

Cyber Security Awareness

MS365 Whitelisting

Ein MS365-Admin hat vielerlei Möglichkeiten, das Eintreffen von E-Mails sicherzustellen. Da Phishingmails von Microsoft Sicherheitsmechanismen oft bereits als solche erkannt werden, ist das Zulassen unserer Absenderdaten im Kundennetzwerk ein wichtiger Schritt.

Dieses Dokument beinhaltet die folgenden Punkte:

- 1. Quarantäneüberprüfung
- 2. Whitelisting speziell für Phishing-Simulationen (unbedingt nötig)
- 3. Umgehung der Antispoofing-Funktion (neu) (bei Warnmeldungen)
- 4. Whitelisting der Landingpage-Links (falls Defender-Lizenz vorhanden)
- 5. Erstellen einer E-Mail-Fluss-Regel (für Spezialfälle)
- 6. Weitere Möglichkeiten
- 7. Einrichten einer Postfach-Weiterleitung für Network Box
 - 7.1 Client-Weiterleitungsregel erstellen (neu)
 - 7.1.1 Outlook Online
 - 7.1.2 Outlook-App
 - 7.2 Antispam-Ausgangsrichtlinie anpassen
 - 7.3 Einrichtung eines kostenfreien Verteilerpostfachs (alt))

Mit hoher Wahrscheinlichkeit landen viele unserer Vorlagen ohne vorherige Freigaben in der Quarantäne. Dies kann, muss aber nicht immer der Fall sein.

<input type="checkbox"/> Empfangen um	Betreff	Absender	Grund für Quarantäne	Freigabestatus	Richtlinientyp
<input type="checkbox"/> 15. Aug. 2023 14:14:56	Zufriedenheit am Arbeitsplatz	info@gfm.de	Nachricht mit hoher Phishingwahrscheinlichkeit	Überprüfung erforderlich	Antispamrichtlinie
<input type="checkbox"/> 15. Aug. 2023 14:10:17	Zufriedenheit am Arbeitsplatz	info@gfm.de	Nachricht mit hoher Phishingwahrscheinlichkeit	Überprüfung erforderlich	Antispamrichtlinie
<input type="checkbox"/> 15. Aug. 2023 13:09:27	Zufriedenheit am Arbeitsplatz	info@gfm.de	Nachricht mit hoher Phishingwahrscheinlichkeit	Überprüfung erforderlich	Antispamrichtlinie

Quarantänebeispiel

Bitte beachten Sie, dass diese Hinweise nur für ein Whitelisting von MS365 gelten. Sollte eine Firewall oder eine UTM beim Empfang involviert sein, müssten dort ggfs. ebenfalls Freigaben erfolgen.

Cyber Security Awareness

MS365 Whitelisting

Stand 05/2024

1. Quarantäneüberprüfung

E-Mails, die in der Quarantäne gelandet sind, kann man mit den entsprechenden Rechten an folgendem Ort einsehen:

<https://security.microsoft.com/quarantine>

Wir geben bei unserem Testversand - die vor der eigentlichen Simulation in aller Regel mind. einmal stattfindet - immer eine Versandzeit mit an, so dass unsere E-Mails leichter auffindbar sind, sollten diese in die Quarantäne gelandet sein.

E-Mail-Details	
Absenderadresse	SMTP-Mail von Adresse
info@gfm.de	info-gfm@status-monitor.info

Da sich aus Verschleierungsgründen die angezeigte Absenderadresse von der tatsächlich genutzten unterscheiden kann, ist **eine Phishingmail in der Quarantäneliste evtl. nicht direkt als solche zu erkennen**. Vor allem bei CEO-Frauds oder anderen Spear-Phishing-Methoden könnten diese auch wie eigentlich bekannte Absender aussehen.

Sollten die Phishingmails in der Quarantäne zu finden sein, beachten Sie bitte Kapitel 2.

Um den Grund herauszufinden, warum unsere Phishing-Mails in der Quarantäne landen, helfen uns folgende Infos, die Sie den Details entnehmen können, indem Sie einfach auf die jeweilige E-Mail im Quarantänebereich klicken:

Zustellungsdetails		E-Mail-Details	
Ursprüngliche Bedrohungen	Neueste Bedrohungen	Anzeigenname des Absenders	Absenderadresse
Phishing / Hoch	Phishing / Hoch	Hausverwaltung	facilitymanagement@f-service.net
Originalspeicherort	Letzter Übermittlungsort	Absender-E-Mail von Adresse	Gesendet im Auftrag von
Quarantäne	Quarantäne	facilitymanagement@emaildigital.de	-
Zustellaktion	Erkennungstechnologien	Rücksendepfad	Absender-IP
Blockiert	URL-Detonation, Externe Domäne spoofen	facilitymanagement@emaildigital.de	62.113.223.254
Primäre Außerkraftsetzung : Quelle			
Keine			

Wenn unsere Phishingversuche weder im Quarantäneordner noch in den Postfächern landen, werden sie entweder an **anderer Stelle geblockt** (z. B. Firewall) oder sie werden von MS365 direkt verworfen.

Zweiteres wäre allerdings eine nichtstandardmäßige Einstellung, bei der die im folgenden Kapitel dargestellten Whitelisting-Einträge ebenfalls zum Erfolg führen können.

Cyber Security Awareness

MS365 Whitelisting

2. Whitelisting speziell für Phishing-Simulationen



Unter <https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation> können im **MS365 Defender** mittlerweile reguläre Phishing-Simulationen durchgeführt werden. Dazu nötig sind mindestens der Eintrag **einer Absender-IP UND einer Absender-Domain**. Diese werden dann bei Empfang abgeglichen und stellen sicher, dass es sich hier wirklich um gewolltes Phishing handelt.

