/ MAURISEC.DE

FIELD NOTES / CHECKLIST 04

Microsoft 365: Mail- und Phishing-Schutz nachweisen

PRUEFEN. BELEGEN. NACHHALTEN.

Für Exchange-Online-Organisationen. Verfügbare Defender-Funktionen, Lizenzen, Mailwege und externe Versanddienste zuerst erfassen. Schutzänderungen anhand legitimer und kontrollierter verdächtiger Nachrichten testen. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Akzeptierte Domänen und sämtliche legitimen Versandquellen einschließlich externer Dienste erfassen.**

  Nachweis: Verantwortete Domänen- und Versandmatrix mit Beispieldaten je Mailweg.

- [ ] **02 / SPF und DKIM für die jeweiligen Versandwege korrekt einrichten und an zugestellten Nachrichten prüfen.**

  Nachweis: DNS-Abfragen und Authentication-Results-Header; keine Bewertung nur anhand vorhandener DNS-Einträge.

- [ ] **03 / DMARC-Ausrichtung und Berichte auswerten; eine strengere Richtlinie erst nach Prüfung legitimer Absender einführen.**

  Nachweis: DMARC-Ergebnisse, Ausrichtungsnachweise und dokumentierter Rollout.

- [ ] **04 / Standard- beziehungsweise Strict-Preset oder entsprechend überprüfte Einzelrichtlinien mit richtiger Zielgruppe einsetzen.**

  Nachweis: Angewandte Richtlinien, Priorität, Ausnahmen und Testzustellungen.

- [ ] **05 / Spoof-Erkennung und, sofern verfügbar, Identitäts- und Domänen-Imitationsschutz prüfen.**

  Nachweis: Konfiguration, geschützte Identitäten und kontrollierte Prüffälle.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 04

- [ ] **06 / Safe Links und Safe Attachments entsprechend vorhandener Berechtigung und unterstütztem Szenario testen.**

  Nachweis: Wirksame Zuweisung, Verarbeitungsnachweise und dokumentierte Einschränkungen.

- [ ] **07 / Automatische externe Weiterleitung ausdrücklich nach Organisationsvorgabe steuern und vorhandene Weiterleitungen prüfen.**

  Nachweis: Outbound-Spam-, Remote-Domain- und Mailflow-Regeln sowie ein freigegebener Weiterleitungstest.

- [ ] **08 / Nutzermeldungen, Quarantäneprüfung und Bearbeitung verdächtiger Nachrichten mit Verantwortlichkeit erproben.**

  Nachweis: Gemeldeter Testfall, Bearbeitungsentscheidung und Rückmeldung an die meldende Person.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Eine harmlose autorisierte Testnachricht und den Meldeweg verwenden; Empfängerwirkung und zuständige Reaktion dokumentieren, keine Schadsoftware einsetzen.

GRENZEN UND VORAUSSETZUNGEN

SPF allein schützt den sichtbaren From-Absender nicht vollständig. DMARC bewertet Ausrichtung; es verhindert keine bereits kompromittierten legitimen Absender. Nicht jede Funktion ist in jedem Paket vorhanden. 'Automatic/System-controlled' bei externer Weiterleitung nicht pauschal als garantiertes Blockieren behandeln; den gewünschten Zustand explizit festlegen. Ausnahmen und Allow-Listen können Schutz schwächen.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Email authentication
learn.microsoft.com

Microsoft Learn: Anti-phishing policies
learn.microsoft.com

Microsoft Learn: Submit and review messages
learn.microsoft.com

Microsoft Learn: Recommended threat policy settings
learn.microsoft.com

Microsoft Learn: External email forwarding
learn.microsoft.com