2016. 03. 10 v1.0.0

기업 보안의 핵심은 '패치 관리', 왜?

AhnLab Patch Management

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

기업 보안의 핵심은 '패치 관리', 왜?

최근 청와대를 사칭해 다수의 공공기관 관계자들에게 악성 한글 파일을 첨부한 메일이 유포된 사실이 알려져 적지 않은 파장을 야기했다. 얼마 전에는 모 설계용역 회사의 업무 시스템에 매크로 취약점을 이용한 악성 엑셀 파일이 유입된 일도 있다. 이처럼 공공기관뿐만 아니라 금융 및 일반 기업에서 소프트웨어의 취약점을 이용한 보안 침해 사고가 지속적으로 발생하고 있다. 문제는 알려지지 않은 새로운 취약점, 즉 제로데이(Zero-day) 취약점을 이용한 공격뿐만 아니라 이미 수년 전에 발견되어 보안 패치까지 제공된 알려진 취약점을 이용한 공격이 상당한 비율을 차지한다는 점이다. 수많은 보안 전문가들의 권고에도 불구하고 여전히 보안 패치 적용에 소홀하고 패치 관리가 미흡하다는 방증이다. 여러 정보보호 관련 규제에도 불구하고 패치 관리가 미비한 이유는 무엇일까?

이 글에서는 여러 정보보호 관련 규제에도 불구하고 기업 및 기관의 패치 관리가 어려운 이유를 살펴보고 실질적이고 효율적인 패치 관리 방안에는 무엇이 있는지 알아본다.

마이크로소프트(Microsoft, 이하 MS)가 지난 1월 12일을 기점으로 구버전 인터넷 익스플로러(Internet Explorer, 이하 IE)에 대한 기술 지원 및 보안 업데이트를 중단함에 따라 기관 및 기업이 상당한 부담을 느끼고 있다. 일부 공공기관 및 기업의 대고객 서비스를 위한 웹사이트가 구버전의 IE 환경에 최적화되어 있으며, 상당수 기업에서는 인트라넷 등 업무 프로그램과의 호환성을 이유로 구버전의 IE를 사용하고 있기 때문이다. 최근 미래창조과학부가 발표한 '2015년 하반기 국내 인터넷 이용환경 현황조사'에 따르면 국내 기업에서 구버전 IE를 사용하는 비율은 약 50.34%로, 절반 이상의 기업에서 구버전 IE를 이용하는 것으로 나타났다.

더 이상 보안 업데이트가 지원되지 않는 구버전 IE를 계속 사용한다는 것은 심각한 보안 위협에 노출될 가능성이 높아진다는 의미다. 대부분의 악성코드가 소프트웨어의 취약점을 이용하고 있기 때문이다. 악성코드가 악용하는 소프트웨어 취약점은 IE에 한정된 것은 아니다. 공격자들은 윈도우(Windows) 등 주요 OS와 MS 오피스, 어도비 플래시 플레이어(Adobe Flash Player), 자바(Java) 등 많은 사용자들이 이용하는 소프트웨어의 취약점도 악용하고 있다. 특히 어도비 플래시와 자바의 경우, 현재 대부분의 웹사이트가 이들을 기반으로 하고 있어 공격자들이 집요하게 파고든다. 국내에서는 한글 프로그램의 취약점을 이용한 악성코드 유포도 지속적으로 이루어지고 있다. 이 외에도 최근 공공 기관 및 기업의 클라우드 및 가상화 도입이 증가함에 따라 베놈(VENOM) 취약점(CVE-2015-3456), VM웨어 워크스테이션 취약점(CVE-2015-2336) 등도 발견됐다.

알려진 취약점을 이용한 공격은 언제나 유효하다, 왜?

한국인터넷진흥원(KISA)이 최근 발표한 '악성코드 은닉 사이트 탐지 동향 보고서'를 살펴보면 현재 유포되고 있는 악성코드들은 최신 취약점이 아닌 이전의 취약점을 이용하는 경우가 더 많다는 것을 알 수 있다. [표 1]은 지난 2015년 12월 한 달간 유포된 악성코드가 이용한 주요 취약점으로, 2015년 이전에 발견된 취약점이 대부분이며 심지어 6~7년 전에 발견된 취약점까지 여전히 이용되고 있다.

