기업을 위한 DMARC 설정 방법

기업체에서 상표 표기 인증서 (VMC)를 발급받을 수 있기 전에, 해당 기업체는 먼저 DMARC (도메인 기반의 메시지 인증, 보고 및 준수)를 준수해야 합니다. 이 안내서를 통해, 기업체에서 DMARC를 올바르게 실행하는데 필요한 방법을 소개하고자 합니다.

digicert®

digicert®

DMARC란 무엇인가?

DMARC는 사칭 및 피싱 공격을 비롯하여 도메인의 무단 사용을 방지하도록 지원하는 기업체를 위한 이메일 인증, 정책 및 보고 프로토콜입니다.

기본적인 요약은 다음과 같습니다.

- DMARC는 DNS에 저장된 TXT 기록이며, 이를 통해 이메일 수신자는 수신된 이메일의 진본 여부를 확인할 수 있습니다.
- 이는 기업체에 이미 존재하는 인바운드 인증 프로세스에 꼭 맞도록 설계되어, 이메일 수신자가 발신자에 관해 알아야 하는 정보와 메시지가 "일치"하는지 여부를 판별하도록 지원합니다.
- 기업체는 3가지 정책 옵션을 통해 "일치하지 않는" 메시지를 취급할 수 있습니다.

- "p = 없음" (시행하지 않음)
- "p = 격리"
- "p = 거부"

- DMARC가 효과적으로 작동하려면, 발신자 정책 프레임워크 (SPF) 및 도메인 키 식별 메일 (DKIM) 프로토콜을 사전에 설정해야 합니다.
- 기업체의 DMARC 기록은 기존의 인터넷 기반 "툴"을 통해 확인할 수 있습니다 - valimail.com 에서 확인 가능한 이것처럼 말이죠.

DMARC로 보다 효과적인 인증 확인

DMARC의 목표는 발신자의 메일 인증 방법을 개선하고 수신자가 인증되지 않은 메시지를 거부하도록 상호 협조가 가능한 발신자 및 수신자 시스템을 구축하는 것입니다.

digicert®

왜 DMARC인가?

DMARC를 실행하면, 기업체는 4가지 이점을 확보할 수 있습니다.

1. 보안

이메일 도메인의 무단 사용을 차단하여 스팸, 사기 및 피싱으로부터 보호합니다.

2. 가시성

인터넷 전반에 걸쳐 귀사의 도메인을 사용하여 이메일을 발송하는 자 및 그 내용에 관해 상세한...에 관해 상세한 보고서를 확보합니다.

3. 전달률

이메일의 전달률을 5-10% 증가시키고, 이메일이 SPAM으로 분류되지 않게 합니다.

4. 브랜드 보호

아이덴티티를 표적으로 한 공격으로부터 브랜드를 방어합니다.

42% 의 고객은 피싱 사기에 도용된 브랜드를 다시 찾기를 꺼린다고 합니다.

digicert®

SPF 설정 방법:

1. 귀사의 도메인으로 이메일을 전송하는데 쓰이는 IP 주소를 취합하십시오. 예를 들면:
   - 웹 서버
   - 사무실 내 메일 서버
   - ISP의 메일 서버
   - 제3자 업체의 메일 서버
2. 이메일 발신에 사용하는/사용하지 않는 도메인의 목록을 만드십시오.
3. 텍스트 편집 프로그램 (Notepad ++, Vim, Nano 등)을 사용하여 각 도메인에 대해 .txt로 SPF 기록을 생성하십시오.

   예 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -전부

   예 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -전부
4. SPF를 DNS에 공개하십시오.

   DNS를 직접 관리하는 경우, SPF 텍스트가 포함된 새로운 TXT 기록을 추가하십시오. DNS를 직접 관리하지 않는 경우, 서버 관리자에게 문의하여 기록을 추가하십시오.
5. 이 기록이 DNS에 추가되고 나면, SPF 확인 툴을 사용하여 확인하십시오.

SPF란?

무단 발신자로 인해 큰 손해를 입지 마십시오.

SPF는 도메인 기반 이메일 인증의 컨셉을 개척한 표준입니다. 도메인 소유자는 도메인을 대신하여 이메일을 발송하는 서버의 IP 주소를 자동으로 승인하므로, 스푸핑을 방지할 수 있습니다. 목록에 없는 IP 주소를 갖는 메일 서버에서 해당 도메인을 사용하여 이메일을 발송하려는 경우, PSF 인증을 통과하지 못합니다.

digicert®

DKIM 설정 방법:

1. DKIM 셀렉터를 고르십시오.

단순하고, 사용자 정의 가능한 문자열로 도메인 이름 옆에 붙어서 DKIM 공용 키를 식별할 수 있어야 합니다 (예: "standard").

