Cisco Email Security Image Analysis: 명시적 이미지를 통해 네트워크 보호

당면 과제

전 세계의 업무적 커뮤니케이션 중 80%는 이메일로 진행됩니다. 즉, 규모에 관계없이 모든 조직의 1 차 커뮤니케이션 방법은 이메일입니다.[1] 이메일은 업무적으로 다양한 이점을 제공하지만 그와 동시에 의도적으로 또는 기타 성희롱 수단으로 사용되는 이메일은 조직에 큰 위험이 됩니다.

기업 이메일 시스템을 통해 노골적인 성적 콘텐츠를 보내고 받는 직원은 심각한 문제인 동시에 보안 위협이 됩니다. 이러한 이메일은 확인하지 않는 경우 회사의 분위기를 떨어뜨리고 적대적 업무 환경을 조장하여 기업이 법적 책임을 져야 할 수 있습니다.

"음란물과 성적 요구가 오랜 기간 동안 기업 전반에서 지속적으로 확산되는 경우 적대적 업무 환경이 조성될 수 있습니다."

– 미국 Equal Employment Opportunity Commission

대다수 고용주에게는 성희롱으로부터 직원을 보호해야 하는 법적 책임이 있습니다. 고용주는 직원의 행동에 책임을 져야 할 수 있으며, 이로 인해 경제적으로도 손실을 입을 수 있습니다. 이러한 책임을 피하려면 고용주는 적대적 업무 환경을 방지하기 위해 적절한 모든 단계를 수행했음을 입증해야 합니다.

최소한 고용주는 효율적으로 **시행, 모니터링** 및 **전달**되는 이메일 사용 제한 정책을 마련해야 합니다. 그러나 서면으로 작성된 정책 자체만으로는 충분하지 않습니다. 커뮤니케이션, 교육 및 시행을 통해 구현하지 않는 정책은 관련 책임을 방지하는 과정에서 거의 또는 전혀 활용할 수 없습니다.

*"효율적인 예방 프로그램에는 직원에게 정기적으로 명확하게 **전달**되며 효율적으로 **구현**되는 성희롱에 대한 명시적 **정책**이 포함되어야 합니다."*

– 미국 Equal Employment Opportunity Commission

발생한 성희롱을 파악하지 못했다고 해서 고용주에게 책임이 없는 것은 아닙니다. 문제를 무시하는 경우 회사 재무 상태가 나빠질 뿐 아니라, 불법적인 이미지가 사용된 경우 고용주가 형사 기소되는 상황까지 발전할 수 있습니다. 고용주는 정책을 모니터링, 교육 및 시행하는 예방 조치를 취하여 다음과 같은 결과의 위험을 크게 완화할 수 있습니다.

- 회사 평판 및 브랜드 실추
- 적대적 작업 환경 조성
- 생산성 감소
- 성희롱 소송
- 형사 소송

[1] 출처: Radicati(2014 년)

솔루션

Cisco® Email Security Image Analysis 솔루션은 노골적인 성적 이미지 첨부 파일을 필터링하며, 수상 경력에 빛나는 Cisco X-Series 및 C-Series Email Security Appliance 에서 사용하거나 Cisco Cloud Email Security 서비스를 통해 사용할 수 있도록 라이센스를 적용할 수 있습니다. 이 기술을 통해 고용주는 다음을 수행함으로써 직원 관리 의무를 이행하고 있음을 제시할 수 있습니다.

- 고위험 이미지 첨부 파일이 포함된 이미지 **식별**
- 이메일 시스템을 오용하는 사용자 **모니터링**
- 사용자를 대상으로 회사의 이메일 사용 정책 **교육**
- 필요 시 정책 **시행**

그림 1. Cisco Email Security Image Analysis 는 각기 다른 12 가지 탐지 레이어를 사용해 수신/발신 이메일에서 노골적 콘텐츠를 식별합니다.

기능

Cisco Email Security Image Analysis 는 이메일 이미지 정책을 식별, 모니터링, 교육 및 시행하기 위한 제어 기능을 제공합니다.

식별

멀티레이어 탐지 엔진. Cisco Email Security Image Analysis 는 각기 다른 12 가지 탐지 방법을 사용하여 이메일 게이트웨이를 통과하는 대량의 합법적 업무 이미지 내에 숨겨진 노골적 이미지를 식별합니다.

1 세대 이미지 분석 기술은 부정확한 "피부색" 분석 기술에 크게 의존했습니다. 이 솔루션에서는 오탐 횟수가 많다는 불만이 흔히 제기되었습니다. 반면 Cisco Email Security Image Analysis 에서는 이 피부색 분석 기술 요소가 오탐 횟수가 매우 적은 정확한 탐지 기능을 제공하는 보다 정교한 의사 결정 프로세스의 부수적인 부분으로만 사용됩니다.