소프트웨어	취약점	소프트웨어	취약점
인터넷 익스플로러 (Internet Explorer)	CVE-2010-0249	어도비 플래시 플레이어 (Adobe Flash Player)	CVE-2010-2884
	CVE-2010-0806		CVE-2011-0611
	CVE-2010-0249		CVE-2011-2140
	CVE-2011-1255		CVE-2012-0754
	CVE-2012-4792		CVE-2012-1535
	CVE-2012-4969		CVE-2013-0634
	CVE-2013-1347		CVE-2014-0515
	CVE-2013-2551		CVE-2014-0556
	CVE-2013-3893		CVE-2014-0569
	CVE-2013-3897		CVE-2014-8439
	CVE-2014-0322		CVE-2015-0311
	CVE-2012-1875		CVE-2015-0313
	CVE-2008-2551		CVE-2015-3043
	CVE-2008-0015		CVE-2015-0336
	CVE-2015-2419		CVE-2015-3113
자바 애플릿 (Java applet)	CVE-2011-3544		CVE-2015-3133
	CVE-2012-0507		CVE-2015-5119
	CVE-2012-1723	MS OLE	CVE-2014-6332
	CVE-2012-4681	MS Windows Media	CVE-2012-0003
	CVE-2012-5076	Adobe reader (PDF)	CVE-2010-0188
	CVE-2013-0422	MS XML	CVE-2012-1889
	CVE-2013-1493	MS Silverlight	CVE-2013-0074
	CVE-2013-2423		
	CVE-2013-2460		
	CVE-2013-2465		

[표 1] 2015년 12월 악성코드 취약점 악용 현황 (*출처: 한국인터넷진흥원)

공격자들이 최신 취약점이 아닌 패치까지 배포된 오래된 취약점을 이용하는 이유는 무엇일까? 우선 공격자 입장에서도 새로운 취약점을 발견하는 게 쉬운 일은 아닐 것이다. 알려진 취약점을 이용해 악성코드를 자동으로 생성하는 공격 툴을 암시장에서 쉽게 구할 수 있다는 점도 공격자들에게 매력적인 부분이다. 결국 새로운 취약점을 찾아내기 위해 시간과 노력을 들이기 보다는 이미 알려진 취약점을 이용하는 것이 가성비 대비 효과가 훨씬 좋다는 의미다.

게다가 알려진 취약점에 대한 패치가 배포되었더라도 전세계 모든 사용자가 동시에 패치를 적용한다는 것은 현실적으로 불가능하다. 소프트웨어 업체들은 취약점을 최소화하는 한편 취약점의 신속한 제거를 위해 주기적으로 보안 패치를 배포하는 등 사용자 보호를 위해 노력하고 있다. 문제는 패치의 배포 속도와 실제 사용자들이 패치를 적용하는 속도에 상당한 차이가 존재한다는 점이다. 취약점을 악용한 공격은 빠르게 증가하고 있는데 보안 패치를 적용하는 속도는 상대적으로 느리다 보니 취약점이 누적되어 위협에 노출되는 범위도 확대된다.

기업의 경우에는 전사에 보안 패치를 적용하는 것부터 쉽지 않다. 임직원들이 사용 중인 소프트웨어도 다양할 뿐만 아니라 사용 중인 버전도 제각각인 경우가 많아 이를 보안 관리자가 일일이 확인하고 최신 패치를 적용하도록 강제하는 것은 사실상 불가능에 가깝다. 게다가 기업에서 자체적인 업무용 프로그램을 사용하는 경우, 상용 소프트웨어에 최신 보안 패치를 적용했을 때 프로그램간의 호환성 및 충돌 등의 문제가 발생할 수 있다. 그리고 공격자들은 이러한 상황과 오래된 취약점을 이용하는 공격이 여전히 유효하다는 것을 잘 알고 있다.

컴플라이언스 강화로 PMS 도입 늘어...실제 효과는?

패치가 적용되지 않은 시스템을 노린 알려진 취약점을 이용한 공격이 지속적으로 발생함에 따라 개인정보보호법 등을 비롯한 다수의 정보 보안 관련 규제들이 패치 관리 또는 패치 관리 시스템(Patch Management System, 이하 PMS) 도입을 강제화하는 추세다. 최근에는 은행뿐만 아니라 보험, 카드사를 중심으로 망분리 환경에도 PMS를 도입하는 움직임이 확대되고 있다.

