CONCERT FORECAST 2008

2008 기업 정보보호 이슈 전망

사단법인 한국침해사고대응팀협의회(CONCERT)에서는 지난 1월 7일부터 25일까지 3주간에 걸쳐 364개 회원사 중 105개 정회원사를 대상으로 '2008년도 기업 정보보호 이슈' 전망에 대한 조사를 실시했다. 예년과 마찬가지로 각 기업별로 2008년도에는 기업 정보보호에 있어 어떤 이슈들이 등장할 것으로 예상하고 있는지, 또 이러한 이슈들에 대해 어떤 대비책을 마련할 예정인지 등이 조사의 핵심이었으며, 조사를 통해 얻어진 분석자료를 회원사에 재배포함으로써 자사와 타 기업의 준비상황을 비교할 수 있도록 한다는 데 본 조사의 목적이 있다.
CONCERT FORECAST 보고서는 제품/서비스 공급자나 학계 등의 의견이 아닌, 순수 기업 사용자들의 입장에서 기업 실무와 직접적으로 관련된 이슈들만을 추려냈다는 점에서 타 전망 자료와 차이가 있으며, 그렇기에 기업 실무자의 입장에서는 가장 흥미롭고 유용한 전망자료가 될 수 있다. CONCERT의 2008년 기업 정보보호 이슈 전망 조사결과를 소개한다.

심상현 (사)한국침해사고대응팀협의회 사무국장(sean@concert.or.kr)

ISSUE 1

DDoS 공격 우려 더욱 확대
"제발 누구라도 좀 막아주세요"

올해 CONCERT 정회원사들의 관심은 단연 DDoS(Distribute Denial of Service) 공격에 집중돼있었다. 지난해의 경우 아이템 거래 사이트를 필두로 성인/화상채팅 사이트 등 제도권 밖에 있는 주요 사이트들을 타깃으로 했던 중국발 DDoS 공격이 올해부터는 그 대상을 더욱 확대해 일반 쇼핑몰은 물론, 기업, 금융, 기관 등으로까지 확대될 것이라는 우려 섞인 전망의 목소리가 높았다. 이른바 'DDoS 방어 전용 장비'를 구축하거나 웹 방화벽, IPS, 그리고 최근 등장한 UTM과 같은 장비들을 통해 기본적인 DDoS 공격을 차단해 왔던 회원사들 또한 장비보다 한두걸음 앞선 진화를 거듭하고 있는 DDoS에 대해 불안감을 느끼는 것은 마찬가지였다.

웹사이트와 애플리케이션의 개발단계에서부터 DDoS를 포함한 중국발 공격에 대비해야 한다는 주장이 있는가 하면, 설계단계에서부터 SPICE 및 CMMI 등과 같은 개발방법론을 적용함으로써 기본적인 공격에 대비해야 한다는 주장도 있다. 그런가 하면 DDoS에 대한 대책을 일개의 기업 또는 기관에 맡길 것이 아니라 관련 부처 주도 하에 인터넷침해사고대응센터 및 사이버테러대응센터 등과 민간업체(ISP, IDC 등) 간의 협력관계 강화를 통해 DDoS 공격의 근원지부터 차단될 수 있도록 실질적인 협의체가 활성화되어야 한다는 주장도 있었다.

이처럼 수요가 있으면 반드시 공급이 따르는 법. DDoS 방어 전용장비를 비롯해 DDoS 공격에 특화된 전용장비는 올해 그 어느 때보다 활황을 누릴 것으로 보인다. CONCERT 회원사들에 따르면, 이전에는 DDoS 공격 대응 솔루션이 극소수 벤더에만 존재했으나, 올해 들어 이른바 'Anti-DDoS' 솔루션의 공급이 활발해졌으며, 이에 따라 지난 2006년의 NAC(Network Access Control), 2007년의 UTM에 이어 올해도 또 하나의 새로운 보안시장이 형성될 것으로 전망된다.

