

Defender for Office 365: Safe Links und Safe Attachments — was wirklich schützt und was nur Klickzahlen produziert

Es gibt eine Sorte Satz, die man in Sicherheitsbesprechungen erstaunlich oft hört: „Wir haben Defender for Office 365, das ist lizenziert.“ Er wird mit dem Tonfall vorgetragen, den man sonst für einen abgeschlossenen Bauabschnitt reserviert. Und er ist ungefähr so aussagekräftig wie „Wir haben einen Feuerlöscher gekauft“ — richtig, beruhigend, und vollkommen unabhängig davon, ob das Ding jemals aufgehängt, geprüft oder auch nur ausgepackt wurde.

Denn Defender for Office 365 ist kein Schalter, sondern eine Sammlung von Richtlinien, die erst dann etwas tun, wenn jemand sie Postfächern zuweist. Es gibt keine Safe-Links-Standardrichtlinie und keine Safe-Attachments-Standardrichtlinie. Es gibt einen eingebauten Sockel namens Built-in Protection, der greift, solange niemand etwas anderes konfiguriert hat — und der ist bewusst zurückhaltend eingestellt. Wer sich darauf verlässt, hat einen Schutz, bei dem die Belegschaft am Warnbildschirm weiterhin auf „Trotzdem fortfahren“ klicken darf. Das ist kein Fehler von Microsoft, das ist Voreinstellung. Es ist trotzdem nicht das, was du dir vorgestellt hast.

Dieser Beitrag arbeitet das Handlungsfeld sauber durch: Preset Security Policies im Vergleich Standard gegen Strict, Safe Links in Mail, Teams und den Office-Apps, die Prüfung zum Zeitpunkt des Klicks, das Klick-Protokoll als forensische Grundlage, Safe Attachments für SharePoint, OneDrive und Teams, Anti-Phishing mit Impersonation-Schutz, die nachträgliche Bereinigung durch ZAP und die Quarantäne-Richtlinien, die entscheiden, wer eine Nachricht wieder herausholen darf. Er ist Teil der Reihe zu [Microsoft 365 Security](#) und setzt voraus, dass Identität und Zugriff bei dir bereits ein Thema waren — E-Mail-Schutz ohne Mehrfaktor-Anmeldung ist ein Sicherheitsgurt in einem Auto ohne Bremsen.

Vorweg die schlechte Nachricht, damit sie aus dem Weg ist: Keine dieser Schichten verhindert, dass jemand in deinem Haus auf einen Link klickt. Sie verschieben nur, was danach passiert. Das ist weniger, als der Vertrieb verspricht, und deutlich mehr, als es klingt.

Erst die Lizenz, dann die Illusion: Plan 1, Plan 2 und der Sockel

Bevor du irgendetwas konfigurierst, solltest du wissen, worüber du eigentlich verfügst. Microsoft beschreibt den E-Mail-Schutz als Leiter mit drei Sprossen. Ganz unten stehen die eingebauten Schutzfunktionen, die jede Organisation mit Cloud-Postfächern hat: Anti-Malware, Anti-Spam, Spoof-Schutz, Verbindungsfilter, Quarantäne, die Mandantenliste für erlaubte und blockierte Absender und die nachträgliche Bereinigung per ZAP. Das ist mehr, als viele denken, und es kostet nichts extra.

Darüber liegt Defender for Office 365 Plan 1. Das ist die Sprosse, auf der Safe Links und Safe Attachments wohnen, dazu der Impersonation-Schutz in den Anti-Phishing-Richtlinien und die Phishing-Schwellenwerte. Plan 2 setzt obendrauf, was du nach dem Vorfall brauchst: Explorer statt

der abgespeckten Echtzeiterkennungen, Kampagnenansichten, Bedrohungsverfolgung, automatisierte Untersuchung und Reaktion sowie das Attack Simulation Training.

FAKTEN · Seit dem 1. Juli 2026 ist Plan 1 in E3 enthalten

Microsoft hat Defender for Office 365 Plan 1 zum 1. Juli 2026 in Microsoft 365 E3 und Office 365 E3 aufgenommen; die Ausrollung an die Mandanten begann am 18. Juni 2026. Wer bisher mit dem Argument „haben wir nicht lizenziert“ um Safe Links herumgekommen ist, sollte in der Verwaltungsoberfläche unter „Deine Produkte“ noch einmal nachsehen. Für Microsoft 365 Business Premium war Plan 1 ohnehin schon immer dabei.

- › Plan 2 steckt weiterhin in Microsoft 365 E5, A5 und G5 oder wird als Zusatz gekauft.
- › Safe Documents ist kein Bestandteil der Defender-Pläne, sondern hängt an A5 beziehungsweise der Defender-Suite.

Woran du in zwanzig Sekunden erkennst, welchen Plan du hast

Der schnellste Test führt nicht über die Lizenzübersicht, sondern über das Menü. Öffne im Defender-Portal den Bereich E-Mail und Zusammenarbeit. Steht dort „Echtzeiterkennungen“, hast du Plan 1. Steht dort „Explorer“, hast du Plan 2. Das ist kein Trick, das ist die von Microsoft selbst empfohlene Unterscheidung — und sie erspart dir zwanzig Minuten Diskussion mit der Beschaffung.

Funktion	Eingebaut	Plan 1	Plan 2
Anti-Malware, Anti-Spam, Spoof-Schutz	ja	ja	ja
Quarantäne und Quarantäne-Richtlinien	ja	ja	ja
ZAP für E-Mail	ja	ja	ja
Safe Links (Mail, Teams, Office-Apps)	nein	ja	ja
Safe Attachments in der Mail	nein	ja	ja
Safe Attachments für SharePoint, OneDrive, Teams	nein	ja	ja
Impersonation-Schutz, Phishing-Schwellenwerte	nein	ja	ja
ZAP für Teams	nein	ja	ja
Echtzeiterkennungen	nein	ja	—
Explorer, Kampagnen, Bedrohungsverfolgung	nein	nein	ja
Automatisierte Untersuchung und Reaktion	nein	nein	ja
Attack Simulation Training	nein	nein	ja
Erweiterte Suche über Teams-Nachrichten	nein	nein	ja

Was in welchem Plan steckt — und was ohnehin alle haben

Die Trennlinie ist praktisch relevant. Mit Plan 1 kannst du verhindern und erkennen. Für die geordnete Nacharbeit — wer hat geklickt, wohin lief die Kampagne, welche Postfächer sind noch betroffen — brauchst du Explorer und damit Plan 2. Wenn du Phishing-Übungen im eigenen Haus fahren willst, ebenfalls: Das Trainingsmodul steckt in Plan 2. Wie du daraus etwas Sinnvolles machst, steht in [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#).

Preset Security Policies: Standard, Strict und der stille Sockel

Microsoft bietet dir drei vorgefertigte Schutzprofile an, und die sind das mit Abstand beste Angebot in diesem gesamten Produktbereich — weil sie dir eine Entscheidung abnehmen, die du sonst über vierzig Einzeleinstellungen selbst treffen müsstest, jedes Mal neu, wenn Microsoft eine Empfehlung ändert. Preset-Richtlinien werden zentral gepflegt. Deine handgeschnittene Anti-Spam-Richtlinie von 2021 nicht.

