Cisco ESA(Email Security Appliance) 안티스팸 효율성 체크리스트

목차

소개

다음 절차 및 권장 사항은 ESA를 통해 전달되는 스팸 양을 줄이기 위한 "모범 사례"입니다.모든 고객은 다르며 이러한 권장 사항 중 일부는 스팸으로 분류된 합법적인 이메일(오탐)의 수를 늘릴 수 있습니다.

기본 설정

1. 안티스팸이 켜져 있는지 확인합니다.

   모든 MX 레코드(낮은 우선 순위 포함) MX 레코드가 ESA를 통해 메일을 릴레이하는지 확인합니다.어플라이언스에 유효한 안티스팸 기능 키가 있는지 확인합니다.적절한 모든 수신 메일 정책에 대해 안티스팸이 활성화되었는지 확인합니다.

2. 안티스팸 규칙 업데이트를 받고 있는지 확인합니다.Security Services(보안 서비스) > Anti-Spam(안티스팸)의 업데이트에 대한 **가장 최근** 타임스탬프가 지난 2시간 내에 있는지 확인합니다.

3. 안티스팸에서 메시지를 검사하는지 확인합니다.

   다음 헤더에 대한 누락된 스팸 메시지의 샘플을 확인합니다.X-IronPort-안티스팸 결과:헤더가 없는 경우

   스팸 검사를 우회하는 허용 목록 항목 또는 필터가 없는지 확인합니다(아래 참조).메시지가 최대 메시지 스캔 크기를 초과하므로 검사를 우회하지 않는지 확인합니다(기본값은 262144바이트). 이 설정을 줄이면 성능이 크게 향상되지 않으며 스팸이 누락될 수 있습니다.평가 중에 IPAS 설정이 테스트 중인 다른 제품과 동일한지 확인하는 것도 중요합니다.각 HAT 항목을 통해 모든 인바운드 메일 플로우 정책에 대해 "spam_check=on"을 확인합니다.기본값에 "spam_check= on"이 있고 메일 플로우 정책 중 명시적으로 해제하지 않는 한 올바르게 구성됩니다.TRUSTED/allowLIST 설정에 특별히 주의하십시오.고객이 실수로 스팸을 전달하는 허용 목록에 발신자를 추가하는 경우가 종종 있습니다. 예를 들어, 스팸 및 합법적인 이메일을 허용 목록 발신자 그룹에 전달하는 ISP 또는 파트너의 도메인을 추가하는 경우가 있습니다.

   메시지 필터를 빠르게 검사하여 "skip-spamcheck" 필터가 없는지 확인합니다. 있는 경우, 해야 할 작업을 수행하는지 확인합니다(단일 수신 대기를 일치시키면 30명 이상의 수신자가 있는

메시지에 대해 일치할 수 있음).

최근 SPAM 예(시간, 날짜, 수신 등)를 찾고 mail_logs를 참조하여 발생한 상황을 확인합니다 .안티스팸에서 부정적인 판정을 반환했는지 확인합니다.

4. 스팸 판정 메시지에 대해 원하는 작업을 수행하는지 확인합니다.Anti-Spam 판정이 처리되는 방법에 대한 인바운드 메일 정책을 확인합니다.SPAM 판정 및 의심되는 메시지가 기본 정책에서 삭제 또는 격리되는지, 그리고 다른 모든 정책이 기본 동작을 사용하거나 의도적으로 기본 값을 재정의하는지 확인합니다.

5. 오탐(false-positives)이 누락된 스팸보다 덜 문제가 있을 경우 더 적극적인 스팸 임계값 적용:

   '특정' 임계값에 오탐이 없는 경우 Positive Spam Threshold(양의 스팸 임계값)를 80(기본값은 90)으로 줄입니다.

   오탐(false-positive)이 'suspect' 임계값에 영향을 미치지 않을 경우 Suspected Spam Threshold(의심스런 스팸 임계값)를 40으로 감소(기본값은 50)합니다.

   대부분의 스팸 불만 사항이 수신자의 하위 집합에서 발생하는 경우, 이러한 수신자에 대해 더욱 공격적으로 필터링하기 위해 낮은 스팸 임계값을 가진 사용자에 대해 별도의 메일 정책을 생성할 수 있습니다.

   이러한 가치들에 대한 변화는 가볍게 여겨져서는 안 되며, 어떤 의도적 효과가 있는지 확인하기 위한 어떠한 하드 자료도 없이 행해져서도 안 된다.

   또한 오탐을 방지하기 위해서만 다른 방향의 값을 조정하지 마십시오.오탐 및 오탐이 TAC에 전송되었는지 확인하십시오.

6. SBRS 설정 및 HAT 정책 최적화:

   대부분의 조직은 SBRS -10에서 -3.0까지 차단 목록에 추가하고 SBRS -3.0에서 -1.0을 SUSPECTLIST에 추가하는 것이 좋습니다.보다 적극적인 고객은 SBRS -10에서 -2.0으로 차단 목록을 만들고 SUSPECTLIST에 -2.0에서 -0.6으로 추가할 수 있습니다.

   경우에 따라 발신자가 아직 SenderBase Reputation Score를 가지고 있지 않다는 사실은 이 발신자가 스패머일 수 있다는 증거입니다.SBRS "none"을 SUSPECT 발신자 그룹에 "Throttled" 정책을 가져오는 발신자 그룹에 직접 추가할 수 있습니다(예:

   "Throttled" 정책에 대해 시간당 최대 수신자 수를 5로 변경합니다.

