White Paper

이메일 보안을 사용하여 피싱, 스팸 및 표적 공격으로부터 보호: 고등 교육 기관용 기능 통합

온라인 범죄자들은 표적에 접근할 수 있는 새로운 방법을 지속적으로 모색하고 있습니다. 예를 들어, 조직의 이메일 계정을 가로채거나 평판이 좋은 기업 행세를 하여 인증서 피싱을 통해 대량 스팸을 발송하고 사용자의 계정, 금융 및 개인 정보를 탈취합니다. 고등 교육과 관련하여 여러 가지 중요한 보안 문제가 있지만, 그중에서도 고등 교육에서 일반적으로 당면하고 있는 문제가 바로 이것입니다. 고등 교육 기관의 데이터 유출 사고는 감소하는 추세이긴 하지만, 만약 발생할 경우 비용 손실이 막대할 수 있습니다. 2011년 11월 VCU(Virginia Commonwealth University)에서 발생한 데이터 유출 사고의 경우, 176,567건의 기록이 유출되었으며 대학 측의 비용 손실은 약 2,000만 달러에 달했습니다.[1] 표적 공격은 이러한 유출 사고로 이어지거나 더 심각한 결과를 초래할 수 있습니다. 교육 기관은 인증서 피싱 공격의 대상이 되고 블랙리스트에 등재되지 않도록 노력해야 하는 상황에 자주 놓이게 됩니다. 본 백서에서는 이러한 보안 문제를 방지하기 위해 통합할 수 있는 보안 기능에 대해 자세히 살펴봅니다.

배경

학생과 교수진의 이메일 및 온라인 보안에 대한 경험은 각자 매우 다양하므로 해당 교육 기관에서 발송한 진짜 커뮤니케이션을 식별하는 문제와 관련하여 일관된 수준의 교육을 제공하기가 어렵습니다. 사용자의 받은 편지함에 피싱 및 유도 또는 표적 공격 메시지가 전달되지 않게 하려면 높은 수준의 보호가 필요하며, 추후 공격 및 공격자가 확보한 인증서에 따른 피해가 발생하지 않도록 부수적인 기능 또한 필요합니다.

포괄적인 이메일 보안 솔루션은 다음과 같은 기능을 제공해야 합니다.

- 피싱 공격의 수신 방지
- 최종 사용자를 교육하여 스팸 또는 피싱 이메일을 인식할 수 있도록 지원
- 아웃바운드 스팸 차단
- 업무의 일환으로 대량 이메일을 보내는 교수진과 시스템에 영향을 미치지 않는 선에서 아웃바운드 이메일의 속도 제한
- 속도 제한에 도달할 경우 이메일 관리자에게 이를 알려 조사 및 문제 개선을 조기에 실행할 수 있도록 지원

Cisco Email Security에서 필요한 기능은 다음과 같습니다.

- Outbreak Filters
- Outbreak Filters의 고지 문구 추가
- 아웃바운드 안티스팸 스캐닝
- 메일 발신자별 속도 제한
- 관리 알림 메시지

[1] Daily Open Source Infrastructure Report, 미국. Department of Homeland Security, 2012 년 3 월 14 일.

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

조직에서는 이러한 기능을 통합하여 계층적 보호를 형성할 수 있으며, 여기에는 조직이 이메일을 통해 수행하는 작업 및 수행하지 않는 작업과 관련하여 최종 사용자에 대한 정책 보강이 포함됩니다.

기능 설명

Cisco AsyncOS® 7.5 for Cisco Email Security의 새로운 기능인 **Outbreak Filters**는 소규모 유도 및/또는 표적 공격에 대처하기 위한 기능입니다. 이러한 필터는 의심스러운 이메일에 포함된 URL을 재작성하고 Cisco에서 지원하는 Cisco 인터넷 프록시 서버를 통해 해당 URL을 리디렉션합니다. 또한, Cisco Email Security에는 이메일의 본문 텍스트 위에 맞춤형 고지 사항을 추가할 수 있는 기능이 포함되어 사용자에게 조직의 이메일 정책(예: 이메일을 통해 사용자 ID 또는 비밀번호를 묻지 않음)을 상기시킵니다.