Built-in Protection: der Sockel, den du schon hast

Built-in Protection ist standardmäßig allen Empfängern zugewiesen, sobald mindestens eine Defender-Lizenz im Mandanten liegt. Es liefert Safe Links und Safe Attachments — und zwar nur diese beiden. Das ist der Grund, warum in vielen Häusern „irgendwie schon etwas läuft“, obwohl niemand je eine Richtlinie angelegt hat.

Der Haken steckt in den Voreinstellungen. Built-in Protection ist bewusst reibungsarm konfiguriert: URLs werden nicht umgeschrieben, sondern nur über die Schnittstelle geprüft, interne Nachrichten bleiben außen vor, und die Belegschaft darf sich über die Warnseite hinwegsetzen. Genau diese drei Punkte sind die Unterschiede zu Standard und Strict.

Einstellung	Built-in Protection	Standard und Strict
Durchklicken zur Originaladresse erlauben (AllowClickThrough)	erlaubt	nicht erlaubt
Keine URL-Umschreibung, nur Prüfung über die Schnittstelle (DisableURLRewrite)	aktiv — kein Rewrite	inaktiv — mit Rewrite
Safe Links auch auf interne Nachrichten anwenden (EnableForInternalSenders)	aus	an
Safe Links für Teams (EnableSafeLinksForTeams)	an	an
Safe Links für Office-Apps (EnableSafeLinksForOffice)	an	an
Klicks protokollieren (TrackClicks)	an	an
Safe Attachments: Reaktion auf unbekannte Schadsoftware	Blockieren	Blockieren

Safe Links: Built-in Protection gegen Standard und Strict

WARNUNG · Der Sockel lässt durchklicken — und das ist der ganze Unterschied

In Built-in Protection ist „Let users click through to the original URL“ eingeschaltet. Die Warnseite erscheint also, aber darunter steht ein Knopf, mit dem man weitergeht. Wer schon einmal einen Vorfall aufgearbeitet hat, weiß, wie oft dieser Knopf gedrückt wird. In Standard und Strict ist er abgeschaltet — und das ist der einzelne wirksamste Unterschied zwischen „wir haben Safe Links“ und „Safe Links schützt uns“.

Standard oder Strict: die tatsächlichen Unterschiede

Jetzt wird es interessant, weil die verbreitete Vorstellung falsch ist. Standard und Strict unterscheiden sich nicht bei Safe Links und nicht bei Safe Attachments — dort sind die Einstellungen identisch. Der Unterschied liegt ausschließlich in der Schärfe der Spam- und Phishing-Bewertung und darin, wohin eine erkannte Nachricht wandert: in den Junk-Ordner oder in die Quarantäne.

Einstellung	Standard	Strict
Schwellenwert für Massensendungen (BulkThreshold)	6	5
Aktion bei erreichtem Massenwert (BulkSpamAction)	Junk-Ordner	Quarantäne
Aktion bei Spam (SpamAction)	Junk-Ordner	Quarantäne
Aktion bei sicherem Spam (HighConfidenceSpamAction)	Quarantäne	Quarantäne
Aktion bei Spoofing durch Spoof Intelligence (AuthenticationFailAction)	Junk-Ordner	Quarantäne
Aktion bei Identitätsnachahmung über Mailbox Intelligence (MailboxIntelligenceProtectionAction)	Junk-Ordner	Quarantäne
Phishing-Schwellenwert (PhishThresholdLevel)	3 — aggressiver	4 — am aggressivsten
Aufbewahrung in der Quarantäne (QuarantineRetentionPeriod)	30 Tage	30 Tage
Safe Links und Safe Attachments	identisch	identisch

Standard gegen Strict — die Einstellungen, die sich wirklich unterscheiden

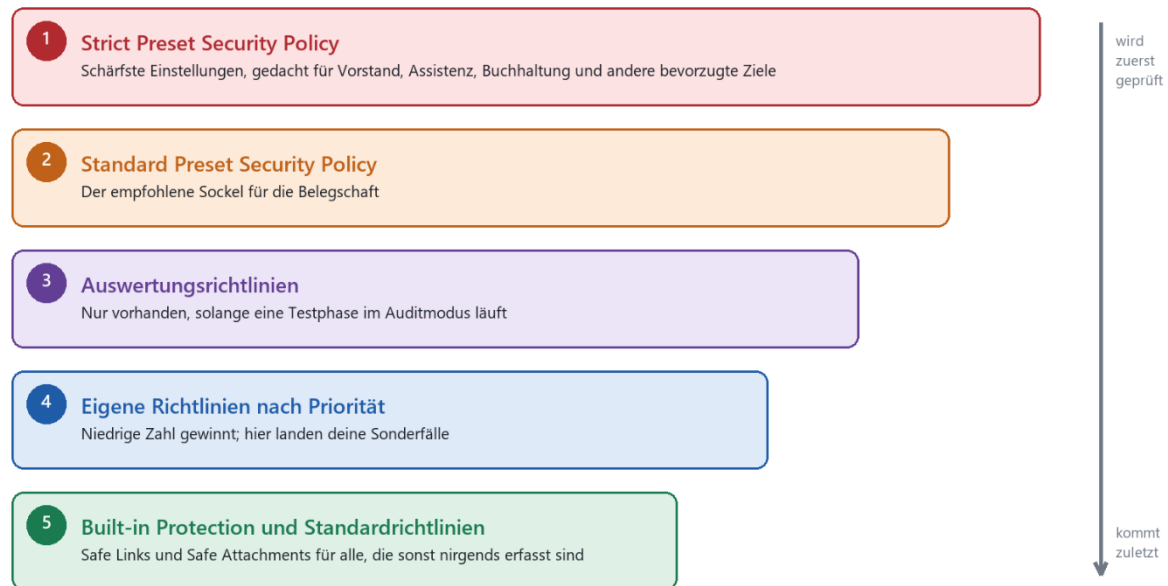
Übersetzt heißt das: Strict verschiebt weniger in den Junk-Ordner und mehr in die Quarantäne. Damit steigt die Zahl der Fälle, in denen jemand aus der IT eine Nachricht freigeben muss. Genau das ist der Grund, warum Microsoft Strict nur für Personengruppen empfiehlt, für die es eine Betreuung durch die Administration gibt — Geschäftsführung, Vorstandsassistenten, Buchhaltung, Personalabteilung. Wer Strict flächendeckend ausrollt und dann keine Zeit hat, die Quarantäne durchzusehen, produziert genau den Effekt, den er vermeiden wollte: Die Belegschaft ruft nicht mehr in der IT an, sondern lässt sich Rechnungen aufs private Postfach schicken.

Vorrangfolge: warum deine Ausnahme nicht greift

Der zweithäufigste Konfigurationsfehler in diesem Bereich ist eine eigene Richtlinie, die nie zur Anwendung kommt. Die Regel ist einfach und unerbittlich: Für jedes Postfach gilt genau eine Richtlinie je Schutzart, nämlich die erste passende in einer festen Reihenfolge. Danach wird nichts mehr ausgewertet.

Vorrangfolge: welche Richtlinie am Ende wirklich greift

Die erste Regel, die auf ein Postfach passt, gewinnt — alle weiteren werden nicht mehr ausgewertet



Praktische Folge: Wer im Strict-Preset steht, bekommt niemals die Einstellungen einer eigenen Richtlinie — auch dann nicht, wenn diese Priorität 0 hat.