Richtlinien und Regeln > Bedrohungsrichtlinien > Erweiterte Zustellung

Erweiterte Zustellung

Konfigurieren Sie IP-Adressen, Absenderdomänen und URLs, die als Teil Ihrer Phishingsimulations-E-Mails verwendet werden sollen.

SecOps-Postfach Phishing-Simulation

 Bearbeiten  Aktualisieren

Wert	Typ
62.113.223.254	Sending IP
emaildigital.de	Domain
status-monitor.info	Domain
pstatistics.nb-awareness.eu/*	Allowed Simulation URL

Falls hier noch keine Daten hinterlegt sind, können Sie diese „Hinzufügen“. Maximal sind 30 Einträge möglich.

Hier einmal in Kürze die einzutragenden Werte für die Durchführung einer Phishing-Simulation mit Network Box:

Sending IP = 62.113.223.254

Domain = emaildigital.de or status-monitor.info

Allowed Simulation URL = pstatistics.nb-awareness.eu/*

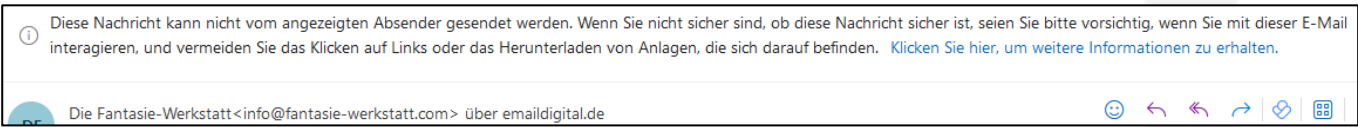
Nach dem Eintragen und Speichern sollten die Werte wie oben angezeigt auftauchen und wir könnten einen Test durchführen.

Achtung! Falls die E-Mails vor Eintreffen im Exchange365 schon geprüft werden, z. B. durch einen Mdaemon oder eine Hornet, kann es sein, dass die Sending IP dort überschrieben wird. Mit welcher Sending IP eine E-Mail am Exchange365 eintrifft, können Sie in der Quarantäne auslesen. (siehe 1.) Die neue IP müsste ggfs. ebenfalls hier eingetragen werden.

Sollte diese Einstellung die Phishingmails noch immer nicht durchlassen bzw. die Phishingmails als bspw. „Spam“ markiert werden, fahren Sie bitte mit Kapitel 3 fort.

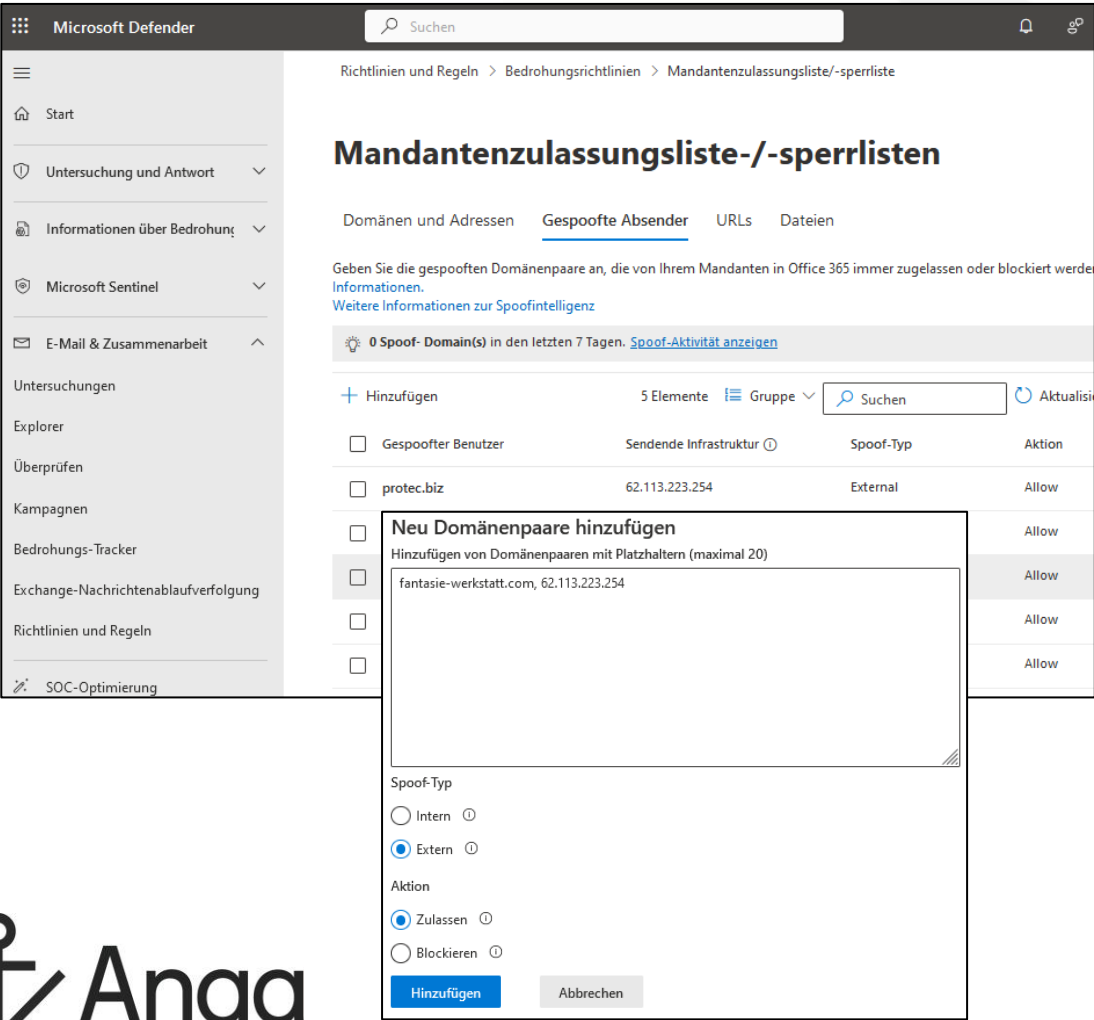
3. Umgehen der Antispoofing-Funktion

Ebenfalls im **Defender365** unter *E-Mail & Zusammenarbeit > Richtlinien und Regeln > Mandantenzulassungsliste/-sperrlisten* findet sich der Punkt *Gespooft Absender*. Einträge in diese Liste sollen vermeiden, dass nach erfolgreicher Zustellung Warnmeldungen zur Mail und die tatsächliche Absendedomain im Postfach der Teilnehmer zu sehen sind. Diese Warnmeldungen treten gehäuft seit der Einführung des neuen Outlook auf.



