Schutz der Domain- und E-Mail-Reputation

Diese Checkliste wurde entwickelt, um IT-Administratoren dabei zu unterstützen, die E-Mail-Kommunikation ihrer Domain mithilfe von SPF, DKIM und DMARC abzusichern.

Diese Authentifizierungsprotokolle stellen sicher, dass E-Mails Ihrer Organisation nicht gefälscht oder manipuliert werden, und schützen die Reputation Ihrer Domain, indem sie den Absender verifizieren und Phishing- oder Spam-Angriffe verhindern.

 # 1. Einrichtung von SPF (Sender Policy Framework)

☐ Definieren Sie, welche Mailserver berechtigt sind, E-Mails im Namen Ihrer Domain zu senden.
☐ Aktualisieren Sie die DNS-Einträge Ihrer Domain mit einem SPF-Eintrag (z. B. v=spf1 include:_spf.google.com ~all).
☐ Testen und validieren Sie Ihren SPF-Eintrag mit Tools wie dem Google Admin Toolbox.

 # 2. Einrichtung von DKIM (DomainKeys Identified Mail)

☐ Aktivieren Sie die DKIM-Signierung in der Google Workspace Admin-Konsole.
☐ Generieren Sie DKIM-Schlüssel und fügen Sie den öffentlichen Schlüssel in die DNS-Einträge Ihrer Domain ein.
☐ Stellen Sie sicher, dass die DKIM-Signierung aktiviert ist, und prüfen Sie, ob ausgehende E-Mails signiert werden.

 # 3. Einrichtung von DMARC (Domain-based Message Authentication, Reporting, and Conformance)

☐ Erstellen Sie eine DMARC-Richtlinie, um festzulegen, wie E-Mail-Provider mit nicht authentifizierten E-Mails umgehen (z. B. ablehnen, unter Quarantäne stellen oder nichts tun).
☐ Aktualisieren Sie die DNS-Einträge mit einem DMARC-Eintrag (z. B. v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com).
☐ Überwachen Sie DMARC-Berichte, um nicht authentifizierte E-Mails zu bewerten und Ihre Richtlinien anzupassen.

 # 4. Testen und Überwachen der E-Mail-Authentifizierung

☐ Verwenden Sie Tools zum Testen der E-Mail-Authentifizierung, um zu bestätigen, dass SPF, DKIM und DMARC korrekt konfiguriert sind.
☐ Überprüfen Sie regelmäßig DMARC-Berichte, um unautorisierte Sendequellen zu identifizieren und Richtlinien bei Bedarf anzupassen.

Brauchen Sie beim nächsten Schritt Hilfe?

Wenn Sie zu einem dieser Schritte eine Frage haben oder Hilfe beim Einrichten einer fortgeschritteneren oder maßgeschneiderten Lösung benötigen, sind wir für Sie da!

Senden Sie uns einfach eine E-Mail an contact@403bits.com.

Bei einfacheren Fragen geben wir Ihnen gerne Ratschläge oder weisen Sie in die richtige Richtung – kostenlos!

Und wenn Sie vor einer komplexeren Herausforderung stehen oder Zeit sparen möchten, können unsere Experten übernehmen und eine umfassende Einrichtung bereitstellen, die perfekt zu Ihren Anforderungen passt.

Wir sind hier, um Ihnen beim Aufbau von Sicherheit und Effizienz zu helfen, damit Sie sich auf das Wachstum Ihres Unternehmens konzentrieren können!

Wenn Ihnen diese Checkliste gefallen ist oder Sie Verbesserungsvorschläge haben, lassen Sie es uns unter contact@403bits.com wissen.