Cisco Email Security Outbound 소프트웨어 서브스크립션에 포함된 **아웃바운드 안티스팸 스캐닝** 기능은 관리자가 도용된 계정에서 전송되는 스팸을 필터링할 수 있도록 지원합니다. Cisco의 유연한 라이센스는 안티스팸 스캐닝용 사용자 라이센스를 사용하여 인바운드 및 아웃바운드 이메일 흐름을 모두 스캔할 수 있도록 합니다.

AsyncOS 7.6의 새로운 기능인 **메일 발신자별 속도 제한** 기능은 특정 기간 사용자가 전송할 수 있는 이메일 수를 제한하도록 설정합니다. 제한 값에 도달하면 메시지의 아웃바운드 흐름이 중단되며 스팸 아웃바운드를 대량으로 쏟아내는 도용된 계정은 강제로 중지됩니다. 또한, 제한에 도달할 경우 특정 관리자 또는 헬프데스크 이메일 계정에 전달할 **경고 메시지도** 구성할 수 있습니다. **예외 목록을** 사용하면 특정 발신자(사용자 또는 자동 시스템)가 불가피하게 대량 이메일을 발송해야 하는 상황 등에서 속도 제한을 건너뛸 수 있습니다.

AsyncOS 7.5의 새로운 기능인 **대용량 스팸 메시지 스캐닝** 기능은 스캔할 항목에 대한 제한을 강화하여 스팸을 탐지하고 차단합니다. 스팸 생성자가 안티스팸 스캐닝을 피하려고 시도하는 한 가지 방법은 대용량 메시지를 작성하는 것입니다. 대용량 스팸 메시지 스캐닝 기능은 "Always Scan(항상 스캔)" 옵션의 기본 제한을 512KB로 올리고 "Never Scan(스캔 안 함)" 옵션의 최대 상한값을 1MB로 설정합니다. 이 두 크기 제한 사이에 속하는 메시지는 Cisco Anti-Spam에서 부분적으로 스캔됩니다.

작업 1: 수신 메일 정책에서 Outbreak Filters 구성

이러한 설정은 수신 메일 정책에 구성되어 있습니다.

1. 적절한 권한을 가진 계정을 사용하여 Email Security Appliance에 로그온합니다.
2. *Mail Policies*(메일 정책) > *Incoming Mail Policies*(수신 메일 정책)를 클릭합니다.
3. 원하는 정책 아래에서 *Retention Time: Virus 1 day*(보관 시간: 바이러스 1일) 하이퍼링크를 클릭합니다.

이렇게 하면 Outbreak Filters 설정을 구성할 수 있는 페이지가 표시됩니다.

4. *Enable Message Modification*(메시지 수정 사용) 확인 상자를 선택합니다.

Note: Enable Message Modification(메시지 수정 사용) 확인란을 선택하지 않으면 Virus Outbreak Filter 기능이 사용됩니다. 새 URL 재작성 기능을 사용하려면 이 확인 상자를 선택해야 합니다.

5. *Enable only for unsigned messages*(서명되지 않은 메시지에만 사용)를 클릭합니다.

이는 온전히 정책 결정 사항이지만, 모든 메시지에 URL 재작성을 사용할 경우 서명된 메시지의 시그니처가 분리됩니다.

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

6. *Bypass Domain Scanning*(도메인 스캔 건너뛰기) 상자에 URL 재작성을 건너뛰어야 할 도메인을 입력합니다. 여기에는 비즈니스 파트너가 포함될 수 있습니다.

이 기능을 사용할 경우 신중해야 합니다. 특정 도메인의 URL 재작성을 건너뛰도록 설정하면 감염된 시스템의 악성 메시지가 네트워크에 침투할 수 있습니다.

7. *System Generated*(시스템 생성) 위협 고지 사항을 선택하고 이를 클릭하여 미리 보기를 수행합니다.

