복잡한 기능보다 손쉬운 필수 기능이 '중요'

NAC는 IT 기기의 입국심사 … 적재적소 구축으로 비용 · 운영 효율 확보

연재순서

- NAC 10분만에 이해하기(이번호)
- 1주만에 NAC 구축하기
- 최소비용으로 NAC 구축 · 운영하는 4가지 노하우

"NAC 너무 복잡하고 어렵다." 최근 기업 보안 및 관리를 담당하고 있는 현업 담당자들의 푸념 섞인 목소리들이다.

기업 보안의 새로운 패러다임으로 화두가 되고 있는 NAC이지만, 관심을 갖고 막상 알아보려 하면 공부해야 할 내용이 상당하다. NAC솔루션을 제공한다는 업체도 한 둘이 아니고, 각 업체에서 제안하는 NAC 구현 방법도 가지각색이다. 기업 보안 업무에 있어서 NAC 아니고도 신경 쓸 것들이 많은데 과연 이렇게까지 시간 투자를 해서 도입할 가치가 있는 것인지 고민하며, 도입 검토 엄두도 내지 못하고 있을 담당자들의 표정이 눈에 선하다.

이런 담당자들의 어려움을 덜어주고자, 단순히 3분 정도 분량의 글을 읽는 것만으로도 NAC 검토에 필요한 필수 지식을 쉽고 빠르게 이해할 수 있도록 3편의 글을 연재한다. 첫 시작은 NAC 개념 및 올바른 구현 방법이며, 다음으로 구축 방법과 비용을 절감할 수 있는 방법에 대해 차례로 알아보겠다. 그럼 이번 편에서는 도대체 NAC가 무엇이길래 관심을 가져야 하는 것인지, 어떻게 구현하는 것이 맞는 방법인지 알아보자.

NAC는 출입국관리소다

지난해 봄부터 한 해가 끝나기까지, 전 세계는 신종 인플루엔자 A(H1N1), 즉 초기 '돼지독감'으로 알려진 바이러스성 질병으로 한차례 큰 홍역을 치렀다. 국내에서도 감염된 사람이 만명을 넘었으며 사망자도 10여명을 넘겼다.

초기 미주 지역에 방문했던 수녀를 시작으로 외국인 강사들 집단 감염, 초등생 집단감염, 그리고 나중에는 연예인 감염까지 한 해 내내 떠들썩했다. 다행히 타미플루라는 치료제가 효과가 있는 것으로 알려지면서 급한 대로 불은 껐지만 타미플루만으로는 근본적인 해결이 될 수 없었다. 이에 정부는 뒤늦게나마 인천공항 등 출입국 심사가 있는 곳에 검역을 강화했다. 외국에서 인천공항에 도착했을 때를 회상해 보면, 검역 담당 직원들이 온도계를 귀에 대고 체온을 측정하고, 입국 심사장으로 걸어가는 동안에도 여러 개의 감지 센서로 지나가는 승객들을 한차례 더 온도 측정을 했던 것으로 기억한다.

NAC는 바로 이 공항에서 출입국관리소가 하는 업무와 매

네트워크접근제어(NAC)는 접근하는 모든 기기를 검사, 악성코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함으로써 네트워크의 안전을 담보하는 솔루션으로 정보보안의 새로운 패러다임으로 관심을 끌고 있다. 하지만 NAC의 복잡성은 여전히 기업 담당자를 괴롭하는 상황이다. 손쉬운 NAC에 대해 알아본다.〈편집자〉

이원규 미디어랜드 기획팀장 / qlee66@medialand.net

우 닮았다. 더 정확히 얘기하자면, 보호해야 할 대상이 국가 자산이냐 아니면 기업 IT자산이냐 정도의 차이는 있지만, 입국 심사와 거의 똑같다고 할 수 있다. 입국 심사가 국내로 들어오려는 사람이 사회적 범죄를 일으킬 사람이거나 병균을 퍼트릴 사람인지 또는 문제를 일으킬 만한 물건을 들여오는 것은 아닌지를 확인함으로써 국민을 보호하고 국내 산업에 피해가 가지 않도록 확인하는 것이라면 NAC는 사내망으로 들어오려는 단말기, 또는 사람은 누구인지, 단말기가 사내 네트워크를 마비시키거나 다른 단말기들을 오염시킬만한 잠재적 요소가 있는지를 확인함으로써 사내 네트워크, 서버, 데이터, 및 사내 망에 접속되어 있는 단말기들을 보호하는 역할을 한다.

"NAC, 입국심사와 같다"

땅은 한국 땅이지만 사실상 한국이 아닌 제3의 DMZ같은 영역인, 입국심사대의 풍경을 다시 한 번 되돌아보자. 경찰복 비슷한 유니폼을 입은 심사관들은 들어오려는 사람이 내국인인지, 외국인이지를 판단하고 문제가 있는 사람은 아닌지 확인한다. 또 여러 검역 담당관들은 신종 플루 의심 환자인지를 판단하기 위해 여러 방법으로 체온을 측정한다.

▲ 출입국검사소

NAC가 하는 역할도 같다. 내부 직원이던 외부직원이던 유선랜을 PC에 꽂거나 무선랜으로 사내망에 접속했을 때 NAC는 우선 이 사용자들의 PC를 DMZ존으로 격리시켜 놓는다. 그리고 사내망으로 들어오려는 PC가 등록이 된 PC인지, IP 또한 사용해도 되는 등록 IP인가를 확인한다. 또 PC가 백신이 설치돼 있는지, 최신 패턴이 업데이트된 백신인지, 보안패치도 최신 업데이트돼 건강한지 등을 확인한 후 이 모든 검사에 합격했을 경우에 사내망으로 접근을 허용한다.

종종 기업 보안 담당자들은 백신 소프트웨어를 사용하고 있고 패치관리시스템(PMS)가 있는데 NAC가 왜 필요하냐고 반문하는 경우가 있다. 비슷하지만 확연히 다른 이유를 입국심사 컨셉에서 다시 확인할 수 있다. 핵심은 바로, 입국심사를 통과하기 전까지 내외국인들은 땅은 한국땅이지만 한국이 아닌 엄연히 분리되고 격리된 DMZ 존에 있다는 사실에 있다. 간단해 보이지만 엄격한 이 심사를 통과하지 못하면 외국인들의 경우에는 실질적인 한국땅에 한 발짝도 못 디딘 채 바로 본국으로 송환될 수 있는 것이다.

기존의 백신 및 PMS에 의존한 보안 관리의 가장 큰 문제점을 예로 들어 보면, 신종플루에 걸린 내 외국인이 특별한 심사 없이 바로 한국땅에 들어와서 전국 방방곡곡을 돌아다니다가 뒤늦게 감염 사실이 발견돼 찾아다니면서 신분 확인도 하고 타미플루로 치료해주는 개념이라고 보면 되겠다. 잠재적으로 문제를 일으킬 수 있는 단말들을 다른 영역으로 격리시키지 않고 방치했을 때 생기는 문제점은 기업 보안 담당자라면 필자가 이 지면을 할애하지 않더라도 충분히 가늠해 볼 수 있을 것이다. 지금까지는 백신이 보안의 대명사로 인식됐지만 타미플루만 갖고 신종플루를 근본적으로 해결할 수 없었듯 사전 차단 방식의 NAC가 필수적인 보안 컨셉으로 등장했다.

스마트 사내망 보안, 'NAC'

보안에 있어서 망분리는 큰 의미가 있다. 공공기관이나 몇몇 기업 연구소는 아예 물리적으로 내부망 사용 전용 PC와 인터넷용 PC를 분리시켜 놓고 사용한다. PC 두 대를 따로 쓰는 불편함을 감소하고라도 인터넷 등 외부로부터의 감염 가능성을 원천 차단하겠다는 의지이다. 최근에는 가상화를 통해 한 PC에서 다른 두 개의 망을 사용하는 기술까지 등장하고 있다.

