorer-Feature – manchmal auch als Echtzeiterkennung in der GUI bezeichnet – ermöglicht es deinem Sicherheitsteam, im Auge zu behalten, was um dich herum und speziell mit deinem Mandanten geschieht. Nahezu in Echtzeit kannst du im Threat-Explorer-Dashboard durch verschiedene Informationsquellen navigieren und dir einen Überblick über Aktivitäten wie potenzielle Angriffe verschaffen, denen dein Mandant ausgesetzt ist. Zum Zeitpunkt des Schreibens bietet der Threat Explorer verschiedene Arten von Erkenntnissen:

- Für E-Mails kannst du Informationen über Phishing-Nachrichten, Nachrichten mit Malware, Übermittlungen (sowohl durch Administratoren als auch Benutzer) und aktive Kampagnen einsehen. Du kannst auch Einblicke in benutzerdefinierte Filter erhalten, indem du die Option „Alle E-Mails“ auswählst.

- Für Inhalte – also Informationen aus Safe Attachments in Office 365 – kannst du die Malware-Erkennungen der letzten 30 Tage anzeigen lassen.

In der folgenden Abbildung siehst du ein Beispiel für die E-Mail-Malware-Aktivität eines Mandanten in den letzten 30 Tagen.

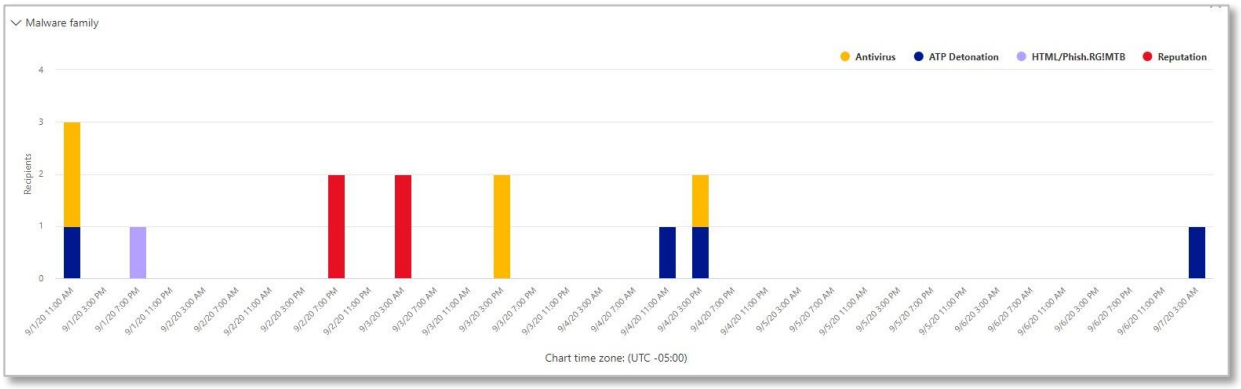


Abbildung 6-28: Aktuelle Aktivitäten im Explorer.

Die Legende oben rechts zeigt die verschiedenen erkannten Malware-Familien an. Wie du sehen kannst, enthält sie jedoch nicht immer den tatsächlichen Namen der Malware-Familie und ersetzt ihn manchmal durch die Art und Weise, wie die Malware erkannt wurde.

Unterhalb des Diagramms siehst du die Details (Quelldaten), aus denen das Diagramm besteht. Du kannst diese verwenden, um weitere Informationen zu bestimmten Ereignissen abzurufen oder gezielt Details zu überprüfen. Nützlich ist auch, dass du sofort erkennen kannst, ob eine Nachricht zugestellt wurde und – falls ja – wohin. In dem unten stehenden Beispiel kannst du beispielsweise sehen, dass die Nachricht an die Quarantäne zugestellt wurde.

Abbildung 6-29: Gefilterte Malware-Ansicht.

Je nachdem, welche Informationen du überprüfst, werden dir unterschiedliche Datensätze angezeigt. Wenn du zum Beispiel analysierst, für welche Kampagnen dein Mandant anfällig war, siehst du entsprechende Übersichten:

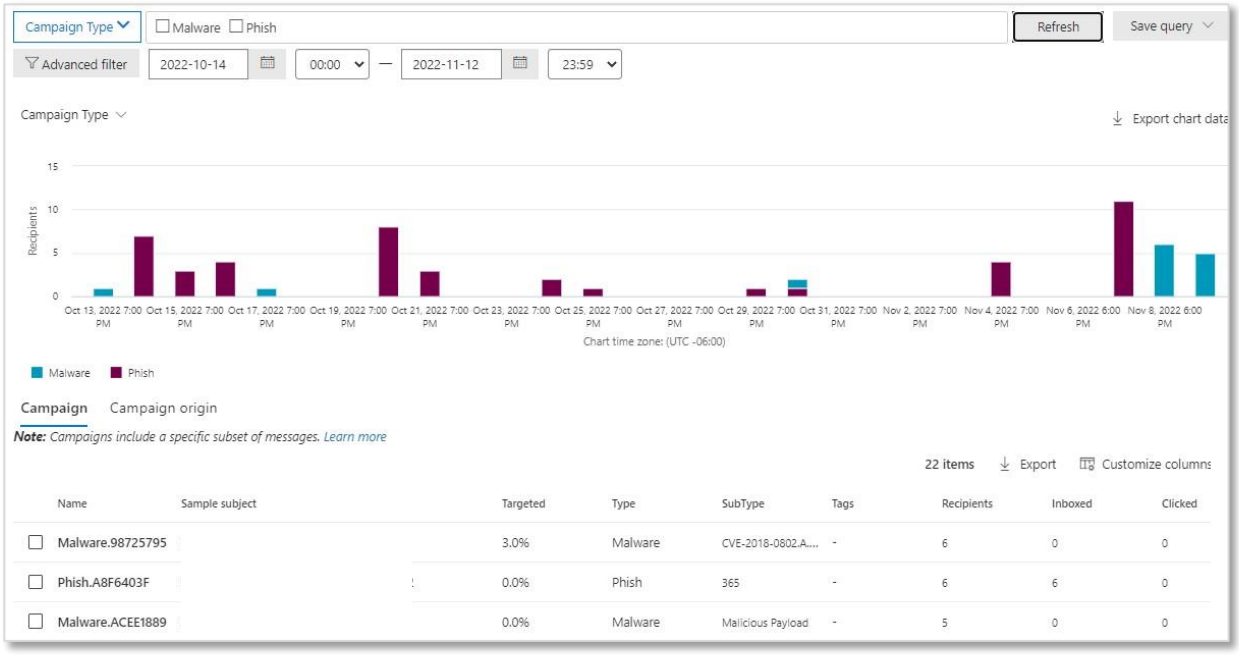


Abbildung 6-30: Kampagnenansicht.

Du kannst auf jede dieser Kampagnen klicken, um weitere relevante Informationen abzurufen – zum Beispiel, wie viele Nachrichten zugestellt wurden oder wie viele Personen auf eine URL geklickt haben. All diese Informationen sind sehr hilfreich, um ein besseres Verständnis der allgemeinen Cybersicherheitslage speziell für deinen Mandanten zu gewinnen.

Darüber hinaus kannst du über die Threat-Explorer-Oberfläche auch Maßnahmen gegen entdeckte Bedrohungen ergreifen:

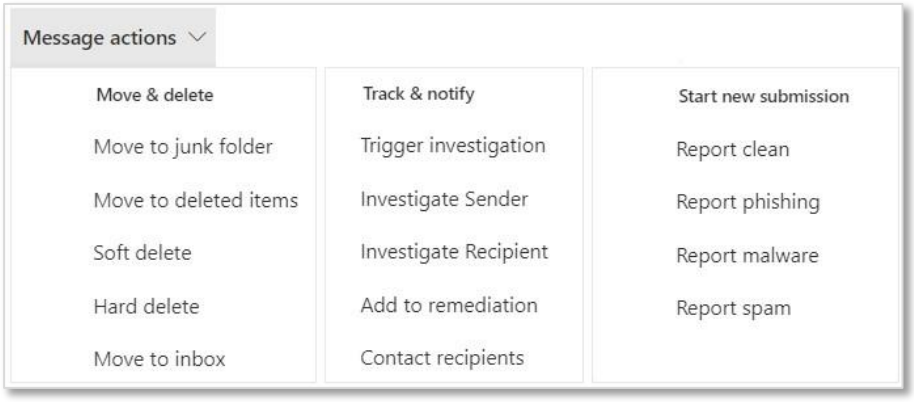


Abbildung 6-31: Threat Explorer-Aktionen

Unter den verfügbaren Optionen findest du verschiedene Aktionen, die du für eine E-Mail im Threat Explorer ausführen kannst. Du könntest zum Beispiel eine Untersuchung zu einer bestimmten E-Mail starten:

Abbildung 6-32: Eingeleitete Untersuchung.

Alternativ kannst du entscheiden, dass die E-Mail in den Junk-E-Mail-Ordner des Benutzers verschoben werden soll. Wenn du auf die Option „In Junk-E-Mail-Ordner verschieben“ klickst, erscheint ein Assistent, der dich durch den Prozess der Erstellung einer Korrekturaufgabe führt und bestimmte Informationen von dir abfragt :

- Name und Beschreibung
- Schweregrad. Dieser bezieht sich auf die Bedrohung und ist nützlich, wenn später Korrekturmaßnahmen überprüft werden.

Nach der Erstellung erscheinen die Korrekturen im Action Center, das du über **Überprüfen** > **Action Center** aufrufen kannst.

Filterfunktionen

Wenn du mit dem Threat Explorer arbeitest, möchtest du vielleicht verschiedene Visualisierungen erstellen – möglicherweise basierend auf einer Teilmenge von Benutzern, der Art des Angriffs oder im Falle von E-Mails dem Zustellort. So kannst du tiefer in eine bestimmte Kampagne einsteigen und prüfen, ob und wie viele Nachrichten an die Postfächer der Benutzer zugestellt wurden.

Innerhalb des Dashboards stehen dir zwei Möglichkeiten zum Filtern der Ergebnisse zur Verfügung:

- Verwenden der einfachen Filteroption, bei der du eine Bedingung und einen Wert auswählst und anschließend bei Bedarf weitere Bedingungen hinzufügst.
- Verwenden der erweiterten Filteroption, mit der du dieselben Bedingungen wie im Basisfilter in einer einzigen Abfrage kombinieren kannst (AND/OR). Das bietet dir deutlich mehr Flexibilität.

Das folgende Bild bietet einen Überblick über alle filterbaren Eigenschaften für E-Mail-Nachrichten:

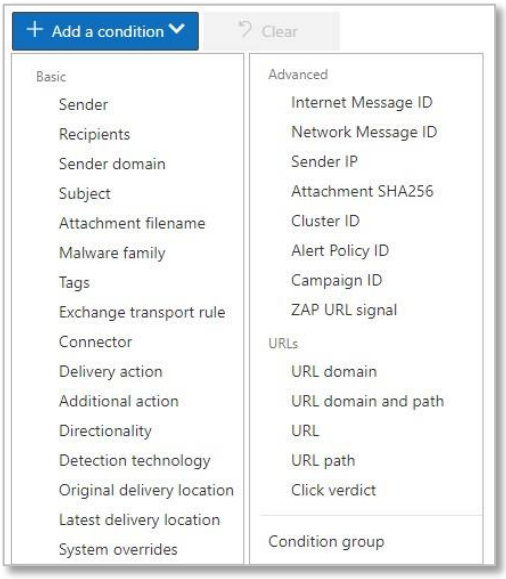


Abbildung 6-33: Erweiterte Filterung, verfügbare Bedingungen.

Mit diesen Filterbedingungen kannst du zum Beispiel eine Abfrage erstellen, die nach Phishing-Nachrichten sucht, die an bestimmte Empfänger oder Gruppen von Personen gesendet wurden. Wenn du Tags verwendest (diese Funktion befindet sich aktuell in der Vorschau) und einem Benutzer in deiner Organisation ein Tag zugewiesen hast, kannst du dieses Tag als Filterbedingung einsetzen.

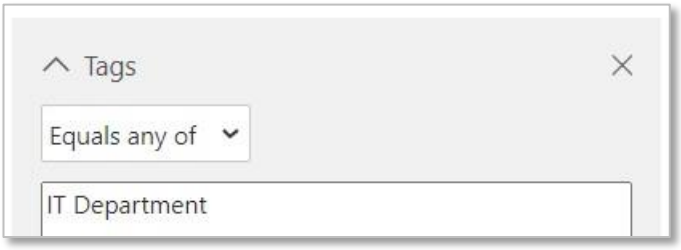


Abbildung 6-34: Als Filter verwendete Tags.

Ergebnisse untersuchen

Wie bereits erwähnt, werden bei der Arbeit mit dem Threat Explorer die Rohdaten, die zur Darstellung der Diagramme verwendet werden, direkt unter dem jeweiligen Diagramm angezeigt. Diese Daten sind kontextbezogen – das heißt, die Art der angezeigten Informationen und deren Eigenschaften unterscheiden sich je nach Diagrammtyp. Die Kampagnenansicht zeigt Informationen, die für die jeweilige Kampagne relevant sind, während die Phishing-Ansicht wesentlich mehr Details zu einzelnen Nachrichten anzeigt.

Die Rohdaten sind interaktiv. Du kannst auf ein Element klicken, um weitere Informationen dazu zu erhalten. Wenn du beispielsweise auf eine E-Mail klickst, erscheint eine Auswahlleiste mit zusätzlichen Details zur Nachricht, zu Anhängen, Geräten, dem Zeitstrahl der E-Mail und zu ähnlichen E-Mails.

Einige Registerkarten ermöglichen dir einen noch tieferen Einblick. Wenn du dir beispielsweise die Details einer Kampagne anzeigen lässt, siehst du am unteren Bildschirmrand eine Aktion. Wenn du darauf klickst, wird das Threat Explorer-Dashboard erneut geöffnet – diesmal mit einem vordefinierten Filter, der auf den Eigenschaften des Elements basiert. Im Fall einer Kampagne wird dir das Diagramm dann gefiltert nach der Kampagnen-ID angezeigt, die der ID der ausgewählten Kampagne entspricht:

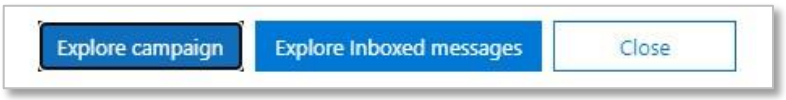


Abbildung 6-35: Kontextbezogene Aktionen in den Details eines Elements

Behebung

Der Threat Explorer ist nicht nur ein Untersuchungstool. Du kannst ihn auch nutzen, um auf bestimmte Vorfälle zu reagieren. Nimm zum Beispiel eine Phishing-Kampagne: Wenn du die verschiedenen für deinen Mandanten relevanten Kampagnen überprüfst, kannst du – wie bereits erwähnt – zugestellte Nachrichten analysieren. Dabei erhältst du einen Überblick über alle Nachrichten, die Teil dieser Kampagne waren und in die Postfächer der Benutzer zugestellt wurden, anstatt in Quarantäne oder Junk zu landen.

Neben den Daten zu den Nachrichten siehst du eine Schaltfläche „Aktionen“, über die du eine von mehreren Aktionen auf die ausgewählten Nachrichten anwenden kannst. Dazu gehören das Verschieben in den Junk-E-Mail-Ordner, das vorläufige oder endgültige Löschen, das Starten einer zusätzlichen Untersuchung und mehr. Das ist besonders hilfreich, wenn du während eines Vorfalls bestimmte Nachrichten schnell und gezielt aus Benutzerpostfächern entfernen möchtest.

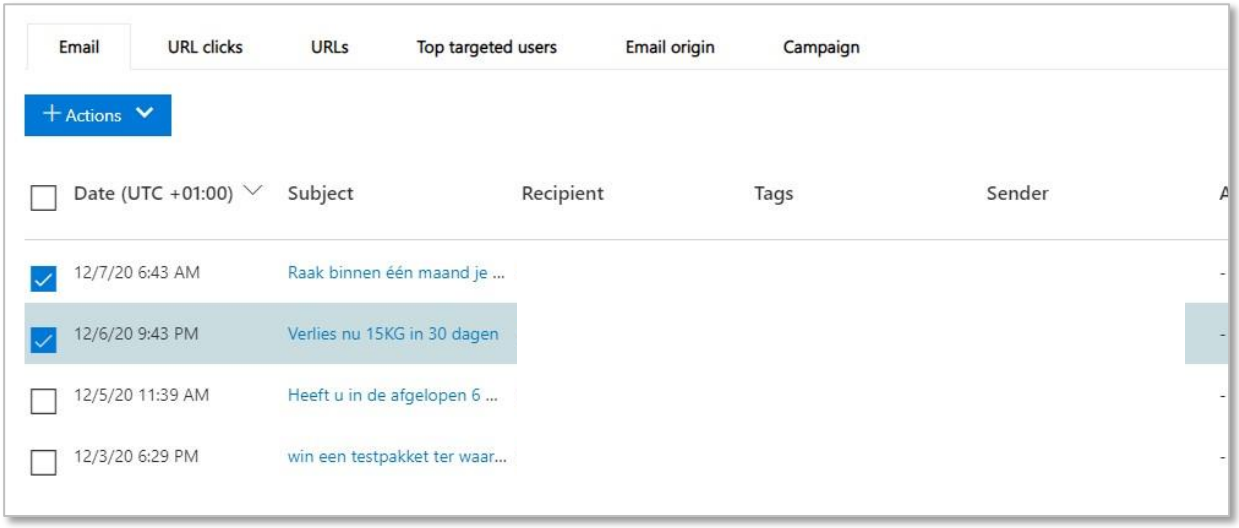


Abbildung 6-36: Durchführen von Aktionen für Nachrichten über den Threat Explorer.

Filter für alle E-Mails

Wenn du einen umfassenderen Überblick über E-Mails erhalten möchtest, die zugestellt, als Junk markiert, blockiert oder unter Quarantäne gestellt wurden, kannst du den Filter „**Alle E-Mails**“ verwenden. Dieser ist inzwischen die Standardansicht im Explorer. Um ihn optimal zu nutzen, solltest du den Datumsbereich anpassen (nicht den voreingestellten verwenden) und zusätzlich den Filter „Directionalität“ auf „Inbound“ setzen.

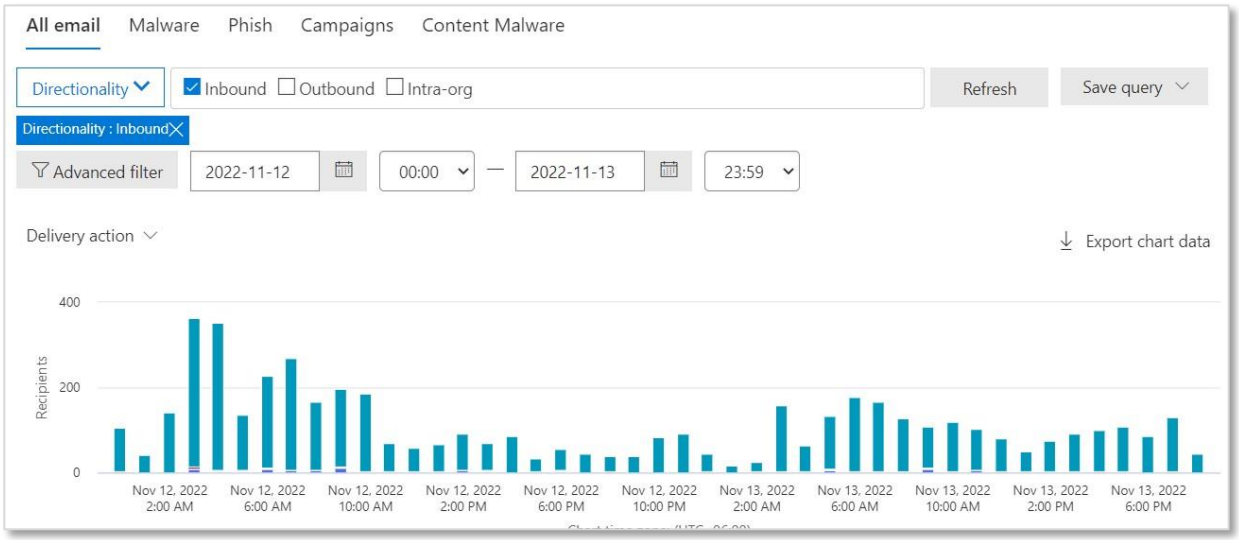


Abbildung 6-37: Arbeiten mit der Ansicht "Alle E-Mails" unter Verwendung des Werts "Inbound" für die Direktionalität (ganz rechts).

Wie du sehen kannst, ermöglicht dir die Ansicht, die vier Kategorien von E-Mails und ihre jeweiligen Anteile im Vergleich zueinander zu sehen. Das ist auch eine ziemlich aussagekräftige Möglichkeit, um zu erkennen, wie viele Nachrichten verarbeitet wurden.

Was jedoch interessanter sein könnte, ist das, was du siehst, wenn du die Direktionalität auf „Outbound“ umstellst.

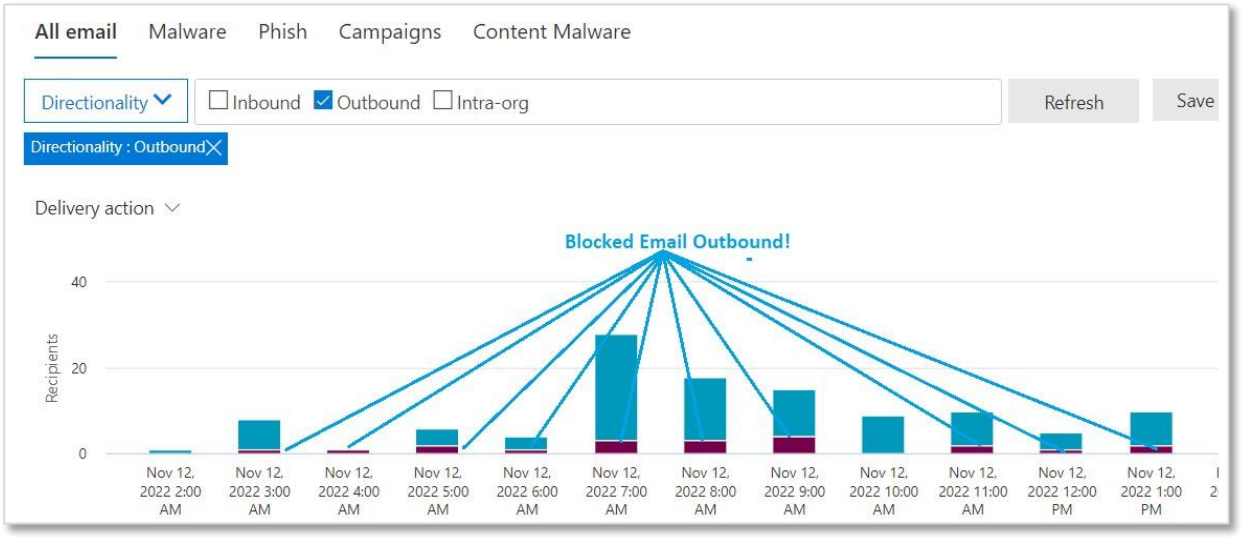


Abbildung 6-38: Betrachten ausgehender Nachrichten.

Aus dieser Ansicht erkennst du, dass mehrere (ausgehende) Nachrichten blockiert wurden. Wie du dir vorstellen kannst, ist das definitiv etwas, das untersucht werden sollte, da blockierte ausgehende Nachrichten auf eine Kompromittierung eines deiner Konten hindeuten könnten. Es könnte aber auch bedeuten, dass jemand in deiner Organisation versucht hat, Nachrichten zu senden, die als bösartig oder als Spam eingestuft wurden. In diesem Fall ist es immer noch ein Problem, aber wahrscheinlich weniger kritisch als eine Kompromittierung.

Integration von Microsoft Defender für Endpunkt

Wie in Kapitel 7 ausführlich erörtert, ist Microsoft Defender für Endpunkt Microsofts Lösung für Endpunkterkennung und -reaktion sowie Antimalware. Die einzigartigen Erkenntnisse, die es über die Endpunkte in deiner Umgebung hat, können für Office 365 und umgekehrt äußerst nützlich sein. Durch die Aktivierung der Integration zwischen beiden können Geräteinformationen in Warnungen einbezogen und angezeigt werden, was deinem Sicherheitsbetriebsteam helfen kann, den Umfang und die Auswirkungen bestimmter Phishing-Vorfälle besser zu verstehen.

Um die Integration zu aktivieren, öffnest du den Threat Explorer und klickst in der oberen rechten Ecke des Bildschirms auf „**MDE-Einstellungen**“:

Abbildung 6-39: Verbindung von Microsoft Defender für Endpunkt mit Threat Explorer.

Um die Integration vollständig und bilateral zu machen, navigierst du auch zu den Microsoft-Defender-für-Endpunkt-Einstellungen und aktivierst die Funktion „Bedrohungsintelligenz“ in den erweiterten Funktionen.

Erstellen einer gespeicherten/verfolgten Abfrage

Verfolgte Abfragen, wie bereits erörtert, basieren auf dem Explorer unter Threat Management. Sobald du dich in der Explorer-Oberfläche befindest, musst du eine Ansicht auswählen und dann die Optionen auswählen, die zu dieser Ansicht passen.

Abbildung 6-40: Verfügbare Ansichten in verfolgten Abfragen.

Wenn du beispielsweise „Phish“ auswählst, musst du dich für den Filter, die Zustellungsaktion und den Datenbereich entscheiden, wie in Abbildung 6-42 dargestellt:

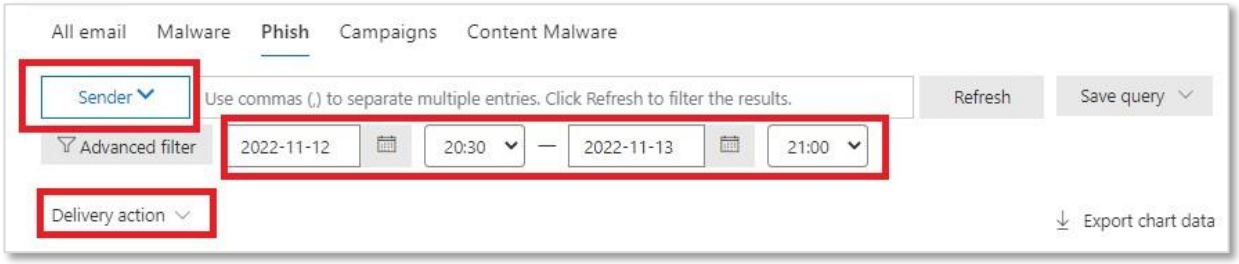


Abbildung 6-41: Filtern nach Phishing-Angriffen.

Sobald alle Optionen festgelegt sind, klickst du auf „Aktualisieren“, um sicherzustellen, dass die Daten korrekt sind. Wenn die Abfrage dann deinen Vorstellungen entspricht, kannst du sie speichern.

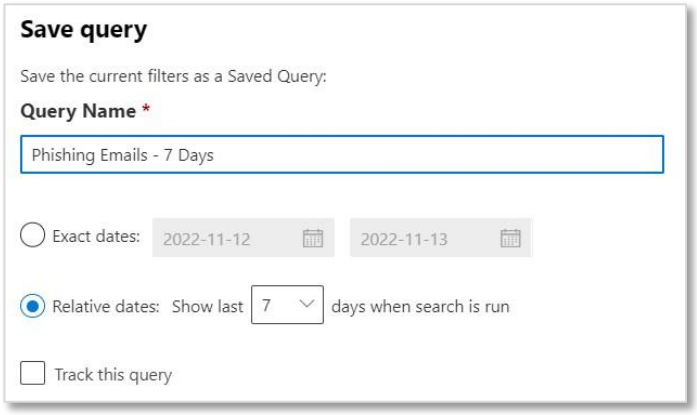


Abbildung 6-42: Speichern einer Abfrage (beachte das Kontrollkästchen "Diese Abfrage verfolgen").

Hinweis: Microsoft hat auch die Anzahl der Datensätze geändert, die sowohl im Security Center als auch im Explorer exportiert werden können - auf 200.000 Datensätze, gegenüber den 9.900 Datensätzen, die zuvor erlaubt waren.

Automatisierte Untersuchung und Reaktion (AIR)

Automated Investigation and Response (AIR) ist eine Funktion, die Teil von Microsoft Defender für Office 365 Plan 2 ist. Der Zweck von AIR ist es, Automatisierung bei der Analyse von Warnungen in deinem Mandanten zu bieten, um die Arbeit deines zweifellos ausgelasteten Sicherheitsteams zu entlasten. Sobald eine Analyse abgeschlossen ist, werden – falls zutreffend – Korrekturmaßnahmen empfohlen. Die Empfehlungen werden jedoch nicht automatisch ausgeführt. Es liegt immer noch an einem Responder oder Analysten, über die Empfehlung zu entscheiden.

AIR ist standardmäßig aktiviert und erfordert keine Konfiguration. Noch mehr: Es kann nicht deaktiviert werden. Um mit AIR-Untersuchungen zu interagieren, benötigst du eine der folgenden Rollen: globaler Administrator, Sicherheitsadministrator, Sicherheitsleseberechtigter und das Recht „Suchen und Löschen“. Beachte, dass für die Rolle „Suchen und Löschen“ möglicherweise eine neue Rollengruppe erstellt werden muss.