맞춤형 위협 고지 사항을 사용하는 것은 정책 결정 사항입니다. 이러한 고지 사항은 *Mail Policies*(메일 정책) > *Text Resources*(텍스트 리소스) 구성 옵션을 사용하여 작성할 수 있습니다. 이메일에서 정보를 가져오는 변수를 맞춤형 고지 사항에 추가하여 최종 사용자에게 더욱 강력한 영향력을 행사할 수 있습니다. 언어 및 URL을 추가하여 회사 정책에 맞는 고지 사항을 제공할 수 있습니다.

8. *Submit*(제출)을 클릭한 다음 변경 사항을 *Commit*(적용)합니다.

작업 2: 대용량 스팸 메시지 스캐닝 확인

대용량 스팸 메시지 스캐닝의 기본값이 변경되지 않았는지 확인합니다. 이러한 기본값을 낮출 경우 실제 효과에 부정적인 영향을 미칠 수 있습니다.

1. *Security Services*(보안 서비스) > *Cisco Anti-Spam*을 엽니다.
2. 아래의 *Message Scanning Thresholds*(메시지 스캐닝 임계값)를 확인합니다.
   a. Always scan messages smaller than(다음보다 작은 메시지는 항상 스캔): 512KB.
   b. Never scan messages larger than(다음보다 큰 메시지는 스캔하지 않음): 1MB.

시스템에서는 Always Scan(항상 스캔) 설정(기본값: 512KB)과 Never Scan(스캔 안 함) 설정(기본값: 1MB) 사이에 속하는 메시지를 부분적으로 스캔합니다.

작업 3: 아웃바운드 안티스팸 스캐닝 구성

Cisco의 유연한 라이센스는 안티스팸 스캐닝(다른 기능과 함께 Cisco Virus Defense도 포함)를 사용하여 고객이 추가 라이센스 비용 없이 인바운드 스캔, 아웃바운드 스캔 또는 이 두 가지를 모두 스캔할 수 있도록 지원합니다. 대부분의 고객은 아웃바운드 스캔을 사용하지 않지만, 이를 활용하면 계약 의무(예: 비즈니스 파트너에게 스팸 발송 금지)를 준수하는 것은 물론, 감염된 시스템에 의해 조직이 이메일 블랙리스트에 등재되는 상황을 방지할 수 있습니다.

이러한 작업은 우선 랩 환경에서 모델링해야 하며, 아웃바운드 안티스팸 스캐닝을 구성하기 전에 최소한 어플라이언스의 부하를 검토하여 디바이스가 과부하 상태는 아닌지 확인해야 합니다. 메시지 필터를 사용하여 프로덕션 이메일 흐름의 부분적인 사본을 랩 환경에 전송한 다음, 서서히 양을 늘려 그에 따른 영향을 파악할 수 있습니다.

1. *Mail Policies*(메일 정책) > *Outgoing Mail Policies*(발신 메일 정책)를 엽니다.
2. 해당 정책 아래에서 수정할 *Anti-Spam*(안티스팸) 설정을 클릭합니다.
3. *Anti-Spam Scanning for This Policy: Use Cisco Anti-Spam service*(이 정책에 대해 안티스팸 스캐닝: Cisco Anti-Spam 서비스 사용)를 활성화합니다.

정책 요구 사항에 따라 몇 가지 추가적인 제어를 설정해야 합니다. 여기에는 명확하게 확인된 스팸 및 의심되는 스팸에 취할 조치가 포함됩니다.

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

4. *Submit*(제출)을 클릭하여 변경 사항을 *Commit*(적용)합니다. 이제 Outgoing Mail Policy(발신 메일 정책) 페이지에는 선택한 정책에 대해 Cisco Anti-Spam이 구성된 것으로 표시되어야 합니다.