Skizze 1: Die Vorrangfolge der Richtlinien. Wer weiter oben erfasst ist, sieht von allem darunter nichts mehr.

Wenn also jemand im Strict-Preset steht und du zusätzlich eine eigene Safe-Links-Richtlinie mit Priorität 0 anlegst, gewinnt trotzdem Strict. Die einzige saubere Lösung: Wer die Einstellungen einer eigenen Richtlinie bekommen soll, muss im Preset als Ausnahme eingetragen werden. Und wer die Einstellungen von Built-in Protection bekommen soll, muss aus deinen eigenen Richtlinien ausgenommen werden. Das klingt nach Buchhaltung, weil es Buchhaltung ist.

TIPP · Nimm dir die Konfigurationsanalyse vor, bevor du diskutierst

Im Defender-Portal gibt es die Konfigurationsanalyse für Bedrohungsrichtlinien. Sie vergleicht deine aktuellen Einstellungen mit den Standard- und Strict-Empfehlungen und zeigt Abweichungen zeilenweise an. Das ist die schnellste Art, eine gewachsene Landschaft zu bewerten — und die einzige Argumentationsgrundlage, die in einer Besprechung mit der Geschäftsführung standhält, weil sie von Microsoft stammt und nicht von dir.

- › Anschließend gehört die Zuweisung von Preset-Richtlinien in die Dokumentation, nicht in den Kopf einer einzelnen Person.
- › Die Zuweisung für die eingebauten Schutzfunktionen und die für Defender for Office 365 lassen sich getrennt vergeben — praktisch für gestufte Ausrollungen.

Was du in Presets nicht ändern kannst — und was du selbst eintragen musst

Die Einstellungen in Preset-Richtlinien sind gesperrt. Das ist Absicht und meistens ein Vorteil. Es gibt allerdings eine Lücke, die regelmäßig übersehen wird: Der Impersonation-Schutz braucht Futter. Die Presets richten automatisch den Schutz für alle Domänen ein, die dir gehören, und schalten Mailbox Intelligence ein. Die Liste der zu schützenden Personen und die Liste fremder

Domänen, mit denen du häufig zu tun hast, musst du selbst pflegen. Ohne diese Listen läuft der teuerste Teil des Phishing-Schutzes im Leerlauf.

Der Weg einer Mail durch die Schutzschichten

Damit die einzelnen Bausteine nicht als lose Sammlung von Kontrollkästchen im Kopf bleiben, lohnt sich der Blick auf die Reihenfolge. Eine Nachricht durchläuft die Schichten nicht gleichzeitig, sondern nacheinander — und jede Schicht kann die Nachricht entnehmen, bevor die nächste sie überhaupt sieht.

Der Weg einer Mail durch die Schutzschichten

Von der Annahme am Rand bis zum Nachlauf 48 Stunden später



Teams und die Office-Apps durchlaufen die Stufen 1 bis 5 nicht: dort greift Safe Links ausschließlich zum Zeitpunkt des Klicks, ohne Rewrite.

Skizze 2: Der Weg einer Mail durch die Schutzschichten. Die Zustellung ist nicht das Ende der Prüfung, sondern die Mitte.

Zwei Dinge an dieser Darstellung sind der eigentliche Erkenntnisgewinn. Erstens: Die Prüfung endet nicht mit der Zustellung. Der Klick wird erneut bewertet, und bis zu 48 Stunden nach der Zustellung kann die Nachricht nachträglich noch aus dem Postfach verschwinden. Zweitens: Teams und die Office-Apps hängen nicht an diesem Fließband. Dort greift ausschließlich die Prüfung zum Zeitpunkt des Klicks. Wer eine Datei über Teams teilt, umgeht sämtliche Mail-Schichten.

Safe Attachments in der Mail: Blockieren, Beobachten, dynamische Zustellung

Safe Attachments öffnet Anhänge in einer virtuellen Umgebung und schaut zu, was passiert. Diese Detonation ist der eigentliche Grund für die Existenz des Produkts: Sie erkennt Schadsoftware, für

die es noch keine Signatur gibt. Sie kostet dafür Zeit — typischerweise unter 15 Minuten, gelegentlich länger, wenn Wiederholungsversuche und Analysezeit zusammenkommen.

Einstellung	Was passiert	Wann sinnvoll
Aus	Keine Detonation. Die reguläre Malware-Prüfung läuft weiter.	Praktisch nie. Microsoft rät ausdrücklich ab, weil ZAP dann ohne Bedrohungssignal ebenfalls nicht greift.
Beobachten	Nachricht wird zugestellt, Funde werden nur nachverfolgt.	Für eine befristete Beobachtungsphase, in Verbindung mit der Weiterleitung an ein Analysepostfach.
Blockieren	Nachricht wird nicht zugestellt, sondern in die Quarantäne gelegt; künftige Wiederholungen ebenfalls.	Der Normalfall. Voreinstellung und Empfehlung in Standard und Strict.
Dynamische Zustellung	Der Nachrichtentext kommt sofort an, die Anhänge werden durch Platzhalter ersetzt, bis die Prüfung fertig ist.	Wenn Verzögerungen fachlich nicht tragbar sind. Funktioniert ausschließlich mit Postfächern in Exchange Online.

Die vier Reaktionen auf unbekannte Schadsoftware in Safe-Attachments-Richtlinien

Die dynamische Zustellung klingt nach der eleganten Lösung und ist es oft auch. Sie hat allerdings eine erstaunlich lange Liste von Fällen, in denen sie Anhänge nicht ersetzen kann: Nachrichten in öffentlichen Ordnern, Nachrichten, die durch eigene Regeln aus dem Postfach heraus- und wieder hineinlaufen, Nachrichten, die automatisch in ein Archiv verschoben werden, gelöschte Nachrichten und alles, was mit S/MIME verschlüsselt ist. Wer in einem Haus mit vielen Posteingangsregeln arbeitet, sollte das vorher wissen und nicht hinterher erklären.

Passwortgeschützte Anhänge: der Klassiker im Bewerbungspostfach

Ein kennwortgeschütztes Archiv lässt sich nicht detonieren, solange das Kennwort fehlt. Angreifer wissen das seit Jahren, und es funktioniert weiterhin, weil es in Personalabteilungen und Steuerkanzleien legitime Gründe für kennwortgeschützte Anhänge gibt. Safe Attachments probiert bekannte Kennwörter und typische Muster durch und versucht außerdem, das Kennwort aus dem Nachrichtentext zu ziehen. Wenn das nicht reicht, kannst du die Option zum Blockieren nicht prüfbarer verschlüsselter Anhänge einschalten. Dann wandert die Nachricht in die Quarantäne, statt zugestellt zu werden.

Der elegante Teil dieser Funktion: Die betroffene Person kann die Nachricht selbst freigeben, indem sie im Defender-Portal das Kennwort für den Anhang eingibt. Safe Attachments führt daraufhin eine neue Detonation durch. Ist der Anhang sauber, wird zugestellt. Ist er es nicht, bleibt die Nachricht liegen. Das Kennwort wird nicht gespeichert, und es gibt genau einen Versuch je Nachricht.

