2015

연례 보안 보고서

Executive Summary

현대 위협 환경은 끊임없이 변화하고 있지만 변하지 않는 부분도 있습니다.

공격자들은 탐지를 우회하고 악의적인 활동을 은폐할 수 있는 새로운 기술을 끊임없이 발전시키며 개발하고 있습니다. 한편, 방어자들, 즉 보안 팀은 이렇게 점점 더 지능화되고 있는 공격으로부터 조직과 사용자를 보호하는 방식을 끊임없이 개선해야 합니다.

사용자는 중간에 끼어 있습니다. 최근 사용자는 공격 대상일 뿐만 아니라 자신도 모르는 사이에 공격을 지원하게되는 것으로 나타났습니다.

Cisco® Security Research 와 Cisco 내 여타의 보안 전문가들이 제공하는 *Cisco 2015 연례 보안 보고서*에서는 공격자와 방어자 간의 지속적인 경쟁과 보안 사슬에서 사용자들이 점점 더 취약한 링크가 되고 있는 현상에 대해 살펴보았습니다.

사이버 보안은 사용자, 기업, 정부는 물론 기타 전 세계의 조직에 엄청난 영향을 미치는 광범위하고 복잡한 문제입니다. *Cisco 2015 연례 보안 보고서*는 4가지 논의 영역으로 나누어져 있습니다. 각 섹션과 섹션 사이에서 설명하고 있는 문제는 언뜻 보기에는 서로 관련이 없는 것처럼 보이지만, 자세히 살펴보면 그 상관 관계를 알 수 있습니다.

Cisco 2015 연례 보안 보고서 의 4가지 논의 영역:

1. 위협 인텔리전스
2. Cisco 보안 기능 벤치마크 조사
3. 지정학 및 업계 트렌드
4. 사이버 보안에 대한 관점의 변화 - 사용자부터 기업 경영진까지

1. 위협 인텔리전스(Threat Intelligence)

이 섹션에서는 익스플로잇 킷, 스팸, 위협 및 취약점, 맬버타이징(malvertising, 악성 광고) 트렌드에 대한 업데이트를 비롯하여 Cisco의 최신 위협 조사 결과를 개괄적으로 소개합니다. 점점 더 사용자에게 공격 실행을 의존하는 온라인 범죄자들의 동향도 함께 살펴보았습니다. 2014년에 관찰된 트렌드를 분석하기 위해 Cisco Security Research에서는 포괄적인 텔레메트리 데이터를 활용했습니다. 보고서에서 언급한 위협 인텔리전스는 Cisco 내 최고의 보안 전문가들이 실시한 조사 결과입니다.

2. 보안 기능 벤치마크 조사(Security Capabilities Benchmark Study)

보안 전문가들이 자기 연구 조직의 보안 상태에 대해 어떤 인식을 갖고 있는지 파악하기 위해, Cisco에서는 9개국 다양한 조직 규모의 CISO(Chief Information Security Officer, 최고정보보호책임자)와 보안 담당 중역에게 보안 리소스 및 절차에 대해 질문했습니다. 그 연구 결과는 *Cisco 2015 연례 보안 보고서*에서만 볼 수 있습니다.

3. 지정학 및 업계 트렌드(Geopolitical and Industry Trends)

이 섹션에서는 Cisco 보안, 지정학 그리고 정책 전문가들이 조직, 특히 다국적 기업에서 모니터링해야 하는 현재 그리고 새로운 지정학적 트렌드에 대해 알아보았습니다. 특히, 거버넌스가 취약한 영역에 사이버 범죄가 얼마나 성행되고 있는지에 대해 집중적으로 알아보았습니다. 또한, 데이터 주권(Data Sovereignty), 데이터 현지화(data localization), 암호화 및 데이터 호환성과 관련하여 전 세계에서 최근 전개된 사건도 함께 살펴보았습니다.

4. 사이버 보안에 대한 관점의 변화 – 사용자부터 기업 경영진까지

Cisco 보안 전문가들은 조직이 실제적인 보안을 원한다면 조직에서 사이버 보안에 접근하는 방식을 달리해야 한다고 말합니다. 이러한 전략에는 공격의 전범위에서 전방위적으로 위협을 막을 수 있는 더욱 정교한 보안 제어 기능 도입, 기업 경영진 차원에서 보안 논의, 조직이 더 적극적으로 보안에 접근할 수 있는 보안 원칙인 Cisco 보안 강령(Cisco Security Manifesto) 실행을 들 수 있습니다. 또한, 공격자들보다 더 뛰어난 적응력과 혁신력도 필요합니다.

결론적으로 *Cisco 2015 연례 보고서*에서 다루고 있는 보안 문제들은 다음과 같은 연관성을 갖고 있습니다. 공격자는 자신의 악의적인 활동을 숨기고 은폐하기 위해 보안 허점을 활용하는 데 더 능숙해졌습니다. 사용자와 보안 팀도 보안 문제의 일부입니다. 많은 방어자들이 자신의 보안 프로세스가 최적화되어 있고 보안 툴이 효과적이라고 생각하지만, 사실은 보안 준비 상태를 개선해야 합니다. 법률 제정에서 보안 위협에 이르기까지 지정학적 환경에서 발생하는 일이 비즈니스 운영과 조직의 보안 문제 해결 방식에 직접적인 영향을 미칠 수 있습니다. 따라서, 이러한 점을 모두 고려할 때, 모든 규모의 조직에서 보안이 사람의 문제이고, 절충이 불가피하며, 지금이 보안에 대한 새로운 접근 방식을 택해할 시점이라는 것을 이해하는 것이 그 어느 때보다 중요합니다.

핵심 분석 결과

다음은 Cisco 2015 연례 보안 보고서의 핵심 분석 결과입니다.

공격자는 자신의 악의적인 활동을 숨기고 은폐하기 위해 보안 허점을 활용하는 데 더 능숙해졌습니다.

- 2014년에는 1퍼센트의 고위험 CVE(Common Vulnerabilities and Exposure, 일반 취약점 및 노출) 경고가 적극적인 공격을 받았습니다. 이것은 조직에서 이 1퍼센트의 모든 취약점에 대해 신속하게 우선 순위를 지정하고 패치해야 합니다. 하지만, 최고의 보안 기술을 사용하더라도, 보안 취약점을 해결하려면 뛰어난 프로세스가 필요합니다.
- 2013년 블랙홀 익스플로잇 킷(Blackhole exploit kit)이 사라진 이후 비슷한 수준의 성공을 거둔 익스플로잇 킷은 없습니다. 하지만, 익스플로잇 킷 개발자들이 예전만큼 1위 자리를 탐내지 않을 수도 있습니다.
- 자바(Java) 보안이 개선되고 공격자들이 새로운 공격 벡터를 수용함에 따라 자바 익스플로잇은 34퍼센트 감소했습니다.
- 플래시(Flash) 악성코드를 이제 자바스크립트(JavaScript)와 연동하여 악의적인 활동을 은폐하는 데 사용하기 때문에 탐지와 분석이 훨씬 더 어렵습니다.
- 스팸 양은 2014년 1월부터 2014년 11월까지 250퍼센트 증가했습니다.
- 보안 탐지를 피하기 위해 대량의 IP 주소에서 소량의 스팸을 발송하는 스노우슈(Snowshoe) 스팸이 새롭게 떠오른 위협입니다.

사용자와 IT 팀은 자신도 모르는 사이 보안 문제의 일부가 되었습니다.

- 온라인 범죄자들은 사용자에게 의존하여 악성코드를 설치하거나 보안 허점을 이용하고 있습니다.
- 위험한 보안 허점인 하트블리드(Heartbleed)에 의해 OpenSSL이 심각하게 노출되어 있습니다. 그러나 전체 OpenSSL 버전의 56퍼센트가 50개월 이상 된 것으로 여전히 취약합니다.
- 인터넷 사용 시 사용자의 부주의한 행동은 공격자의 표적 공격이 더해져 여러 업종을 더 큰 웹 악성코드 노출의 위험에 빠뜨리고 있습니다. Cisco Security Research에 따르면, 2014년에는 제약 및 화학 산업이 웹 악성코드 노출 위험이 가장 높은 업종으로 떠올랐습니다.
- 악성코드 작성자들은 웹 브라우저 애드온을 악성코드와 원치 않는 애플리케이션을 배포하는 매체로 사용하고 있습니다. 이런 악성코드 배포 방식은 많은 사용자가 근본적으로 애드온을 신뢰하거나 단순히 정상적인 것으로 간주하기 때문에, 악의적인 공격자에게 유용한 것으로 확인되고 있습니다.

***Cisco 보안 기능 벤치마크 조사* 결과, 보안 준비 상태에 대한 인식에 차이가 있는 것으로 나타났습니다.**

- CISO(Chief Information Security Officer, 최고정보보호책임자)의 59퍼센트가 자사의 보안 프로세스가 최적화되어 있다고 생각하는 반면, 보안 담당 중역은 46퍼센트가 그렇다고 응답했습니다.
- CISO의 약 75퍼센트가 자사의 보안 툴이 효과적 또는 매우 효과적이라고 생각하며 약 25퍼센트는 효과가 제한적이라고 생각하고 있습니다.
- 정교한 보안 툴을 보유한 기업의 응답자 중 91퍼센트가 회사 경영진이 보안을 최우선 순위로 생각한다고 응답했습니다.
- 응답자의 50퍼센트 미만이 패칭 및 컨피그레이션과 같은 표준 툴을 사용하여 보안 침해를 방지하고 있습니다.
- 규모가 더 큰, 중견기업이 조사에 포함된 다른 규모의 조직에 비해 보안 상태가 더 정교할 가능성이 높습니다.

목차

Executive Summary 2

핵심 분석 결과 4

공격자 대 방어자: 계속되는 경쟁 6

1. 위협 인텔리전스 6

웹 익스플로잇: 익스플로잇 킷 개발자의 경우 1위가 최고를 의미하지 않을 수도 있다 7

위협 및 취약점: 공격 벡터로서 Java 이용 감소 8

오래된 취약점의 발견: 오래된 소프트웨어의 위험성과 패칭이 유일한 솔루션이 아닌 이유 12

업종별 위험 보고서: 공격자의 표적 공격과 사용자의 부주의한 행동이 고위험 업종의 회사들을 위험에 빠뜨리고 있음 13

스팸 업데이트: 스패머, "스노우슈" 전략 채택 18

브라우저 애드온의 맬버타이징: 경미한 사용자별 피해, 엄청난 수익 21

2. Cisco 보안 기능 벤치마크 조사 24

Cisco 보안 기능: 조직이 기준에 얼마나 부합하는가? 24

3. 지정학 및 업계 트렌드 39

거버넌스가 취약한 영역에서 성행하는 사이버 범죄 39

데이터 주권, 데이터 현지화 및 암호화의 문제 40

데이터 정보 보호 호환성 41

4. 사이버 보안에 대한 관점의 변화 – 사용자부터 기업 경영진까지 43

보안 액세스: 누가, 언제, 어떻게 네트워크에 액세스하는지 이해 43

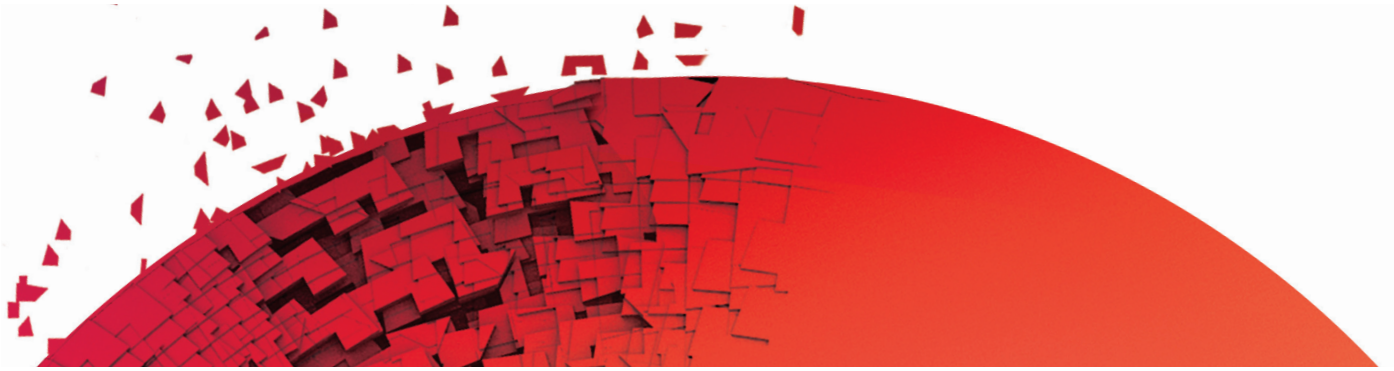
경영진의 참여에 달린 오늘날의 사이버 보안 45

Cisco 보안 선언: 현실의 보안을 달성하기 위한 기본 원칙 46

회사 소개 47

부록 48

미주 53



공격자 대 방어자: 계속되는 경쟁

보안 전문가와 온라인 범죄자는 상대방을 앞서기 위해 지속적으로 경쟁하고 있습니다.

보안 측면에서 기업은 공격을 방지하고 공격의 영향을 줄일 수 있는 더욱 정교한 툴을 채택함으로써 이 경쟁에서 우위를 차지한 것으로 보입니다. 기업은 비즈니스 측면에서 강력한 보안 상태의 필요성을 인식했으며, 자사의 보안 프로세스가 최적화되어 있다고 확신합니다. 기술 벤더들 또한 자사 제품에서 취약점을 찾아 수정하는 데 관심을 기울이고 있으며, 이로 인해 범죄자들이 익스플로잇을 실행할 기회가 최소화되고 있습니다.

하지만, 이와 동시에 공격자은 공격을 실행하는 방식뿐만 아니라 탐지를 피하는 데 더 지능화되고 있습니다.

- 매 순간 전술과 툴을 변경하여, 차단당하기 전에 네트워크에서 사라지거나 신속하게 다른 진입 방법을 선택합니다.
- 공격자들은 유명한 IP 기반 안티스팸 제품을 우회하기 위해 수백 개의 IP 주소를 사용하는 스팸 공격을 계획합니다.
- 지속적으로 감염시키고 시스템 내에 뻔히 보이는 곳에 숨어 있기 위해서 사용자가 신뢰하거나 정상적인 것으로 생각하는 툴에 의존하는 악성코드를 설계합니다.
- 벤더가 다른 제품에서 취약점을 차단하는 경우 새로운 취약점을 찾습니다.
- 공격의 표적이 되는 조직에 숨거나 섞여들기 위해 애쓰며, 때로는 수주 또는 수개월에 걸쳐 인프라 및 사용자 데이터베이스에 여러 개의 거점을 마련합니다. 준비가 되었을 때만 공격을 실행합니다.

최신 *Cisco 보안 기능 벤치마크 조사*(24페이지 참조)에 따르면, 보안 전문가들은 온라인 공격자를 저지할 준비가 잘 되어 있다고 자신 있게 말합니다. 하지만, 공격자들은 계속해서 정보를 훔치고, 사기 행위를 통해 돈을 벌고, 정치적인 목적으로 네트워크를 중단시킵니다. 결국, 보안은 숫자 게임입니다. 조직에서 수십억 개 스팸 메시지의 99.99 퍼센트를 차단해도 일부는 통과하게 됩니다. 100퍼센트 효과를 보장할 수 있는 방법은 없습니다.

이러한 메시지나 익스플로잇이 사용자에게 도달하게 되면, 사용자 자신이 네트워크의 취약점이 됩니다. 기업들이 네트워크 침입, 악성코드 및 스팸을 차단하는 솔루션을 사용하는 데 더욱 능숙해졌기 때문에, 대신 악의적인 공격자들은 허위 비밀번호 재설정 요청을 보내는 등의 방법으로 사용자를 속일 수도 있습니다.

사용자들이 점점 더 취약한 링크가 되고 있는 상황에서, 기업은 보안 기술 및 정책을 실현할 때 선택을 해야 합니다. 개발자들이 애플리케이션과 소프트웨어를 더 직관적이고 사용하기 쉽게 만들려고 노력함에 따라, 조직은 사이버 범죄자들이 공격할 수 있는 새로운 허점을 만들고 있는 것은 아닐까요? 조직은 사용자를 신뢰할 수 없거나 교육할 수 없다는 가정하에, 사용자를 무시하고, 사용자의 업무에 방해가 되는 더 엄격한 보안 제어 기능을 설치하고 있는 것은 아닐까요? 기업은 시간을 들여 사용자에게 보안 제어 기능을 설치하는 이유를 설명하고, 비즈니스를 지원하는 동적 보안을 달성하는 데 있어 사용자가 어떤 중요한 역할을 하는지에 대해 명확하게 설명하고 있을까요?

45페이지의 Cisco 보안 강령에 설명되어 있듯이, 기업들은 후자에 해당합니다. 사용자가 기술 솔루션을 통해 적극적으로 참여하여 보안을 관리하기는 매우 힘듭니다. 오히려, 기술 솔루션 때문에 업무 수행에 방해가 되는 보안 툴을 피해 일하게 되고, 따라서 비즈니스의 보안 수준이 약화됩니다. 보안은 더 이상 네트워크가 감염될 것인지 여부에 대한 문제가 아닙니다. 모든 네트워크는 어느 시점에는 *반드시* 감염될 것입니다. 그런 상황이 발생하면 조직은 무엇을 해야 할까요? 더불어, 보안 직원이 네트워크가 감염될 것임을 안다면 다른 방식으로 보안에 접근할 수 있을까요?

*Cisco 2015 연례 보안 보고서*에는 Cisco Security Research 그룹의 최신 조사 결과가 포함되어 있습니다. 연구 팀에서는 보안 업계에서 조직과 사용자가 공격을 방어하는 데 도움이 될 수 있도록 개발한 새로운 기술과 함께, 공격자가 이러한 방어망을 뚫기 위해 채택한 기술과 전략에 대해서도 살펴보았습니다. 또한 기업의 보안 상태와 공격 방어 준비 상태에 대한 인식을 조사한 *Cisco 보안 기능 벤치마크 조사*의 주요 분석 결과를 보고서에서 알아볼 수 있습니다. 지정학적 트렌드, 데이터 현지화(data localization)에 관한 전 세계적인 국면, 더 정교한 보안 액세스 제어 기능의 가치, 역할 기반 액세스를 기반으로 한 세그멘테이션, 그리고 경영진 논의 주제로서 사이버 보안 문제의 중요성에 대해서도 살펴보았습니다.

1. 위협 인텔리전스

Cisco Security Research에서는 광범위한 델레메트리 데이터를 기반으로 이 보고서에 보안 인사이트(insight)를 정리하고 분석했습니다. Cisco의 보안 전문가들은 향후 발생할 수 있는 범죄 행위를 파악하고 위협 탐지에 도움을 줄 수 있는 악성코드 트래픽과 같은 발견된 위협을 지속적으로 연구하고 분석합니다.

웹 익스플로잇: 익스플로잇 킷 개발자의 경우 1위가 최고를 의미하지 않을 수도 있다

기업은 업계에서 최고가 되기 위해 노력합니다. 하지만, 소위 "지하 경제"에서 활동하는 익스플로잇 킷 개발자의 경우에는 주요 익스플로잇 킷 중에서 4위나 5위를 유지하는 것은 명백하게 성공을 거두었다는 표시 일수 있다고 Cisco Security Research는 말합니다.

*Cisco 2014 중기 보안 보고서*에서 보고 되었듯이, 2013년 이후 확실한 1위를 차지한 익스플로인 킷은 없습니다.[1] 2013년은 당국에서 개발자 및 배포자로 알려진 "폰치(Paunch)"를 체포한 후, 널리 사용되고 잘 관리되던 매우 효과적인 블랙홀 익스플로잇 킷(Blackhole exploit kit)을 축출한 해입니다. Cisco Security Research에서는 아직 지배적인 익스플로잇 킷이 존재하지 않는 이유가 단지 경쟁자들 중에 진정한 기술적 리더로 등극한 킷이 없기 때문이라고 말합니다. 또 한 가지 관찰된 트렌드는 폰치와 블랙홀이 와해된 이후, 탐지를 피할 수 있는 기능적 측면에서 더 많은 익스플로잇 킷 사용자들이 기술적으로 더 정교한 킷에 투자하는 경향이 있다는 것입니다.

Cisco 보안 보고서에 따르면, 2014년 한 해 동안 "실전에서" 가장 자주 관찰된 익스플로잇 킷은 앵글러(Angler), 스위트 오렌지(Sweet Orange) 및 군(Goon)입니다. 전체 익스플로잇 킷 가운데 앵글러가 2014년 동안 현장에서 가장 자주 탐지되었으며, 명확하지 않은 이유로 8월 말에 특히나 확산되었습니다. Cisco Security Research에서는 앵글러가 인기를 얻은 이유는 개발자가 윈도우 실행 파일을 다운로드하지 않고도 악성코드를 전달할 수 있도록 했기 때문이라고 보고 있습니다.

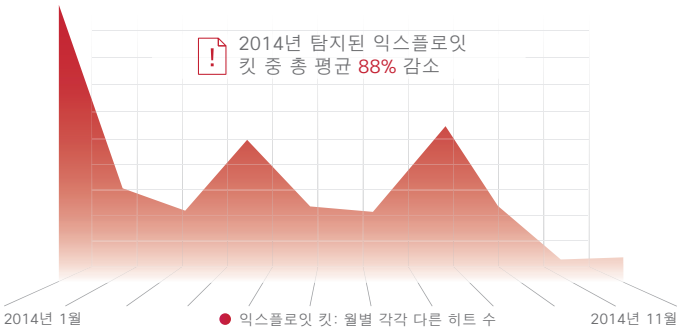
Cisco의 조사자들은 앵글러가 플래시(Flash), 자바(Java), Microsoft IE(Internet Explorer)와 심지어 실버라이트의 취약점을 이용하므로 "주목해야 할" 익스플로잇 킷이라고 말합니다. 공격을 실행하게 되면, 악성코드 페이로드가 과정을 통해 iexplore.exe와 같이 디스크가 아닌 메모리에 직접 작성됩니다. 앵글러에 의해 전달되는 페이로드는 암호화된 데이터의 오점처럼 보이기 때문에 식별하고 차단하기가 더 어렵습니다.

"Angling for Silverlight Exploits"를 참조하기시 바랍니다.

스위트 오렌지 익스플로잇 킷 역시 매우 동적입니다. 구성 요소, 포트와 페이로드 URL을 끊임없이 변화시켜 효과를 유지하고 탐지를 피할 수 있습니다. Cisco Security Research에 따르면, 이 때문에 스위트 오렌지는 익스플로잇 킷 중에서 "성공할 가능성이 가장 높다"고 합니다. 스위트 오렌지는 다양한 악성코드를 패칭되지 않은 최종 사용자의 시스템에 배포하며 어도비 플래시 플레이어(Adobe Flash Player), 인터넷 익스플로러 및 자바의 취약점에 대한 익스플로잇도 포함합니다. 스위트 오렌지를 사용하는 공격자는 합법적인 사이트를 포함하여 익스플로잇 킷을 호스팅하는 웹사이트로 사용자를 리디렉션하도록 보통 맬버타이징(malvertising)에 의존합니다. 사용자는 이 과정에서 일반적으로 적어도 2번 리디렉션 됩니다. 워드프레스(Wordpress), 줌라(Joomla)와 같은 CMS(content management system, 콘텐츠 관리 시스템)의 구 버전을 실행하는 감염된 웹사이트도 스위트 오렌지 익스플로잇 킷을 호스팅하는 데 이용되는 것으로 알려져 있습니다.[2]

군(Goon) 익스플로잇 킷의 경우, 2014년에 크진 않지만 꾸준한 인기를 얻은 이유는 신뢰성에 대한 평판 때문이라고 Cisco Security Research에서는 지적합니다. 군(Goon)은 또한 "가장 체계적인" 익스플로잇 킷이라는 명성을 얻었습니다. 2013년 보안 전문가들에 의해 처음 발견되었으며 "군/인피니티 익스플로잇 킷(Goon/Infinity exploit kit)"으로도 알려진 군은 악성코드 배포 프레임워크로서 윈도우(Windows)와 맥(Mac) 플랫폼에서 플래시, 자바 또는 실버라이트 구성 요소와 관련된 브라우저 취약점에 사용할 수 있는 익스플로잇을 생성합니다.[3]

그림 1. 익스플로잇 킷 트렌드: 2014년 1월부터 11월까지 탐지된 Unique Hit 수



출처: Cisco Security Research

기업에서 피에스타 익스플로잇 킷(Fiesta exploit kit)을 방어할 수 있는 방법에 대해 알아보려면 Cisco 보안 블로그에서 "Fiesta Exploit Pack Is No Party for Drive-By Victims"를 참조하기시 바랍니다. 이 킷은 실버라이트와 같은 공격 벡터를 통해 악성코드를 전달하고 동적 DDNS(Dynamic DNS domains)를 익스플로잇 랜딩 페이지로 사용합니다.