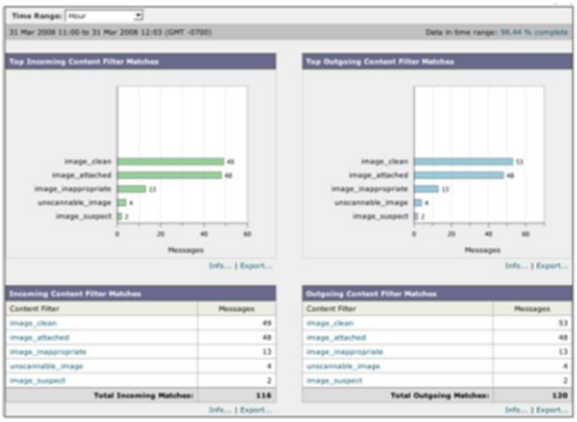
임베디드 이미지 스캔 기능. Cisco Email Security Image Analysis 에서는 JPEG, BMP, PNG, TIFF, GIF, TGA, PCX 등의 첨부된 파일과 임베디드 파일 유형을 검사할 수 있습니다. 이미지가 다른 파일에 임베디드된 경우 Cisco 의 콘텐츠 스캔 엔진이 해당 파일을 추출합니다. 콘텐츠 스캔 엔진은 Word, Excel, PowerPoint 문서를 비롯하여 400 개가 넘는 파일 유형에서 이미지를 추출할 수 있습니다.

조정 가능한 민감도. 민감도 설정이 제공되므로 관리자가 고유한 요건에 맞게 엔진의 분석 레벨을 조정할 수 있습니다.

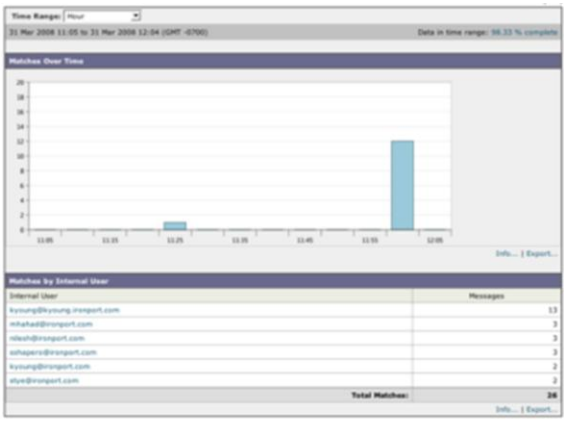
모니터링

관리 보고서. 대부분의 네트워크 관리자는 부적절한 이미지 콘텐츠가 네트워크에서 전송되는지 여부 또는 해당 시기를 파악하지 못하고 있음을 인정합니다. Cisco Email Security Image Analysis 를 통해 관리자는 수신/발신 이메일 트래픽에서 오용 사례를 파악할 수 있는 관리 보고서를 생성할 수 있습니다. 필터 일치 항목에 따라 관리자는 기존 보고 기능을 사용하여 PDF 및 CSV 형식으로 쉽게 사용 가능한 보고서를 생성할 수 있습니다. 이러한 보고서는 온디맨드 방식으로 생성할 수도 있고 자동으로 생성하도록 예약할 수도 있으며 인사부 등의 다른 부서로 배포할 수 있습니다.

그림 2. 콘텐츠 필터 보고서에는 특정 사용자의 수신/발신 메시지에서 확인된 부적절하거나 의심스러운 이미지가 표시됩니다.



Cisco Email Security Image Analysis를 통해 관리자는 인바운드 및 아웃바운드 메시지 콘텐츠를 확인할 수 있습니다.



정책 필터와 가장 일치하는 사용자를 신속하게 찾아냅니다.

교육

이메일 알림. Cisco Email Security Image Analysis 는 정책을 위반하는 사용자에게 사용자 정의된 이메일 알림을 보내는 옵션을 제공합니다. 이처럼 알림은 회사의 사용 제한 정책을 사용자에게 정기적으로 명확하게 전달할 수 있으며 향후 오용을 방지하기 위한 효율적인 도구로 활용할 수 있습니다.

시행

정책 통합. Cisco Email Security Image Analysis 를 메시지 및 콘텐츠 필터와 통합하여 수신자 또는 발신자를 기준으로 정책 기반 필터링을 활성화할 수 있습니다. 기존 필터링 인프라에서는 단일 필터 일치를 기준으로 여러 동작을 결합할 수 있습니다. 예를 들어 엔진이 이메일에서 노골적 이미지를 탐지하면 여러 동작(첨부 파일 격리/제거, 이미지에 회사 정책 메시지 스탬프 표시 등)을 수행할 수 있습니다.