AIR wird automatisch bei Warnungen ausgelöst, die im Microsoft 365 Defender-Portal erstellt werden. Beispiele für solche Warnungen sind:

- Erkennung eines Klicks auf eine bösartige URL
- Phishing-E-Mail gemeldet
- Malware in E-Mail nach Zustellung erkannt (ZAP)
- Phishing-URLs nach Zustellung entfernt (ZAP)
- Muster erkannt – verdächtige E-Mails
- Eingeschränkte Benutzer - am Senden von E-Mails gehindert
- Übermittlungen - durch Benutzer und Administratoren

Untersuchen von Warnungen

Bitte beachte, dass der Übergang vom Security & Compliance Center zum Microsoft 365 Defender-Portal noch im Gange ist. Daher können sich diese Erfahrungen bald ändern. Im Folgenden werden die Änderungen so dargestellt, wie sie stattgefunden haben.

Wenn eine automatisierte Untersuchung gestartet wird, erscheint sie im Microsoft 365 Defender-Portal unter **E-Mail & Zusammenarbeit** > **Untersuchungen**, wie in Abbildung 6-43 dargestellt:

Abbildung 6-43: Beispiel für eine automatisierte Untersuchung.

Wenn du auf das Symbol klickst ( ), um die Untersuchung zu öffnen, kannst du eines der angezeigten Elemente auswählen, um zu sehen, woraus eine Untersuchung besteht. Die Seite enthält mehrere Registerkarten, darunter:

- **Untersuchungsgraph**: Eine grafische Darstellung des Angriffs, die die Beziehung zwischen den beteiligten Entitäten, gesammelten Beweisen und empfohlenen Aktionen zeigt.
- **Warnungen**: Ein Überblick über die Warnungen, die zur automatisierten Untersuchung beigetragen (sie ausgelöst) haben.
- **E-Mail**: Weitere Details zu der/den untersuchten Nachricht(en) sowie zur Anzahl der zugestellten Nachrichten und zum Urteil über diese Nachrichten.
- **Benutzer**: Welche Benutzer von der/den untersuchten Nachricht(en) betroffen waren.
- **Computer**: Welche Computer von der/den untersuchten Nachricht(en) betroffen waren.
- **Entitäten**: Alle Entitäten, die an der Untersuchung beteiligt sind. Dazu gehören Benutzer, Nachrichten, Dateien (Anhänge) usw.
- **Protokoll**: Ein chronologischer Überblick über die von AIR durchgeführten Aktivitäten. Dies ist nützlich, um zu verstehen, welche Elemente AIR untersucht hat, um sein Urteil und die empfohlenen Aktionen besser zu verstehen.
- **Aktionen**: Dies sind die von AIR empfohlenen Aktionen. Eine häufig vorgeschlagene Aktion ist das vorläufige Löschen der relevanten Nachricht(en) aus den Postfächern (Entitäten) in der Untersuchung.

Um auf empfohlene Aktionen zu reagieren, genügt es, auf die vorgeschlagene Aktion zu klicken und dann entweder „**Genehmigen**“ oder „**Ablehnen**“ auszuwählen. Wenn du auf den Betreff einer Nachricht klickst, erscheint eine Auswahlleiste mit weiteren Details zur betroffenen Nachricht. So kannst du besser beurteilen, ob du die Nachricht entfernen oder ob eine weitere Nachverfolgung mit dem betroffenen Benutzer erforderlich ist.

Hinweis: Beachte, dass diese Aktionen nicht automatisiert werden können und dass Administratoren regelmäßig prüfen sollten, ob Nachverfolgungen oder Maßnahmen notwendig sind.

Manuelles Auslösen von AIR

Wie bereits festgestellt, wird AIR zwar automatisch ausgelöst, du kannst jedoch auch manuell eine Untersuchung starten, während du eigene Analysen durchführst. Im folgenden Beispiel wird eine AIR direkt über das Threat-Explorer-Dashboard ausgelöst. Um das Menü zu öffnen, wähle eine Nachricht in der entsprechenden Ansicht aus und klicke dann auf **Nachrichtenaktionen** > **Untersuchung auslösen**.

Priorität Kontoschutz

Wenn es darum geht, ein Unternehmen oder eine Organisation anzugreifen, suchen böswillige Akteure nach jedem Winkel, um eine Schwachstelle in der Verteidigung zu finden. Egal ob per E-Mail, Telefon, Text oder über andere Wege – ein schwaches Ziel zu finden, ist von höchster Bedeutung. Bei gezielten Angriffen ist das Ziel umso wertvoller, je größer der potenzielle

Schaden oder Gewinn ist. Es ist daher nicht verwunderlich, dass Führungskräfte auf C-Level häufiger ins Visier genommen werden.

Priority Account Protection soll Sicherheitsteams dabei unterstützen, schneller zu erkennen, wenn eine Warnung ein potenziell hochwertiges Ziel betrifft. Dabei wird ein visueller Hinweis (ein sogenanntes Tag) zur Warnung hinzugefügt, wann immer ein markierter Benutzer betroffen ist.

Priority Account Protection ist eine interessante Funktion von Microsoft, die Organisationen helfen kann, besonders sensible Konten zu schützen. Laut Microsoft-Dokumentation ist die volle Nutzung dieser Funktion, inklusive Premium-Mailflow-Überwachung, auf Kunden mit Office 365 E3, Microsoft 365 E3 oder Microsoft E5 sowie mindestens 10.000 Lizenzen und 50 Exchange Online-Postfächern beschränkt. Du kannst aber trotzdem Benutzertags verwenden, um Gruppen von Benutzern in Office 365 in Berichten zu filtern oder zu gruppieren – denn es gibt eine aufgelistete Spalte und einen verfügbaren Filter für Tags. Wenn du über die entsprechende Lizenzen (10k+) verfügst, solltest du die Funktion aktivieren und nutzen.

Um einem Benutzer ein Tag hinzuzufügen, navigierst du zu https://security.microsoft.com/userTags . Beim Erstellen eines neuen Tags kannst du direkt Postfächer zuweisen. Alternativ kannst du auf „Tag bearbeiten“ klicken, um bestehende Tags Benutzern zuzuweisen. Nach der Zuweisung eines Tags erscheint dieses auch in der Benutzeroberfläche:

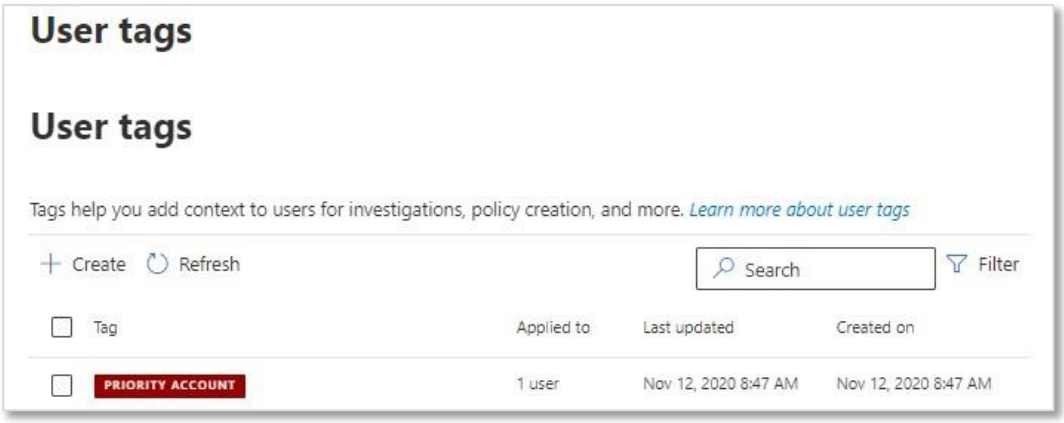


Abbildung 6-44: Zuweisen von Tags zu Benutzern

Sobald ein Benutzer ein Tag erhalten hat, enthalten alle für diesen Benutzer generierten Warnungen einen visuellen Hinweis mit dem jeweiligen Tagwert. So kann dein Sicherheitsteam sofort erkennen, mit welcher Art von Benutzer es zu tun hat. Du könntest zum Beispiel Tags für besonders gefährdete Benutzer oder für Mitarbeiter bestimmter Abteilungen einführen.

Diese Tags lassen sich auch zur Filterung von Berichten nutzen. So bekommst du einen besseren Überblick darüber, wie oft markierte Konten angegriffen werden. Obwohl das hilfreich ist, sorgt

die Uneinheitlichkeit in den verschiedenen Berichten gelegentlich für Verwirrung – es ist nicht immer ersichtlich, welche Berichte eine Tag-Filterung standardmäßig unterstützen und welche nicht. Da sich die Funktion derzeit noch in der Vorschau befindet, ist jedoch mit weiteren Verbesserungen bis zur allgemeinen Verfügbarkeit zu rechnen.

E-Mail-Entitätsseite

Innerhalb des Security Admin Centers bietet Microsoft nun eine neue Oberfläche für **Untersuchungen** in Defender für Office 365. Du findest die Seite unter **E-Mail & Zusammenarbeit** > **Untersuchungen**. Zunächst siehst du eine Liste der Untersuchungen für den gewählten Zeitraum. Bei Bedarf kannst du den Zeitbereich ändern, indem du den Filter aktualisierst. Um weitere Informationen zu einer bestimmten Untersuchung zu erhalten, klickst du auf das Fenster mit dem Pfeil neben der ID der jeweiligen Untersuchung. Dadurch wird die Detailseite der Untersuchung geöffnet. Eine Sache, die dir auffallen wird, ist, dass das Aussehen und die Bedienung der Seite denen der Detailansicht einer Untersuchung in Microsoft Defender für Endpunkt ähneln. Das ist beabsichtigt, um eine konsistente Nutzererfahrung über die verschiedenen Produkte hinweg sicherzustellen.

Lass uns zunächst die neue Registerkarte "Entitäten" in den Details einer Untersuchung erkunden, die du nun durch Klicken auf das Symbol ( ) finden kannst.

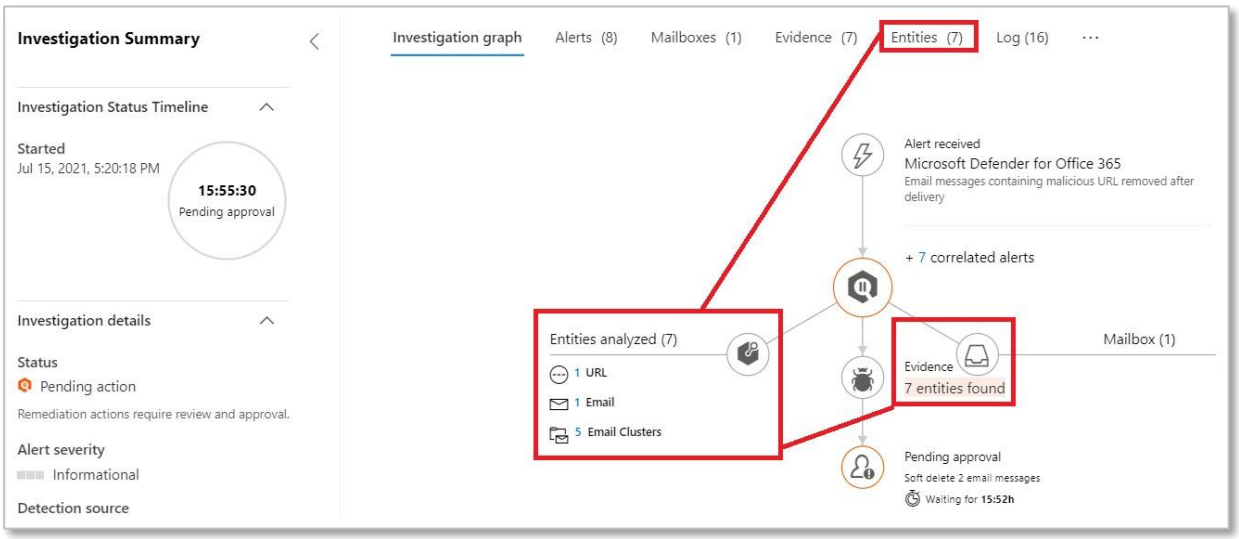


Abbildung 6-45: Jetzt in Untersuchungen verfügbare Entitäten.

Wenn du dir die Registerkarte “Entitäten” ansiehst, erkennst du die Referenzartefakte, aus denen die Entitäten bestehen, die Defender für diese Nachricht analysiert hat. Du siehst hier eine komprimierte Ansicht beider Registerkarten:

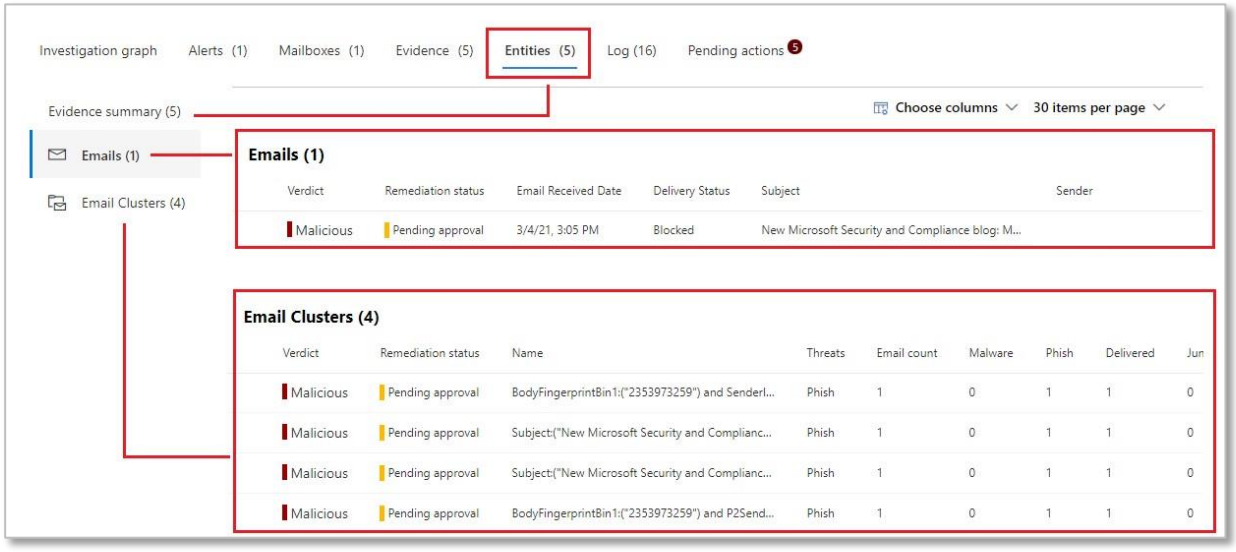


Figure 6-46: Ansicht der Entitäten der Untersuchung.

Was bedeuten die einzelnen Entitäten?

- **E-Mail**: Die ursprüngliche E-Mail, die untersucht wird.
- **E-Mail-Cluster**: E-Mail-Nachrichten, die durch eine Suche als ähnlich zur ursprünglichen E-Mail eingestuft wurden. Wie du sehen wirst, taucht dieselbe Nachricht oft in verschiedenen Formen auf.

Jede dieser Entitäten kannst du durch Klicken auf das jeweilige Element weiter untersuchen, um zusätzliche Informationen zu erhalten.

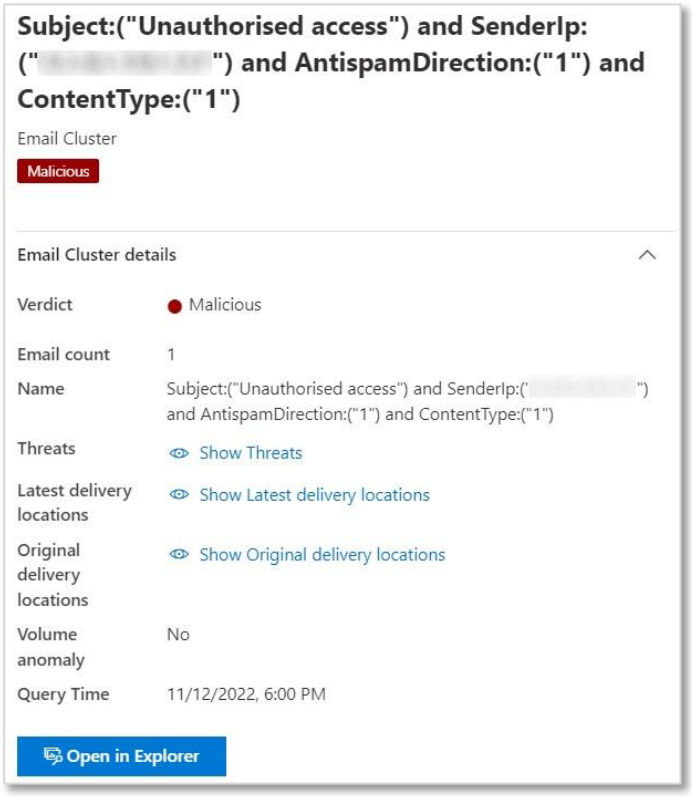


Abbildung 6-47: Rote Rechtecke markieren verfügbare Aktionen für diese Entität.

Von dieser neuen Auswahlleiste aus kannst du die Entität in der Explorer-Funktion des Security Centers anzeigen sowie das vorläufige Löschen der E-Mail(s) entweder ablehnen oder genehmigen. Du hast außerdem die Möglichkeit, mit den in dieser E-Mail bereitgestellten Details eine Jagd durchzuführen.

Wenn du dich für eine Jagd entscheidest, wird automatisch eine Abfrage in der Advanced-Hunting-Funktion erstellt, die in Kapitel 12 ausführlicher behandelt wird. In diesem speziellen Beispiel ist die Abfrage so eingestellt, dass sie in den letzten sieben Tagen nach derselben Nachricht sucht. Das kann nützlich sein, um herauszufinden, ob jemand versucht hat, die Nachricht an mehrere Empfänger zu senden. Beachte dabei, dass die vorgefüllte Abfrage den zuvor von dir eingestellten Zeitbereich nicht berücksichtigt. Wenn du beispielsweise zuvor den Zeitraum auf die letzten dreißig Tage angepasst hast, berücksichtigt die vorgefertigte Abfrage dennoch nur sieben Tage. Achte also auf den Zeitraum in deiner Abfrage, wenn du keine Ergebnisse erhältst.

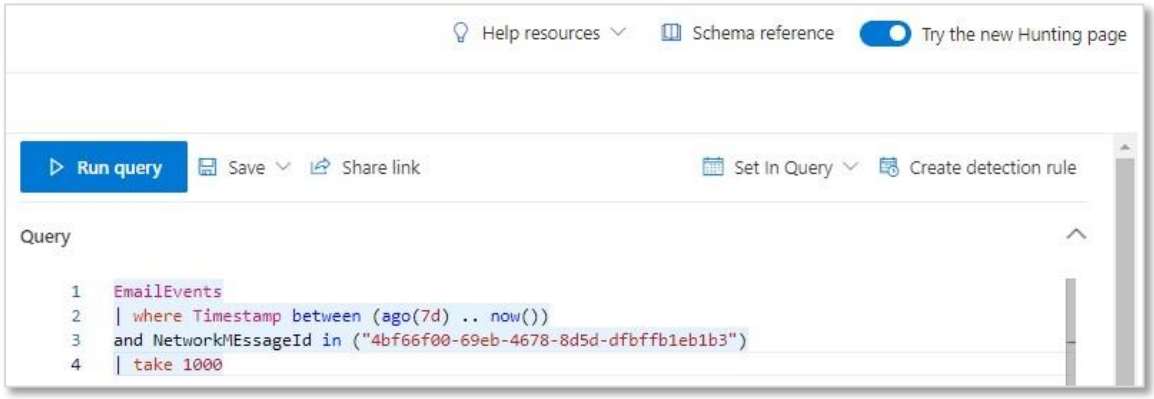


Abbildung 6-48: Abfrage für die Entität aus der Untersuchung.

Wenn wir zu den verfügbaren Aktionen zurückkehren und ein vorläufiges Löschen genehmigt wird, erscheint nach Abschluss der Aktion eine entsprechende Meldung:

Abbildung 6-49: Übermittlung der Genehmigung zum vorläufigen Löschen.

Wenn du in der Auswahlleiste auf „Weitere Details zur E-Mail…“ klickst, wird die Untersuchung auf die E-Mail-Entitätsseite übertragen.:

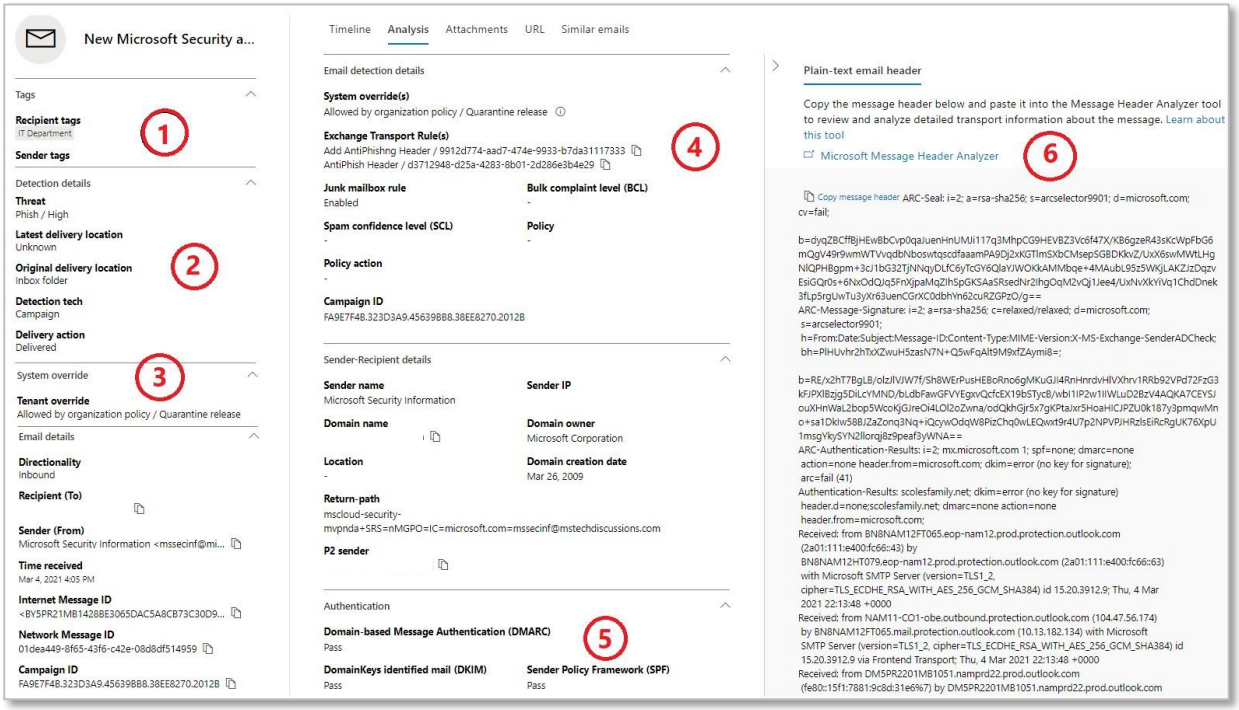


Abbildung 6-50: Die Registerkarte "Analyse" bietet eine Fülle von Informationen über die E-Mail.

(1) Alle Tags, die bei der Verarbeitung auf die Nachricht angewendet wurden. Im obigen Beispiel wurde ein Benutzertag gesetzt, da die E-Mail-Empfänger Teil der IT-Abteilung sind.

(2) Was in der Nachricht erkannt wurde, wohin die Nachricht gweitergeleitet wird, welche Bedrohungserkennungsfunktion verwendet wurden ob die E-Mail zugestellt wurde oder nicht.

(3) Alle Außerkraftsetzungen, die in deinem definiert sind und dazu führen könnten, dass die Nachricht bestimmte Scan-Engines überspringt. Diese werden hier klar aufgeführt.

(4) Backend-Prozesse werden hier vermerkt -- Systemüberschreibungen, Transportregeln, Junk-Mail-Richtlinien, SCL- und BCL-Verarbeitung inklusive der getroffenen Richtlinienmaßnahmen.

(5) Informationen zur E-Mail-Authentifizierung über den Absender -- DMARC, DKIM, SPF und weitere Authentifizierungsindikatoren.

(6) Vollständiger Nachrichtenkopf der E-Mails ist ebenfalls einsehbar. Du kannst ihn zur tiefergehenden Analyse im Message Header Analyzer öffnen.

Wie bei den Entitätsseiten für Benutzer, IP-Adressen und andere Daten findest du auch hier zahlreiche Registerkarten mit ergänzenden Informationen:

- **Zeitachse**: Bietet dir einen chronologischen Überblick über den Weg der Nachricht vom Empfang bis zur Zustellung. Vergleichbar mit der Nachrichtenverfolgung, allerdings mit Fokus auf Sicherheitsaspekte wie Filterung usw.
- **Analyse**: Liefert dir ein strukturierteres, tieferes Verständnis zur Nachricht, den Kopfzeilen und den Ergebnissen der Authentifizierung.
- **URLs und Anhänge**: Hier bekommst du einen Überblick über die potenziell bösartige Anhänge und URLs in der Nachricht - falls solche gefunden wurden. Du kannst auf jedes Elemente klicken, um weitere Details zu erhalten. Bei URLs erfährst du zum Beispiel, ob und wie die Seite geprüft wurde und ob bösartige Inhalte identifiziert wurden – vorausgesetzt, die Seite wurde überhaupt gescannt.
- **Ähnliche E-Mails**: Auflistung von Nachrichten, die der analysierten ähnlich sind. Das können E-Mails mit identischem Betreff, Gleicher Abesender-IP oder Kombinationen daraus sein.

Bei der Untersuchung von Vorfällen ist die Menge an Informationen oft eine Herausforderung. Gleichzeitig kann ein Mangel an Details ein echtes Hindernis für eine gründliche Analyse darstellen. Die E-Mail-Entitätsseite scheint hier einen guten Mittelweg zu bieten: Sie stellt viele der für die Untersuchung wichtigen Informationen an einer zentralen Stelle bereit, ohne zu überfordern. Wenn du Ursprung, Kopfzeilen oder andere Daten zu einer E-Mail nachvollziehen musst, liefert dir diese Seite strukturierte Einblicke. Sie zeigt dir auch auf, worauf Microsofts Scan-Engines achten – was dir wiederum helfen kann, deine Analyseprozesse zu optimieren. Du kannst dir E-Mails in der Vorschau anzeigen lassen und sie bei Bedarf herunterladen, um sie weiter zu untersuchen.

Attack Simulation Training (AST)

Einführung

Der Attack Simulator ist Teil von Microsoft Defender für Office 365 Plan 2. Das Ziel des Tools ist es, simulierte Angriffe auf deine eigene Umgebung durchzuführen, um das Sicherheitsbewusstsein deiner Benutzer zu prüfen und messbar zu machen. Um ihn nutzen zu können sind hier ein paar Hinweise:

- Du musst der Rolle "Organisationsverwaltung" oder "Sicherheitsadministrator" zugewiesen sein.
- Die simulierten Angriffe sammeln über 30 Tage hinweg Daten, die anschließend für insgesamt 90 Tage gespeichert bleiben.

- Für den "Attack Simulator" gibt es keine PowerShell-Cmdlets.

Ausführen eines simulierten Angriffs

Wenn die Voraussetzungen erfüllt sind, kannst du die verschiedenen Angriffsszenarien untersuchen und analysieren, welche Relevanz sie für deine Umgebung haben. Warum solltest du dieses Tool nutzen? Ganz einfach: Wenn du über die entsprechende Lizenz verfügst, gibt es keinen Grund, es nicht zu tun. Ohne dieses integrierte Tool müsstest du auf kostenpflichtige Angebote anderer Anbieter wie KnowBe4 zurückgreifen, die ähnliche Funktionen bereitstellen. Ein weiterer Vorteil ist, dass die integrierten Angriffsszenarien nicht von bestehenden Richtlinien wie Anti-Phish, AIR oder anderen Schutzmaßnahmen blockiert werden – ein klarer Pluspunkt im Vergleich zu externen Lösungen.

Der neue Attack Simulator ist eine deutliche Verbesserung gegenüber der bisherigen Version, die weiterhin im Microsoft 365 Defender-Portal verfügbar ist. Er bietet dir ein wesentlich moderneres Erlebnis in Bezug auf Angriffssimulationen, Anpassungsmöglichkeiten, Berichtsfunktionen und integriertes Benutzerschulungssystem – insbesondere dann, wenn ein Benutzer bei einem simulierten Angriff durchfällt.

Lass uns ein Beispiel durchgehen, bei dem wir ein Social-Engineering-Szenario für unsere Endbenutzer erstellen. Um den Attack Simulator zu öffnen, gehst du in das Microsoft 365 Defender-Portal und klickst auf „**Attack Simulator**“. Anschließend wählst du „**Simulation starten**“ aus – damit öffnet sich der Assistent für die Konfiguration deines Angriffszenarios.