"Evolution of the Nuclear Exploit Kit"를 참조하시기 바랍니다.

블랙홀 익스플로잇 킷이 소멸된 후 몇 개월 동안 현장에서 탐지된 전체 익스플로잇 킷 수는 87퍼센트 감소했지만, 2014년 여름 동안 Cisco Security Research에 의해 탐지된 킷의 수는 증가했습니다(그림 1 참조). 8월 마지막 2주간 현장에서 탐지된 앵글러 익스플로잇 킷의 수가 크게 증가했습니다. 하지만, 11월이 되자 알려진 익스플로잇 킷의 전체 탐지 건 수는 다시 한 번 감소했으며, 여전히 앵글러 및 군/인피니티가 가장 자주 탐지되었습니다. 2014년 5월과 11월 사이에 탐지된 전체 익스플로잇 킷의 전체 평균 감소율은 88퍼센트였습니다.

위협 및 취약점: 공격 벡터로서 Java 이용 감소

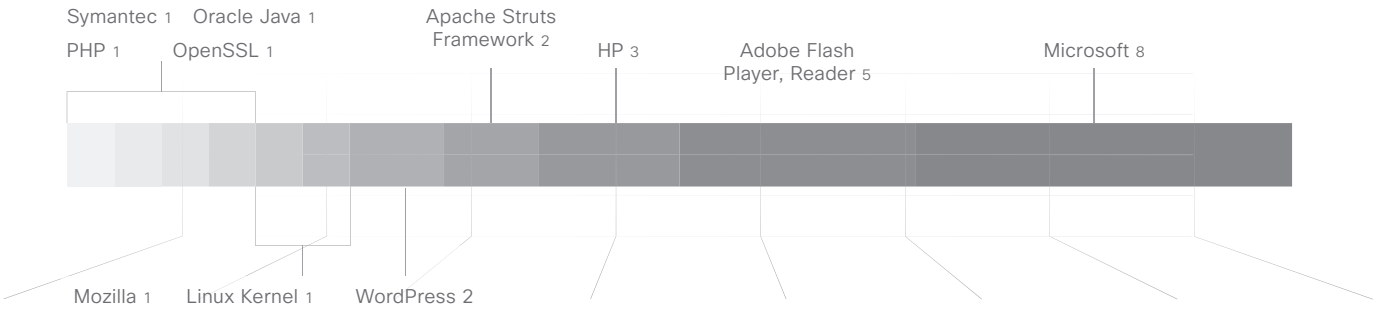
최근 수년간 자바는 본의 아니게 가장 보편적이고 심각한 취약점으로 이용되었습니다. 하지만, Cisco Security Research에 따르면, 소프트웨어 취약점을 이용하여 익스플로잇을 실행할 수 있는 가장 빠르고, 쉽고, 탐지가 어려운 방법을 찾고 있는 공격자들은 더 이상 자바를 선호하지 않는 것으로 보입니다.

2014년 1월 1일부터 2014년 11월 30일까지 상위 25개의 벤더 및 제품 관련 취약점 경고 중에서 단지 1개만이 자바 관련 경고였습니다(10페이지 표 1의 CVSS(Common Vulnerability Scoring System) 차트 참조). 2013년 Cisco Security Research에서는 54개의 긴급한 새 자바 취약점을 추적했습니다. 2014년에 추적한 자바 취약점의 수는 19개로 감소했습니다. 하지만 이는 오늘날에도 존속되는 이 오래된 취약점에 대한 공격의 인기와 효율성으로부터 온라인 범죄자들의 관심이 완전히 떠났다는 의미는 아닙니다.

NVD(National Vulnerability Database, 미국의 NIST 취약점 데이터베이스)의 데이터도 비슷한 감소세를 보입니다. NVD는 2013년에 309개의 자바 취약점을 보고했으나 2014년에는 253개의 새로운 자바 취약점을 보고했습니다. (Cisco Security Research에서는 CVSS 점수가 높은 중요한 취약점을 추적하기 때문에 숫자가 적지만, NVD에는 보고된 모든 취약점이 포함됩니다.) 그림 2는 2014년의 벤더 및 제품별 주요 취약점 익스플로잇입니다.

어도비 플래시 플레이어 및 Microsoft IE의 클라이언트 측 취약점과 관련된 익스플로잇이 서버를 표적으로 하는

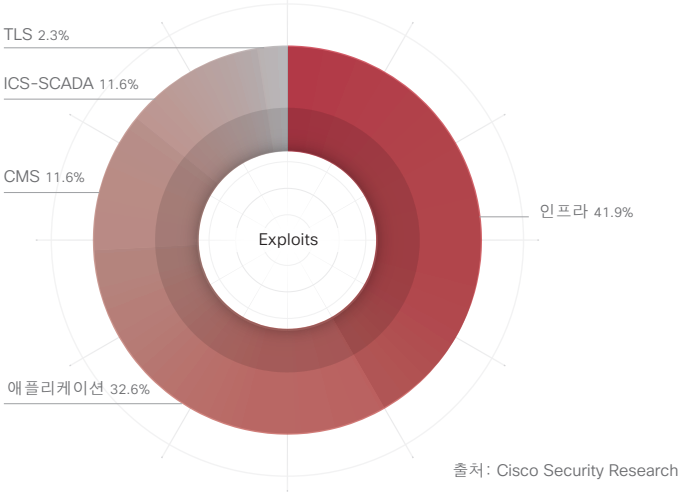
그림 2. 상위 벤더 및 제품 취약점 익스플로잇



출처: Cisco Security Research

보고서 공유

그림 3. 공격 받은 주요 품목



출처: Cisco Security Research

익스플로잇과 함께 자바 대신 1위 자리를 차지했습니다(예를 들어, 오픈소스 웹 프레임워크, 아파치 스트럿츠 프레임워크(Apache Struts Framework)의 취약점과 관련된 익스플로잇). 아파치 스트럿츠 프레임워크 익스플로잇의 증가는 공격자들이 공격 범위와 기능을 확장하기 위한 수단으로 온라인 인프라를 감염시키는 트렌드를 보여주는 예입니다.

아파치 스트럿츠 프레임워크는 그 인기 때문에 익스플로잇의 시작점으로 사용하기에 적합합니다.

그림 3에서 2014년에 가장 많이 공격을 받은 품목을 볼 수 있습니다.

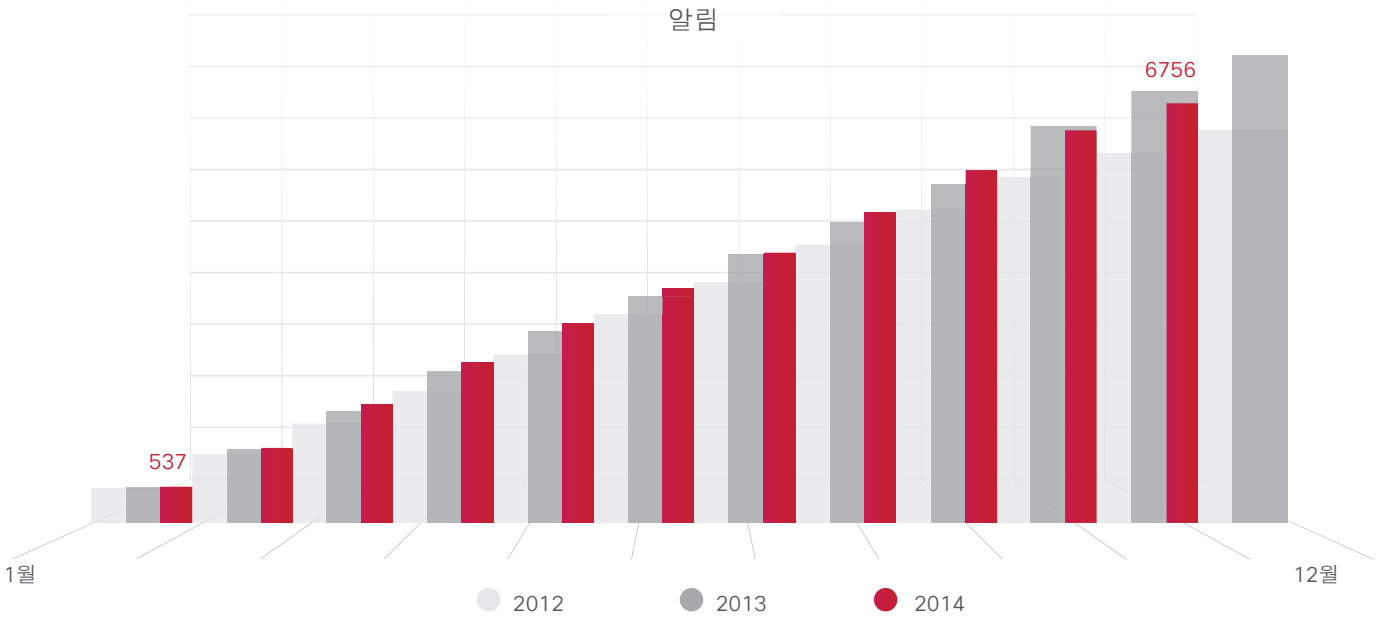
Cisco Security Research 데이터에 따르면, 2014에는 애플리케이션 및 인프라가 가장 자주 공격을 받았습니다. CMS(Content management system) 역시 선호하는 표적입니다. 공격자들은 익스플로잇을 전달하는 데 CMS 구 버전을 실행하는 웹사이트에 의존합니다.

연간 누적 경고 수 감소

2014년에 보고되고 Cisco Security Research에서 정리한 새로운 제품 취약점과 업데이트된 제품 취약점 누적 수, 연간 경고 합계는 감소한 것으로 보입니다(그림 4). 2014년 11월 현재, 총 경고 수는 2013년 합계보다 1.8퍼센트 감소했습니다. 감소율은 낮지만 최근 수년간 전년도에 비해 경고 수가 감소한 것은 처음입니다.

이런 감소세를 보인 이유는 소프트웨어 테스트와 개발에 대한 벤더의 관심이 증가했기 때문일 가능성이 가장 큽니다. 개발 라이프 사이클이 개선되어 범죄자들이 쉽게 이용할 수 있는 취약점의 수가 감소한 것으로 보입니다.

그림 4. 연간 누적 경고 합계



출처: Cisco Security Research

보고서 공유

표 1. 공격 빈도가 가장 높은 취약점

CVSS(Common Vulnerability Scoring System)

IntelliShield ID	제목	긴급도	신뢰도	심각도	기본	임시
33695	OpenSSL TLS/DTLS 하트비트 정보 노출 취약점				5.0	5.0
35880	GNU Bash 환경 변수 콘텐츠 처리 임의 코드 실행 취약점				10.0	7.4
35879	GNU Bash 환경 변수 기능정의 처리 임의 코드 실행 취약점				10.0	7.4
36121	Drupal Core SQL 주입 취약점				7.5	6.2
32718	Adobe Flash Player 원격 코드 실행 취약점				9.3	7.7
33961	Microsoft Internet Explorer 삭제된 메모리 객체 코드 실행 취약점				9.3	7.7
28462	Oracle Java SE 보안 우회 임의 코드실행 취약점				9.3	7.7
30128	복수 공급업체 제품 스트럿 2 작업: 매개 변수 처리 명령 주입 취약점				10.0	8.3

출처: Cisco Security Research

새로운 경고 vs. 업데이트된 경고

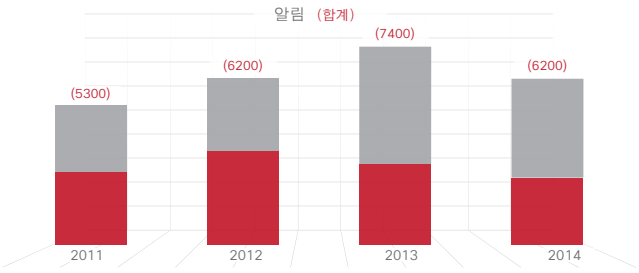
2013년과 2014년의 새로운 경고 수를 살펴보면 계속해서 전년도보다 더 많은 수의 새로운 취약점이 보고되고 있으며, 이는 벤더, 개발자 및 보안 전문가가 해당 제품에서 더 많은 새로운 취약점을 찾고, 수정하고, 보고하고 있다는 것을 의미합니다. 그림 5에 나타난 바와 같이, 2014년의 새로운 경고의 총 수 및 연간 합계는 2013년과 같거나 2013년보다 약간 감소했습니다.

표 1은 CVSS(Common Vulnerability Scoring System)에 따른, 가장 보편적으로 공격당한 취약점 중 일부를 보여줍니다. 미국 NIST(National Institute of Standards and Technology)의 NVD(National Vulnerability Database, 취약점 데이터베이스)는 IT 취약점의 특성과 영향에 대한 정보를 공유할 수 있는 프레임워크를 제공하며 CVSS를 지원합니다. CVSS 차트의 "긴급성(Urgency)" 점수는 해당 취약점이 적극적인 공격을 받고 있다는 것을 나타냅니다. 이는 활발한 공격을 나타내는 "시간적(Temporal)" 점수와 일치합니다. 기업은 또한 공격 대상이 된 제품의 목록을 검사하여, 현재 사용 중이며 따라서 모니터링하고 패치해야 하는 제품을 파악할 수 있습니다.

그림 6은 CVSS 점수가 가장 높은 벤더와 제품을 보여줍니다. Cisco에서는 CVSS 점수를 통해 개념 증명 익스플로잇 코드가 존재한다는 것을 보여줍니다. 하지만, 이 코드는 공개되지 않은 것으로 알려져 있습니다.

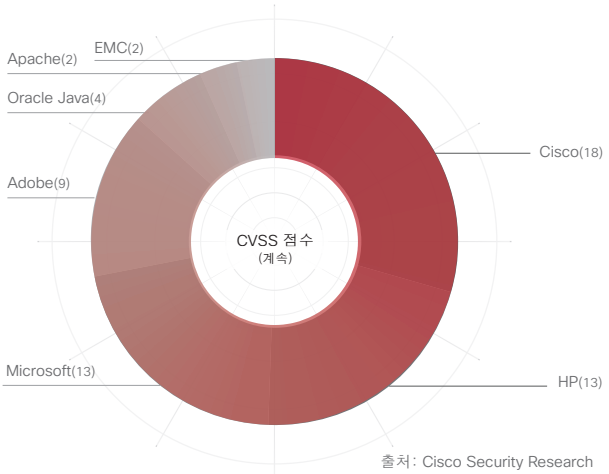
참고: 표 1의 취약점은 관찰한 기간 동안 익스플로잇 활동의 초기 징후를 보여주는 취약점이었습니다. 이러한 취약점 중 대부분은 아직 주류로 진입하지는 않은 것이며, 이는 해당 취약점이 아직은 판매용 익스플로잇 킷이 되지는 않았다는 의미입니다.

그림 5. 새로운 경고와 업데이트된 경고의 비교



출처: Cisco Security Research

그림 6. CVSS 점수가 가장 높은 벤더 및 제품



출처: Cisco Security Research

보고서 공유

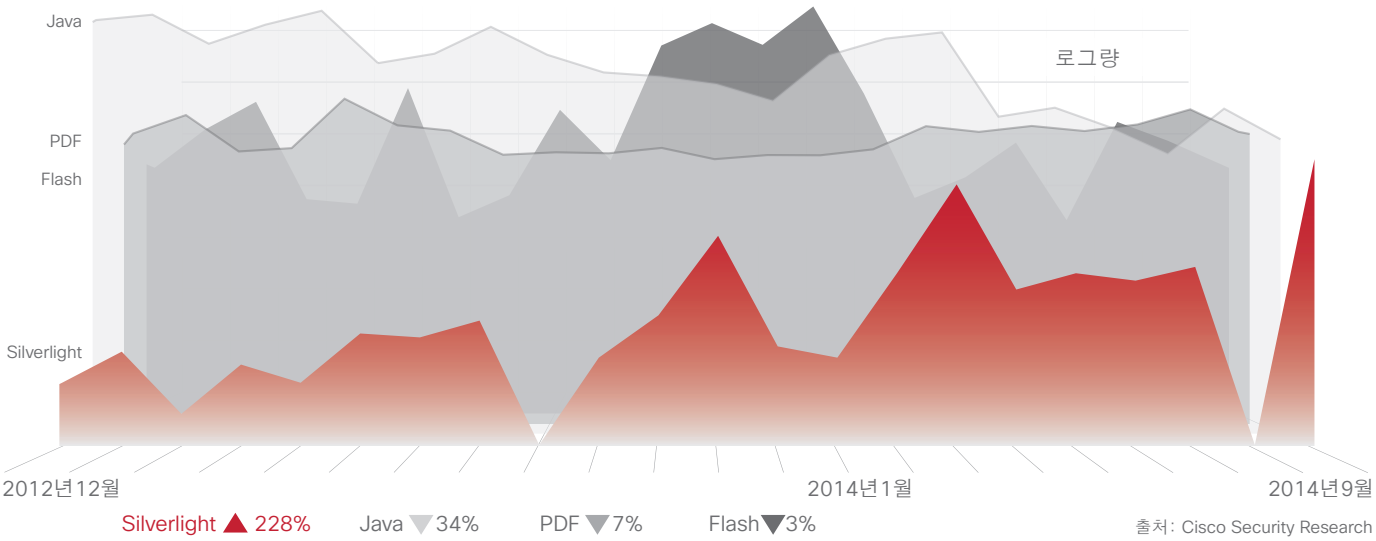
분석: 공격자들이 자바 익스플로잇을 포기한 이유

2014년에 자바 익스플로잇이 감소한 것은 부분적으로 공격자들이 이용할 수 있는 새로운 제로 데이 자바 익스플로잇이 공개되지 않은 사실과 관련이 있다고 Cisco Security Research에서는 말합니다. 자바의 최신 버전은 자동으로 패치되며, 더 오래되고 취약한 Java Runtime Environment 버전은 브라우저 벤더에 의해 기본적으로 차단되고 있습니다. Apple은 자동 업데이트를 통해 오래되고 취약한 자바 버전을 비활성화하는 데 심지어 한 단계를 더 취하고 있습니다. 또한, US-CERT(U.S. Computer Emergency Readiness Team)는 2013년 1월부터 컴퓨터 사용자에게 자바를 보안, 비활성화 또는 삭제할 것을 권장하고 있습니다.

최신 자바 버전인 Java 8은 이전 버전보다 강력한 제어 기능을 갖추고 있습니다. 또한, 이제 코드 서명 및 사용자에게 자바를 활성화할 것을 요청하는 사용자 대화 상자 등 사용자 상호작용이 필요하기 때문에 공격하기가 더 어렵습니다. 온라인 범죄자들은 더 쉬운 표적을 발견했으며 더 높은 투자 수익을 낳는 자바 외의 벡터로 주의를 돌렸습니다. 예를 들어, 많은 사용자들이 어도비 플래시(Adobe Flash)와 PDF 리더 그리고 브라우저를 정기적으로 업데이트하지 않기 때문에, 범죄자가 공격할 수 있는 더 광범위하게 오래된 취약점과 새로운 취약점을 제공하고 있습니다. 더불어, *Cisco 2014 중기 보안 보고서*에서 보고했듯이 Microsoft 실버라이트(Silverlight) 익스플로잇이 포함된 익스플로잇 킷의 수가 증가하고 있습니다.[4]

그림 7을 보면 자바를 주요 공격 벡터로 사용하는 경우가 1년 이상 꾸준히 감소했다는 것을 알 수 있습니다. 플래시를 사용하여 익스플로잇을 실행하는 경우는 다소 불규칙적이었으며 2014년 1월에 가장 많이 증가했습니다. PDF는 일정하게 사용되고 있으며, 따라서 많은 악의적인 공격자가 여전히 PDF 파일이 첨부된 이메일을 이용해 고도의 표적 공격을 실행하는 데 집중하고 있는 것으로 보입니다. 실버라이트 공격은 더 확실히 자리를 잡은 다른 벡터에 비해 여전히 매우 적은 수이지만, 8월 이후 특히 증가하고 있습니다.

그림 7. 공격 벡터별 용량 트렌드 비교



출처: Cisco Security Research

플래시와 자바스크립트: 함께 할 때 더 효율적일까?

2014년에는 자바스크립트(JavaScript)와 상호작용하는 플래시 악성코드를 사용하는 경우가 증가하는 것을 Cisco Security Research는 관찰했습니다. 이 익스플로잇은 플래시 파일 하나와 자바스크립트 파일 하나, 2개의 서로 다른 파일에 공유됩니다. 2개의 서로 다른 파일이나 형식 간에 익스플로잇을 공유하면 보안 디바이스에서 익스플로잇을 식별하여 차단하고 리버스 엔지니어링 툴을 사용하여 분석하기가 더 어렵습니다. 이 접근 방식은 또한 공격자가 더 효율적이고 효과적으로 공격을 실행하는 데 도움이 됩니다. 예를 들어, 공격의 첫 번째 단계가 전적으로 자바스크립트에서 실행될 경우 자바스크립트가 성공적으로 실행될 때까지는 두 번째 단계인 페이로드 전송이 발생하지 않습니다. 이 방법으로, 악성 파일을 실행할 수 있는 사용자만 페이로드를 받게 됩니다.

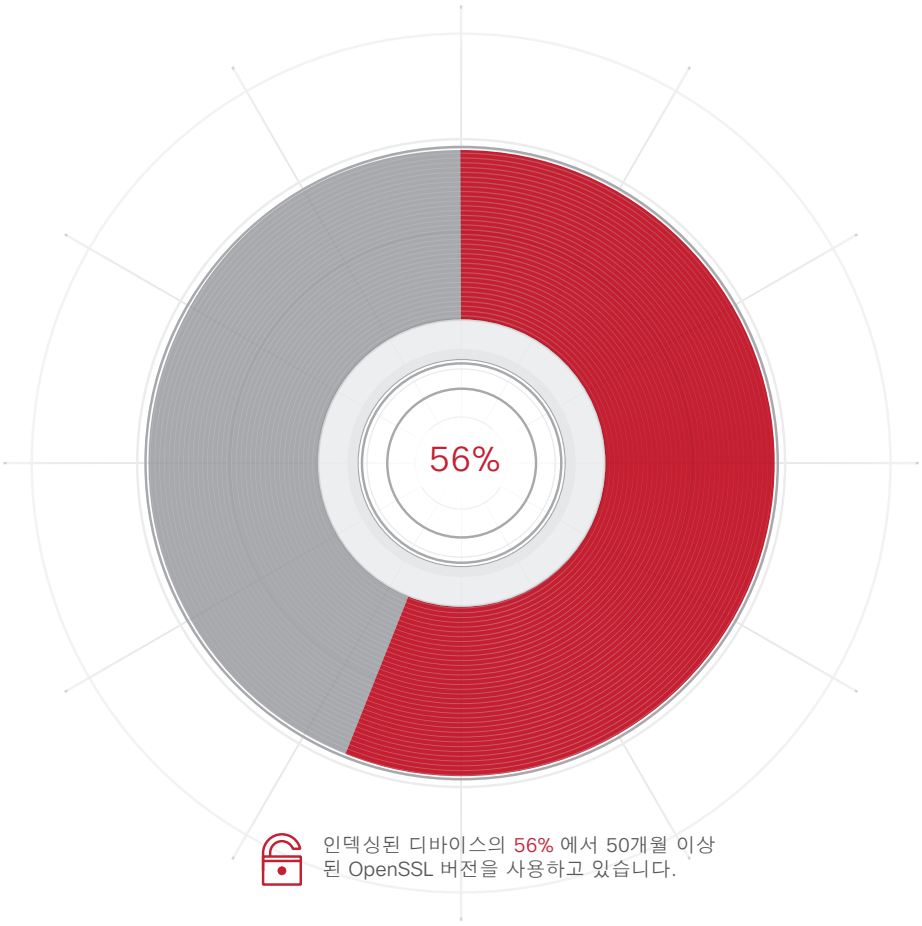
보고서 공유

오래된 취약점의 발견: 오래된 소프트웨어의 위험성과 패칭이 유일한 솔루션이 아닌 이유

취약점에 대한 논의에서 설명한 바와 같이(8페이지 참조), 공격자들은 익스플로잇이 성공할 방법과 위치를 결정할 때 이용 가능한 가장 쉬운 경로를 선택합니다. 이들은 더 많은 공격 표면 기회를 제공하는 제품을 선택하며, 이러한 기회는 일반적으로 패치되지 않거나 오래된 소프트웨어를 사용할 경우 생겨납니다. 예를 들어 많은 시스템이 여전히 SSL Poodle 공격에 취약하기 때문에, 어플라이언스를 패칭하는 것이 쉽지 않습니다.[5] 관찰된 트렌드를 토대로 Cisco Security Research에서는 공격 가능한 오래된 소프트웨어의 확산이 대규모 보안 문제로 계속 이어질 것으로 예상합니다.

