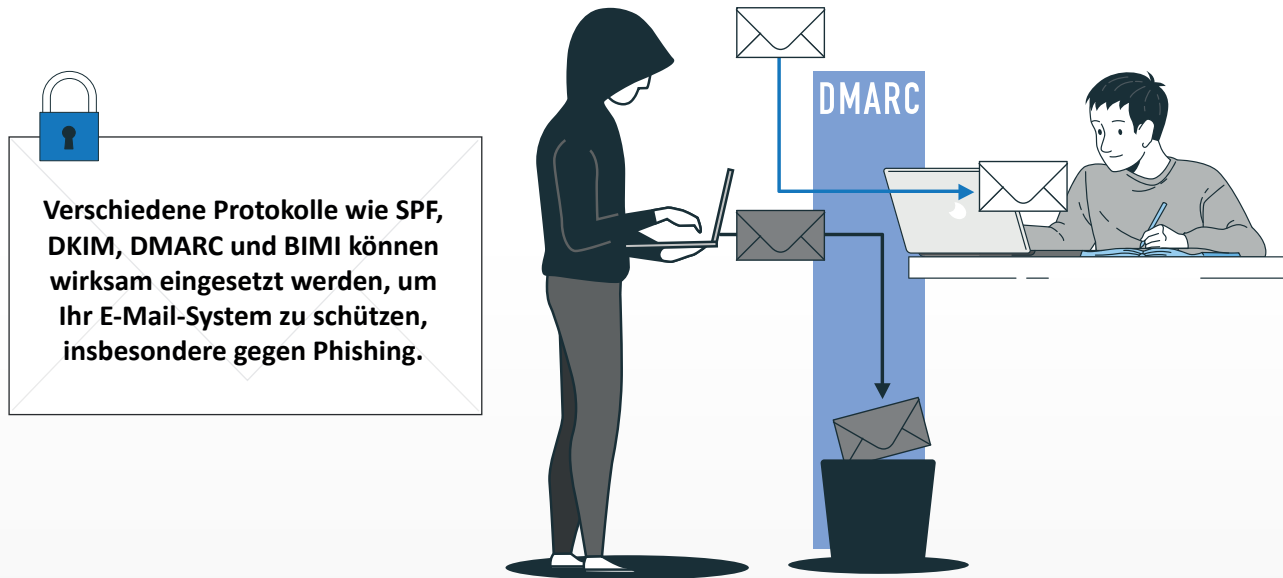


Sichern Sie Ihr E-Mail-System ab – mit DMARC

Die E-Mail ist der wichtigste Kommunikationskanal in Unternehmen - gleichzeitig jedoch auch das am häufigsten genutzte Einfallstor für Cyberangriffe, mit verheerenden Folgen für die betroffenen Unternehmen und Behörden.



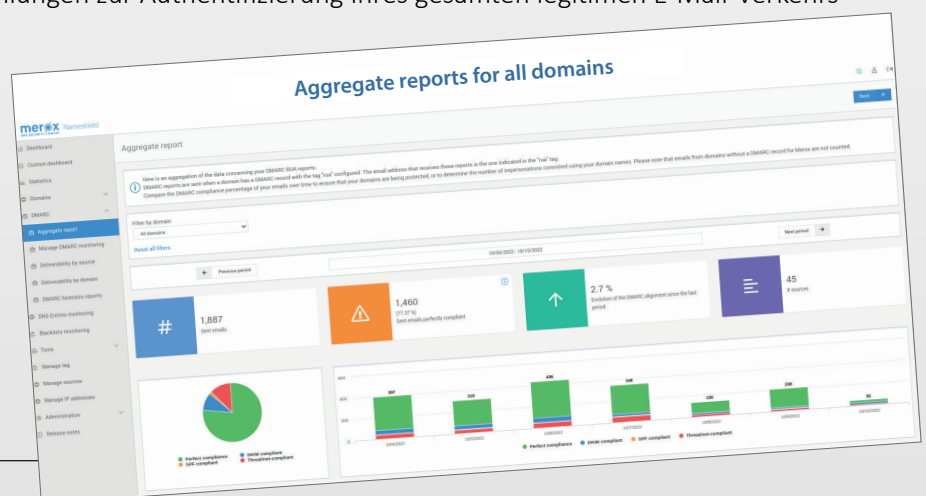
Warum ist die Konformität mit der DMARC Norm sinnvoll?

- Verhinderung von Spoofing der für den E-Mail-Versand verwendeten Domains und Schutz geparkter Domains, die allzu oft vergessen werden
- Verbesserung der Zustellbarkeit von E-Mails: Wenn der E-Mail-Verkehr ordnungsgemäß organisiert und authentifiziert ist, werden Ihre E-Mails von Webmailern und Anti-Spam-Systemen als zuverlässiger eingestuft
- Implementierung von BIMI, wodurch Ihr Markenlogo in den Postfächern der Empfänger angezeigt werden kann