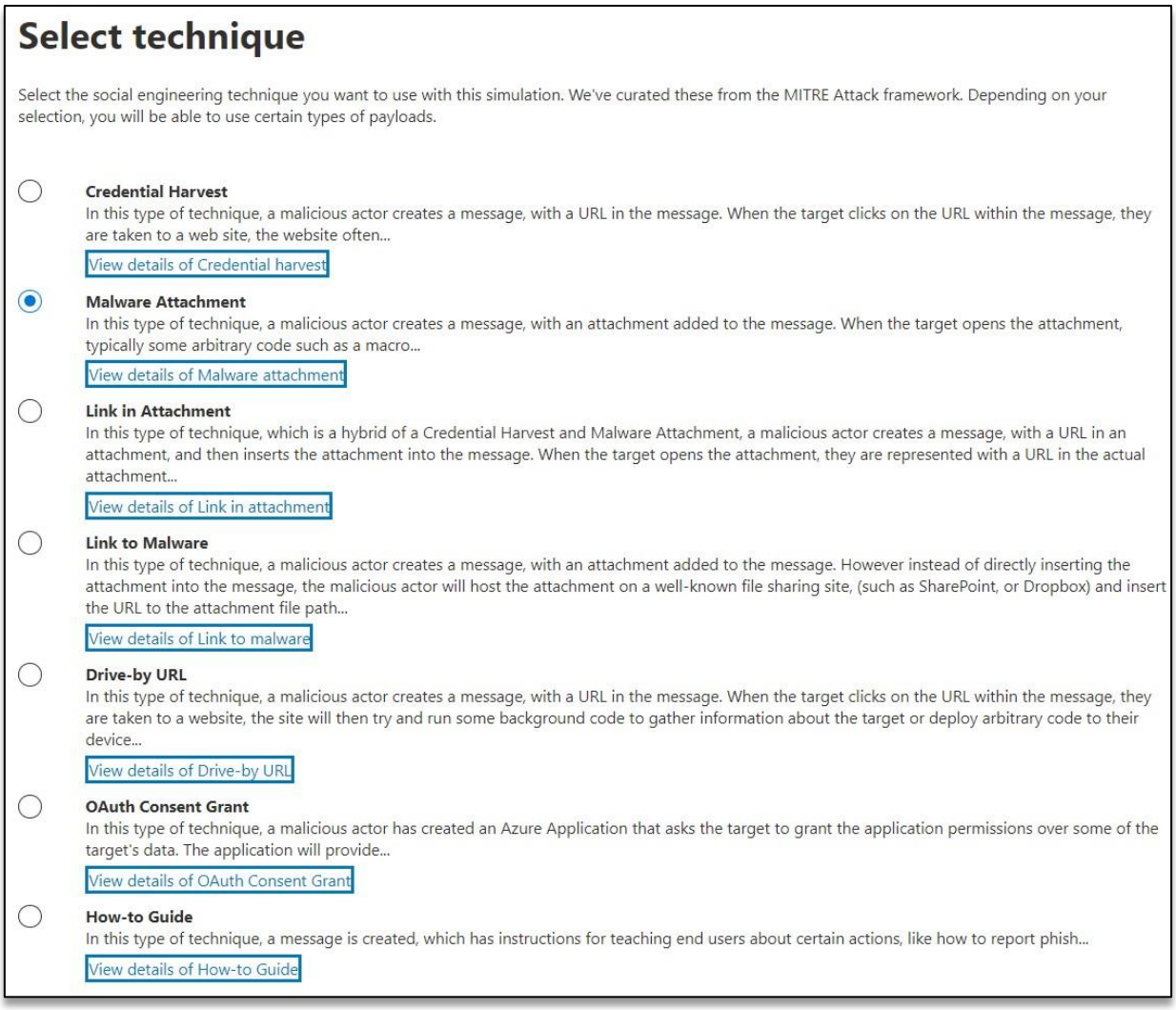


Abbildung 6-51: Starten eines simulierten Angriffs mit dem Attack Simulator

Um zu erklären, wie der Attack Simulator funktioniert, erstellen wir eine Beispielsimulation mit einem der häufigsten Angriffe: Credential Harvesting. Dabei versucht der Angreifer, deine Anmeldeinformationen abzugreifen, indem er dich dazu verleitet, sie auf einer gefälschten Website oder in einem Formular preiszugeben. Auf dem ersten Erstellungsbildschirm kannst du aus fünf Haupttypen von Szenarien wählen: Credential Harvest (unser Szenario), Malware-Anhang, Link im Anhang, Link zu Malware und Drive-by-URL.

Jedes dieser Szenarien wird im Assistenten verständlich beschrieben. Zusätzlich bietet der Link „Details anzeigen“ für jedes Szenario weiteres Hintergrundwissen. Wenn du darauf klickst, erscheint eine Auswahlleiste auf der rechten Seite mit zusätzlichen Informationen.

Microsoft hat außerdem einen neuen Nutzlasttyp namens „Oauth Consent Grant“ hinzugefügt. Was ist das und warum ist es wichtig? Diese Simulation imitiert eine Berechtigungsanfrage, wie sie typischerweise von Azure-Anwendungen gestellt wird, die auf Daten zugreifen möchten. Der

Benutzer muss dabei den Zugriff aktiv gewähren. Die Simulation bildet also realitätsnah ab, was ein Endbenutzer sehen würde, wenn er einer neuen App Zugriffsrechte im Mandanten erteilen soll.

Nachdem du dein Szenario ausgewählt hast, klickst du auf „Weiter“ und gibst eine Bezeichnung und Beschreibung für die Simulation an:

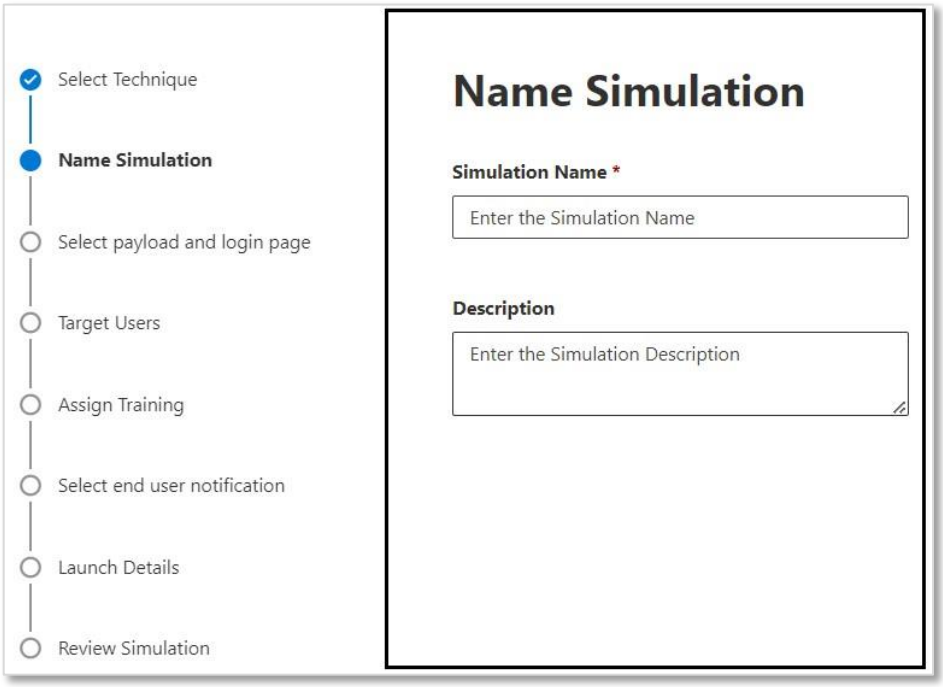


Abbildung 6-52: Eingeben grundlegender Details zur Simulation.

Anschließend wählst du eine passende Nutzlast für das Szenario aus. Die Nutzlast bestimmt, wie die Nachricht aussieht, die deine Benutzer erhalten, um ihre Widerstandsfähigkeit gegen den jeweiligen Angriffstyp zu testen. Microsoft erweitert die Auswahl an Payloads laufend, sodass in Zukunft noch mehr Varianten zur Verfügung stehen werden:

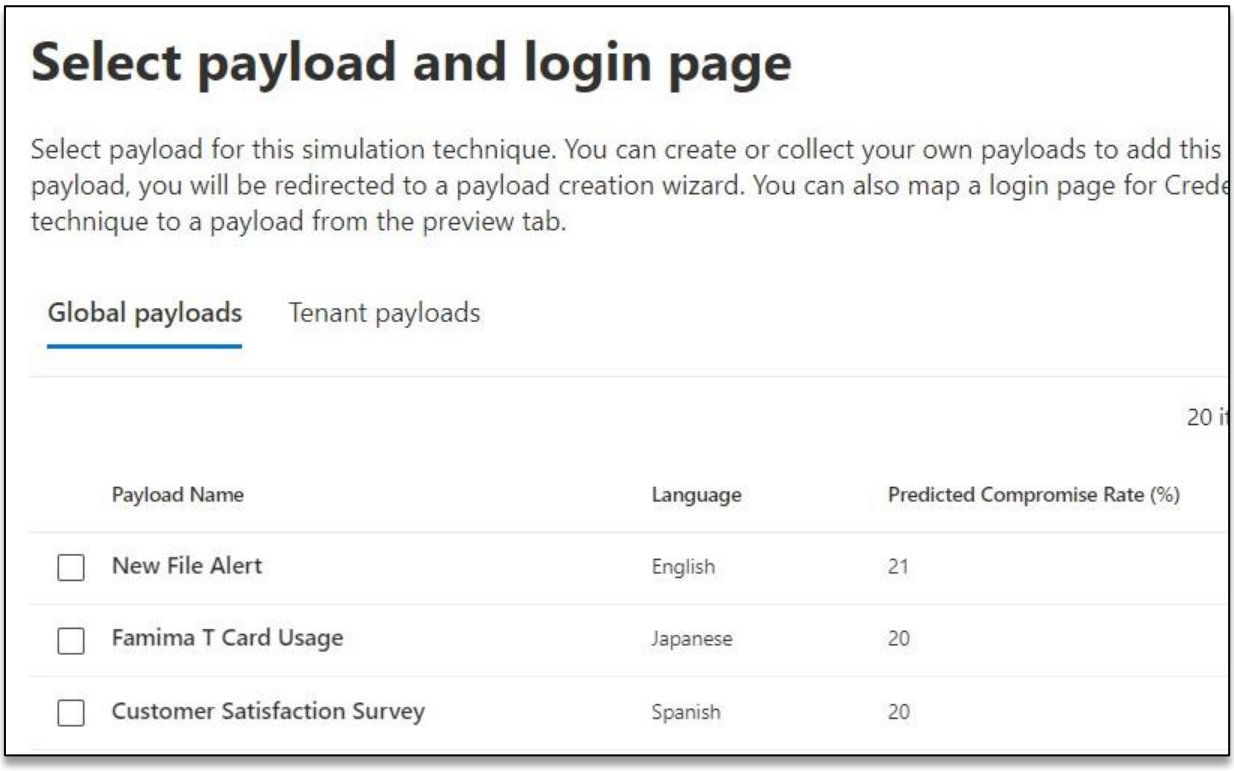


Abbildung 6-53: Auswählen einer relevanten Nutzlast.

Wenn du die Liste der verfügbaren Payloads durchgehst, kannst du aus zahlreichen Szenarien wählen. Dabei stehen globale und mandantenspezifische Optionen zur Auswahl. Die globalen Payloads basieren auf realen Angriffsszenarien. Für unser Beispiel verwenden wir die Payload „Postfach voll“. Zu jeder Payload siehst du folgende Zusatzinformationen:

- **Klickrate:** Wie viele Benutzer auf den Angriff geklickt haben und dadurch kompromittiert wurden.
- **Prognostizierte Kompromittierung:** Microsofts geschätzte an gefährdeten Benutzern bei diesem Szenario.
- **Simulationen:** Wie viele Simulationen eine Organisation für dieses Szenario durchgeführt hat.

Zusätzlich kannst du die Anmeldeseite für das Szenario anpassen. Entweder nutzt du eine von Microsoft bereitgestellte Standardseite oder gestaltest deine eigene. Wenn du eine Payload ausgewählt hast, hast du die Möglichkeit, eine Testnachricht an dich selbst zu schicken, um zu prüfen, wie sie aussieht und ob sie zum Szenario passt:

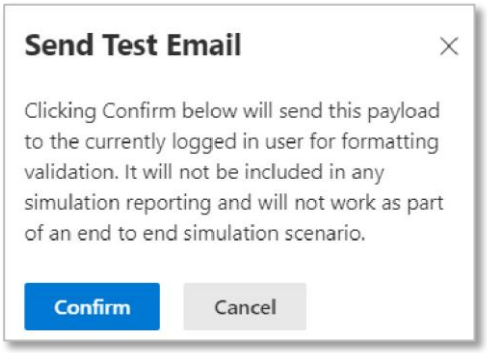


Abbildung 6-54: Senden einer Test-Simulations-E-Mail an dein angemeldetes Konto.

Im nächsten Schritt wählst du die Benutzer aus, die an der Simulation teilnehmen sollen:

Abbildung 6-55: Auswahl der Zielbenutzer für die Simulation.

Du kannst die gesamte Organisation einbeziehen oder gezielt bestimmte Benutzergruppen auswählen. Falls nötig, lassen sich auch Ausnahmen definieren. Danach legst du die Einstellungen für das Benutzertraining fest.

Die empfohlene Einstellung ist, die Standardwerte beizubehalten und Microsoft das Training durchführen zu lassen.

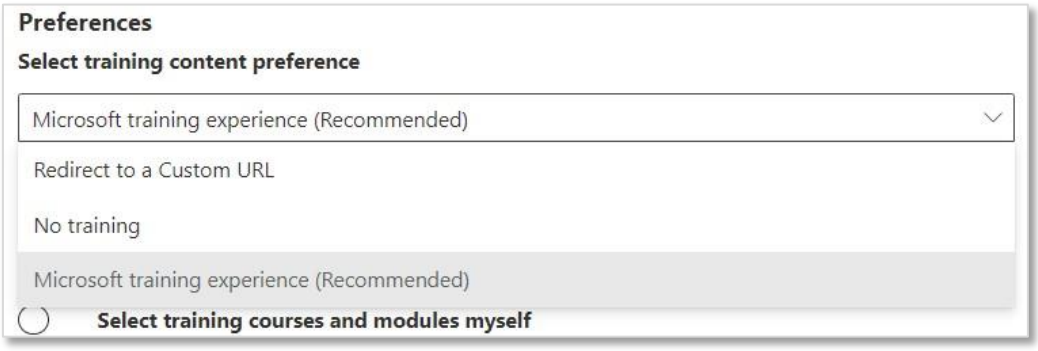


Abbildung 6-56: Auswahl der Trainingsinhalte.

Training. Das enthaltene Training wird von einem Unternehmen namens Terranova Security bereitgestellt, das mit Microsoft zusammenarbeitet, um Benutzern zu helfen, aus ihren Fehlern im Umgang mit verschiedenen Phishing- und anderen bösartigen Angriffen auf ihre Organisation zu lernen.

Abschließend legst du eine Frist für den Abschluss der Schulung fest. Standardmäßig beträgt diese 30 Tage. Du kannst den Zeitraum jedoch auch verkürzen, zum Beispiel auf 7 bis 14 Tage, wenn du eine schnellere Umsetzung bevorzugst.

Zukünftige Optionen für benutzerdefinierte Payloads: Bei der Erstellung einer benutzerdefinierten Payload gibt es Optionen für E-Mail und Teams, aber diese sind im Erstellungsprozess noch nicht verfügbar und ausgegraut.

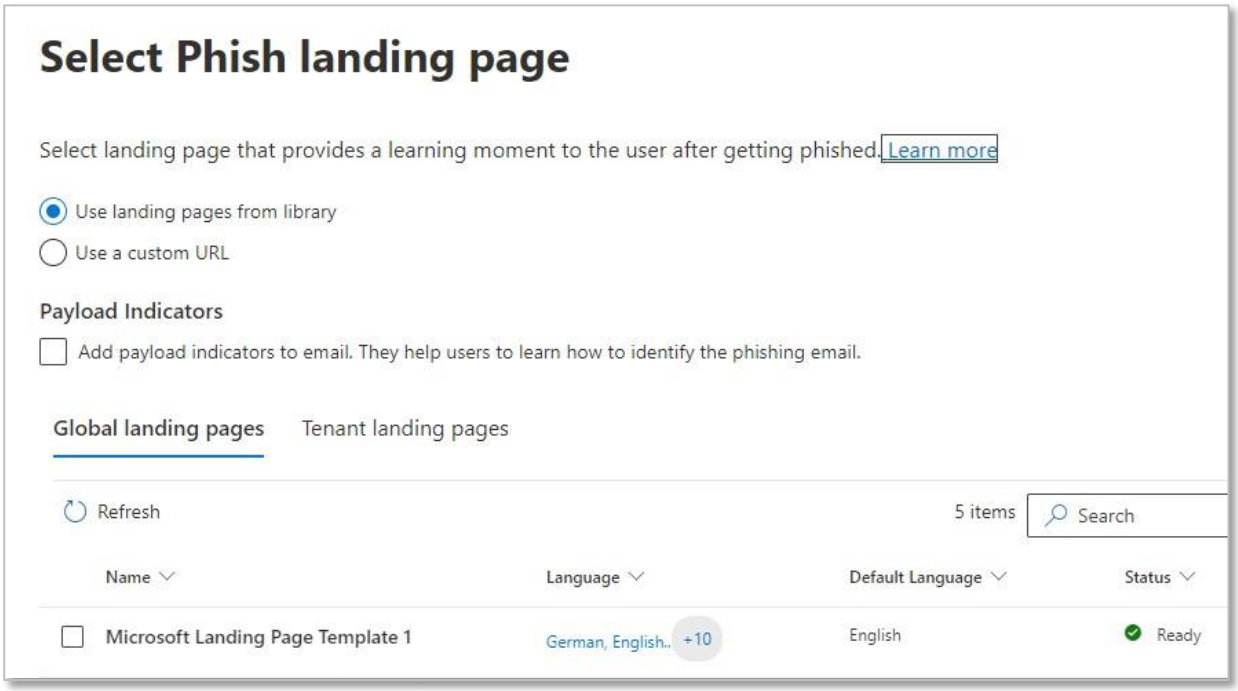


Abbildung 6-57: Auswahl einer Phishing-Zielseite

Du kannst dir die Zielseite, die den Benutzern beim Phishing angezeigt wird, in der Vorschau ansehen; sie ist in mehreren Sprachen verfügbar. Es stehen sowohl vorgefertigte Zielseiten von Microsoft als auch solche zur Verfügung, die von Mandantenadministratoren selbst erstellt werden können. Für den ersten Einsatz ist es empfehlenswert, mit den von Microsoft bereitgestellten Seiten zu starten, da diese sofort einsatzbereit sind. Sobald du mit dem Aufbau vertraut bist, kannst du in Erwägung ziehen, eigene, angepasste Seiten zu erstellen.

Anschließend passt du die Benachrichtigungen an, die an die Endbenutzer gesendet werden. Du kannst wählen, ob keine Benachrichtigung versendet wird, ob du die von Microsoft empfohlenen Benachrichtigungen verwendest oder ob du eigene, benutzerdefinierte Nachrichten erstellst. Grundsätzlich gilt: Je mehr Informationen deine Benutzer erhalten, desto besser. Daher ist es für den Einstieg sinnvoll, die Microsoft-Vorlage zu verwenden und später auf eine eigene Nachricht umzustellen, wenn du mit dem Ablauf vertraut bist.

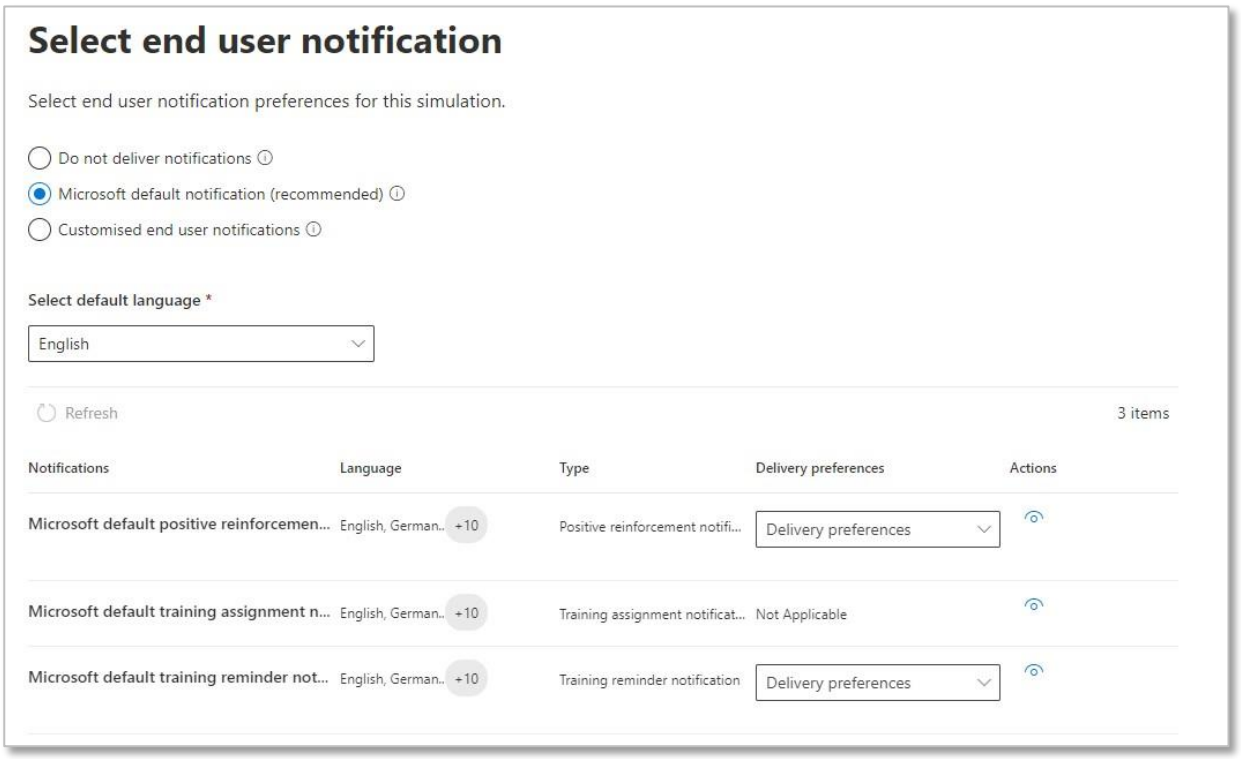


Abbildung 6-58: Endbenutzerbenachrichtigungen für die Simulation.

Du kannst dabei die gewünschte Sprache einstellen. Es gibt auch Optionen für positive Rückmeldungen und für den Zeitpunkt der Zustellung. Die Zustelloptionen sind:

- **Nicht zustellen:** Es werden keine Benachrichtigungen an die Endbenutzer gesendet.
- **Nach der Kampagne zustellen:** Sobald die Simulation beendet ist.

- **Während der Kampagne zustellen:** Benachrichtigungen werden zugestellt, wenn der Endbenutzer während der Simulation eine Aktion ausführt.

Für Erinnerungshinweise zum Training kannst du einstellen, dass diese entweder einmal oder zweimal pro Woche versendet werden.

Sobald du alle Einstellungen vorgenommen hast, kannst du die Simulation sofort starten oder für einen späteren Zeitpunkt planen. Wenn du sie verzögert starten willst, kannst du zwischen 2 oder 7 Tagen wählen und die Startzeit an die jeweilige Zeitzone anpassen:

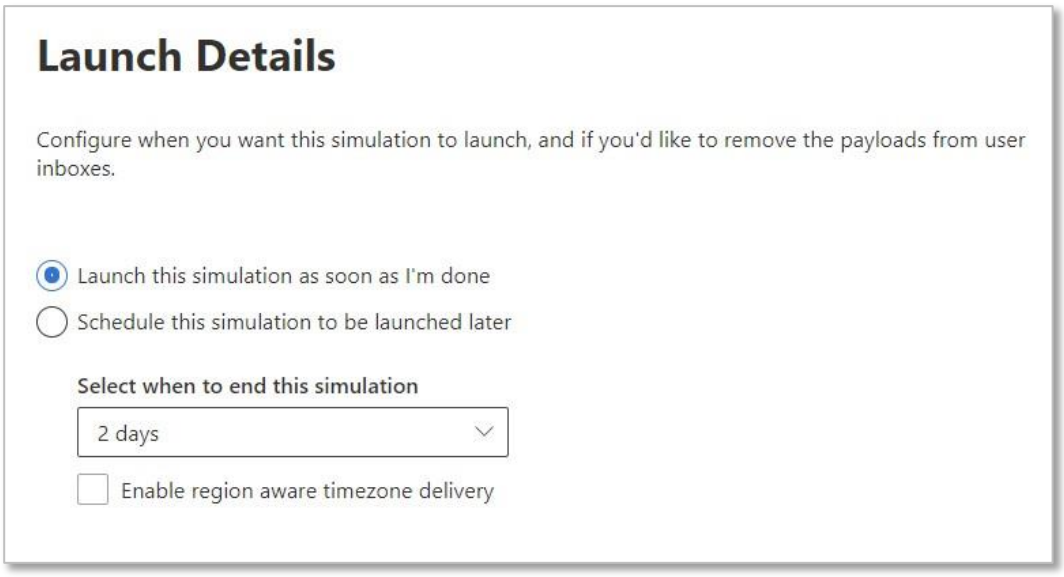


Abbildung 6-59: Starten einer Angriffssimulation.

Nach erfolgreicher Planung oder dem Start der Simulation erscheint diese auch im Dashboard:

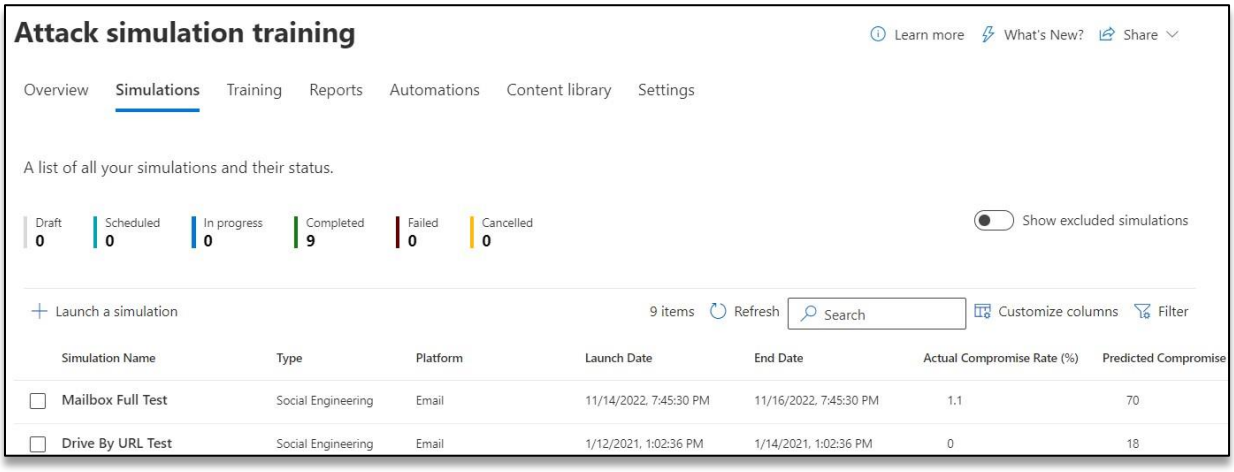


Abbildung 6-60: Eine Übersicht über aktive Simulationen in einer Umgebung.

Simulationen kopieren

Nachdem eine Angriffssimulation erstellt wurde, kannst du sie duplizieren. Das ermöglicht es dir, ein bestehendes Szenario schnell auf eine andere Benutzergruppe anzupassen. Wenn du zum Beispiel eine Credential-Harvesting-Simulation für deine Marketingabteilung erstellt hast, kannst du diese kopieren, die Zielgruppe und die Payload anpassen und sie dann für die Personalabteilung oder das Management erneut durchführen. So vermeidest du den Aufwand, jedes Mal eine neue Simulation von Grund auf zu erstellen.

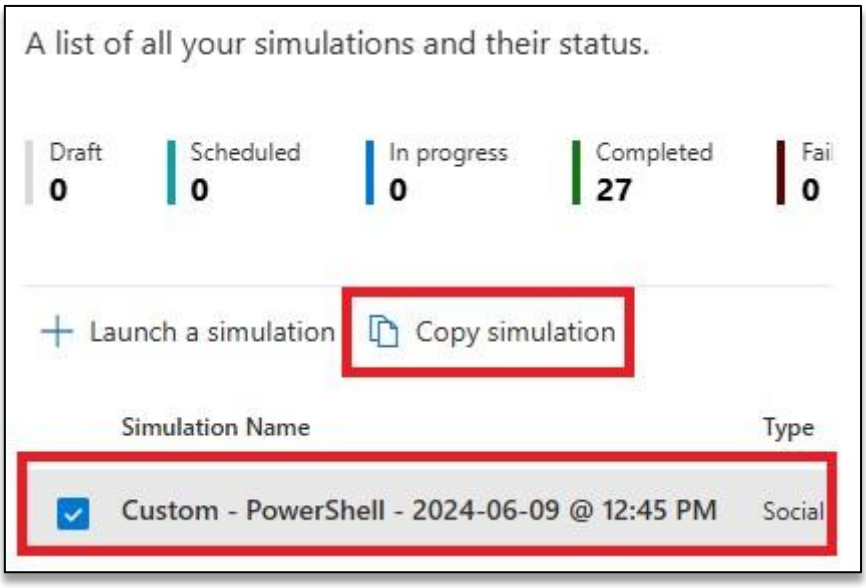


Abbildung 6-61: Die im April 2024 hinzugefügte Funktion "Simulation kopieren" ist ein Segen für Administratoren.