오늘날 '스마트폰', '스마트워크' 등이 화두가 되면서 똑똑하고 효율적으로 일하자는 움직임이 산업전반에 걸쳐 일어나고 있는데 NAC 또한 '스마트 사내망 보안'이라고 할 수 있다. 물리적으로 PC를 두개를 배치해 망분리해 운영할 필요없이 PC가 내부망에 접속하기 전에 일단 별도의 DMZ 망에 격리시켜놓고, 접속하려는 자가 누구인지, 건강한지를 철저히 확인한 후에 안전하다 판단되면 내부망 사용을 허용하는 것이다. 또한 내부망에 들어온 이후에도 주기적으로 검사해 감염이 의심되는 즉시 다시 별도 DMZ망으로 재격리시킨

다. 혹시 단순 인터넷만 사용하길 원하는 외부 방문자의 경우에는 이 별도 DMZ망에서 인터넷만 사용 가능하게 하면 된다. 이는 추가적으로 인터넷만 사용하게 하는 별도의 PC를 배치하는 개념과 크게 다르지 않다.

출입국 관리소에서 인증과 검역은 둘 모두 필수다. 약 50년 전으로 돌아가서 국제공항을 처음 만든다고 가정해보자. 해외 공항을 한 번도 가보지 않은 담당자가 공항을 만든다고 한다면 입출국 심사 절차가 필요한 것인지 수하물 검사는 해야 하는 것인지 잘 모를 수 있을 것이다. 현재 NAC를 도입하는 담당자들이 그런 경우라고 볼 수 있겠다.

현재 NAC 시장에서는, 인증만 해도 NAC고, 검역만 해도 NAC고, 둘 다 해도 NAC이니 고객이 원하는 만큼만 하면 된다는 식의 허울만 좋은 형태로 NAC가 제안되고 도입되는 것을 종종 볼 수 있다. 명절마다 공항이 해외여행객으로 북새통일 정도로 해외 경험을 한 국민이 많아진 오늘날에 누군가가 "인천국제공항에서 출입국 검사만 하고 수하물 검사는 불편하니 하지 맙시다"라고 주장한다면 납득할 만한 사람이 과연 얼마나 될까.

모든 길은 출입국 관리소로 통한다.

현재 기업 보안 담당자가 검토해야 할 NAC 구현 기술은 너무 많다. 이것은 시장의 리더가 시장 형성에 실패했기 때문에 초래된 결과다.

최근 거의 매일 같이 그 성공사례가 언급되고 있는 아이폰을 예로 들어보자. 만약 애플이 아이폰을 지금 같이 혁신적으로 사용이 간편하고 예쁘게 만들지 못했다면 오늘날 스마트폰 시장은 어땠을까? 구글 안드로이드는 만약 애플 아이폰을 만나지 않았다면 현재의 경쟁력 있는 모습으로 만들 수 있었을까? 삼성이 이렇게 빨리 스마트폰을 제조하려 했을까? 아이폰이 실패했다면, 아마 스마트폰 시장도 현재의 NAC 시장과 같이 여러 업체들이 각자의 기술적 강점만을 내세우며 시장을 다양하게 분산시켜 놓아 선택을 어렵게 하면서 느린 성장을 이어갔을 것이다.

대형 네트워크 장비 업체가 초기에 제안했던 네트워크 장비 기반의 NAC 프레임워크는 기술적 컨셉이 잘못됐다기보다는 현실적 환경에 맞지 않았다고 볼 수 있다. 외부 공격보다 내부에서의 관리 소홀로 보안 사고가 빈번했던 문제를 정확히 짚어내고 이를 해결할 수 있는 방법으로 NAC를 제안했을 때는 업계로부터 폭발적인 호응을 받았다.

하지만 이익을 추구하는 기업이라는 태생적 한계에서 벗어나지 못하고 주력상품 중 하나인 스위치 기반의 기술을 제안했고, 초기 NAC 시장은 이 방법이 정석인 것처럼 이해하고 받아들였다. 나아가 달궈지기 시작한 NAC 시장에서 가능성을 보고 신규 진입한 기업들 또한 같거나 비슷한 방법으로 제작된 솔루션을 판매하거나 이 스위치 기반 NAC 프레임워크와 호환되도록 제품 구성을 했다. 이것이 무엇이 문제였는지를 우선 알아보자.

출입국 관리소는 적재적소의 길목에서 완벽한 제 기능을 해야 한다. 다시 신종플루 이야기로 돌아가 보자. 만약 입국 심사를 현재같이 공항 메인 터미널 건물에서 한꺼번에 하지 않고, 더욱 철저한 심사를 위해 내외국인들이 비행기에서 내리는 순간에 이를 수행한다고 가정해보자. 그곳도 국내로 들어오는 입구라고 말할 수 있으며, 아무 문제없이 확실히 이행될 수 있다면 이 방법은 매우 훌륭한 방법일 수 있다.

하지만 조금만 더 생각해 보면 이 방법은 구축비용이나 운영 측면에서도 매우 비싼 방법임을 쉽게 알 수 있다. 일단 수적인 면부터 생각해보자. 우선 게이트마다 약 둘 셋 정도의 심사관을 배치하고, 체온 감지 센서의 배치도 요구된다. 인천국제공항의 경우, 게이트 수는 약 40개 이상에 달하는데, 모든 게이트에 신분 심사관 및 체온 측정 센서기를 각 2개 이상씩 배치하기 위한 비용은 대략적으로만 생각해도 상당할 것임을 예상할 수 있다. 나아가 항공사들 중에 만약 게이트에서 특정 요구 조건을 내세우는 곳이 있다거나 체온 측정기가 고장이라도 날 경우에는 이를 처리 해결하기 위한 운영비용 또한 적지 않을 것이다.


▲ 비행기 게이트

이는 무선이든 유선이든 스위치 기반 NAC 구현 방식의 문제이다. 출입구처럼 보이는 곳을 모두 막겠다는 것이다. 언뜻 보면 가장 확실히 문제를 해결하는 듯 보이기에 기업 보안 담당자가 처음 들었을 때는 그럴듯하게 들렸을 수 있다. 약간 의심을 했더라도, 스스로 전문가임을 자처한 업체들이 영업적으로 설득하고 시장을 드라이브하고 있는 상황이

라면, 기업 입장에서는 실제 구매해 운영 해보기 전까진 그 실상을 파악하기 힘들 수밖에 없다.

물론 기업내 모든 스위치들이 수문장 역할을 하면서 어떤 문제없이 명령을 잘 듣고 유무선으로 접속하려는 PC들을 확실히 제어한다면 매우 훌륭할 것이다. 하지만 현실적으로 이는 쉽지 않거나 효율적이지 않다.

모든 입구를 막을 필요는 없이 꼭 필요한 적재적소에 통제소를 배치해 놓으면 되는 것이다. 밖으로 나가기 위해 어차피 지나갈 터미널 출구 이전 길목에서 한 번에 검사하는 것이 투자비 및 운영 비용 측면에서 모두 각 비행기 게이트에서 실시하는 것보다 훨씬 비용효율적임은 자명한 사실이다.

인천국제공항의 경우에는 메인 터미널로 나가기 전 입국 심사장 한곳에만 확실히 신분 심사 및 검역을 하면 되며, 다른 국제공항들도 마찬가지이다. NAC를 도입하려는 회사의 경우도 동일하다. 서울 본사에 하나, 다른 네트워크를 사용하는 지방 사무소에 각각 하나씩만 놓으면 된다. 이렇게 되면 초기 투자뿐 아니라 운영 측면에서도 엄청난 비용을 절약할 수 있다.

출입국 관리소는 스스로 운영되야

실제로 인천국제공항에 가보면 입국 심사관들이 직접 심사를 하는 곳 옆에 서너대의 자동 입국 심사기가 설치돼 있다. 필자도 사용해 본 적이 있는데 심사관들 앞에서 길게 서거나 혹시 모를 걱정 때문에 심사관과 눈을 마주치며 긴장할 필요없이 여권과 지문 한 번씩 스캔만 하면 되기에 여간 편리한 게 아니었다.

심사관도 덜 바쁘고, 입국하는 사람도 편하고 시간을 대폭 절약할 수 있는데 이렇게 좋은 것을 이제야 도입했나 싶었다. 자동 입국 심사기를 관리하는 책임자는 등록되지 않은 입국자가 발견될 경우 격리시키고 당일 담당자에게 보고시키게 했을 것이라고 쉽게 짐작할 수 있었다.