Um für unsere gespooft Adresse einen Eintrag zu setzen, muss ein Paar bestehend aus der **Domain**, wie Sie beim Empfänger angezeigt werden soll, und unserer **Versand-IP 62.113.223.254** gesetzt werden. Danach sollte beim nächsten Versand sowohl die 2. Warnmeldung als auch das „über emaildigital.de“ in der Adresszeile verschwinden. (Beachten Sie bitte, dass die IP durch eine Hornet oder andere Contentfilter bspw. überschrieben werden kann. In solchen Fällen kontaktieren Sie uns gern direkt

Eine Liste mit sämtlichen gespooften Absenderadressen zu unseren Portfoliovorlagen stellen wir Ihnen auf Anfrage gern zur Verfügung.



Cyber Security Awareness

MS365 Whitelisting

4. Whitelisting der Landing-Page-Links

Wie in Kapitel 2 kann im Defender unter <https://security.microsoft.com/safelinks> unsere Landing-Page auf die Whitelist gesetzt werden.

(Sollte die Seite leer bleiben, gehen Sie bitte, sicher, dass Sie mit dem korrekten Admin-Account bei MS365 im Defender/Admin-Bereich angemeldet sind. Bei Verwendung von mehreren Accounts gleichzeitig kann es zu Verwechslungen kommen. Haben Sie eine MS365-Lizenz ohne Defender gebucht, ist die Safe-Link-Option nicht verfügbar, sollte aber auch nicht blockiert werden.)

Nun erstellen wir eine neue Policy.

Richtlinien und Regeln > Bedrohungsrichtlinien > Sichere Links

Sichere Links

Sichere Links helfen dabei, Ihre Benutzer daran zu hindern, Links in E-Mails und Dokumenten zu folgen, die Ihrer Organisation mit sicheren Links einzurichten. [Weitere Informationen über sichere Links](#)

+ Erstellen ↓ Exportieren ↻ Aktualisieren

☐ Name

☐ Standard Preset Security Policy

Ihre Richtlinie benennen

Fügen Sie einen Namen und eine Beschreibung für Ihre Richtlinie für sichere Links hinzu.

Name *

Network-Box Phishing Landingpage WL

Beschreibung

Whitelisting der Landing-Page bei Phishing-Simulationen der Firma Network-Box.

Benutzer und Domänen

Fügen Sie Benutzer, Gruppen und Domänen hinzu, die

Diese Benutzer, Gruppen und Domänen einschließen *

Benutzer

Und

Gruppen

Und

Domänen

NetworkBoxTest.onmicrosoft.com ✕

☐ Diese Benutzer, Gruppen und Domänen ausschließen

Danach beliebigen
Namen wählen.

Anschließend **Ihre eigene
Empfängerdomäne** hinzufügen.
Diese muss danach unter dem
Textfeld sichtbar sein.

Dann **Weiter**.

Cyber Security Awareness

MS365 Whitelisting

4. Whitelisting der Landing-Page-Links

Die Häkchen wie im Bild setzen bzw. entfernen.

Danach **0-URLs verwalten** anklicken und die URL https://pstatistics.nb-awareness.eu/* inkl. Stern am Ende hinzufügen.

URL- & Klick-Schutzeinstellungen

Legen Sie die URL für sichere Kinks fest, und klicken Sie für diese Richtlinie auf „Schutzeinstellungen“. [Weitere Informationen.](#)

E-Mail

- ☒ Ein: „Sichere Links“ überprüft eine Liste bekannter, bösartiger Links, wenn Benutzer auf Links in E-Mails klicken. URLs werden standardmäßig umgeschrieben.
- ☐ Wenden Sie „Sichere Links“ auf E-Mail-Nachrichten an, die innerhalb der Organisation gesendet werden
- ☐ Echtzeit-URL-Prüfung für verdächtige Links und Links, die auf Dateien verweisen, anwenden
- ☐ Vor dem Zustellen der Nachricht auf den Abschluss der URL-Prüfung warten.
- ☐ URLs nicht umschreiben, nur über Safe Links API überprüfen.

Überschreiben Sie die folgenden URLs nicht in E-Mails (0)

0-URLs verwalten

Teams

- ☐ Ein: „Sichere Links“ überprüft eine Liste bekannter, bösartiger Links, wenn Benutzer auf Links in Microsoft Teams klicken. URLs werden nicht umgeschrieben.

Office 365-Apps

- ☐ Ein: „Sichere Links“ überprüft eine Liste bekannter, bösartiger Links, wenn Benutzer auf Links in Microsoft Office-Apps klicken. URLs werden nicht umgeschrieben.

Klick-Schutzeinstellungen

- ☒ Benutzerklicks verfolgen
- ☒ Erlauben, dass sich Benutzer zur ursprünglichen URL zurückklicken
- ☐ Das Branding der Organisation auf Benachrichtigungen anwenden

URLs hinzufügen

Geben Sie eine URL ein, und klicken Sie dann auf „**Speichern**“, um die Änderungen anzuwenden.