Benutzerdefinierte Payloads

Payloads sind vorgefertigte Angriffsszenarien, die Microsoft im Angriffssimulator bereitstellt. Du musst nicht alle verwenden. Es ist möglich, gezielte Tests oder zufällig ausgewählte Simulationen zu starten, um eine bestimmte Benutzergruppe zu trainieren. Zum Zeitpunkt dieses Textes stehen mehr als 380 einsatzbereite Payloads zur Verfügung:

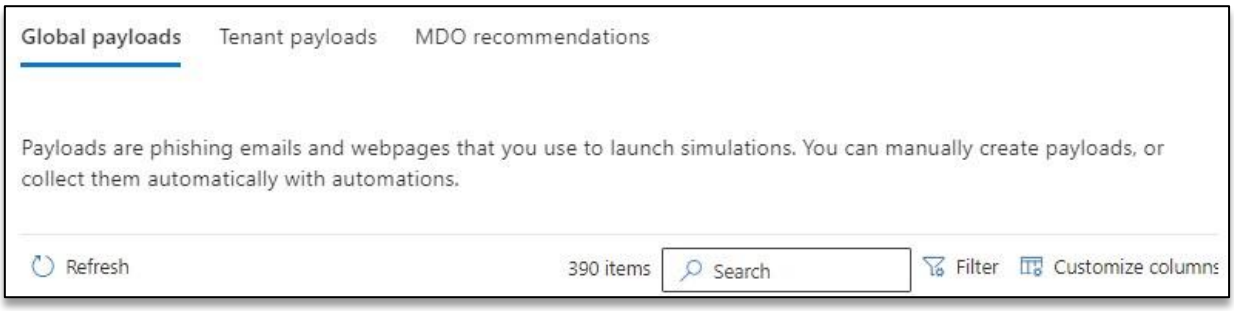


Abbildung 6-62: Verfügbare Payloads im Angriffssimulator.

Auf derselben Payload-Seite findest du auch einen Link zu allen Simulationen, die bereits mit dieser Payload durchgeführt wurden:

Abbildung 6-63: Gestartete Simulation mit einer bestimmten Payload.

Eine neue Funktion im Angriffssimulator ist die Möglichkeit, eigene Payloads zu erstellen. Das ist besonders hilfreich, wenn du Szenarien entwickeln möchtest, die speziell auf dein Unternehmen, deine Branche oder auf aktuelle Phishing-Wellen zugeschnitten sind. Diese Anpassungen lassen sich direkt in der Benutzeroberfläche durchführen.

Um eine eigene Payload zu erstellen, hast du zwei Möglichkeiten: Entweder du startest eine neue Simulation und erstellst die Payload dabei, oder du nutzt die Registerkarte „Payloads“, um eine neue direkt dort anzulegen. In diesem Beispiel verwenden wir den Weg über eine Simulation. Du wählst zunächst eine der verfügbaren Techniken aus – etwa Credential Harvesting, Malware-Anhang, Link im Anhang oder Link zu Malware – und erstellst im Anschluss die benutzerdefinierte Payload. Beim Erstellen stehen dir aktuell zwei Optionen zur Verfügung, allerdings ist derzeit nur die Variante per E-Mail nutzbar.

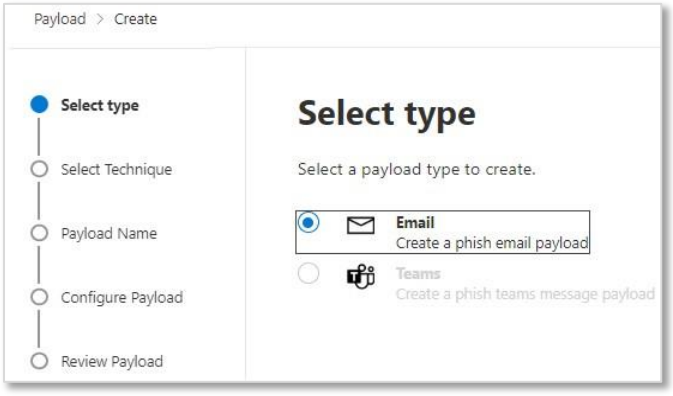


Abbildung 6-64: Erstellung einer benutzerdefinierten Payload.

Zunächst musst du die Payload einer der Techniken im Angriffssimulator zuweisen. Diese sind:

- Anmeldeinformationen ernten
- Malware-Anhang
- Link im Anhang
- Link zu Malware
- Drive-by-URL
- OAuth-Zustimmungserteilung
- Anleitungen

Danach gibst du einen Namen und eine Beschreibung für deine Payload ein. So kannst du sie später wiederverwenden und gezielt auf bestimmte Benutzergruppen anwenden:

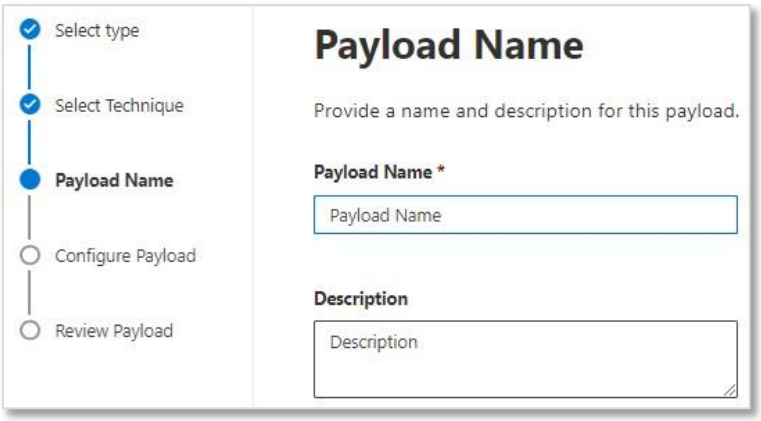


Abbildung 6-65: Angabe grundlegender Payload-Informationen.

Für ein zuverlässigeres Benutzererlebnis kannst du dieses Kontrollkästchen aktivieren, damit die Benutzer die E-Mail als externe Nachricht erkennen. Auch wenn das keine perfekte Lösung ist, besteht ohne diese Einstellung die Möglichkeit, dass eine vom Angriffssimulator generierte E-Mail wie eine interne E-Mail aussieht.

Abbildung 6-66: Kontrollkästchen für die Anzeige externer E-Mails.

Abbildung 6-67: Durch das Kontrollkästchen wird der Hinweis auf externe Nachrichten angezeigt.

Im nächsten Schritt gibst du den Absendernamen bzw. die Absenderadresse, einen Betreff und den Phishing-Link an. Zusätzlich kannst du ein Thema, eine Marke, eine Branche, ein aktuelles Ereignis, den Grad der Kontroverse sowie die Sprache der E-Mail festlegen.

Abbildung 6-68: Zusätzliche Anpassungen für die simulierte E-Mail.

Diese Optionen – also **Tags, Thema, Marke, Branche, aktuelles Ereignis** und **kontrovers** – scheinen als Filter für die verfügbaren Payloads zu dienen, die du beim Erstellen der Simulation nutzen kannst. Für den Phishing-Link stellt dir Microsoft eine Auswahl vorgegebener Links zur Verfügung. Eigene Links kannst du an dieser Stelle nicht verwenden. Wenn du nach unten scrollst, trägst du den Textkörper der E-Mail ein.

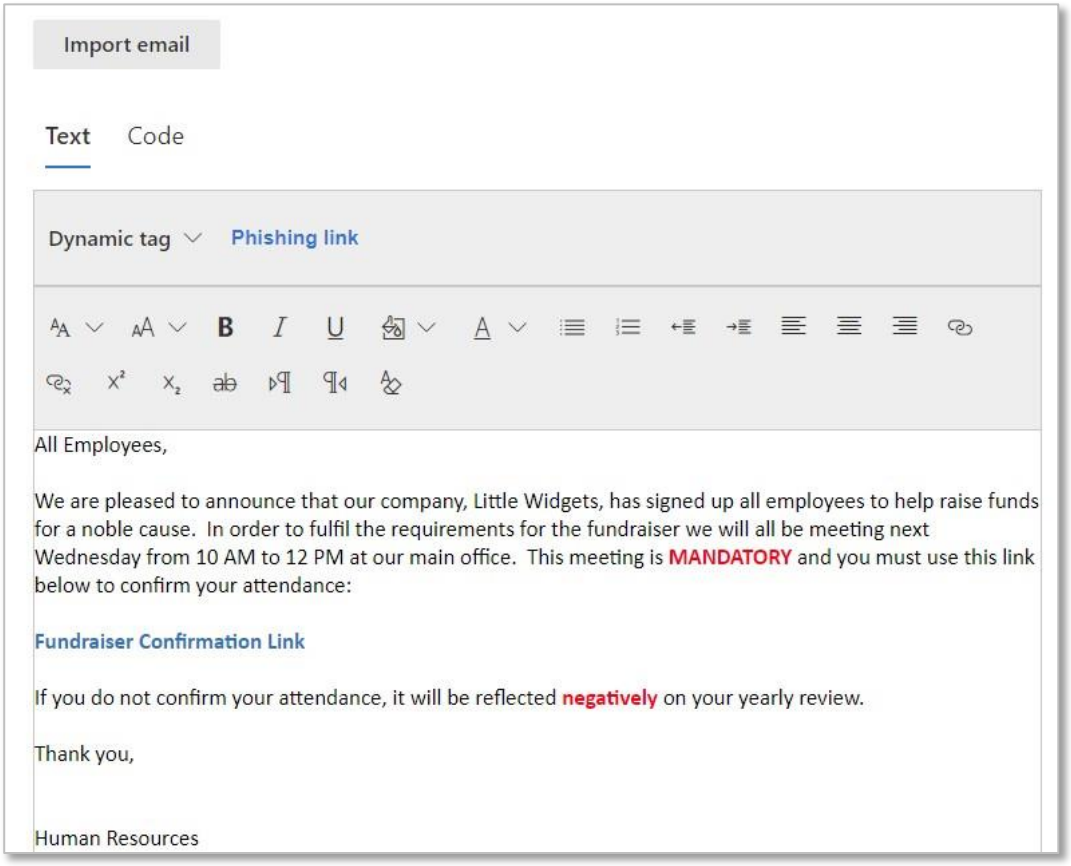


Abbildung 6-69: Anpassung des Textkörpers einer benutzerdefinierten Payload

Wenn du die E-Mail weiter anpassen möchtest, kannst du sogenannte Indikatoren hinzufügen. Diese dienen später als Lernhilfe für die Benutzer und zeigen auf, warum es sich bei der Nachricht um eine gefährliche E-Mail handelt – nachdem jemand auf den Phishing-Link geklickt hat. Microsoft stellt hierfür eine Liste mit über 20 möglichen Indikatoren bereit, die du verwenden kannst.

Sobald die E-Mail erstellt ist, kannst du die gewünschten Indikatoren hinzufügen. Sie werden später im Rahmen der Angriffssimulation angezeigt, um dem Benutzer die Schwachstellen in der Nachricht zu erklären.

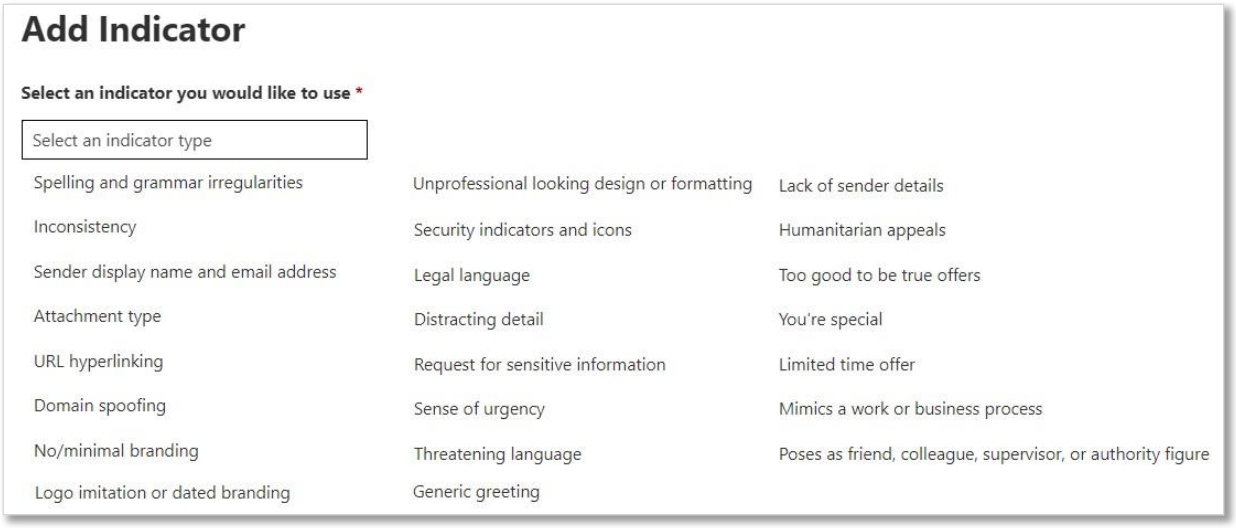


Abbildung 6-70: Für benutzerdefinierte Payloads verfügbare Indikatoren.

Beispielindikator:

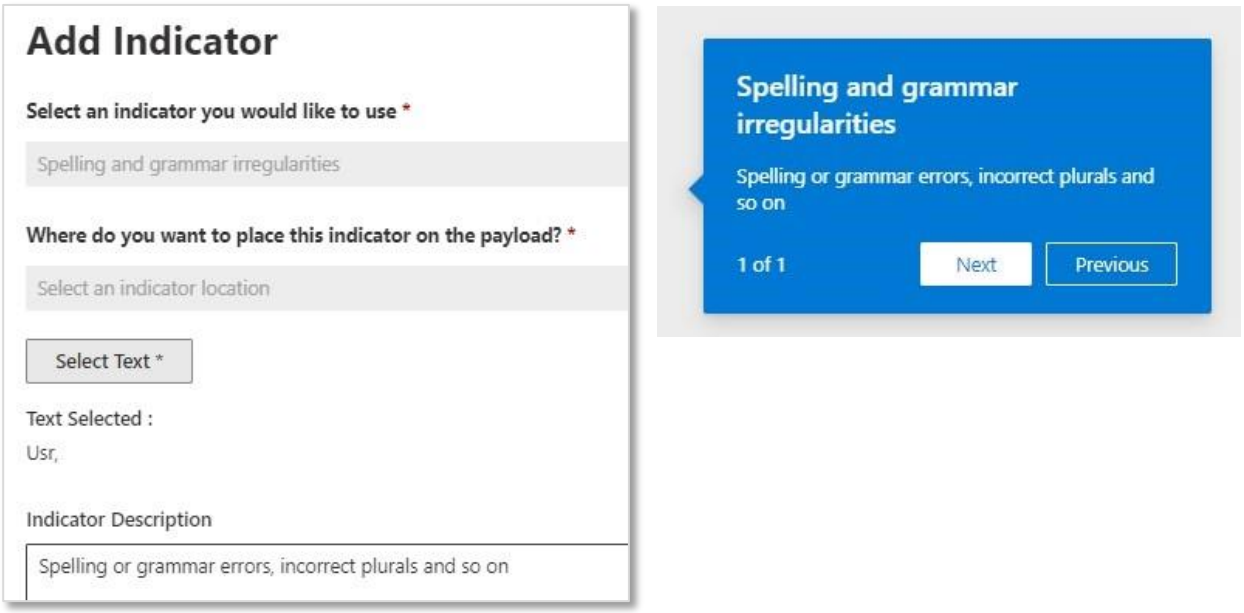


Abbildung 6-71: Indikator für schlechte Rechtschreibung oder Grammatik in der Nachricht.

Am Ende hast du einen Payload-Überprüfungsbildschirm, in dem du bei Bedarf Anpassungen vornehmen kannst:

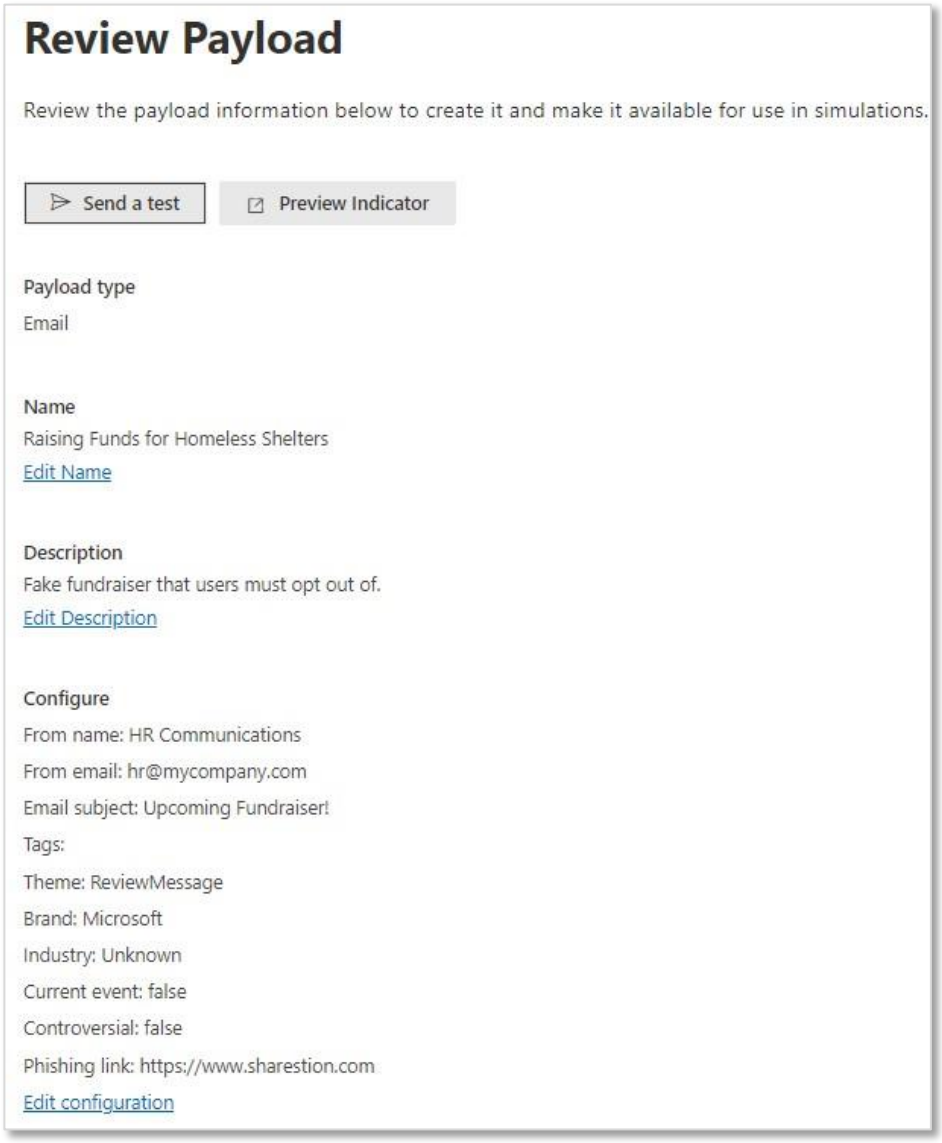


Abbildung 6-72: Überprüfung der benutzerdefinierten Payload.

Sobald du mit der Erstellung deiner Payload fertig bist, kannst du auf „Senden“ klicken, um sie zur Verwendung bereitzustellen. Die neue Payload erscheint dann am Ende der Liste der verfügbaren Optionen für den gewählten Angriffstyp:

Abbildung 6-73: Auswahl einer benutzerdefinierten Payload beim Starten einer Simulation.

Wenn du die Simulation startest, wird deine benutzerdefinierte Payload-E-Mail automatisch verwendet und in der neu erstellten Simulation eingesetzt:

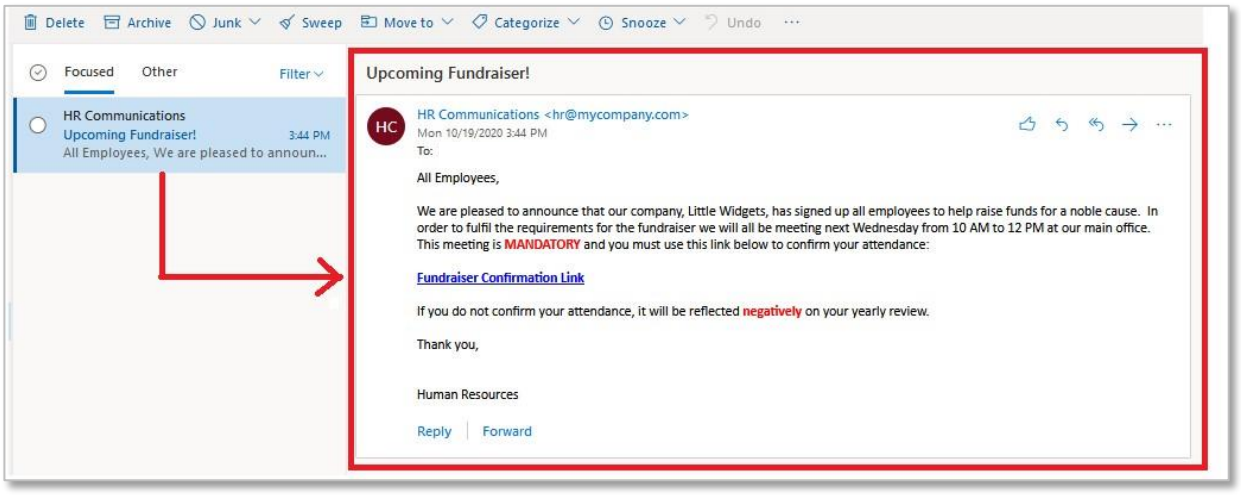


Abbildung 6-74: Textkörper einer benutzerdefinierten Payload, die in einer Simulation verwendet wird.

Nicht übertreiben. Natürlich könntest du eine Payload entwerfen, die selbst erfahrene Administratoren täuschen würde. Das ist aber nicht das Ziel. Eine Angriffssimulation soll Lernpotenzial bieten, nicht deine benutzer bloßstellen. Denke daran, dass echt Phishing-Mails oft Rechtschreibfehler, schlechte Formulierungen oder andere Hinweise enthalten, die auf ihren betrügerischen Charakter hinweisen. Gib deinen Benutzern auch bei benutzerdefinierten Payloads die Möglichkeit, solche merkmale zu erkennen. Das erhöht sogar die Realitätsnähe.

Endbenutzer-Erfahrung

Sobald du eine Simulation gestartet hast, erhalten die Endbenutzer entsprechende E-Mails, und der Test- und Lernprozess beginnt. Sie sehen das von dir konfigurierte Phishing-Szenario, sobald die Nachrichten durch den Angriffssimulator versendet wurden. Die E-Mails landen direkt im Posteingang, wie in der entsprechenden Abbildung dargestellt:

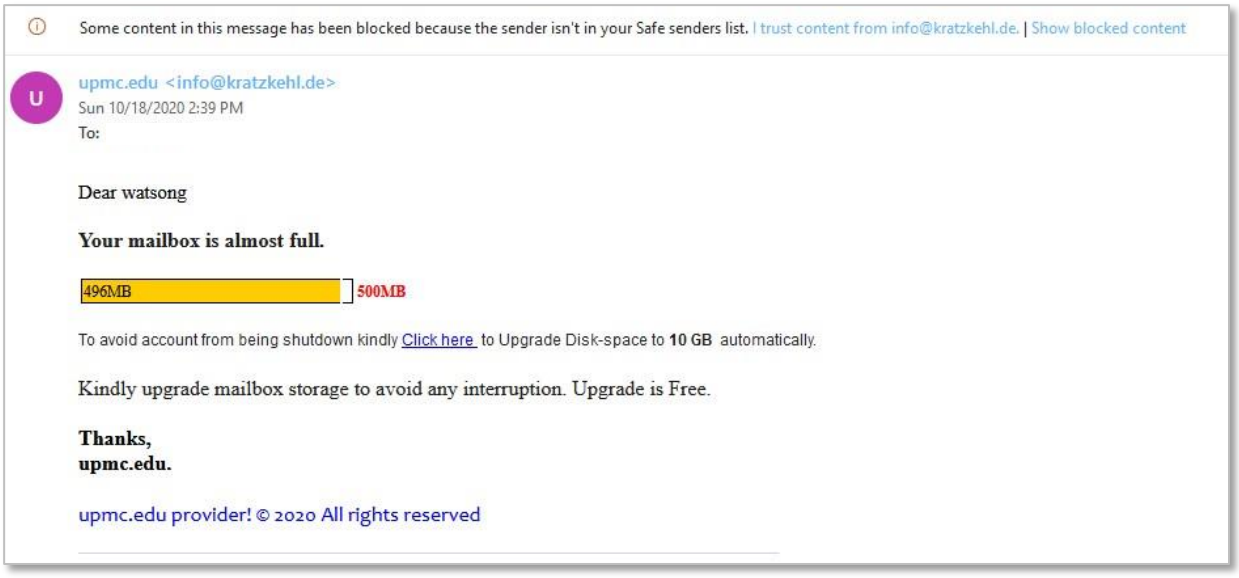


Abbildung 6-75: Beispiel für eine simulierte Phishing-Angriffsnachricht

Wenn du genau hinsiehst, lassen sich typische Hinweise auf eine Phishing-Mail erkennen. Ein geschultes Auge bemerkt diese schnell – aber wie sieht es bei deinen Benutzern aus?

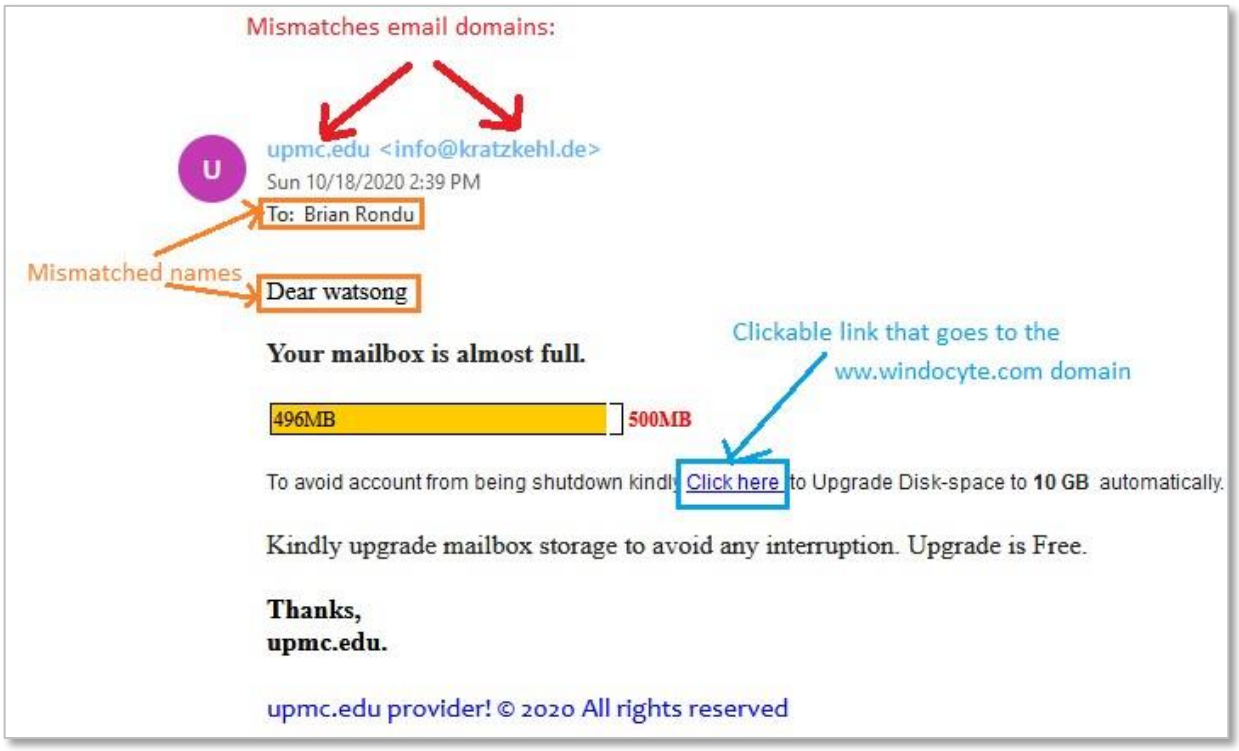


Abbildung 6-76: Erkennen von Phishing-Nachrichten.

Angenommen, ein Benutzer klickt auf den Link, um scheinbar sein Postfach zu bereinigen. In diesem Fall landet er auf einer Anmeldeseite, die aussieht wie die offizielle Microsoft-Loginseite. Achte auf die URL!

