NACHRICHTEN
Österreich

E-Mail-Sicherheit auf dem Prüfstand: So schützen Sie sich vor Betrug!

Am 9.01.2025 erläutert der Artikel die Bedeutung von E-Mail-Authentifizierung und gesetzlichen Anforderungen für sichere E-Mail-Kommunikation.

** Deutschland ** - Am 9. Januar 2025 berichtete **ZDF** von einem Problem bei der Eingabe von Anmeldedaten. Dabei traten verschiedene Fehler auf, die eine erfolgreiche Registrierung verhinderten. Benutzer mussten die Schreibweise ihrer Eingaben überprüfen, einen Anzeigenamen auswählen und sicherstellen, dass ihr Benutzername maximal 256 Zeichen lang war. Zudem war die Eingabe einer gültigen E-Mail-Adresse erforderlich.

Fehler in der Eingabe von E-Mail oder Passwort führten häufig zu einer unvollständigen Registrierung. Die E-Mail-Adresse musste ein „@“ enthalten und zu einer existierenden Domain gehören, wie beispielsweise zdf.de. Auch die Anforderungen an das Passwort waren strenger: Es musste mindestens 8 Zeichen lang sein und jeweils einen Groß- und Kleinbuchstaben sowie eine Zahl enthalten. Zudem war die Zustimmung zu den Nutzungsbedingungen und der Datenschutzerklärung zwingend notwendig, um die Registrierung abzuschließen.

Anforderungen an die E-Mail-Authentifizierung

Darüber hinaus thematisierte **AdGuard** die Bedeutung der E-Mail-Authentifizierung. Dieser technische Prozess dient der Überprüfung der Authentizität von E-Mail-Absendern und

-Inhalten und wird auch als E-Mail-Validierung bezeichnet.

Richtig konfiguriert kann die E-Mail-Authentifizierung betrügerische Aktivitäten wie Spoofing, Phishing und Fälschung effektiver blockieren. E-Mails sind heutzutage anfällig für eine Vielzahl von Angriffen, darunter Phishing-Attacken, wo Cyberkriminelle versuchen, sensible Daten von Nutzern zu stehlen, indem sie sich als legitime Institutionen ausgeben.

- Phishing-E-Mails
- Spoofing – Fälschen der Absenderadresse
- Mit Malware infizierte E-Mails
- Business Email Compromise (BEC)
- E-Mail-Antwortkettenangriffe
- Whaling-Angriffe auf hochrangige Personen

Wichtige Methoden zur E-Mail-Authentifizierung umfassen das Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) und Domain-based Message Authentication, Reporting & Conformance (DMARC). Diese Technologien tragen dazu bei, die Sicherheit von E-Mails zu erhöhen, die Zustellbarkeit zu verbessern und den Missbrauch von Domains zu verhindern. E-Mail-Authentifizierung ist somit eine grundlegende Praxis zum Schutz sensibler Informationen.

– Übermittelt durch **West-Ost-Medien**

Details	
Ort	Deutschland
Quellen	• **www.zdf.de** • **adguard.com**

Besuchen Sie uns auf: die-nachrichten.at