WICHTIG · Sag deiner Belegschaft vorher, welches Kennwort gemeint ist

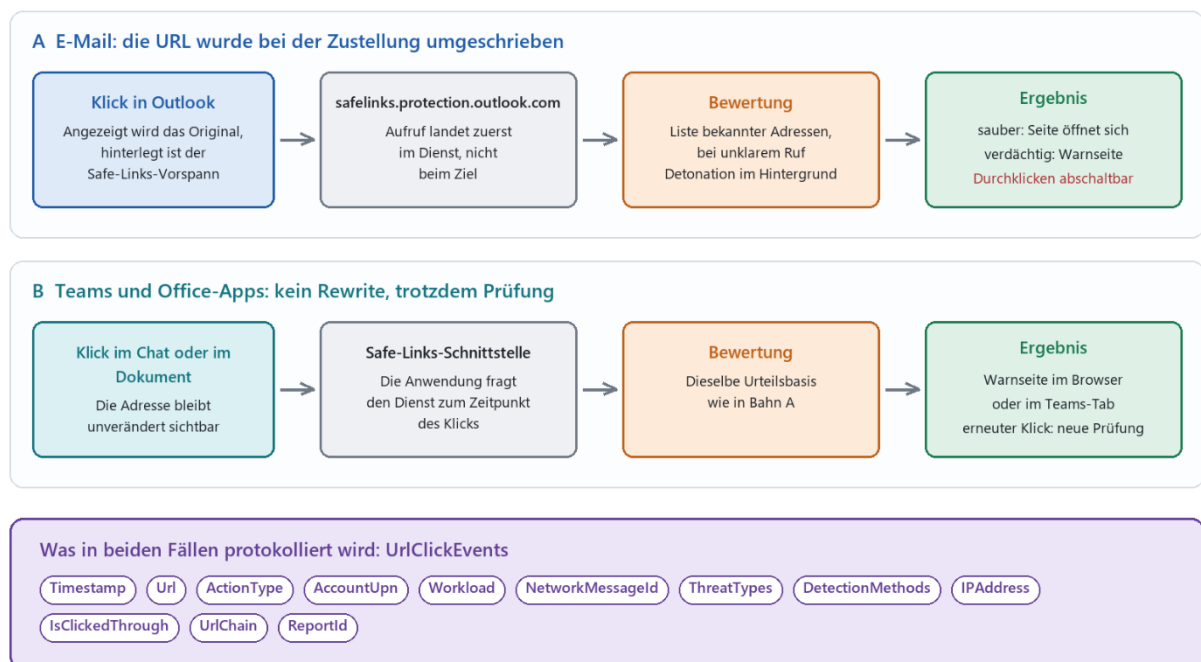
Ein Eingabefeld mit der Beschriftung „Kennwort“ in einem Microsoft-Portal ist genau die Situation, in der Menschen ihr Anmeldekennwort eintippen. Gemeint ist ausschließlich das Kennwort des Anhangs. Wer diese Funktion einschaltet, sollte das in der internen Ankündigung in einem Satz erklären — und dazuschreiben, dass unerwartete geschützte Anhänge an die IT gemeldet gehören und nicht selbst freigegeben werden.

Safe Links: Rewrite, Teams, Office-Apps und die Prüfung beim Klick

Safe Links macht zwei Dinge, die man auseinanderhalten sollte. In der Mail schreibt es Adressen um, sodass jeder Aufruf zuerst beim Prüfdienst landet. In Teams und in den Office-Apps schreibt es nichts um, sondern die Anwendung fragt zum Zeitpunkt des Klicks über eine Schnittstelle nach. Das Urteil ist dasselbe, der Weg dorthin nicht.

Was beim Klick passiert — zwei Wege, ein Urteil

Mit Rewrite in der Mail, ohne Rewrite in Teams und in den Office-Apps



IsClickedThrough verrät, wer sich über die Warnseite hinweggesetzt hat. Workload trennt Mail, Teams und Office-Apps.

Skizze 3: Zwei Wege zum selben Urteil — und die Spuren, die dabei entstehen.

Warum die Prüfung beim Klick der wichtigere Teil ist

Der zentrale Trick moderner Phishing-Kampagnen ist zeitversetztes Scharfschalten. Die Mail kommt mit einem Link auf eine harmlose Seite. Alle Prüfungen bestätigen: sauber. Zustellung. Ein paar Stunden später tauscht der Angreifer die Zielseite gegen ein Anmeldeformular aus. Genau für diesen Fall existiert die erneute Bewertung beim Klick. Und weil sie bei jedem einzelnen Klick stattfindet, hilft auch der zweite Versuch nichts: Wer auf der Warnseite auf „Zurück“ geht und die Adresse erneut anklickt, bekommt eine neue Prüfung und dieselbe Warnseite.

Dass genau dieser Angriffsweg keine Theorie ist, lässt sich an einem konkreten Fall nachvollziehen: Im Dossier [TerminalFix und der Berlin-Hack](#) kommt der Köder per Link — und zwar über einen Weg, den ein reines Anhangsscanning nie erfasst hätte. Das ist kein exotischer Sonderfall, sondern der Normalfall geworden: Der gefährliche Teil einer Nachricht ist heute meist eine Adresse und keine Datei.

Teams: Prüfung ohne Umschreibung, mit 24 Stunden Anlauf

In Teams werden Adressen nicht umgeschrieben. Geprüft wird beim Klick — in Unterhaltungen, in Gruppenchats, in Kanälen und in angehefteten Registerkarten. Unterstützt werden Desktop, Web und die mobilen Anwendungen für Android und iOS. Wenn du diese Funktion ein- oder ausschaltest, kann es bis zu 24 Stunden dauern, bis die Änderung wirkt. Plane das in einer Testphase ein, sonst hältst du eine funktionierende Konfiguration für kaputt.

Eine Eigenheit ist erwähnenswert: Wird ein Link aus einer angehefteten Registerkarte heraus angeklickt und als schädlich erkannt, erscheint die Warnseite innerhalb von Teams, und das Öffnen im Browser ist aus Sicherheitsgründen deaktiviert. Außerdem gilt der Schutz für die empfangende Seite: Wer selbst nicht von einer Safe-Links-Richtlinie mit Teams-Schutz erfasst ist, kann den Originallink auf dem eigenen Gerät ungehindert öffnen.

Office-Apps: Voraussetzungen, an denen es scheitert

Safe Links in den Office-Apps prüft Adressen in Dokumenten — nicht in Mails. Das ist ein Unterschied, der in Diskussionen gern verrutscht. Ein Link in einer angehängten Präsentation wird also geprüft, sobald jemand die Präsentation öffnet und darauf klickt. Damit das funktioniert, müssen drei Bedingungen erfüllt sein: eine aktuelle Version von Word, Excel, PowerPoint, Visio unter Windows, auf dem Mac, im Browser oder auf Mobilgeräten; moderne Authentifizierung in den Anwendungen; und eine Anmeldung mit dem Geschäfts- oder Schulkonto.

Die dritte Bedingung ist die, an der es in der Praxis scheitert. Wer Office ohne angemeldetes Konto benutzt — auf dem Fertigungsrechner, auf dem Terminalserver eines Dienstleisters, auf dem geteilten Arbeitsplatz in der Werkstatt — ist an dieser Stelle ungeschützt. Das gehört in die Risikobetrachtung und nicht in die Kategorie „läuft schon irgendwie“.

