Cisco, 업계 선두 제조업체를 위한 이메일 보안 솔루션 구축

EXECUTIVE SUMMARY

KOMATSU 요약

본사: 일본 도쿄

업종: 세계적인 산업 장비 및 차량 제조업체

2007년 수익: 통합 순 매출액 16억 달러

직원 수: 33,836명(회사), 6,231명(독립)

Cisco IronPort의 장점

- 강력한 이메일 보안 및 보안 관리 어플라이언스를 통해 사전 대응 및 사후 대응형 위협 방지와 관리 지원
- Cisco IronPort C350 Email Security Appliance를 Komatsu와 지사에 알맞은 방식으로 고유하게 구성하여 뛰어난 보안 및 안정성 제공
- 구축 일주일 만에 스팸 탐지율 약 75% 향상
- 관리 부담 및 다운타임을 줄여 원활한 관리 및 업데이트로 총 소유 비용 절감

개요

도쿄에 본사를 둔 Komatsu, Ltd.는 건설/굴착 장비, 산업 기계 및 차량 분야에서 업계 선두를 달리는 세계적인 제조업체입니다. 이 회사에서는 최근 Cisco®와 파트너십을 체결하여 광범위한 이메일 네트워크에 편재하는 스팸, 바이러스 및 관련 위협을 퇴치할 수 있는 능동적이고 포괄적인 솔루션을 구현했습니다.

상황

2004년, Komatsu에서는 조직으로 유입 또는 반출되는 중요 정보의 보안과 관련한 규제 검사(예: 일본판 Sarbanes-Oxley Act)가 강화됨에 따라 조직이 규정을 완벽하게 준수하고 있는지 확인하기 위해 전사 이메일 보안 및 위협 억제 기능에 대해 대대적인 평가를 시행했습니다.

조사 결과, 스팸 차단 기능이 떨어지고 있다는 사실이 발견되었습니다. 2005년, 이 회사에서는 한 보안 공급업체를 선정하여 점차 증가하고 있는 이 문제를 해결하고자 했습니다. 그러나 해당 공급업체의 솔루션은 충분한 탐지, 보호 및 정확성을 제공하지 못했습니다. 2007년 여름경에는 Komatsu의 국내 회사 그룹에 전송된 스팸 양이 기하급수적으로 증가했으며, 2005년에는 하루에 약 40,000개였던 메시지가 이때에는 하루에 200,000개씩 수신되곤 했습니다. 그 결과, 최종 사용자에게 전달되는 사기성 메시지의 수가 대폭 증가하게 되었습니다.

또한, 스팸 메시지의 첨부 파일로 유입되거나 메시지 본문의 URL로 삽입된 바이러스가 네트워크를 통과하면서 문제는 더욱 심각해졌습니다. 기존의 보안 시스템으로는 조직에서 새로운 바이러스 패턴 파일을 적시에 자동으로 삭제하여 확산을 방지하는 것이 불가능했습니다. 이에 따라 Komatsu에서는 백신 및 24시간 고객 서비스/시스템 지원 등 한층 강화된 서비스를 받기 위해 자사 보안 공급업체와 새로운 계약을 체결하게 되었습니다.

> "Cisco IronPort 제품을 구현한 결과, 뛰어난 성과를 얻었으며 이에 매우 만족합니다."
>
> **— Komatsu, Department Supervisor, Kenichi Tabata**

기술적 문제

결국 Komatsu에서는 이러한 이메일 기반 위협의 경우 상황을 주시하다가 문제가 나타나면 증상을 해결하는 정도에 그치는 것이 아니라, 더욱 포괄적인 솔루션이 필요하다는 사실을 깨닫게 되었습니다. 이 회사에서는 동급 최고의 위협 탐지율 및 바이러스 발생 시 이를 식별하고 퇴치할 수 있는 기능을 제공하는 솔루션이 필요하다는 판단을 내렸습니다.

Komatsu의 Department Supervisor인 Kenichi Tabata는 "급격하게 증가하는 스팸 양을 차단할 수 있는 정보 보안은 중요한 당면 과제가 되었습니다. 이전에 사용하던 제품은 스팸 탐지율이 낮았으므로 만족스럽지 않았습니다. 따라서 새로운 솔루션을 구현하여 평가하기로 했습니다. 또한, 정의 파일을 제공하기 전에 의심스러운 첨부 파일이 포함된 이메일을 격리할 수 있는 기능도 필요했습니다."라고 말했습니다.