▲자동 출입국심사기

NAC는 단순히 보안을 강화해주는 보안용 단말기 관리도구가 아니다. 간단하게 몇 가지 정책만 하달받으면 알아서 작동하는 시스템으로, NAC에게 일을 시켜놓고 바쁜 보안 담당자는 더 중요한 업무에 집중할 수 있다. 쉽게 말해 "백신 최신 업데이트 꼭 하세요.", "IP 주소 함부로 바꾸면 안됩니다", "외부 방문자는 함부로 회사 네트워크에 접속하면 안 됩니다"라고 안내해놓고 지켜지지 않을까 전전 긍긍하는 하는 것이 아니라 NAC 시스템이 알아서 위의 일들을 처리하고 다른 더 중요한 업무를 보다가 가끔 정기적으로 이상이 없는지 확인하며, 문제발생시에만 보고를 받으면 된다. 이렇게 운영하려면 우선 사용이 매우 쉬워야 한다.

기능이 많다고 더 좋은 것이 절대로 아니다. 현대인은 피곤하다. 신경 쓸 것들이 너무 많다. 애플은 쓸데 없는 기능을 최대한 줄이고 꼭 필요한 핵심 기능을 쉽게 사용할 수 있게 함으로써 아이폰이라는 초대박 상품을 만들어 냈다. 컴퓨터를 잘 쓸 줄 모르는 50대 60대 아주머니들도 아이폰은 사고 싶어 한다고 한다.

기업용 소프트웨어도 마찬가지다. 기능이 많으면 훨씬 더 잘 쓰고 유용할 것 같지만 절대 그렇지 않다. 대부분의 직장인들이 거의 매일 사용하는 마이크로소프트 워드, 파워포인트 같은 오피스 제품을 보면, 그 수많은 기능들을 모두 알고 잘 사용하는 사람은 많지 않다. 달리 보면, 필요하지도 않고 사용하지도 않는 그 수많은 기능이 탑재된 오피스를 쓰기 위해 기업이나 개인이 지불한 비용은 적절하지 않다고 말할 수 있다.

NAC 시스템 또한 많은 기능을 가지고 있을 필요가 없다. 너무 많은 기능은 사용 방법을 어렵게 할 뿐이다. 오토 방식의 차를 사용하는 운전자에게 매뉴얼 방식의 차를 운전하라 하면 약간의 부가적인 기능만 더 있을 뿐인데도 무척이나 어려워하는 것을 보면 알 수 있다. 사용자는 간단하게 명령하고 시스템은 스마트하게 알아서 움직여야 한다.

지금까지 NAC가 무엇인지, 어떤 기술이 올바른 것인지, 그리고 어떤 특징이 있어야 하는지를 알아보았다. NAC는 '입국 심사' 와 같은 간단하면서 필수적인 개념이며, 적재적소에 하나만 있으면 충분하고, 간단한 명령 만으로도 스스로 잘 작동하게 해야 한다. 다음호에서는 '1주일만에 NAC 구축하기' 를 통해 간단히 NAC 구축방법에 대해 알아보도록 하겠다.

간단한 정책 · 정확한 타깃 · 스마트한 판단 '필수요소'

NAC 도입으로 기투자 효율 극대화 … 기업 보안 필수요소 인식 '절실'

연재순서

1. NAC 10분만에 이해하기
2. 1주만에 NAC 구축하기(이번호)
3. 최소비용으로 NAC 구축 · 운영하는 4가지 노하우

지난호에서는 NAC가 무엇이고 어떤 기술이 올바른 것인지, 그리고 어떤 특징이 있어야 하는지를 알아봤다. 요약하면 NAC는 '입국 심사'와 같은 간단하면서 필수적인 개념이며, 적재적소에 하나만 있으면 충분하고, 간단한 명령만으로도 스스로 잘 작동하게 해야 한다는 점이 핵심이다. 이번호에서는 'NAC 구축이 너무 복잡하고 어렵다'라는 인식의 전환을 돕기 위해 NAC 를 회사에 구축할 때 꼭 알아야 할 핵심 포인트에 대해 쉽게 이야기해 보고자 한다. 그리고 1주일이라는 설정 하에 도입에서부터 구축할 때까지 꼭 짚고 넘어가야 할 포인트들에 대해서 알아보겠다.

우선 NAC를 구축할 때 꼭 알고 있어야 하는 기준이 되는 개념이 있다. 이 개념들만 잘 숙지하고 있으면 설령 어려운 상황이 발생한다 하더라도 수월하게 올바른 판단을 내릴 수 있다. 나무 기둥이 튼튼하면 바람이 아무리 불어도 쓰러지지 않는 것과 같은 이치로 만약 이 핵심 개념을 잘 이해하지 못하고 NAC 구축을 진행한다면, 상사나 동료 또는 솔루션 업체들이 하는 한 마디 한 마디 말에 흔들리게 돼 더딘 구축 또는 최악의 경우 구축 실패까지 초래할 수 있다.

따라서 세 가지 핵심 포인트는 매우 중요하며, 이 세 가지 핵심 포인트만 알고 있으면 NAC를 구축할 준비가 됐다고 말할 수 있다. 세 가지 핵심 포인트는 첫째가 '정책은 간단해야 하고 통제는 강력해야 한다'이며 둘째는 '타깃이 정확해야 한다'다. 그리고 마지막 세 번째 핵심포인트는 '스마트하게 판단하고 강력하게 추진해야 한다'다.

간단한 정책, 강력한 통제

첫 번째 핵심 포인트는 '정책은 간단해야 하고 통제는 강력해야 한다'이다. 다양한 곳에서 사용되기에 정책이라는 단어가 포함하는 의미가 어렵게 느껴질 수 있겠지만 NAC에서 말하는 정책은 간단하다.

지난호에서 언급했던 인천국제공항의 입국 심사장으로 가보자. 입국심사에 적용되는 정책은 매우 간단해 대부분의 승객들이 이해하고 있다. 바로, 내가 누구인지를 검사하고 내가 어떤 소지품을 가지고 들어오려 하는지 심사해 아무 문제

네트워크접근제어(NAC)는 접근하는 모든 기기를 검사, 악성코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함으로써 네트워크의 안전을 담보하는 솔루션으로 정보보안의 새로운 패러다임으로 관심을 끌고 있다. 하지만 NAC의 복잡성은 여전히 기업 담당자를 괴롭히는 상황이다. 손쉬운 NAC에 대해 알아본다. 〈편집자〉

이원규 미디어랜드 기획팀장 / qlee66@medialand.net

가 없을 경우에 입국을 허가한다는 것이다. 또 이것은 국가 및 국민을 보호하기 위한 필수 과정이라는 것이다.

정책이 모두 이해할 수 있을 정도로 간단하지 않고 복잡할 경우, 정책을 내리는 책임자와 정책 운영 담당자, 그리고 승객 모두 정책에 대한 이해가 어려워 각각의 접점에서 혼돈이 초래된다. 이의 결과는 입국 시간이 길어질 뿐만 아니라 국내를 방문하는 외국인으로부터 이미지가 실추될 수 있다. 이처럼 사람에게 직접 영향을 미치는 보안 정책은 그 목적 및 방법이 모두가 이해할 수 있을 만큼 쉬워야 한다.

NAC 정책도 마찬가지로 매우 간단해야 한다. 가장 큰 이유는 내부 외부 직원에게 직접적인 영향을 미치기 때문이며, 이에 보안 정책을 만드는 사람, 운영하는 사람, 영향을 받는 PC를 이용하는 직원 모두 그 정책의 목적 및 방법에 대해서 쉽게 인지할 수 있어야 하는 것이다. 물론 사람의 의견은 다양하기에 해당 정책에 공감 또는 이해하지 못하는 사람들이 있기 마련이겠지만 적어도 그 목적과 방법은 알기 쉬워야 한다.

예를 들면, '우리회사는 누가 회사 네트워크에 접속하는지를 모니터링하고 사내 네트워크를 사용자로부터 보호하기 위한 시스템을 운영합니다. 모든 직원은 사내망 접속시에 로그인을 해야 하며, PC보안 상태가 최적화돼 있지 않을 경우 사내 네트워크 사용이 불가능할 수 있습니다.' 와 같은 정책이다. 회사 환경에 따라 약간 다를 수 있겠지만 NAC 정책은 이렇게 단순해야 모든 관계자가 같은 생각으로 NAC 구축에 동참할 수 있다.