URL

Benutzerdefinierte URL eingeben

https://pstatistics.nb-awareness.eu/* ✕

URLs verwalten, die nicht neu geschrieben werden sollen

Folgende URLs nicht mit sicheren Links neu schreiben:

+ URLs hinzufügen 1 Element ⋮

URLs
https://pstatistics.nb-awareness.eu/*

Die Standardbenachrichtigungen können danach aktiviert bleiben.

Sobald diese Richtlinie gespeichert wurde, wird sie aktiviert.

Cyber Security Awareness

MS365 Whitelisting

5. Erstellen einer E-Mail-Fluss-Regel (Teil 1)

Unter <https://admin.exchange.microsoft.com/#/transportrules> kann eine neue Transportregel eingefügt werden, um die Sortierung in den Junk-Ordner bzw. eine Spam-Markierung zu umgehen.

Erstellen Sie nach folgender Vorlage eine Regel, in der die **SCL-Bewertung** für die Domains *emailedigital.de* und *status-monitor.info* auf **,-1'** oder **,'Bypass Spam Filtering'** o.ä. festgelegt wird. Die Bilder stellen die derzeitige Einrichtungsweise dar.

Cyber Security Awareness

MS365 Whitelisting

5. Erstellen einer E-Mail-Fluss-Regel (Teil 2)

Regeleinstellungen festlegen

Einstellungen für Ihre Transportregel festlegen

Regelmodus

☒ Erzwingen

☐ Test mit Richtlinienipps

☐ Test ohne Richtlinienipps

Schweregrad *

Nicht angegeben

☐ Die Regel aktivieren am

8/15/2023 - 3:30 PM

☐ Die Regel deaktivieren am

8/15/2023 - 3:30 PM

☒ Verarbeiten weiterer Regeln beenden

☐ Nachricht zurückstellen, wenn die Regelverarbeitung nicht abgeschlossen wird

Absenderadresse in Nachricht abgleichen *

Kopfzeile oder Umschlag

Kommentare

Zurück Weiter

Beachten Sie bitte, das Häkchen **Verarbeiten weiterer Regeln beenden** zu setzen und **Kopfzeile oder Umschlag** für den Abgleich mit der Absenderadresse zu aktivieren.

5. Erstellen einer E-Mail-Fluss-Regel (Teil 3)

Neue Transportregel

✓ Regelbedingungen festlegen

✓ Regeleinstellungen festlegen

● Überprüfen und fertigstellen

Überprüfen und fertigstellen

Nachdem Sie diese Regel erstellt haben, wird sie standardmäßig deaktiviert, bis Sie sie auf der Seite "Regeln" aktivieren.

Regelname

NP_Phishing_Domains

Regelkommentare

Regelbedingungen

Diese Regel anwenden, wenn
Die Absenderdomäne ist 'emaidigital.de' or 'status-monitor.info'
Gehen Sie wie folgt vor:
SCL-Bewertung (Spam Confidence Level) festlegen '-1'
Außer wenn
[Regelbedingungen bearbeiten](#)

Regeleinstellungen

Modus

Enforce

Zeitraum festlegen

Ein bestimmter Datumsbereich ist nicht festgelegt

Priorität

2

Schweregrad

Nicht angegeben

Bei Regelverarbeitungsfehlern

Ignore

Verarbeiten weiterer Regeln beenden

true

[Regeleinstellungen bearbeiten](#)

NP_Phishing_Domains

Regelbedingungen bearbeiten

Regeleinstellungen bearbeiten

Status: Enabled

Regel aktivieren oder deaktivieren

Aktiviert

✓ Regelstatus erfolgreich aktualisiert

Regeleinstellungen

Regelname

NP_Phishing_Domains

Schweregrad

Nicht angegeben

Absenderadresse

Matching HeaderOrEnvelope

Bei Regelverarbeitungsfehlern

Ignore

Modus

Enforce

Zeitraum festlegen

Ein bestimmter Datumsbereich ist nicht festgelegt

Priorität

2

Regelbeschreibung

Diese Regel anwenden, wenn


sender's address domain portion belongs to any of these domains: 'emaidigital.de' or 'status-monitor.info'

Gehen Sie wie folgt vor:

Set the spam confidence level (SCL) to '-1'
and Stop processing more rules

Neu Transportregeln sind standardmäßig deaktiviert und müssen dementsprechend nach Erstellung manuell aktiviert werden. Dazu im Anschluss noch einmal die Regel in der Liste aufrufen.

Die Priorität der Regel kann ebenfalls im Nachhinein bei Bedarf verändert werden. Je kleiner der Wert, desto höher die Priorität.

 **Anqa**
IT-Security

Awareness | MS365 Whitelisting

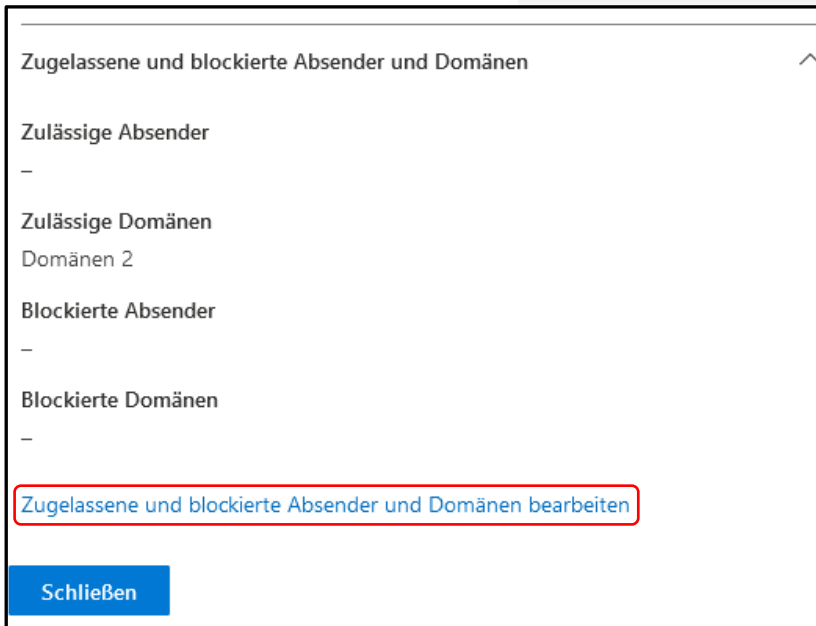
Seite 9

Cyber Security Awareness

MS365 Whitelisting

6. Weitere Möglichkeiten

Wie in Kapitel 2 kann im Defender unter <https://security.microsoft.com/antispam> die Antispam-Eingangsrichtlinie so angepasst werden, dass unsere Domains als zulässig gewertet werden.