ISSUE 2

중요하나 복잡한 개인정보보호
"고민은 깊어지는데, 법은 빨리 안 만들어지고"

여타의 전망치에서도 대부분 그랬듯이, 2008년도 CONCERT 정회원사들의 큰 관심 역시 개인정보보호 문제였다. 먼저 지난 2005년 3명의 국회의원에 의해 각각 발의된 이후 2006년도 위원회의 실질적인 심의를 단 한 차례도 거치지 않은 채 지난해에는 급기야 그 필요성에 대한 의문까지 제기된 개인정보보호법은 법 제정시 많은 이해관계가 얽히게 될 기업들의 궁금증을 자아내고 있다. 그러나 올해는 새로운 정권이 들어선 만큼 개인정보보호법 이외에도 처리해야 할 현안이 산적해 있어, 법 제정까지 시간이 예상보다 더 걸릴 수 있는 상황이다.

개인정보보호 문제에 있어 기업들은 단순히 개인정보에 대한 보호에만 관심이 있는 것이 아니라, '최대한 보호하면서 최대한 사용할 수 있는' 아이러니한 방안을 찾아야 하기 때문에 여간 골치가 아픈 것이 아니다. 여기에 개인정보에 대한 국민들의 인식 또한 최근 일련의 개인정보보호 관련 분쟁들로 인해 급격히 제고되고 있어 기업들의 고민은 그만큼 깊어지고 있다. 실제로 최근 출범한 개인정보보호 담당임원들의 모임인 한국CPO포럼에서 논의되고 있는 내용들을 들춰봐도 이런 고민들이 대부분을 차지하고 있다.

임원급에서 제도에 관심을 두고 있는 동안 실무자들은 현실적인 솔루션을 찾고 있는데, 역시 DB에 대한 암호화 통신과 조회내역 로깅 등을 지원하는 DB 보안 솔루션 등이 그 핵심에 있으며, '코에 걸면 코걸이, 귀에 걸면 귀걸이' 식으로 '개인정보보호 솔루션'이라고 명명됐던 정체불명의 솔루션들이 올해부터는 본격적으로 제 색깔을 찾을 수 있을 것으로 전망된다. 실제로 다수의 회원사들은 개인정보보호 담당자와 보안업체들간의 개인정보보호 솔루션에 대한 의사소통의 갭이 어느 정도 메워졌다는 의견을 보이고 있었다.

ISSUE 3

외부해킹 방어 보단 내부유출 방지
"외부 해킹보다 더 무서운 게 있다?"

지난해 수 건의 대형 산업기밀 유출사고가 발생하면서, 내부정보 유출방지에 대한 관심이 그 어느 때보다 높아지고 있는 시점이다. 심지어 적지 않은 회원사들은 "이제 외부로부터의 해킹은 내부정보 유출에 비하면 관심사도 아니다"라고 말한다.

DRM이나 문서보안 솔루션 등을 중심으로 한 사내정보 유출방지 시스템을 구축, 운영해왔던 기업들도 이제는 더욱 강화된 보안대책 수립에 여념이 없다. 뒤에서 언급할 또 하나의 이슈인 '정보보호 전담팀의 리빌딩(Rebuilding)' 움직임 역시 이러한 분위기와 밀접한 관계를 맺고 있다. 내부정보 유출이라는 것은 한 두 개의 시스템, 또는 한 두 명의 사람으로 해결할 수 없는, 아니 어쩌면 모든 시스템, 모든 사람으로도 해결할 수 없는 문제일지도 모르기 때문이다. 실제로 CONCERT가 회원사들을 대상으로 실시했던 설문에 의하면, '현 시점에서 내부정보유출을 완전히 막을 수 있는 방법은 사실상 없는 것이 현실인데, 미래에는 이것이 가능할 것으로 보는가'라는 질문에 CONCERT 회원사의 76.4%가 '불가능할 것'이라고 응답한 바 있다.

그럼에도 불구하고, 우리의 기업보안 담당자들은 내부보안 강화를 위해 사내 여타 부서의 직원들과 한바탕 전쟁을 치러야 한다. 타 부서와의 갈등시 임원진의 중재(13.6%)나 규정제시(27.3%) 등의 방법보다는 설득(59.1%, CONCERT 2007 기업 정보보호 의식조사)에 의존하고 있는 기업보안 담당자들의 검은 머리카락이 올해가 지나면 희끗희끗해질까 걱정이다.