하지만 사용방법이 쉽고 기능이 단순하다고 해서 구현 방법까지 쉬운 것은 아니다. 예를 들어 최근 몇 년 전 히트를 친 닌텐도 Wii나, 여전히 화두가 되고 있는 아이폰의 경우, 그 사용 방법은 누구나 이해할 수 있고 즐길 수 있을 정도로

〈그림 1〉 간단한 정책 · 강력한 통제

간단하지만, 그 안에 녹아 들어가 있는 기술은 최첨단이다.

NAC의 경우도 마찬가지이다. PC 사용자 입장에서 보면 웹메일이나 포털 서비스를 사용할 때 항상 하는 같은 로그인 절차처럼 보이지만, 그 안에는 IP 관리 기술, 데스크톱 관리 기술, 패치 관리 기술 등이 모두 유기적으로 녹아 있어야 한다. 대부분 보안 업체가 NAC의 컨셉에만 매료돼 자사가 보유한 특정 기술을 토대로 한 NAC를 제공하면서 제공 못하는 기술들은 제 3자 솔루션을 사용하면 된다고 한다. 하지만 다른 솔루션들을 연동할 때 유기적인 연동이 가능한지 잘 살펴봐야 한다. 실제로 아무리 대형 업체라 하더라도 써드파티 솔루션과 유기적인 연동을 제공하기는 쉽지 않은 까닭이다.

기구축된 솔루션과의 호환성도 고려해야 할 부분이다. 이미 많은 기업들이 DMS나 IPMS 같은 솔루션들을 도입해 사용하고 있다. NAC는 PC관리나 제어, 그리고 IP와 뗄 수 없는 깊은 연관이 있기에 기존에 구축돼 있는 이러한 시스템들을 잘 활용해야 한다. 스위치와 같은 네트워크 장비를 기반으로 하는 NAC의 경우, 기존에 구축된 네트워크 장비들을 이용화면 활용도가 높을 수 있지만, 지난호에서 언급했듯 스위치 호환 관련 문제나 성공 스토리를 잘 검토해 봐야 한다.

나아가 실제 도입을 검토하다 보면 PC 사용자의 편의성 문제도 고려하지 않을 수 없다. 대표적인 경우가 기존에 구축된 다른 목적의 기업 솔루션, 예를 들어 싱글사인온(SSO) 등이 이미 로그인을 요구하고 있을 수 있다는 점이다. A 솔루션 때문에 로그인 한 번 하고, B 솔루션 때문에 한 번 다시 하고, C솔루션 때문에 또 로그인해야 한다면, 그만큼 업무 효율성이 떨어질 수밖에 없다. 이러한 장애물 또한 NAC를 통해 유기적으로 해결돼야 할 부분이다.

다시 입국 심사장으로 돌아가서 통제 이야기를 해보자. 입국 심사는 정책은 매우 간단한 반면에 통제는 매우 강력하다. 문제가 있는 인물이거나 허가되지 않은 물품을 들어오려 하는 것이 감지됐을 경우 강력하게 입국을 차단하고, 재심사, 벌금 또는 추방해야 한다. 만약 통제가 허술하다면 입국 심사 자체의 존재 가치가 떨어질 것이며, 국민 또한 불안해 할 수밖에 없다. 만일 총기류나 마약과 같은 물품들이 강력하게 통제되지 않을 경우 많은 사회적 문제를 일으킬 수 있는 것이다.

이와 같이 NAC의 통제도 강력해야 한다. 문제가 있는 경우에도 통제가 안 되면 NAC의 도입 목적 자체가 무의미해진다. 따라서 인증되지 않은 사람이나 PC상태가 회사가 원

하는 기본적인 보안 상태를 유지하고 있지 않다면, 강력하게 차단해야 한다.

물론 처음에는 불편할 수 있다. 해외로 출국하려 할 때 보안 검색대가 어떤 통제를 하는지 모르는 사람은 로션, 치약, 물과 같은 크게 문제되지도 않을 것 같은 액체 물품류를 갖고 갔다가 검색대에 가서야 보안요원들의 요구로 바로 버려야 하는 어처구니없는 경우를 경험하고 화가 날 수도 있다. 하지만 한 번 경험한 사람은 액체류는 큰 가방에 넣어 화물칸으로 보내거나 꼭 필요한 경우 검색대를 통과한 후 게이트 근처 터미널에서 구입 하는 방법 등으로 자체 대응해 문제없이 바로 통과할 수 있다. 또 검색대 통과를 기다리는 줄이 너무 길어서 탑승 시간을 놓치게 되어 여행 및 출장 일정을 망쳤다고 화를 내는 사람도 있을 수 있다. 하지만 출입국관리소는 이러한 사람들 때문에 검색대를 없애거나 검색 강도를 낮추지 않는다.

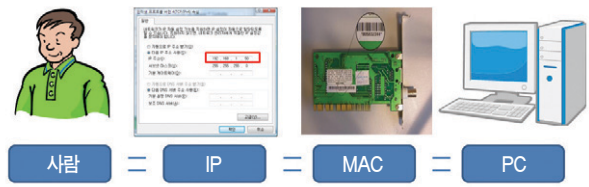
이와 마찬가지로 NAC 도입도 처음에는 이런 불만이 있을 것을 예상해야 한다. 그리고 이에 대처하는 의연하고 주관있는 자세 또한 갖추고 있어야 한다. 자주 해외여행이나 출장을 가는 사람에게는 입국 심사 때 검색대 통과하는 장애정도는 큰 문제가 되지 않는 것처럼 NAC에 대한 인식이 정착되면, 오히려 NAC를 도입하지 않고 사내망을 운영하는 회사들을 보게 되면 되려 걱정스런 눈으로 보게 될 것이다. 마치 옆 동료가 백신 없이 컴퓨터를 사용하는 것을 보면 걱정되듯 말이다.

정확한 타깃

두 번째 핵심요소는 '타깃이 정확해야 한다'는 점이다. 여기서 타깃은 사용자 PC를 지칭한다. 결론부터 말하면 사용자, PC, IP, MAC이 정확히 일치해야 한다. 이는 강력한 통제와 같은 맥락으로, 강력한 통제를 하려면 정확한 사용자와 그 PC를 파악하는 것이 전제조건이다. 특히 NAC는 네트워크 접근 차단이라는 수단을 이용해 통제하기에 타깃이 정확하지 않으면 엉뚱한 사람이 사내망을 통한 업무를 못하게 되는 결과를 초래할 수 있다.

예를 들어 A라는 협력사 직원이 사내망 네트워크를 접속하려 할 때 인가되지 않은 사용자라 판단해서 차단했는데 그 타깃 PC가 B라는 내부 직원의 것이라면, B라는 직원은 영문도 모른 채 갑자기 업무를 못하게 될 수 있다. 또 보안상 문제가 있는 A라는 PC가 발견돼 해당 PC에 매칭되는 IP주소가 X라는 것을 알고 차단했는데 결과적으로는 B라는 PC가 차단된다면 이 또한 엉뚱한 사람이 일을 못하게 되는 문제를 초래하게 된다.

〈그림 2〉 정확한 타깃



IP관리 기술력 및 노하우가 타깃을 정확히 일치시키는데 큰 역할을 한다. 바로 정확한 장비 인증을 가능케 하기 때문이다. 수시로 변경되거나 변조될 수 있는 IP와 MAC 정보를 일치시킴과 동시에 로그인을 통한 PC 사용자 계정 정보 또한 일치시킴으로써 항상 타깃이 정확히 일치되도록 유지시켜준다. 간단해 보이는 기술이지만 정확한 타깃은 매우 중요한 요소이기에 실제 NAC 도입에 있어서는 이 분야에 오랜 시간 동안 여러 회사를 통해 그 전문성 및 안정성이 검증된 업체를 잘 판단하는 것도 큰 도움이 될 것이다.

다양한 환경의 PC로부터 정확한 필수 소프트웨어 설치 정보를 추출할 수 있어야 한다. 보다 확실한 검역을 위해서는 어떠한 형태로든 PC에 소프트웨어가 설치돼야 하며, 이때 정확한 소프트웨어 및 하드웨어 정보를 추출해 낼 수 있는 안정적인 프로그램 솔루션이 필요하다. 조언한다면 고도의 기술력보다는 다양한 플랫폼의 PC를 안정적으로 자산관리해온 솔루션을 잘 검토해 보는 것이 장기적인 안목에서 도움이 될 것이다.