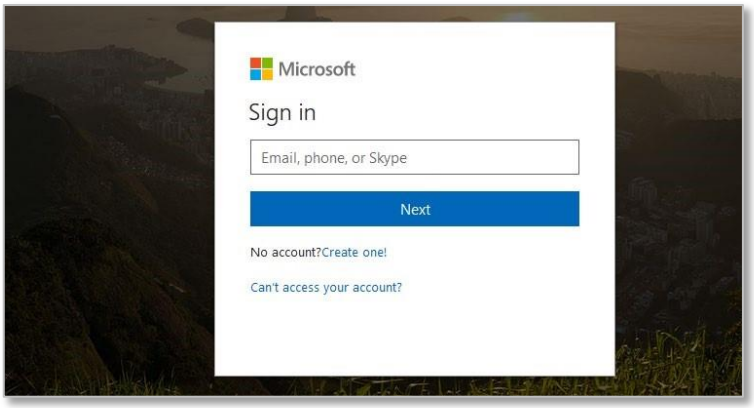


Abbildung 6-77: Eine Phishing-Anmeldeseite

Wenn der Benutzer seine Anmeldedaten eingibt, sieht er anschließend einen Bildschirm, der dem im Simulationsassistenten angegebenen Standardtext entspricht. Dort wird ihm unmittelbar signalisiert, dass er auf einen Phishing-Versuch hereingefallen ist, und er erhält Hinweise, woran er den Betrug hätte erkennen können. Ziel ist es nicht, den Benutzer zu kritisieren, sondern ihm zu helfen, künftig besser vorbereitet zu sein:

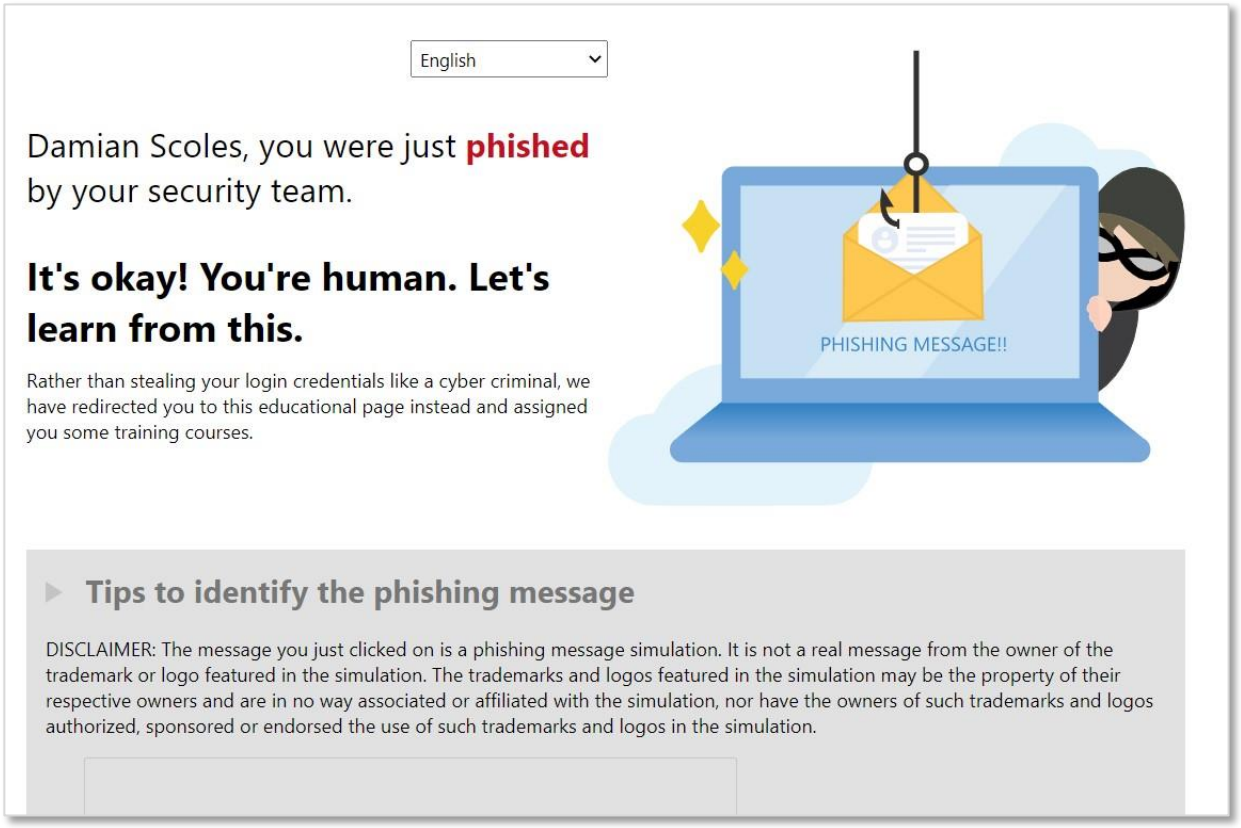


Abbildung 6-78: Erwischt! Ein Benutzer ist auf die vom Administrator erstellte Falle hereingefallen.

Innerhalb dieses Bildschirms wird dem Benutzer sofort mitgeteilt, dass er einen Fehler gemacht hat, und er erhält einige Hinweise, wie er hätte erkennen können, dass dies keine legitime Anfrage war. Schließlich geht es nicht darum, die Benutzer zu tadeln, sondern ihnen zu helfen, beim nächsten Start eines Angriffs besser vorbereitet zu sein.

Wenn Benutzer die E-Mail melden oder auf den Link klicken, kannst du als Administrator die Ergebnisse im Angriffssimulator unter dem Status der erstellten Simulation einsehen:

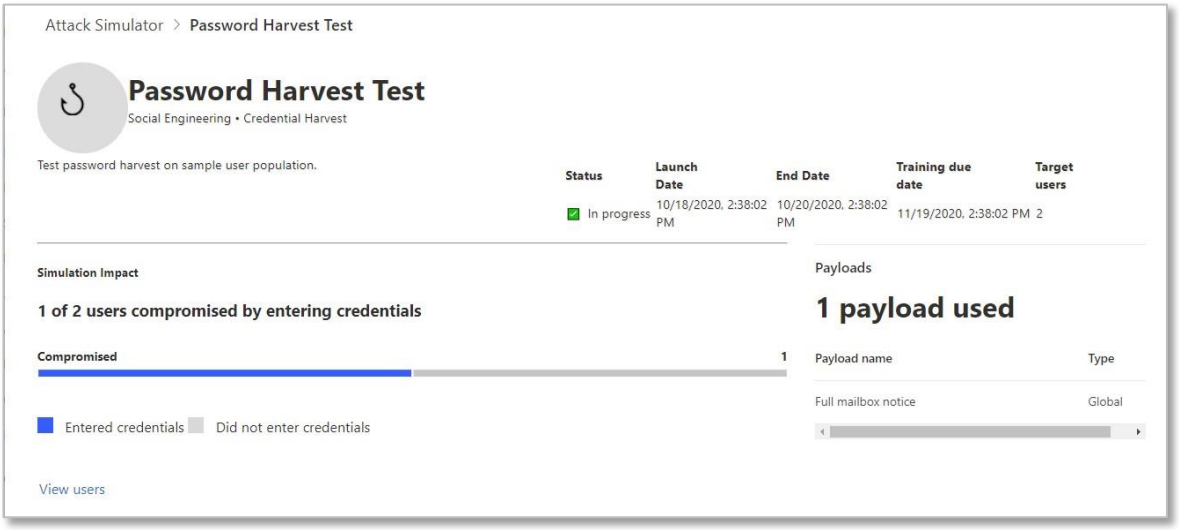


Abbildung 6-79: Überprüfung der Ergebnisse eines simulierten Angriffs.

Schulung nach dem Angriff

Was passiert, wenn ein Benutzer in der Simulation auf den Link klickt oder sogar seine Anmeldedaten eingibt? Dann wechselt die Simulation in den Schulungsmodus. Der Benutzer erhält E-Mails mit Lerninhalten zum spezifischen Angriff, dem er zum Opfer gefallen ist:

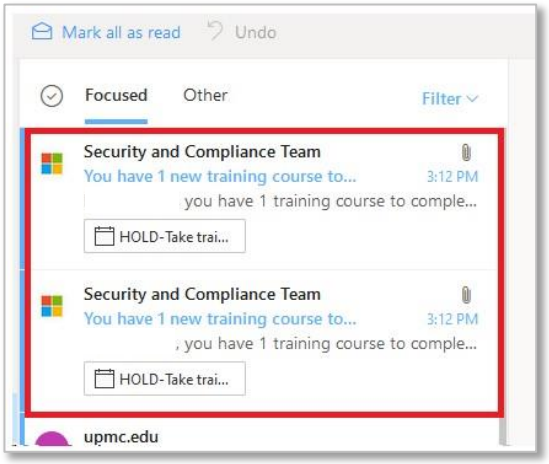


Abbildung 6-80: Schulungs-E-Mails des Angriffssimulators

Diese E-Mails enthalten unter anderem eine Einladung, einen Schulungskurs zu absolvieren. Der Benutzer klickt auf einen Link, der ihn direkt zur Schulung führt.

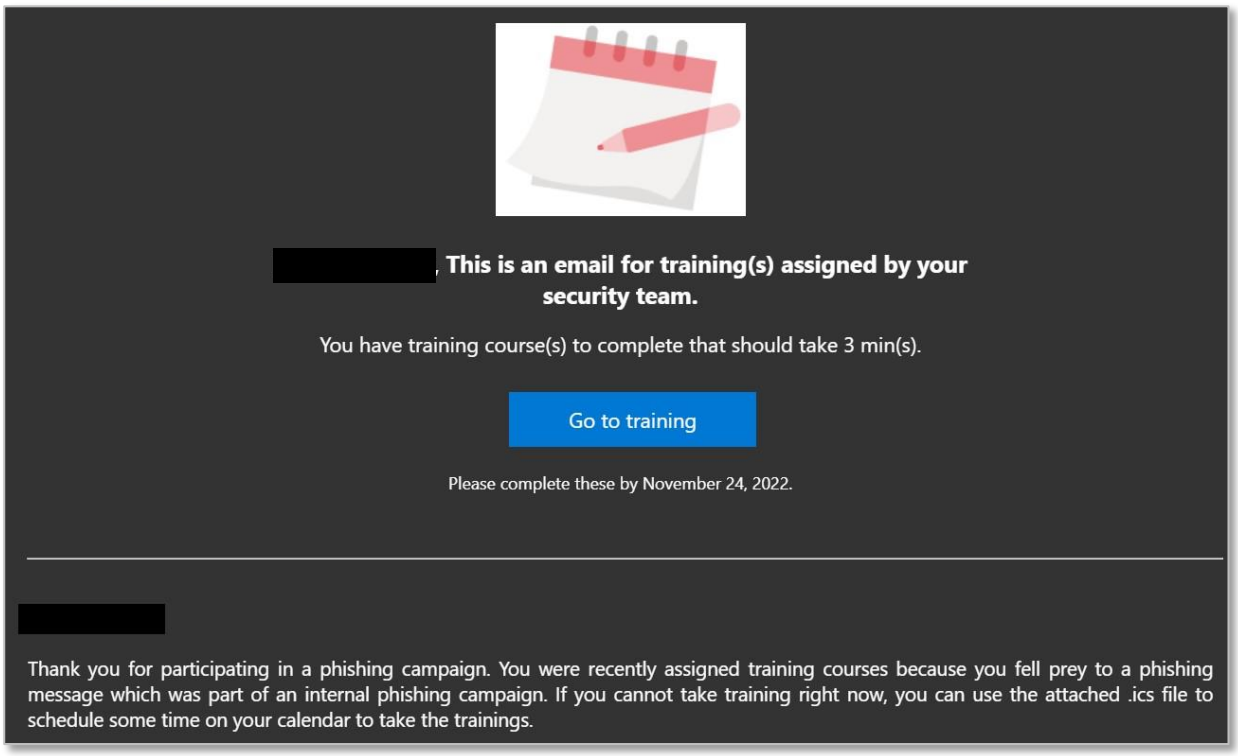


Abbildung 6-81: Textinhalt einer Schulungs-E-Mail des Angriffssimulators.

Mit einem Klick auf „Zur Schulung“ wird er zur Seite „Schulungszuweisungen“ weitergeleitet. Dort kann er die ihm zugewiesenen Kurse absolvieren. Je nachdem, welche Optionen du in der Simulation festgelegt hast, kann ihm auch mehr als ein Kurs zugewiesen worden sein.

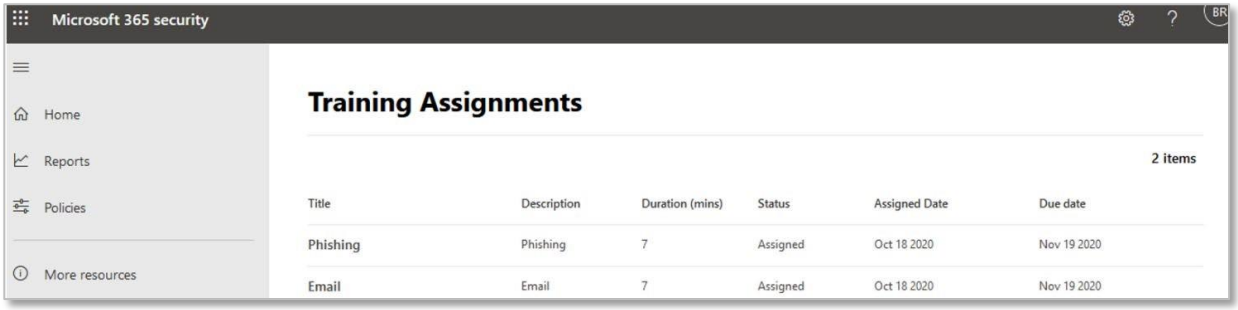


Abbildung 6-82: Seite mit Schulungszuweisungen.

Wenn er dann auf einen der Schulungslinks klickt – beispielsweise für Phishing oder E-Mail-Sicherheit – startet der jeweilige Kurs. Die Schulung ist interaktiv und endet mit einem kurzen Quiz, das überprüft, was der Benutzer gelernt hat.

Abbildung 6-83: Schulung zur Sensibilisierung der Benutzer.

Nach Abschluss der Schulung erhält der Benutzer eine Übersicht mit seinem Ergebnis. In seiner Schulungsansicht wird der Kurs jetzt als „Abgeschlossen“ statt „Zugewiesen“ angezeigt.

Auch du als Administrator kannst den Schulungsfortschritt verfolgen. Dazu klickst du auf „**Bericht zur Durchführung der Schulung anzeigen**“, um zu sehen, welche Benutzer teilgenommen haben und wie weit sie sind.

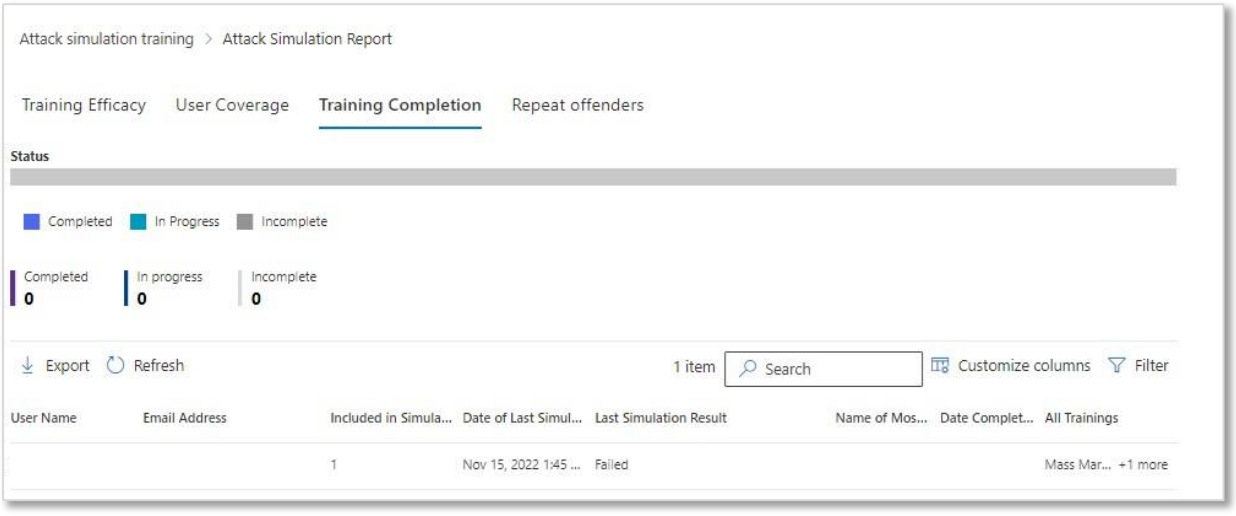


Abbildung 6-84: Verfolgung der Benutzeraktivitäten.

Payload-Automatisierungen

Innerhalb des Angriffssimulationstrainings findest du unter **Automatisierung** den Punkt „**Payload-Automatisierungen**“. Mit dieser Funktion werden Angriffstechniken gesammelt, die gegen einen Mandanten eingesetzt wurden. Der Gedanke dahinter ist, dass du dich nicht nur auf selbst erstellte Payloads verlassen musst, sondern auch auf Angriffe böswilliger Akteure zurückgreifen kannst, die bereits blockiert wurden. Diese realen Beispiele kannst du dann effektiver in deinen Trainings einsetzen. Du kannst eine Automatisierung einrichten, um solche Payloads zu erfassen – alle gesammelten Payloads werden anschließend auf der Registerkarte „Payloads“ hinzugefügt.

Erstellen einer Automatisierung

Auf der Registerkarte „Simulationsautomatisierungen“ kannst du auf „Automatisierung erstellen“ klicken:

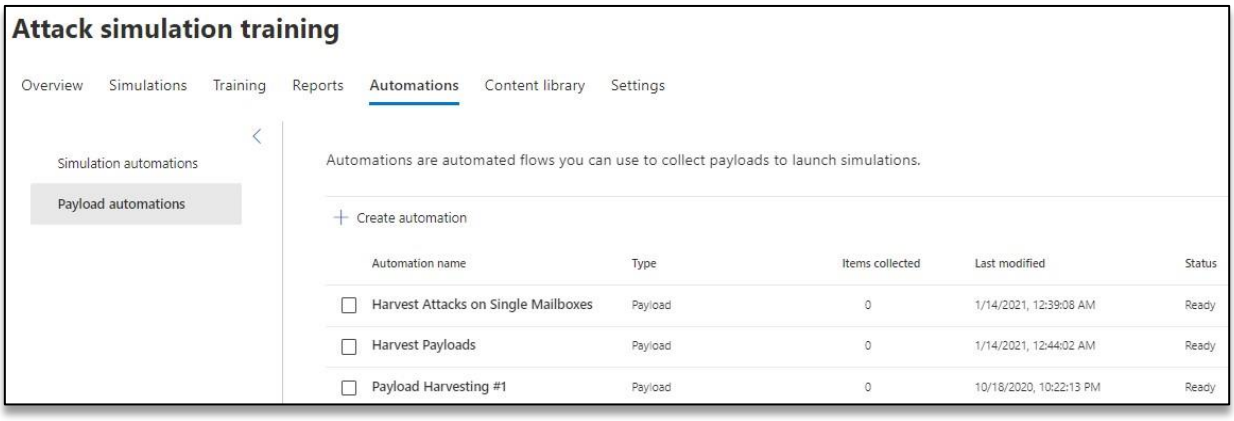


Abbildung 6-85: Aktuelle Automatisierungen.

Achte darauf, dass du einen gültigen Namen und eine passende Beschreibung für die Automatisierung angibst. Danach musst du Bedingungen festlegen, die erfüllt sein müssen, damit eine Payload erfasst wird:

Abbildung 6-86: Automatisierungsbedingungen.

Bei der Erstellung kannst du eine oder mehrere Bedingungen auswählen, um den Automatisierungsprozess zu starten:

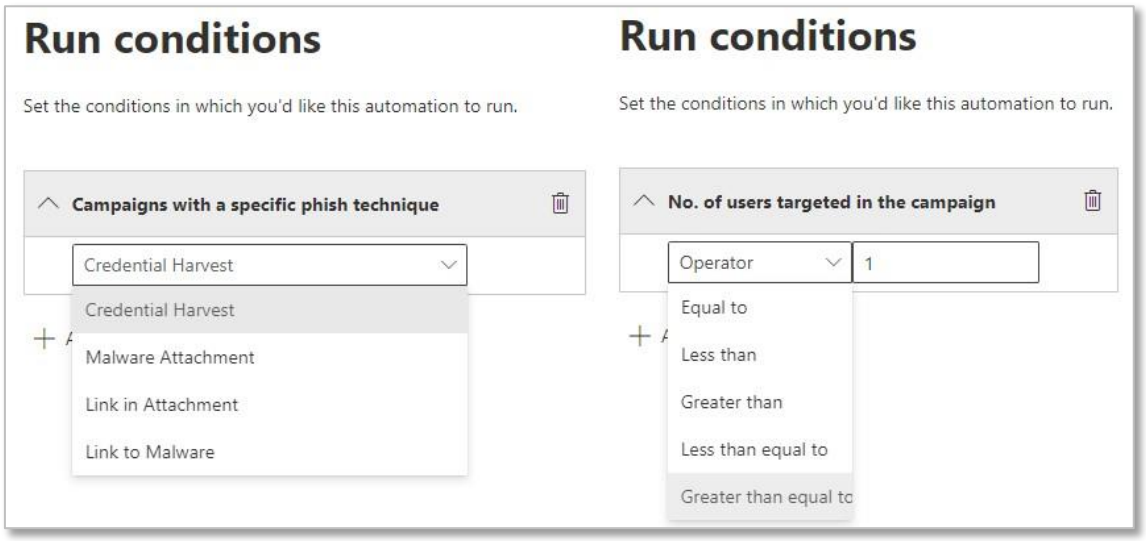


Abbildung 6-87: Beispielbedingungen oben.

Nachdem du die Bedingungen definiert hast, kannst du die neue Automatisierung absenden, damit sie aktiviert wird und mit dem Sammeln beginnt. Beachte dabei, dass die Automatisierung beim Erstellen aktiviert werden muss – andernfalls fehlt aktuell in der Benutzeroberfläche die Möglichkeit, sie später manuell zu aktivieren oder zu deaktivieren (dies ist ein bekannter Fehler).

Sobald die Automatisierungen erstellt wurden und eine Zeit lang gelaufen sind, erscheinen die erfassten Nutzdaten auf der Registerkarte „Nutzdaten“. Wenn du einige dieser Payloads

gesammelt hast, kannst du sie in deinen Kampagnen einsetzen, um das Sicherheitsbewusstsein deiner Endbenutzer mit realen Beispielen zu stärken.

Simulationsautomatisierungen

Unter der Registerkarte „Automatisierungen“ befindet sich auch die Registerkarte „Simulationsautomatisierungen“. Hier kannst du Tests mit denselben Techniken, Benutzern und Schulungszielen automatisieren, die du bereits bei einzelnen Simulationen verwendet hast. Der Unterschied besteht darin, dass du diese Tests planen und zu einem zukünftigen Zeitpunkt automatisch ausführen lassen kannst.

Erstellen einer Simulationsautomatisierung

Wenn du eine solche Automatisierung erstellst, gib bitte einen aussagekräftigen Namen und eine passende Beschreibung an. So weißt du später genau, wofür die geplante Simulation gedacht war. Du kannst dabei entweder eine bestimmte Payload auswählen oder Microsoft eine zufällige Payload auswählen lassen.

Der erste Schritt besteht darin, einen Namen und eine Beschreibung für diese Automatisierung anzugeben. Anschließend wählst du wie bei regulären Automatisierungen eine Angriffstechnik aus – etwa Anmeldeinformationsabgreifen, Malware-Anhang, Link im Anhang, Link zu Malware, Drive-by-URL oder OAuth-Zustimmungserteilung.

Abbildung 6-88: Manuelle oder zufällige Nutzlastauswahl.

Im nächsten Schritt legst du fest, welche Benutzer betroffen sein sollen. Du kannst entweder alle Benutzer in der Organisation einbeziehen oder gezielt einzelne Benutzer und Gruppen auswählen. Nach der Auswahl der Zielgruppe kannst du das Schulungsszenario bestimmen – wie auch beim herkömmlichen Simulationserstellungsprozess. Dabei legst du auch fest, welche Zielseite den Benutzern nach der Simulation angezeigt wird.

Wie bei den einmaligen Simulationen musst du also **Schulungsmaßnahmen** zuweisen und eine **Endbenutzer-Zielseite** auswählen.

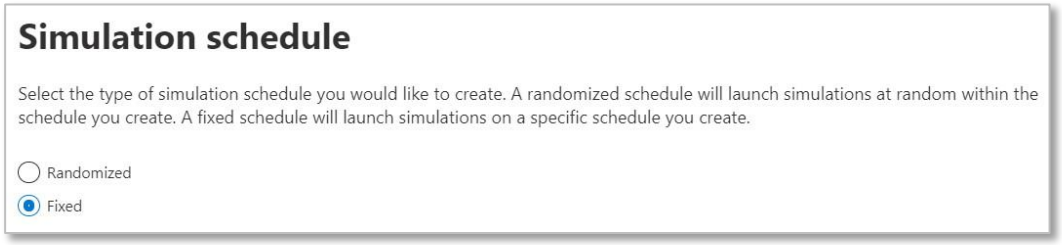


Abbildung 6-89: Entscheide, ob die Automatisierung nach einem zufälligen oder festen Zeitplan ausgeführt wird.

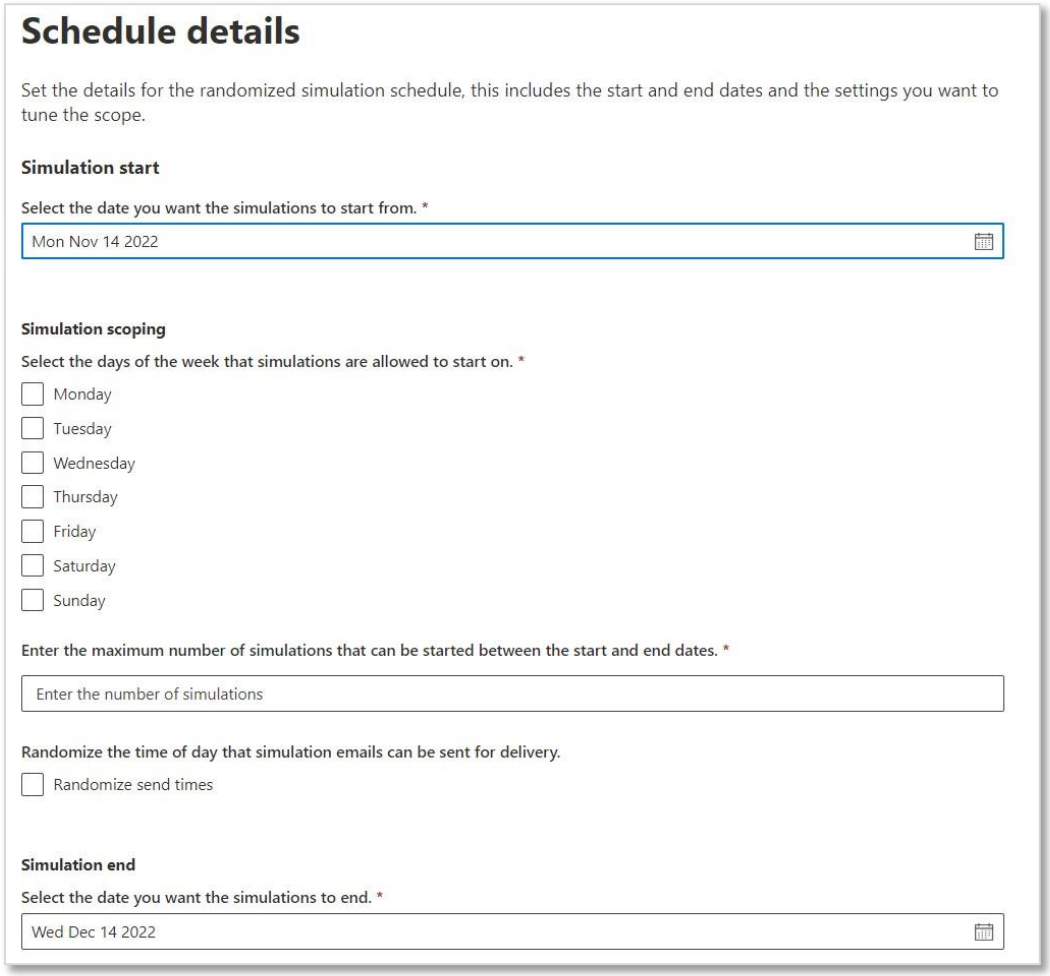


Abbildung 6-90: Konfiguriere den Zeitplan der Simulationen mit einem Bereich von 1 bis 10 Simulationen.