The screenshot shows a window titled 'Zugelassene und blockierte Absender und Domänen' with a close button in the top right corner. The window is divided into four sections: 'Zulässige Absender' (containing a minus sign), 'Zulässige Domänen' (containing 'Domänen 2'), 'Blockierte Absender' (containing a minus sign), and 'Blockierte Domänen' (containing a minus sign). At the bottom of the window, there is a blue button labeled 'Schließen'. A red rectangular box highlights the text 'Zugelassene und blockierte Absender und Domänen bearbeiten' located just above the 'Schließen' button.

Weitere nötige Optionen könnten abhängig davon sein, wie Ihr Unternehmen die Richtlinien von MS365 für sich angepasst hat. Zudem ändert sich bei MS Azure/Entra regelmäßig etwas, so dass der ein oder andere Screenshot innerhalb dieses Dokuments nicht mehr aktuell sein kann.

Cyber Security Awareness

MS365 Whitelisting

7. Einrichten einer Postfach-Weiterleitung für Network Box

Im folgenden Teil soll es darum gehen, eine Weiterleitung an unser Phishing-Test-Postfach zu erstellen. Ist diese einmal eingerichtet können wir testen, ob Phishingvorlagen (nach dem einmaligen Einrichten der Allow-Regeln) weiterhin zu einem späteren Zeitpunkt noch in Ihrem Netzwerk ankommen oder ob ggf. eine neu eingeführte Microsoft-Policy dies inzwischen verhindert.

Cyber Security Awareness

MS365 Whitelisting

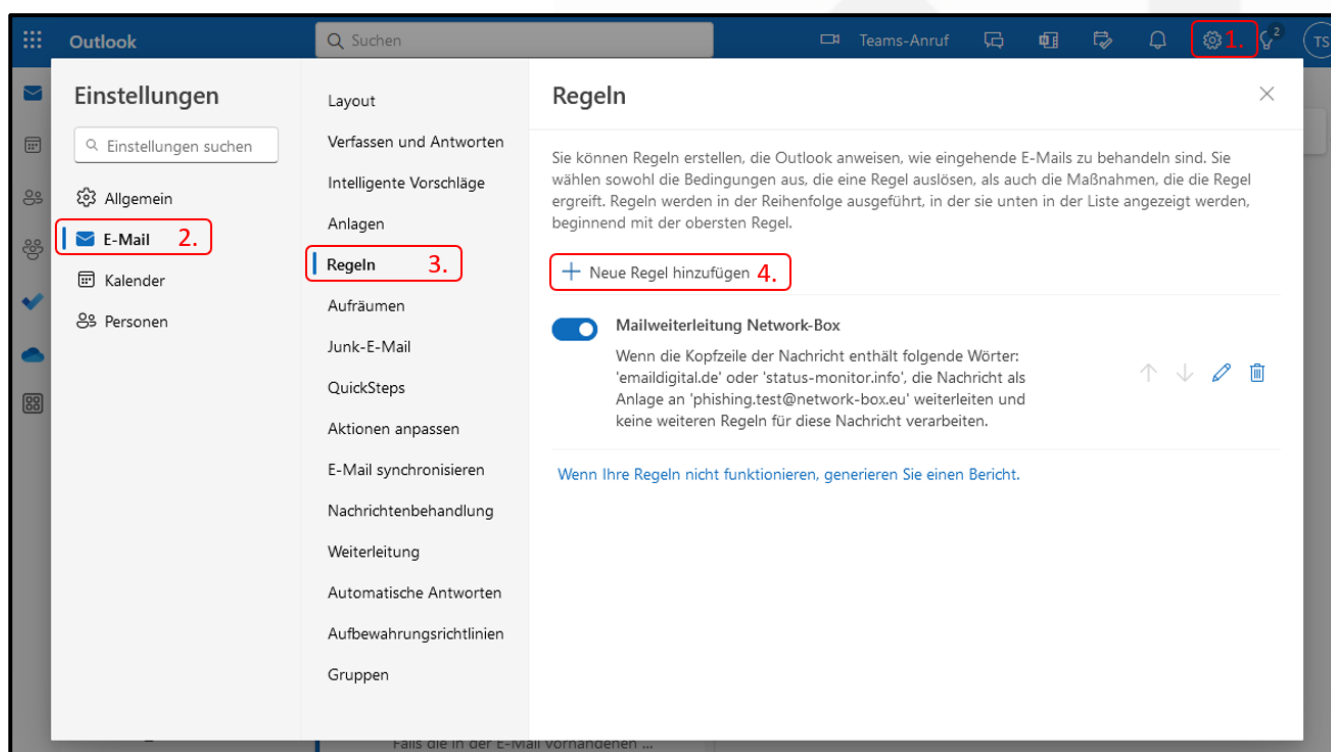
7.1 Client-Weiterleitungsregel erstellen (neu)

Um eine Weiterleitungsregel zu erstellen, die aus einem Postfach heraus die Testmails als Anhang weiterleitet, muss über Outlook selbst eine solche Regel eingestellt werden. **Über das Admincenter ist dies nicht möglich.**

Dort hinterlegte E-Mail-Fluss-Regeln greifen immer vor Eintreffen im Clientpostfach. Es könnte also sein, dass die Testmails an uns weitergeleitet werden, obwohl diese gar nicht beim Empfänger, sondern in der Quarantäne angekommen sind.