마지막으로 윈도우 패치 및 백신 패치의 설치 현황을 파악하고 업데이트 해주는 PMS 기술력 또한 중요 검증 포인트다. 패치 없이는 어제의 PC 보안 상태와 오늘의 보안 상태가 같다고 할 수 없다. 얼마나 자주 패치돼야 하느냐는 보안 담당자의 견해에 따라 다르겠지만, 최신의 패치가 업데이트돼야 함은 분명하다. 위의 기술력에 보태 PMS 기술력까지 갖춘 솔루션이라면 보다 안정적인 시스템 운영이 가능할 것이다.

'스마트' 한 판단과 강력한 추진력

어떤 솔루션이던 현명하게 선택해야 하겠지만, NAC의 경우는 보다 스마트하게 도입 여부와 방법을 판단해야 한다.

우선 경제적으로 이득이 되는지 잘 판단해야 한다. NAC는 네트워크 차단을 다루는 솔루션이기 때문에 PC를 사용하는 직원 입장에서 보면 업무상 불편이 따를 수 있기에 도입 자체가 조심스러운 것이 현실이다. 일 잘하는 것과 보안을 놓고 단순 비교하면다면, 이윤을 추구하는 기업이라는 주체의 특성상 당연히 일 잘 하는 것이 중요하다. 하지만 비용적인 측면을 세밀하게 따져 본다면 보면 이야기는 달라진다.

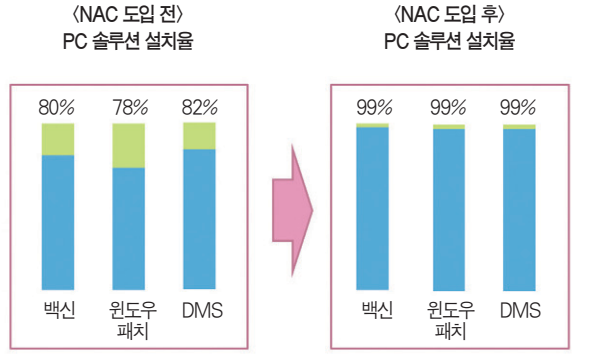
먼저 도입 비용을 생각해보자. 시스템 솔루션의 경우 잘만 도입하면 10년 이상 사용할 수 있다. 보수적으로 생각해서 3년 정도 사용한다고 했을 때의 예상 솔루션 구매비용을 우선 생각할 수 있다. 이에 더해 사내망 접속 시, 로그인 및 PC 보안 수준 미달로 네트워크 접속 차단됐을 때의 업무상 불편한 정도에 대한 비용도 포함시켜야 한다. 마지막으로 솔루션의 기술적 장애에 의한 네트워크 차단으로 인한 업무상 장애를 생각해 볼 수 있으며, 기타 회사 환경에 따른 추가 비용들도 고려해야 한다.

반대로 도입하지 않았을 때 비용을 생각해보자. 가장 눈에 보이는 큰 비용은 바로 기존 타 시스템의 운영 효율성 증대 효과를 포기하는 비용이다. NAC는 강력한 사용자 및 장비 인증으로 거의 100%에 가까운 자산관리를 가능케 한다. 비싼 비용을 들여 도입한 백신 또한 거의 완벽히 설치 및 운영시킬 수 있다. 큰 비용을 들여 도입했을 PMS 또한 거의 완벽하게 설치 · 운영할 수 있다. 필수 소프트웨어 및 불법 소프트웨어도 강력하게 관리할 수 있다. 큰 비용을 지불하고 도입했지만 PC단의 설치가 완벽하지 않아 보안 취약점으로 남아 있어 그 도입 효과가 의심될 수 있을 여러 솔루션의 가치를 살려 줄 수 있는 것이 바로 NAC로, 도입하지 않았을 때는 10~20% 정도의 백신, PMS, DMS 운영 효율성을 높일 수 있는 기회비용을 포기하는 것과 같다.

다음은 관리 비용을 생각해 볼 수 있다. '백신 끄면 안 됩니다', '최신 업데이트 항상 하세요', '관리자 허가받고 사내망을 써야 합니다', '불법 소프트웨어 설치하면 안 됩니다' 등등 관리자가 신경 쓰고 해야 할 직접 해야 할 인건비 및 같은 시간에 다른 더 중요한 일을 했을 때의 기회비용을 추가할 수 있겠다.

마지막으로, 가장 예측하기 어렵지만 파장이 적지 않은, 백신 및 필수 소프트웨어/패치 미설치로 인한 잦은 장애 비용도 생각할 수 있다. 이런 장애 발생시 PC 사용자의 업무 지연은 물론 IT담당자의 시간 비용이 발생한다. 나아가 누가

〈그림 3〉 NAC = 기존 시스템 성능 '업'



사내망에 접속하는지 관리가 안 됨으로써 핵심정보가 유출될 경우의 수도 고려해야 한다. 내부 사용자PC 관리 부주의로 인한 보안 사고가 전체 보안 사고의 20% 이상인 점도 고려요소다. 물론 NAC 도입만으로 내부 정보 유출을 방지할 수는 없다. 하지만 회사 대문 또는 뒷문이 잠겨있을 때와 열려있을 때의 도둑이 침입할 확률 정도를 계산해 보면 답은 쉽게 나온다.

경제적인 판단 후에는 기술적으로도 NAC의 역할에 대해 정확히 판단해야 한다. NAC는 다양한 관리 솔루션들과 밀접한 관련이 있다. IPMS, DMS, PMS 등의 관리 솔루션, 백신과 SSO같은 시스템과도 연관이 있다. 따라서 종종 관리자들은 통합이라는 이름 하에 모두 한꺼번에 되는 솔루션을 찾기도 한다. 하지만 각각의 전문성을 가진 솔루션들을 하나의 콘솔 또는 하나의 시스템으로 운영 또는 도입하는 것은 무리가 있을 수도 있고 전문성이 현저히 떨어질 수도 있으므로 주의해야 한다.

예를 들어, 직장인들이 가장 많이 사용하는 마이크로소프트 워드, 엑셀, 파워포인트의 경우 각각의 전문적인 기능이 있는 소프트웨어다. 하지만 누군가 업무용 프로그램들은 하나로 '통합' 돼야 한다고 하고 각각 프로그램들을 따로따로 실행하는 것이 번거로워 하나의 콘솔 프로그램으로 돼야 한다고 어떨까. 전문 프로그램간의 유기적 연동이 더 중요하며, 잘못된 통합은 피해야 할 것이다.

'스마트' 한 ROI 분석으로 도입이 결정됐다면 도입 추진은 강력해야 한다. 중소기업의 경우, 적은 규모의 인력들이 NAC 운영을 함께 맡아서 하겠지만 큰 회사의 경우 네트워크팀, 보안팀, PC 관리팀 등으로 세분화돼 있을 수 있다. 이런 경우 각 부서의 이해관계 때문에 전체적인 효과를 보지

못해 NAC 구축에 실패할 가능성이 있다. 그러나 일단 그 효용성에 대해 최고 책임자가 판단이 섰다면 각 부서 및 이해관계자들을 잘 설득해서 강력하게 추진해야 한다. 최고 책임자의 강력한 의지 없이 진행될 경우에는 구축 후에도 작은 불만 하나 둘에 어렵게 도입한 솔루션 운영이 쉽게 포기되거나 무너질 수 있다. NAC 구축은 반드시 해야 하는 시스템이라는 인식이 확고할 때 성공할 수 있다.

1주일 만에 NAC 구축하기

지금까지 NAC 구축에 앞서서 꼭 알고 있어야 할 핵심 포인트 세가지에 대해 알아보았다. 이번에는 약 1주일을 기준으로 구축에 필요한 팁들에 대해 알아보도록 하겠다.