   시간당 서로 다른 수신인 제한을 적용하기 위해 두 개 이상의 "Throttled" 정책을 생성하는 것이 좋습니다. 예를 들어, 시간당 SBRS가 -2에서 -1에서 5인 발신자와 SBRS가 -1에서 0~20인 발신자 사이의 수신자 제한 속도를 예로 들 수 있습니다.

7. "Throttled" Mailflow 정책에 대해 발신자 확인 활성화:

   고객은 존재하지 않거나 잘못 구성된 DNS가 있는 발신자를 SUSPECTLIST 발신자 그룹에 추가할 수 있습니다.

연결 호스트 PTR 레코드가 DNS에 없습니다.연결 호스트 PTR 레코드 조회가 임시 DNS 실패로 인해 실패했습니다.

연결 호스트 역방향 DNS 조회(PTR)가 정방향 DNS 조회(A)와 일치하지 않습니다.

잘못 구성된 DNS를 가진 발신자의 오탐(false-positive)이 발생할 수 있으므로 고객은 거부 사유를 나타내는 사용자 지정 4xx 응답을 반환하는 별도의 Mailflow 정책을 설정할 수 있습니다.

발신자 확인에 대한 자세한 내용은 온라인 도움말 또는 AsyncOS 사용 설명서를 참조하십시오.

8. LDAP 수락 및 디렉토리 수집 공격 보호 활성화:

   많은 스팸 발송자가 유효하지 않은 주소의 수가 많은 주소로 이메일을 전송하므로 잘못된 수신자에게 보내는 발신자를 차단하면 스팸도 줄일 수 있습니다.

   LDAP 수락이 이미 설정되어 있는 경우 IP당 최대 5에서 10 사이의 잘못된 시도를 통해 각 인바운드 리스너에 대해 DHAP(Directory Harvest Protection)도 구성되었는지 확인합니다.

9. 콘텐츠 사전 사용:

   ESA에는 두 개의 컨텐트 사전이 있습니다.annique.txt 및 searchy_content.txt이러한 사전을 사용하면 오탐(false positive)이 발생할 수 있지만, 부적절한 단어를 위해 메일 스트림을 필터링하면 "잘못된 사용자"가 "잘못된 이메일"을 받을 위험이 줄어들 수 있다는 것을 일부 고객이 발견했습니다. 이러한 필터는 특정 메일 정책의 사용자 그룹에 대해 사용하도록 설정하여 "삐걱거리는 바퀴"에만 적용될 수 있습니다.

10. 잘못 분류된 메시지를 Cisco TAC에 보고합니다.

11. 다수의 오탐을 방지하려면 아웃바운드 스캔을 위해 SBRS를 비활성화해야 합니다.이는 SBRS가 수신 IP의 평판을 확인하고 내부 네트워크에서 이러한 IP의 대부분은 동적이므로 발생합니다.다음 섹션의 단계를 따릅니다.

SBNP 활성화

1. 인바운드 및 아웃바운드 메일이 별도의 리스너에 있는지 확인합니다.

2. 아래에서 아웃바운드 이메일에 대해 SenderBase 조회를 비활성화합니다.GUI에서 이 작업을 수행하려면 Network(네트워크) > Listeners(리스너)로 이동하여 아웃바운드 리스너를 선택하고 "Advanced(고급)"를 선택한 다음 "Use SenderBase IP profiling(SenderBase IP 프로파일링 사용)" 옆에 있는 상자의 선택을 취소합니다.

   SBNP(SenderBase Network Participation)는 평판 필터, 안티스팸 및 신종 바이러스 필터의 효율성을 크게 높일 수 있습니다.SBNP는 안티스팸을 사용할 때 활성화될 경우 성능에 큰 영향을 미치지 않으며 매우 안전합니다.

참고:조직에서 수신하는 스팸의 양은 시간이 지남에 따라 변경됩니다.단순히 과거에 비해 더 많은 스팸을 수신하고 있기 때문에 더 많은 스팸이 ESA를 통과할 가능성이 있습니다 .Incoming Mail Overview(수신 메일 개요) 페이지를 보고 "Stopped by reputation filtering(평판 필터링에 의해 중지됨)" 및 "spam messages detected(탐지된 스팸 메시지)" 라인 항목을 추가하여 시간에 따른 이 동작을 추적할 수 있습니다.

SBRS 근거

False Positives의 가장 큰 문제는 중요한 이메일이 손실될 수 있다는 것입니다.이러한 맥락에서 SPAM Positive 이메일 격리 또는 삭제 방식은 문제가 됩니다.합법적인 이메일을 쿼런틴이나 스팸 폴더로 보낼 경우 사전 검색을 통해 스팸으로 잘못 분류된 햄을 "알림"해야 합니다.

이와 달리 차단 목록 및 속도 제한 이메일은 발신자에게 즉시 알릴 수 있는 방식으로 차단됩니다.이 발신자가 스팸 발송자가 아닌 경우, 귀하와 연락할 수 있는 다른 방법을 찾게 될 것입니다.실제로, 전반적인 정책으로서, 기본적으로 차단을 하고 요청에 따라 신뢰할 수 있는 파트너를 수락하는 것이 일부 기업에 더 나은 위치입니다.

조절을 적절히 설정하면 파트너에게 영향을 미치는 경우는 거의 없어야 하지만 바이러스에 감염된 도메인으로부터 보호됩니다.스로틀링(throttling)은 스패머에게 소진됩니다.우리는 많은 수의 IP를 구매하고, 적절한 SBRS 점수를 받은 다음 스팸 발송을 시작할 수 있는 충분한 "좋은" 이메일을 생성하는 스패머 기술을 알고 있습니다.더 큰 의심스러운 목록 범위는 이러한 항목을 포착하여 피해를 제한해야 하며, 이로 인해 도메인에 스팸을 보내지 못하게 될 수 있습니다.