Cisco Security Research에서는 검사 엔진을 사용하여 인터넷에 연결되어 있으며 OpenSSL을 사용 중인 디바이스를 조사했습니다. 조사 결과, 조사 대상 디바이스의 56퍼센트가 50개월 이상 된 OpenSSL 버전을 사용하고 있는 것으로 확인되었습니다. 즉, 2014년에 발견된 TLS(Transport Layer Security) 취급 관련 보안 허점인 하트블리드(Heartbleed)가 확산되고,[6] 이 취약점을 피하기 위해서는 OpenSSL 소프트웨어를 시급히 최신 버전으로 업그레이드해야 하는데도 불구하고, 많은 조직이 아직도 최신 버전을 사용하지 않고 있습니다. 그림 8은 사용 중인 OpenSSL 버전을 보여줍니다.

그림 8. OpenSSL 버전 연령



출처: Cisco Security Research

보고서 공유

가능한 솔루션: 자동 업데이트 및 패칭

자동 업데이트를 더 많이 사용하여 오래된 소프트웨어 문제를 해결할 수도 있습니다. Cisco Security Research에서는 온라인으로 연결되어 있으며 Chrome 또는 IE 브라우저를 사용하는 디바이스의 데이터를 조사했습니다. 조사 결과, Chrome 요청의 64퍼센트가 최신 버전에서 시작되었습니다. IE 사용자의 경우, 10퍼센트만 최신 버전을 사용하여 요청되었습니다.

Cisco Security Research에서는 Chrome의 자동 업데이트 시스템 덕분에 최대한 많은 사용자가 최신 소프트웨어 버전을 사용하고 있다고 생각합니다. (또한, Chrome 사용자가 IE 사용자보다 기술적으로 능숙하고, 따라서 브라우저를 업데이트하고 업데이트를 설치할 가능성이 더 높습니다.)

조사 결과, 자바 취약점 및 이를 이용한 공격의 감소와 더불어, 업데이트를 자동으로 설치하는 소프트웨어가 안전한 보안 프레임워크를 구축하는 데 더 유리한 것으로 보입니다. 수동 업데이트 프로세스에 따라 확실히 발생할 궁극적인 감염을 극복하기 위해서는 조직에서 자동 업데이트가 간혹 실패하고 호환되지 않는 문제를 받아들여야 할 수도 있습니다.

업종별 위험 보고서: 공격자의 표적 공격과 사용자의 부주의한 행동이 고위험 업종의 회사들을 위험에 빠뜨리고 있음

2014년에는 제약 및 화학 업종이 웹 악성코드 발생에 대한 노출 위험이 가장 큰 업종으로 떠올랐습니다. 2014년 전반기에는 언론 및 출판 업종이 1위 자리를 지켰지만, 11월에는 2위로 하락했습니다. 나머지로는 제조, 운송 및 배송, 항공 업종이 각각 5위 안에 들었습니다. 2014년 전반기에는 이들 업종이 모두 5위 안에 들었습니다.

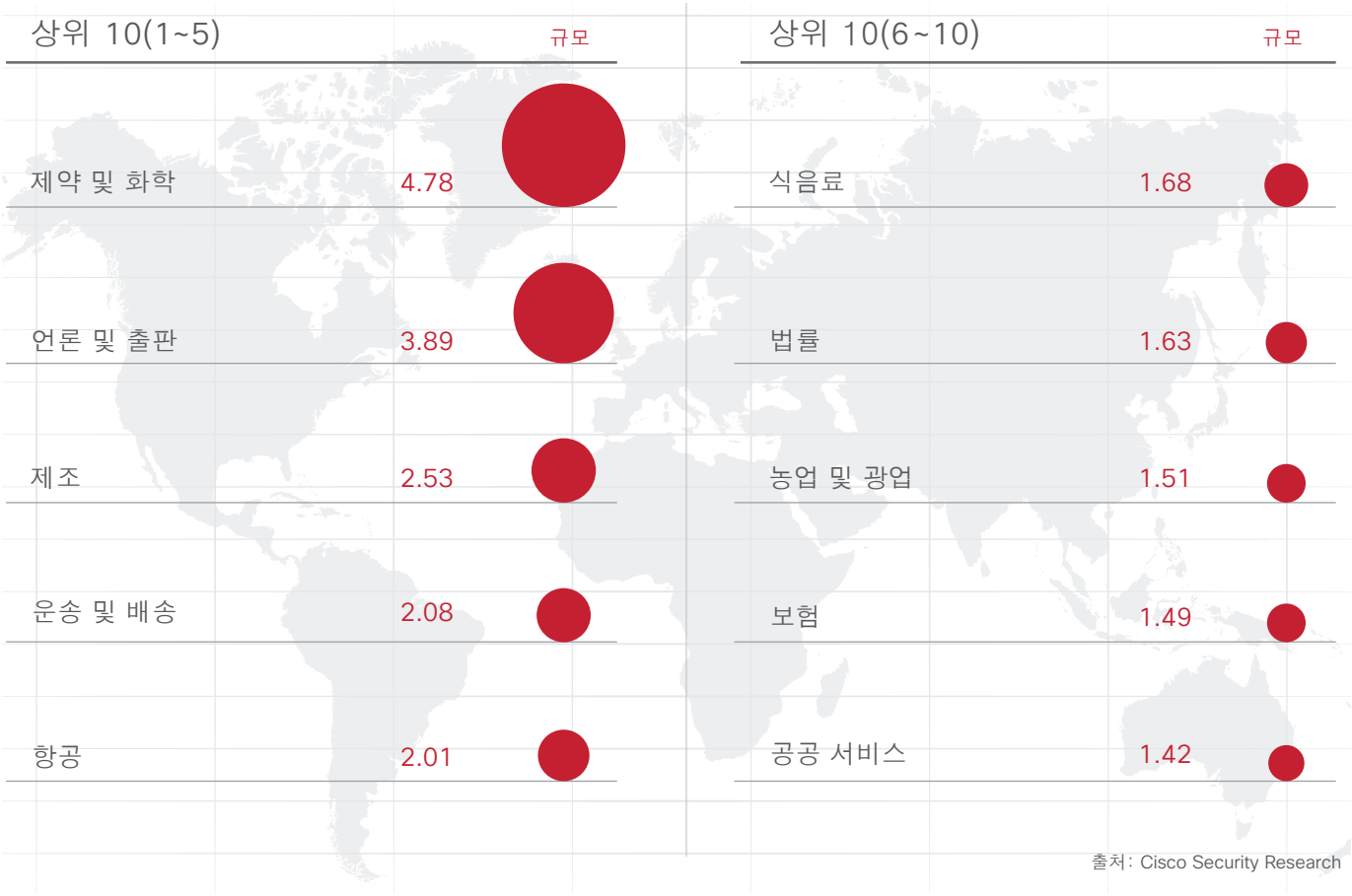
최근에 세간의 이목을 끄는 공격이 업계를 강타했기 때문에 소매 업종이 높은 순위를 차지했을 것으로 예상할 수도 있지만, 순위 산정에 고려되는 것은 실제적인 침해가 아니라 악의적인 발생입니다.

Cisco Security Research에서는 업종별 악성코드 발생 현황을 알아보고자 Cisco Cloud Web Security를 사용하는 모든 기업의 악성코드 발생률 중앙치(median)와 이 서비스를 사용하는 특정 업종에 속한 모든 기업의 악성코드 발생률 중앙치를 비교했습니다(그림 9). 업종의 발생률이 1보다 크면 평균적인 웹 악성코드 발생 위험보다 높고, 1보다 작으면 위험도가 낮은 것입니다. 예를 들어 발생률이 1.7인 기업은 중앙치에 해당하는 곳에 비해 위험이 70퍼센트 더 높습니다. 반대로, 발생률이 0.7인 기업은 중앙치보다 발생 위험이 30퍼센트 더 낮습니다.

발생과 감염

"발생(encounter)"은 악성코드가 차단되는 경우입니다. "감염(compromise)"과 달리 사용자는 바이너리 파일이 다운로드되지 않았기 때문에 발생 단계에서 감염되지 않습니다.

그림 9. 웹 악성코드 발생의 업종별 위험,
모든 영역, 2014년 1월 1일 – 11월 15일



출처: Cisco Security Research

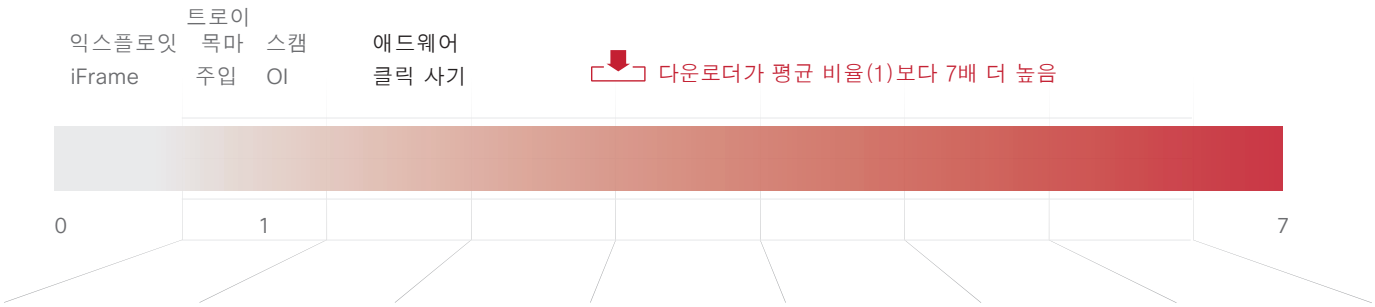
Cisco Security Research에서는 공격자의 표적 설정 또는 사용자의 웹 사용 방식 때문에 업종별 악성코드 발생 위험이 증가했는지 확인하기 위해, 8가지 유형의 공격 방법을 조사했습니다(그림 10). 조사 결과, 표적 공격 방법 및 사용자의 부주의한 온라인 행동이 모두 위험 수준에 영향을 미치는 최악의 상황이 확인되었습니다.

Cisco Security Research에서는 고위험 및 저위험 업종의 사용자 행동 간에 실제로 차이가 있는지 확인하기 위해 애드웨어, 클릭 사기, 사기, iframe 삽입 등 사용자가 인터넷을 탐색할 때 자주 발생하는 4가지 유형의 비표적 공격 방법을 살펴보았습니다. 연구 팀은 또한 익스플로잇, 트로이 목마, OI(탐지 악성코드), 다운로더 등 공격자들이 표적 공격에 자주 사용하는 4가지 유형의 고급 공격 방법도 살펴보았습니다.

참고: Cisco Security Research에서는 8가지 공격 방법을 휴리스틱 그룹으로 분류했습니다.

보고서 공유

그림 10. 웹 악성코드 공격 방법: 상위 4개 및 하위 4개 고위험 업종의 비교



출처: Cisco Security Research

그런 다음 Cisco Security Researc 팀은 Cisco Cloud Web Security 데이터에 따라, 악성코드에 가장 많이 노출된 상위 4개와 하위 4개 업종에 대해 각 공격 방법 유형별 보안 사고 비율을 파악하고 해당 업종별 평균 비율을 산정했습니다. 그림 10에 표시된 비교 결과는 상위 업종 평균을 하위 업종 평균으로 나눈 것입니다. 비율 1은 가장 많이 공격의 표적이 된 그룹과 가장 적게 공격의 표적이 된 그룹 사이에 동일한 활동 패턴이 관찰되었다는 것을 의미합니다.

조사 결과, 위험이 가장 높은 업종에서 하위 4개의 고위험 업종에 비해 7배 더 자주 다운로더 공격이 발생한 것으로 나타났습니다. 이는 위험이 가장 높은 업종에 대해 표적 공격이 이루어졌을 것이라는 예상과 일치합니다.

클릭 사기 및 애드웨어의 발생률 역시 가장 많이 공격의 표적이 되는 고위험 업종이 적게 공격의 표적이 되는 저위험 업종에 비해 더 높습니다. 이는 그 차이가 악의적인 공격자의 표적 공격 때문만은 아닐 수도 있다는 것을 의미합니다.

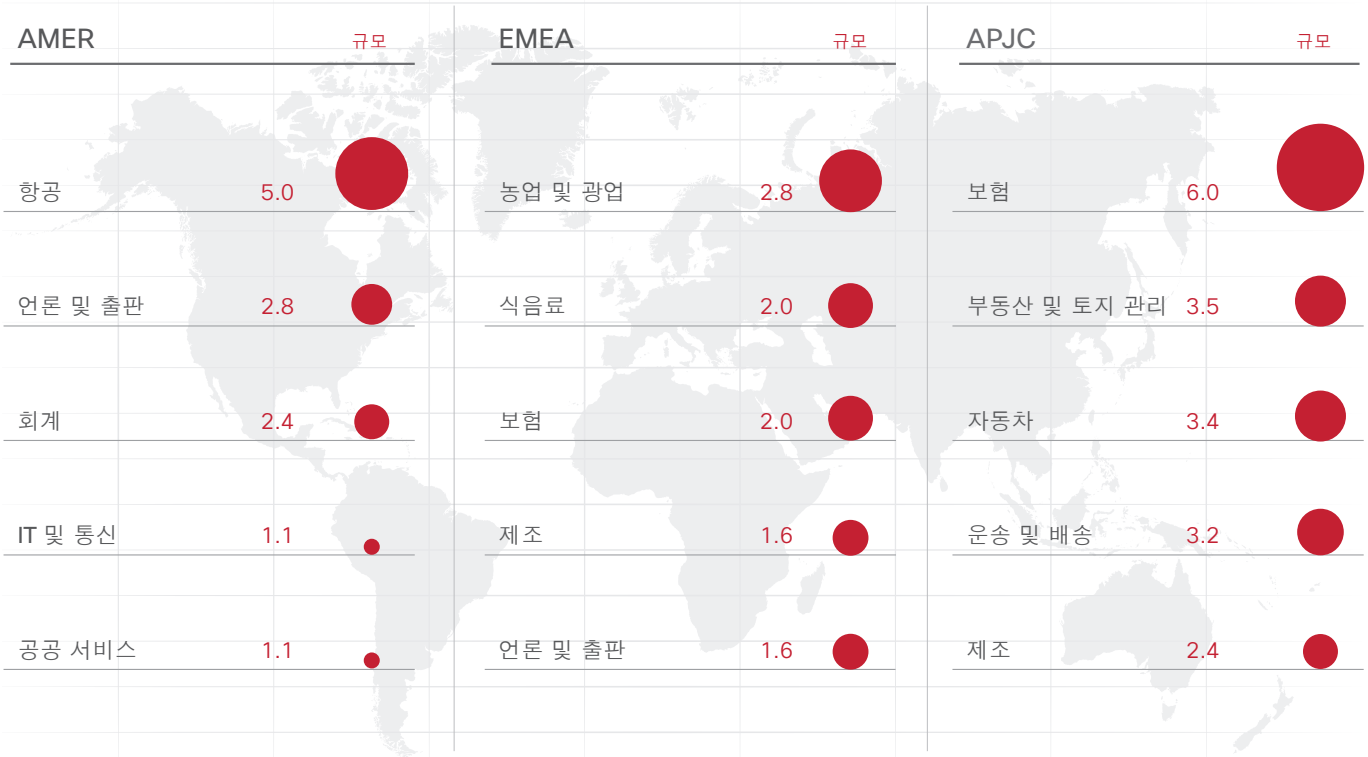
사용자의 인터넷 사용 방식 및 탐색 습관에 차이가 있기 때문에, 사용자 행동에 따라 악성코드에 더 노출되고, 따라서 고위험 업종에서 더 자주 웹 악성코드 공격 방법을 접하게 될 가능성이 있습니다. 또한, 경쟁과 혁신을 위해 새로운 매체를 신속하게 수용할 것이 권장되고 요구되는 업종의 사용자는 인터넷 사용이 더 제한적이거나 엄격하게 통제되는 정부 등 다른 업종의 사용자보다 더 빨리 웹 악성코드 공격 방법을 접하게 될 가능성이 높습니다.

예를 들어, 언론 및 출판 업종의 사용자는 일반적으로 인터넷을 많이 사용하기 때문에 다른 업종의 사용자보다 웹 익스플로잇이 발생할 위험이 높습니다.

참고: 2014년 언론 및 출판 업종의 웹 악성코드 발생률은 2008년 이후 관찰된 평균 발생률에 비해 현저하게 높았습니다. 사용자가 합법적인 웹사이트의 악성 광고에 광범위하게 노출되는 것도 이 비율이 증가하는 요인이 될 수 있습니다.

보고서 공유

그림 11. AMER, APJC 및 EMEA 지역별로 악성코드 노출 위험이 가장 높은 업종



출처: Cisco Security Research

지역별 악성코드 발생률

다음은 지역별 고위험 업종의 웹 악성코드 발생 위험입니다. 다음과 같이 세 지역이 정의되었습니다.

- AMER(북아메리카, 중앙아메리카, 라틴 아메리카)
- APJC(아시아 태평양, 중국, 일본, 인도)
- EMEA(아프리카, 유럽, 중동)

Cisco Security Research에서는 각 지역에서 노출 위험이 가장 높은 업종을 식별하고(그림 11의 업종 참조), 다음과 같은 사실을 확인했습니다.

- APJC 지역의 보험 업종의 사용자는 세 지역 모두에서 조사된 12개 업종에 비해 악성코드에 노출될 가능성이 6배 더 높습니다. (기본 평균: 1.5.)
- AMER 지역의 항공 업종의 사용자는 악성코드에 노출될 가능성이 5배 더 높습니다.
- APJC 지역의 부동산 및 토지 관리 업종의 사용자 및 해당 지역의 자동차 업종의 사용자 모두 악성코드에 노출될 가능성이 3.5배 더 높습니다.
- APJC 지역의 운송 및 배송 업종의 사용자는 악성코드에 노출될 가능성이 3.25배 더 높습니다.

Cisco Security Research에서는 APJC 지역의 치솟는 토지 및 주택 가격, 최근의 자연재해 및 대규모 수출과 제조 활동이 공격자들이 해당 지역의 자동차, 보험, 부동산 및 토지 관리, 운송 및 배송 업종에 종사하거나 이 업종에서 비즈니스를 운영하는 사용자를 공격의 표적으로 삼는 이유라고 생각합니다. 고객 데이터, 지적 재산(국가 단위의 표적 공격 포함) 및 항공 화물 데이터 도용이 AMER 지역 항공 업종의 사용자를 공격 대상으로 삼는 주된 동기로 추정됩니다.

보고서 공유

지역별 악성코드 배포에 사용된 공격 방법

그림 12a - 12c에서 공격자들이 악성코드 배포를 위해 주로 사용하는 지역별 기술을 볼 수 있습니다. 이 차트의 내용은 웹 기반 위협의 유형보다는 Cisco Cloud Web Security 데이터에 기초하여 웹 악성코드 차단(즉, 발생)이 일어난 위치를 중심으로 작성된 것입니다.

2014년에 AMER 지역 사용자들은 주로 악의적인 스크립트의 공격 대상이 되었으며, 그 다음은 iframe 감염이 큰 차이를 두고 2위를 차지했습니다. APJC 지역의 공격자들은 작년에 스캠, 악의적인 스크립트 및 웹 기반 익스플로잇을 주로 사용하여 모든 업종의 사용자를 공격했습니다. EMEA 지역에서는 웹 기반 익스플로잇이 특히 많이 발생했습니다.

Cisco 보안 블로그에서 "Threat Spotlight: Group 72"를 참조하시어 제조, 산업, 항공우주, 방위 및 미디어 부문의 고부가가치 지적 재산권을 소유한 유수의 조직을 대상으로 공격자 그룹의 활동을 식별하여 차단하는 데 Cisco Security Research가 어떤 역할을 하는지 알아보시기 바랍니다.

Group 72가 사이버 스파이 활동을 하는 데 사용한 RAT(Remote Administration Tool)에 대한 자세한 내용은 블로그 게시글 "Threat Spotlight: Group 72, Opening the ZxShell"을 참조하시기 바랍니다.

그림 12a. 공격 방법 분포, AMER

공격 방법	총 비율%
스크립트	24.93%
iFrame 주입	17.43%
익스플로잇	13.63%
OI(탐지 악성코드)	10.35%
트로이 목마	10.06%

출처: Cisco Security Research

그림 12b. 공격 방법 분포, APJC

공격 방법	총 비율%
스캠	25.26%
스크립트	25.04%
iFrame 주입	18.68%
OI(탐지 악성코드)	9.93%
익스플로잇S	6.72%

출처: Cisco Security Research

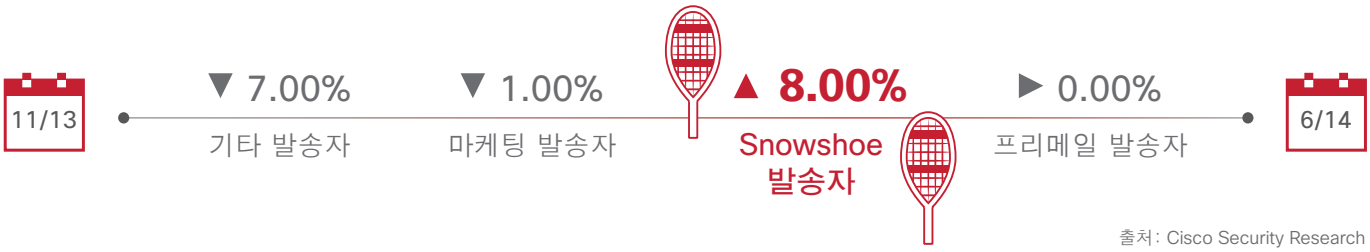
그림 12c. 공격 방법 분포, EMEA

공격 방법	총 비율(%)
iFrame 감염	51.48%
스크립트	15.17%
무단 사용	8.64%
스캠	7.31%
OI(탐지 악성코드)	4.16%

출처: Cisco Security Research

보고서 공유

그림 13. 스노우슈 발신자의 스팸 증가



출처: Cisco Security Research

스팸 업데이트: 스패머, "스노우슈" 전략 채택

사용자들이 여전히 익숙한 스팸 전술에 속기 때문에 피싱(Phishing)은 범죄자들이 악성코드를 전달하고 개인정보를 훔치는 데 중요한 역할을 합니다. 공격자들은 브라우저와 이메일을 통해 사용자를 공격하는 것이 서버 손상을 노리는 것보다 더 쉽다는 것을 깨달았고, 이 때문에 스패머가 계속해서 진화하고 있습니다.

일반적으로 안티스팸 시스템은 스팸의 99% 이상을 걸러냅니다. 대부분의 주요 안티스팸 시스템은 스팸의 99.9% 이상을 차단합니다. 이러한 환경에서 스패머는 스팸 필터를 피하기 위해 할 수 있는 모든 시도를 다 합니다. 원하는 대상에게 스팸을 보내기 위해, 스패머들은 IP 기반 안티스팸 평판 기술에 의한 검색을 피하려고 더욱더 다음과 같은 전술을 사용하고 있습니다.

