CONCERT FORECAST 2009

2009 기업 정보보호 이슈 전망

사단법인 한국침해사고대응팀협의회(CONCERT) 사무국은
지난 1월 4일부터 23일까지 3주간에 걸쳐
CONCERT 396개 회원사 중 125개 정회원사를 대상으로
'2009년도 기업 정보보호 이슈'에 대한 조사를 실시했다.

CONCERT의 정회원사는 현재 보안전담팀이
구축·운영되고 있는 기업 및 기관, 즉 기업 정보보호에 있어
그들만의 뚜렷한 의식을 지니고 있는 곳을 의미하기에,
이들을 대상으로 한 설문결과는
사실상 우리나라 기업 정보보호의 방향성을 제시한다고 해도
과언이 아니다.
매년 그렇듯이 CONCERT FORECAST 보고서는
제품/서비스 공급자나 학계 등의 의견이 아닌
순수 유저들의 입장에서 기업 실무와 직접적으로 연관된
이슈들만을 추려냈다는 점에서 타 전망자료들과는
그 궤를 달리하며, 그렇기에 기업 실무자의 입장에서는
가장 흥미롭고 유용한 참고자료로 사용될 수 있다.

기업 정보보호 담당자들의 현실적인 고민들이
듬뿍 묻어있는 금번 조사결과를 소개한다.

글 **심상현** | (사)한국침해사고대응팀협의회 사무국장 _ sean@concert.or.kr

미증유의 경기침체가 사이버 세계에 미칠 영향은?

1

"생계형 사이버범죄 창궐 전망"

지난해부터 전 세계를 강타하고 있는 전 세계적인 경기침체가 세계 곳곳에 미치고 있는 영향은 실례를 나열하기 힘들 정도로 다양하다. 경기침체, 쉽게 말해 먹고 살기 어려워질수록 으레 짐작해볼 수 있는 사회현상이 있다. '범죄행위의 증가'가 그것이다. 오프라인 세상에서의 이 같은 경험을 이제는 사이버 세상에서도 겪게 될 것이라는 걱정이 올해의 첫 번째 이슈로 꼽혔다. 이른바 '생계형 사이버 범죄'가 창궐하게 되리라는 걱정 섞인 전망이다. CONCERT 정회원사 보안담당자들의 우려를 자아내고 있는 이 생계형 사이버 범죄의 형태 또한 다양할 것으로 전망되고 있다. 이를테면, 그 형태는 보이스 피싱이나 메신저 피싱 등의 형태를 띨 수도, 작년 내내 담당자들을 괴롭혔던 DDoS의 형태를 띨 수도 있다. 그런가하면 개인정보의 매매, 즉 고객정보의 유출이 범죄행위라는 사실을 인식하고 있음에도 불구하고 '이번 딱 한번만'이라는 마음가짐을 갖도록 강요할 수도 있다.
여기에 우려를 더하고 있는 점은 바로 기업들의 구조조정과 이에 따른 대량 이직 사태다. 불의의 이직을 경험하게 된, 또는 아예 무직으로 전락하게 된 당사자들이 좋은 마음으로 회사를 떠날 리는 만무하다. 하지만 회사는 이들 중 과연 누가, 무엇을, 얼마 만큼 알고 있는지 모른다는 점이 불안할 뿐이다. 그래도 그것이 회사

전체가 사라지는 것보다는 낫다는 판단에 구조조정을 단행하지만, 그에 따른 고민은 고스란히 보안담당자들에게 떠안겨지기 마련이다.

이렇듯 우려를 자아내고 있는 '생계형 사이버 범죄'의 창궐이 어떤 결과를 가져올 것인지를 짐작하기는 쉽지 않다. 삶의 터전을 잃을 위기에 처한 사람들이 어떤 모습으로까지 변해버릴 수 있는지를 여실히 보여줬던 '용산 철거민 사태'를 직면한 직후라서 더더욱 그렇다.

계륵(?)이 되어버린 고객정보

issue 2

"개인정보보호"

지난 한 해 동안 '전성기'를 누렸던 개인정보보호 이슈는 올 한해 그 위세를 더 확장할 것으로 전망되기에 부족함이 없다. 그도 그럴 것이 지난 한해 내내 내로라하는 통신사, 포털사들이 마치 경쟁이라도 하듯 개인정보 유출로 인한 철퇴를 맞았고, 이런 실태를 더욱 심각하게 받아들인 유관 부처들은 관련법규 강화에 '올인'하는 분위기이기 때문이다.