Die **Einstellungen** können in der **Online- oder der App-Version von Outlook** vorgenommen werden. Sie sollten in beiden Fällen in dem Postfach innerhalb des Netzwerks Ihrer Organisation eingeloggt sein, an das unsere Testmails gesendet werden sollen.

7.1.1 Outlook Online



Die Regel kann in den Einstellungen (das Rädchen oben rechts, ggf. hinter drei Punkten) recht einfach erstellt werden.

Cyber Security Awareness

MS365 Whitelisting

7.1.1 Outlook Online

Geben Sie nun der Regel einen Namen und legen die Einstellungen wie im Bild zu sehen fest.

Die Weiterleitung beschränkt sich dann auf E-Mails, die im Nachrichtenkopf unsere Versanddomänen **emaidigital.de** bzw. **status-monitor.info** enthalten.

Regeln

1 Mailweiterleitung Network-Box 5.

✓ Bedingung hinzufügen

Nachrichtenkopfzeile enthält Nachrichtenkopfzeile enthält
emaidigital.de status-monitor.info 6.

Eine weitere Bedingung hinzufügen

✓ Aktion hinzufügen

Als Anlage weiterleiten Als Anlage weiterleiten
phishing.test@network-box.eu 7.

Weitere Aktion hinzufügen

Ausnahme hinzufügen

✓ Verarbeiten weiterer Regeln beenden

Speichern 8. Verwerfen

Die Testmails werden danach aus dem Postfach als Anlage an unsere Phishing-Test-Adresse **phishing.test@network-box.eu** gesendet.

Sollten Sie nach einem Test eine E-Mail auf englisch erhalten, die folgende Zeilen enthält, so ist die Weiterleitung an extern für Ihre Adresse gesperrt. In diesem Fall befindet sich die Lösung unter 6.2.

Diagnostic information for administrators:

Generating server: FR0P281MB2124.DEUP281.PROD.OUTLOOK.COM

phishing.test@network-box.eu

Remote server returned '550 5.7.520 Access denied, Your organization does not allow external forwarding. Please contact your administrator for further assistance. AS(7550)'

Cyber Security Awareness

MS365 Whitelisting

7.1.2 Outlook-App

Für die Appversion navigieren Sie zu:

Datei -> Regeln und Benachrichtigungen verwalten -> Neue Regel -> Regel auf von mir empfangene Nachrichten anwenden

Kontoinformationen

Microsoft Exchange

Konto hinzufügen

Kontoeinstellungen

Automatische Antworten

Tools

Regeln und Benachrichtigungen verwalten

COM-Add-Ins verwalten

Add-Ins verwalten

Regel-Assistent

Mit einer Vorlage oder einer leeren Regel beginnen

1. Schritt: Vorlage auswählen

Den Überblick behalten

- Nachrichten von einem bestimmten Absender in einen Ordner verschieben
- Nachrichten mit bestimmten Wörtern im Betreff in einen Ordner verschieben
- An eine öffentliche Gruppe gesendete Nachrichten in einen Ordner verschieben
- Nachrichten von einer bestimmten Person für die Nachverfolgung kennzeichnen
- RSS-Elemente von einem bestimmten RSS-Feed in einen Ordner verschieben

Auf dem Laufenden bleiben

- Nachrichten von einer bestimmten Person im Benachrichtigungsfenster anzeigen
- Beim Erhalt von Nachrichten von einer bestimmten Person einen Sound abspielen
- Beim Erhalt von Nachrichten von einer bestimmten Person eine Benachrichtigung senden

Regel ohne Vorlage erstellen

- Regel auf von mir empfangene Nachrichten anwenden**
- Regel auf von mir gesendete Nachrichten anwenden

2. Schritt: Regelbeschreibung bearbeiten (auf unterstrichene Werte klicken)

Nach Erhalt einer Nachricht

Abbrechen < Zurück Weiter > Fertig stellen

Cyber Security Awareness

MS365 Whitelisting

7.1.2 Outlook-App

Hier können Sie Schritt für Schritt die Optionen einstellen.

Text suchen

Im Nachrichtenkopf zu suchende Wörter:

Hinzufügen

Suchliste:

"emaildigital.de" oder
"status-monitor.info"

OK Abbrechen

An phishing.test@network-box.eu

Auch hier wieder die Domains **emaildigital.de** und **status-monitor.info** als Suchparameter im Nachrichtenkopf angeben und die E-Mail als Anlage an **phishing.test@network-box.eu** weiterleiten lassen. Bei Fehlermeldungsmail nach versuchter Zustellung siehe 6.2.

Regel-Assistent

Regel fertig stellen.

1. Schritt: Regelnamen eingeben

Network-Box Phishingtest-Weiterleitung

2. Schritt: Regeloptionen festlegen

☐ Diese Regel jetzt auf Nachrichten anwenden, die sich bereits im Ordner "Posteingang" befinden.