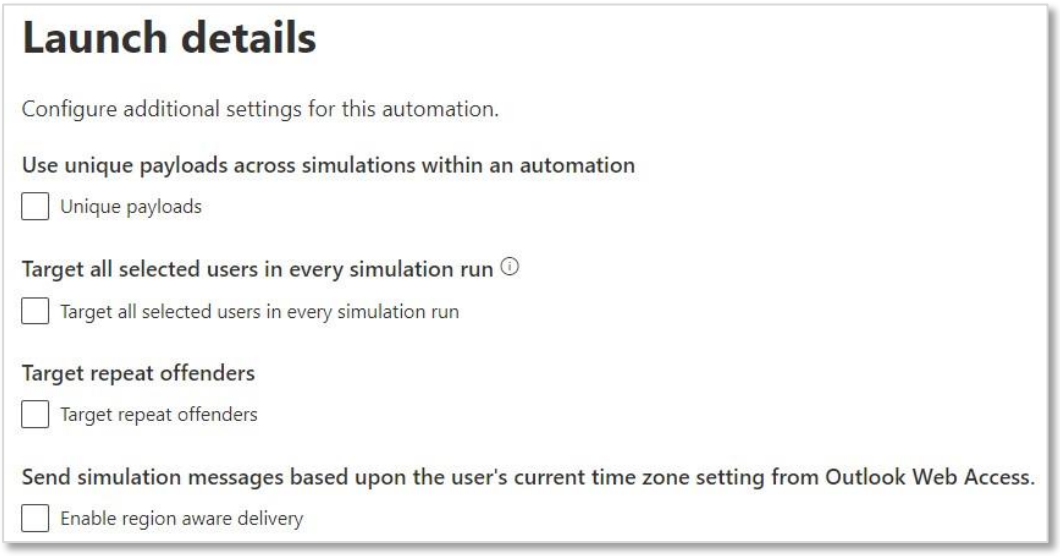


Abbildung 6-91: Zusätzliche Konfigurationsoptionen für Nutzdaten, Umgang mit Wiederholungstätern und Aktivierung regionsbewusster Einstellungen.

Registerkarte Einstellungen

Diese neue Registerkarte ist inzwischen in einigen Mandanten verfügbar. Leider gibt es noch keine offizielle Roadmap-Ankündigung dazu, sodass wir an dieser Stelle ein wenig spekulieren müssen. Gehen wir vorerst davon aus, dass diese Funktion künftig für alle Mandanten innerhalb der Angriffssimulationsschulung zur Verfügung stehen wird. Hier ist die Registerkarte samt der aktuell freigegebenen Einstellungen:

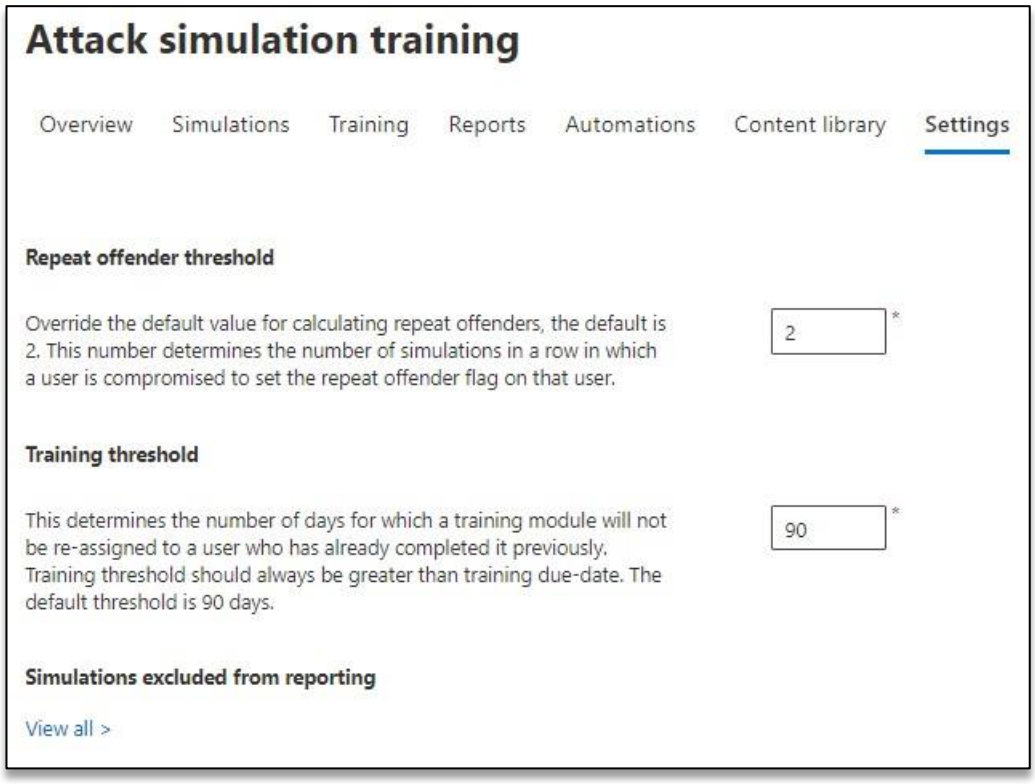


Abbildung 6-92: Registerkarte Einstellungen für die Angriffssimulationsschulung.

Wie du oben sehen kannst, stehen dir zwei Einstellungen zur Verfügung, mit denen du das Verhalten deiner Angriffssimulation anpassen kannst:

- **Schwellenwert für Wiederholungstäter**: Wie du mit Endbenutzern umgehst, deren Schulung nicht erfolgreich war.
- **Simulationen, die von der Berichterstattung ausgeschlossen sind**: Damit kannst du bestimmte Simulationen, beispielsweise Test-Simulationen, von der Auswertung ausnehmen.

Endbenutzer-Benachrichtigungen

Diese Funktion befindet sich nun unter „**Inhaltsbibliothek**“. Vor ihrer Einführung erhielten Endbenutzer in der Regel nur dann automatische E-Mails, wenn sie auf einen Link klickten oder bei einem simulierten Phishing-Angriff scheiterten. Für Mandantenadministratoren gab es keine Möglichkeit, diese E-Mails zu steuern oder anzupassen. Microsoft hat inzwischen eine neue E-Mail-Benachrichtigung eingeführt, die versendet wird, wenn ein Endbenutzer eine Phishing-E-Mail meldet. Diese wird als „positive Verstärkungsbenachrichtigung“ bezeichnet.

Diese neue Registerkarte stellt eine Erweiterung der Angriffssimulationsfunktion dar. Die Benachrichtigungen sind unterteilt in globale und Mandanten-Benachrichtigungen. Aktuell gibt

es zwei globale Benachrichtigungen, die du weder ändern noch löschen kannst, sowie keine vordefinierten Mandanten-Benachrichtigungen – du kannst jedoch eigene hinzufügen.

Wie zu erwarten, handelt es sich bei den globalen Benachrichtigungen um die standardmäßig eingesetzten Benachrichtigungen, die bereits vor der Möglichkeit zur individuellen Konfiguration verwendet wurden. Microsoft unterscheidet dabei zwischen zwei Kategorien:

- **Positive Verstärkungsbenachrichtigung**: Eine E-Mail für Benutze, die eine simulierte Phishing-E-Mail korrekt meldet.
- **Simulationsbenachrichtigung**: Eine E-Mail, die Benutzer darauf hinweist, dass sie kompromittiert worden wären, wenn es sich um einen echten Angriff gehandelt hätte.

Mandanten-Benachrichtigung erstellen

Wenn du deinen Benutzern ein personalisiertes Erlebnis bieten möchtest, kannst du zwei Arten benutzerdefinierter Benachrichtigungen erstellen: eine für Benutzer, die auf einen Phishing-Link klicken und damit die Simulation nicht bestehen, und eine für Benutzer, die eine simulierte E-Mail als Phishing melden. Beides kannst du unter der Registerkarte „Mandanten-Benachrichtigungen“ konfigurieren.

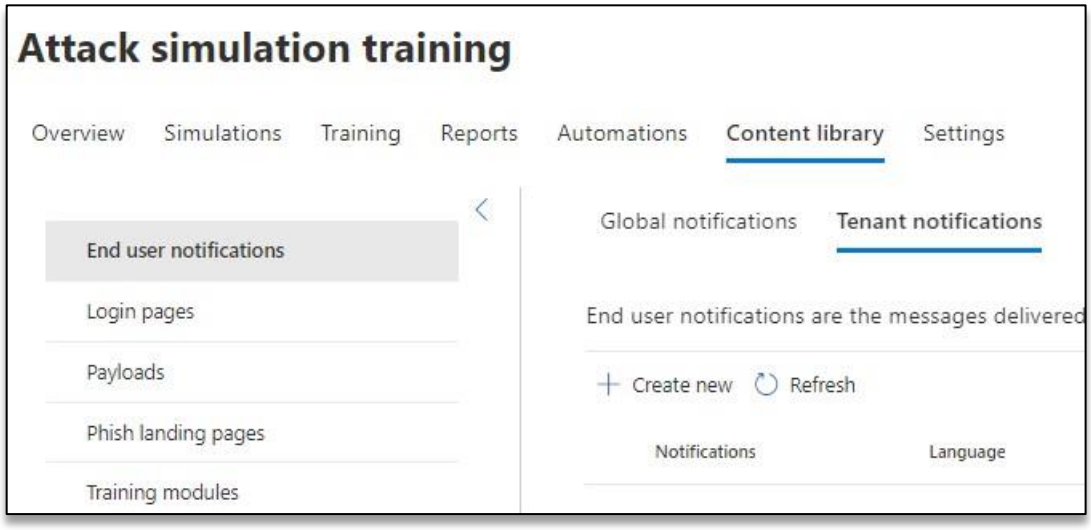


Abbildung 6-93: Nach dem Klicken auf "Mandanten-Benachrichtigungen" kannst du auf "Neu erstellen" klicken, um eine benutzerdefinierte Benachrichtigung zu erstellen.

Beim Erstellen einer neuen Benachrichtigung musst du zunächst festlegen, ob es sich um eine Simulationsbenachrichtigung oder eine positive Verstärkungsbenachrichtigung handelt. Dabei kannst du entweder die Vorlagen von Microsoft als Ausgangspunkt verwenden oder deine eigene Nachricht komplett neu gestalten – je nachdem, welche Inhalte du aus rechtlichen oder unternehmensinternen Gründen einfügen möchtest.

Im nächsten Schritt gibst du den Text für den Hauptteil der E-Mail ein:

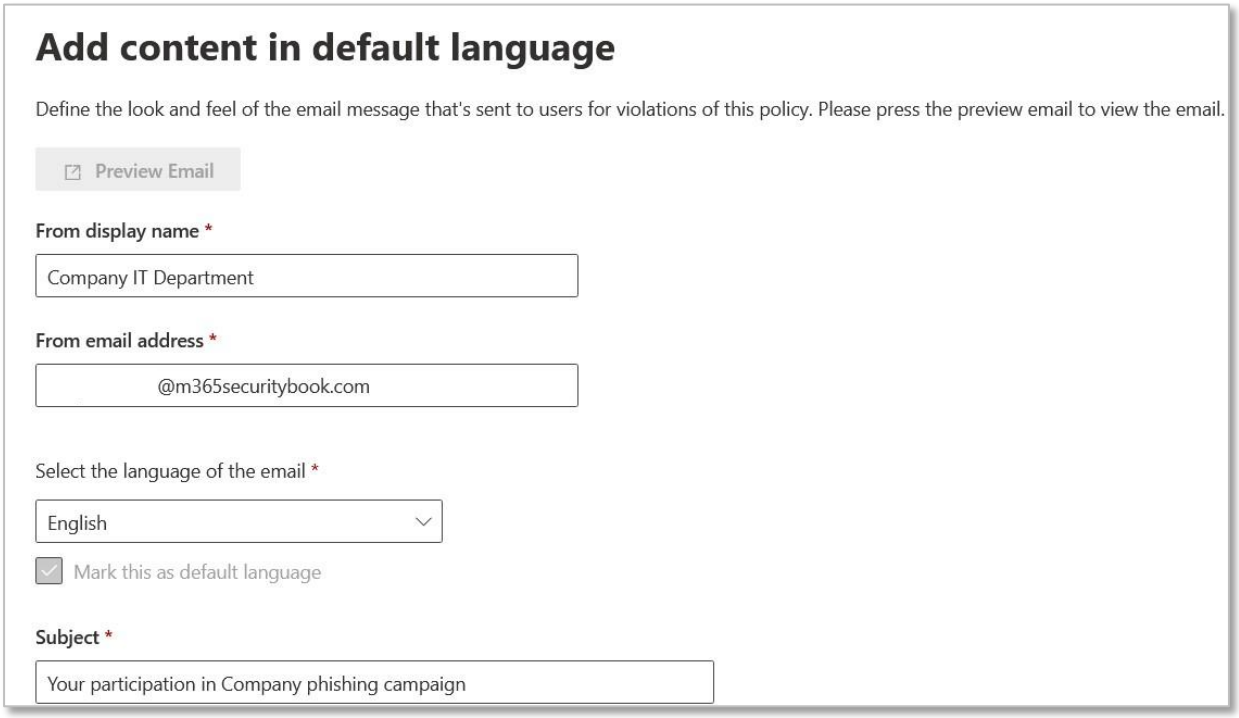


Abbildung 6-94: Hinzufügen von Details zur zu versendenden E-Mail: Wer, E-Mail-Adresse, Sprache und Betreffzeile.

Das ist der Abschnitt, den deine Endbenutzer zu sehen bekommen. Zum Abschluss klickst du auf „Speichern“. Falls du mehrere Sprachen benötigst, kannst du über „Übersetzung hinzufügen“ eine weitere Sprachversion anlegen und dort die entsprechenden Inhalte hinterlegen.

Zusätzlich hast du die Möglichkeit, dynamische Platzhalter zu verwenden, um beispielsweise den Vornamen, Nachnamen, UPN oder die E-Mail-Adresse des Empfängers automatisch einzufügen.

Wenn du mit der Benachrichtigung zufrieden bist, klickst du auf „Weiter“, überprüfst die Details und sendest sie anschließend ab. Die neue Benachrichtigung erscheint dann wie erwartet in der Liste deiner Mandanten-Benachrichtigungen:

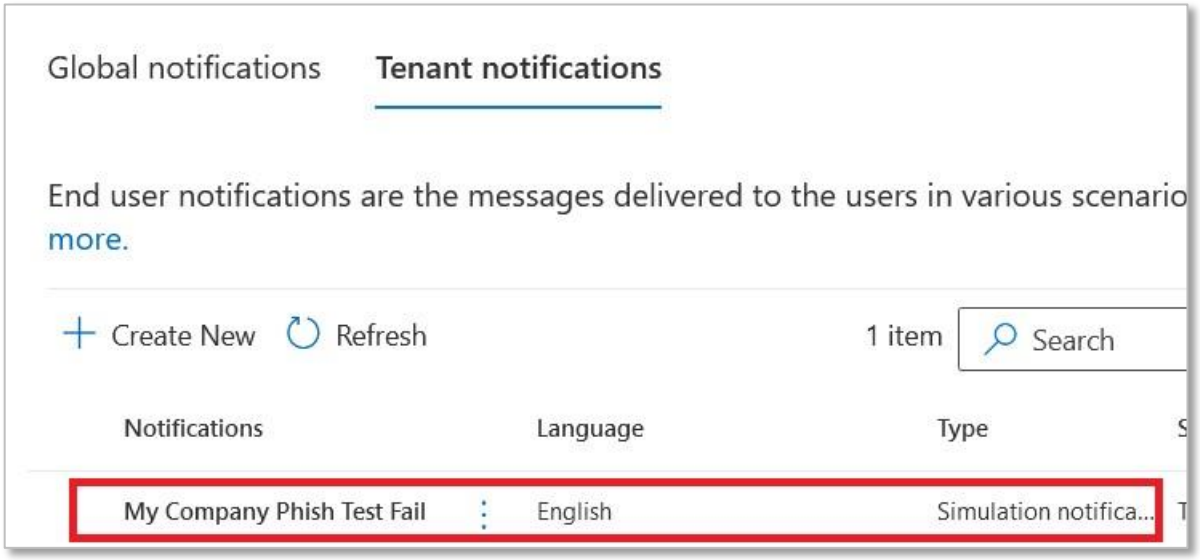


Abbildung 6-95: Deine benutzerdefinierte Mandanten-Endbenachrichtigung

Anwenden der Benachrichtigung auf eine Simulation

Wenn du eine zu verwendende Simulation konfigurierst, kannst du auch die benutzerdefinierten Endbenutzer-Benachrichtigungen auswählen.

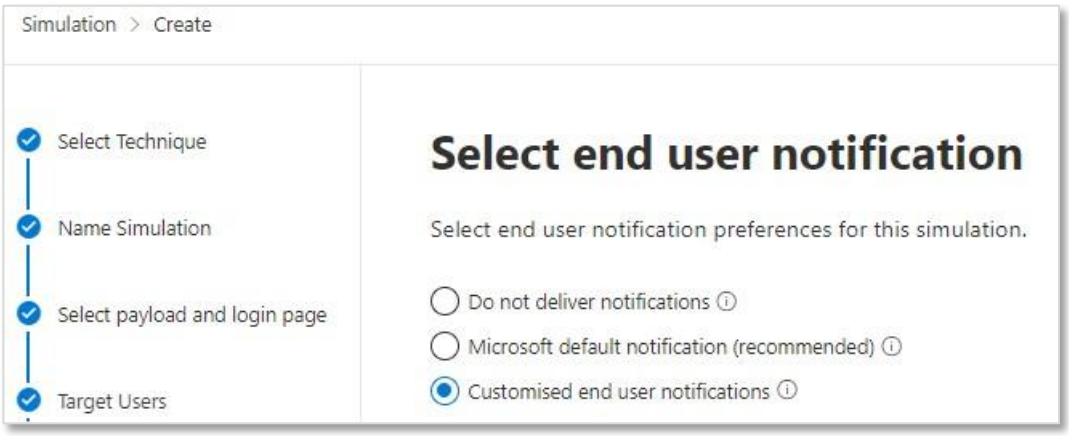


Abbildung 6-96: Wo du eine benutzerdefinierte Benachrichtigung für die Angriffssimulation hinzufügst.

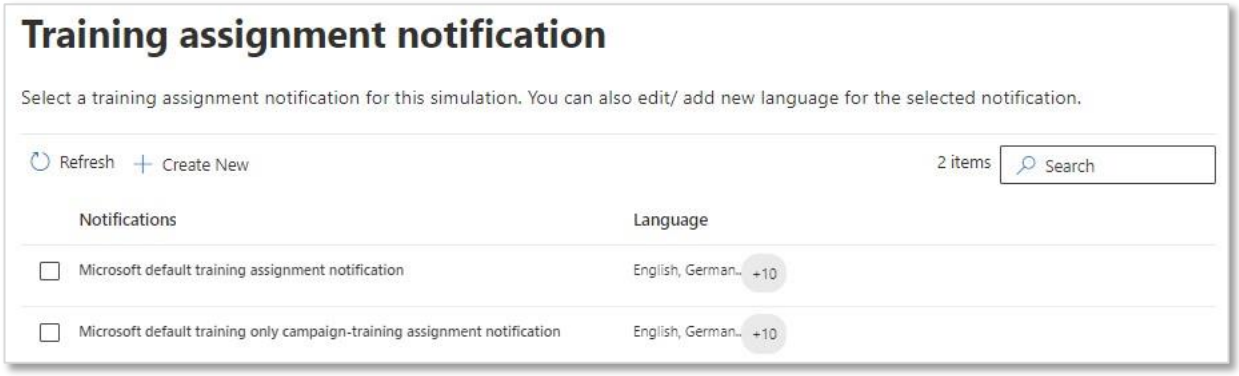


Abbildung 6-97: Schulungs-E-Mail, die an den Endbenutzer gesendet wird, der auf einen Link klickt.

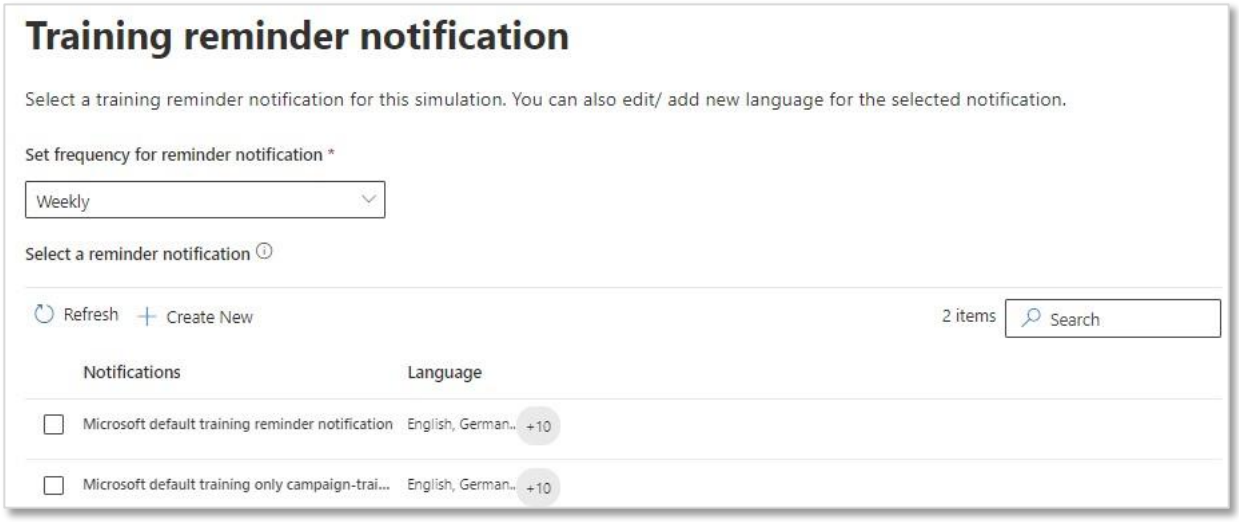


Abbildung 6-98: E-Mail-Erinnerung für erforderliche Schulungen für Angriffssimulation.

Positive Verstärkung

Microsoft hat auch eine standardisierte E-Mail zur positiven Verstärkung hinzugefügt. Damit kannst du Endbenutzern, die eine Nachricht als Phishing melden, eine E-Mail senden, in der ihnen für ihre Aufmerksamkeit gedankt wird. Diese positive Rückmeldung kann entweder über die Standardbenachrichtigung von Microsoft oder über eine selbst erstellte Mandanten-Benachrichtigung erfolgen.

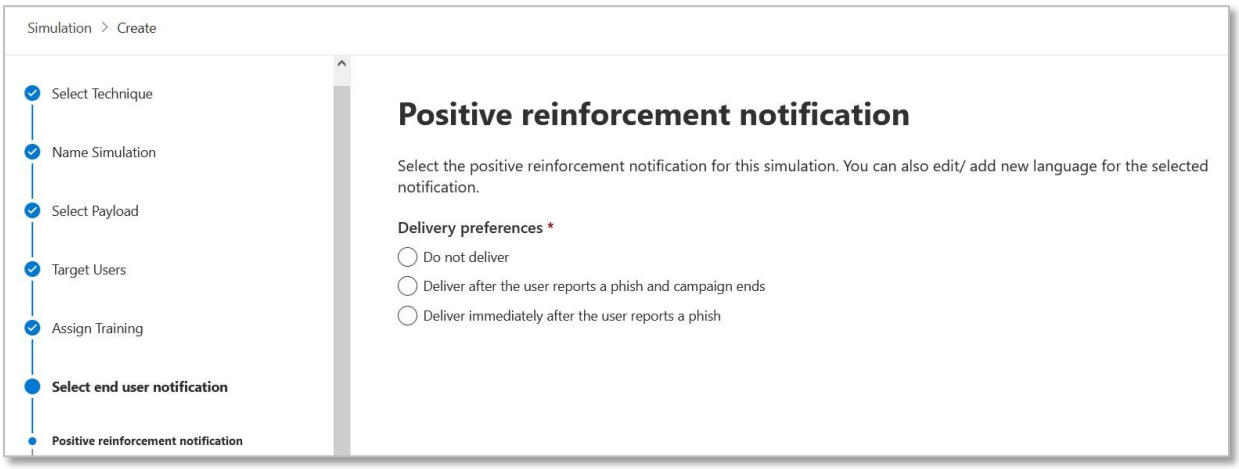


Abbildung 6-99: Wo du eine E-Mail zur positiven Verstärkung für eine Angriffssimulation hinzufügst.

Zielseiten

Neben den neuen Benachrichtigungen hat Microsoft auch das Konzept benutzerdefinierter Zielseiten eingeführt, die du für die Schulung deiner Benutzer nutzen kannst. Eine Zielseite ist die Webseite, auf der der Endbenutzer nach dem Klicken auf eine Nutzlast in einer simulierten Phishing-Mail landet. Du hast hier die Wahl, entweder eine eigene Seite zu erstellen, eine Microsoft-Vorlage zu verwenden oder eine externe benutzerdefinierte Zielseite zu hinterlegen.

Wenn du „Eigene Zielseite erstellen“ auswählst, wird dir ein Editor angezeigt, der dem zum Erstellen der benutzerdefinierten Benachrichtigungen ähnelt.

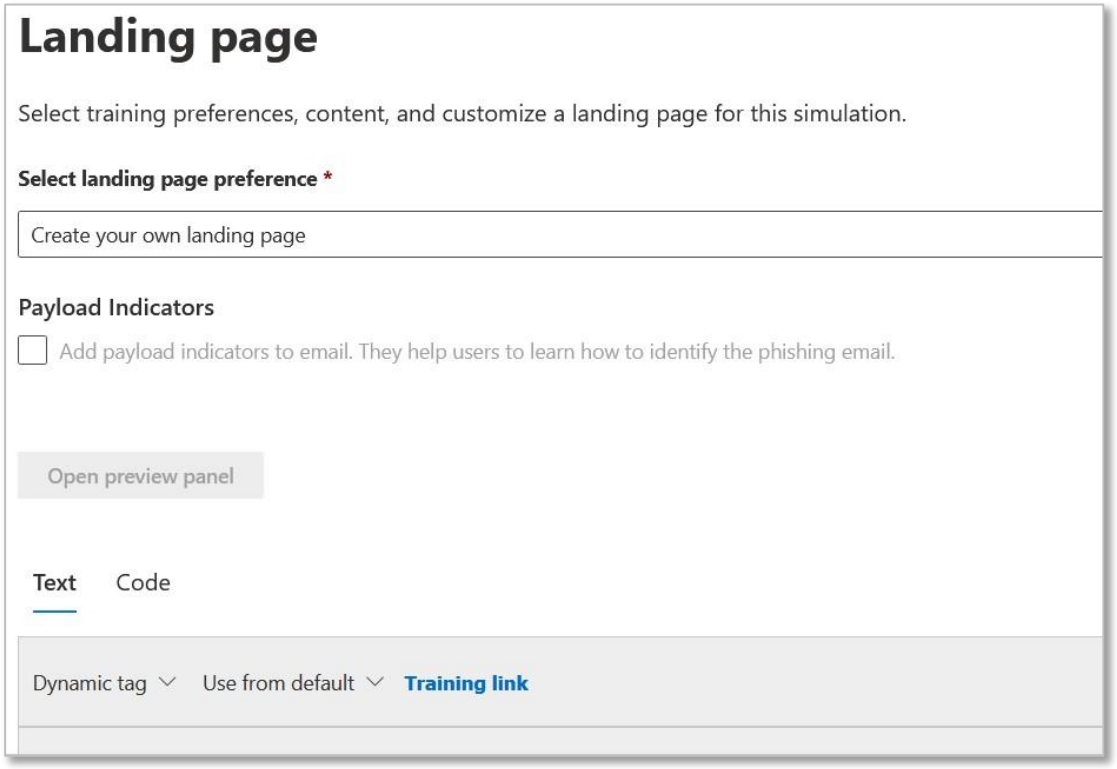


Abbildung 6-100: Benutzerdefinierter Zielseiten-Editor.

Die Standardoption ist die Microsoft-Zielseite, die bisher die einzige Auswahlmöglichkeit war. Du hast jetzt die Möglichkeit, deine eigene Seite mit dem im Assistenten enthaltenen Text-/HTML-Editor zu erstellen. Eine dritte Option besteht darin, „Benutzerdefinierte URL“ auszuwählen. Damit kannst du eine bereits vorhandene Zielseite angeben, die beispielsweise auf einem von deiner Organisation gehosteten Webserver liegt.

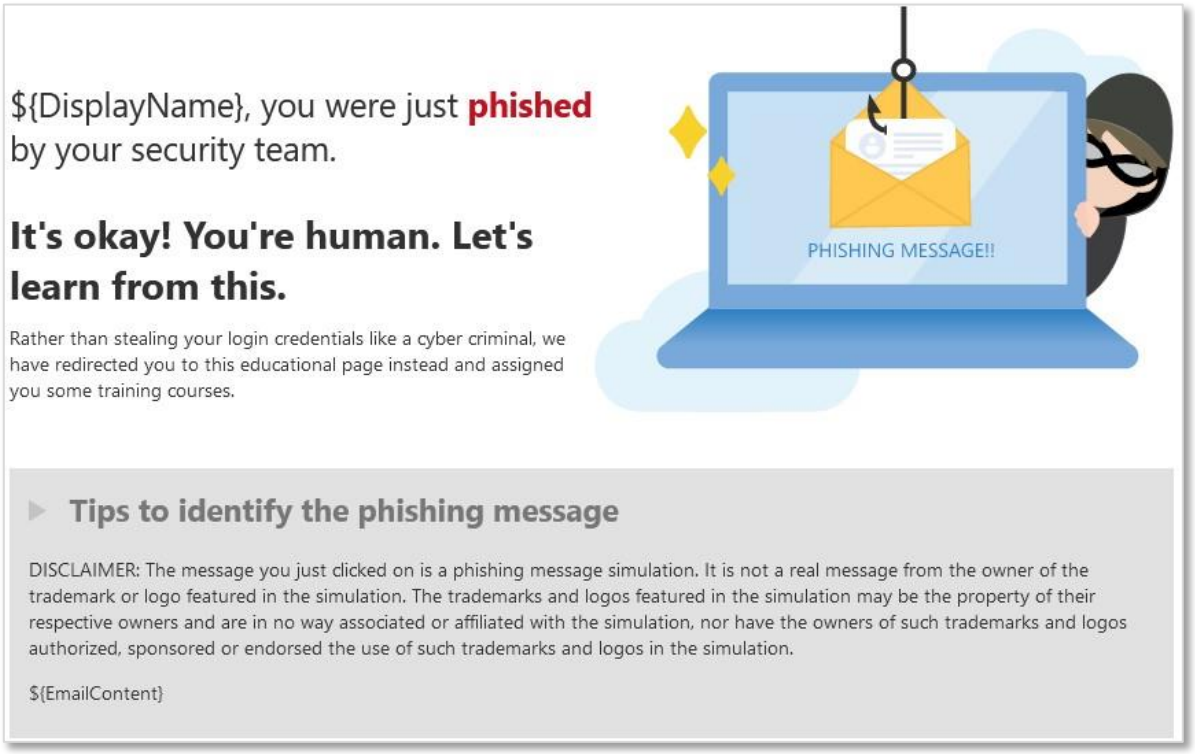


Abbildung 6-101: Zielseite - Microsoft-Vorlage 1.