관련 규제	내용 요약
개인정보보호법 (행정자치부고시, 개인정보의 안전성 확보조치 기준)	<제8조, 악성프로그램 등 방지> 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시
전자금융 안전성 제고를 위한 금융전산 보안 강화 종합대책 (금융위원회)	내부 업무용 시스템 인터넷 접속 차단 • 내부망에 설치된 패치 관리, 그룹웨어 등 내부 업무용 시스템은 원칙적으로 외부 인터넷 접속을 차단 - 업데이트용 패치 파일 등 외부에서 파일 전송이 필요한 경우, 관리자가 수동으로 다운로드하고 무결성 검증 및 확인 후 적용
요양기관 개인정보보호 자율점검 (행정자치부, 건강보험심사평가원)	< 제29조 안전조치의무> • 개인정보처리시스템에 백신 프로그램 등 최신의 보안 프로그램을 설치하여 관리 • 보안 프로그램을 정기적(일 1회이상)으로 업데이트

[표 2] 주요 정보보호 관련 규제 중 패치 관리에 관한 규정

그러나 기업 및 기관의 규모, 비즈니스 특성, IT 인프라 등 PMS 도입에 앞서 고려해야 할 사항이 적지 않다. 은행 등 금융 기관에서는 폐쇄망 환경에서의 오프라인 패치 지원 및 패치 검증 지원 여부 등도 꼼꼼히 따져봐야 한다. 지난 2013년 발표된 '금융전산 보안 강화 종합대책'에서는 업데이트용 패치 파일의 경우 무결성을 검증 및 확인 후 적용하도록

규정하고 있기 때문이다. 또한 다수의 지점을 운영해야 하는 경우, 전 지점망으로 패치 적용 시 네트워크 과부하가 발생할 가능성 등도 필수 고려 사항이다.

한편 보안 관리자 입장에서는 관리해야 할 패치의 종류와 범위도 다양해 이를 파악하기도 쉽지 않을 뿐더러 기존에 도입된 다수의 보안 솔루션에 PMS까지 추가되면서 업무 부담이 늘어나기 때문에 컴플라이언스 준수를 위해 '관리를 위한 관리만 하는 꼴'이라는 불만도 적지 않다.

안랩 패치 매니지먼트가 주목받는 이유는?

보안 및 소프트웨어 패치 관리 솔루션인 '안랩 패치 매니지먼트(AhnLab Patch Management, APM)'는 기업 내 PC의 각종 소프트웨어 패치를 실시간으로 중앙에서 관리할 수 있을 뿐만 아니라 보안 정책에 위배되는 PC에 대한 인터넷 접근 차단 등의 조치가 가능해 사용자들의 적극적인 참여를 유도할 수 있다. 특히 ▲국정원 권고 패치 자동 적용 ▲네트워크 대역폭(QoS) 설정 기능 ▲패치랩 및 테스트 그룹 기능 등을 통한 안정적인 패치 제공 등에 고객 만족도가 높다.

[그림 1] 안랩 패치 매니지먼트 관리자 화면

1. 국정원 권고 패치 자동 적용

한글, 어도비 등 국정원 권고 패치를 제공할 뿐만 아니라 이를 검증하고 자동으로 적용할 수 있도록 지원한다. 핵심은 국정원 권고 패치 제공이 아니라 이들 패치를 적용하는 방식이 '자동화'되어있다는 점이다. PMS 제품 중에는 일부 프로그램의 경우 메일이나 오프라인 방식으로 패치를 전달해 보안 관리자가 서버에 올리거나 공유 폴더를 통해 사내 배포를 하는 등 일정 수준 이상의 관리자의 조작이 요구되는 경우가 있다. 이에 반해 안랩은 AST 서버를 통해 고객사의 APM 서버로 패치 파일을 자동으로 전달하며 이 APM 서버를 통해 사내 시스템에 패치를 자동으로 업데이트할 수 있다. 특히 한글 프로그램 패치와 관련해 타 PMS 제품은 한글 패치를 강제 업데이트나 검증이 이루어지지 않는 반면 안랩 패치 매니지먼트는 서버를 통해 강제로 에이전트 시스템에 내릴 수 있다. 또한 안랩은 실제 사용자들의 불편을 최소화하기 위해 한글 패치에 대한 '사일런트 패치(Silent Patch)' 기능을 연내 제공할 예정이다. 이 기능을 이용할 경우, 신규 한글 패치 발생 시 사용자에게 알림창이 보여지는 것이 아니라 백그라운드에서 자동으로 업데이트되기 때문에 사용자의 별도 조작이 필요 없게 된다. 즉, 사용자 편의성은 높이고 한글 패치를 강제로 적용할 수 있어 한글 프로그램을 주로 사용하는 공공기관에 더욱 유용하게 활용될 전망이다.