올해부터 개인정보보호 담당자, 책임자들은 정보통신망법 개정, 그리고 개인정보보호법 재정에 따른 개인정보보호 대책마련과 함께 이와 관련한 컴플라이언스 이슈에 대응하기 위한 제반작업을 준비해나가야 한다. 그런데 이것이 결코 만만한 작업이 아니라서, 때로는 조직자체를 헤쳐 모아야 하는 골치 아픈 작업을 감내해야 할 수도 있다.

이같은 작업이 기업들을 더욱 피곤하게 하고 있는 이유는, 기존의 기업 정보보호를 위한 작업과는 달리, 개인정보보호는 법과 컴플라이언스 문제가 더욱 밀접하게 연관되어 있어 법규와 관련한 민감한 문제들을 처리할 수 있는 전문가를 필요로 하고 있다는 점이다. 때문에 개인정보보호 문제에 가장 민감한 통신사, 포털 등은 관련법 전공자들을 앞세운 전담팀을 구성하기도 하지만, 이보다 규모가 작은 기업들은 이렇다 할 방법이 없어 고민만 하루 하루 쌓아가고 있는 형편이다.

상황이 이렇다 보니 지난해에는 개인정보보호 분야가 관련분야 전문 변호사들의, 그것도 공격하는 사람과 방어하는 사람 모두의 '블루 오션'이라는, 웃을 수만은 없는 우스갯소리가 등장하기도 했다.

한 단계 더 깊이 살펴보면, 올 한해 개인정보보호 담당자들은 아이핀 등 주민번호 대체수단의 의무도입에 따른 제반작업, 주민번호·카드번호·계좌번호 등 금융정보 암호화 – 이 암호화 작업 또한 말이 쉽지 결코 만만한 작업이 아니다 – 법제화에 따른 후속작업 등의 각종 숙제들과 함께 개인정보 업무 프로세스 개선, 개인정보 전용 추출 툴 개발, 모니터링 프로세스 강화 등 관리체계 개선을 통한 개인정보 유출 원천차단을 목표로 뛸 것이다. 이것 하나만큼은 확실한 전망이 가능하다. 개인정보보호 담당자들은 올해 말 그들의 2009년을 이렇게 회상할 것이다.

"도대체 2009년이 어떻게 지나갔지?"

프라이버시 확보를 위한 프라이버시 침해?

issue 3

"사내 모니터링의 확대"
: 내부정보 유출방지 :

사무실 내에 펜과 종이노트를 PC가 대체하기 시작한 이래로 기업에 존재하는 PC의 소유권(Ownership), 그리고 그 PC의 내부에 존재하는 컨텐츠의 소유권에 관한 문제는 아주 오랫동안 수면 밑에서 논란이 되어 왔다. 쉽게 말해, 업무를 위해 기업에서 구매한 PC를 업무 이외의 용도로 사용하는 행위, 그 PC에 업무용 정보가 아닌 개인의 정보를 저장하는 행위, 그리고 바로 그 PC를 통해 회사 내부에서만 존재해야 할 정보들을 외부로 유통하는 행위들을 그동안 기업에서는 나름대로의 규칙을 바탕으로 '사내 모니터링'이라는 이름으로 저지해왔다. 그러나 그 정도가 지나칠 경우 직원들의 심리적인 반발로 인해 사내 모니터링을 통해 거둘 수 있는 이익만큼의 사기저하, 능률저하라는 불이익을 감수해야 하기 때문에, 회사 측에서는 그간 보다 적극적인 모니터링을 시행하는데 주저할 수밖에 없었던 게 사실이다.

하지만 달라진 환경과 분위기는 달라진 규범을 만들어내기 마련. 지난 한해 동안 발생했던 사고 중 기업의 직접적 재정손실로 이어진 개인정보보호 유출사고를 비롯한 절대 다수의 사고들이 대부분 내부자에 의한 것이어서, 사내 모니터링 작업의 확대와 강화는 그 충분한 명분을 얻은 셈이다. 실제로 CONCERT 정회원사 중

올해 사내 모니터링을 강화할 계획을 세우고 있는 기업이 높은 비중을 차지했으며, 나아가 모니터링 전담인력 배치계획을 세운 곳도 다수 있었다.