혜택

안심하고 이메일 사용. 대부분의 회사는 기업 이메일 시스템을 통해 교환되는 이미지 유형을 완전하게 확인하지 못합니다. Cisco Email Security Image Analysis 를 사용하는 회사의 경우 이메일 시스템이 규정을 준수하며 적절하게 사용되므로 안심할 수 있습니다.

법적 책임 방지. 미국 대법원은 적대적 업무 환경이 조성되는 경우 직원의 행동에 고용주가 책임을 져야 한다는 판결을 내린 바 있습니다. Equal Employment Opportunity Commission 에서 수집한 데이터에 따르면, 고용주에 대한 성희롱 평결에서 평균적으로 25 만 달러 이상의 배상 판결이 내려지고 있습니다. 고용주가 그러한 소송에서 성공적으로 방어하더라도 평균적으로 10 만 달러의 소송 비용이 발생합니다. 그러나 법원 판결과 법률에 따르면, 고용주가 희롱 행위를 예방하고 신속하게 바로잡기 위한 적절한 조치를 취하는 과정에서 최선을 다한 경우 법적 책임을 지지 않거나 피해를 제한할 수 있습니다. Cisco Email Security Image Analysis 는 고용주가 그러한 소송에서 방어하는 데 도움이 되는 다양한 탐지, 보고 및 정책 이행 기능을 제공합니다.

"회계 연도 2010 년에 EEOC 의 고용주는 4 억 4 백만 달러라는 천문학적인 액수를 보상해야 했습니다."

– 미국 Equal Employment Opportunity Commission

브랜드 이미지 보호. 기업은 브랜드 정체성을 개발하고 전 세계에 알리는 데 많은 비용을 투자합니다. 금융, 정부/공공, 의료 분야의 기업과 기관은 보수적이고 전문적인 이미지를 구축하며, 지역 정부의 경우에는 자금 지원을 받기도 합니다. 대형 소매업체의 경우 "가족 친화적" 이미지가 중요합니다. 이와 같이 심혈을 기울여 쌓은 브랜드 이미지가 실추될 경우 큰 타격이 될 수 있습니다. 미디어에서 비판을 받고 수익 상실로 이어지기도 합니다. 고용주는 Cisco Email Security Image Analysis 를 통해 회사의 이메일 메시징을 지속적으로 모니터링하고 필요한 개선 조치를 취함으로써 그러한 위협을 사전에 방지할 수 있습니다.

직원 보호. 회사는 직원들을 잘못된 행동으로부터 보호하고 부적절한 이메일 콘텐츠의 영향으로 인해 회사의 건전한 분위기가 나빠지지 않도록 예방 조치를 취해야 합니다. Cisco Email Security Image Analysis 는 위협이 조직 전반에 확산되기 전에 사전 제거하는 툴을 회사에 제공합니다.

생산성 향상. 작업장에서 노골적인 이미지 콘텐츠를 사전에 관리하면 모든 직원이 규정을 준수하는 안전한 업무 환경을 조성함으로써 업무 시간에 업무와 관련이 없는 활동을 하고자 하는 충동을 없애 생산성을 높일 수 있습니다.

국제 법률 및 규정

이메일로 성인물을 표시하거나 외설적 자료를 유통시키는 행위는 성희롱으로 간주될 수 있습니다. – 영국 Equality and Human Right Commission

성희롱은 다양한 형식일 수 있으며 노골적인 성적 이메일 전송도 포함될 수 있습니다.
– 호주 Human Rights Commission

작업장에서 다른 직원이 불쾌감을 유발하는 성적 사진을 보여준 경우 성희롱을 당한 것으로 간주할 수 있습니다.
– 뉴질랜드 Human Rights Commission

결론

기업 네트워크에서 성인물 및 부적절한 이미지를 배포하는 행위는 고용주에게 사업상 큰 위험이 됩니다. 부적절한 행위를 하는 사용자를 파악하고 회사 정책을 시행하는 것은 이러한 행위로 인해 발생할 수 있는 법적 책임과 브랜드 실추로부터 조직을 변경하는 데 있어서 중요한 단계입니다. Cisco Email Security Image Analysis 는 노골적 콘텐츠가 조직에서 송수신되기 전에 탐지하여 제어하는 쉽게 사용 가능한 솔루션입니다.

추가 정보

Cisco 는 전 세계 영업 사원 및 리셀러 네트워크를 통해 "무료 데모" 프로그램을 제공합니다. Cisco Email Security 가 포함된 Cisco Email Security Image Analysis 45 일 무료 평가판을 통해 관리 담당자는 기업 이메일 시스템 오용 사항을 완벽하게 파악할 수 있습니다. 자세한 내용은 http://www.cisco.com/go/emailsecurity를 참고하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C22-719504-01 6/15