ISSUE 4

정보보호 전담조직의 리빌딩(Rebuilding)
"보안조직은 이제 더 이상 보안만 해서는 안 된다"

한 대기업의 보안담당자가 이렇게 말한 적이 있다. "우리는 보안임원에게 보고를 할 때, 물리적 보안이니 관리적 보안이니 이런 단어를 쓰면 혼나요." 보안이면 그냥 다 보안이지 무슨 물리적 보안, 관리적 보안 같은 구분이 있냐는 것이었다. 그럼에도 불구하고, 물리적 보안, 관리적 보안, 또는 IT 보안과 같은 단어들은 수많은 보안 공급업체들의 제안서와 기업 내부의 보안관련 보고서를 끊임없이 장식해 왔던 것이 사실이다. 그때 그 보안임원의 생각은 이제 거의 현실이 되어 있다. 기업 비상계획실이나 총무팀에서 관할하던 이른바 '물리적 보안', 그리고 전산담당부서에서 관할하던 이른바 'IT 보안' 업무의 통합작업은 이제 CONCERT 회원사들에게서 눈에 띄는 트렌드로 자리잡아가고 있다.

단순한 업무의 통합 정도로만 끝나는 것이 아니라 CONCERT 회원사들의 정보보호 전담조직의 변화는 '리빌딩'이라 표현해도 무방할 정도의 움직임을 보이고 있었다. '이제 보안조직은 단순히 보안만 해서는 안 된다'는 것이 리빌딩의 핵심이다. 즉, 관리적·물리적·기술적 보안영역의 통합을 넘어서, 보안조직이 비즈니스의 연장선상에 위치할 수 있도록 하는 Repositioning, 성과관리를 강조한 부서 재배치, 모든 부서에 정보보호 업무가 녹아들 수 있도록 하는 정보보호 업무의 집중과 분산정책 등이 적극적으로 검토되고 있다.

ISSUE 5

사내교육 방법론의 진화
"지루한 교육은 이제 그만"

앞서 내부보안 이슈에 대해서는 대다수 회원사들이 대책보다는 한숨이 앞섰던 반면, 사내정보보호 인식제고를 위한 방법에는 앞다퉈 적극적인 대책을 내놓고 있었다. 시간 때우기 식이 되기가 일쑤인 지루한 보안교육을 시행하며 스스로도 답답해왔던 우리의 기업보안 담당자들은 올해 들어 '당근과 채찍'이 혼합된 교육방안 마련에 여념이 없다.

심지어 사내 보안인식제고를 올해 중점추진 사업으로 내걸고, 각종 포상금을 비롯한 대대적인 '당근정책'을 준비하고 있는 회원사도 있었다. 2~3년전부터 임직원 보안교육을 위해 구축됐던 사내 보안 홈페이지 등 온라인 교육수단들은 올해도 대부분 대대적인 업그레이드가 계획되고 있다.

올해 CONCERT 회원사의 사내교육과 관련한 계획 중 특히 눈에 띄는 것은 한 회원사가 기획하고 있는 '보안 FAQ 라이브러리' 구축계획이다. 고급 해킹 기법을 보유한 정보보호 전문인력을 활용해 대외 서비스의 잠재적 취약점을 사전에 진단 및 제거하고, 공격 기법별 대응방안들이 지속적으로 적용 및 활용될 수 있도록 관련 내용의 라이브러리화를 주 내용으로 추진되는 이 계획은 기술적인 내용뿐 아니라 정보보호 관련 국내/외 기준, 법률적 요구사항, 사고사례 분석 및 대응책, 해킹 동향 분석 등의 내용도 포함하고 있으며, 올 한해 동안 기업 내의 현황과 사회 이슈를 반영해 커스터마이징한 후, 사내 그룹웨어에 등록해 정보보호 업무에 지침서로써 활용 및 관리할 예정이다.

소위 FAQ라는 부분은 언제 어디서든 활용도가 높지만, 변함없는 컨텐츠로 일정기간을 보내면 아무도 그것을 거들떠보는 사람이 없기 마련이다. 그러나 그것이 이 회원사의 계획대로 '라이브러리' 수준으로 확대된다면 전혀 얘기가 달라진다는 점에서 충분히 지켜볼만한 가치가 있다고 본다.

