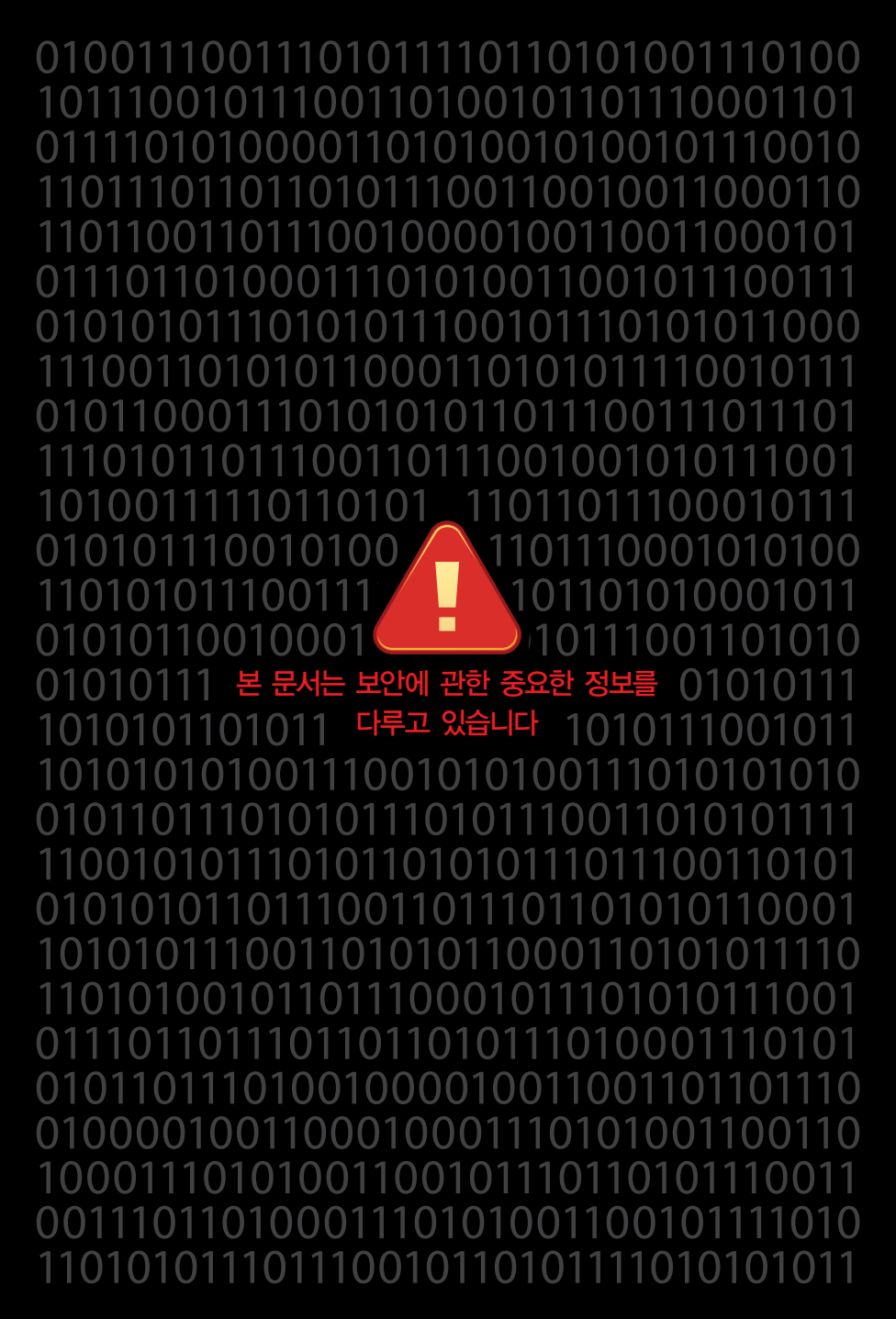
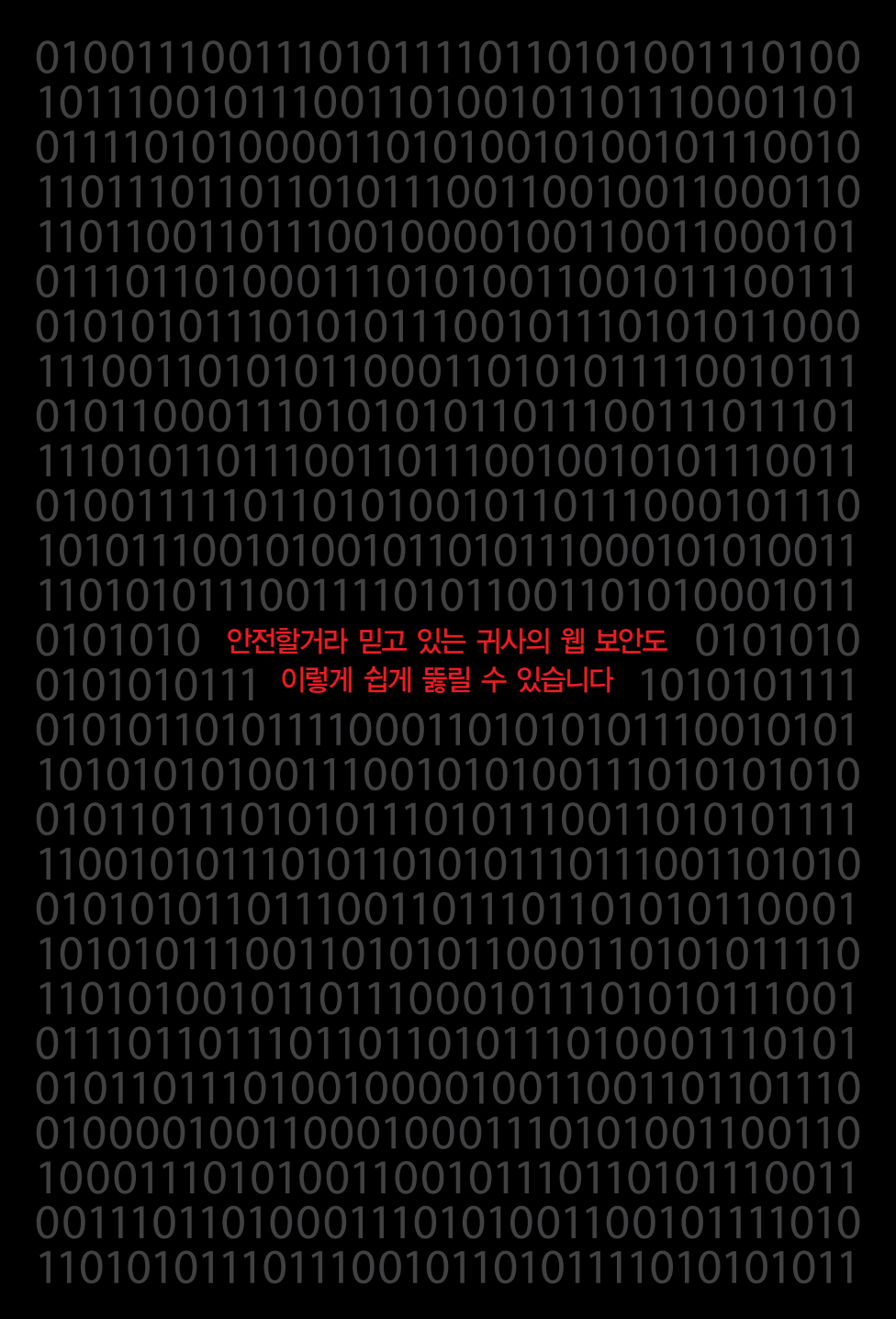