예: "standard._domain.example.com" = 호스트 이름

2. 해당 도메인에 대한 공개-개인 키 쌍을 생성하십시오.

- Windows 사용자는 PUTTYGen 사용
- Linux 및 Mac 사용자는 ssh-keygen 사용

3. 새 TXT 기록의 생성 및 공개

위의 쌍으로부터 공개 키를 사용하여 DNS 관리 콘솔을 통해 새 기록 생성

예: v=DKIM1; p=YourPublicKey

DKIM이란?

이메일이 전송 도중에 간섭받지 않도록 방지

DKIM은 이메일 메시지에 서명하기 위한 공개/개인 키 암호화를 사용하는 이메일 인증 표준입니다.

DKIM은 이메일이 DKIM 키가 연관되는 도메인으로부터 생성되었고, 해당 이메일은 전송 중에 수정되지 않았다는 점을 검증하는데 사용합니다.

digicert

DMARC 모니터링 모드 설정

1. SPF 및 DKIM을 올바르게 설정
2. DNS 기록 생성

   "txt" DMARC 기록은 "_dmarc.your_domain.com"과 유사한 이름이어야 합니다.

   예: "v=DMARC1;p=none; rua=mailto:dmarcreports@your_domain.com"

   도메인에 대한 DNS를 직접 관리하는 경우, SPF 및 DKIM 기록과 마찬가지로 "p=none" (모니터링 모드) DMARC 기록을 생성하십시오.

   DNS를 직접 관리하지 않는다면, DNS 관리자에게 문의하여 DMARC 기록을 생성하십시오.

3. DMARC 확인 툴을 통해 DMARC 기록 검사

   주: 복제 완료에는 통상 24-48시간이 소요됩니다.
   DMARC 확인 툴

DMARC 모니터링 모드란 무엇인가?

도메인에서 전송되는 내용에 대한 가시성 확보

모니터링 모드를 통해, 도메인 소유자는 도메인에 대한 이메일 트래핑 등을 포함하는 DMARC 보고서를 검토할 수 있습니다.

이 보고서는 DMARC가 완전 시행으로 설정되고 난 후에 격리되거나 거부 처리될 가능성이 있는 메시지를 식별합니다. 또한, DMARC 보고서는 모니터링되는 도메인을 이용하여 이메일을 발송하는 모든 시스템 및 서비스에 관한 정보를 나타냅니다.

유의: 모니터링 모드는 강압적으로 시행되지 않습니다. 인증에 실패한 메일은 정상적으로 전달되므로, DMARC를 실행하는 동안 간섭이 발생하지 않습니다.

digicert®

DMARC .TXT 기록에 사용하는 일반적인 태그

태그 명칭	필수/선택사항	목적
V	필수	프로토콜 버전
P	필수	프로토콜 버전
PCT	선택사항	필터링 대상인 메시지의 %
RUA	선택사항	전체 보고서의 보고 UTI
SP	선택사항	도메인의 부속 도메인을 위한 정책

digicert®

DMARC 보고서가 제공하는 정보는 무엇인가?

이 보고서는 얼마만큼의 사기성 메시지가 해당 도메인을 사용하고 있는지, 어디서 비롯되었는지, 그리고 그것들이 DMARC "격리" 또는 "거부" 정책으로 중지될 수 있는지에 대한 여부를 도메인 소유자에게 표시합니다.

각 수신자의 보고서는 다음의 필드가 포함된 XML 파일입니다.

- 각 IP 주소로부터 받은 메시지의 수
- 표기된 DMARC 정책에 따른 처리 결과
- 해당 메시지에 대한 SPF 결과
- 해당 메시지에 대한 DKIM 결과

XML 보고서는 가독성이 떨어져 불편할 수 있습니다. 도메인 소유자들에겐 Valimail 과 같은 DMARC 보고서 프로세서의 사용을 권고 드립니다.

DMARC 보고서를 사용하는 4가지 방법

시행하기 전에 기준선 확보

1. 적법하지 않다고 표시된 트래픽을 파악하십시오.

2. DMARC에 의해 적법하지 않다고 표시된 적법한 이메일을 찾으십시오. 이런 이메일은 정책에 따라서, 시행하고 난 후에 "거부" 또는 "격리"될 것입니다.

3. 잠재적 시스템/애플리케이션 소유자에게 연락하여 적법하지 않다고 표시된 이메일의 적법성을 명확히 파악하십시오.