Die Liste der nicht umzuschreibenden Adressen und ihre Tücken

Jede Safe-Links-Richtlinie hat eine Liste von Adressen, die beim Versand nicht umgeschrieben werden. Der übliche Anwendungsfall sind interne Dienste, deren Aufruf über den Umweg des Prüfdienstes Probleme macht. Diese Liste ist nützlich und gleichzeitig eine hervorragende Quelle für Fehlannahmen.

Annahme	Wirklichkeit
„Die Adresse ist freigegeben.“	Sie wird beim Versand nicht geprüft und nicht umgeschrieben. Beim Klick kann sie trotzdem blockiert werden.
„Die Liste gilt überall.“	Teams und die Office-Web-Anwendungen werten sie nicht aus. Dort kann die Adresse weiterhin blockiert werden.
„Die blanke Domäne deckt alles ab.“	Sie deckt genau diese eine Adresse ab. Weder Unterdomänen noch Unterpfade sind mitgemeint.
„Ein Eintrag reicht für die ganze Domäne.“	Für alle Varianten brauchst du zwei Einträge, in der Schreibweise <domäne>/* und *.<domäne>/*.
„Platzhalter kann ich beliebig setzen.“	Höchstens drei Platzhalter je Eintrag. Die Form *<domäne>* lässt auch nachgeahmte Schreibweisen durch — deshalb besser die Form *.<domäne>/*.
„Wenn ich https eintrage, ist http mitgemeint.“	Nur wenn du das Protokoll weglässt. Sonst brauchst du beides — oder handelst dir gegenseitiges Überschreiben ein.

Was die Ausnahmeliste tut — und was nicht

TIPP · Für echte Ausnahmen ist die Mandantenliste der richtige Ort

Wenn eine Adresse wirklich überall unbehelligt bleiben soll, meldest du sie als geprüft sauber und legst über die Meldung einen Zulassungseintrag in der Mandantenliste für erlaubte und blockierte Einträge an. Nur so wird sie beim Versand und beim Klick nicht mehr angefasst. Beachte die Kehrseite: Zulassungseinträge in der Mandantenliste schließen die Adresse nicht von der Umschreibung aus — sie unterdrücken nur das Blockieren.

WARNUNG · Wo Safe Links prinzipbedingt nicht greift

Diese Fälle sind keine Fehler, sondern Grenzen des Verfahrens. Sie gehören in dein Lagebild, damit du im Vorfall nicht nach der falschen Ursache suchst.

- › E-Mail-aktivierte öffentliche Ordner werden nicht abgedeckt.
- › Nur http, https und ftp werden verarbeitet.
- › Nachrichten im Rich-Text-Format (TNEF) bleiben ungeschützt.
- › S/MIME-signierte Nachrichten werden übergangen.
- › Adressen auf SharePoint und OneDrive werden nicht mehr umgeschrieben, aber weiterhin geprüft — das ist eine Verbesserung der Ladezeit, kein Schutzverlust.
- › Wenn ein vorgelagerter Dienst die Links bereits verpackt, kann Safe Links sie unter Umständen gar nicht mehr bewerten.

Der letzte Punkt verdient Nachdruck, weil er teuer ist. Wer vor Exchange Online noch ein fremdes E-Mail-Gateway betreibt, das seinerseits Links umschreibt, bezahlt für Safe Links und bekommt im schlechtesten Fall nichts dafür. Die Entscheidung, welches System die Links verpackt, ist keine Geschmacksfrage, sondern eine Architekturentscheidung — und sie gehört auf den Tisch, bevor jemand Preset-Richtlinien zuweist.

Klick-Protokoll: was du forensisch wirklich in der Hand hast

Die Einstellung „Klicks protokollieren“ ist in allen Profilen eingeschaltet, und sie ist der Grund, warum du nach einem Vorfall überhaupt etwas sagen kannst. Ohne sie hast du eine Liste von Empfängern. Mit ihr hast du eine Liste derer, die tatsächlich geklickt haben — und derer, die sich über die Warnseite hinweggesetzt haben.

Die Daten landen in der erweiterten Suche in der Tabelle `UrlClickEvents`. Sie erfasst Klicks aus E-Mail, aus Teams und aus den Office-Apps, sauber getrennt über die Spalte `Workload`. Für die Aufarbeitung sind vier Spalten entscheidend: `AccountUpn` sagt dir wer, `ThreatTypes` sagt dir das Urteil zum Zeitpunkt des Klicks, `IsClickedThrough` sagt dir, ob jemand trotz Warnung weitergegangen ist, und `NetworkMessageId` verbindet den Klick mit der Nachricht, sodass du über die E-Mail-Tabellen an alle weiteren Empfänger kommst.

```
// Wer ist trotz Warnung weitergegangen?
UrlClickEvents
| where Timestamp > ago(7d)
| where ActionType == "ClickAllowed" or IsClickedThrough != "0"
| where ThreatTypes has "Phish"
| summarize by ReportId, IsClickedThrough, AccountUpn,
    NetworkMessageId, ThreatTypes, Workload, Timestamp
```

Diese Abfrage ist der erste Griff in den ersten Minuten eines Vorfalls, weil sie die Frage „wen müssen wir jetzt anrufen“ in Sekunden beantwortet. Wie es danach weitergeht — Sitzungen beenden, Kennwörter zurücksetzen, Posteingangsregeln prüfen, Weiterleitungen suchen — steht in [Phishing-Vorfall: die ersten 60 Minuten](#) und für den Fall, dass es ein Konto tatsächlich erwisch hat, in [Kompromittiertes Konto erkennen und aufräumen](#).

Eine Einschränkung solltest du kennen: Bei Klicks aus Entwürfen und aus gesendeten Elementen fehlen die Nachrichtendaten oder die Kennung wird pauschal vergeben. Eine Verknüpfung mit den E-Mail-Tabellen über NetworkMessageId funktioniert dann nicht. Und die Spalte ReportId ist bei Durchklick-Vorgängen für beide Ereignisse identisch — genau deshalb eignet sie sich zur Korrelation.

WICHTIG · Klick-Protokolle sind personenbezogene Verhaltensdaten

Eine Tabelle, die festhält, wer wann welche Adresse angeklickt hat, ist eine technische Einrichtung, die zur Verhaltens- oder Leistungskontrolle geeignet ist. Ob sie dazu eingesetzt werden soll, ist unerheblich — die Eignung genügt. Das gehört vor der Einführung auf den Tisch des Betriebsrats, zusammen mit einer klaren Zweckbindung und einem Löschkonzept.

- › Regelt üblicherweise: Wer darf abfragen, zu welchem Anlass, mit welcher Aufbewahrungsfrist, und was ist ausdrücklich untersagt.
- › Ein sauber verhandelter Rahmen ist kein Hindernis, sondern die Voraussetzung dafür, dass du die Daten im Ernstfall überhaupt benutzen darfst.

Welche Überwachungsfunktionen in Microsoft 365 mitbestimmungspflichtig sind und wie eine Betriebsvereinbarung aussieht, die beide Seiten trägt, ist ein eigenes Thema: [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#). Wenn du die Auswertung darüber hinaus in ein zentrales System überführen willst, lohnt der Blick auf [Microsoft Sentinel anbinden: wann es sich lohnt](#).