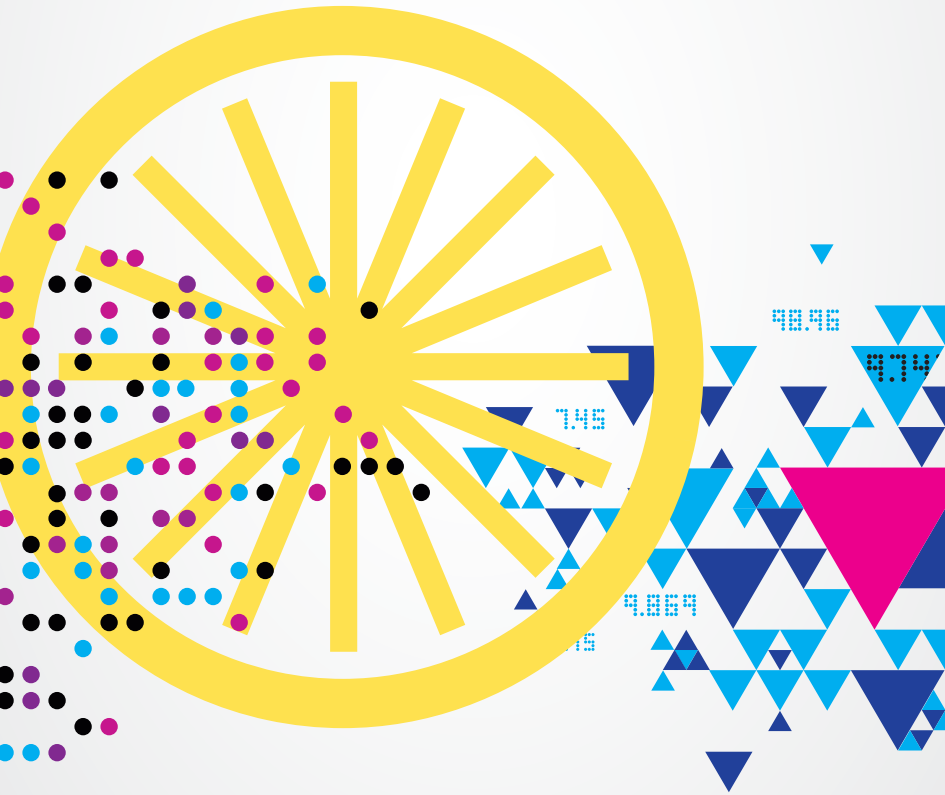