작업 4: 발신자별 속도 제한 활성화 및 예외 목록과 제한에 대한 관리 알림 생성

발신자별 속도 제한 기능을 사용하면 사용자가 발송할 수 있는 이메일 수에 대한 시간 범위 기준 제한을 구성할 수 있습니다. 또한, 예외 목록 기능을 사용할 경우 업무 요구 사항에 따라 대량 이메일을 발송하는 사용자를 위해 예외를 생성할 수 있습니다. 조직의 아웃바운드 마케팅, 고객 지원 및 기타 부서에서는 이 방법을 통해 제한 없이 업무를 수행하는 동시에 감염된 호스트의 징후인 이상 현상을 모니터링하고 포착할 수 있습니다.

이 작업에 드는 구성 시간을 최소화하려면 이메일 발신자에 대한 제한을 설정하기 전에 예외 목록을 생성해야 합니다.

1. *Mail Policies*(메일 정책) > *Address Lists*(주소 목록)를 엽니다.
2. 속도를 제한하지 않으려는 이메일 주소 또는 와일드카드 주소를 사용하여 *Add Address List*(주소 목록 추가)를 실행합니다.

이러한 주소는 전체 주소 또는 부분 주소가 될 수 있습니다. 예를 들어, @.example.com은 @dc1.example.com과 같은 모든 하위 도메인에는 일치하지만 @example.com에는 일치하지 않을 수 있습니다. 제외할 이메일 주소의 또 다른 적절한 예는 조직의 경영진이 사용하는 주소입니다.

3. *Submit*(제출)만 클릭하고 *Commit*(적용)은 클릭하지 마십시오.

예외 목록이 생성되면 속도 제한을 구성할 수 있습니다.

4. *Mail Policies*(메일 정책) > *Mail Flow Policies*(메일 흐름 정책)를 엽니다.
5. *RELAYED*(전달됨)를 클릭하여 엽니다.

이 페이지에서 다양한 설정을 변경할 수 있습니다. 각 설정에서 어떤 작업을 수행하는지 파악하려면 제품 문서를 참조하십시오. 작업 내용을 올바르게 숙지하지 않은 상태에서 이 페이지의 내용을 변경하지 마십시오. 그럴 경우 조직의 메일 흐름에 부정적인 영향을 미칠 수 있습니다.

6. 아래로 스크롤해 Mail Flow Limits(메일 흐름 제한) 섹션으로 이동한 다음 *Rate Limit for Envelope Senders*(봉투 발신자에 대한 속도 제한)를 클릭하여 확장합니다.
7. *Max. Recipients Per Time Interval*(시간 간격당 최대 수신자)을 60분간 원하는 수신자 수로 설정합니다.

이는 사용자가 60분간 아웃바운드를 발송할 수 있는 이메일의 개수입니다. 이 값을 너무 낮게 설정하면 사용자 생산성에 영향을 미칠 수 있습니다. 또한, 너무 높게 설정하면 어카운트가 도용된 경우 원치 않는 이메일이 지나치게 많이 발송될 수 있습니다.

참고: 기간 변경은 Default Policy Parameters(기본 정책 매개변수)에서 완료합니다. 이 설정 및 미리 정의된 전체 정책 목록의 기본값은 *Unlimited*(무제한)입니다. Default Policy(기본 정책)에서 기간을 변경한 경우, HAT(호스트 액세스 테이블)에 있는 모든 정책 기간이 변경되며 이는 메일 흐름에 영향을 미칠 수 있습니다. 기본 정책에 대한 개시 기간을 변경할 경우, 향후 초기화하기 전에 이전에 설정된 기타 메일 흐름 정책의 기본값이 Unlimited(무제한)로 구성되어 있는지 확인해야 합니다.

8. Exceptions(예외) 아래에 있는 *Ignore Rate Limit for Address List*(주소 목록의 속도 제한 무시) 풀다운 메뉴에서 구성된 Address List(주소 목록)를 선택합니다.

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

9. 변경 사항을 *Submit*(제출)하되, 아직 *Commit*(적용)하지는 마십시오.