Der Bedarf an Anpassung hängt von den Anforderungen deiner Organisation ab. Es wird empfohlen, zumindest das Branding anzupassen, damit deine Seiten eindeutig deiner Organisation zugeordnet werden können. Füge unbedingt Kontaktinformationen deiner IT-Abteilung hinzu, damit der Endbenutzer im Zweifelsfall bestätigen kann, was er sieht.

Schulungskampagnen

Bevor Microsoft die zusätzliche Schulungsoption in der Angriffssimulationsfunktion eingeführt hat, erhielten Benutzer nur dann einen Link zu einer Schulung, wenn sie bei einem simulierten Angriff versagt hatten. Jetzt bietet Microsoft Administratoren die Möglichkeit, ihre Benutzer auch präventiv zu schulen – mit einer Vielzahl an Materialien zur Sensibilisierung, bevor überhaupt eine Angriffssimulation durchgeführt wird. Die Idee dahinter ist, dass Benutzer dadurch besser auf simulierte E-Mails und auf echte Phishing-Angriffe vorbereitet sind.

Das Ausführen eines Schulungsszenarios erfolgt über die Registerkarte „Training“ innerhalb der Angriffssimulator-Funktion.

Erstellen einer neuen Schulungskampagne

Wie bei den Angriffssimulationsszenarien musst du auch hier einen eindeutigen Namen und eine aussagekräftige Beschreibung angeben, damit Administratoren später nachvollziehen können, welche Schulung zugewiesen wurde.

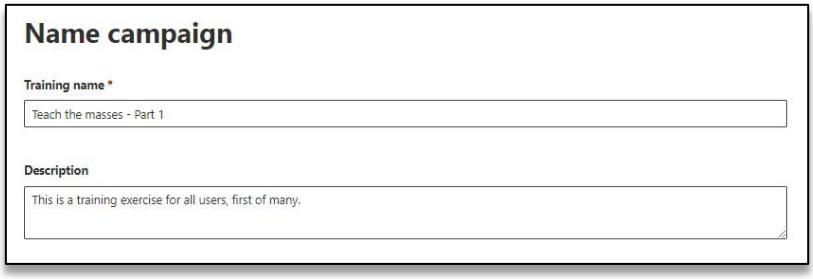


Abbildung 6-102: Gib einen Namen und eine relevante Beschreibung an, auf die später von Administratoren Bezug genommen werden kann.

Als Nächstes überlegst du, wer die Schulung erhalten soll – betrifft es alle Benutzer deiner Organisation oder nur eine bestimmte Abteilung bzw. eine Teilmenge der Benutzer, die besondere Aufmerksamkeit benötigt:

Abbildung 6-103: Benutzer, die Schulungslinks erhalten.

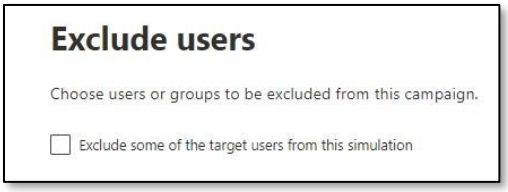


Abbildung 6-104: Endbenutzer vom Erhalt der Schulungslinks ausschließen.

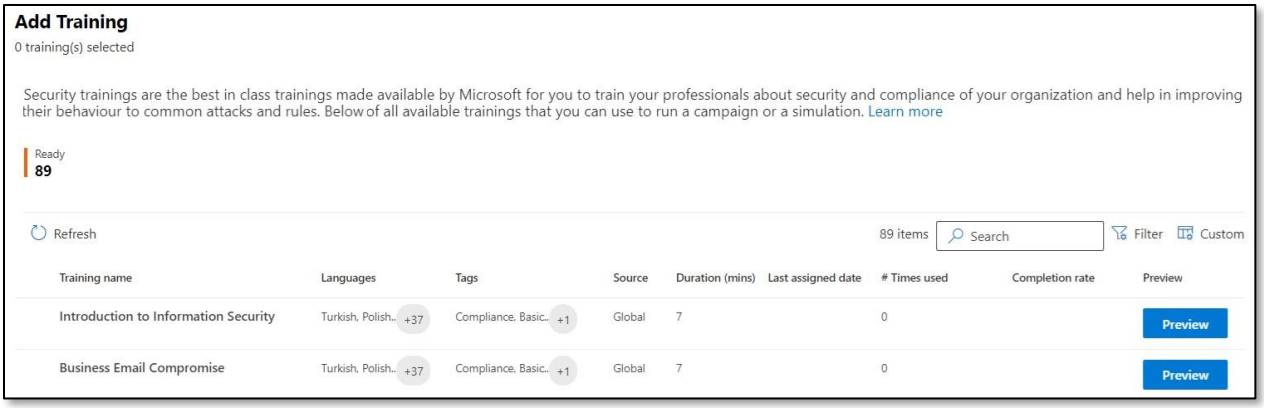


Abbildung 6-105: Wähle eine oder mehrere Schulungen für Endbenutzer aus, wobei bis zu 89 zur Auswahl stehen.

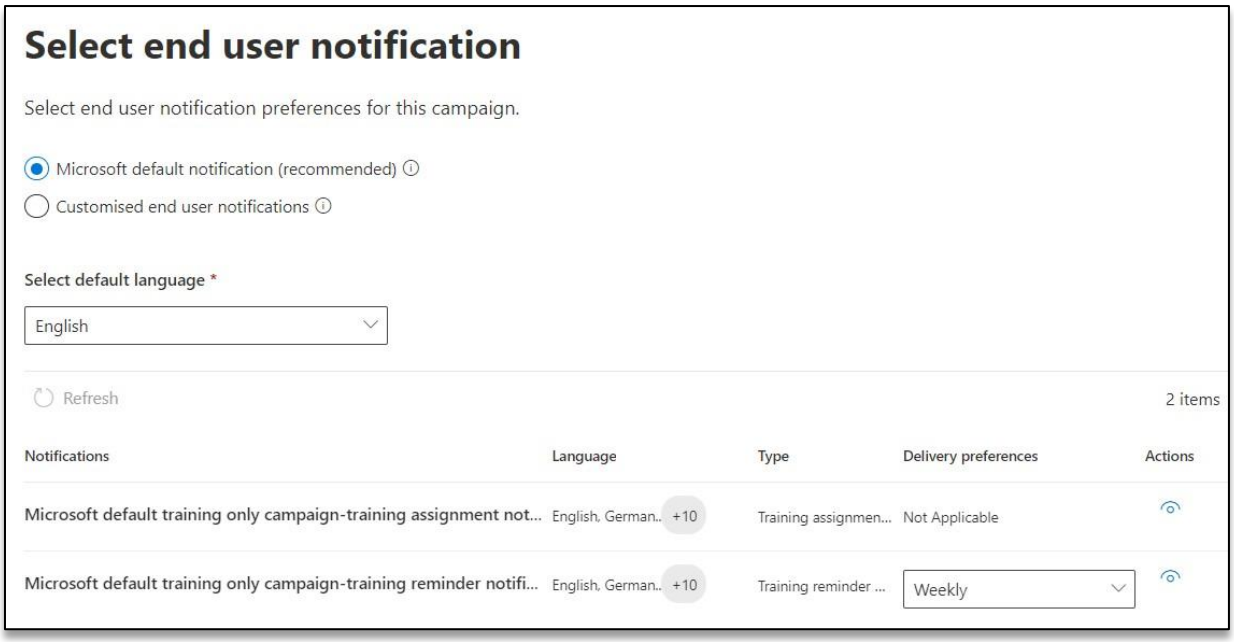


Abbildung 6-106: Entscheide, wie die Empfänger der Schulung Benachrichtigungen erhalten, beachte die verschiedenen Sprachen und die Häufigkeit der Benachrichtigungen.

Abbildung 6-107: Wähle einen Zeitplan und den Zeitpunkt, zu dem die Schulungskampagne gestartet wird.

Erfahrung der Endbenutzer

Sobald die Kampagne startet, erhalten alle in der Kampagne enthaltenen Benutzer eine E-Mail mit Informationen zur zugewiesenen Schulung. Die relevanten Inhalte der Schulung werden direkt in der E-Mail aufgeführt:

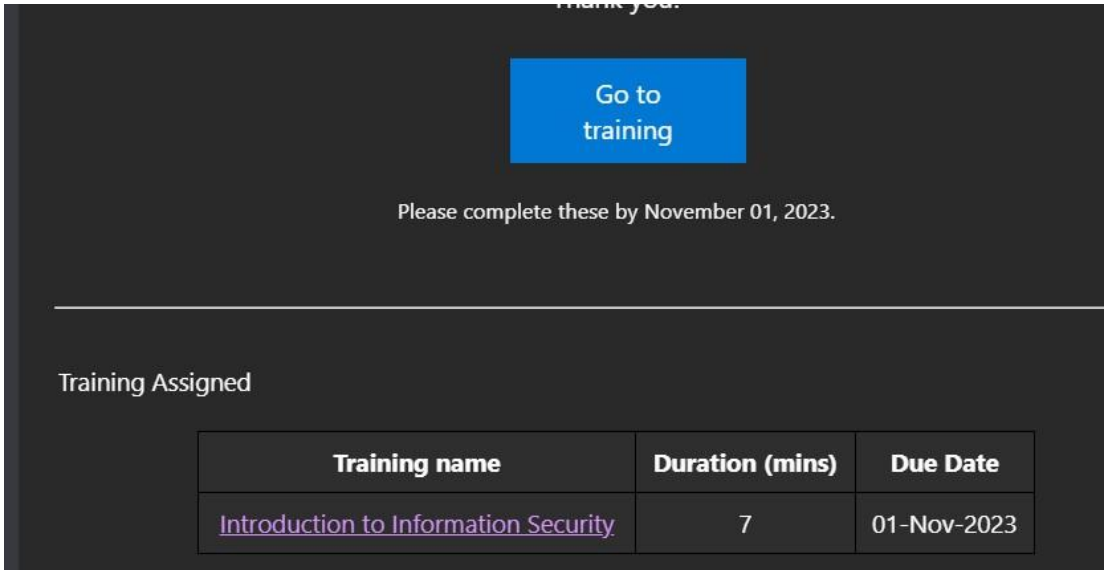


Abbildung 6-108: Hier werden zwei Links bereitgestellt, einer für die gesamte Schulungsliste für den Benutzer und die gerade zugewiesene Schulung für diese Kampagne.

Es ist möglich, mehreren Schulungen innerhalb derselben Kampagne zuzuweisen. Wenn ein Benutzer auf den Link in der E-Mail klickt, wird er direkt zu seiner jeweiligen Schulung weitergeleitet, wie in der folgenden Abbildung dargestellt:

Abbildung 6-109: Beispiel-Schulungs-Landingpage, auf der du den Kurs ansehen oder beenden kannst.

In der E-Mail ist auch ein Link zu allen Schulungszuweisungen enthalten, die ein Benutzer in der Vergangenheit hatte oder noch hat. Ein Klick auf ‘Zur Schulung gehen’ führt zu dieser Seite.

Training Assignments

Refresh 3 items

Title	Description	Total duration (mi...	Status	Assigned Date	Due date
Introduction to Information Sec...	Introduction to Information Security	7	Assigned	10/25/2023, 10:21:07 AM	11/1/2023, 12:00:00 PM
Web Phishing	Web Phishing	3	Overdue	11/14/2022, 7:51:11 PM	11/23/2022, 7:45:30 PM
Mass Market Phishing	Mass Market Phishing	3	Overdue	11/14/2022, 7:50:58 PM	11/23/2022, 7:45:30 PM

Abbildung 6-110: Aktuell einem Benutzer zugewiesene Schulung und ob sie abgeschlossen wurde oder nicht.

QR-Codes

'Das nächste große Ding' für böswillige Akteure sind QR-Codes - und diese Angriffsform hat sich im letzten Jahr deutlich zugenommen. Du siehst QR-Codes sheute überall: auf Postern, in Webinaren und auf Websites. Microsoft holt nun auf, um besser dabei zu helfen, diese Bedrohungen zu identifizieren, Schulungen innerhalb des Attack Simulation Training (Anleitungen) bereitzustellen und QR-Code-basierte Angriffe zu erkennen und darauf zu reagieren

Abbildung 6-111: QR-Code, der dich zu unserer Buchwebsite führt, https://m365securitybook.com/

Empfehlung

Wenn du AST verwendest, stelle sicher, dass du die Schulungsanleitung für QR-Codes an deine Endbenutzer weitergibst.

Allgemeine Empfehlungen

Ziel von Administratoren ist es, Benutzer so zu schulen, dass sie gewissermaßen zu einer E-Mail-Firewall werden, die in Kombination mit der eingesetzten Sicherheitssoftware oder -lösung funktioniert, um vor böswilligen Akteuren zu schützen. Mit den neuen Schulungskampagnen kannst du Benutzer jetzt gezielt schulen und testen – angepasst an die spezifischen Anforderungen deiner Organisation. Diese Kampagnenfunktion sollte ein integraler Bestandteil deiner Schulungs- und Sicherheitsstrategie sein.

Konfigurations-Analyzer

Derzeit bietet Microsoft zwei Möglichkeiten, die Konfiguration von Exchange Online Protection und Microsoft Defender for Office 365 zu analysieren. Die erste Option ist der neue, integrierte Konfigurationsanalysator. Die zweite – und ältere – Möglichkeit ist ORCA, was für Office Recommended Configuration Analyzer steht.

Da beide Optionen ihre Vorzüge haben, werden wir beide besprechen.

Konfigurations-Analyzer (Microsoft 365 Defender)

Das ORCA PowerShell-Modul wurde öffentlich bereitgestellt und war ein äußerst hilfreiches Werkzeug zur Analyse der Office 365 ATP- bzw. E-Mail-Sicherheitskonfiguration. Im Laufe des vergangenen Jahres hat das Modul an Funktionalität und Umfang gewonnen und liefert mittlerweile noch präzisere Empfehlungen. Inzwischen hat Microsoft eine vergleichbare Funktion direkt im Security Center eingeführt: den Konfigurationsanalysator. Auch dieses Tool führt Prüfungen durch und gibt Empfehlungen, ähnlich wie das ORCA-Skript.

Abbildung 6-112: Zugriff auf den Konfigurations-Analyzer über das Security Center.

Es gibt jedoch einige deutliche Unterschiede zwischen ORCA und dem Konfigurationsanalysator – insbesondere in der Art und Weise, wie die Informationen aufbereitet werden. Während ORCA einen detaillierten und portablen HTML-Bericht erstellt, zeigt der

Konfigurationsanalysator eine einfachere Übersicht direkt in der Benutzeroberfläche an. Diese Ansicht ist nicht exportierbar oder portabel, dafür aber interaktiv und erlaubt es dir, Empfehlungen direkt umzusetzen.

Die Benutzeroberfläche selbst bietet eine strukturierte Darstellung und eine übersichtliche Zusammenfassung der gefundenen Probleme:

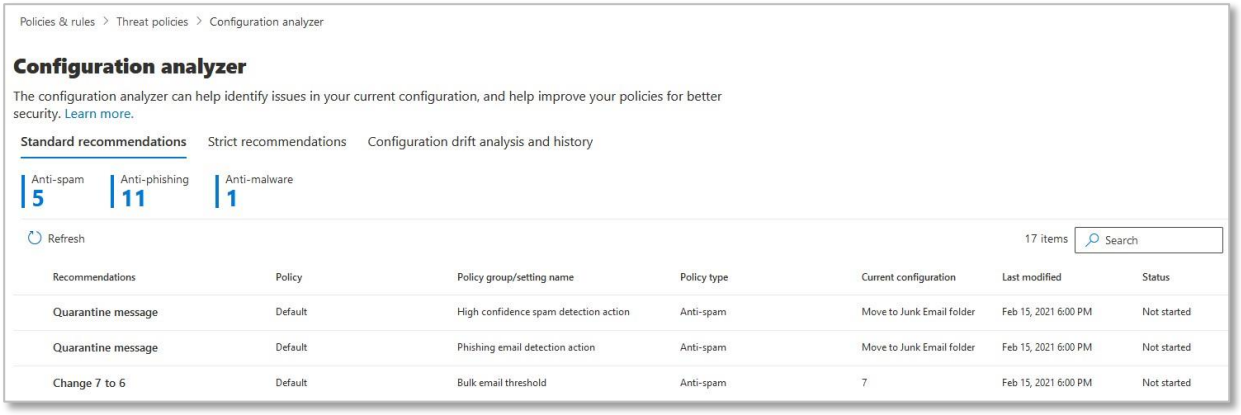


Abbildung 6-113: Übersicht über den Konfigurations-Analyzer

Du findest dort Registerkarten für Standard- und Strikt-Empfehlungen sowie die bestehende Registerkarte zur Konfigurationsabweichung. Statt einzelne Themenbereiche zu öffnen, werden alle Empfehlungen in Listenform angezeigt – ähnlich wie beim Microsoft Secure Score. Der neue Bereich verwendet beschreibende, sortierbare Spalten: Empfehlung, Richtlinie, Richtlinien- oder Einstellungsname, Richtlinientyp, aktueller Status oder Konfiguration. Oberhalb der Liste befindet sich eine Zusammenfassung mit der Anzahl der Empfehlungen, die visuell in Blau hervorgehoben ist.

Wenn du auf einen Eintrag in der Liste klickst, erscheinen derzeit keine weiteren Details. Das ist ein Punkt, der in Zukunft verbessert werden könnte – denn ORCA liefert hier deutlich mehr Kontext, etwa zu betroffenen Domänen oder E-Mail-Adressen.

Ein klarer Vorteil des neuen Konfigurationsanalysators gegenüber ORCA ist jedoch die Möglichkeit, Empfehlungen direkt über einen sogenannten „Easy Button“ umzusetzen.

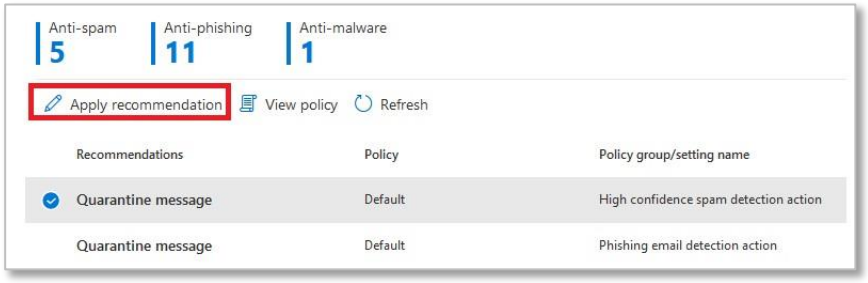


Abbildung 6-114: Übernahme von Empfehlungen aus dem Konfigurations-Analyzer heraus.

Du kannst Änderungen bestätigen oder abbrechen, um unbeabsichtigte Anpassungen zu vermeiden. Beachte, dass bestätigte Änderungen nicht mehr über die Benutzeroberfläche rückgängig gemacht werden können. Eine weitere sehr nützliche Funktion ist die Verfolgung von Änderungen und Konfigurationsabweichungen über die Zeit hinweg. Gehe dazu in der Benutzeroberfläche zur Analyse und zum Verlauf der Konfigurationsabweichungen, wie im nächsten Schritt gezeigt.

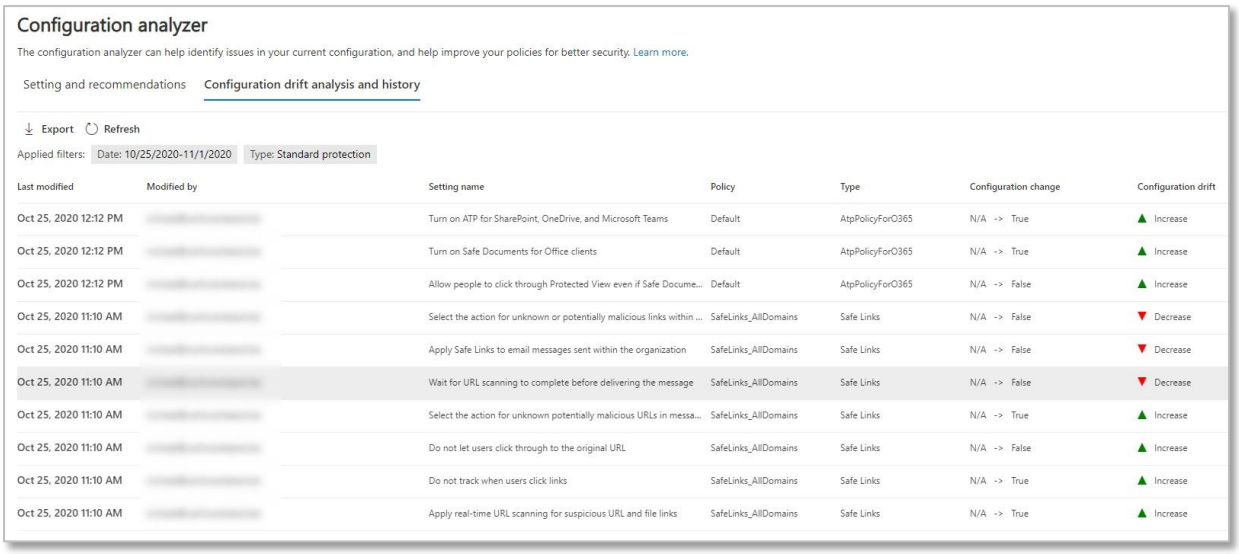


Abbildung 6-115: Nachverfolgung von Konfigurationsabweichungen

In dieser Übersicht siehst du, wer welche Änderung vorgenommen hat, wann sie erfolgt ist und welcher Wert geändert wurde. Außerdem wird der vorherige Konfigurationswert angezeigt und wie sich diese Änderung im Vergleich zur gewählten Baseline auf die Sicherheitslage ausgewirkt hat. Aktuell stehen zwei Baselines zur Verfügung: Standard und Strikt. Beide beziehen sich auf Microsofts empfohlene Konfigurationsrichtlinien.

Berechtigungen: Du kannst den Konfigurationsanalysator aktiv oder passiv (also schreibgeschützt) verwenden. Für die aktive Nutzung, also wenn du Empfehlungen direkt in der Oberfläche umsetzen willst, benötigst du zusätzliche Berechtigungen wie Organization Management, Security Administrator oder Hygiene Management. Für den schreibgeschützen

Modus reichen die Berechtigungen Security Reader oder View-Only Organization Management aus. In diesem Fall kannst du nur lessen, aber keine Maßnahmen durchführen.

Neue voreingestellte Sicherheitsrichtlinie

Microsoft hat im Defender for Office-Portal inzwischen eine vierte Schutzstufe eingeführt. Bisher konntest du zwischen benutzerdefinierten Einstellungen, dem Standardschutz und dem strikten Schutz wählen. Die neue Option nennt sich „Integrierter Schutz“ und greift, wenn keine anderen Schutzkonfigurationen aktiv sind – sie hat also die niedrigste Priorität. Die aktuelle Reihenfolge lautet: Strikt, Standard, Benutzerdefiniert und Integriert. Die jeweils höhere Schutzstufe überschreibt alle darunterliegenden.

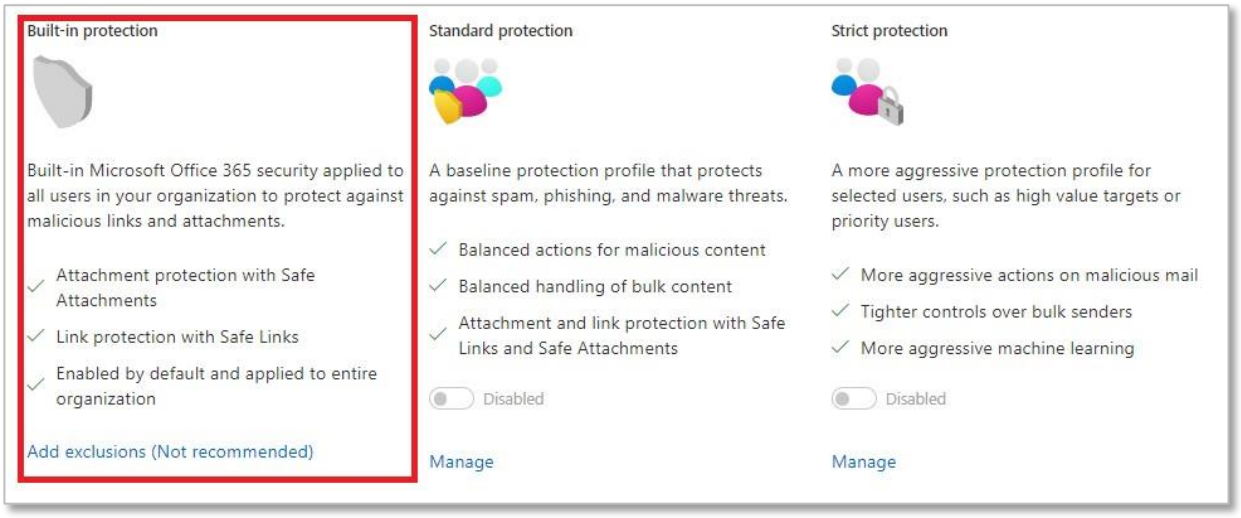


Abbildung 6-116: Neue integrierte Sicherheitsrichtlinie

Im Fall eines neuen Mandanten gelten zunächst die integrierten Schutzeinstellungen, da noch keine anderen Konfigurationen vorhanden sind. Sobald du jedoch den strikten Schutz oder eine benutzerdefinierte Richtlinie aktivierst, werden diese übernommen und der integrierte Schutz außer Kraft gesetzt. Microsoft gibt an, dass die integrierten Schutzmaßnahmen möglichst unauffällig und benutzerfreundlich gestaltet sind. Die allgemeine Empfehlung lautet daher, zunächst mit dem integrierten Schutz zu arbeiten und Ausschlüsse nur bei Bedarf vorzunehmen.

Konfigurationsanalyzer (ORCA)

Microsoft Defender for Office 365 ist ein komplexes Angebot von Microsoft mit vielen beweglichen Teilen und Einstellungen, um deinen Mandanten zu schützen. Diese Komplexität macht es jedoch auch schwierig zu überprüfen, ob dein Mandant korrekt für alle Funktionen konfiguriert ist. Glücklicherweise gibt es ein PowerShell-Skript von Microsoft, das viele dieser

Einstellungen validieren und einen Ausgabebericht erstellen kann, um dich bei notwendigen Änderungen oder Empfehlungen zur aktuellen Konfiguration zu unterstützen.

Das Skript heißt Office 365 ATP Recommended Configuration Analyzer - kurz ORCA - und ist hier zum Herunterladen verfügbar. Sobald du es heruntergeladen hast, kannst du es mit einem Konto ausführen, das über die nötigen Berechtigungen für deinen Mandanten verfügt. Eine Microsoft Defender for Office 365-Lizenz ist nicht zwingend erforderlich, um das Skript auszuführen. Wenn dein Mandant jedoch über diese Lizenz verfügt, wirst du mehr Ergebnisse und Empfehlungen im Bericht sehen.

Vorschau- vs. stabile Versionen

Eine wichtige Sache, die du bei ORCA beachten solltest, ist, dass es zwei verschiedene Versionen des PowerShell-Moduls gibt: eine stabile Version für den produktiven Einsatz und eine Vorschauversion zum Testen. Welche Version du nutzt, liegt ganz bei dir:

- Produktion (stabil) - https://www.powershellgallery.com/packages/ORCA
- Vorschau (Test) - https://www.powershellgallery.com/packages/ORCAPreview

Installieren und Aktualisieren der PowerShell-Module

Wie bei jedem modernen PowerShell-Modul kannst du das Cmdlet Install-Module verwenden, um das Modul auf deinem Computer zu installieren. Verwende ORCA oder ORCAPreview, je nachdem, welche Version du nutzen möchtest:

```
Install-Module -Name ORCA
Install-Module -Name ORCAPreview
```

Das ORCA-Modul stammt aus einem PowerShell-Repository und lässt sich daher einfach aktualisieren. Die Versionen werden regelmäßig erweitert, um neue Funktionen und Fehlerbehebungen zu integrieren. Um dein Modul zu aktualisieren, verwende einfach den folgenden Befehl. Eine praktische Funktion des Moduls ist, dass es bei jedem Start automatisch prüft, ob Updates verfügbar sind, und dich entsprechend informiert, falls es nicht aktuell ist:

```
Update-Module -Name ORCA
Update-Module -Name ORCAPreview
```

Eine gute Funktion des Moduls ist, dass es bei jedem Ausführen nach Updates sucht und etwas Text anzeigt, wenn es nicht auf dem neuesten Stand ist:

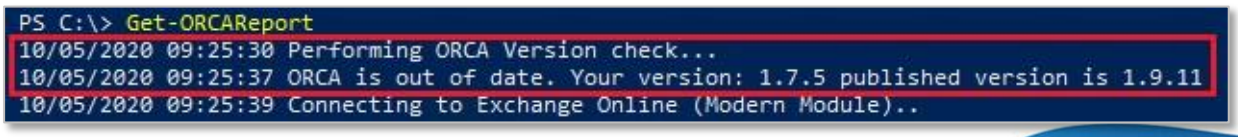


Abbildung 6-117: ORCA-Bericht überprüft auf die neueste Version.