본 문서는 보안에 관한 중요한 정보를
다루고 있습니다


안전할거라 믿고 있는 귀사의 웹 보안도
이렇게 쉽게 뚫릴 수 있습니다

단계적인 구성으로 더욱 강력한 웹 보안 솔루션!

IBM Rational AppScan



웹사이트 보안이 뚫리면
고객의 신뢰는 무너집니다

대부분의 웹사이트는 고객의 매우 중요한 정보를 다루고 있기 때문에 정보가 노출될 경우, 고객은 물론 그 기업에게 상상 이상의 피해가 발생할 수 있습니다. 실제로 수 많은 웹사이트들이 해커들에게 공격받고 있고, 그로 인한 피해는 단순하게 금전적으로 수치화 할 수 있는 것이 아니었습니다. 웹사이트의 매출 감소는 물론, 신용손상, 법적인 책임 및 배상, 고객의 신뢰 상실로 이어져 기업의 위기를 초래하고 있습니다.

금융감독원, 2010년부터 정보보호 의무 강화

금융권의 사이버테러 대응시스템 등 정보보호 의무가 강화된다. 이를 위해 전문인력과 예산확보 등에 대한 기준이 마련되는 등 금융권의 보안분야가 크게 확대될 것으로 전망된다.

9일 금융감독원 산하 금융정보보호협의회는 이 같은 내용을 골자로 은행·증권사·보험사·카드사 등 92개 금융회사의 정보보호전문가와 함께 서울 가든호텔에서 정보보호 거버넌스 개선에 대한 논의를 가졌다.

이 자리에서는 사이버테러 대응시스템 도입과 24시간 모니터링 체계 구축, 정기적인 모의훈련 실시 등의 기술적 대응을 의무화하는 방안과 최고정보보호책임자(CSO) 임명, 정보보호 전문인력과 예산을 전체 IT부문의 5% 이상 확보하도록 하는 등 정보보호 관리체계를 큰 폭으로 개선하는 내용을 다뤘다.

금감원은 이 같은 IT감독정책의 실효성을 확보하기 위해 종합검사 시 IT부문 경영실태평가를 실시하고 사이버테러 대응 역량을 중점 검사해 감독기준의 이행여부를 점검할 예정이다.

-ITDAILY-

웹은 누구에게나 열려있기 때문에
그 만큼 보안의 취약점도 많이 존재합니다

국정원의 발표에 따르면, 대부분 홈페이지 해킹사고는 개발 또는 운영 중에 보안 사항을 소홀히 한 것에서 비롯된다고 합니다. 많은 개발자가 보안관련 중요도 인식과 전문성이 부족하여 보안을 고려한 코딩을 하지 않고 있고, 홈페이지 운영자 또한 콘텐츠 관리 같은 서비스에만 치중하는 등 보안관리를 소홀히 하고 있기 때문에 그 피해 사례는 매년 증가하고 있습니다.