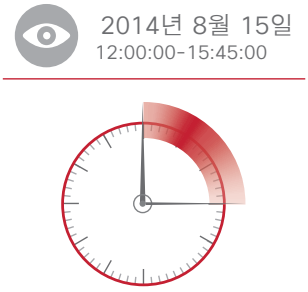
스노우슈(Snowshoe) 스팸 시작: 설상화를 착용하면 더 넓은 표면으로 몸무게가 분산되어 쌓인 눈 위를 발이 빠지지 않고 걸을 수 있으므로 적절한 비교라고 할 수 있습니다. 스노우슈 스팸(Snowshoe spam)은 대량의 IP 주소를 사용하여 원하지 않은 대량의 이메일을 보내며 일부 스팸 시스템에서 스팸으로 걸러지지 않도록 IP 주소당 소량의 메시지를 발송합니다. 그림 13에 2013년부터 2014년까지 스노우슈 스팸의 증가세가 나와 있습니다.

Cisco Security Research에서 관찰한 최근 스노우슈 스팸 공격에서 기습 공격 방식이 사용되었습니다. 즉, 전체적인 스팸 공격이 단 3시간 동안 실행되었지만, 전 세계 스팸 트래픽의 10%를 차지한 시점이 있었습니다(그림 14).

스노우슈 스팸에 대한 자세한 내용은 Cisco 보안 블로그 게시물 "Snowshoe Spam Attack Comes and Goes in a Flurry"를 참조하시기 바랍니다.

Cisco 연구원들이 확인한 바에 의하면 스노우슈 메시지는 일반적인 스팸의 특성을 나타내고 있습니다. 예를 들어 "inovice 2921411.pdf" 처럼 제목에 잘못된 철자와 임의로 생성된 숫자가 포함되어 있습니다. 첨부 파일은 일반적으로 Adobe Reader의 취약점을 공격하는 트로이 목마가 포함된 PDF 파일이었습니다.

그림 14. 스노우슈 스팸 공격 사건



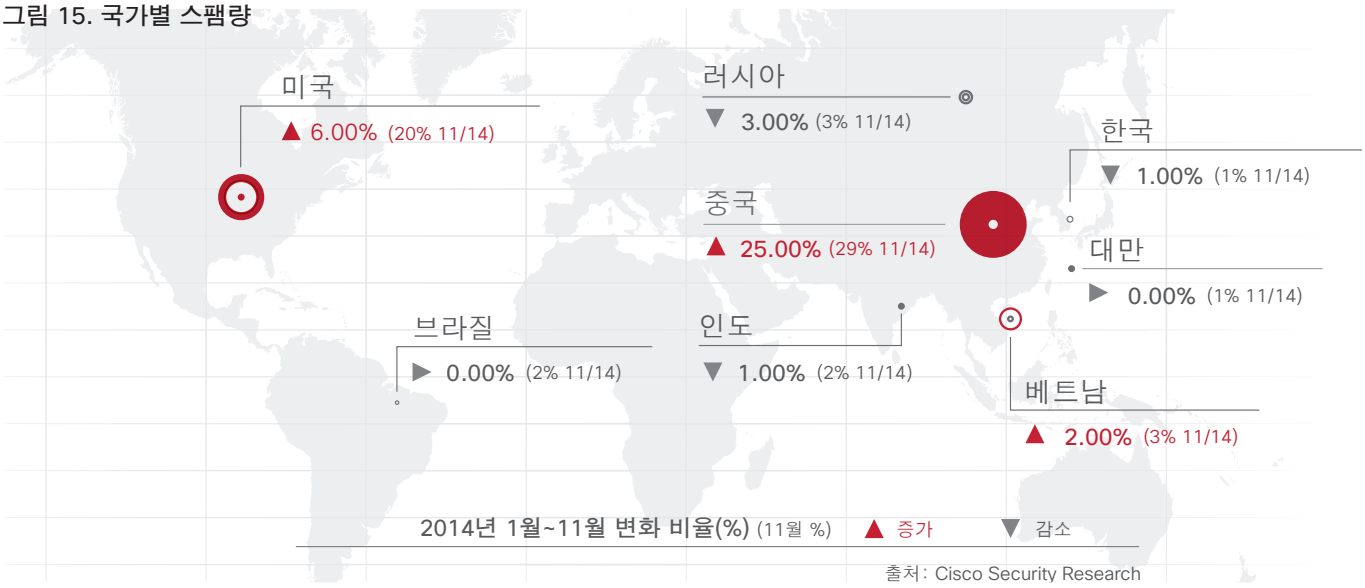
출처: Cisco Security Research

봇넷 파생 공격의 경우, 공격의 동일한 메시지가 수백 또는 수천 곳에서 시작될 수도 있으므로 스노우슈 스팸을 차단하기 위해 보안 전문가는 단순히 평판에 기반을 둔 솔루션에 의존해서는 안 됩니다. 이메일 서버 청결(hygiene) 상태 등과 같은 스팸의 다른 특징을 조사한다면 보다 정밀하게 탐지할 수 있습니다. 예를 들어 Cisco Security Research에서 관찰한 공격에서 다수의 IP 주소의 순방향 또는 역방향 DNS(Domain Name System)가 일치하지 않았습니다. 이것은 일반적으로 메일 서버가 불법적임을 나타내는 명확한 증거입니다.

이러한 IP 주소 중 대부분은 스노우슈 공격이 시작되기 이전의 이메일 전송 기록이 없습니다. 이는 온라인 범죄에서 감염된 시스템을 활용하여 스노우슈 스팸용 인프라를 구축하고 있다는 것을 보여줍니다.

보고서 공유

그림 15. 국가별 스팸량



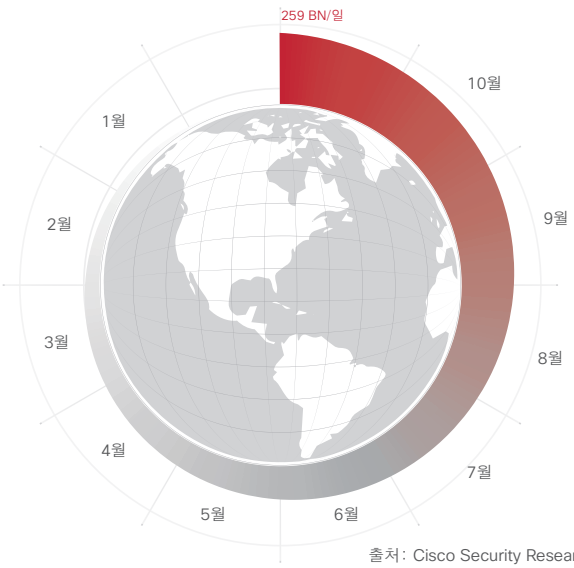
출처: Cisco Security Research

소비자보다 한발 앞서 전술을 확장하는 스패머

전 세계 스팸량의 증가는 스팸이 여전히 온라인 범죄자들에게 좋은 수익원이 되고 있다는 것을 의미합니다(그림 16). 공격자들은 대부분 사회공학적 전술 등을 사용하여 스팸에 수신자가 위험한 링크를 클릭하도록 메시지를 지속적으로 개선하고 있습니다.

2014년에 미국의 스팸량은 감소했지만 같은 기간 동안 다른 국가의 스팸량은 증가했습니다(그림 15). Cisco Security Research에 따르면 이는 일부 악의적인 공격자가 활동 기반을 변경하고 있을 가능성을 의미합니다. 일부 국가에서의 스팸량 증가는 전 세계 스팸의 최대 발생지인 미국의 스팸 발생량을 다른 지역에서 따라 잡고 있다는 증거이기도 합니다. 궁극적으로는 2014년 미국의 발생량이 더 높았습니다.

그림 16. 2014년의 전 세계 스팸량 증가



출처: Cisco Security Research

수년 동안 온라인 범죄의 중심이 되고 있는 스피어 피싱(Spear-phishing) 메시지는 경험이 많은 사용자조차 진짜 이메일과 위조 메시지를 구분하기 어려울 정도로 발전했습니다. 잘 짜여진 메시지로 특정 개인을 표적으로 삼는 이러한 메시지는 배송 서비스, 온라인 쇼핑 사이트, 음악 및 엔터테인먼트 공급자 등과 같이 사용자가 자주 메시지를 받는 잘 알려진 벤더 또는 서비스 공급자가 보낸 것처럼 보입니다. 신뢰할 수 있는 이름과 로고가 포함된 이메일은 스푸핑된 경우라해도 약품, 시계 등을 홍보하는 구식 스팸 메시지보다 더 믿음이 갑니다. 최근한 주문에 대한 알림, 배송 추적 번호 등과 같이 수신자에게 익숙한 내용이 포함된 메시지일 경우, 사용자는 이메일에 포함된 링크를 클릭하도록 더 큰 유혹을 받게 됩니다.

Cisco Security Research는 최근에 수신자가 모바일 iOS 디바이스용 인기 게임을 다운로드했다며 Apple Inc. 에서 보낸 알림을 사칭하는 일부 스피어 피싱 메시지를 확인했습니다. 이메일 제목 줄에는 임의로 생성된 영수증 번호가 포함되어 있었습니다. 합법적인 이메일에 일반적으로 이런 번호가 포함되어 있으므로 진짜처럼 보이기 위한 수작입니다. 메시지에 포함된 링크에는 수신자가 게임 다운로드를 허가한 적이 없을 경우 로그인하여 암호를 변경하라고 설명되어 있지만, 링크를 클릭하면 알려진 피싱 웹사이트로 리디렉션됩니다.

보고서 공유

스패머, 탐지를 회피하기 위해 메시지 개조

사용자가 스팸에 포함된 링크를 클릭하거나 허위 제품을 사도록 설득할 수 있는 스패머의 성공 공식을 찾는다면 기본 구조는 그대로 유지하면서 메시지를 개조하는 것입니다. 하지만 메시지는 적어도 짧은 시간 동안 스팸 필터를 회피할 수 있을 정도로 달라야 합니다. 표 2는 Cisco 연구원들이 샘플 수집 기간 동안 스패머들이 계속되는 차단 노력을 우회하기 위해 메시지 내용을 변경하려고 시도한 횟수의 집계입니다. 이 표에서는 Cisco ESA(Email Security Appliance) 규칙 변경이 필요한 위협을 보여줍니다.

표 2. 보안 침해 경고: 가장 지속적인 스팸과 피싱 위협

IntelliShield ID	제목	Version	Urgency	Credibility	Severity
24986	위협 발생 알림: 위조 FedEx 배송 알림	95			
31819	위협 발생 알림: 위조 팩스 메시지 전달 이메일	88			
30527	위협 발생 알림: 악의적인 개인 사진 첨부 파일	81			
36121	위협 발생 알림: 위조 전자 결제 취소	80			
23517	위협 발생 알림: 위조 제품 주문 이메일 메시지	79			
23517	위협 발생 알림: 위조 송장 내역서 첨부 파일	78			
27077	위협 발생 알림: 위조 이체 알림	78			
26690	위협 발생 알림: 위조 금융 결제 이체 알림	78			

출처: Cisco Security Research

보고서 공유

브라우저 애드온의 맬버타이징: 경미한 사용자별 피해, 엄청난 수익

Cisco Security Research에서는 최근에 웹 브라우저 애드온의 맬버타이징(malvertising, 악성 광고)을 악성코드와 원치 않는 애플리케이션의 배포용으로 활용하는 웹 기반 위협을 세부적으로 분석했습니다. Cisco Security Research에서는 위협이 봇넷의 움직임과 흡사한 강력한 특징이 있음을 확인했습니다. Cisco Security Research에서는 팀 연구를 통해 2014년 1월 1일부터 11월 30일까지 70개 회사의 800,000명 이상의 사용자 활동을 조사하여 위협 총규모를 측정했으며 그 의도와 구조를 입증했습니다.

분석을 통해 브라우저 애드온 제품군이 예상한 것보다 훨씬 더 포괄적이며 악성코드 작성자가 장기적으로 악성코드의 수익성을 유지하기 위해 매우 정교하고 전문적으로 작성된 코드와 구체적인 비즈니스 모델을 사용하고 있다는 사실을 밝혀냈습니다. 다시 말해서 성공적으로 수익을 얻기 위해 대상 호스트를 완벽하게 제어하지 않아도 됩니다. 감염된 호스트에 미치는 영향을 줄이도록 의도적으로 설계되고 대규모 감염자들로부터 장기적으로 수익을 창출하도록 최적화된 악성코드가 점점 더 확산되고 있습니다.

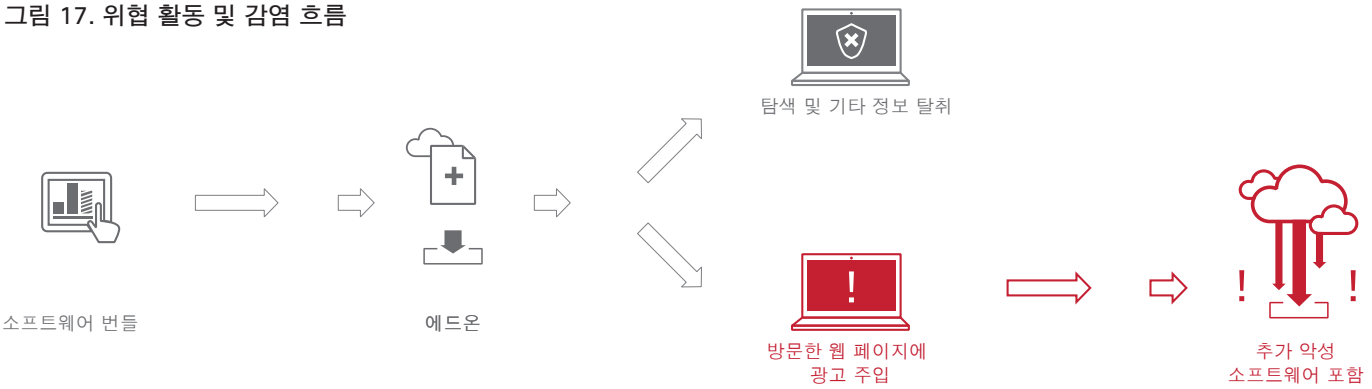
감염된 사용자는 일반적으로 사용자의 동의 없이 번들 소프트웨어(다른 소프트웨어 패키지 또는 제품과 함께 배포되는 소프트웨어)를 통해 악의적인 브라우저 애드온에 감염됩니다. 신뢰할 수 없는 소스로부터 다운로드한 PDF 툴 또는 비디오 플레이어와 같은 애플리케이션을 사용자가 합법적인 애플리케이션이라고 믿기 때문에 직접 설치합니다. 애플리케이션이 원치 않는 악의적인 소프트웨어와 "번들로" 묶여 있을 수 있습니다. 이러한 악성코드 배포 방식은 PPI(pay-per-install) 수익 체계를 따릅니다. 즉, 원본 애플리케이션에 번들로 제공된 소프트웨어의 모든 설치에 대해 게시자가 요금을 받습니다.

많은 사용자가 기본적으로 애드온을 신뢰하거나 정상적인 것으로 여기기 때문에 악의적인 공격자가 이 접근 방식으로 악성코드를 성공적으로 배포할 수 있습니다. 이러한 악성코드 배포 방법을 사용하면 공격자가 익스플로잇 킷과 같은 탐지되기 쉬운 다른 기술에 의존하지 않아도 됩니다. (7페이지 "웹 익스플로잇: 익스플로잇 킷 작성자의 경우 1위가 최고를 의미하지 않을 수도 있다" 참조)

Cisco Security Research는 이 브라우저 애드온 제품군에 의해 생성되는 웹 트래픽이 특정한 특성을 가지며, 두 가지 정의된 패턴으로 식별될 수 있다는 것을 확인했습니다. 일반적으로 애드온 이름, 이전에 방문한 URL(인트라넷 링크 포함) 등과 같은 정보를 유출하는 인코딩된 데이터가 쿼리 문자열에 포함되어 있습니다.

이 분석 중에 Cisco Security Research는 PassShow, Bettersurf, Bettermarkit, 조합 SHA(bee4b83970ffa8346f0e791be92555702154348c14bd8a1048abaf5b3ca049e35167317272539fa0dece3ac1a6010c7a936be8cbf70c09e547e0973ef21718e5)를 비롯하여 4,000가지 이상의 애드온 이름을 확인했습니다. 개별 설치당 둘 이상의 애드온 이름을 사용할 수 있으므로 악성코드를 추적하기가 매우 어렵습니다 (그림 17).

그림 17. 위협 활동 및 감염 흐름



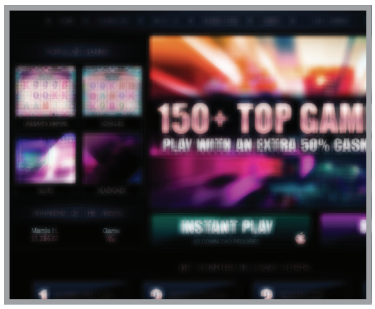
출처: Cisco Security Research

보고서 공유

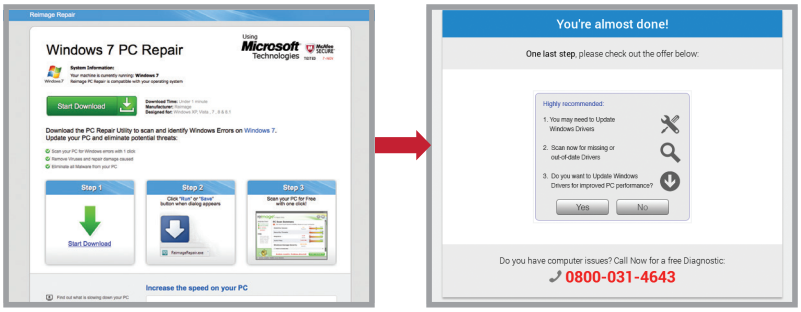
OS 유형을 탐지하는 악성코드, 적절한 익스플로잇 전파

Cisco 보안 연구원들은 자신들이 분석한 악성코드 애드온이 사용자의 브라우저 "지문(fingerprint)"에 따라 특정 유형의 광고를 표시한다는 사실을 확인했습니다. Linux 사용자용으로 삽입되는 광고는 일반적으로 온라인 게임 사이트와 관련이 있습니다. Microsoft IE를 설치한 사용자는 합법적인 것처럼 보이지만 실제로는 악의적인 소프트웨어의 다운로드를 유도하는 광고로 리디렉션됩니다.

Linux



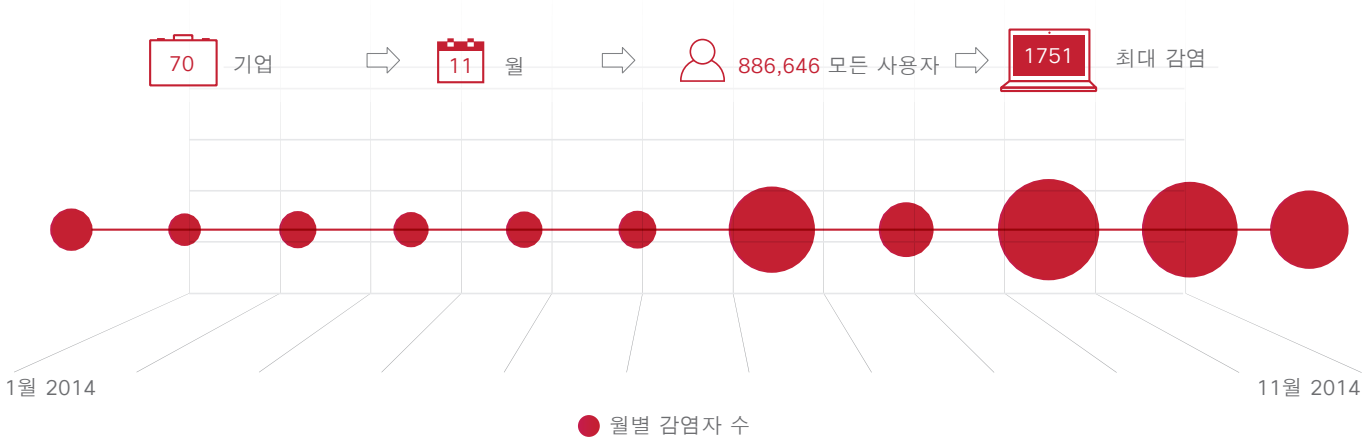
Microsoft IE



70개 회사에서 11개월 동안 실시한 사용자 활동 분석에 따르면 이 위협에 감염되는 사용자 수가 점점 증가하고 있습니다. 1월에는 711명의 사용자가 감염되었지만 하반기에는 감염자 수가 1,000명을 초과하고, 9월에는 1,751명으로 최고를 기록했습니다(그림 18). 9월과 10월에 감염자 수가 급격하게 증가한 이유 중 하나는 여름 휴가에서 복귀한 사용자들의 온라인 활동 증가가 주요 원인입니다.

Cisco의 보안 전문가들은 연구를 통해 공격자들이 악성코드 캠페인을 지원하기 위해 다양한 서버를 이용하고 있다는 것을 확인했습니다. 이는 활동을 분할하여 유지하는 데 정통한 사이버 범죄 조직에서 위협을 담당하거나 "기술 공급자"가 다양한 그룹에 제품을 판매하고 있다는 것을 의미합니다. 어찌 되었든 악성코드 배포를 담당하는 공격자가 상당한 크기의 봇넷을 만들려고 시도하는 것으로 보입니다.

그림 18. 월별 감염된 사용자 수, 1월 - 11월 2014



출처: Cisco Security Research

보고서 공유

또한 Cisco Security Research에서는 이 위협과 연관된 500개 이상의 고유 도메인을 확인했으며, 그중 24개는 알렉사(Alexa)에 상위 100만 개 도메인 순위에 올랐습니다. 또한 많은 도메인이 상대적으로 높은 순위를 기록했습니다(그림 19). 즉, 이들 도메인은 대중적인 도메인이지만 감염의 위험으로 인해 방문하는 것이 매우 위험하다는 것을 의미합니다.

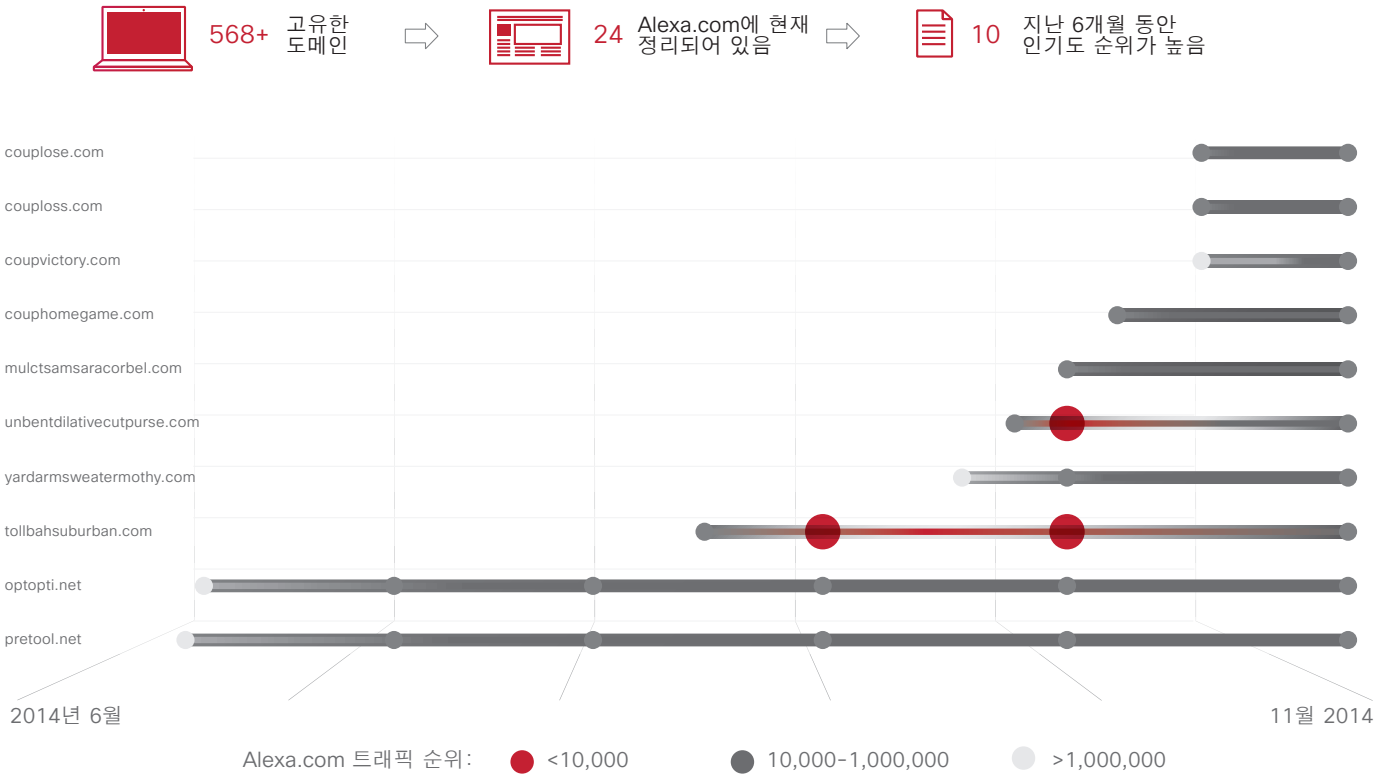
1년 넘게 활성화된 도메인도 있지만, 대부분은 수명이 훨씬 짧아 단 몇 주에 불과합니다(그림 19). 모든 도메인은 인기가 빠르게 상승했다는 동일한 특징을 갖고 있습니다.