1단계(약2일) – 구축 시나리오 구상

구축이 결정되면 어떻게 구축을 진행할 것인지 구상해야 한다. 네트워크 현황을 재점검하고 어떤 순서로 진행을 할 것인지 일정 점검을 한다. 다음은 보안 정책 점검을 확실히 해야 한다. NAC를 사용하는 기본 개념은 비슷하겠지만 회사마다 어떤 소프트웨어들을 필수 소프트웨어로 사용할 것인지, 꼭 설치시킬 것인지 아닌지, 백신의 최신 버전을 얼마나 강력히 설치시킬 것인지 등등을 확립한다.

점검이 끝나면, 기존 시스템과 연동할 필요가 있는 것들이 어떤 것이 있는지 결정해야 한다. 로그인에 필요한 인사 DB 및 직원에 대한 정보는 어디에서 연결해 쓸 것인지, ID/PW는 어디서 가져다 쓸 것인지, 또는 새로 생성할 것인지 등을 잘 판단해야 한다. 기존에 이미 도입하고 사용하고 있는 SSO, 백신, PMS, DMS, 매체제어 등의 솔루션이 있다면 그 효과를 증대시키기 위해 유기적으로 연동시키는 방안에 대해서도 점검할 필요가 있다.

더불어 구축전 사용자에게 미리 공지 및 홍보를 충분히 해 구축시 발생되는 사용자 불편을 최소화해야 한다. 공지시에는 혹시 발생할 수 있는 장애 상황일 경우에 어떻게 사용자가 직접 대처할 수 있는지도 잘 안내해야 한다.

2단계(약2일) – 구축 시작 및 단계별 적용

구축에 있어 가장 먼저 해야 할 작업은 타깃을 정확하게 일치시키는 작업이다. 우선 부서별 혹은 영역별로 가장 먼저 적용할 곳과 순차적으로 적용할 곳을 선정한다. 가장 먼저 적용할 곳부터 장비를 통해 IP 정보를 스캔, 타깃과 비타깃을 구분짓는 것이 우선이다. 타깃이 정해지면 설치유도를 통한 에이전트 설치로 PC자산정보와 IP정보를 정확하게 매칭시킨다. 다음은 패치관리 솔루션 설치 또는 연동을 통해 패치가 가능하게 한다.

첫 부서의 설치가 완료되면 정책을 적용시켜 본다. 내부직원, 공용PC, 외부 방문객 PC 등 각 사용자 타입별로 미리 컨설팅 단계에서 정한 시나리오대로 사용자 인증이 잘 되는지 테스트를 해본다.

다음은 네트워크가 차단된 상태에서 검역이 잘 되는지를 확인하는 단계다. 백신, 윈도우 패치, 필수 소프트웨어 등의 설치 또는 미설치 상황이 잘 나타나는지와 검역이 끝난 PC의 경우, 정상적으로 네트워크 사용을 승인받았는지를 확인하면 우선 NAC의 기본 기능은 잘 되는 것임을 알 수 있다. 부수적으로 부서별, 직급별 권한 관리 기능을 적용할 수 있겠지만 이것은 회사 환경마다 많은 차이가 있어 세부적 조정이 필요하다.

정책이 잘 적용되는 것이 확인된다면 다음 부서에 같은 순서로 작업해 전사적용이 될 때까지 진행한다.

3단계(약2일) – 모니터링 및 완료

NAC 구축이 완성 된 후에는 전체적으로 이상이 없는지 확인한다. 우선 콘솔상에 나타나는 통계, 보고서상에 이상이 없는지 점검한다. 하루 동안 모니터링하고 큰 이상이 없으면 구축 완성 결과를 책임자에게 보고한다.

현실적으로는 테스트 과정은 적어도 1주 이상 잘 지켜봐야 한다. 본편에서는 이해를 돕기 위해 1주라는 가상의 시나리오로 이야기했지만 회사 환경 및 새 시스템을 도입하는 업무처리 문화에 따라 다양한 시간이 걸릴 수 있다.

이번 편에서는 NAC 구축에 있어서 꼭 알아야 할 핵심 포인트 세 가지에 대하 알아보고 간단하게 구축 과정에 대해 알아보았다. ▲정책은 간단하고 통제는 강력해야 한다 ▲타깃은 정확해야 한다 ▲도입 검토는 '스마트'하게 판단하고 추진은 강력해야 한다 등이 바로 NAC 구축의 세 가지 핵심 포인트다. 다음호에서는 보안 제품 도입시의 가장 큰 고민인 '비용'을 최대한 줄일 수 있는 방법에 대해 알아 보겠다. 어떻게 하면 최소 비용으로 NAC 구축/운영을 할 수 있는지에 대한 정보를 통해 많은 보안/네트워크 담당자에게 도움이 되기를 기대해 본다.

"NAC 도입은 반드시 성공해야 한다"

부서간 원활한 협업체계 구축 '필요조건' … 향후 확장 필수 고려 요소

연재순서

1. NAC 10분만에 이해하기
2. 1주만에 NAC 구축하기
3. 최소비용으로 NAC 구축/운영하는 4가지 노하우 (이번호)

지난호에서는 NAC 구축에 있어서 꼭 알아야 할 핵심 포인트 세 가지에 대해 알아보고 간단한 구축 과정을 제시했다. 지난호의 핵심을 다시 정리하면 ▲정책은 간단하고 통제는 강력해야 한다 ▲타깃은 정확해야 한다 ▲도입 검토는 '스마트'하게 판단하고, 추진은 강력해야 한다 등이다. 지난 2회를 통해 NAC가 무엇인지, 또한 구축시 핵심 포인트는 무엇인지를 이해했으니, 이번 마지막호에서는 보안 솔루션 도입 시 가장 큰 고민인 '비용'을 최대한 줄일 수 있는 노하우를 알아보고, 3회에 걸친 'NAC 쉽게 이해하기' 연재를 마무리 하고자 한다.

지금부터 알고자 하는 최소 비용으로 구축/운영하는 노하우는 NAC 솔루션 업체와 거래를 잘 해서 가장 저렴한 가격을 쟁취할 수 있는 방법에 대한 얘기를 하려는 것이 아니다. NAC 솔루션은 보안을 관장하는 중요한 시스템이다. 컨셉을 잘 잡아야 하고 조금 거창하게 말하자면 IT 컨설팅에 의해 도입돼야 할 필요가 있는 시스템인 것이다. 다시 말해 성능에 큰 차이가 없어 단순히 가격만 비교하면 되는 사무용 가구나 집기같은 것이 아니기에 가격 위주로 저렴한 제품을 도입했다가는 최소 몇 년간 쓰라린 경험을 할 수도 있다.

최소 비용으로 NAC 구축/운영을 이룰 수 있는 핵심 노하우를 먼저 제시하면 첫째 '반드시 성공해야 한다', 둘째 '중복 투자를 피해야 한다', 셋째 '운용하기 쉬워야 한다', 넷째 '첫째,둘째 그리고 셋째 노하우를 절대 잊지 않는다' 등으로 요약할 수 있다.

NAC는 실패할 수 있다

NAC 도입은 반드시 성공해야 한다. 실패할 경우 그 피해 비용은 단순 도입 비용뿐 아니라 도입을 위해 관계자들이 투자한 정신적, 시간적 비용의 낭비란 문제가 추가로 발생한다. 레퍼런스가 있는 이름난 업체의 솔루션을 도입을 하는데 성공/실패를 운운하는 것이 이상하게 생각할 수 있을 것이지만, NAC는 구매했다고 해서 반드시 기대했던 대로 잘 작동하고 잘 사용할 수 있는 것이 아니다.