4. 필요한 경우, 적법하지만 이전에 포함되지 않았던 IP 주소를 화이트리스트로 작성하여 SPF를 업데이트하십시오.

digicert®

DMARC 보고를 사용하여 시행하기 전에 정리정돈 먼저

DMARC 보고서를 분석하려면 시간이 많이 소요될 수 있습니다. 하지만, 도메인 소유자가 발신자를 간과하거나 잘못 확인하면, DMARC 정책이 시행으로 설정되는 경우에 "양호한" 이메일을 저지하게 되어 ("격리" 또는 "거부") 진행을 지연시켜서 더 많은 시간이 소요될 수도 있습니다.

대신, DMARC를 시행하기 전에 내부에서 해결해야 할 몇 가지 업무가 있습니다.

- DMARC 보고서에서 파악된 모든 이메일 발신자 그리고 이해관계자들이 언급한 기타 발신자의 저장
- 각 서비스/이메일 발신자에 대한 소유자 식별
- 발신 서비스를 허가됨, 허가되지 않음 또는 악의적 으로 범주화
- 이해관계자의 도움을 받아서, DMARC 보고서에 표시되지 않을 수 있는 기타 발신자의 식별
- 식별된 모든 신규 발신자에 대해 이해관계자에게 연락
- 새롭게 발견된 적법한 이메일 발신자의 IP 주소로 SPF 기록 업데이트

시행 전 소통을 위한 권장사항

채택율을 개선하기 위한 5가지 정보

- 이해관계자와 공유할 수 있는 실행 정책의 문서화
- DMARC 업무가 너무 심하거나 지원이 필요한 경우, Valimail 같은 DMARC 기술지원 사업자에게 연락
- DMARC 보고서에서 새롭게 파악된 내용으로 즉시 소통
- DMARC 배치를 내부 프로젝트로 시작
- 임원진을 이 프로젝트의 후원자로 활용

digicert®

DMARC를 모니터링 모드에 얼마나 오래 둬야 하는가?

기업체마다 소요되는 시간은 다르지만, 일반적으로 엔터프라이즈급은 소규모 기업체보다 더 많은 시간이 필요합니다. 수 주에서 수 개월을 염두하여 준비하세요.

인벤토리가 완전하고, 허가받은 모든 발신자를 맵핑했으며, 귀사에서 충분한 정보를 확보하고 나면, 차단 단계로 이동할 준비가 된 것입니다.

격리 모드가 켜지면, 인증에 실패한 메시지는 격리됩니다.
일반적으로, 이는 해당 메시지가 사용자의 스팸 폴더로 이동했음을 의미합니다.

DMARC 격리 시행의 설정 방법

1. DNS 서버에 로그인하여 DMARC 기록 검색
2. 지정된 도메인에 대한 DMARC 기록을 열람하여 정책을 "p=none"에서 "p=quarantine"으로 업데이트
   예: "v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@you_domain.com"
3. "pct" 플래그 (필터링 되는 메시지의 %)를 추가하십시오. 10%로 시작하는 것이 좋습니다,
4. DMARC 사용에 별다른 어려움이 없다면, 필터링 되는 메시지의 백분률을 "pct=100" (100%)까지 점진적으로 높이십시오.

   주: BIMI 및 VMC 표준을 충족하려면 "pct=100"이어야 하지만, 정책은 "격리" 또는 "거부" 중 하나입니다.

플래그의 작동 원리:

- "p=없음" 이외의 정책이 지정되는 경우, 해당 정책은 "pct" 플래그의 백분률에 적용됩니다.
- 이보다 덜 제한적인 정책은 나머지에 적용됩니다 (예: "p=차단" 및 "pct=10"인 DMARC 기록인 경우, 인증에 실패한 트래픽의 10%가 차단되고 나머지 90%는 정상적으로 전달됨).

digicert®

100% 필터링에 도달하고 나면, 최고 수준의 시행 수준인 "P=reject"로 이동할 준비를 마친 것입니다.

digicert

DMARC 거부 정책의 설정 방법

1. DNS 콘솔을 통해 DMARC 기록 열람
2. "p=quarantine"을 "p=reject"로 변경
   예: "v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports@ you_domain.com
3. 기록 저장

팁: 적법한 이메일이 거부되어 삭제되지 않도록 이 단계에서 지속적인 모니터링을 수행하는 것이 특히 중요합니다.

거부 정책은 이메일에 어떤 영향을 주나?

DMARC 확인에 실패하는 모든 메시지 (허가되지 않은 메시지)는 저지되거나 삭제되며, 이메일 수신자는 그 사본을 수령하지 못하며 삭제에 대해 통보를 받게 됩니다.