예방 및 침해 복구 팁

브라우저 애드온 체계에 의해 감염되는 것을 방지하거나 기존 감염에 대처하려면 다음 팁을 적용해야 합니다.

- 믿을 수 있는 소스로부터 애플리케이션 다운로드
- 번들 설치 시 원치 않는 소프트웨어 선택 취소
- 위협 분석, 샌드박싱 기술, 웹 보안 기술을 사용하여 이러한 유형의 위협을 예방 및 탐지
- 가능하면 애드온을 수동으로 제거하고 안티스파이웨어 툴을 사용하여 원치 않는 프로그램 정리

그림 19. 브라우저 애드온 체계에서 맬버타이징에 사용되는 대중적인 도메인, Alexa 순위 기준



S처: Cisco Security Research

보고서 공유

2. Cisco 보안 기능 벤치마크 조사

조직의 보안 상태에 대한 인식을 평가하기 위해 Cisco에서는 다양한 국가와 다양한 규모의 조직에 소속된 CISO(Chief Information Security Officer, 최고정보 보호 책임자) 및 보안 담당 중역에게 해당 조직의 보안 리소스와 절차에 대해 질문했습니다. 2014년 10월에 완료된 *Cisco 보안 기능 및 벤치마크 조사*는 보안 운영의 정교성과 실제 보안 업무에 대한 정보를 제공합니다.

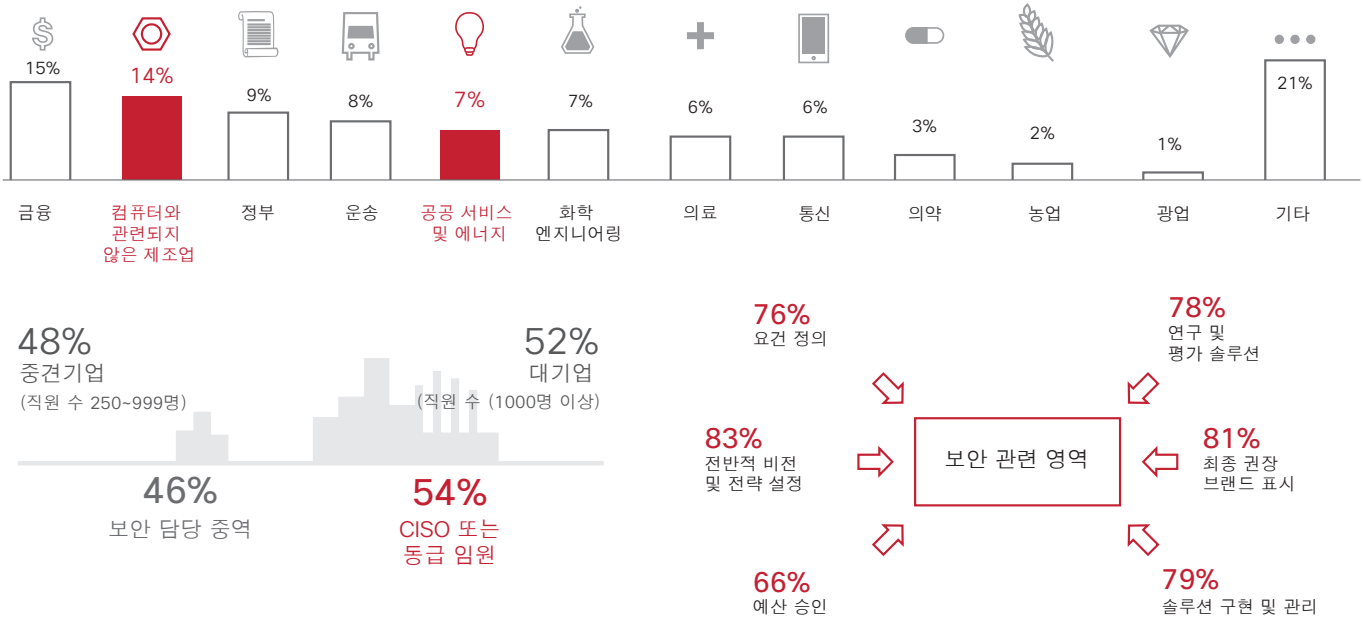
Cisco 보안 기능: 조직이 기준에 얼마나 부합하는가?

엔터프라이즈 보안 전문가들은 보안 위협에 대비한 자사의 준비 상태를 어떻게 생각하고 있을까? 새로운 Cisco 보안 기능 벤치마크 조사에 따르면 조직 내에서 맡은 역할과 업종에 따라 그 대답이 다를 수 있다고 합니다.

그림 20에서는 업종 및 회사 규모별 전문가의 응답을 보여줍니다. 컴퓨터와 관련이 없는 제조업체와 공공 서비스/에너지 업종의 응답자는 최고 수준의 보안 상태와 지식을 갖추고 있다고 대답했습니다.

N(응답자 수) = 1,738

그림 20. 응답자 프로필 및 보안 침해 준비 상태



출처: *Cisco 보안 기능 벤치마크 조사*

보고서 공유

이 연구에서는 CISO 및 보안 담당 중역을 대상으로 설문조사를 실시하여 회사의 사이버 보안 담당 리소스, 보안 운영, 정책, 절차, 사이버 보안 운영의 정교성 등을 확인했습니다. 다행히 대부분의 보안 전문가들은 보안을 효율적으로 유지 관리하기 위한 툴과 프로세스를 적용하고 있다고 생각합니다. 하지만 CISO는 보안 담당 중역에 비해 보안 상태에 대해 지나치게 낙관적입니다. 예를 들어 CISO의 62%가 조직의 보안 프로세스를 정확하게 파악하고 있다고 생각하는 것에 비해 보안 담당 중역의 경우 그 수가 48%에 불과합니다. 또한 CISO는 자사의 보안 프로세스를 유리하게 해석하는 경향이 있습니다. 설문조사에 응답한 CISO의 59%가 프로세스가 최적화되어 있으며 현재는 프로세스 개선에 주력하고 있다고 응답한 반면에 보안 담당 중역의 경우 46%만 그렇다고 대답했습니다.

확신의 정도에 격차가 생긴 이유는 무엇일까요? CISO는 일상 보안 활동에 참여하지 않는 반면에 보안 담당 중역은 크고 작은 보안 사고를 해결하기 위해 긴밀하게 협력하고 있기 때문입니다. 대기업의 CISO는 하루에 1,000대의 시스템이 악성코드에 감염된다는 사실을 모를 수도 있지만, 보안 담당 중역는 감염을 차단하는 데 많은 시간을 투자하고 있으므로 조직의 보안을 낙관적으로 보지 못합니다.

또한 CISO는 소셜 미디어 액세스 차단과 같은 정책을 수립할 수 있습니다. 이런 조치는 침입할 수 없는 강력한 보안 방어의 환상을 그들에게 안겨줍니다. 하지만 그러한 채널을 완벽하게 차단할 경우 보안 팀이 네트워크 외부에 존재하는 위협을 파악하거나 경험할 수 없게 됩니다.

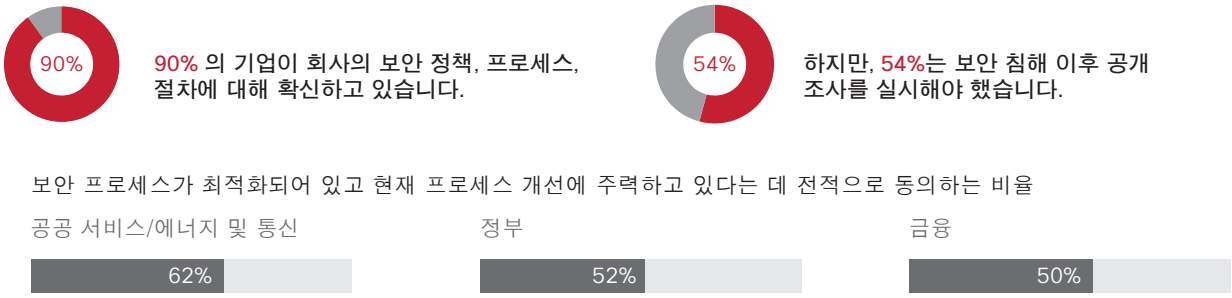
응답자에게 조직의 보안 정책에 대한 신뢰도 질문을 했을 때에도 다시 한번 격차가 나타났습니다. CISO와 보안 담당 중역 모두 정책에 대해서는 높은 수준의 신뢰를 나타냈지만 (그림 21 참조), 감염 피해 범위와 억제 능력에 대해서는 신뢰하지 못했습니다(그림 28 참조).

보안 제어에 대한 질문에서도 응답자 간에 비슷한 격차가 나타났습니다. 거의 모든 응답자가 보안 제어 상태가 양호하다고 대답했지만, 약 1/4은 보안 툴의 효율성을 "매우 높음" 또는 "가장 높음" 대신 "다소 높음"으로 대답했습니다(그림 29 참조).

보안 프로세스와 관행에 대한 신뢰도도 업종별로 다른 것으로 나타났습니다. 공공 서비스/에너지 기업, 통신 회사의 CISO 및 보안 담당 중역의 신뢰도가 가장 높은 반면에, 정부, 금융 서비스, 제약 및 의료 기관의 신뢰도는 낮게 나타났습니다. 예를 들어 통신 및 공공 서비스/에너지 보안 경영진의 62%는 자사의 보안 프로세스가 최적의 상태라는 데 전적으로 동의한다고 대답한 반면에, 금융 서비스(50%)와 정부 기관(52%)의 경우 그 수치가 훨씬 낮았습니다.

공공 서비스/에너지 및 통신 보안 전문가는 가장 정교한 보안 관례를 보유한 반면, 정부와 금융 서비스 조직은 그만큼 정교한 보안 관례가 없는 것처럼 보입니다. 공공 서비스 및 에너지 조직의 경우 사고 추적을 위해 프로세스와 절차를 명확히 문서화하는 경향이 있습니다. 하지만 이렇게 하는 것이 다른 업종의 조직보다 반드시 더 안전하다는 것을 의미하지는 않습니다.

그림 21. 산업 및 직책별 주요 조사 결과



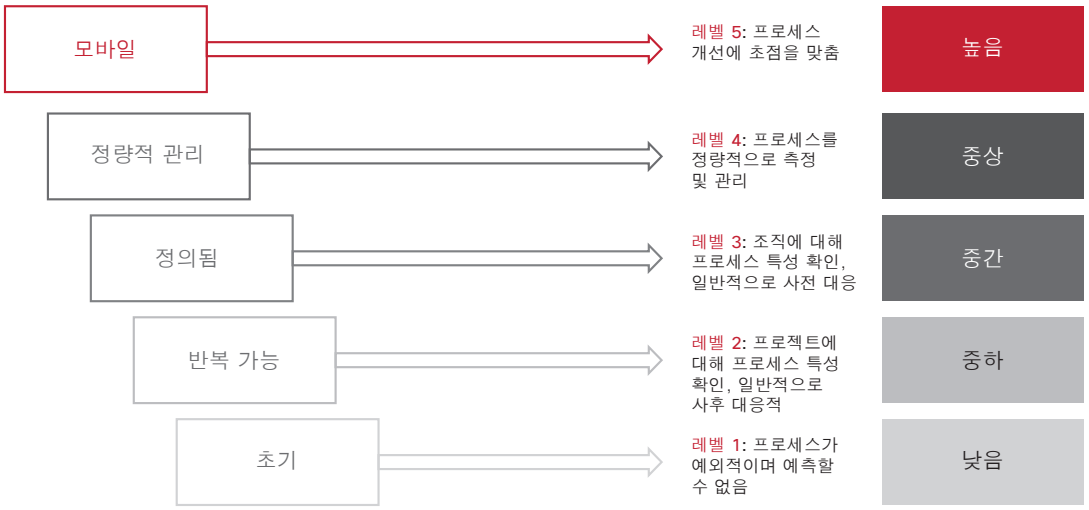
엔터프라이즈와 중견기업 시장 조직 사이에 차이점이 거의 없는 것으로 나타나, 직원 수가 수준 높은 보안과 거의 관련이 없는 것으로 나타났습니다.

출처: Cisco 보안 기능 벤치마크 조사

보고서 공유

그림 22. 현재 샘플에 지능화된 보안 수준 매핑

Cisco는 보안 프로세스에 대한 일련의 질문을 기준으로 5세그먼트 솔루션을 선택하기 전 샘플 세그멘테이션에 대한 몇 가지 선택 사항에 대해 알아보았습니다. 5세그먼트 솔루션은 CMMI(Capability Maturity Model Integration)와 거의 가깝게 매핑됩니다.



출처: *Cisco 보안 기능 벤치마크 조사*

보안 정교성 징후

*Cisco 보안 기능 벤치마크 조사*에서는 다른 조직보다 보안 상태가 더 정교한 조직의 특성을 중점적으로 다루었습니다. 그 특성은 다음과 같습니다.

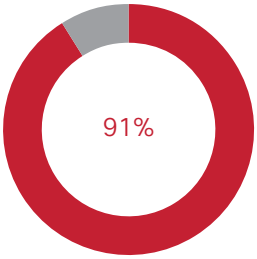
- 보안을 우선적으로 고려하는 경영진
- 명확하고 체계적으로 문서화된 정책과 절차
- 함께 사용이 가능한 통합 툴 사용

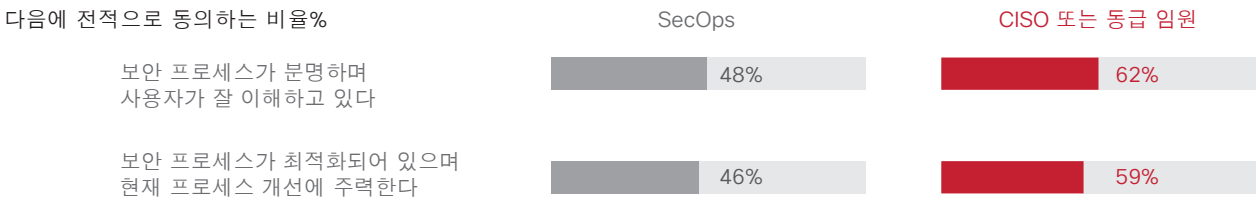
지능화된 보안을 갖춘 회사의 응답자 중 91%가 회사 경영진이 보안에 높은 우선 순위를 두고 있다고 대답한 반면에, 그렇지 못한 회사의 경우 응답자 중 22%만 그렇다고 대답했습니다. 또한 지능화된 보안을 갖춘 회사의 응답자 중 88%가 보안 프로세스가 명확하게 이해된다고 응답한 반면에 그렇지 못한 회사의 경우 그렇다고 대답한 응답자가 없습니다.

보고서 공유

그림 23. 조직 내 보안 리더십에 관한 주요 조사 결과

91% 는 보안에 대해 직접적으로 책임지는 임원이 있다고 응답했으며
이는 대부분 CISO(29%) 또는 CSO(24%) 에 해당합니다.





CISO(및 동급 임원)는 일상적 현실을 잘 모르기 때문에 회사의 보안 상태에 대해 보안 담당 중역 관리자보다 더 낙관적입니다.

출처: *Cisco 보안 기능 벤치마크 조사*

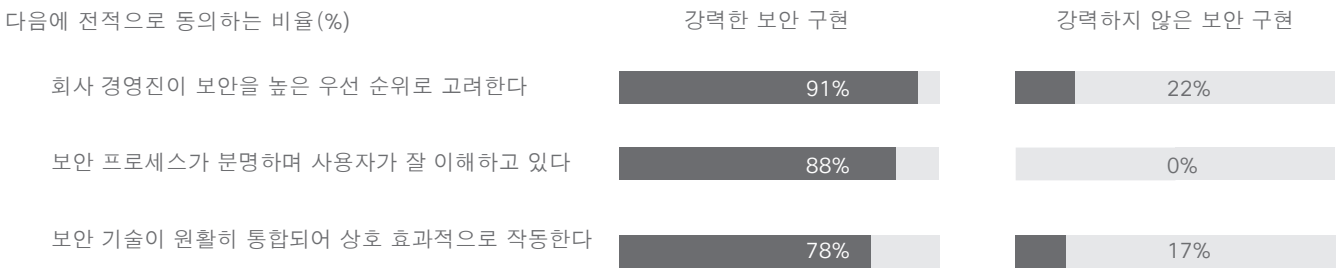
그림 23을 보면 응답자의 91%는 보안을 전담하는 경영진을 두고 있으며 대부분 이러한 책임이 CISO 또는 CSO(Chief Security Officer, 최고 보안 책임자)에게 있습니다. 보안 담당자를 둔 높은 레벨의 조직이 필요합니다. 보안 리더가 없을 경우 프로세스를 제대로 정의하여 전달하고 시행할 수 없습니다. 최근에 조직을 대상으로 발생한 유수의 보안 침해 사건들로 인해 보안 관리가 경영진의 최우선 순위로 자리 잡았을 것입니다.

보다 지능화된 보안을 갖춘 기업의 경우 응답자의 78%가 보안 기술이 업무를 효율적으로 할 수 있도록 잘 통합되어 있다는 데 동의한 반면에, 그렇지 못한 기업의 경우 응답자의 17%만 동의했습니다.

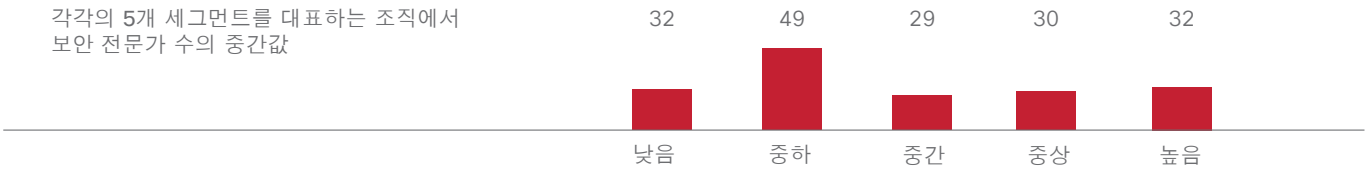
보안 프로세스를 더 지능화하려는 기업에게 다행인 점은 찾기 어려운 보안 인재들로 대규모 팀을 조성할 필요가 없다는 점입니다. 수준 높은 보안을 갖추지 못한 조직의 경우 보안 전문가 수의 중앙치는 32명이며, 가장 보안을 잘 갖춘 조직의 경우에도 보안 직원 수의 중앙치는 32명입니다. 따라서 많은 수의 직원을 고용하는 것이 보안 프로세스의 효율적인 관리와 직접적인 연관이 있는 것은 아닙니다. 보안 직원 배치와 관련하여 더 나은 접근 방식은 보안 직원과 기업의 전체 직원수 사이에 최적의 비율을 찾는 것입니다.

그림 24. 보안 우선순위에 관한 주요 조사 결과

강력한 보안을 구현한 조직은 그렇지 않은 조직과 쉽게 구분됩니다.



하지만, 보안 직원 규모로 강력한 정도를 예측할 수 없습니다.



출처: *Cisco 보안 기능 벤치마크 조사*

그림 24를 보면 수준 높은 보안을 갖추지 못한 조직의 경우 일반적으로 경영진이 보안을 우선적으로 고려하지 않고 보안 프로세스를 명확하고 확실하게 이해하지 못합니다.

국가별 조직의 지능화된 보안 수준을 비교하면 다행히도 모든 분야에서 보안을 잘 갖춘 조직이 과반수를 차지했습니다. 하지만 일부 국가의 응답자는 자체 보안 상황을 외부에서 생각하는 것보다 더 긍정적으로 보는 경향이 있습니다. 일부 국가의 경우 응답자의 지나친 자신감은 문화의 사회적 가치에서 기인한 것일 수 있습니다. 따라서 자신과 조직을 긍정적으로 표현하고 있습니다.

지나친 자신감에 주의

CISO 및 보안 담당 중역은 보안 운영을 신뢰하면서도 보안 침해 사고를 막을 수 있는 표준 툴을 사용하지 않는다고 했습니다. 응답자의 50% 미만이 다음의 툴을 사용하고 있습니다.

- 신원 관리 또는 사용자 프로비저닝
- 패칭 및 컨피그레이션
- 침해 테스트
- 엔드포인트 포렌식
- 취약점 검사

보고서 공유

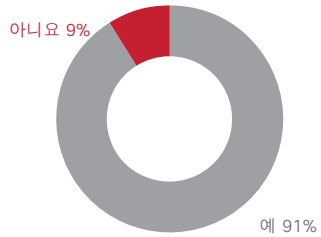
조직 보안 리소스

그림 25. 조직 내 전담 보안 전문가 수

조직의 보안 전담 전문가 수는 평균 123명입니다. 보안 서비스를 아웃소싱할 가능성이 가장 높은 조직은 정부 조직입니다.

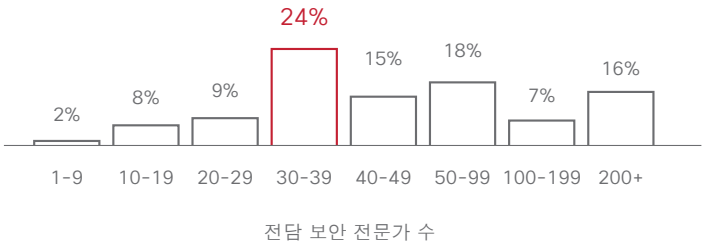
보안 리소스 스냅샷

여러분의 회사에 보안 사고 대응 팀이 있습니까?



평균 보안 전담 전문가 수

보안 관련 작업에 사용하는 평균 시간 비율(%)



정부가 다른 업계보다 더 많은 보안 서비스를 아웃소싱하는 것으로 나타났습니다.

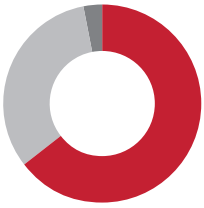
출처: *Cisco 보안 기능 벤치마크 조사*

그림 26. 조직에서 사용하는 보안 기술

응답자의 약 2/3는 보안 기술이 최신의 상태이고 자주 업데이트된다고 대답했습니다.

여러분 회사의 보안 인프라를 어떻게 설명하시겠습니까?

기준: n=1738



64% 저희 회사의 보안 인프라는 최신 상태이며 이용 가능한 최고의 기술로 계속 업그레이드되고 있습니다.

33% 저희 회사는 보안 기술을 정기적으로 업그레이드하고 있지만 가장 뛰어난 최신 툴을 갖추고 있지는 않습니다.

3% 저희 회사는 기존 기술이 더 이상 작동하지 않거나 진부화된 경우 또는 완전히 새로운 요구 사항이 식별되는 경우에만 보안 기술을 교체 또는 업그레이드합니다.

CISO 중 상당히 높은 비율(70%)은 조직 인프라가 상당히 최신이라고 대답한 반면, 그렇게 대답한 보안 담당 중역은 57%에 불과했습니다.

보안 인프라가 최신 상태라고 응답한 비율이 가장 높은 회사는 통신 회사입니다.

출처: *Cisco 보안 기능 벤치마크 조사*

그림 27. 조직에서 사용하는 보안 위협 방어

2014년에는 다양한 보안 위협 방어가 조직에서 사용되었습니다.