Cisco IronPort의 장점

철저한 조사 끝에 Komatsu에서는 Cisco를 새로운 이메일 보안 업체로 선택했으며 Cisco IronPort® C350 Email Security Appliance의 검증된 기능을 활용하여 지능적으로 위협을 방지하고, 스팸을 차단하며, 회사 정책을 손쉽게 시행하고자 했습니다. 지사를 보유한 중견기업의 이메일 보안 요구 사항을 충족하기 위해 개발된 Cisco IronPort C350에서는 사전 대응 및 사후 대응형 접근 방식을 모두 사용하여 스팸을 퇴치합니다. Cisco IronPort Reputation Filters에서는 실시간 위협 평가를 제공하고 의심스러운 발신자를 식별합니다. Cisco IronPort Anti-Spam 기술의 경우 각 메시지의 전체 컨텍스트를 검토하는 강력하고 고유한 스캔 엔진을 구축하여 다양한 위협을 차단함으로써 사용자에게 해당 위협이 전달되지 않도록 합니다. 또한 Cisco IronPort Spam Quarantine에서는 기존 디렉토리 및 메일 시스템과 쉽게 통합되는 안전한 스팸 메시지 보관 영역을 최종 사용자에게 제공합니다.

Cisco IronPort C350 Email Security Appliance를 설치한 지 일주일 후, Komatsu의 스팸 탐지율은 일일 200,000건에서 346,000건으로 증가하여 기술에 대한 최종 사용자의 만족도와 신뢰도를 신속히 구축할 수 있었습니다.

Cisco IronPort Virus Outbreak Filters는 이러한 이메일 보안 어플라이언스에서 제공하는 또 다른 강력한 기능입니다. 이러한 필터에서는 주로 기존의 바이러스 시그니처가 적용되기 몇 시간 전에 의심스러운 이메일 첨부 파일을 정확하게 탐지하는 중요한 첫 번째 방어 레이어를 제공하고 해당 파일을 자동으로 격리합니다. 또한, Sophos와 McAfee 안티바이러스 기술을 완전히 통합하여 피해가 발생하기 전에 문제를 차단하는 데 도움이 되는 추가적인 방어 레이어를 제공합니다.

Cisco IronPort C350에서는 규정 컴플라이언스에 대한 위협으로부터 방어하는 통합된 컴플라이언스 필터, 기밀 데이터를 보호하고 고객의 규정 요구 사항을 준수하는 고급 암호화 기능, 콘텐츠 스캔 엔진에서 플래그된 메시지를 격리할 수 있는 기능도 제공합니다.

고급 이메일 인증 및 전사적인 관리 툴에서는 위협 발생 시 이러한 위협에 대해 뛰어난 통찰력을 제공합니다. 이는 이메일 운영과 보안을 단일 플랫폼에 통합하여 문제의 소지가 있는 이메일을 처리해야 하는 관리 부담을 줄이고 비용을 낮추며, 네트워크 게이트웨이에서 완충제 역할을 하여 생산성을 높이고, 사용자가 스팸, 바이러스 및 관련 문제로 곤란을 겪지 않도록 보호합니다.

Komatsu에서는 Cisco IronPort M650 Security Management Appliance를 구현함으로써 Cisco IronPort Email Security Appliance와 관련된 모든 정책, 보고 및 감사 정보의 게이트웨이에서 유연하고 포괄적인 제어력을 행사할 수 있게 되었습니다. 관리자는 이러한 중앙 집중식 보고 기능을 통해 여러 보안 어플라이언스의 트래픽 데이터를 하나로 모아 통합된 방식으로 보고를 할 수 있게 되었습니다.

Komatsu의 Kenichi Tabata는 "Cisco를 통해 총 소유 비용을 대폭 절감하고 바이러스 및 스팸을 퇴치할 수 있는 새로운 기능을 실제로 구현하게 되었습니다."라고 말하며 "Cisco IronPort 제품을 구현한 결과, 뛰어난 성과를 얻었으며 이에 매우 만족합니다."라고 덧붙였습니다.

이 문서는 8월 1일에 처음 게시되었으며, 10월 8일에 한정적인 명목상의 업데이트와 함께 다시 게시되었습니다.

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, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C36-599562-00 10/10