Zusammenarbeit, ZAP und Quarantäne: die Schichten nach der Zustellung

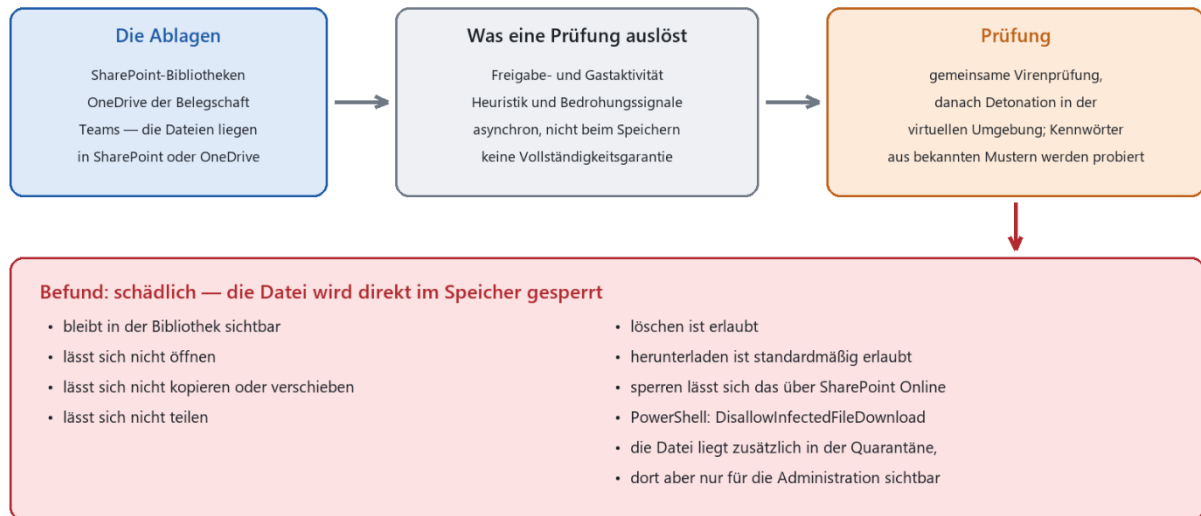
Der klassische Blick auf E-Mail-Sicherheit endet mit der Zustellung. Das ist ungefähr so zeitgemäß wie ein Faxgerät im Empfang. Die interessanten Bewegungen finden danach statt: Dateien werden in Teams geteilt, Bedrohungen werden nachträglich erkannt, und irgendwo sitzt jemand vor einer Quarantäne-Benachrichtigung und überlegt, ob er auf „Freigeben“ drückt.

Safe Attachments für SharePoint, OneDrive und Teams

Diese Funktion ist global geschaltet und hängt an keiner Safe-Attachments-Richtlinie. In Built-in Protection ist sie eingeschaltet. Sie prüft Dateien in den Ablagen, und weil Teams seine Dateien in SharePoint und OneDrive ablegt, deckt sie Teams gleich mit ab.

Safe Attachments für SharePoint, OneDrive und Teams

Nicht jede Datei wird geprüft — und genau das ist der Punkt, den man kennen sollte



Der Sperrhinweis erscheint nur in der modernen SharePoint-Oberfläche — in klassischen Seiten sieht niemand, dass etwas blockiert wurde.

Skizze 4: Wie Dateien in den Ablagen geprüft werden — und was eine Sperre praktisch bedeutet.

Der wichtigste Satz zu dieser Funktion steht in der Dokumentation erfreulich unverblümt: Es wird nicht jede Datei geprüft, und das ist so gewollt. Die Prüfung läuft asynchron und wird über Freigabeereignisse, Gastaktivität, Heuristik und Bedrohungssignale ausgelöst. Wer daraus einen vollständigen Virenschutz für die Dateiablage ableitet, hat sich verlesen. Es ist eine zusätzliche Schicht, keine Garantie.

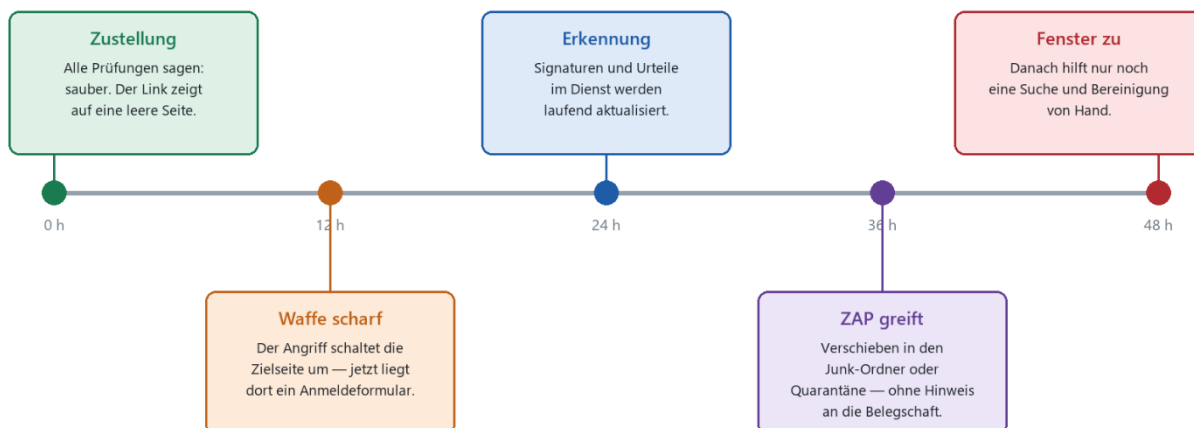
Zwei Punkte solltest du aktiv einstellen. Erstens: Eine gesperrte Datei lässt sich standardmäßig weiterhin herunterladen. Das Verhalten änderst du in der SharePoint-Verwaltung über PowerShell mit der Einstellung DisallowInfectedFileDownload — Microsoft empfiehlt das ausdrücklich. Zweitens: Der Sperrhinweis erscheint nur in der modernen Oberfläche. Wer noch klassische Seiten betreibt, sieht nichts. Wenn ohnehin gerade Freigaben und Gastzugriffe auf dem Tisch liegen, gehört das Thema in dieselbe Runde wie [Gastzugriff und externe Freigaben härten](#).

ZAP: das 48-Stunden-Fenster

Zero-hour Auto Purge räumt nachträglich auf. Der Dienst beobachtet laufend neue Signaturen und Urteile und wendet sie rückwirkend auf bereits zugestellte Nachrichten an. Das Suchfenster umfasst die letzten 48 Stunden. Die betroffenen Personen werden nicht benachrichtigt — die Nachricht ist einfach weg beziehungsweise woanders.

Das 48-Stunden-Fenster: was ZAP nachträglich noch regelt

Bedrohungen, die zum Zeitpunkt der Zustellung noch keine waren



ZAP wirkt nur in Postfächern in Exchange Online. Für Teams braucht es Defender for Office 365 — und dort trifft es sämtliche Beteiligten eines Chats gleichzeitig.

Skizze 5: Zeitversetzt scharfgeschaltete Angriffe und das Fenster, in dem ZAP sie noch einfängt.