	조직에서 사용하는 보안 위협 방어		클라우드 기반 서비스를 통해 관리하는 방어	
	보안 담당 중역 n=797	CISO n=941	보안 담당 중역 n=759	CISO n=887
네트워크 보안, 방화벽/침입 방지	57%	64%	30%	39%
웹 보안	56%	62%	33%	41%
이메일/메시징 보안	53%	58%	33%	41%
데이터 손실 방지	55%	55%	-	-
암호화/프라이버시/데이터 보호	52%	55%	-	-
액세스 제어/권한 부여	55%	52%	24%	24%
Authentication	54%	51%	24%	22%
모바일 보안	48%	54%	24%	32%
보안 무선	47%	52%	22%	30%
엔드포인트 보호/악성코드 차단	45%	52%	24%	27%
취약점 검사	44%	51%	24%	26%
VPN	49%	46%	25%	27%
ID 관리/사용자 프로비저닝	43%	47%	16%	23%
SIEM(Security Information and Event Management)	39%	46%	-	-
네트워크 포렌식	41%	43%	-	-
패칭 및 컨피그레이션	38%	40%	-	-
침입 테스트	39%	37%	20%	19%
DDoS 방어	35%	37%	-	-
엔드포인트 포렌식	29%	33%	-	-

보안 위협 방어를 사용하는 보안 응답자, n=1646

응답자의 **13%**는 사용 중인 보안 위협 방어를 클라우드 기반 서비스를 통해 관리하지 않는다고 대답했습니다. 특히 의료, 금융 서비스, 제약 업계에서 이와 같이 대답한 비율이 높게 나타났습니다.

출처: *Cisco 보안 기능 벤치마크 조사*

보고서 공유

조직 보안 정책, 절차 및 운영

그림 28. 조직의 보안 정책 및 보안 침해 사고 억제 능력에 대한 신뢰도

조직에서는 자체 조직 보안 정책을 신뢰하지만 보안 침해 사고 피해 범위와 억제 능력에 대해서는 신뢰하지 못했습니다.

조직 보안 정책의 신뢰도

보안 정책 n=1738	보안 담당 중역 n=797			CISO n=941		
	반대/동의/전적으로 동의			반대/동의/전적으로 동의		
보안 자산을 인벤토리로 보관하고 명확히 분류하고 있다	11%	40%	49%	4%	38%	58%
HR 보안을 효과적으로 관리하고 있다	9%	45%	46%	4%	36%	60%
조직내 컴퓨터 관련 시설이 잘 보호되고 있다	10%	39%	51%	4%	34%	62%
시스템과 네트워크의 기술 보안 제어를 효과적으로 관리하고 있다	6%	41%	53%	3%	31%	66%
네트워크, 시스템, 애플리케이션, 기능, 데이터에 대한 액세스 권한을 적절히 제어하고 있다	8%	35%	57%	4%	32%	64%
시스템과 애플리케이션에 보안을 효과적으로 구현하고 있다	10%	38%	52%	4%	32%	64%
시스템 구입, 개발, 유지 관리 절차에 보안을 효과적으로 구현하고 있다	9%	41%	50%	4%	35%	61%

조직의 보안 침해 사고 억제 능력에 대한 신뢰도

조직적 보안 n=1738	보안 담당 중역 n=797			CISO n=941		
	반대/동의/전적으로 동의			반대/동의/전적으로 동의		
보안 사례를 정기적, 공식적, 전략적으로 검토 및 개선하고 있다	7%	42%	51%	3%	36%	61%
보안 사례의 기능을 검토하고 이와 관련하여 피드백을 제공할 수 있는 툴이 있다	10%	41%	49%	4%	39%	57%
보안 사고를 정기적, 체계적으로 조사한다	11%	40%	49%	3%	37%	60%
상황에 따라 고가치 자산에 대한 보안 제어를 강화할 수 있다	10%	43%	47%	3%	38%	59%
보안 수단이 의도된 대로 작동하는지 확인하기 위해 네트워크에 대한 연결 활동을 정기적으로 검토한다	8%	39%	53%	4%	33%	63%
위협 탐지 및 차단 기능이 최신 상태이다	9%	38%	53%	3%	36%	61%
보안 기술이 원활히 통합되어 상호 효과적으로 작동한다	9%	40%	51%	3%	37%	60%
보안이 조직 목표 및 비즈니스 기능에 원활히 통합되어 있다	10%	39%	51%	2%	34%	64%
감염 범위를 쉽게 확인하고 억제하며 익스플로잇에서 해결할 수 있다	15%	44%	41%	8%	42%	50%

엔터프라이즈 응답자에 비해 "보안 사례를 정기적, 공식적, 전략적으로 검토 및 개선하고 있다"라는 데 전적으로 동의하는 중견기업 시장의 응답자가 더 많았습니다.

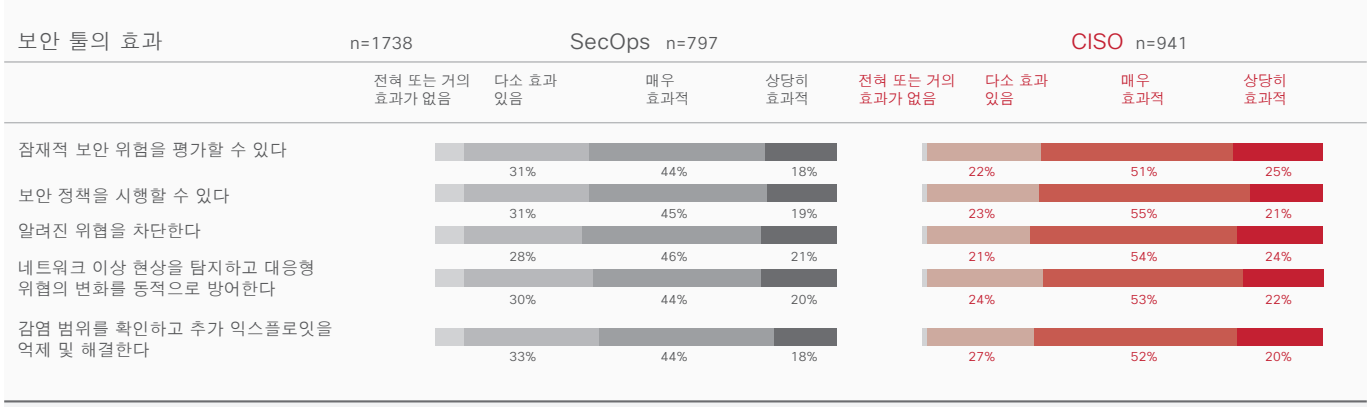
출처: *Cisco 보안 기능 벤치마크 조사*

그림 29. 회사 보안 제어와 조직의 보안 툴에 대한 응답자의 신뢰도

보안 전문가들은 조직의 보안 제어 능력이 양호하다고 믿지만, 응답자의 약 1/4은 보안 툴이 효과적이지 않다고 했습니다.

보안 제어 n=1738	SecOps n=797			CISO n=941		
	반대/동의/전적으로 동의			반대/동의/전적으로 동의		
RFC2350, ISO/IEC 27035:2011 또는 미국 인증과 같이 표준화된 사고 대응 사례를 따르고 있다	15%	42%	43%	6%	40%	54%
수신된 사고 보고서를 해석하고 우선 순위를 정하며 이해하는 효과적 프로세스가 있다	11%	46%	43%	4%	39%	57%
보안 사고가 실제로 발생했는지 여부를 확인하는 효과적 시스템이 있다	11%	41%	48%	4%	36%	60%
사고 관련 정보를 분류하는 효과적인 시스템이 있다	10%	43%	47%	4%	37%	59%
이해 관계자에게 보안 사고에 대해 효과적으로 알리고 협업하고 있다	10%	46%	44%	3%	40%	57%
사고 대응 및 추적에 대해 명확히 문서화된 프로세스와 절차가 있다	9%	40%	51%	4%	35%	61%
전반적 위험 평가 프로세스에 사이버 위험 평가를 정기적으로 통합하고 있다	10%	37%	53%	4%	36%	60%

기타 모든 업계 전문가보다 공공 서비스/에너지 부문에서 훨씬 더 많은 응답자들이 "사고 대응 및 추적에 대해 명확히 문서화된 프로세스와 절차가 있다"라는 문장에 전적으로 동의하는 것으로 나타났습니다.



운송 업계의 보안 전문가는 조직이 알려진 보안 위협을 탐지 및 방어하는 능력에 대해 큰 자신감을 보이지 않았습니다.

출처: Cisco 보안 기능 벤치마크 조사

보고서 공유

그림 30. 감염된 시스템을 분석하고 보안 사고의 원인을 제거하는 데 사용되는 프로세스

대부분의 보안 전문가는 방화벽 로그를 사용하여 보안 침해 사고를 분석하지만 이러한 로그에는 일반적으로 정보에 대한 고품질 데이터 또는 상황이 포함되어 있지 않습니다. 보안 침해 사고를 보다 효율적으로 분석하기 위해 보안 전문가는 IDS 및 IPS 로그, 프록시, HIPS(Host-based Intrusion Prevention System), 애플리케이션 로그, NetFlow 등을 주기적으로 확인해야 합니다.

놀랍게도 "연계된 이벤트/로그 분석" 이 보안 침해 사고를 분석하는 데 사용되는 툴 목록에서 낮은 순위를 차지했습니다. 이는 응답자들이 보안 이벤트를 세부적으로 분석하는 데 도움이 되는 데이터 또는 데이터 소스를 상호 비교하고 있지 않다는 것을 의미합니다.

감염 시스템 분석 프로세스	보안 담당 중역	CISO
	n=797	n=941
방화벽 로그	59%	62%
시스템 로그 분석	58%	60%
악성코드 또는 파일 회귀 분석	51%	58%
네트워크 흐름 분석	51%	54%
레지스트리 분석	48%	51%
전체 패킷 캡처 분석	44%	48%
이벤트/로그 상관관계 분석	40%	44%
메모리 포렌식	39%	43%
디스크 포렌식	38%	41%
(IOC)Indicators of Compromise	38%	38%
외부[또는 서드파티] 사고 대응/분석 팀	36%	38%

정부 응답자들은 대부분의 기타 업계 응답자에 비해 더 많은 프로세스를 사용하여 감염된 시스템을 분석하는 것으로 나타났습니다.

보안 사고 원인 제거 프로세스	보안 담당 중역	CISO
	n=797	n=941
악성 애플리케이션 격리 또는 제거	55%	60%
근본 원인 분석 (Root cause analysis)	55%	56%
악성 소프트웨어 통신 중단	51%	55%
추가 모니터링	51%	53%
정책 업데이트	50%	51%
감염된 애플리케이션 통신 중단	47%	49%
장기적 해결 방법 개발	46%	48%
이미지로 재설치하여 시스템을 이전 상태로 복원	43%	47%

CISO 및 보안 담당 중역의 응답자들은 악성 소프트웨어 통신 중단을 제외하고 일관적으로 대답했습니다.

출처: Cisco 보안 기능 벤치마크 조사

그림 31. 보안 사고 후 제어에 대한 CISO 및 보안 담당 중역의 응답
대부분의 CISO는 보안 운영 전문가보다 사고 후 제어를 더 강화한다고 보고했습니다.

감염 시스템 복원 프로세스	보안 담당 중역	CISO
	n=797	n=941
사고 발생 후 식별된 취약점을 기준으로 추가 또는 신규 탐지 및 제어 수단을 구현한다	55%	65%
취약한 것으로 간주된 애플리케이션을 패치 및 업데이트한다	59%	60%
사고 발생 전 백업에서 복원한다	53%	60%
차등 복원	53%	58%
골드 이미지 복원	33%	36%

통신 및 공공 서비스/에너지 업계 응답자는 다른 업계보다 골드 이미지 복원을 더 많이 활용한다고 대답했습니다.

그림 32. 보안 사고 알림을 받는 사람
일반적으로 보안 사고는 공식 프로세스를 통해 운영 직원과 기술 파트너에게 알려집니다.

사고 발생 시 보고를 받는 그룹	보안 담당 중역	CISO
	n=797	n=941
운영	44%	48%
기술 파트너	42%	47%
엔지니어링	38%	37%
인사 담당	37%	35%
법률	37%	35%
전체 직원	38%	33%
제조	31%	36%
비즈니스 파트너	31%	33%
마케팅	30%	31%
PR	30%	27%
외부 당국	25%	20%

정부 당국은 더 많은 관련 그룹에 명확히 정의된 알림 프로세스를 갖추었을 가능성이 다른 업계에 비해 훨씬 높습니다.

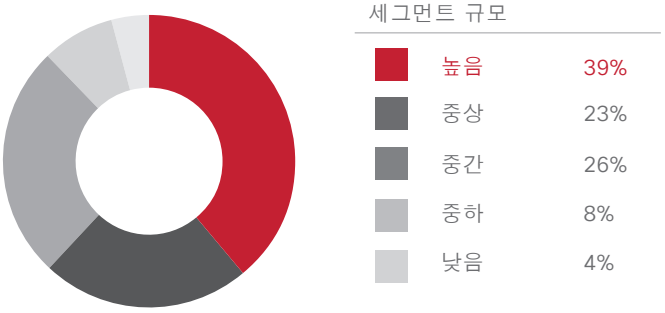
출처: Cisco 보안 기능 벤치마크 조사

조직 보안 지능화 정도

그림 33. 보안 프로세스의 지능화 정도

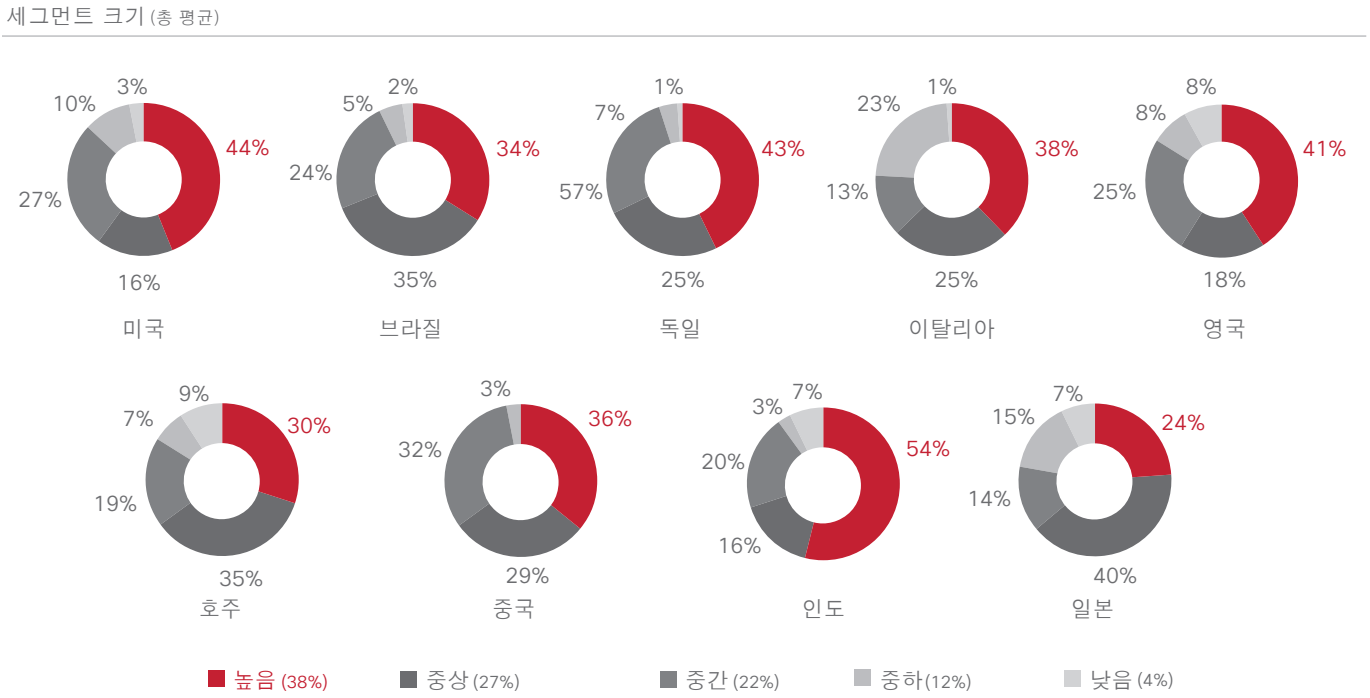
대부분의 회사는 정교한 보안 프로필을 갖추고 있습니다. 이는 모든 국가(그림 34)와 모든 산업(그림 35)에서 마찬가지입니다.

세그먼트는 보안 우선 순위의 정교성 수준 증가와 프로세스 및 절차에 어떻게 반영되는가를 나타냅니다.



출처: *Cisco 보안 기능 벤치마크 조사*

그림 34. 국가별 보안 프로세스의 정교성

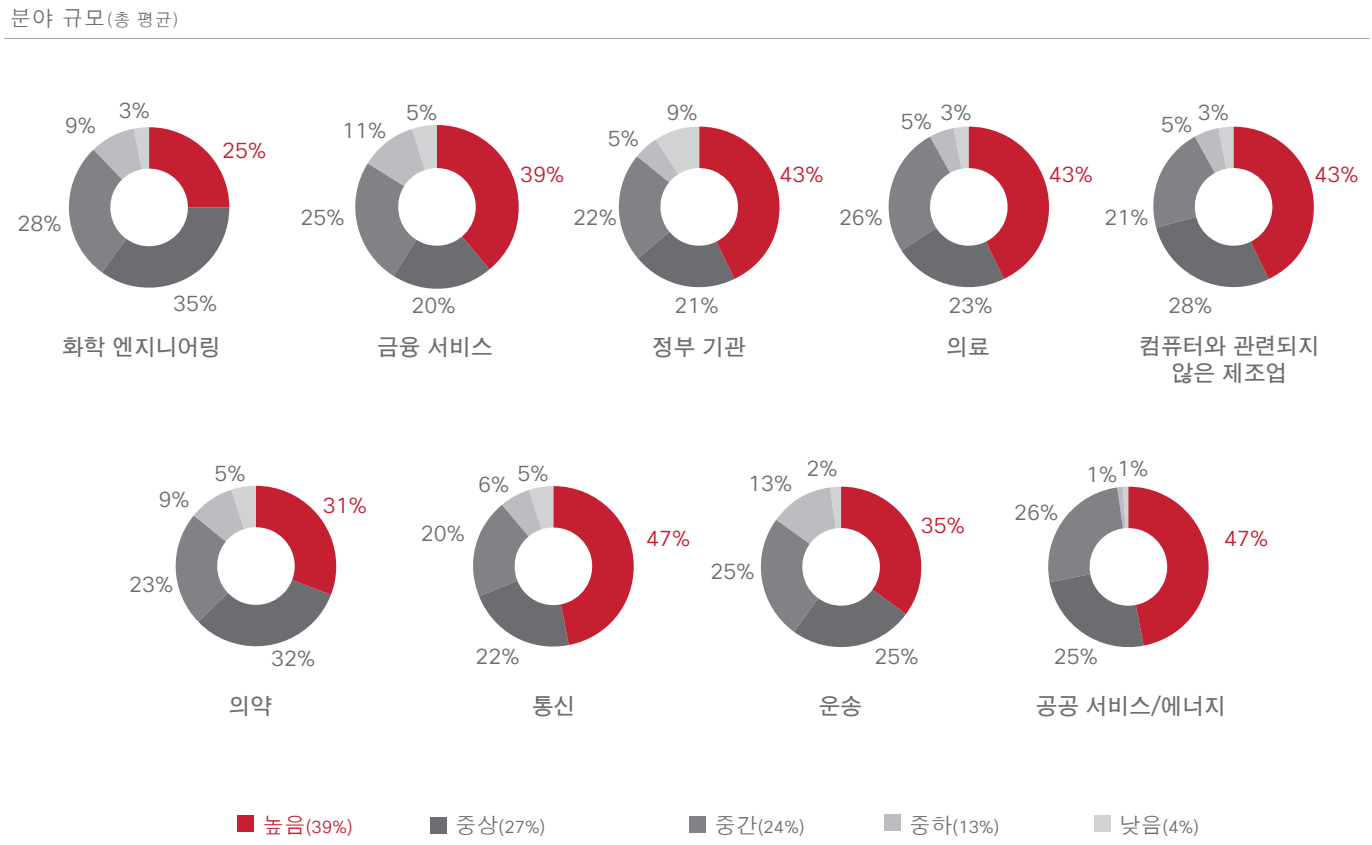


출처: *Cisco 보안 기능 벤치마크 조사*

보고서 공유

그림 35. 산업별 보안 프로세스의 정교성

통신 및 공공 서비스/에너지 조직의 약 1/2이 매우 지능화된 보안 분야로 분류됩니다.



출처: *Cisco 보안 기능 벤치마크 조사*

중견기업의 체계적인 보안 준비 상태

대기업에서는 최신 기술 구매 예산, 예산을 관리하는 숙련된 직원 등 대부분의 리소스에 액세스할 수 있으므로 보안을 성공적으로 관리할 것이라고 기대합니다. 대규모 중견기업(연구 목적에 따른 분류 정의: 직원 수 500-999명)은 보안 사고에 대비한 준비 상태가 대기업(직원 수 1,000명 이상)에 뒤질 것이라고 추측할 수 있습니다. 하지만 *Cisco 보안 기능 벤치마크 조사*에 따르면 대규모 중견기업은 조직의 유연성과 민첩도 향상으로 인해 많은 영역의 보안 준비 상태가 대기업에 필적할 뿐만 아니라 일부 영역에서는 더 앞서는 것으로 나타났습니다.

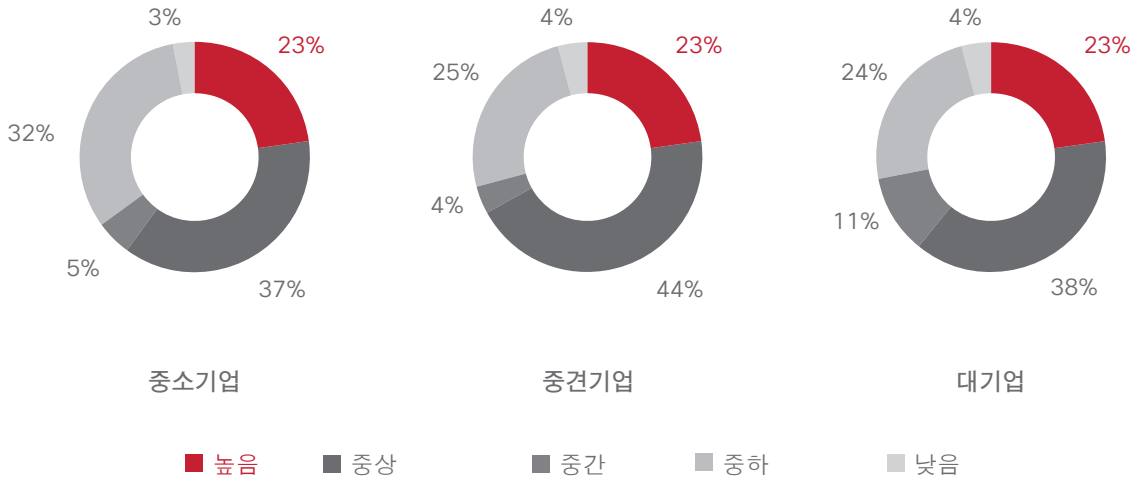
실제로 이번 연구에 따르면 대규모 중견기업은 매우 정교한 보안 상태를 구축하고 있습니다. 그림 36을 보면, 대규모 중견기업은 소규모 중견기업(직원 수 250-499명) 및 대기업(직원 수 1,000명 이상)보다 지능화된 보안의 수준이 더 높게 나타났습니다.

중견기업은 경제 회복의 동력이므로 중견기업이 공평한 경쟁을 할 수 있다는 것은 참 고무적인 소식입니다.

중견기업과 그 보안 준비 상태에 관한 벤치마크 설문조사의 주요 조사 결과:

- 중견기업의 92%와 대기업의 93%는 내부에 보안 사고 대응 팀을 운영하고 있습니다.
- 중견기업의 94%와 대기업의 92%는 보안을 직접 전담하는 책임자를 두고 있습니다.

그림 36. 대규모 중견기업의 보안 상태 정교성 수준



세그먼트는 조직 내에서 보안 우선 순위와 관련하여 높아지는 정교성 수준과 그에 따른 프로세스 및 절차 해석 방법을 보여줍니다.