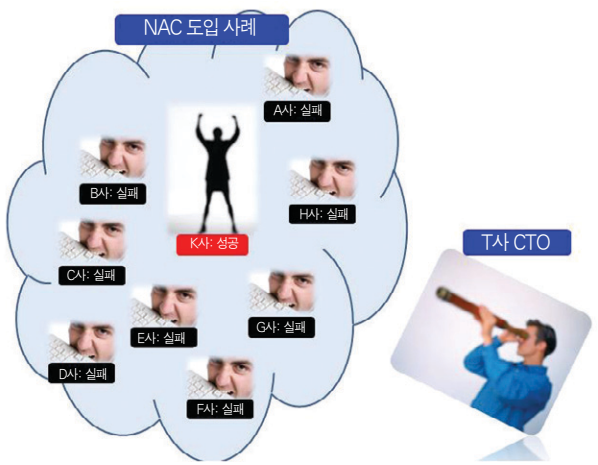
네트워크접근제어(NAC)는 접근하는 모든 기기를 검사, 악성코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함으로써 네트워크의 안전을 담보하는 솔루션으로 정보보안의 새로운 패러다임으로 관심을 끌고 있다. 하지만 NAC의 복잡성은 여전히 기업 담당자를 괴롭히는 상황이다. 손쉬운 NAC에 대해 알아본다. 〈편집자〉

이원규 미디어랜드 기획팀장 / qlee66@medialand.net

간단히 말해 NAC는 실패할 수 있다. 이것은 주관적인 의견이 아니며 단순히 우리나라 만에 국한된 문제도 아니다. 전 세계적으로 많은 기업들이 NAC 도입 실패를 경험했다. 유명 IT전문 글로벌 매체도 다음과 같은 제목의 NAC에 대한 기사를 내보내 왔다. "Is NAC dead?", "NAC, not Dead yet". NAC 자체가 실패냐 아니냐를 운운하고 있는 것이다. 실패 경험이 나오는 배경에 대한 의견들도 다양하다.

NAC 도입에 있어서 가장 큰 비용은 바로 '실패 비용'이다. 야심차게 큰 비용을 들여 NAC를 구축했다가 실패했을 때 비용은 단순히 구매 비용만 고려하더라도 상당히 크다. 도입시에 솔루션 업체와 거래를 잘 해서 10%, 20% 저렴하게 구매하는 것과는 비교도 안 된다. 전 직원에게 영향을 미치는 시스템인 만큼 실패했을 경우 IT 부서에 대한 신뢰도 역시 낮아질 수 있다. 새로운 시스템을 구매하려 해도 실패 비용의 여파때문에 재도입하는데 시간이 걸릴 수밖에 없으며, 그 기간 동안에 보안은 타사에 비해 취약해질 수밖에 없다. 게다가 시간적 비용 등을 고려한다면, 실패비용은 가파르게 증가하게 된다.

〈그림 1〉 NAC 도입 사례



따라서 '성공 사례'를 꼭 확인해야 한다. 특정 솔루션 도입을 고려할 때 현재 많은 보안 담당자들은 실패를 피하기 위해 레퍼런스를 참고하고 있다. 솔루션 업체들 또한 홍보할 만한 레퍼런스를 만들기 위해 최선을 다한다. 그만큼 레퍼런스는 중요하다.

하지만 여기서 반드시 확인해야 할 사항이 있다. 그것은 바로 '도입 사례'와 '성공 사례'는 다르다는 점이다. 누구나 알 만한 업체가 도입했다고 해서 반드시 성공했다고 말하기 어렵다. 또한 레퍼런스가 많이 있다고 해서 반드시 좋은 솔루션은 아니다.

사실 이름난 기업일수록 실패 사실이 알려지길 꺼려 한다. 따라서 도입을 고려하고 있는 기업의 담당자들은 특정 회사가 솔루션을 구매했는지, 안 했는지만 알 수 있을 뿐, 잘 사용하고 있는지, 또는 사용하길 포기했는지의 여부는 알기 힘들다.

다시 강조하지만, 실패했을때의 비용은 너무 크기 때문에 NAC 도입을 고려하는 담당자는 꼭 '성공 사례'를 알기 위한 노력을 게을리 해서는 안 될 것이다.

나아가 담당자가 NAC를 정확하게 알아야 한다. 그동안 SI 업체나 국내외 솔루션 업체가 제품을 판매하기 위해 잘못된 환경을 조성하고, 컨설팅함으로써 기업이 도입된 시스템을 잘못 사용하는 경우를 종종 볼 수 있다.

NAC는 특히 내부 보안의 컨트롤 타워 역할을 해야 할 솔루션인 만큼 기업 내 담당자가 기본 컨셉을 알아야 한다. 아무리 솔루션 업체가 전문성 있는 벤더라 하더라도 담당자는 어떤 것이 올바른 컨셉인지 정도는 이해하고 판단할 줄 알아야 한다.

각 제품들의 세세한 기능까지는 알 수도 없고 알 필요도 없겠지만 장기적인 안목으로 어떻게 NAC를 구성하고 동작돼야 하는지에 대한 컨셉만큼은 확실히 알고 있어야 한다. 그래야만 실패하지 않는다. 단순히 솔루션 업체에게 맡기는 식의 NAC 도입이라면 차라리 안하는 것이 낫다. 기다렸다가 NAC도입을 훌륭히 성공한 업체가 나왔을 때, 그 때 따라하더라도 늦지 않다. 성공하는 NAC는 스마트하고 강한 의지가 있는 담당자의 노력에 달려있다.

기존 솔루션 대체 아닌 '활용 · 통제'

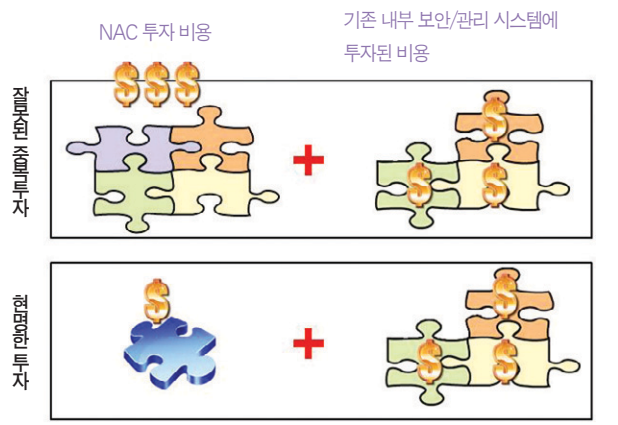
NAC는 기존의 내부 PC 관리 및 보안 솔루션과 밀접한 관계가 있다. 그것은 NAC의 태생 자체가 치료할 수 없었던 문제를 해결해 주는 혁신적인 새로운 보안 제품이 아니라, 기존에 있는 보안 및 자산 솔루션의 도입 효과를 최대한 증대시켜 확실히 통제하자는데 그 목적을 두고 있는 까닭이다.

회사 내부 솔루션을 함부로 사용 못하게 하는 사용자 인증

시스템도 이미 존재해 왔고, 내부망 외부망을 분리하는 시스템도 있다. 안티바이러스, 자산관리 솔루션, IP관리 솔루션, 패치관리 솔루션도 이미 시장에 등장한 지 꽤 됐다. 하지만 아무리 위의 솔루션들을 잘 써도 취약점은 존재하고 그 효과를 모두 누릴 수 없기에 강력한 통제 시스템을 마련, 기구축 솔루션들의 역량을 최대한으로 끌어 올려야겠다는 아이디어가 창출됐으며, 이것이 NAC인 것이다. 그리고 이러한 NAC는 그동안 '관리'라는 패러다임을 '통제'라는 새로운 개념으로 바꾸는 계기가 되고 있다.

NAC의 역할은 기구축된 시스템을 '통제'하는 것이다. NAC가 백신 소프트웨어를 대체할 수는 없으며, 전문 IP관리 솔루션을 대체할 수도 없다. 마찬가지로 전문 자산관리 솔루션을 대체할 수도 없고, 전문 패치관리 솔루션을 대체할 수도 없다. NAC는 이를 대체하는 것이 아니라 위의 솔루션들을 통제하는 시스템이기 때문이다.

〈그림 2〉 비용효율적인 NAC 투자



하지만 현실은, 솔루션 업계들이 경쟁을 하고 상품화에 힘을 쓰다 보니 위의 모든 관리 기능을 모두 수행할 수 있는 것이 NAC 솔루션으로 인식이 돼 버린 양상이다. 많은 NAC 제품들 또한 위의 기능들이 조금씩 모두 되는 형태로 개발돼 판매되고 있고, 가격도 자연스레 모든 기능들의 개발 비용이 녹아들어간 가격으로 형성되고 있다.

기구축된 솔루션들은 고유의 중요한 역할과 가치가 있다. 다시 한 번 강조하지만, NAC는 기존의 내부 보안 및 자산관리 시스템의 성능을 향상시키고 앞으로 도입할 시스템들이 확실히 모든 단말에 적용되도록 하는 강력한 지휘자 역할을 하는 시스템이다. NAC란 것이 기존에 구축된 엔트포인트 보안 및 관리 시스템의 역할을 모두 다 해주는 만능 시스템이 아니란 얘기다.