Was ZAP tut, hängt vom Urteil ab. Schadsoftware und sicher erkannter Phishing-Versuch landen in der Quarantäne, unabhängig davon, ob die Nachricht schon gelesen wurde. Bei Spam und einfachem Phishing richtet sich die Aktion nach der Einstellung in deiner Anti-Spam-Richtlinie: Steht dort „in den Junk-Ordner verschieben“, verschiebt ZAP; steht dort „in Quarantäne“, isoliert ZAP; steht dort etwas anderes, tut ZAP nichts. Deshalb wirkt Strict auch hier schärfer als Standard.

FAKTEN · ZAP in Zahlen und Grenzen

Die Eckdaten, die du in einer Besprechung parat haben solltest:

- › Suchfenster: die letzten 48 Stunden nach der Zustellung.
- › Wirkt nur in Postfächern in Exchange Online — nicht in Postfächern, die weiterhin lokal betrieben werden.
- › Wirkt auch im Ordner „Gelöschte Elemente“ und in anderen Ordnern, solange die Nachricht nicht gelöscht ist.
- › Für E-Mail keine besondere Lizenz nötig; für Teams braucht es Defender for Office 365.
- › ZAP wird nicht im Postfachüberwachungsprotokoll als Systemaktion festgehalten — sichtbar wird es im Berichtswesen und im Explorer.
- › In Teams-Chats trifft die Sperre alle Beteiligten gleichzeitig, weil es keine Vervielfältigung der Nachricht gibt.

Es gibt Konstellationen, in denen ZAP bewusst nichts tut: bei Zulassungslisten, bei Transportregeln, bei Adressen aus fremden Phishing-Simulationen in der erweiterten Zustellungsrichtlinie, bei eigens eingerichteten Sicherheitspostfächern und dann, wenn der MX-Eintrag deiner Domäne auf ein vorgelagertes System zeigt und eine Transportregel die Filterung umgeht. Diese Ausnahmen sind sinnvoll — und jede einzelne von ihnen ist ein Loch, das jemand kennen und verantworten muss.

Quarantäne-Richtlinien: wer darf was herausholen

Die Quarantäne ist der Ort, an dem Sicherheit auf Alltag trifft. Quarantäne-Richtlinien legen fest, was die Belegschaft mit den eigenen isolierten Nachrichten tun darf und ob überhaupt eine Benachrichtigung verschickt wird. Das ist keine Nebensache: Eine scharfe Filterung ohne Benachrichtigung erzeugt zuverlässig den Eindruck, das E-Mail-System sei kaputt.

Richtlinie	Was die Belegschaft darf	Typischer Einsatz
AdminOnlyAccessPolicy	Nichts. Nur die Administration sieht und verwaltet die Nachrichten.	Schadsoftware, sicher erkannter Phishing-Versuch, Funde von Safe Attachments
DefaultFullAccessPolicy	Ansehen, freigeben, löschen — aber ohne Benachrichtigung.	Spam und Massensendungen im Standard-Profil
DefaultFullAccessWithNotificationPolicy	Wie oben, zusätzlich mit periodischer Benachrichtigung.	Standard bei sicherem Spam und Phishing; im Strict-Profil durchgängig
Eigene Richtlinie mit eingeschränktem Zugriff	Alles außer eigenständiger Freigabe — die muss beantragt und genehmigt werden.	Der praktische Mittelweg für Häuser mit knapper Betreuung

Die eingebauten Quarantäne-Richtlinien und ihre Wirkung

Zwei Regeln lassen sich durch keine Konfiguration aushebeln: Nachrichten, die als Schadsoftware oder als sicher erkannter Phishing-Versuch isoliert wurden, kann die betroffene Person nie selbst freigeben. Sie kann die Freigabe höchstens beantragen, wenn die Richtlinie das vorsieht. Das ist gut so, und es erspart dir eine Diskussion.

Die Benachrichtigung lässt sich alle vier Stunden, täglich oder wöchentlich verschicken. Für die meisten Häuser ist täglich der richtige Wert: oft genug, dass niemand zwei Tage auf eine Bestellbestätigung wartet, selten genug, dass die Nachricht nicht zum Hintergrundrauschen wird. Absenderanzeige, Betreff und ein Hinweistext lassen sich anpassen — nutze das, denn eine Quarantäne-Benachrichtigung, die aussieht wie eine Quarantäne-Benachrichtigung eines Angreifers, ist ein Eigentor mit Ansage.

Anti-Phishing mit Impersonation-Schutz: die Schicht, die niemand einrichtet

Safe Links und Safe Attachments bekommen die Aufmerksamkeit, weil sie Produktnamen haben. Der Impersonation-Schutz bekommt sie nicht und ist bei gezielten Angriffen auf die Geschäftsführung häufig die einzige Schicht, die überhaupt anschlägt. Er kennt drei Verfahren.

- Nachahmung von Personen: Du hinterlegst Absenderadressen, die geschützt werden sollen — Geschäftsführung, Vorstand, Buchhaltungsleitung, extern etwa Beiratsmitglieder. Nachrichten, die diese Namen imitieren, werden erkannt.
- Nachahmung von Domänen: Alle eigenen Domänen werden von den Presets automatisch geschützt. Fremde Domänen, mit denen du häufig zu tun hast — Hausbank, Steuerkanzlei, Hauptlieferant — musst du selbst eintragen.

- Mailbox Intelligence: Der Dienst lernt aus dem tatsächlichen Kommunikationsverhalten, wer mit wem üblicherweise schreibt, und erkennt Abweichungen. Das funktioniert ohne Pflege einer Liste und ist der Grund, warum sich diese Einstellung immer lohnt.

In Standard und Strict werden Personen- und Domännennachahmung isoliert. Der Unterschied liegt bei Mailbox Intelligence: Standard verschiebt in den Junk-Ordner, Strict isoliert. Dazu kommen die Sicherheitshinweise in Outlook — der Hinweis bei erstmaligem Kontakt, die Kennzeichnung nachgeahmter Personen und Domänen und der Hinweis auf ungewöhnliche Zeichen im Namen. Diese Hinweise sind in den Standardrichtlinien ausgeschaltet und in beiden Presets eingeschaltet. Sie kosten nichts und wirken erfahrungsgemäß besser als drei Schulungsfolien.

Der gesamte Spoof-Schutz steht und fällt allerdings mit sauberer Absender-Authentifizierung. Solange deine Domänen keine belastbaren SPF-, DKIM- und DMARC-Einträge haben, arbeitet Defender mit halben Informationen — und deine eigene Domäne bleibt der bequemste Ausgangspunkt für Angriffe auf deine Partner. Die Reihenfolge ist eindeutig: erst [SPF, DKIM, DMARC für Exchange Online](#), dann die Feinjustierung der Bedrohungsrichtlinien.

TIPP • Eine sinnvolle Reihenfolge für die Einführung

Wenn du bei null anfängst, hat sich diese Abfolge bewährt — sie erzeugt früh Wirkung und spät Diskussionen, statt umgekehrt:

- › Absender-Authentifizierung für alle eigenen Domänen fertigstellen, auch für die ungenutzten.
- › Standard-Preset auf eine überschaubare Testgruppe zuweisen, zwei Wochen beobachten.
- › Listen für den Impersonation-Schutz befüllen — Personen und fremde Domänen.
- › Standard-Preset auf das ganze Haus ausweiten.
- › Strict-Preset für die bekannten Zielgruppen nachziehen und die Quarantäne-Betreuung dafür verbindlich klären.
- › Quarantäne-Benachrichtigung einschalten und den Meldeweg für verdächtige Nachrichten bekannt machen.
- › Erst danach über eigene Richtlinien und Ausnahmen reden.