ISSUE 6

올해 시장수요 정점 예상

"웹, 엔드포인트, VoIP를 막아라"

혹자는 '이제 정보보호 솔루션은 나올 만큼 나왔고, 시장 또한 포화상태'라고 말할지 모른다. 하지만 과연 그럴까? 우리나라는 우리의 생각보다 훨씬 더 넓고, 시장 또한 그렇다. 하나의 시장이 포화상태에 이르면, 자연스럽게 새로운 시장이 등장하기 마련이다. 올해 조사에서 CONCERT 회원사들은 웹 보안과 엔드포인트 관리, 그리고 VoIP 보안과 관련된 솔루션에 가장 큰 관심을 보이고 있었다.

웹 보안의 경우 이제는 어떤 설명도 진부하게 느껴질 정도로 그 필요성이 오래전부터 강조돼왔으나, CONCERT 회원사 중에는 오랫동안 지켜본 끝에 올해 실제 도입을 계획하고 있는 곳이 예년에 비해 압도적으로 많았다. 이에 따라 웹 보안 솔루션은 올해 그 시장확대의 정점을 이룰 수 있을 것으로 조심스럽게 전망해본다. 또한, 엔드포인트 관리를 위한 NAC(Network Access Control)의 경우, CONCERT가 지난 2005년 지상 BMT를 수행하며 회원들을 대상으로 조사한 결과 본격적인 도입시기를 약 2~3년 후로 예상했는데, 올해가 그때가 된 셈이다. 실제로 많은 CONCERT 정회원사들이 올해 NAC의 도입을 예정하고 있었다.

VoIP의 경우 IPTV와 함께 인터넷 폰 또는 IP 폰이라는 이름으로 지난해 말부터 그 이용률이 급격히 높아지면서 올해는 그 비율을 크게 높일 것으로 예상된다. 여기에 따르는 보안문제 또한 비슷한 정도의 혹은 더 급격한 형태의 상승 그래프를 보일 것으로 보인다. 이를 공급하는 대형 통신사들이 보안정책을 마련하는 것이 우선이겠지만, 어쨌든 유저들의 입장에서 보안사고가 나게 되면 그 피해를 완전히 보상받을 수 있는 길은 없다. 현대의 기업에 있어서 보안사고는 아름다운 여인의 얼굴에 지울 수 없는 상처를 내는 것과 같아서, 아무리 보상을 받아도 흉터는 지우지 못하기 때문이다.

부록 0

사용자들의 눈높이는 높아졌다

"올해 뜰 솔루션은?"

CONCERT 정회원사들이 예상하는 '올해 뜰 솔루션'은 무엇일까. 우선 앞서 소개한 대로 DDoS 공격으로부터 사용자들을 안심시킬 Anti-DoS 솔루션과 개인정보보호 이슈의 심각성에 따라 새롭게 조명받게 될 DB 보안 솔루션을 포함한 개인정보보호 솔루션, 그리고 실제로 가장 많은 회원사들이 도입을 예정하고 있다고 밝힌 웹 보안 솔루션과 엔드포인트 보안 솔루션을 꼽을 수 있겠다.

또한, 기 구축된 정보보호 시스템들에 대한 관리상태와 성과를 자동으로 리포팅할 수 있는 솔루션, 내부유출방지를 위한 저장매체 폐기 및 USB 보안 솔루션 등을 다수의 회원사들이 원하고 있었다. 한편, VoIP, 유비쿼터스, 홈네트워크 등 미래환경에 대비한 보안 솔루션이 뜰 것이라는 아직은 다소 막연한(VoIP는 제외) 예상들도 많이 있었다.

사용자들의 수준과 눈높이는 분명 눈에 띄게 높아졌다. 따라서 요구사항 또한 기존 보안 솔루션들의 기능을 훌쩍 뛰어넘거나 비켜가고 있다.

일례로 한 회원사에서는 SOS(Site Oriented Solution)이라는 - 스스로 만들어 낸 명칭 - 개념의 솔루션이 다수 등장하게 될 것으로 예상했다. 즉, 사이트 적용을 위해 많은 커스터마이징 작업들이 선행돼야 했던 그 동안의 경험을 발판으로 각 사이트의 요건, 성격 등을 파악해 온 보안 솔루션 업체에서 이제 그 경험치들을 반영한 솔루션을 출시할 수 있으리라는 기대다. 물론, 커스터마이징 작업이라는 것이 그동안 많은 보안업체들에게는 '양날의 칼'로 작용해왔다는 점에서, 어떻게 될지는 두고 볼 일이기는 하지만 말이다. S