Was prüft ORCA?

ORCA überprüft eine Vielzahl von Einstellungen in Exchange Online Protection und Microsoft Defender for Office 365. Die Prüfung ist sehr umfassend und lohnt sich, regelmäßig durchzuführen – genauso wie das regelmäßige Aktualisieren des Moduls.

Microsoft hat beispielsweise eine Reihe von Parametern für Spamfilterrichtlinien in Exchange Online definiert.

Diese befinden sich im Bereich „Erweitert“ einer Spamfilterrichtlinie. Beispiele für solche Einstellungen sind:

- Bildverknüpfungen zu Remote-Sites
- Leere Nachrichten
- JavaScript oder VBScript in HTML
- Bedingtes Absender-ID-Filtering: Harter Fehler

Früher hatte Microsoft empfohlen, diese Einstellungen nicht zu verwenden, da sie als veraltet galten. Diese Empfehlung hat sich jedoch geändert - Informationen zu dieser Änderung findest du hier. Daher gibt es einen Grund mehr, das Modul stets aktuell zu halten, da es solche Änderungen berücksichtigt.

Alle von ORCA geprüften Elemente in diesem Text aufzulisten, würde wenig Mehrwert bieten. Es genügt zu wissen, dass das Skript viele unterschiedliche Bereiche abdeckt, darunter Richtlinien, Konfigurationen, Domänen und Dienstgrenzen. Weitere Informationen zu ORCA-Tests findest du hier.

Ein Vorteil von ORCA besteht darin, dass es direkt von Microsoft entwickelt wurde und somit auf internes Wissen zurückgreift, welche Einstellungen besonders wirksam sind. Bedeutet das, dass du alles genauso umsetzen musst, wie es der HTML-Bericht empfiehlt? Nein. Du solltest die Empfehlungen prüfen und nur die Änderungen übernehmen, die zu deiner Umgebung passen. Wie so oft gilt: Es gibt keine Einheitslösung für alle. Manche Einstellungen könnten in deinem Szenario zu streng oder zu locker sein.

Wie man ORCA verwendet

Zwischen der stabilen Version und der Vorschauversion gibt es lediglich einen Unterschied: das Cmdlet, das zur Ausführung des Tests verwendet wird. Jedes Modul stellt nur ein einziges Cmdlet bereit. Um den Bericht zu erstellen, verwende den entsprechenden Befehl:

```
Get-ORCAReport
```

Wenn du nicht bei deinem Mandanten angemeldet bist, wirst du zur Anmeldung aufgefordert. Anschließend durchläuft das Skript alle Prüfungen – von Anti-Spam-Einstellungen bis zur DKIM-Konfiguration.Sobald das Skript abgeschlossen ist, öffnet sich eine HTML-Datei mit einem detaillierten Bericht. Dieser enthält Empfehlungen sowie eine Übersicht über die geprüften und als „in Ordnung“ bewerteten Elemente. Durch die Farbcodierung erkennst du schnell, welche Einstellungen korrekt (grün) und welche auffällig (orange) sind. Die Ergebnisse sind nach Kategorien gruppiert und mit Zählern versehen, damit du schnell siehst, wie viele Punkte du eventuell anpassen solltest.

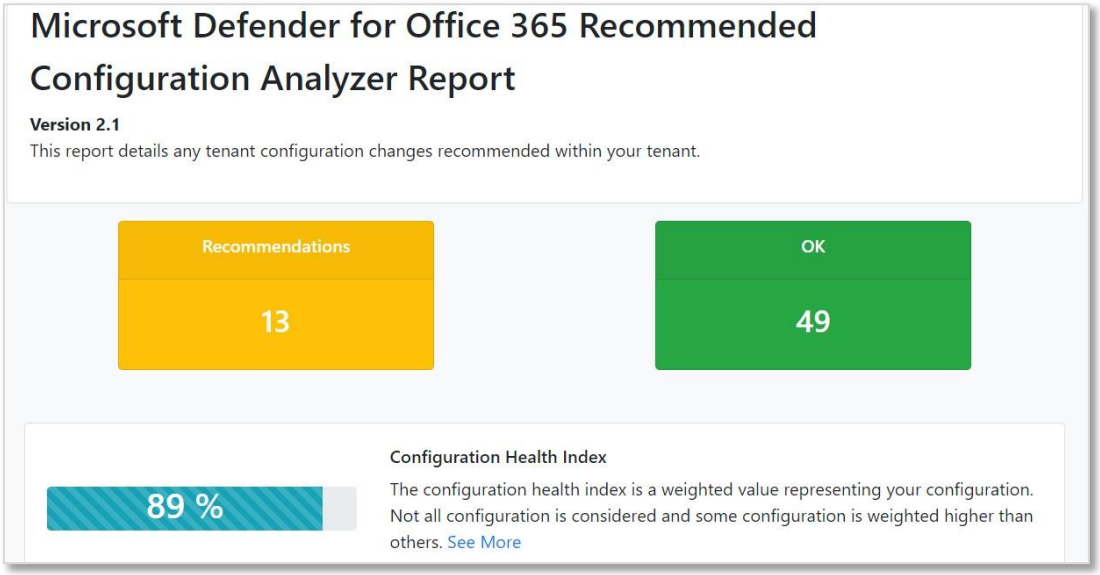


Abbildung 6-118: Zusammenfassung der ORCA-Ergebnisse und Gesundheitsindex insgesamt.

Mit dem aktualisierten Tool hast du immer noch eine Zusammenfassung der zu untersuchenden Probleme:

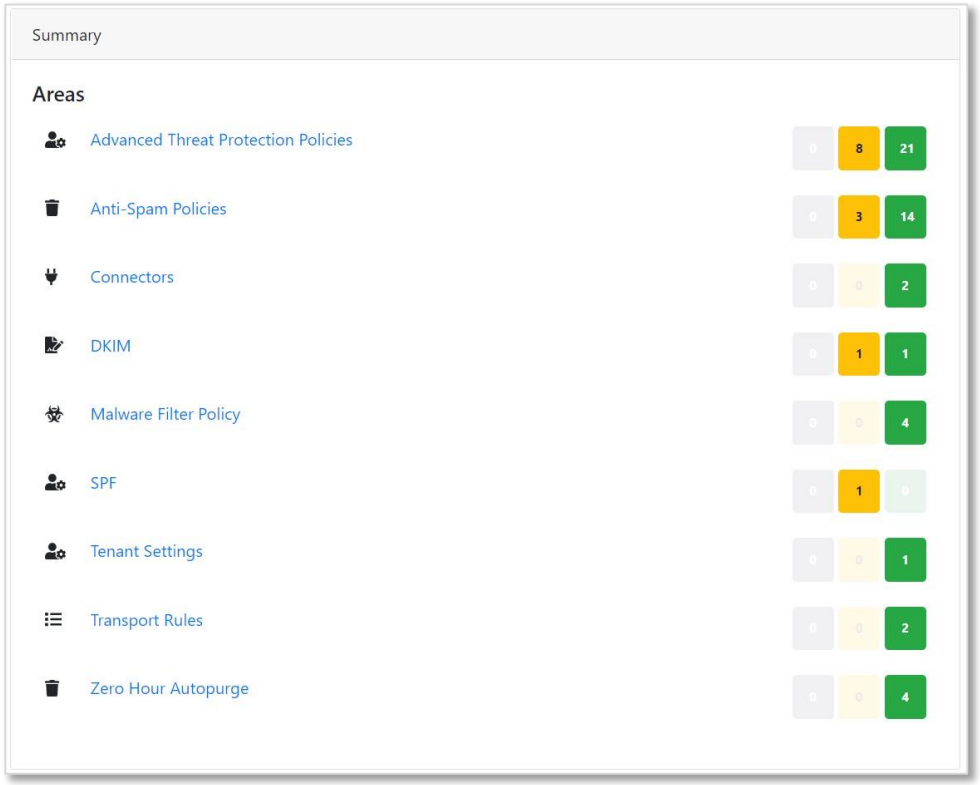


Abbildung 6-119: Gekürzte Ansicht des ORCA HTML-Ausgabeberichts.

Der aktualisierte Bericht enthält weiterhin eine Zusammenfassung aller zu prüfenden Themen. Wie du siehst, werden sowohl die Gesamtanzahl der Empfehlungen als auch die Anzahl der befolgten Best Practices angezeigt. Diese Liste solltest du jedoch mit Vorsicht betrachten. Sie basiert auf allgemeinen Microsoft-Empfehlungen und ist nicht verbindlich. Während viele Punkte sinnvoll und gängig sind, könnten andere nicht den Erwartungen deiner Benutzer entsprechen. Im Bericht findest du außerdem Angaben zur verwendeten ORCA-Version, zum Namen deines Office 365-Mandanten und weitere zusammenfassende Informationen.

Wenn du im Bericht weiter nach unten scrollst, findest du detaillierte Empfehlungen und Hinweise zu umgesetzten Best Practices:

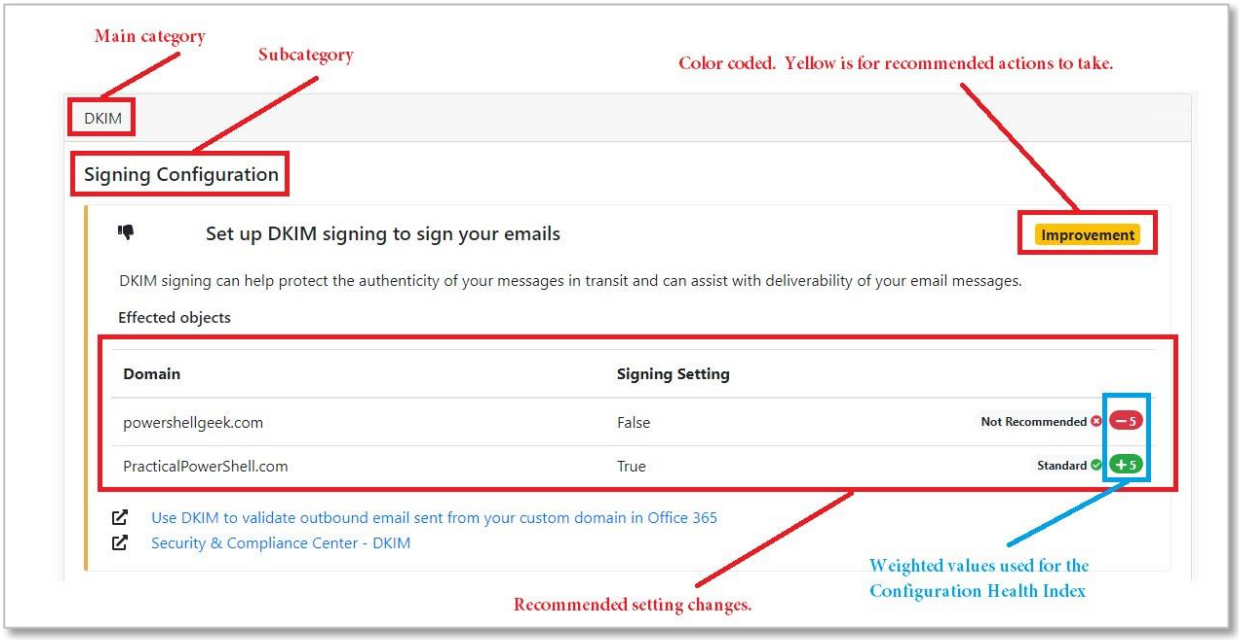


Abbildung 6-120: Beispielelement zur Behebung im HTML-Ausgabebericht.

Beachte die neuen gewichteten Werte aus dem Bild, die berechnet und in den Konfigurationsgesundheitsindex aufgenommen werden.

Beim Durchgehen der Liste wirst du sehen, dass es viele sinnvolle Empfehlungen und Einstellungen für einen Mandanten gibt. Manche davon betreffen veraltete oder nicht mehr unterstützte Konfigurationen. In solchen Fällen weist dich das Tool auf entsprechende Änderungen hin. Im obigen Beispielbericht wurde der Mandant nicht konfiguriert und ausschließlich zu Testzwecken verwendet. Dein eigener Bericht wird entsprechend abweichen und andere Ergebnisse zeigen.

Parameter und Schalter für Get-ORCAReport

Auch wenn das Skript einfach auszuführen ist, gibt es ein paar zusätzliche Parameter, die du beim Start mitgeben kannst. Um dir anzeigen zu lassen, welche Parameter verfügbar sind, gib einfach den Befehl ein und drücke dann **Strg + Leertaste** auf deiner Tastatur.

Für das Get-OrcaReport-Cmdlet verfügbare Parameter.

- **NoConnect**: Nutze diesen Parameter, wenn du bereits mit Exchange Online verbunden bist, um eine erneuete Verbindung zu vermeiden.
- **NoUpdate**: Verhindert, dass das Skript abbricht, wenn es nicht aktuell ist.
- **NoVersionCheck**: Schaltet die Versionsprüfung beim Start ab.
- **AlternateDNS**: Kann andere DNS-Server angeben, anstelle der local konfigurierten.

Evaluierung vom Defender for Office 365

Wenn deine Organisation Microsoft Defender for Office 365 noch nicht nutzt oder du testen möchtest, wie sich strengere Einstellungen auf deine Umgebung auswirken, kannst du jetzt eine neue Funktion verwenden. Im Microsoft 365 Defender-Portal unter **Richtlinien und Regeln > Bedrohungsrichtlinien** findest du die Option, Änderungen vor der Umsetzung zu testen:

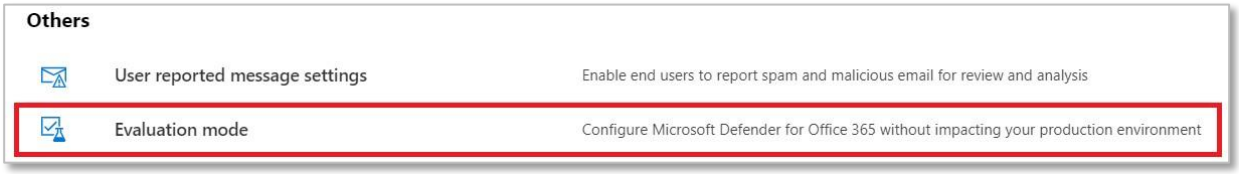


Abbildung 6-122: Microsoft Defender-Konfigurationstest

Nach einem Klick auf die Schaltfläche wirst du durch einen einfachen, szenariobasierten Konfigurationsassistenten geführt:

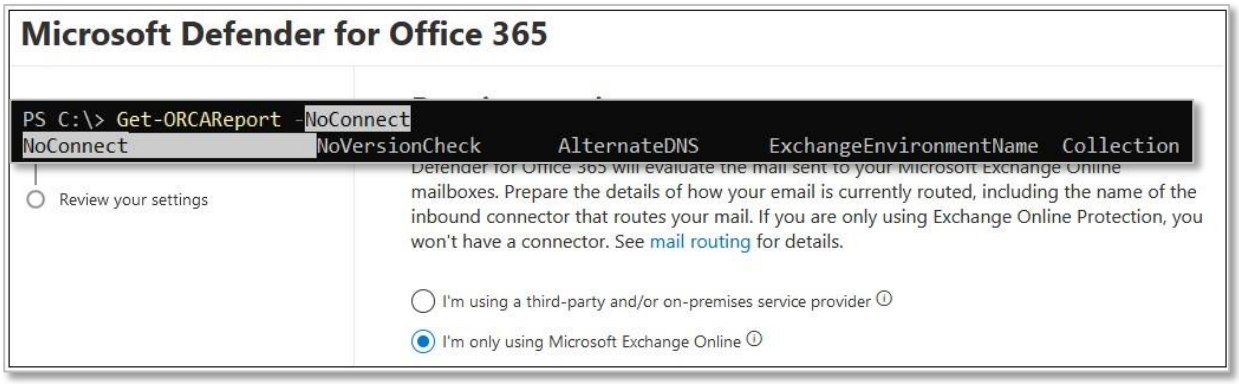


Abbildung 6-123: Auswahl deines Szenarios für die Konfiguration

Triff deine Auswahl, klicke auf „Weiter“ und dann auf „Auswertung erstellen“, um die Analyse zu starten:

Abbildung 6-124: Klicke auf Auswertung erstellen, um das Szenario zu starten.

Beachte, dass diese Funktion derzeit in der öffentlichen Vorschau ist. Wenn sie aktiviert ist, läuft sie etwa 90 Tage lang. Die Daten werden täglich aktualisiert und geben Einblicke darüber, welche Nachrichten blockiert worden wären und aus welchem Grund.

Es findet jedoch keine tatsächliche Blockierung statt.

Diese Berichte helfen dir dabei, 1) die Effektivität von Microsoft Defender for Office 365 zu prüfen und 2) mögliche Auswirkungen auf legitime Nachrichten zu erkennen, bevor du neue Richtlinien aktivierst.

Die Möglichkeit, bestimmte Konfigurationen vor der Umsetzung zu testen, ist besonders hilfreich. Aus meiner Sicht eignet sich diese Funktion vor allem für Organisationen, die Defender for Office 365 noch nicht nutzen, weniger als vollumfänglicher „Was-wäre-wenn“-Modus für bestehende Umgebungen.

Berichterstellung

Nach der Erstellung einer Auswertung wird dir ein Dashboard angezeigt, das die aktuellen Ergebnisse zusammenfasst. Dieses ersetzt den vorherigen Konfigurationsbereich, über den die Auswertung gestartet wurde:

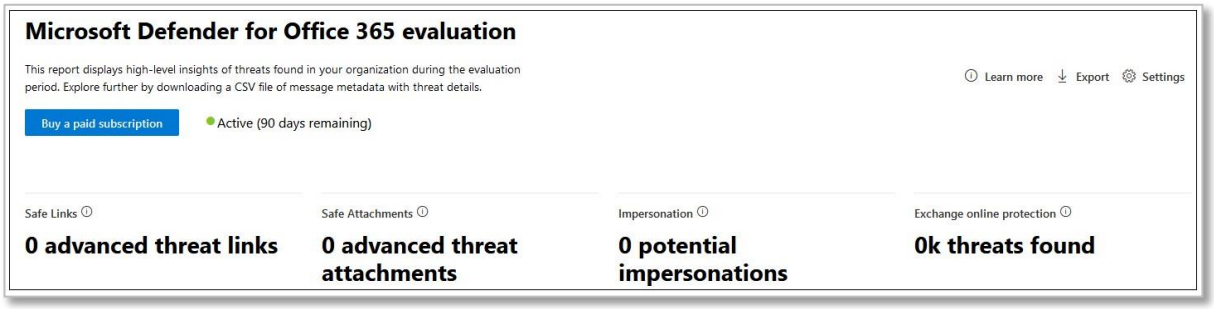


Abbildung 6-125: Microsoft Defender for Office 365 Auswertungs-Dashboard.

Mit fortschreitender Datensammlung zeigt das Dashboard E-Mails an, die durch den Auswertungsmodus erkannt wurden. Es wird entsprechend aktualisiert und stellt dir konkrete Informationen bereit:

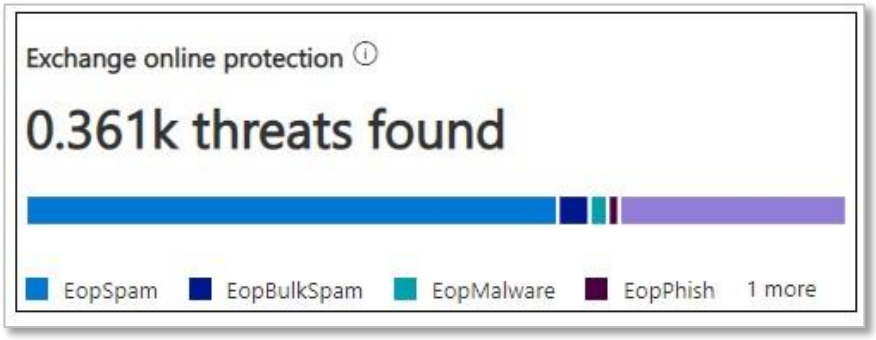


Abbildung 6-126: Microsoft Defender for Office 365 Auswertungs-Dashboard - Live-Daten.

Du kannst auch eine CSV-Datei mit den betroffenen E-Mails anfordern. Klicke dafür einfach auf die Schaltfläche **Exportieren** und warte auf eine E-Mail mit dem Downloadlink:

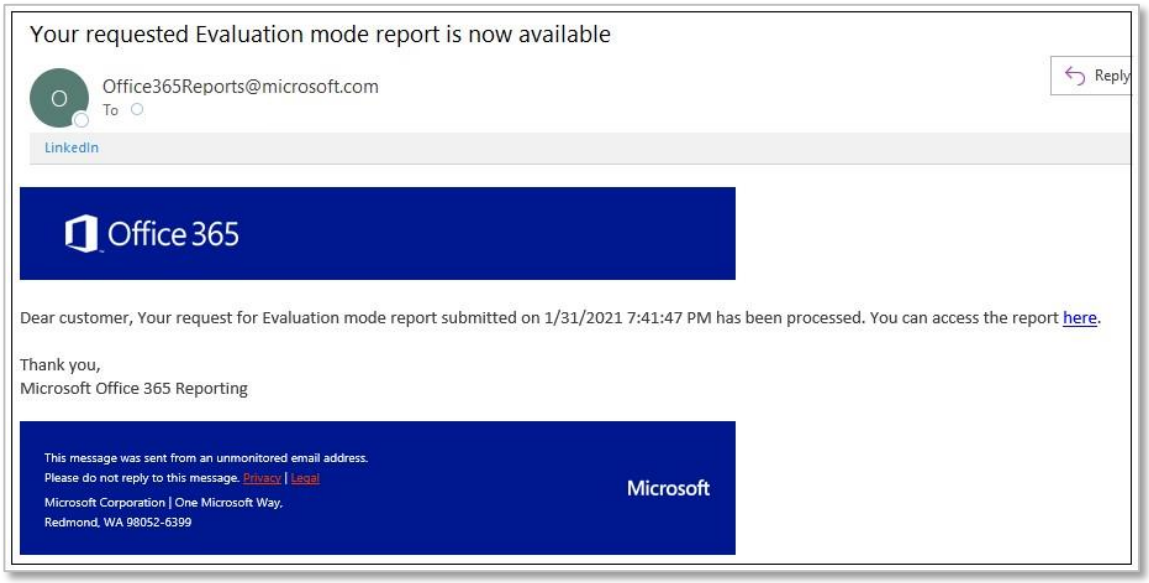


Abbildung 6-127: Microsoft Defender for Office 365 Auswertungsbericht Download-E-Mail.

Nach dem Herunterladen kannst du die CSV-Datei gezielt analysieren. Im Beispiel siehst du einige Spalten, die dir helfen, E-Mails in ihrer Relevanz und Bedrohungseinstufung besser einzuordnen:

A	B	C	D	E	F
Date	Sender	Subject	Recipient	NetworkMessageId	Technology
1/29/2021 21:46	v-bhenmli_icojpgblab_hbfmiejo_hbfmiejo_a@bounce.em.sierratradingpost.com	Beat the cold with epic SAVINGS		7e04e953-3fbe-4659-3387-08d8c49f4a85	Spam
1/29/2021 21:45	bounce-mc.us20_114270466.112030-c3da7ef928@mail87.atl51.rsgsv.net	Nicholas: 2021 Regalia Recommended For You P+		5fa69275-8d2e-4500-ee40-08d8c49f2cfa	Unauthenticated
1/29/2021 20:00	<>	Testing Progress Update		ebbc95b6-c68f-46d1-4459-08d8c4909339	Phish
1/29/2021 13:14	bounce-21974_HTML-272395485-2187066-6240568-636@bounce.email.nationstarmail.com	You may qualify for a lower mortgage payment.		7446914f-a27f-4441-0512-08d8c457c971	Spam
1/28/2021 20:48	heartland@mail198.connectingdonors.org	You make an impact each time you donate blood		43f3abe3-f222-4898-ea9a-08d8c3ce0dab	Spam
1/28/2021 18:06	<>	$10 Off Again!		60310770-c673-4db6-f27e-08d8c3b773d8	Unauthenticated
1/28/2021 14:09	1axb4fdhm4ach3mnjxbgfxrc9nib5vt7duy2jv-nicholas=m365securitybook.com@pgg3jc.cs.hubs	More Testosterone - For Half the Price.		7e5c1282-db96-4a3a-df2d-08d8c3964113	Spam
1/27/2021 22:33	bounce-69181_HTML-217078340-1537560-520000649-5233@bounce.inboxdollarsemail.com	New day + new question = Easy cash		21fcdbea-b835-489f-4692-08d8c313a177	Spam
1/26/2021 21:56	16116858029374773-125541-1-practicalpowershell.com@delivery.mail.sheerseo.com	SEO Analysis for m365securitybook.com		f04d85c7-7fa3-4039-6081-08d8c2453eb6	Spam
1/26/2021 16:08	346ae7fc-e450-11e6-afd8-a45e60e86e11@bounce.r.livingsocial.com	20 Units of Jeuveau + Up to 20% OFF		9cc75347-ecb7-43d1-6cea-08d8c2148c77	Spam
1/26/2021 14:20	v-bheimmo_icojpgblab_hbfijdlg_hbfijdlg_a@bounce.em.sierratradingpost.com	Shoes on shoes on SHOES		f765cdcf-9f9a-4da3-3e83-08d8c2058d43	Spam
1/26/2021 13:05	bounce_hibfobl_o-sarah=m365securitybook.com@cp20.com	Best of the Best from Bell's Best Cookbook		7a953008-5dd3-4b62-a2f3-08d8c1fb02eb	Unauthenticated
1/25/2021 12:26	bounces+6630771-d74f-sarah=m365securitybook.com@sg-email.robinhood.com	"<ÿåß Walmart, Amazon, and the vaccine rollout "		21f3e6b1-52a3-4998-1e0f-08d8c12c7cca	Spam
1/23/2021 15:51	robin.appexpert@aol.com	## Mobile Apps ##		79919b4c-9b43-4edf-4261-08d8bfb6c96e	Spam
1/23/2021 10:01	12140-1153-70844-3277-damianscoles=m365securitybook.com@mail.bemedic.digital	The 3 plants you need to throw in your shopping cart to fight coronavirus		27dd58c4-173c-4be6-7a85-08d8bf85d157	Spam
1/22/2021 16:32	bounce-784_HTML-38252055-38707-514007218-78@bounce.email.vertoeducation.org	COVID-free Spring Semester in Fiji		9d3b5290-afcc-45ce-0bdd-08d8bef3450e	Spam
1/22/2021 14:01	email_feedback_handler@bbcsreturn.convio.net	"Webinar: My ALS Communication Passport to Quality Care, January 29 a		a1313713-9fb3-409a-4e76-08d8bede2cd1	Unauthenticated
1/20/2021 21:09	346ae7fc-e450-11e6-afd8-a45e60e86e11@bounce.r.livingsocial.com	Time for Winter Wellness		ff2fc01f-a3c0-41f5-fbeb-08d8bd8798da	Spam
1/20/2021 12:58	info@pinklouds.com	A shipment from order PS3780 is out for delivery		06c260b2-c591-447d-2a6b-08d8bd4305fe	Phish

Abbildung 6-128: Microsoft Defender for Office 365 Auswertungs-CSV-Datei.

Ganz links findest du die Analyse von Defender, die angibt, ob eine Nachricht als Phishing, Spam, nicht authentifiziert oder anderweitig auffällig eingestuft wurde. Kombiniere diese Info mit dem Absender oder Betreff, um zu bewerten, ob das Ergebnis zutreffend ist. Die Spalte „NetworkMessageID“ kann zur späteren Nachverfolgung oder zur Einleitung einer detaillierten Untersuchung verwendet werden.

Microsoft Defender for Endpoint

Die letzten beiden Kapitel haben sich stark auf Exchange Online, E-Mail und den zusätzlichen Schutz durch Defender for Office 365 konzentriert. Diese Lösungen stellen eine von hoffentlich mehreren Verteidigungsschichten in deiner Umgebung dar. In der Praxis greifen deine Nutzer meist über Endgeräte auf diese Dienste zu. Da der Schutz durch Defender allein nicht verhindert, dass deine Endpunkte Bedrohungen ausgesetzt werden, ist ein zuverlässiger Endpunktschutz unverzichtbar. Wechsle jetzt zum nächsten Kapitel, um zu erfahren, wie dich Microsoft Defender for Endpoint dabei unterstützen kann.