2. 네트워크 대역폭 설정 기능을 통한 QoS 보장

안랩 패치 매니지먼트의 '네트워크 대역폭 설정' 기능은 특히 은행 등 금융권에서 각광받고 있다. 네트워크 대역폭 설정 기능이란 말 그대로 패치 적용 시 사용할 네트워크 대역폭을 설정하는 QoS(Quality of Service) 기능으로, 기업의 환경에 따라 패치 적용을 위한 대역폭 조정이 가능해 패치 적용 시 네트워크 과부하를 방지한다.

은행들이 전국에 걸쳐 운영하고 있는 수 천대의 ATM 기기들도 패치 관리의 대상이다. 문제는 ATM 기기가 사용하는 네트워크 대역폭이 작아 모든 ATM 기기에 패치를 한 번에 내리면 네트워크 장애가 발생 가능성 높다는 점이다. 안랩 패치 메니지먼트는 네트워크 대역폭을 초당 기본 200KB, 필요에 따라 초당 100 ~ 1024KB 범위로 설정할 수 있어 업무망을 안정적으로 유지하면서 패치 적용이 가능하다. 네트워크 대역폭 설정 기능은 주로 은행권에서 사용되고 있지만 지점망을 갖고 있는 곳이라면 모두 활용할 수 있다.

3. 패치랩 및 테스트 그룹 기능을 통한 안정성

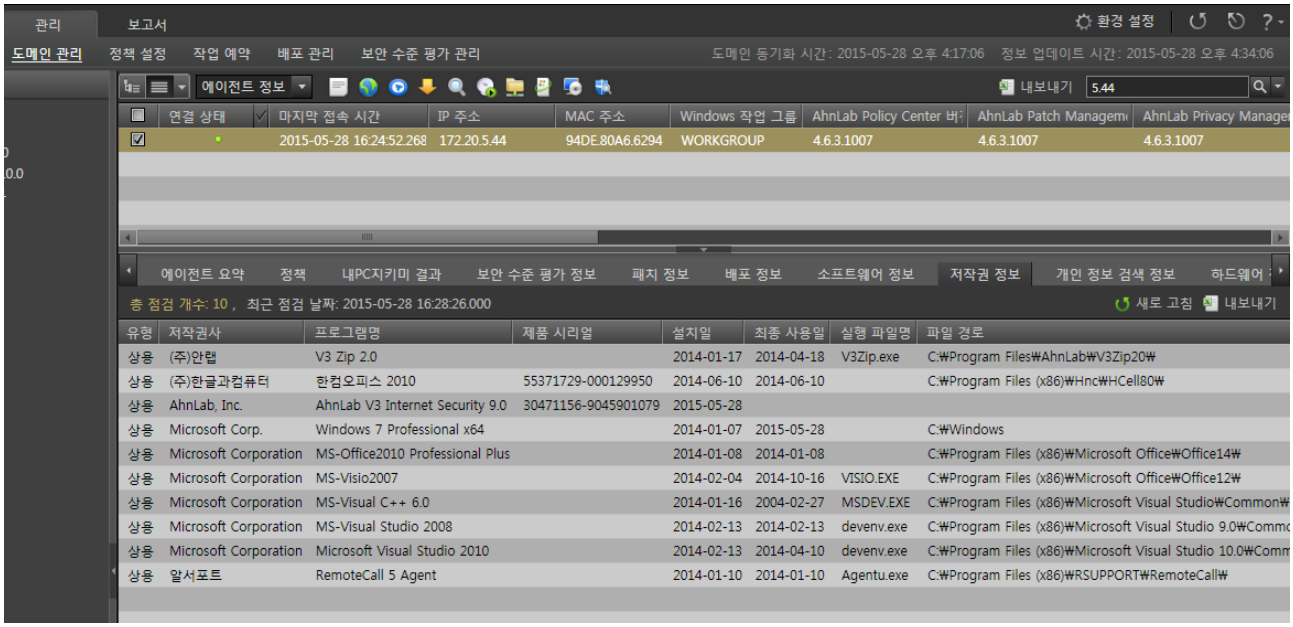
안랩은 전문 인력을 기반으로 한 자체 패치랩을 통해 패치 검증을 수행한다. 패치 검증이란 MS 오피스 등 상용 프로그램의 최신 패치와 ERP 시스템, 사내 메신저 등 고객사에서 사용하는 주요 애플리케이션과의 호환성을 사전에 확인하는 것으로, 프로그램 충돌로 인한 장애를 방지하는데 있어 매우 중요한 절차다. 안랩의 패치랩은 별도의 전담 인력으로 운영되고 있어 탁월한 안정성을 제공한다.