☒ Diese Regel aktivieren

☐ Diese Regel für alle Konten erstellen

3. Schritt: Regelbeschreibung überprüfen (auf unterstrichene Werte klicken)

Nach Erhalt einer Nachricht mit 'emaildigital.de' oder 'status-monitor.info' im Nachrichtenkopf diese als Anlage an Phishing Test weiterleiten

Abbrechen < Zurück Weiter > Fertig stellen

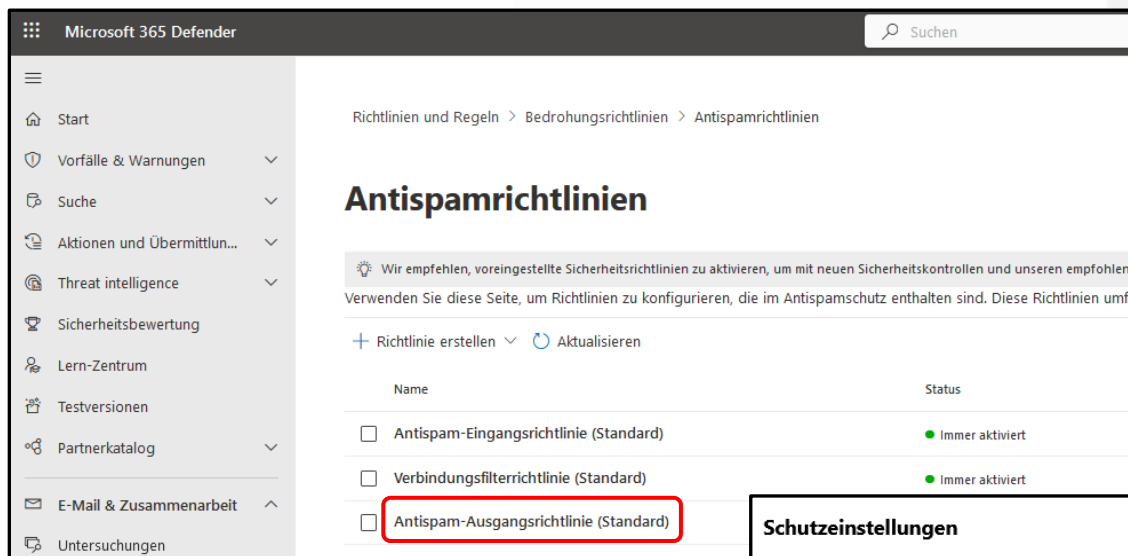
7.2 Antisperm-Ausgangsrichtlinie anpassen

Damit überhaupt E-Mails an Ihre Domain nach extern weitergeleitet werden können, muss diese Option für den gesamten Tenant aktiviert sein.

Als Standardeinstellung ist diese Option deaktiviert.

Gehen Sie dazu auf folgende Seite:

<https://security.microsoft.com/antispam>

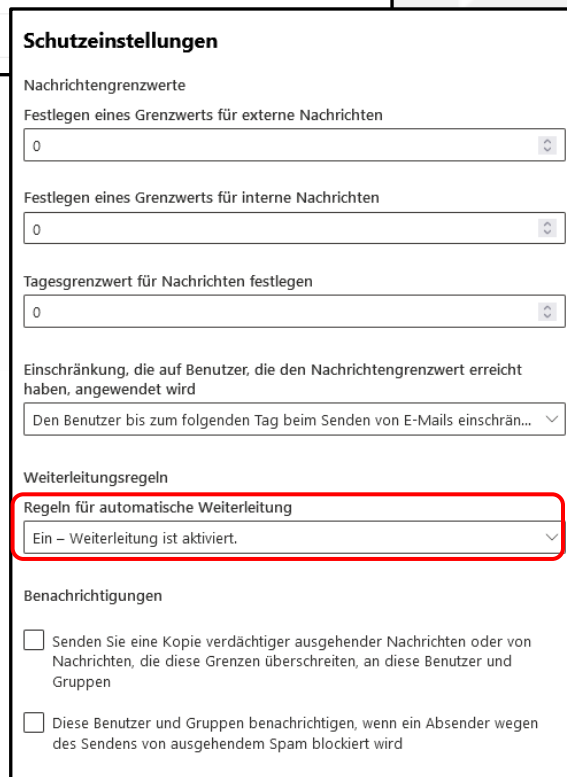


Dort können Sie nun die Schutzeinstellungen bearbeiten.

Aktivieren Sie hier bitte die **Regeln für automatische Weiterleitung**.

Bei Bedarf können Sie außerdem Benachrichtigungen Und Grenzwerte aktivieren.

Sind diese beiden Schritte zusätzlich zum Whitelisting, wie in den NB-Allowregeln beschrieben, erfolgt, können wir den Versand von unserer Seite aus testen. **Teilen Sie uns dazu bitte die von Ihnen angelegte Postfachadresse mit.**



7.3 Einrichtung eines kostenfreien Verteilerpostfachs (alt)

!FALLS BEREITS EINE CLIENTWEITERLEITG.(6.1) EINGERICHTET WURDE, ENTFÄLLT DIESER PUNKT!

Ein neues Postfach jedweder Art können Sie auf Ihrem M365-Tenant, sobald sie dort als Admin eingeloggt sind, am folgenden Ort einsehen:

<https://admin.exchange.microsoft.com/#/mailboxes>

Exchange Admin Center Suchen (Vorschau)

Start > Postfächer

Postfächer verwalten

Erstellen und verwalten Sie Einstellungen für freigegebene Postfächer. Sie können auch Einstellungen für Benutzerpostfächer verwalten. Um sie hinzuzufügen oder zu löschen, müssen Sie jedoch zur [Microsoft 365 Admin Center](#) und führen Sie dies auf der Seite **aktiv Benutzer** aus. [Weitere Informationen zu Postfächern](#)

+ Freigegebenes Postfach hinzufügen

☐ Anzeigename ↑

☐ **NB-Phishingtest**

Freigegebenes Postfach hinzufügen

E-Mails können an und von dem Namen und der E-Mail-Adresse des freigegebenen Postfachs und nicht an eine Einzelperson gesendet werden. Nachdem Sie das freigegebene Postfach erstellt haben, können Sie Mitglieder hinzufügen, die E-Mails lesen und beantworten können.

Anzeigename *

NB-Phishingtest

E-Mail-Adresse *

NB-Phishingtest @ NetworkBoxTest.onmicrosoft.com

Alias

Alias

Hier ein *Freigegebenes Postfach* hinzufügen.
Die hier eingetragene E-Mail-Adresse müssten Sie uns dann später mitteilen.