다음 단계는 관리 알림을 구성하는 것입니다. 이 알림은 구성된 속도 제한에 도달한 경우 전송됩니다. 속도 제한에 도달하면 조사를 시행하여 시스템이 감염되었으며 스팸을 전송하는 중인지 또는 사용자가 제한에 도달했으나 업무를 고려했을 때 이 사용자는 예외로 처리해야 하는지를 확인해야 합니다.

10. *System Administration*(시스템 관리) > *Alerts*(알림)를 엽니다.
11. 알림 수신자의 이메일 주소를 추가하고 시스템의 알림 유형을 *Info*(정보) 수준으로 설정합니다.

> 빠른 팁: 받은 편지함을 헬프데스크에서 모니터링하도록 설정하거나 헬프데스크 소프트웨어를 통해 문제 해결 티켓이 자동으로 열리도록 설정합니다. 이렇게 하면 올바른 담당자를 추적할 뿐만 아니라 알림도 전송할 수 있습니다.

12. 변경 사항을 *Submit*(제출)하고 *Commit*(적용)합니다.

작업 5: 구성된 기능 확인

이제 기능이 구성되었으며 이메일 보안 디바이스에 대한 변경 사항이 적용되었습니다. 이러한 기능에 대한 데이터는 Reporting(보고), Outbreak Filters Quarantine(Outbreak Filters 격리), Message Tracking(메시지 추적) 및 System Logs(시스템 로그)에서 확인할 수 있습니다. 또한, 구성에 따라 Cisco Anti-Spam Quarantine(Cisco Anti-Spam 격리)에서 메시지를 받을 수도 있습니다.

메일 발신자별 속도 제한에 대한 보고서는 *Monitor*(모니터링) > *Rate Limits*(속도 제한)에서 확인할 수 있으며 인시던트별 주요 원인 및 거부된 수신자별 주요 원인이 표시됩니다.

Cisco Anti-Spam 규칙에 포착된 메시지 수는 *Monitor*(모니터링) > *Overview*(개요) 보고서 또는 *Monitor*(모니터링) > *Outgoing Senders*(발신자) 보고서에서 확인할 수 있습니다.

Outbreak Filters에서는 임시 격리를 사용하여 의심스러운 메시지를 보류합니다. 메시지가 해제되면 Cisco Anti-Spam에서는 이메일이 격리되고 난 후 수신한 업데이트된 안티스팸 규칙을 모두 사용하여 해당 메시지를 다시 스캔합니다. 이 Quarantine(격리)에 액세스하려면 *Monitor*(모니터링) > *Quarantines*(격리)를 연 다음 *Outbreak* Quarantine(바이러스 격리)를 클릭하여 엽니다.

Outbreak Filters 보고서에 액세스하려면 *Monitor*(모니터링) > *Outbreak Filters*를 클릭합니다.

Message Tracking(메시지 추적)을 사용할 수 있으며 이 기능에서는 메시지가 Outbreak Filters, 안티스팸 또는 속도 제한에 의해 포착된 경우를 비롯한 다양한 경우에서 이 메시지의 속성을 보여줍니다.

mail_logs 로그 파일에서도 메시지 속성에 대한 정보가 포함됩니다.

로그 항목의 예는 다음과 같습니다.

```
Outbreak Filters: Fri Apr 20 09:02:09 2012 Info: MID 2099 quarantined to
"Outbreak" (Outbreak rule: Phish: Phish)
Rate Limiting per Mail From: Mon Jul 2 15:38:12 2012 Info: MID 2219 To:
<user2@example.com> From: <user1@internal.com> Rejected by Rate Limiting per
Envelope Sender
```

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

결론

구성된 기능을 조합하여 함께 사용하면 유입되는 스팸 공격을 강력하게 방어할 수 있습니다. 교육 기관에서는 추가적인 보고, 로그 항목 및 알림 이메일을 활용하여 문제를 신속하게 해결하고 이메일 블랙리스트에 등재되는 상황을 방지할 수 있습니다.

Cisco Anti-Spam 또는 Cisco Email Security에 대한 자세한 내용은 www.cisco.com/go/emailsecurity를 참조하십시오.

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.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

Printed in USA C11-720311-01 11/12

© 2012 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.