대부분의 중견기업이 소기업 및 대기업보다 더 높은 중상 이상의 수준으로 평가되었습니다.

60% 이상이 정교한 보안 프로필을 갖추고 있습니다.

출처: *Cisco 보안 기능 벤치마크 조사*

보고서 공유

3. 지정학 및 업계 트렌드

Cisco 보안, 지정학 그리고 정책 전문가들이 조직, 특히 다국적 기업에서 모니터링해야 하는 현재 그리고 새로운 지정학적 트렌드에 대해 알아보았습니다. 또한, 데이터 주권(Data Sovereignty), 데이터 현지화(data localization), 암호화 및 데이터 호환성과 관련하여 전 세계에서 최근 전개된 사건도 함께 살펴보았습니다.

거버넌스가 취약한 영역에서 성행하는 사이버 범죄

CISO와 기타 보안 리더들이 언제나 지정학적 역학관계에 주목할 수는 없지만, 특히 다국적 기업에 소속된 경우라면 지정학적 역학관계에 주목해야 합니다. 지정학적 환경의 변화는 글로벌 공급망과 기업의 국가별 고객 및 직원 데이터 관리 방법에 영향을 미칠 뿐만 아니라, 법률 및 규제 비용, 영업 비밀 도난 위험, 물리적 명예 훼손의 가능성 등이 높아질 수 있습니다.

사이버 범죄가 전 세계 특히, 거버넌스가 약한 영역을 중심으로 성행하고 있습니다. 예를 들어 동유럽은 오래전부터 조직범죄의 온상이 되고 있습니다. 거버넌스가 약한 영역에서 정부 인텔리전스 서비스와 사이버 범죄 조직 그룹이 연루된 확실한 증거를 찾는 것은 드문 일이 아닙니다.

미국 당국에 따르면 자국 내 자산을 대상으로 최근에 발생한 주요 공격 중 일부는 이들 지역을 근거로 한다고 합니다. 일부 공격은 수익을 노리지 않고 정치적 성향의 공격이나 지적 정보 수집 또는 인프라 침입을 목적으로 하는 것으로 드러났습니다.[7] 이는 공격이 정부 주도하에 이루어지거나 정교한 사이버 범죄 조직에 의해 조직적으로 수행되었다는 증거일 수 있습니다.

많은 정부가 법률과 규제를 통해 사이버 거버넌스를 강화하기 위해 조직적으로 움직이고 있습니다. 예를 들어 중국에서는 18회 중국 공산당(CCP) 대표회의 4차 총회의 테마로 "법규범"을 설정했습니다.[8] 베이징에서는 기업과 정부 내에서 부패를 근절하고 법률을 시행할 것을 약속했습니다. 이러한 노력으로 인해 법률 시행과 사이버 범죄를 추적하여 색출하려는 국제적 노력이 강화됨에 따라 사이버 범죄자들이 은신하기가 점점 더 어려워지고 있습니다.

인터넷을 활용하는 다국적 테러리스트 그룹

새로운 지정학적 트렌드로 이슬람 국가(ISIS 또는 ISIL이라고도 함)와 같은 다국적 테러리스트 그룹이 출현하고 있습니다. ISIS와 같은 그룹은 주요 사이버 범죄 활동에는 참여하지 않는 것 같지만 인터넷 즉, 소셜 미디어를 중심으로 조직원을 모집하고 있습니다. 현재로는 주요 다국적 테러리스트 그룹에서 갈취, 인신매매, 석유 등과 같은 기존의 자금 조달 방식으로 충분한 자금을 조달하고 있는 것 같습니다. 하지만 조직이 성장할수록 전 세계에서 자금을 조달하기 위해 사이버 범죄로 전환할 수 있습니다. 또한 기존의 그룹과 동일한 리소스에 접근할 수 없는 신흥 테러리스트 조직은 빠른 성장을 위해 사이버 범죄를 모색할 수 있습니다.

사이버 스파이를 방어하기 위한 새로운 제안 방식은 Cisco 블로그 게시물 "Cupcakes and Cyberespionage"를 참조하시기 바랍니다.

데이터 주권, 데이터 현지화 및 암호화의 문제

미국 정부의 감시 범위 확장, 데이터 주권(일방적 접근을 모색하는 외국 정부 또는 법원이 아닌 데이터가 상주하는 국가의 관할권이 데이터에 적용된다는 개념) 및 데이터 현지화(데이터를 특정 위치에 저장하도록 하는 정부 규정)에 대한 에드워드 스노든(Edward Snowden)의 주장이 뜨거운 쟁점이 되고 있습니다.

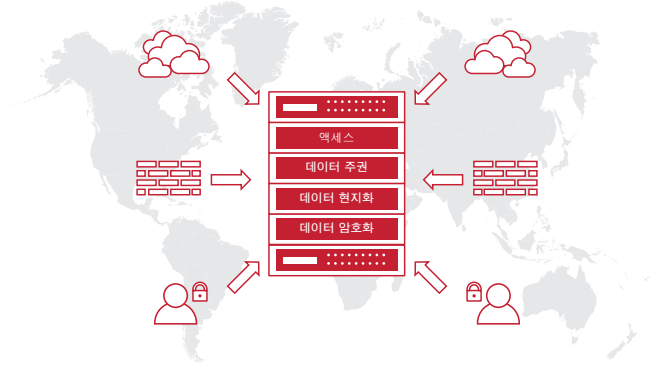
일부 국가에서는 외국 정부에서 시민의 데이터에 액세스하지 못하도록 데이터를 현지화하는 방법을 모색하기 시작했습니다. 이러한 국가에서는 데이터를 자국 내에 유지하거나 특정한 방식으로 경로를 지정하고 기업에서는 국내에서 제조된 장비를 사용하도록 요구하는 규정을 입안하고 있습니다.

예를 들어 브라질에서는 "[연루된] 기업의 사용자 개인 정보, 통신 및 특정 온라인 로깅 데이터 공유를 광범위하게 제한하는 개인 정보 요건 제약" 법률을 최근에 실행했습니다.[9] 한편, 러시아에서는 인터넷 데이터를 비롯하여 러시아 국민의 개인 데이터를 처리하는 모든 데이터 운영자에게 러시아 내부의 서버와 데이터베이스에 해당 데이터 사본을 유지하도록 하는 데이터 보호 및 정보 관련 법률을 최근에 개정했습니다. 이 법률은 2015년에 효력이 발생할 예정입니다.[10]

상호 운용성이 없는 법률을 규정하여 데이터 현지화를 규정하는 국가의 경우 다국적 기업의 법률 요건이 충돌하는 부정적인 결과를 초래할 수도 있습니다. 한 국가의 데이터 생성, 유지 또는 폐기 규정을 준수할 책임이 다른 국가의 법률을 위반할 수 있습니다.

잠재적인 법적 책임의 충돌 외에도 데이터 현지화 요건은 국가 간 데이터 흐름을 제한할 수 있습니다. 이로 인해 혼동이 발생하고 네트워크를 관리하는 데 문제가 될 수 있습니다.

그림 37. 데이터 주권, 현지화 및 암호화의 균형 조정 문제



공급망의 측면에서도 마찬가지입니다. 많은 글로벌 공급망 운영자들이 클라우드 기반 기술을 사용하여 전 세계의 모든 파트너를 연결하고 있습니다. 데이터 현지화는 비즈니스 네트워크를 통한 데이터 교환을 방해하거나 차단하여 사이버 범죄 활동을 단속하기 위해 국가 간 활동을 방해할 수 있습니다.

또한 일부 국가에서는 국내 기술만 사용하도록 채택하거나 국민의 데이터를 취급할 수 있는 사람을 엄격하게 제한하므로, 글로벌 인재 풀에서 삭제되어 새로운 아이디어를 교류하는 혁신적인 활동에서 제외될 가능성이 있습니다.

미국의 일부 선도적 기술 기업에서는 국경없이 인터넷을 통과하는 데이터 보호에 대한 고객의 우려를 해결하기 위한 방안으로 엔드 투 엔드 암호화를 사용하려고 합니다. 하지만 미국 정부는 그런 암호화로 인해 국민 보호 능력이 저해될 것을 우려합니다. 미국 NSA(National Security Agency)와 유사한 영국 최고 전파 정보국인 GCHQ의 새로운 이사는 미국의 거대 소셜 미디어 기술 기업이 테러리스트들이 암호화된 통신을 전 세계로 보낼 수 있도록 허용하여 테러리스트 그룹을 지원하고 있다고 주장했습니다.[11]

이러한 비판에도 불구하고 기술 기업들은 정부가 공공 안전과 국가 보안에 대한 위협으로부터 보호하면서 언론의 자유와 보호 무역의 중요성을 효율적으로 반영하는 정책을 채택할 때까지, 고객의 신뢰 회복을 목적으로 기술적 조치를 개발하여 채택하려는 노력을 계속할 가능성이 큽니다.

기술 제품 및 해당 제품을 개발하는 회사에 대한 신뢰는 국가와 정부와 국민이 자신들의 데이터가 보호된다고 신뢰하는 데 많은 도움이 될 것입니다. Cisco의 법무 자문 담당 상임 부사장 겸 총장인 Mark Chandler는 올해 초에 Cisco 블로그에 "이러한 문제를 해결하기 위한 진지한 노력은 신뢰를 구축할 뿐 아니라, 차세대 인터넷에 대한 전망을 밝히고 인간과 디바이스를 연결하는 세상을 더욱 자유롭고 번영하게 하여 세계 시민의 시대가 도래하게 할 것입니다."라고 게시했습니다.[12]

데이터 정보 보호 호환성

데이터 정보 보호에 대한 개인 또는 조직의 태도는 생활 및 업무 위치에 따라 크게 다를 수 있습니다. 이러한 서로 다른 관점은 정부가 데이터 정보 보호를 규제하는 방식과 이러한 규제가 서로 일치하지 않을 때 기업이 비즈니스를 수행하는 방식에 영향을 미칩니다. Cisco에서 후원하고 Cloud Security Alliance에서 작성한 ***데이터 보호 히트 인덱스 설문조사 보고서 (Data Protection Heat Index Survey Report)***에는 기업이 자국 밖에 있는 데이터를 사용하거나, 비즈니스를 운영하는 국가 밖의 특정 집단에 속한 자사의 데이터를 활용하면서 겪는 몇 가지 과제가 자세히 설명되어 있습니다.

클라우드 서비스 증가로 인해 데이터 정보 보호 호환성에 대한 대화, 즉, 데이터 정보 보호에 대한 일관적, 전역적 방식이 긴급히 필요하게 되었습니다. 예를 들어, 미국에 기반을 둔 기업이 인도 회사에서 클라우드 스토리지를 구매하고 이 클라우드를 사용하여 독일에 거주하는 고객의 데이터를 저장할 경우 어느 지역 또는 국가의 정보 보호 법률이 적용될까요?

그림 38. 다양한 규제 및 소비자 기대 충족

데이터 정보 보호 호환성에 대한 기타 동인으로는 IoT(Internet of Things)와 빅데이터가 있습니다. 엔터프라이즈에서 디바이스를 연결할 새로운 방법을 찾고 많은 양의 데이터세트를 사용하여 비즈니스 결정을 내림에 따라, 이 데이터를 글로벌 규모로 처리할 수 있는 체계와 규칙이 필요하게 되었습니다.

지역 또는 국가 그룹 전반에서 데이터 정보 보호 요건을 조정하기 위한 다양한 노력이 진행 중입니다. 예를 들어, 데이터 보호 규제의 조화를 위해 기존 데이터 보호 프레임워크를 업데이트할 EU 법률, *일반정보보호규제(General Data Protection Regulation, GDPR)*이 제정 중입니다. 데이터 정보 보호 및 데이터 주권 법률에 대한 합의를 달성하기 위한 노력이 강화되고 있습니다. 조화가 이루어질수록 좋지만, 최종 문구가 결과 중심적이고 다른 지역과 상호 운용되며 새로운 기술 현실에 적합한 것도 중요합니다. 아시아 태평양 지역은 현지 경제에서 더 용이하게 데이터를 공유할 수 있도록 APEC(Asia-Pacific Economic Cooperation)에서 CPEA(Cross-Border Privacy Enforcement Arrangement, 개인정보 감독기관간 협력협의회 협정)를 개발했습니다. 국가 및 지역 간에 모두 데이터를 자유롭게 이동할 수 있는 개방된 인터넷을 장려하는 글로벌 표준으로 데이터 정보 보호 및 보안의 호환 체제를 구축하기 위해서는 정부들이 더 많은 노력을 해야 합니다.

국가와 지역이 데이터 정보 보호에 대한 접근 방식을 확실히 정할 경우 엔터프라이즈는 전 세계에서 일관적 정보 보호 사례를 적용하고 효과적인 "계획적인 정보 보호(privacy by design)" 프레임워크를 구현하여 처음부터 제품과 서비스에 정보 보호 역량을 실현할 수 있습니다. 분명하고 일관된 정보 보호 규제 프레임워크는 제품과 서비스를 어디에 구축하는가와 상관없이 기업이 정보 보호 요건을 충족 및 초과하여 혁신적 제품 개발 및 데이터 사용을 도와줍니다.

데이터 정보 보호: 인식 공유

북미, EU, 아시아 태평양 지역의 글로벌 정보 보호 전문가를 대상으로 데이터 보호 설문조사를 실시하고 해당 지역의 데이터 규제, 정부 사례, 사용자 콘텐츠, 보안 표준에 대해 질문했습니다. 응답 결과에 따르면, 데이터 정보 보호 및 글로벌 정보 보호 표준의 의미에 대한 응답자들의 이해가 상당히 일치하고 있는 것으로 나타났습니다.

- **데이터 거주주 및 주권(Data residency and sovereignty):** 응답자들은 개인 데이터 및 PII(Personally Identifiable Information, 개인식별정보)를 대부분의 국가에서 그대로 유지해야 하는 데이터로 식별했습니다.
- **합법적 도청(Lawful interception):** 응답자들은 범죄 수사에 필요한 경우와 같이 데이터를 도청할 수 있는 시기와 방식에 대해 동일하게 해석하고 있는 것으로 나타났습니다.
- **사용자 동의(User consent):** 응답자의 73%는 지역에만 국한되지 않고 전 세계적으로 적용되는 소비자 정보 보호 권리 선언이 있어야 한다는 데 동의했습니다. 65%는 UN에서 이러한 선언을 만드는 데 적극적인 역할을 해야 한다고 말했습니다.
- **정보 보호 원칙(Privacy principles):** 응답자에게 OECD(Organisation for Economic Cooperation and Development)의 정보 보호 원칙이 데이터의 조화로운 이용에 도움이 될지, 아니면 더 큰 긴장이 조성될지에 대해 질문했습니다. 설문조사에 참여한 데이터 정보 보호 전문가들은 대부분 이러한 원칙을 채택하는 데 동의했습니다.

요약하면, 데이터 정보 보호 설문조사는 많은 전문가들이 기본적 정보 보호 원칙에 동의하며, 전 세계적으로 채택 및 표준화할 경우 비즈니스를 방해하는 대신 비즈니스를 지원할 것이라는 점에 대해 동일한 생각을 하고 있는 것으로 나타났습니다. 이 결과는 또한 데이터 정보 보호 전문가들이 정보 보호 요건에 맞게 기술 솔루션을 새로 바꾸는 대신, 새로운 기술 솔루션에 맞게 정보 보호 원칙을 "조정" 하는 데 관심이 있는 것으로 나타났습니다. 하지만, 현재 정보 보호 규제 프레임워크는 상대적으로 초창기이며 빠르게 변화하고 있습니다.

조화 수준이 진전될수록 기업과 개인은 더 많은 이점을 얻을 수 있습니다. 하지만 업계가 전 세계의 정보 보호 프레임워크가 일치하지 않는 것으로 판단하는 이상, 기업은 정보 보호 및 데이터 보호 문제를 주의 깊게 생각하고 제품과 프로세스를 사전 대응적으로 조정하여 다양한 고객 및 규제 기대를 충족해야 합니다.

데이터 보호 문제에 대한 자세한 내용은 Cisco 보안 블로그 게시물 "Data Protection in the Balance—EU Citizen Protection and Innovation" 을 참조하시기 바랍니다.

4. 사이버 보안에 대한 관점의 변화 – 사용자부터 기업 경영진까지

Cisco 보안 전문가는 기업이 조직의 보안을 강화할 수 있도록 사이버 보안에 대한 접근 방식을 다른 시각으로 보아야 할 때라고 제안합니다. 전략으로는 사람, 프로세스, 기술을 연계하여 보안을 경영진 수준의 주제로 만들기 위한 새로운 방식을 고려하는 전략과 더욱 정교한 보안 제어를 채택하여 엔드포인트 및 공격 표면을 줄이고 공격 후 네트워크를 강화하는 전략이 있습니다.

보안 액세스: 누가, 언제, 어떻게 네트워크에 액세스하는지 이해

CISO 및 기타 보안 전문가는 네트워크 정보 및 서비스에 대한 액세스와 관련하여 복잡한 과제에 직면해 있습니다. 모빌리티 및 BYOD(bring-your-own-device) 정책으로 전환되는 트렌드에 따라, 직원이 어디에 있든, 네트워크에 어떤 방법으로 연결하든, 엔터프라이즈 리소스에 액세스할 수 있도록 보장해야 합니다.

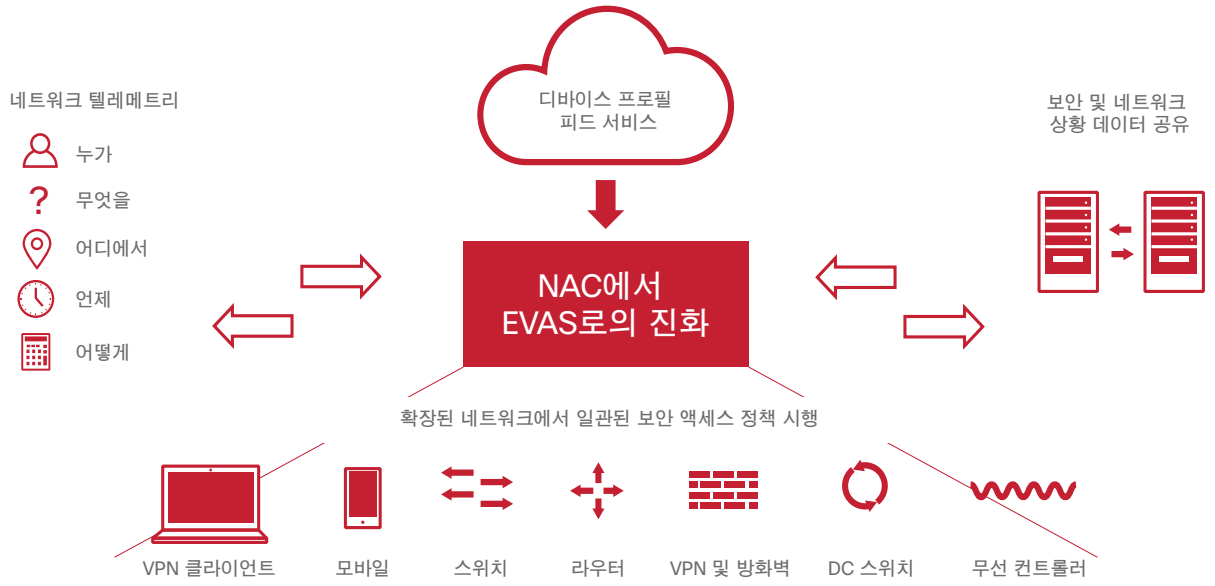
또한 보안 전문가는 적법한 사용자의 액세스를 방해하지 않으면서 승인되지 않은 사용자 또는 범죄 공격으로부터 네트워크를 보호해야 합니다. 예를 들어, VPN(Virtual Private Networks) 가상 사설 네트워크)은 네트워크 액세스 제어를 제공하기 위한 표준 솔루션으로 사용되곤 했습니다. 하지만, 일부 VPN을 이용하려면 사용자뿐만 아니라 특수 소프트웨어의 복잡한 로그인 절차가 필요하여 사람들이 네트워크에 연결하는 시기 및 방식이 제한됩니다. 또한, 대부분의 VPN에서는 IT 부서가 누가 어디에서 액세스 권한을 얻고 있는지 식별할 수 없으며 사용 중인 디바이스도 식별할 수 없습니다. VPN은 보다 나은 엔드포인트 보안을 제공하기 위해 더 많은 가시성을 제공하는 동시에 더욱 투명한 사용자 환경을 제공하도록 진화되었습니다.

NAC(Network Access Control)은 기본적 보안 보호에서 벗어나 더욱 정교한 EVAS(Endpoint Visibility, Access, and Security) 제어로 진화하고 있습니다. 기존 NAC 기술과 달리, EVAS는 사용자 역할, 위치, 비즈니스 프로세스 고려 사항, 위험 관리와 같은 액세스 정책을 시행하기 위해 더욱 세분화된 정보를 사용합니다. 또한 EVAS 제어는 컴퓨터 이외의 디바이스에도 액세스 권한을 부여할 수 있어 네트워크 관리자가 모바일 및 IoT 디바이스를 통해 액세스를 제공할 수 있습니다.

EVAS에서는 보안 시행에 대해 Network-as-a-Sensor 방식을 적용하여 네트워크 서비스에 연결하기 전 원격 디바이스(VPN)에서 액세스를 부여 또는 중지하거나 민감한 리소스 풀 전반의 네트워크 자체 내에서도 확장 네트워크를 통해 액세스를 부여 또는 중지할 수 있습니다. EVAS에서는 또한 조직이 엔드포인트 및 네트워크 공격을 줄이고 공격 규모 및 범위를 제한하며 문제 해결 프로세스를 조정하고 공격 발생 후 네트워크를 더욱 강화할 수 있습니다.

EVAS 솔루션에 대한 자세한 내용 및 이 솔루션을 이용하여 조직의 보안을 개선하는 방법은 Cisco 보안 블로그 게시물, "New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access" 를 참조하십시오.

그림 39. NAC(Network Access Control)에서 EVAS(Endpoint Visibility, Access, and Security) 제어로 진화



공격 전, EVAS는 다음과 같은 기능을 수행할 수 있습니다.

- **위험 자산 식별.** 네트워크에 연결된 모든 자산을 항상 모니터링하여 규제를 준수하지 않는 사용자, 디바이스, 애플리케이션을 식별하고 이 정보를 서드파티 취약점 평가 도구와 연계할 수 있습니다.
- **위험 감소 개선.** 실행 가능한 정보를 수집하고 다른 보안 및 네트워크 애플리케이션과 공유하여 워크플로를 개선하고 운영을 간소화하며 리미디에이션 작업의 우선 순위를 정할 수 있습니다.
- **세분화된 네트워크 액세스 정책 시행.** 세분화된 정책 시행을 위해 상황 정보를 제공하고 민감한 콘텐츠, 자산 또는 네트워크 세그먼트에 대한 액세스를 제한합니다.

공격 중, EVAS는 다음과 같은 기능을 수행할 수 있습니다.

- **고급 네트워크 기반 위협 방어 시스템과 통합.** 시간의 경과에 따라 공격 데이터 엔드포인트 연결, 컨피그레이션, 동작 패턴 간 상관관계를 분석하기 위한 악의적 활동이 탐지될 경우 정보를 공유합니다.
- **감염 시스템에서 "킬 체인" 전술 차단.** 감염된 시스템이 정책에 의해 제어되는 비승인 네트워크 자산에 도달하여 인증서를 훔치거나 권한을 에스컬레이션 하거나 중요 데이터를 탈취하지 못하도록 수평적 공격 이동을 제한합니다.
- **공격 범위 제한.** 이상 동작을 보이는 시스템을 제한하여 격리합니다.

공격이 탐지된 후, EVAS는 다음과 같은 기능을 수행할 수 있습니다.

- **엔드포인트 프로필의 취약점 평가.** EVAS 데이터베이스 정보를 취약점 분석 툴과 공유하여 IT 운영에서 해결 방법의 우선 순위를 결정할 수 있습니다.
- **감염 시스템 해결.** EVAS는 SIEM(Security Information and Event Management) 시스템 및 엔드포인트 보안 시스템과 통합하여 해결을 자동 수행하고 진행 상태를 모니터링할 수 있습니다.
- **액세스 정책 및 보안 제어 정밀 조정.** 네트워킹 및 보안 장비를 사용하여 애플리케이션 트래픽을 분할하거나 새로운 방화벽 규칙 또는 IPS 서명을 추가합니다.