Unterstützung durch Nameshield für Ihre Bedürfnisse

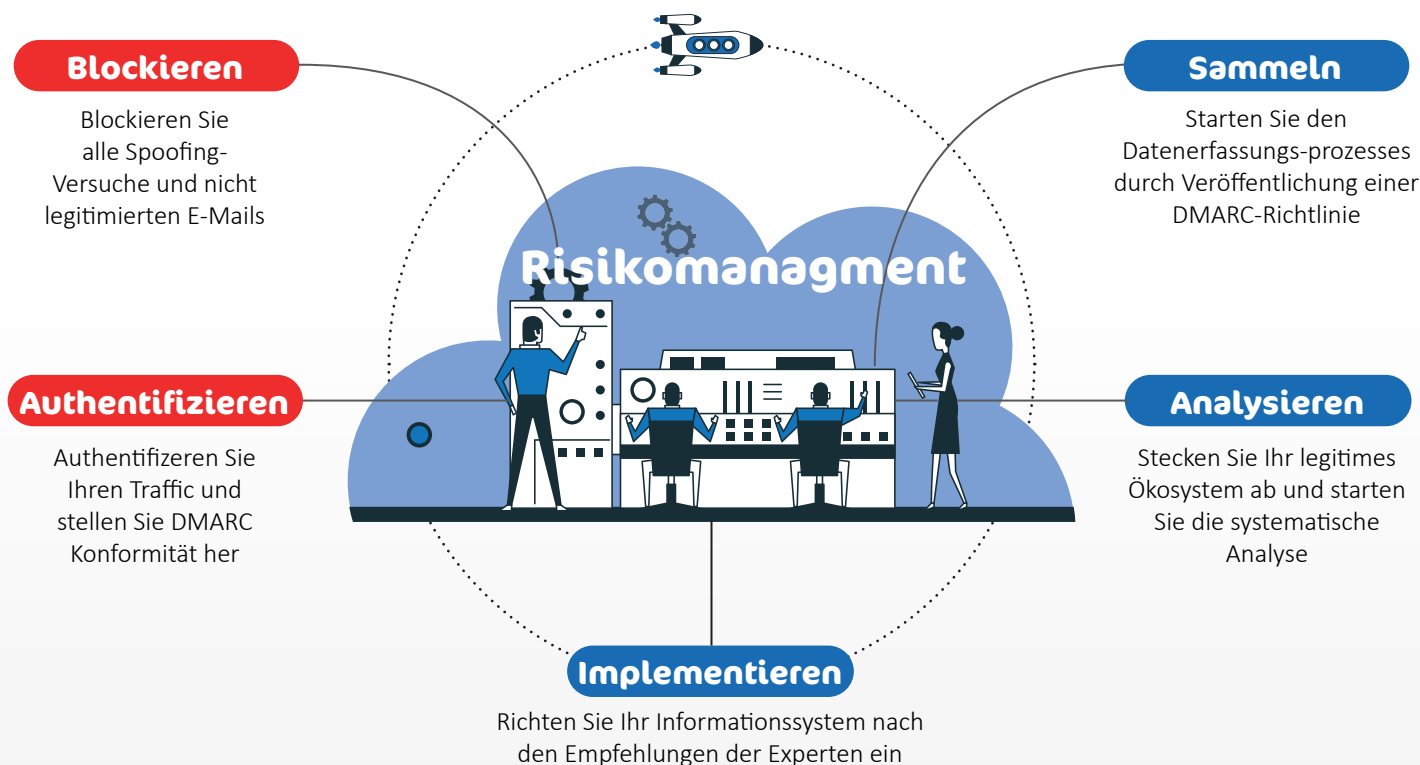
- Einrichtung der Merox Plattform
- Unterstützung bei der Veröffentlichung einer DMARC-Richtlinie für Ihre Domains
- SPF-Überprüfung (Gültigkeit der Syntax, IP-Liste, veraltete oder leere Werte, ...)
- Empfehlung der bestmöglichen E-Mail-Strategie in Bezug auf die Verwendung von Domains, mit dem Ziel das Risiko von Angriffen zu minimieren
- Analyse Ihrer RUA-Berichte und Empfehlungen zur Authentifizierung Ihres gesamten legitimen E-Mail-Verkehrs mit DKIM und SPF
- Unterstützung bei der Aktualisierung der DMARC-Richtlinie, bis 100 % der E-Mails «p=reject» erreichen
- Nachverfolgung von ungewöhnlichem Verhalten und Phishing-Versuchen

Merox platform



DMARC - eine simple Lösung

damit Administratoren schnell Erfolg erzielen



So stellen Sie DMARC Konformität her

1. Die Header From-Domain (für den Empfänger sichtbare Domain) muss mit der SPF-Domain (Envelope-Domain) und/oder der DKIM-Domain übereinstimmen (d=)
2. Die SPF- und/oder DKIM-Authentifizierung muss gültig sein (zusätzlich zur Ausrichtung)

Mit DMARC kann der Inhaber der sendenden Domäne festlegen, welche Maßnahmen auf der Empfängerseite (Webmail oder Anti-Spam des Empfängers) ergriffen werden sollen, wenn er nicht konforme, eingehende E-Mails sieht

3 Policies sind möglich

- Keine Vorgabe → der Domaininhaber überlässt dem Webmail/Anti-Spam-System des Empfängers die Wahl, ob die E-Mails akzeptiert, in den Spam-Ordner verschoben oder abgewiesen werden sollen
- Quarantäne → der Besitzer der Domain gibt dem Webmail/Anti-Spam des Empfängers an, dass E-Mails, die nicht DMARC-konform sind, wenn möglich in Quarantäne oder in den Spam-Ordner verschoben werden sollen
- Ablehnen → Der Inhaber der Domain teilt dem Webmail/Anti-Spam des Empfängers mit, dass E-Mails, die nicht DMARC-konform sind, abgelehnt (gebounce) werden sollen