Häufige Fragen

Wir haben schon ein Sicherheitsgateway vor Exchange Online. Brauchen wir Safe Links dann überhaupt?

Fachlich: Du brauchst genau ein System, das Links umschreibt und beim Klick bewertet. Zwei hintereinander sind nicht doppelt so gut, sondern potenziell schlechter, weil das zweite System die bereits verpackten Adressen unter Umständen nicht mehr bewerten kann. Wirtschaftlich: Wenn Defender for Office 365 ohnehin in deiner Lizenz steckt, ist die Frage weniger „brauchen wir Safe Links“ als „wofür bezahlen wir noch das Gateway“. Die Antwort kann durchaus lauten: für Funktionen, die Defender nicht hat. Sie sollte nur ausgesprochen werden.

Verzögert Safe Attachments die Zustellung spürbar?

Die Prüfung dauert typischerweise unter 15 Minuten, meist deutlich kürzer. Spürbar wird das dort, wo Menschen auf eine Nachricht warten und daneben sitzen — Bewerbungsgespräche, Auktionen, Freigabeprozesse mit Fristen. Für diese Fälle gibt es die dynamische Zustellung: Der Text kommt

sofort, die Anhänge folgen. Wichtig ist, dass du die Verzögerung vorher ansprichst. Eine unerklärte Verzögerung von zehn Minuten erzeugt mehr Unterstützungsanfragen als eine angekündigte von dreißig.

Können wir Strict einfach für alle einschalten?

Technisch ja. Praktisch entscheidet die Frage, ob jemand die Quarantäne durchsieht. Strict isoliert Spam und Massensendungen, die unter Standard nur in den Junk-Ordner wandern würden. Ohne Betreuung fehlen Rechnungen, Newsletter mit Terminen und Bewerbungen — und die Belegschaft entwickelt kreative Umgehungswege. Die belastbare Variante: Standard für alle, Strict für die erkennbaren Zielgruppen, dazu eingeschaltete Quarantäne-Benachrichtigungen.

Sehen wir in der Mail noch die echte Adresse, wenn Safe Links umschreibt?

Ja. Beim Überfahren mit der Maus wird die Originaladresse angezeigt, und die Ansicht bleibt lesbar. Die umgeschriebene Adresse findest du im Quelltext der Nachricht. Für Adressen auf SharePoint und OneDrive wird ohnehin nicht mehr umgeschrieben, obwohl weiterhin geprüft wird — das ist eine reine Verbesserung der Ladezeit.

Was passiert, wenn Safe Links den Dienst nicht erreichen kann?

Es gibt zwei Verhaltensweisen, und du solltest beide kennen. Wenn beim Lesen der Richtlinienkonfiguration in bestimmten Anwendungen ein Fehler auftritt, greift der Schutz nicht und die Person landet direkt beim Ziel. In den Office-Desktopanwendungen wird gewarnt, bevor es weitergeht. Ein Schutz, der offen ausfällt, ist nicht angenehm — er ist aber ehrlicher als einer, der stillschweigend sämtliche Links blockiert und dein Haus lahmlegt.

Zählt Defender for Office 365 für die Nachweise nach NIS2?

Preset-Richtlinien, Klick-Protokolle und Quarantäne-Vorgänge sind gute Belege für die Wirksamkeit technischer Maßnahmen gegen Angriffe per E-Mail — sie decken ein Feld ab, das in jeder Anforderungsliste steht. Sie ersetzen weder ein Informationssicherheitsmanagement noch die Meldeprozesse. Was technisch tatsächlich zählt und wie du es dokumentierst, steht in [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#).

Wie messen wir, ob das alles etwas bringt?

Drei Kennzahlen tragen: die Zahl der blockierten Klicks im Verhältnis zu den Gesamtklicks, die Zahl der Durchklick-Vorgänge über die Warnseite — die in Standard und Strict null sein sollte, weil die Möglichkeit abgeschaltet ist — und die Zeit von der Meldung einer verdächtigen Nachricht bis zur Bereinigung. Der Secure Score liefert dazu eine ergänzende Außensicht, ist aber keine Zielgröße an sich; die Einordnung steht in [Secure Score: sinnvoll nutzen statt Punktejagd](#). Wie du daraus eine Darstellung für die Leitungsebene machst, steht in [Security-Reporting für die Geschäftsführung](#).

Fazit

Defender for Office 365 ist eines der wenigen Sicherheitsprodukte, bei denen der Abstand zwischen „lizenziert“ und „wirksam“ mit überschaubarem Aufwand zu schließen ist. Es braucht keine Projektstruktur und keine externe Ausschreibung. Es braucht eine Nachmittagssitzung, in der jemand die Preset-Richtlinien zuweist, die Listen für den Impersonation-Schutz befüllt und die Quarantäne-Benachrichtigung einschaltet.

Die drei Punkte, die den größten Unterschied machen, sind unspektakulär. Erstens: Weg vom stillen Sockel, hin zu Standard — allein weil damit das Durchklicken an der Warnseite endet und interne Nachrichten mitgeprüft werden. Zweitens: Die Listen für den Impersonation-Schutz pflegen, denn ohne sie läuft der teuerste Teil des Schutzes leer. Drittens: Die Quarantäne betreuen, sonst erzieht dein Schutz die Belegschaft zu Umgehungswegen.

Und dann bleibt der unbequeme Rest. Safe Links prüft beim Klick, aber es entscheidet nicht anstelle des Menschen. ZAP räumt 48 Stunden lang auf, danach nicht mehr. Safe Attachments prüft in den Ablagen nicht jede Datei, und das steht so in der Dokumentation. Diese Grenzen zu kennen ist kein Defätismus, sondern die Voraussetzung dafür, dass du im Vorfall die richtigen Fragen stellst — statt darauf zu warten, dass ein Produkt etwas tut, das es nie versprochen hat.

Wenn du die Zuweisung, die Ausnahmen und die Betriebsübergabe nicht nebenbei erledigen willst, ist das ein typischer Fall für eine begleitete Umsetzung — Bestandsaufnahme, Zuweisung, Testphase, Übergabe: [Microsoft 365 Security — Beratung](#). Wenn die Belegschaft und das eigene Team das Handwerkszeug dafür aufbauen sollen, passt eher die [Schulung Microsoft 365 Security](#).

Passend weiterlesen

- › [Phishing-Vorfall: die ersten 60 Minuten](#) — wenn die Prüfung beim Klick zu spät kam
- › [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#) — die Übung zum Ernstfall, ab Plan 2
- › [TerminalFix und der Berlin-Hack](#) — ein durchgespielter Fall, bei dem der Köder per Link kommt
- › [SPF, DKIM, DMARC für Exchange Online](#) — die Grundlage, ohne die der Spoof-Schutz halbiert arbeitet
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — bevor du Klick-Protokolle auswertest
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — wo dieses Handlungsfeld im Gesamtbild sitzt
- › [Alert Policies und Benachrichtigungen richtig aufsetzen](#) — damit ein Fund nicht in einem ungelesenen Postfach endet
- › [Incident-Response-Plan für Microsoft 365](#) — der Rahmen, in den die Nacharbeit gehört