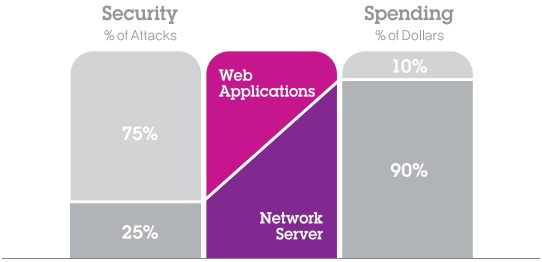
구분	통계 요약
해킹 신고처리	총 1,285건 – 전월(1,119건) 대비 14.8% 증가
•스팸 릴레이	599건 – 전월(495건) 대비 21.0% 증가
•피싱 경유지	86건 – 전월(72건) 대비 19.4% 증가
•단순 침입시도	219건 – 전월(230건) 대비 4.8% 증가
•기타 해킹	291건 – 전월(225건) 대비 29.3% 증가
•홈페이지 변조	90건 – 전월(97건) 대비 7.2% 증가

※출처 : 인터넷 침해사고 대응센터 2009년 3월 집계

웹은 기본적으로 모든 사용자의 접근을 허용하고 있으므로 그에 상응하는 만큼의 공격에 노출되어 있다고 보아야 합니다. 요즘 웹 해킹 추세는 금전적 이득을 목적으로 하는 공격이 크게 증가하고 있으며, 공격 또한 무차별적이라는 특징을 보이고 있습니다. 따라서, 웹 사이트의 취약점을 파악하고 사전에 대비하는 것이 가장 중요합니다.

웹 애플리케이션을 통한 해킹은 늘고 있지만, 이를 방어하기 위한 투자는 부족한 수준입니다

최근 난무하는 악성 소프트웨어, DDoS 사태와 같이 해커들의 공격 75%가 웹 응용프로그램을 통해 발생하고 있습니다. IBM 연구팀의 연구결과에 따르면 기업의 웹사이트 80%가 취약성을 가지고 있는 것으로 보고되었으나, 이에 반해 기업의 투자는 10% 미만에 그치고 있는 실정입니다. 과연 현재의 보안 수준으로 각종 보안장비나 대응방안을 무력화 시키기 위해 보다 지능화된 형태로 발전하고 있는 웹 해킹 공격을 방어할 수 있을까요?



"기업에 널리 보급돼 있는 웹 애플리케이션이 심각한 보안 위협에 노출돼 있으며, 웹 애플리케이션의 취약점 중 82% 이상이 쉽게 악용될 수 있다."

–Symantec–

"최근 발생하고 있는 보안 사고의 70% 이상이 웹 애플리케이션의 취약점을 이용해 해킹을 시도한 것이다."

–Gartner–

사전예방만이 피해·복구에 소요되는 비용과 노력을 줄이는 최선의 방법입니다

우리는 지금까지 웹 해킹에 대한 방어에만 급급했습니다. 이제는 사전예방을 위한 조치가 필요한 때입니다. 피해가 발생한 후 복구하는 비용은 기업의 생존을 위협할 수도 있습니다. 보안성이 강화된 안전한 웹 응용프로그램을 개발하고, 시스템의 분석, 설계 단계부터 이행단계에 이르기까지 보안요소를 고려한 개발이 필요합니다.

연구 결과에 따르면, 문제가 발견되는 시점에 따라 수정하는데 드는 비용은 차이를 보입니다. 특히, 비용 효과적인 측면을 고려하면, 추후 Add-On 형태의 정보보호 고려 보다는 Embedded 방식의 정보보호 반영이 효과적이고 안전합니다. 이미 미국은 국방부를 중심으로 제도화하고, OECD 정보보호 가이드라인을 통한 설계와 구현을 권고하고 있습니다.