Dem Postfach kann, muss aber kein User Ihrer Organisation zugewiesen werden.

Schließen Sie nun die Optionen und aktualisieren Sie die Liste der Postfächer.
Es kann etwas dauern, bis das neu angelegte Postfach auftaucht.

Exchange Admin Center Suchen (Vorschau)

Start > Postfächer

Postfächer verwalten

Erstellen und verwalten Sie Einstellungen für freigegebene Postfächer. Sie können auch Einstellungen für Benutzerpostfächer verwalten. Um sie hinzuzufügen oder zu löschen, müssen Sie jedoch zur [Microsoft 365 Admin Center](#) und führen Sie dies auf der Seite **aktiv Benutzer** aus. [Weitere Informationen zu Postfächern](#)

+ Freigegebenes Postfach hinzufügen Nachrichtenflusseinstellung **Aktualisieren** Postfächer exportieren

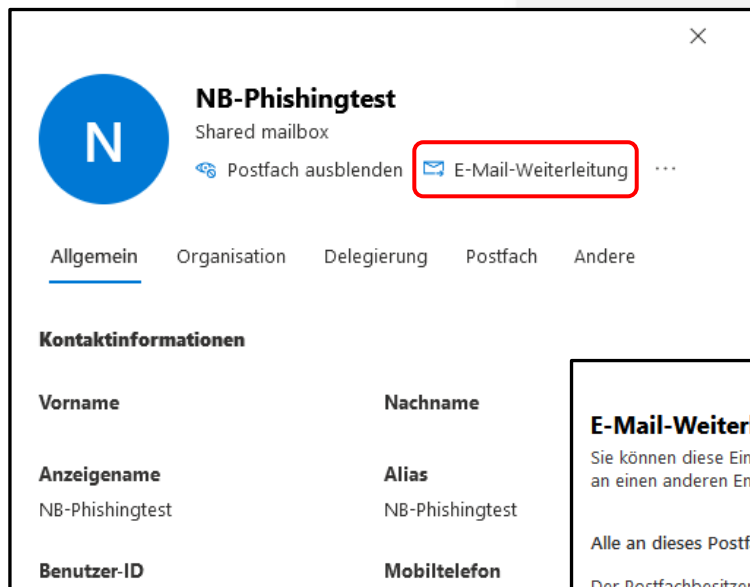
<input type="checkbox"/>	Anzeigename ↑	E-Mail-Adresse	Empfängertyp	Archivstatus
<input type="checkbox"/>	NB-Phishingtest	NB-Phishingtest@NetworkBoxTest.onmicrosoft.com	SharedMailbox	None

Cyber Security Awareness

MS365 Whitelisting

7.3 Einrichtung eines kostenfreien Verteilerpostfachs (alt)

Sobald das neu angelegte Postfach auftaucht, klicken Sie auf dessen Anzeigenamen. In den Optionen finden Sie den Punkt **E-Mail-Weiterleitung**.



NB-Phishingtest
Shared mailbox

Postfach ausblenden **E-Mail-Weiterleitung** ...

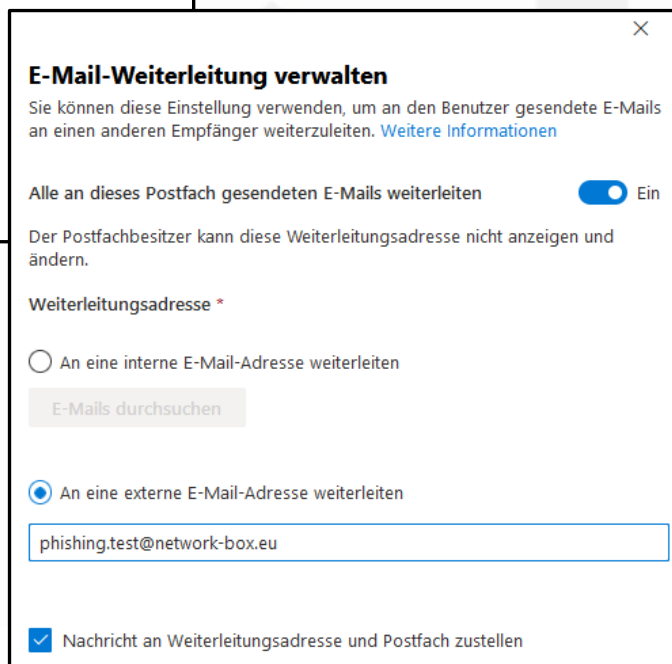
[Allgemein](#)
[Organisation](#)
[Delegierung](#)
[Postfach](#)
[Andere](#)

Kontaktinformationen

Vorname	Nachname
Anzeigenname	Alias
NB-Phishingtest	NB-Phishingtest
Benutzer-ID	Mobiltelefon

Hier tragen Sie bitte die externe Adresse **phishing.test@network-box.eu** ein und **aktivieren die Weiterleitung** sowie ggf. den Haken für die Zustellung an PF und Weiterleitungsadresse.

Speichern Sie nun einfach diese Optionen und die Weiterleitung ist eingerichtet.



E-Mail-Weiterleitung verwalten

Sie können diese Einstellung verwenden, um an den Benutzer gesendete E-Mails an einen anderen Empfänger weiterzuleiten. [Weitere Informationen](#)

Alle an dieses Postfach gesendeten E-Mails weiterleiten ☒ Ein

Der Postfachbesitzer kann diese Weiterleitungsadresse nicht anzeigen und ändern.

Weiterleitungsadresse *

☐ An eine interne E-Mail-Adresse weiterleiten
☒ An eine externe E-Mail-Adresse weiterleiten

phishing.test@network-box.eu

☒ Nachricht an Weiterleitungsadresse und Postfach zustellen