따라서 기존에 구축된 관련 시스템들이 이미 있는 상황에서 NAC 솔루션을 도입한다면, NAC 본연의 역할에 전문성이 있는 것인지를 살펴보고, 이미 도입돼 사용되고 있는 기능들이 제안된 NAC 제품에 포함돼 있는 것은 아닌지를 꼼꼼히 따져 봐야 한다. 많은 대기업, 중견기업 및 공공기관들의 경우에는 이미 엔드포인드 보안 및 관리 솔루션들이 하나 이상 갖춰져 있을 것이다. 빈약한 각각의 기능들이 모두 포함돼 있는 솔루션이 아닌 NAC 기능을 확실히 하는 솔루션을 잘 찾는 것만으로도 중복투자를 피하고 적절한 가격에 NAC를 도입할 수 있을 것이다.

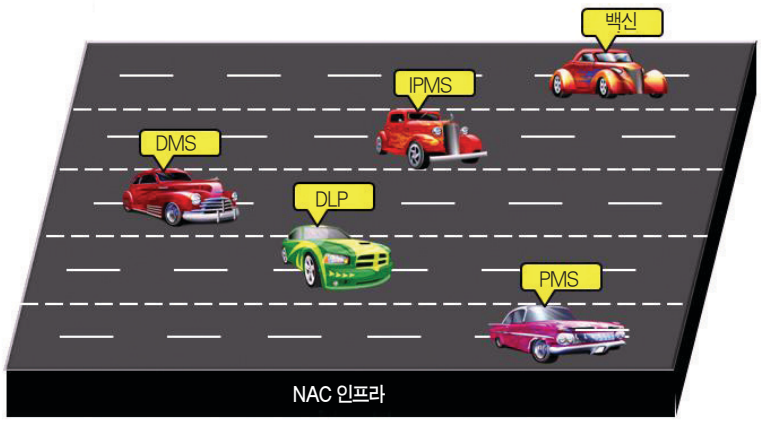
손쉬운 운용, 비용절감 '지름길'

운용상에 들어가는 비용은 원하는 기능을 적용하는데 요구되는 시간이다. 사용법이 어려우면 우선 정책을 내리기가 힘들어진다. 또한 정책 적용 방법이 간단하지 않으면, 정책이 잘 못 반영될 수 있다.

NAC는 단순한 관리 시스템이 아니라 '통제' 시스템이기 때문에 정책이 정확히 내려지지 않을 경우에는 큰 혼란을 초래할 수 있음은 꼭 기억해야 한다. 간단히 말해 정상적으로 일을 할 수 있어야 하는 직원의 업무를 마비시킬 수 있다. 이 경우 각각 직원들의 업무 마비로 인한 손해 비용 및 관리자가 문제를 해결하기 위해 투자해야 할 시간 등을 모두 비용으로 환산하면 그 크기는 엄청나다.

가능한 직관적으로 사용할 수 있어야 한다. '트레이닝 코스트(Training Cost)'라는 용어가 있다. 특정 기기나 제품을 사용하고, 익숙해지는데 필요한 시간 및 비용을 말하는 것이다. 하버드 비즈니스 스쿨 프레스에 기고한 UC버클리대 칼 샤피로 교수의 'Information Rules'이란 글에 따르면, 윈도우가 80~90%에 가까운 시장 지배력을 가지고 매킨토시가 10% 이상의 시장 점유율을 극복하기 힘든 원인이 바로 이 트레이닝 코스트에 있다고 한다. 이미 대부분의 사용자들이 윈도우 환경에 익숙해져 있고 쉽다고 느끼기 때문에 다른 인터페이스를 제공하는 OS에 거부감을 느끼고 또 새로운 시스템을 사용하고 익숙해지는데 시간이 걸릴 뿐 아니라 다른 OS에 대한 거부감 또한 생각보다 크다는 것이다.

〈그림 3〉 NAC 고속도로(내부보안 인프라)



NAC 역시 마찬가지다. 시스템 관리자 또한 UI나 그 사용법이 직관적이지 않으면 잘 쓸 수 있는 기능도 활용 못 할 수도 있고, 또한 통제를 잘 하지 못해 문제를 일으킬 수 있으며, 이러한 우려 때문에 사용이 꺼려질 수도 있는 것이다.

첫째, 둘째 그리고 셋째 노하우를 절대 잊지 않는다

앞서 언급한 세 가지 노하우는 NAC 도입에 있어서 비용을 최소화하기 위해 너무나 중요한 원칙이다. 이 가운데 특히 '반드시 성공해야 한다'는 '중복투자를 피해야 한다'와 '운용이 쉬워야 한다'를 모두 포괄하는 가장 중요한 원칙이다.

성공 여부가 너무나 중요한 이유를 다시 종합 정리해 얘기하자면, NAC는 바로 '내부 보안 인프라'기 때문이다. 앞서 언급했듯 기존의 백신, 패치 관리 솔루션, 자산관리 솔루션, 내부망 사용자 관리 등을 확실히 하기 위한 내부 보안 인프라인 것이다.

NAC가 제대로 구축, 정립되면 향후에는 NAC라는 인프라 위에서 앞으로의 엔드포인트 보안 솔루션들이 컨트롤될 것이며, 그 대상은 데이터유출방지(DLP) 솔루션일 수도 있고 불법소프트웨어 방지 솔루션이 될 수도 있다. 그 이외의 어떤 새로운 엔드포인트 보안 솔루션이 나온다 하더라도 NAC 위에서 통제될 것이다. 이러한 상황을 가정한다면 NAC 인프라 투자가 실패할 경우는 심각한 문제가 야기됨을 알 수 있다.

여기에 한 가지 더 첨언한다면 성공적 NAC를 위해서는 부서간 긴밀한 협조가 절대적으로 필요하다. 대기업의 경우 NAC와 관련이 있는 부서나 담당자가 다수 존재하게 된다. NAC는 내부보안 인프라기 때문에 백신을 관리하는 조직, 자산관리를 담당하는 조직, IP를 관리하는 조직 등등과 협의를 피할 수 없다. 각각 시스템의 '관리'는 계속 유지하더라도 '통제' 권은 NAC에 넘겨야 하기 때문이다.

하지만 각각 부서의 이권을 고려하다 보면 NAC는 절대로 될 수가 없고 도입되더라도 실패할 가능성이 크다. 각 부서의 협의를 끌어 낼 수 있는 강력한 리더의 의지가 반드시 있어야 한다.

1회에서 예로 들었던 출입국 심사장의 경우에도 마찬가지다. 입국 심사는 법무부가 담당하고, 항공 및 수하물은 건교부가 담당하고, 치안은 행자부 소속의 경찰이 담당한다. 위 인프라를 구축하려는 국가의 강력한 의지와 부서간의 긴밀한 협조가 없었다면 공항에서의 국가보안은 이뤄지지 않았을 것이다.

마지막으로 솔루션간 유기적 연동을 언급하고 싶다. NAC는 단독 솔루션이 아닌 여러 엔드포인트 보안/관리 솔루션을 관장하는 인프라이다보니 기존 시스템 및 앞으로 추가 도입할 시스템들을 유기적으로 연결시킬 수 있어야 한다. 때에 따라서는 이기종간의 연동을 위해 커스터마이징이 필요할 수도 있다.

이러한 이유로 기업 환경에 따른 커스터마이징을 고려해 빠른 지원이 가능한 NAC 솔루션을 추천한다. 커스터마이징 비용은 특성상 개발자의 인건비를 수반하기 때문에 추가 비용이 발생할 수 있다. 기존 시스템에 대한 커스터마이징뿐 아니라 새로 도입하게 될 수 있는 시스템에 대한 연동도 고려한 유지보수 계약도 체결하는 것이 중요하다.

지금까지 NAC가 무엇이고 올바른 기술은 어떤 것이며, 구축시 꼭 알아야 할 핵심 포인트 및 비용을 최소화하기 위한 노하우들을 알아봤다. 3회에 걸친 연재가 기업 CEO 또는 보안 담당자들이 NAC에 대해 쉽게 이해하는데 도움이 됐기를 바라며, 'NAC 너무 어렵고 복잡하다'라는 푸념섞인 목소리 또한 조금 줄었기를 희망해본다. NT