에러 유형	단계				
	디자인	코딩	통합	베타 테스트	배포
디자인	1X	5X	10X	15X	30X
코딩		1X	10X	20X	30X
통합			1X	10X	20X

※출처 : IBM 연구 결과(Science Institute)

취약성을 없애는 것은 빠를수록 좋습니다
웹 응용프로그램 개발자가 첫 번째 방어선입니다

외부와 통신을 위해 최소한의 방화벽이라도 열려있다면, 방화벽 등 장비에 의존하는 웹 보안은 취약할 수 밖에 없습니다. 따라서, 공격에 맞서는 첫 번째 방어선은 응용프로그램을 직접 만드는 **'개발자'**여야 합니다. 문제를 누구보다 더 잘 이해하고, 신속하게 문제를 수정할 수 있고, 무엇보다 가장 효과적이고 비용효율적이기 때문입니다.

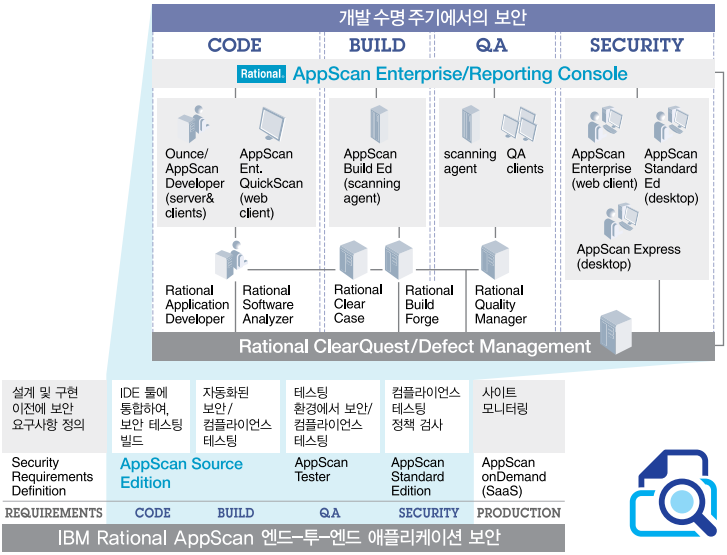
그리고 보안전문가는 가능한 한 빨리 개발수명주기 단계에 참여해 응용프로그램이 얼마나 중요한 정보를 다루고 있는지, 또 이 프로그램을 이용하는 고객의 성향은 어떠한지 미리 파악하는 것이 중요합니다. 품질전문가도 보안 취약성을 기능적인 버그와 동일하게 인식하여 테스트 단계에 임하여야 합니다. 관리자는 프로젝트 주기 내 보안에 관련된 계획을 세우고, 보안을 강화하는 것이 애플리케이션의 가치를 높이는 것입니다.

웹 보안 유형과 그 한계

유형	한계
F/W(방화벽)	80 포트를 막으면 서비스가 중단되므로 웹 애플리케이션 보안에 한계
IDS(침입탐지)	오탐의 문제가 있을 수 있고, 탐지는 가능하나 차단 불가능
IPS(침입방지)	암호화 네트워크 하에서의 잘못된 정보유입/응용프로그램 코드 자체의 취약성에 대한 보호 불가능, 이미 알려진 형태의 공격에 대한 방어만 가능
서버 보안(Secure OS)	계정/권한관리가 주 목적으로 침입방지 기능구현은 제한적
WAF(웹 애플리케이션 방화벽)	알려진 공격유형 패턴에 따른 방어만으로는 다양한 형태로 변종이 발생하는 공격에 대해 근본적인 대처 불가능

IBM Rational AppScan으로
보안 걱정 없이 비즈니스에 집중하십시오

웹 애플리케이션 보안 솔루션 1위, IBM의 Rational AppScan은 코드레벨의 보안을 강화하기 위해 코드레벨 보안 솔루션 선두 기업인 Ounce Labs를 인수하였습니다. 이제 소프트웨어 개발부터 운영, 인프라단까지 단계적으로 관리하는 가장 완벽한 웹 애플리케이션 보안 솔루션, **IBM Rational AppScan**으로 안심하고 비즈니스 하십시오.



귀사의 웹사이트 보안,
이제 코드부터 모듈 레벨까지 완벽하게!
IBM Rational AppScan이 지켜 드리겠습니다!

지금 바로 연락주십시오.

한국IBM 마케팅총괄본부
Call 02-3781-7800
Fax 02-3781-6364
Email mktg@kr.ibm.com

KR0BP01D