Exchange Online, keine Weiterleitungen an externe E-Mail-Adressen

In den letzten Tagen erreichten mich einige Hilferufe, dass automatische Weiterleitungen aus Exchange Online bzw. Microsoft 365 von einem auf den anderen Tag nicht mehr funktionierten.

Dabei ist es unerheblich ob die Mail von einer Regel aus dem Benutzerpostfach oder in den Postfacheinstellungen im Exchange Online Admin Portal eingestellt wurde.

Der Grund dafür liegt in neuen Einstellungen, die Microsoft derzeit in Wellen auf die Kunden ausrollt.

Zug für Zug überführt Microsoft verschiedenen Funktionen und Einstellungen aus Microsoft 365 in das neue Admin Portal Microsoft 365 Security und Compliance.

Dabei werden nicht nur die Administrationsportale zusammengeführt, sondern auch neue Funktionen und auch neue Standard-Einstellungen bereitgestellt.
Diese neuen Einstellungen folgen meist dem Ansatz „Security by Default“. Sind also zunächst einmal sehr stark sicherheitsbetont voreingestellt.

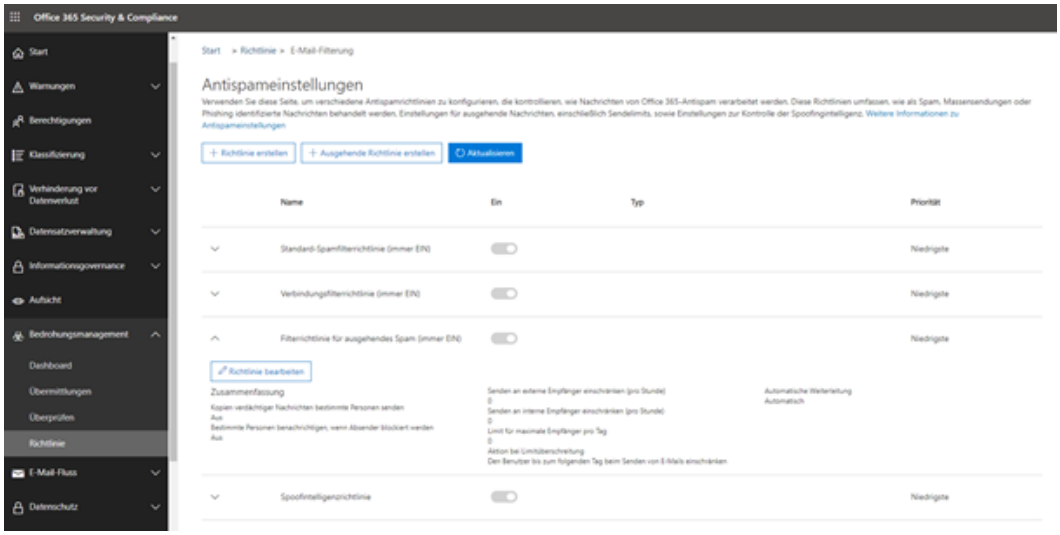
Security by Default

Die neuen Antispameinstellungen im Microsoft Defender für Office 365 (früher Office 365 Advanced Threat Protection) sind nun ein solcher Fall.

Da durch den Wechsel der Administrations-Portale versteckt sich das neue Security und Compliance etwas. Dieser Link führt direkt zu den Spameinstellungen:

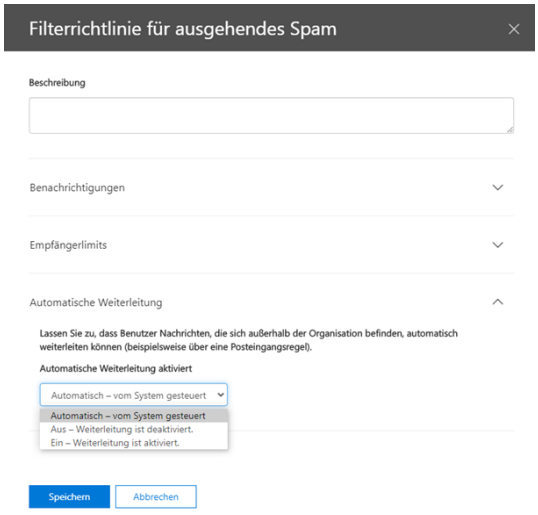
https://protection.office.com/antispam

In den Richtlinien für die Antispameinstellungen finden wir die Filterrichtlinie für ausgehendes Spam.



Die Richtlinien sind per Default immer ein und können über das Webportal nicht komplett deaktiviert werden.

Aber durch Bearbeiten der Richtlinie kommt man zu den granularen Einstellungen.



Dort findet sich unter *Automatische Weiterleitung* die Voreinstellung „*Automatisch, vom System gesteuert*“. Und eben diese Systemvorgabe verhindert die automatische Weiterleitung.

Hier kann die Standard-Einstellung vom Admin über die Web-Konsole geändert werden.

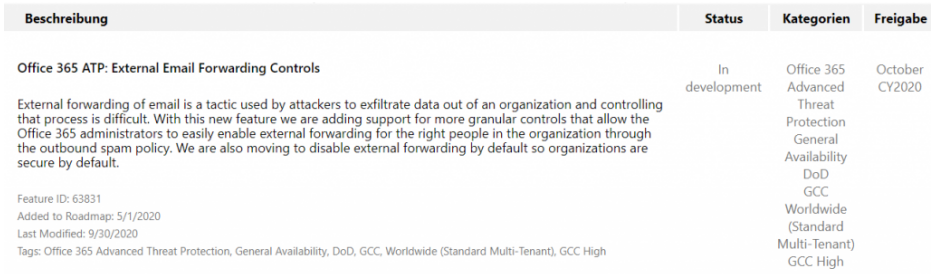
Um die automatische Weiterleitung wieder zu aktivieren wählt man hier „Ein – Weiterleitung ist aktiviert“

Gut gemacht, aber …

Aus meiner Sicht steuert Microsoft grundsätzlich in die richtige Richtung, wenn Sicherheitsschwachstellen auch bei bestehenden Umgebungen angepasst werden.

Problematisch ist das natürlich, wenn solche Änderungen laufende Geschäftsprozesse beinträchtigen.

Wenn man nun genau nachsieht, dann kann man diese Änderung bereits im Januar 2020 in der Office 365 ATP Roadmap erkennen.



Beschreibung	Status	Kategorien	Freigabe
Office 365 ATP: External Email Forwarding Controls External forwarding of email is a tactic used by attackers to exfiltrate data out of an organization and controlling that process is difficult. With this new feature we are adding support for more granular controls that allow the Office 365 administrators to easily enable external forwarding for the right people in the organization through the outbound spam policy. We are also moving to disable external forwarding by default so organizations are secure by default. Feature ID: 63831 Added to Roadmap: 5/1/2020 Last Modified: 9/30/2020 Tags: Office 365 Advanced Threat Protection, General Availability, DoD, GCC, Worldwide (Standard Multi-Tenant), GCC High	In development	Office 365 Advanced Threat Protection General Availability DoD GCC Worldwide (Standard Multi-Tenant) GCC High	October CY2020

Vielleicht hätte Microsoft hier die Partner etwas direkter auf eine solche Veränderung hinweisen können.

Hier noch die passenden Links in den Microsoft Docs

https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide

https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/configure-the-outbound-spam-

policy?view=o365-worldwide&preserve-view=true#use-the-security–compliance-center-to-create-outbound-spam-policies

https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide