2016. 03. 10 v1.0.0

대림대학교,
안랩 제품으로 보안 철옹성 구축

Case Study

AhnLab

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

대학 내 서버와 PC들이 악성코드 유포지로 악용되는 사례가 늘고 있다. 특히 입시철이나 수강신청 시즌에 대학 사이트의 접속자가 증가하는 점을 노려 수많은 좀비PC를 양산해 내는 것이다. 문제는 하위 도메인이 많은 대학의 특성상 하위 도메인에서 악성코드가 유포되는 걸 탐지하기란 결코 쉽지 않다는 점이다. 실제로 모 대학의 경우 웹사이트가 해킹돼 좀비PC를 통해 7주 연속 악성코드가 유포되기도 했다. 이처럼 보안의 사각지대에 있는 대학 내 PC들은 공격자들에게 최고의 먹잇감인 셈이다. 그러나 이를 사전에 철저히 예방하고 있는 대학이 있어 눈길을 끈다. 대림대학교에 구축된 엔드포인트 보안 통합 관리 플랫폼은 가히 보안의 철옹성이라고 해도 과언이 아니다. 대림대학교의 보안 시스템 구현 사례를 들여다 본다.

대학, '보안의 사각지대' 오명 벗어라!

국내의 대학들이 보안의 사각지대로 불리는 이유는 무엇일까. 대학 캠퍼스는 누구나 출입이 자유로울 뿐만 아니라 PC들이 일반인들에게 쉽게 노출될 수밖에 없다는 게 가장 큰 이유이다. 또한 대학 임직원들의 낮은 보안 인식으로 인해 정보보호 분야에 예산과 인력이 투입되어야 함에도 불구하고 대부분의 사립대학들은 서버나 네트워크 같은 외형만 치중했지 보안은 '나중의 일'로 제쳐두는 게 또 다른 이유로 꼽힌다. 이 같은 이유로 인해 대학 등 교육기관에서 2012년부터 지난해까지 이름이나 주민번호 등 개인정보가 노출된 건수가 20만 건이 넘은 것으로 교육부 조사결과 밝혀졌다. 특히 사립대학의 경우 46개교에서 13만 건이 넘는 개인정보가 노출된 것으로 나타났다.
대림대학교의 보안 구축사례는 이런 의미에서 더욱 눈 여겨볼 필요가 있다. 대림대학교의 전체 시스템 관리를 총괄하고 있는 정보전략운영팀 이후재 코디네이터는 "우리 학교는 총장님부터 교수님, 직원과 학생들까지 보안규정을 잘 준수해 주고 있다. 그 결과 어느 대학보다 높은 보안 수준을 유지하고 있다고 자부한다"고 말했다.

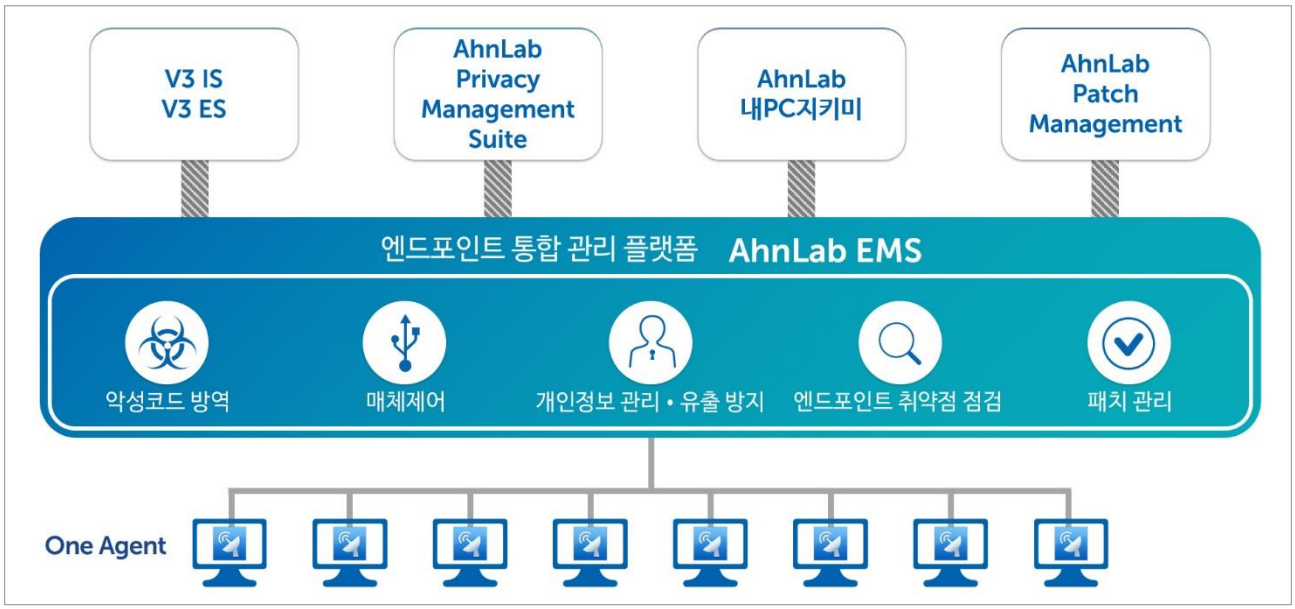
코디네이터라는 낯선 직함에 고개를 갸우뚱하는 분들이 있을 것이다. "왜 코디네이터냐"라는 물음에 "대림대학교의 전체 IT시스템 관리를 책임지고 있는 정보전략운영팀은 지식정보원 원장님 아래 저와 수행사 직원들로 이루어져 있다. 총 11명의 상주직원이 유지보수를 비롯한 정보시스템 통합 운영을 맡고 있는데 현업과 수행사와의 코디네이터 역할을 해야 한다는 의미에서 코디네이터라는 직함이 생겼다"고 이 코디네이터는 답변했다. 현재 수행사는 PM이 1명, 애플리케이션 개발 5명, 서버 및 네트워크 담당 1명, 홈페이지 디자이너 및 개발자 2명, PC 점검 및 관리 2명 등으로 구성되어 있다.

"보안의 기본은 PC에서 시작"

"대림대학교에서 근무를 시작한 게 2004년인데 이때는 안랩의 V3 제품과 함께 소프트런의 패치관리 솔루션인 인사이터를 사용하고 있었다. 그러다가 2010년 정보시스템 관리를 아웃소싱하면서 혼자 모든 걸 책임지고 총괄하게 됐는데 때마침 개인정보보호법이 이슈화가 되어 이전과는 다른 새로운 솔루션이 필요함을 절감하게 됐다"고 이후재 코디네이터는 당시를 회고했다.

대림대학교의 기존 개인정보유출방지 솔루션은 S사의 제품. 특정 PC에서 하드디스크를 계속 읽는 것이 문제로 제기됐다. "내 컴퓨터가 이상하다. 누군가 내 정보를 빼가는 것 아니냐"는 불만을 표시하는 교직원도 있었다. 또한 OS와 충돌로 인해 설치에 문제가 발생하거나 관리 차원에서 로그인을 한번 더 해야 하는 불편함이 문제가 되었다. 때마침 기존 솔루션의 사용 기한도 다 되어 최소한의 정해진 예산으로 어느 솔루션을 선택해야 할 지 고민하던 시기였다. 이를 위해 여러 솔루션에 대한 벤치마크 테스트는 물론 해당 솔루션을 실제 사용 중인 다른 대학을 방문해 사용성과 도입효과를 꼼꼼하게 확인했다.

그 결과 대림대학교에서 도입한 안랩의 제품은 V3 엔드포인트 시큐리티 9.0(V3 ES 9.0)을 비롯해 V3 넷 포 윈도우즈 서버 9.0(V3 Net 9.0), 안랩 폴리시 센터 4.6(APC 4.6), 안랩 EMS, 안랩 프라이버시 매니지먼트 스위트(APrM Suite), 안랩 패치 매니지먼트(APM), 내PC지키미 등이다. 엔드포인트 보안과 관련된 전 제품을 안랩 단일 벤더의 제품으로 일원화한 것이다. "과거에는 보안에 문제가 발생할 경우 제품마다 각기 다른 벤더 담당자들과 커뮤니케이션 해야 하는 불편함이 있었는데 지금은 그 문제가 말끔히 해소됐다. 결국 문제 발생 시 빠르게 대처할 수 있게 됨으로써 학생과 교직원 등 구성원들의 서비스 만족과 직결되었다"고 이 코디네이터는 털어놓았다.



[그림 1] 대림대학교가 구축한 안랩의 엔드포인트 통합 관리 플랫폼

대림대학교에 구축된 보안시스템은 V3와 안랩의 엔드포인트 보안 관리 제품의 연동이 강점이다. 엔드포인트가 중요한 이유는 개인정보나 기밀자료, 서버접속 정보 등과 같은 매력적인 정보들이 모이는 곳이기 때문이다. 하지만 엔드포인트에는 악성코드 방역에서부터 매체제어, 개인정보 관리 및 유출방지, 엔드포인트 취약점 점검, 패치 관리 등 제 각각의 제품을 관리해야 하는 어려움이 따른다. 이들을 단순한 통합이 아닌 플러그인 형태의 제품간 연동을 통해 시너지 효과

를 내야 하는 숙제를 안고 있다. 엔드포인트 보안 상태의 가시성을 확보함은 물론 각각의 환경에 적합한 보안 솔루션을 구축하고 지속적인 업그레이드로 효과적인 보안을 유지해야 하는 것이다. 안랩이 추구하고 있는 제품의 연동을 통한 시너지 효과를 대림대학교는 구현해 놓았다.

엔드포인트 제품 연동으로 시너지 구현

대림대학교는 처음에 V3와 APC를 도입한 후 순차적으로 내PC지키미, 그 다음에 APM과 APrM Suite을 도입, 현재 총 7종의 솔루션을 구축해놓고 있다.

안랩 V3 ES 9.0은 매체제어 기능이 포함된 PC 통합 보안 솔루션으로, USB나 드라이브, 네트워크와 같은 PC의 다양한 경로를 통해 유입되는 악성코드를 원천 차단하며 악성코드 유입단계에서 클라우드 탐지나 시그니처 탐지, 행위 기반 탐지 등을 통해 정보 자산보호에 기여한다. 또한 엔드포인트 통합 관리 플랫폼인 EMS를 통해 효율적인 엔드포인트 보안 솔루션의 통합 설치와 운영 관리를 지원해 엔드포인트 보안 솔루션 활용을 극대화 해준다.

최근 몇 년간 대규모 개인정보 유출 사고가 발생하면서 제정된 개인정보보호법에 대응하기 위한 솔루션인 안랩 프라이버시 매니지먼트 스위트(APrM Suite)도 대림대학교에 안성맞춤이었다. 개인정보 유출방지 솔루션인 APrM Suite는 개인정보 생성 시점부터 점검 및 관리는 물론 개인정보 유출행위를 원천 차단해 안전한 환경을 구현하는 제품이다.

대림대학교는 효율적인 패치 관리 역시 보안위협에 능동적으로 대처하기 위해 매우 중요하다고 판단했다. 그러나 교내 모든 운영시스템과 애플리케이션의 패치 현황을 파악하고 설치를 유도, 관리하는 것은 결코 쉬운 작업이 아니었다. 안랩의 패치관리 솔루션인 APM은 각종 보안 패치에 대한 실시간 중앙 관리뿐만 아니라 보안정책에 위배되는 PC에 대한 인터넷 접근차단 및 소프트웨어 설치 유도 기능을 제공함으로써 대림대학교의 고민을 해결해 주었다.

대림대학교에서 도입한 안랩 솔루션 가운데 '내PC지키미'는 백미 중에 백미라고 할 수 있다. 내PC지키미는 강제조치, 자동조치 등의 기능을 통해 개별 PC의 보안상태를 중앙에서 쉽고 간편하게 점검하고 조치할 수 있는 솔루션인데, 교내 임직원들이 사용하는 내부 그룹웨어 쿼리를 통해 내PC지키미 정보를 연동함으로써 높은 활용도를 보이고 있다. "강력한 정책 적용을 통해 학교 내 전체 사무용 PC의 내PC지키미 점수를 95점으로 유지하고 있다"고 이후재 코디네이터는 어깨를 으쓱했다.

"내PC지키미로 보안 관리 편해졌다"

시스템 관리자의 입장에서 전체 PC에 대한 패치나 보안 상황을 일일이 체크하기란 여간 힘든 일이 아니다. 하지만 대림대학교는 관리자들이 여기저기 사무실을 기웃거리면서 보안 상황을 물어봐야 하는 수고스러움을 덜 수 있게 됐다. 이후재 코디네이터는 "내PC지키미는 10가지 항목에 대해 각 PC별 점수를 매길 수 있다. 개별적으로 찾아가서 물어보기 어려운데, 중앙에서 정확하게 파악하고 정리해주는 게 이 제품의 가장 큰 장점"이라면서 "교육부의 정보보안 기본 지침상에도 부서장 확인을 받아야 하고 교육도 해야 하는데, 인사정보 연동을 통해 그룹웨어에서 공유하고 보고하는 입장에서 데이터가 자동 취합되고 전자결재로 확인할 수 있으며 점검률이 평균 90%가 넘는다. 총장님뿐만 아니라 원장님 이

하 교수님들의 동참률이 매우 높다"고 전했다.

내PC지키미는 개별 PC의 보안 상태를 점검하고 조치를 통해 전반적인 보안 수준을 개선하는 PC취약점 점검 솔루션이다. 대림대학교 교내에 설치되어 있는 사무용 PC는 모두 450여대. 다만, 학과 실습실에 있는 PC는 제외됐다. 자주 전원을 껐다 켜야 하고 원복을 하기 때문에 인사정보 연동을 할 수 없어 실습실 PC는 실습실 관리 솔루션을 통해 백신 검사 등의 보안관리를 한다. 사무용 PC들은 매일 점심시간에 백신 검사를 하도록 정책을 적용하여 실행 중이다. 컴퓨터가 켜져 있는 시간에는 계속 보안검사를 하고 있는 셈이다. 사무용 PC가 SSD 하드디스크에 8GB 메모리의 고사양으로 교체되어 검사 시에도 시스템에 무리가 없지만 혹시나 바쁜 업무 시간에 하는 것보다는 손을 놓고 있을 점심 식사 시간에 검사를 시행하도록 했다. 한 PC당 검사는 10분 내외에서 종료된다. 또한, 대학에서 구입하는 모든 노트북과 데스크톱은 정보전략운영팀를 통해 V3 에이전트를 설치하고 맥 주소(MAC Address) 인증이 된 후에 사용자에게 전달하고 있어 외부의 불순한 사용자가 교내 네트워크 연결을 할 수가 없다. 이로 인하여 교내에서 발생될 수 있는 보안 문제를 원천 봉쇄하고 있다.

대림대학교는 교직원들이 사용하는 그룹웨어를 통해 내PC지키미의 점수를 확인할 수 있도록 해놓았다. 교번으로 로그인을 하면 컴퓨터 이름과 교번이 표시되며 이름은 나타나지 않지만 내 PC의 각 항목별 점수와 총점이 함께 표시되기 때문에 경고의 의미로 느끼고 스스로 조치할 수 있도록 유도하고 있다. 최하점수로 정책을 80점으로 잡아놨지만 평균 90점 이상을 유지하고 있다는 게 대림대학교측의 답변이다.

정보전략운영팀 (2016년01월)

번호	컴퓨터이름	점수	항목1	항목2	항목3	항목4	항목5	항목6	항목7	항목8	항목9	항목1
1	유지보수근로	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
2	유지보수근로	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
3	유지보수근로	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
4	정보전략근로	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
5	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
6	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
7	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
8	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
9	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
10	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
11	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
12	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
13	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
14	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
15	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
16	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
17	DAELIMCORP	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
18	DL	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전
19	DL	100점	안전	안전	안전	안전	안전	안전	안전	안전	안전	안전

※참조

항목 1 : 바이러스 백신 및 실행 여부 점검
항목 2 : 바이러스 백신의 최신 보안 패치 여부 점검
항목 3 : 운영 체제, MS Office의 최신 보안 패치 설치 여부 점검
항목 4 : 한글 프로그램의 최신 보안 패치 여부 점검
항목 5 : 로그인 패스워드 안전성 여부 점검
항목 6 : 로그인 패스워드의 분기 1회 이상 변경 여부 점검
항목 7 : 화면 보호기 설정 여부 점검
항목 8 : 사용자 공유 폴더 설정 여부 점검
항목 9 : USB 자동 실행 허용 여부 점검
항목 10 : 미사용(3개월) ActiveX 프로그램 존재 여부 점검

[그림 2] 대림대학교 그룹웨어를 통해 살펴본 내PC지키미 실행 화면

대림대학교에 구축된 내PC지키미의 항목은 10가지. 이 항목은 교육부 정보보안 기본 지침에 따라 정한 것이며 관리자가 직접 항목을 추가할 수도 있다. 현재는 바이러스 백신 실행 여부 점검과 패치 여부, 운영체제 패치 여부, 한글 프로그램 패치 여부, 로그인 패스워드 안전성 여부, 화면보호기 실행 여부 등의 항목을 정해두었다. 이후재 코디네이터는 "국정원 보안업무규정으로 교육기관이나 공공기관은 모두 이와 같은 보안규정을 준수해야 한다. 대림대학교에서는 내PC지키미를 통해 이러한 규정을 잘 지킬 수 있었다"라고 말했다.

보안은 시스템 관리의 1순위

이후재 코디네이터는 대림대학교의 보안 수준에 대해 어느 학교보다 뛰어나다고 강조한다. "시스템 관리를 책임지고 있는 부서의 책임자로서 서버나 DB가 아무리 좋아도 정보가 새어나가고 변조되면 아무 의미가 없다. 따라서 보안이 1순위이고 서버의 성능이나 애플리케이션 개선은 2순위다"라고 답변했다.

2010년 정보전략운영팀을 아웃소싱 조직으로 개편하면서 이후재 코디네이터는 전산담당자로서 보안을 특별히 강화하는 것으로 전략을 세우고, 시스템을 현재와 같은 구조로 바꾸었다. 특히 이 시기에 개인정보보호법이 발표되고 다양한 보안사고가 발생한 것도 이러한 흐름을 부채질했다. 또한 외부 아웃소싱 업체들이 내 PC의 개인정보를 보는 것에 대한

반감을 없애야겠다는 인식도 보안을 강화하는데 한몫을 했다. 대림대학교 정보전략운영팀은 현재 매월 셋째주 수요일 '사이버 보안 진단의 날'을 운영, 보안에 대한 경각심도 고취하면서 팀의 단합을 꾀하는 시간으로 삼고 있다.

대림대학교 본부건물에 위치한 정보전략운영팀 상황실에 들어가면 학교 내 전반적인 시스템 운영상황을 보여주는 모니터가 4대 있다. 그 중에 3대가 보안 관련 모니터일 정도로 대림대학교는 보안에 무척 신경을 쓰고 있다. "모니터링이 된다는 건 금세 해결책을 제시할 수 있다는 것이다. 시스템 관리자의 입장에서 우리 학교의 보안 점수가 몇 점이나 되는지 매우 궁금할 것이다. 대림대학교는 현재 방학임에도 불구하고 90점 이상의 보안 상황을 꾸준히 유지하고 있다. 교육부의 학교 평가등급에서 PC 보안 점수가 들어가지 않고 있지만 이것이 반영된다면 대림대학교의 전체 등급은 훨씬 올라갈 수 있을 것"이라며 이후재 코디네이터는 자신감을 피력했다.

이후재 코디네이터는 마지막으로 "대림대학교는 그 동안 단 한 건의 보안사고도 발생하지 않았다. 그만큼 철저하게 대비한 것인데, 일례로 분기당 한 번씩 패스워드를 바꾸는 정책의 경우 총장님부터 몸소 실천하고 있기 때문이다. 물론 솔루션이 뒷받침을 해주고 있기에 가능한 일이다. 지금도 여러 대학에서 우리 학교를 벤치마킹하기 위해 방문한다. 많은 대학들이 우리 사례를 보고 보안시스템을 도입했으면 좋겠다"고 전했다.