또한 '테스트 그룹' 설정을 통해 업무 중요도나 민감도에 따라 부서 또는 팀 단위, 또는 적용 시간대 단위로 순차 적용 및 차등 적용이 가능하다. 일부 기업의 경우 사내에서 사용 중인 그룹웨어 호환성 문제 등을 우려해 즉각적인 최신 패치 적용을 부담스러워하는 경우가 있다. 이때 안랩 패치 매니지먼트의 테스트 그룹 설정 기능을 통해 최신 패치를 순차적으로 적용함으로써 시스템 및 업무 장애 등을 미연에 방지할 수 있다.

SW 저작권 점검까지, 패치 관리 그 이상의 '가치'

안랩 패치 매니지먼트가 각광받는 이유는 탁월한 패치 관리의 안정성과 편의성 때문만이 아니다. 공공기관 및 대기업에서는 사내 소프트웨어(이하 SW) 라이선스 수량 점검에도 안랩 패치 매니지먼트가 적극 활용되고 있다.

현재 한국저작권위원회는 SW 저작권 점검을 강력하게 권고하고 있다. 최근 주요 소프트웨어 제공사들이 라이선스 관리를 강화함에 따라 계약 위반 사례에 따른 분쟁이 증가하고 있다는 점이 큰 영향을 끼친 것으로 보인다. 공공기관의 경우 SW 저작권 점검이 법적으로 강제되어 있으며 그 결과가 대통령에까지 보고된다. 일반 기업의 경우 강제 규정은 없으나 소프트웨어 라이선스 사용 위반이 확인될 경우 상당한 금액의 위약금이 발생할 수 있다. 실제로 얼마 전 모 항공사에서는 문서 작성 프로그램의 라이선스를 구매한 수량보다 초과하여 사용 중인 것을 미처 확인하지 못 해 수백만 원에 달하는 벌금을 물기도 했다.



[그림 2] 소프트웨어 저작권 점검 관리 화면

안랩 패치 매니지먼트는 한국저작권위원회의 점검 항목을 기준으로 소프트웨어 현황을 점검하고 관리한다. 별도의 에이전트 프로그램을 설치할 필요 없이 안랩 패치 매니지먼트의 'SW 저작권 관리 점검' 기능을 이용해 각 PC에서 사용 중인 소프트웨어 현황을 손쉽게 파악할 수 있다.

또한 금지 소프트웨어가 설치된 PC의 인터넷 사용을 제한할 수도 있어 적극적인 사용자 참여를 유도할 수 있다. 이 밖에도 기업에서 권장하는 소프트웨어를 자동으로 배포하고 다각도로 사용자의 참여 및 설치 유도가 가능하다는 점도 장점이다.

통합 콘솔로 보안 관리자의 운영 부담도 적어

V3를 비롯해 개인정보보호 솔루션인 '안랩 프라이버시 매니지먼트 스위트(AhnLab Privacy Management Suite)', PC 취약점 점검 및 자동 조치 솔루션 '안랩 내PC지키미' 등과 연동을 통해 통합적인 엔드포인트 보안 관리가 가능하다. 특히 이들 솔루션을 하나의 통합 콘솔을 통해 중앙에서 사내 보안 현황을 한눈에 파악하고 효율적으로 관리할 수 있다는 점이 가장 큰 매력이다. 이 외에도 안랩의 지속적이고 안정적인 서비스로 안전한 비즈니스 운영이 가능하다는 점도 다양한 산업군에서 안랩 패치 매니지먼트를 찾는 이유다.