과거의 과도하게 복잡한 네트워크 액세스 제어와 달리, EVAS 솔루션은 비즈니스를 지원합니다. 조직이 BYOD 정책, 클라우드 컴퓨팅, 모빌리티 이니셔티브를 수용함에 따라, 가시성 향상, 연결된 사용자 및 디바이스에 대한 컨텍스트 개선, 보안 정책의 효과적 시행이 더욱 중요해지고 있습니다. Cisco 보안 전문가는 CISO가 사용자, 디바이스, 네트워크, 클라우드 서비스 간 복잡한 연결 그물을 관리하기 위해 점차 EVAS 솔루션으로 전환할 것으로 내다보고 있습니다.

보고서 공유

경영진의 참여에 달린 오늘날의 사이버 보안

*Cisco 보안 기능 벤치마크 연구*에 따르면, 91%의 조직에는 보안을 직접 책임지는 임원이 있습니다. 하지만 현대 비즈니스에서 보안 리더십은 조직에서 경영진 수준으로 더욱 상승되어야 합니다.

최근에는 유명 기업에서 발생한 대규모 데이터 침해 사건, 데이터 보안과 관련된 추가 법률 및 규제, 지정학적 역학, 주주의 기대 등 경영진이 사이버 보안을 중요 안건으로 고려하게 되었습니다. ISACA(Information Systems Audit and Control Association)의 보고서에 따르면, 기업 이사의 55%가 직접 사이버 보안을 위험 영역으로 이해 및 관리해야 하는 것으로 나타났습니다.[13]

이러한 현상은 긍정적인 발전이지만, Cisco 보안 리더가 올바르다고 생각하는 것은 아직도 진행되지 않고 있습니다. 현대 경제에서는 모든 회사가 IT를 실행합니다. 따라서 직책 또는 직무 기술서에 "보안" 이 포함된 직원뿐만 아니라 CEO부터 신입 직원에 이르는 조직의 모든 사람들에게 보안은 중요한 문제입니다. 모든 사용자가 책임을 지고 피해를 입지 않는 방법을 알아야 합니다.

Cisco 보안 리더는 사이버 보안의 미래에서 핵심적 요소는 경영진의 적극적 참여임을 주장합니다. 업계 전반의 기업 경영진은 비즈니스에 대한 사이버 보안의 위험이 무엇이고 어떤 잠재적 영향이 있는지 알아야 합니다. 조직에 영향을 미치는 사이버 보안 문제의 범위를 확실히 이해하기 위해 일부 경영진은 기술 및 사이버 보안 전문 지식을 갖춘 구성원을 추가해야 할 수 있습니다.

경영진은 또한 보안 제어에 대해 다음과 같이 까다로운 질문을 해야 할 수 있습니다. *어떤 통제 수단을 가지고 있는가? 얼마나 테스트해 보았는가? 보고 프로세스가 있는가? 피할 수 없는 감염을 얼마나 빨리 탐지하고 복구할 수 있는가?* 아마도 가장 중요한 질문은 *또 무엇을 알아야 하는가? 일* 것입니다. CIO는 경영진 구성원에게 의미가 있으면서 비즈니스에 미치는 영향을 나타내는 용어로 경영진에서 이러한 질문에 대답할 준비를 해야 합니다.

최근 FORTUNE magazine에 게재된 인터뷰에서[14] Cisco 최고 보안 및 신임 책임자인 John Stewart는 이러한 질문을 하는 경영진은 "흥미로운 다운스트림 효과" 의 계기를 만들어 결과적으로 보안 업계 성숙으로 이어질 것이라고 말했습니다. Stewart는 이어서 다음으로 중요한 단계는, 아직 희망 단계이지만 제조업체들이 최종적으로 제품에 보안을 구현해야 함을 인식하는 것이라고 말했습니다.

Stewart는 IoT(Internet of Things)가 발전하고 "인터넷에서 사람이 관여하는 디바이스보다 사람이 관여하지 않는 디바이스" 가 더 많아짐에 따라 잠재적으로 큰 "사고" 를 피할 수 없을 것이라고 예상합니다. 제품에 보안을 설계함으로써 이러한 문제의 대부분을 방지하거나, 최소한 그로 인한 영향을 줄일 수 있습니다.

따라서, 기술 제조업체의 경영진은 보안 리더에게 *제품에 보안을 구현하고 있는가? 그렇지 않다면, 얼마나 빨리 시작할 수 있는가? 라는* 질문을 해야 합니다.

Cisco 최고 보안 및 신임 책임자 John Stewart가 사이버 보안의 투명성 및 경영진 책임에 대해 게시한 동영상 블로그를 참조하십시오. http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Cisco 보안 선언: 현실의 보안을 달성하기 위한 기본 원칙

오늘날의 CISO는 어려운 질문을 해야 합니다. *잠재적 보안 문제가 발생할 경우 보안 팀이 최초의 접점으로 비즈니스에 대응하도록 하려면 어떻게 해야 하는가? 어떤 보안 문제가 가장 관련성이 높고 조치가 필요한지 확인하기 위한 툴과 가시성이 있는지 어떻게 확인할 수 있는가? 그리고, 비즈니스 성공의 핵심인 사용자를 현장에서 근무할 때를 포함하여 항상 안전하게 보호하려면 어떻게 해야 하는가?*

Cisco 보안 전문가는 CISO가 Cisco 보안 선언이라고 하는 보안 원칙을 구현 및 준수함으로써 이러한 질문에 대응할 수 있다고 제안합니다.

보안 팀과 조직 내 사용자는 이 최초 보안 선언을 통해 오늘날 사이버 보안의 과제를 더 정확하게 이해하고 대응할 수 있습니다. 이러한 원칙은 조직이 보안에 대해 더욱 동적인 접근 방식을 취하고 적보다 더 효과적으로 대응하고 혁신적으로 발전하기 위해 노력하는 조직의 기준선이 될 수 있습니다.

1. **보안은 비즈니스의 성장 엔진으로 고려되어야 합니다.** 보안은 사용자 생산성을 떨어뜨리거나 비즈니스 혁신을 가로막는 장애물이 되어서는 안 됩니다. 하지만 보안 팀은 아직 이러한 문제가 있는 기술 솔루션을 적용하고 있습니다. 가장 큰 이유는 새로운 기술의 구축이 필요한 비즈니스 프로젝트에 대한 회의에 제때 또는 전혀 참여하지 못했기 때문입니다. 하지만 보안 전문가도 적극적인 회의를 요청하지 않은 잘못이 있습니다. 보안 전문가는 기술 회의에 참여하기 위해 미리 조치를 취하고 보안 프로세스를 통해 조직이 조직의 민첩성과 성공을 지원하는 동시에 데이터, 자산, 이미지를 보호하는 방법을 이해해야 합니다.

2. **보안은 기존 아키텍처에서 작동해야 하며 사용 가능해야 합니다.** 보안 팀은 보안 강화가 목적인 새로운 기술 솔루션을 수용하기 위해 아키텍처를 구축할 필요가 없어야 합니다. 아키텍처는 원래 억제하는 특성이 있습니다. 조직은 새로운 보안 기술을 수용하기 위해 비즈니스 방식을 변경할 필요가 없어야 하고 기존에 구현된 기술로 인해 운영 방식을 변경하지 못하도록 방해되어서도 안 됩니다. "아키텍처 과부하"의 결과로 사용자가 보안 아키텍처를 우회하여 조직이 보안 문제에 노출됩니다. 또한, 너무 어려워 사용하기 어렵거나 극소수의 전문 보안 인력이 유지 관리해야 하는 보안 기술은 조직에 유용하지 않습니다.

3. **보안은 투명해야 하며 정보를 제공해야 합니다.** 사용자는 보안 문제로 특정 작업을 할 수 없을 경우 그 이유를 알 수 있는 정보를 확인할 수 있어야 합니다. 또한 직무를 수행한다는 핑계로 보안을 우회하지 않고 맡은 작업을 안전하게 수행할 수 있는 방법을 알아야 합니다. 예를 들어, 사용자가 웹 페이지에 대한 액세스를 시도할 때 "관리자가 이 사이트에 대한 액세스를 거부했습니다."라는 메시지가 표시될 경우 페이지에 액세스할 수 없는 이유에 대한 상황 정보가 없습니다. 하지만 메시지 내용이 "지난 48시간 동안 이 사이트에서 악성코드가 공급되었기 때문에 액세스가 거부되었습니다."일 경우 사용자는 더 정확한 정보를 확인하고 조직뿐만 아니라 사용자 개인에게 미칠 수 있는 잠재적 위험을 이해할 수 있습니다. 보안 기술은 또한 사용자에게 분명한 행동을 권장하거나 빠른 시간 안에 지원을 받을 수 있도록 적절한 리소스에 연결하여 사용자가 목적을 달성할 수 있도록 해야 합니다.

4. **보안은 가시성과 적절한 행동을 지원해야 합니다.** 보안 팀은 개방형 보안 아키텍처의 보안 솔루션을 이용하여 이러한 솔루션이 확실히 효과적인지 여부를 판단할 수 있습니다. 보안 전문가도 네트워크에 대한 가시성을 자동화하는 툴을 사용하여 트래픽뿐만 아니라 네트워크를 구성하는 자산도 볼 수 있어야 합니다. 보안 팀은 보안 기술의 작동 방식과 IT 환경에서 어떤 부분이 정상이고 정상이 아닌지를 이해함으로써 관리 작업 부하를 줄이는 동시에 더 동적으로, 더 정확하게 위협을 식별 및 대응하고 방어 수단을 조정할 수 있습니다. 이러한 방식에서는 보안 팀이 더욱 관련성이 높은 대상 제어 수단을 활용하여 해결을 지원할 수 있습니다.

5. **보안은 "인적 문제"로 생각해야 합니다.** 보안에 대한 기술 중심 접근 방식은 보안을 개선하는 것이 아니라, 실제로 악화시킵니다. 기술은 사람들이 환경을 보호하는 능력을 향상해 주는 툴에 불과합니다. 보안 팀은 사용자가 사무실에서나 가정에서나 이동 중에 기술을 사용할 때 안전 수칙을 지키도록 교육함으로써 어떤 문제가 발생했다고 생각될 때 정확한 결정을 내리고 빠르게 도움을 요청할 수 있는 역량을 갖추었다고 느끼도록 해야 합니다. 보안 전문가와 사용자가 더 원활히 소통할 경우 사용자들이 기술만으로는 보안을 보장할 수 없다는 것을 이해하게 됩니다. 사람, 프로세스, 기술이 모두 모여 오늘날의 위협에 대한 방어 수단을 구축해야 합니다. 위에서 아래로 조직의 모든 사용자가 노력하고 경계함으로써 보안을 강화할 수 있습니다.

Cisco 보안 선언은 변화에 대한 요청입니다. 현실에서 보안 기술, 정책, 모범 사례는 조직의 모든 사람들에게 평균적 보안 수준을 높이고 기업뿐만 아니라 사용자 개인까지 위험에 대해 더욱 정확한 정보에 기반을 둔 결정을 할 수 있도록 도와야 합니다. 또한 사용자는 지침을 제공하는 확고한 원칙을 바탕으로 특정 작업을 할 수 없는 이유와 보안을 우회할 경우 나타날 수 있는 영향에 대해 확실히 이해할 수 있습니다.

Cisco 보안 선언 또는 이 핵심 원칙을 반영한 다른 선언을 통해 사용자와 보안 관계자 모두 보안을 전반적으로 이해할 수 있습니다. 많은 위협을 방지할 수 있지만 감염이 불가피한 경우 빠른 리미디에이션을 통한 해결이 가능합니다. 목표는 결국 감염이 발생한 경우 해결 시간을 단축하는 것이며 이러한 사건을 방지하기 위한 노력에만 집중하는 것이 아닙니다.

회사 소개

Cisco는 현실에 지능형 사이버 보안을 제공하여 가장 광범위한 공격 환경에 업계에서 가장 포괄적인 첨단 위협 보호 포트폴리오 솔루션을 제공하는 업체 중 하나입니다. 보안에 대한 Cisco의 위협 중심, 조직적 접근 방식은 복잡성과 분산을 줄이는 동시에 공격 전후 및 중간에 뛰어난 가시성, 일관된 제어, 첨단 위협 보호를 제공합니다.

CSI(Collective Security Intelligence) 에코시스템의 위협 연구가들은 다양한 디바이스와 센서, 공개 및 비공개 피드, Cisco의 오픈 소스 커뮤니티에서 얻은 원격 분석 정보를 사용하여 업계 최고의 위협 정보를 하나로 결합했습니다. 이 정보의 양은 매일 수십억 건의 웹 요청, 수백만 개의 이메일, 악성코드 샘플, 네트워크 침입에 해당합니다.

Cisco의 정교한 인프라와 시스템은 이 원격 분석을 사용하여 머신-학습 시스템 및 연구가들이 네트워크, 데이터 센터, 엔드포인트, 모바일 디바이스, 가상 시스템, 웹, 이메일, 클라우드에서 위협 정보를 추적하여 근본 원인을 식별하고 사건 발생을 억제할 수 있도록 합니다. 여기서 얻은 정보는 Cisco 제품 및 서비스에 대한 실시간 보호로 변환되어 전 세계 Cisco 고객에게 즉시 전달됩니다.

CSI 에코시스템은 각각의 선언문을 가진 여러 그룹, 즉, Talos, Security & Trust Organization, MTD(Managed Threat Defense), SR&O(Security Research and Operations)로 구성되어 있습니다.

Cisco의 위협 중심 보안 접근법에 대한 자세한 내용은 www.cisco.com/go/security에서 확인하십시오.

부록

추가 보안 기능 벤치마크 조사 결과

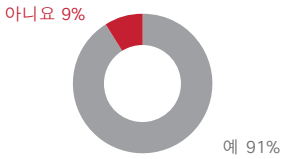
리소스

보안 예산이 IT 예산에 포함되어 있습니까? IT 부서 구성원; n=1720

보안 정책, 절차, 운영

가장 높은 순위로 평가된 보안 담당 경영진 대부분은 CISO 또는 CSO입니다.

여러분 회사에 보안을 전담하는 경영진이 있습니까?
역할과 책임을 밝힌 응답자 수, n=1603



경영진의 직책
보안 책임을 가진 경영진이 있다고 대답한 응답자 수, n=1465

의료 업종의 경우 다른 업종에 비해 보안 담당 경영진을 식별하는 비율이 낮았습니다.

보고서 공유

거의 3분의 2 이상의 응답자가 경영진이 보안을 최우선 순위로 생각한다고 대답했습니다.

경영진 참여 n=1738	보안 담당 중역 n=797			CISO n=941		
	반대/동의/전적으로 동의			반대/동의/전적으로 동의		
조직의 경영진이 보안을 높은 우선 순위로 고려한다	8%	34%	58%	3%	30%	67%
조직의 경영진에 보안 역할과 책임이 명확히 정의되어 있다	9%	39%	52%	2%	32%	64%
조직의 경영진이 보안 프로그램의 효율성 평가를 위한 명확한 메트릭을 보유하고 있다	11%	44%	45%	4%	37%	59%

조직의 보안 침해에 대한 공개 조사를 관리할 필요가 없다고 대답한 많은 응답자들이 "조직의 경영진이 보안을 높은 우선 순위로 고려한다"는 데 전적으로 동의했습니다.

직원 참여를 장려하는 보안 프로세스가 구현되어 있다고 응답한 비율이 높게 나타났습니다.

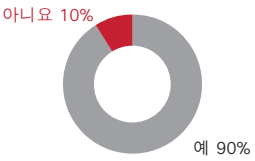
보안 프로세스 n=1738	보안 담당 중역 n=797			CISO n=941		
	반대/동의/전적으로 동의			반대/동의/전적으로 동의		
LOB(line-of-business) 관리자가 보안 정책 및 절차에 기여하도록 장려받는다	12%	39%	49%	6%	40%	54%
조직에서는 큰 사고가 되기 전에 보안 취약점을 탐지할 수 있다	13%	43%	44%	4%	39%	57%
조직의 직원은 보안 실패 및 문제를 보고하도록 장려 받는다	11%	34%	55%	4%	36%	60%
조직의 보안 프로세스 및 절차는 분명하며 이해하기 쉽다	13%	39%	48%	4%	37%	59%
조직의 보안 프로세스를 통해 잠재적 보안 문제를 사전 대응적으로 예상하고 줄일 수 있다	14%	40%	46%	3%	40%	47%
조직의 보안 프로세스는 정량적 데이터를 사용하여 측정 및 제어하고 있다	13%	40%	47%	4%	35%	61%
조직에서는 보안 프로세스를 최적화했으며 이제 프로세스 개선에 집중하고 있다	12%	42%	46%	4%	36%	60%

중견기업 조직의 보안 전문가는 엔터프라이즈 전문가에 비해 보안 프로세스 항목에 대해 더 크게 동의하는 경향을 보입니다.

응답자 10명 중 9명은 일반적으로 보안 팀에서 보안 직원에게 정기적 보안 교육을 제공하고 있다고 대답했습니다.

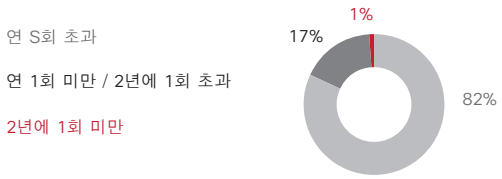
보안 직원에게 보안 인식 및/또는 교육 프로그램을 정기적으로 제공합니까?

보안 전담 응답자 수, n=1726



보안 교육을 얼마나 자주 제공합니까?

보안 전담 응답자 수, n=1556

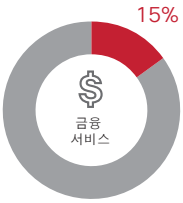


누가 보안 교육을 제공합니까?

보안 팀이 교육을 받은 응답자 수, n=1556

내부 보안 팀 79% | 서드파티 계약자 38% | 인사 담당 25% | 기타 직원 10% | 기타 1%

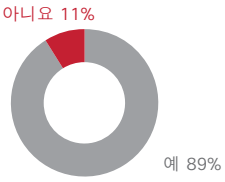
금융 서비스 전문가의 15%가 보안 교육을 정기적으로 제공하지 않는다고 대답했습니다.



직원이 일반적으로 컨퍼런스 또는 교육에 참가하며, 그중 약 3분의 2는 보안 업계 연합에 가입되어 있다고 대답했습니다.

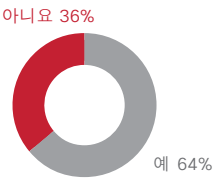
보안 직원이 기술의 유지 및 개선을 위해 회의 및/또는 외부 교육에 참석합니까?

보안 전담 응답자 수, n=1715



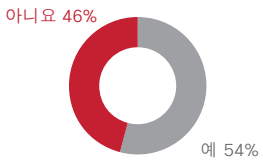
직원들이 보안 업종의 회의나 위원회에 등록되어 있습니까?

보안 전담 응답자 수, n=1690

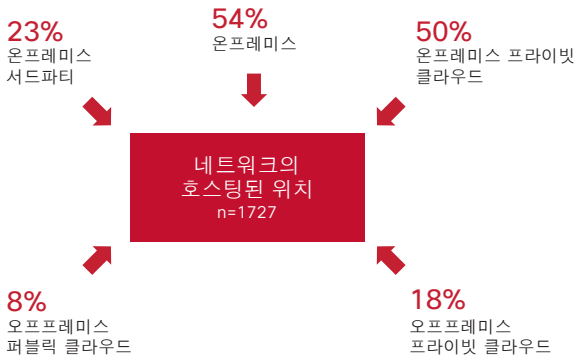


응답자의 절반 이상이 자신의 조직에서 보안 침해에 대한 공개 조사를 관리해야 한다고 대답했습니다.

여러분의 회사에서는 보안 침해에 대한 공개 조사를 관리해야 합니까?
보안 전담 응답자 수, n=1701



조직 네트워크를 온프레미스 호스팅하는 것이 가장 일반적이며 퍼블릭 클라우드에 호스팅한다고 대답한 응답자는 10% 미만입니다.



보안 담당 중역의 경우 조직에서 오프프레미스 호스팅(프라이빗 및 퍼블릭 클라우드)을 사용한다고 대답한 응답자 수가 CISO에 비해 훨씬 더 많았습니다.

수준

세그먼트는 보안 정교성 수단에 따라 다릅니다.

	낮음	중하	중간	중상	높음
회사 경영진이 보안을 높은 우선 순위로 고려한다	22%	38%	45%	71%	81%
… 보안 프로그램의 효율성 평가를 위한 명확한 메트릭을 보유하고 있다	17%	19%	32%	52%	79%
회사에서는 명확하게 이해되는 보안 프로세스/절차를 보유하고 있다	0%	22%	15%	72%	88%
… 정량적 데이터를 사용하여 측정 및 제어한다	0%	17%	33%	65%	76%
… 보안 사례와 툴을 정기적으로 검토하여 최신의 효율적인 상태로 유지한다	0%	17%	33%	65%	76%
회사에서는 전송 및 출발을 위한 효율적인 온보딩 프로세스를 통해 HR 보안을 탁월하게 관리한다	16%	27%	36%	52%	76%
보안 자산을 인벤토리로 보관하고 명확히 분류하고 있다	17%	26%	40%	58%	73%
조직 내 컴퓨터 설비가 효과적으로 보호되고 있다	17%	21%	41%	63%	80%
보안 기술이 원활히 통합되어 상호 효과적으로 작동한다	17%	21%	38%	59%	78%
…회사에서 인시던트로 완전히 이어지기 전에 보안 약점을 탐지할 수 있다	0%	23%	25%	63%	70%

하지만 모두 그런 것은 아닙니다.

	낮음	중하	중간	중상	높음
보안을 전담하는 경영진이 있다	85%	91%	88%	93%	93%
회사에서는 전사적 보안 전략을 서면으로 공식화하여 정기적으로 검토하고 있다	59%	47%	58%	65%	60%
회사에서는 ISO 27001과 같은 표준화된 정보 보안 정책 관행을 따른다	47%	44%	50%	59%	54%

미주

1. *Cisco 2014 중기 보안 보고서:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
2. CMS 취약점에 대한 자세한 내용은 *Cisco 2014 중기 보안 보고서:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027 "Wordpress 취약점: 누가 저장소를 염려하는가?" 를 참조하십시오.
3. "Goon/Infinity/RIG Exploit Kit Activity", Cisco IntelliShield: Security Activity Bulletin, 2014년 7월: http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999.
4. *Cisco 2014 중기 보안 보고서:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
5. "Cisco Event Response: POODLE Vulnerability," 2014년 10월 15일: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html.
6. "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations," Cisco Security Blog, 2014년 4월 9일: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations
7. "JP Morgan and Other Banks Struck by Hackers," by Nicole Perlroth, *The New York Times,* 2014년 8월 27일: http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0; "'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011," by Jack Cloherty, Pierre Thomas, ABC News, 2014년 11월 6일: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.
8. "4 Things We Learned from China's 4th Plenum," by Shannon Tiezzi, *The Diplomat,* 2014년 10월 23일: http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/.
9. "Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices," *Chronicle of Data Protection,* 2014년 5월 16일: http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/.
10. "Russian data localization law may now come into force one year ahead of schedule, in September 2015," by Hogan Lovells, Natalia Gulyaeva, Maria Sedykh, Bret S. Cohen, Lexology.com, 2014년 12월 18일: http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e.
11. "GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice,'" by Ben Quinn, James Ball, Dominic Rushe, *The Guardian,* 2014년 11월 3일: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.
12. "Internet Security Necessary for Global Technology Economy," by Mark Chandler, Cisco Blog, 2014년 5월 13일: http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy.
13. "Cybersecurity: What the Board of Directors Needs to Ask," ISACA and The Institute of Internal Auditors Research Foundation, 2014년 8월: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.
14. "It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why," by Andrew Nusca, FORTUNE magazine, 2014년 4월 25일: http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/.

Americas Headquarters
Cisco Systems Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트www.cisco.com/go/offices에서 확인하십시오.

© 2014 Cisco 및/또는 자회사. 모든 권한은 당사에 있습니다. 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)