[인터뷰] 대림대학교 정보전략운영팀 이후재 코디네이터

"에이전트 하나로 통합 관리하는 게 가장 큰 장점"

대림대학교의 정보전략운영팀은 어떻게 구성되어 있나?

2010년부터 필수인력을 제외한 나머지는 아웃소싱 조직으로 운영하고 있다. 그것이 운영상 효율적이라고 판단했기 때문이다. 코디네이터라는 직함이 필요한 것도 이 때문이다. 대학들의 재정이 풍족하지 않은 관계로 모든 운영을 할 때 비용을 생각하지 않을 수 없다. 솔루션을 도입할 때도 학생들의 등록금을 헛되이 쓰지 않으려고 노력한다. 그래서 여러 가지 도입 대상 솔루션을 꼼꼼하게 비교하는 것은 물론, 타 대학 도입사례 등도 참고하면서 우리 학교에 맞는 솔루션을 최종적으로 도입하고 있다.

엔드포인트 보안 솔루션을 안랩 제품으로 단일화한 이유는?

물론 그 전에 몇 가지의 다른 벤더 제품을 사용했다. 여러 장단점이 있지만 문제가 더 많았다. 인사정보의 연동이 안된다든지 시스템에 너무 많은 부하를 준다든지, 혹은 OS 충돌로 설치에 문제가 되는 경우도 있었다. 안랩 제품으로 처음부터 단일화, 통합화하려던 것은 아니었지만 멀티 벤더의 경우 문제가 발생됐을 때 커뮤니케이션에 상당한 애로가 있었다. 하지만 지금은 에이전트 하나로 관리하는 게 매우 편해졌다.

대림대학교가 보안을 이처럼 강화한 이유는 무엇인가?

보안의 기본은 PC라고 생각한다. 서버는 두 번째다. 좀비PC가 양산되는 이유는 바로 각 PC의 보안에 철저하지 못하기 때문이다. 대림대학교에서 그 동안 단 한차례도 보안사고가 발생하지 않은 건 PC 보안에 치중했기 때문이다.

교수님들이나 직원들이 규정을 잘 지키면서 호응을 많이 해주었다. 안랩의 솔루션이 박자가 잘 맞아서 지원이 잘 된 점도 영향이 크다. 보안은 어렵게 생각하면 불편할 뿐이다. 쉽게 긍정적으로 생각해야 한다. 대림대학교는 올해 개인정보 필터링 기능을 강화하고 여건이 된다면 키보드 보안 솔루션도 도입해 보안을 더욱 강화할 계획이다

대림대학교는.....

경기도 안양에 위치하고 있는 대림대학교는 1977년 학교법인 대림학원에서 대림공업전문학교를 설립한 것이 시초다. 1990년에 대림전문대학으로, 1998년에 대림대학으로, 2011년 대림대학교로 교명을 바꾸었고 현재 공학계열, 인문사회계열, 예체능계열, 자연과학계열 등 29개 학과로 구성되어 있다. 대림대학교는 재학생이 7,600여명으로 일반적인 4년제 대학보다 학생 수가 많다. 2014년 졸업생 2,000명 이상의 수도권 전문대 교육부 취업통계에서 취업률 67.4%로 취업률 순위에서 1위를 차지하기도 했다. 이처럼 높은 취업률을 바탕으로 대림대학교는 교육부가 선정한 세계적 수준의 전문대학(WCC: World Class College), 교육부지정 한국전문대학교육협의회부설 고등직업교육평가인증원으로부터 교육품질 인증대학으로 선정되었다. 대림대학교는 좋은(GOOD) 대학을 넘어 위대한(GREAT) 대학으로 학생과 기업은 물론이고 학부모, 교직원, 지역사회가 감동하는 놀라움으로 가득한 원더풀(WONDER-FULL) 대림대학교가 되고 있다.