상황이 이렇다 보니, 2009년도에는 기업의 손실을 막기 위한 사내 모니터링 확대 움직임이 직원들의 프라이버시 보호문제와 정면으로 충돌하게 될 가능성을 많은 보안담당자들은 우려하고 있었다. 사실 우리나라의 분위기는 개인정보보호라고 하면 곧바로 고객정보보호와 동일시하는 경향을 보이고 있지만, 미국의 경우 개인정보보호 교육을 위한 커리큘럼과 자격증 항목에도 '직장에서의 프라이버시(Workplace Privacy)'가 빼놓지 않고 등장할 만큼 민감한 부분임을 감안하면, 이러한 전망은 더욱 설득력을 얻고 있다.

'발전'이 야기하는 우리들의 두통

issue 4

"모바일을 위시한 신규 서비스 취약점"

"이제 더 발전하지 말고 좀 멈춰 섰으면 좋겠어요." 한 CONCERT 정회원사 보안 담당자의 볼멘소리다. 기존의 유선환경은 이제 무선 랜(Wireless LAN)과 KT에서 사업확대를 천명한 와이브로(Wibro)로 확대되고 있고, 유선 자체의 환경도 IPTV와 VoIP 등의 다변화로 절대 다수의 보안담당자들에게 결코 익숙하지 않은 환경을 선사하고 있다.

여기에 기존의 휴대폰에 대한 보안강화 방안도 마땅치 않은 터에 그마저 '스마트폰' 대세론으로 사실상 PC와 다름없는 각종 스마트폰들이 2009년에는 마구 쏟아져 나올 태세라서 걱정스럽기 그지없다. 게다가 그동안 국내에서 단일 모바일 플랫폼으로 유지해오던 위피 폐지방침이 전해지면서, 이제는 모바일 환경 또한 윈도우, 리눅스, 유닉스 등 다양한 플랫폼을 이해하느라 피곤해하던 보안담당자들의 추가학습을 요구하게 생겼다. 여기서 심각한 문제는 이들이 추가학습을 추구함에 있어서, 해답이나 솔루션을 물어볼만한 대상조차도 우리나라에 그다지 많지 않다는 점이다. 비즈니스라면 '선택과 집중'의 원칙이라도 대입해보겠지만, 보안은 딱히 그럴 수 있는 분야가 아니다.

'보안은 사슬의 가장 취약한 부분만큼만 안전하다'라는 유명한 격언도 있지 않은가. '역사는 미래의 거울이다', '역사는 언제나 되풀이된다'는 말들을 다시 한번 되새기게 하는 요즘이다. 보안하는 사람들이 흔히 말하는 이른바 '정보화 역기능'이라는 것은, 정보화 기술의 발전에 따라 달라질 환경에 대한 예측과 이에 대한 대책 없이 그저 '앞으로 앞으로'만을 외치며 나아간 결과 파생된 각종 부작용들을 의미한다.

우리는 그동안 다양한 정보화 역기능 방지대책에 대해 논의하고 고민해왔지만, 그 중 절대 다수는 단지 지금의 '현상'에 대한 논의와 고민일 뿐, 대책을 마련하는 동안 더 큰 대책이 필요한 역기능을 만들어내기 위한 준비를 병행하고 있는 건 아닐까.

이러다가 로스쿨 들어가는거 아냐?

issue 5

"IT Compliance 대처방안"

10년 전에는 보안전문가라고 하면 으레 '암호 전문가'를 떠올렸고, 실제로도 그랬다. 물론 상당히 기형적인 전문가 분포였던 것이 사실이다. 10년이 지난 지금, 보안전문가라고 불리울만한 사람들은 누구일까? 결론적으로, 보안전문가가 '기술자'라는 인식은 이제 그만이다.

우리는 보안의 영역을 그동안 기술적 보안, 관리적 보안 등의 영역으로 나누어왔지만, 이제는 영역이 하나 더 늘었다.

'법적 보안'이라 영역을 지으면 좀 억지스러울까? 하지만 국회를 통과해 이미 시행되고 있는 정보보호 관련 법안들, 또 아직 국회에 계류 중인 법안들을 합치면, 이 다양한 법안들을 모두 숙지하고 있어야 하는 보안 담당자들에게는 '법적 보안'이라는 영역의 구분이 그다지 억지스럽지도 않아 보인다.

우선, 정보통신망 이용촉진 및 정보보호 등에 관한 법률이 개인정보보호 이슈를 중심으로 큰 폭의 개정안을 선보였고, 하반기에 시행될 것으로 전망되고 있는 개인정보보호법 또한 우리 보안담당자들의 필수 숙지사항이다. 그런가 하면 개인건강정보의 수집, 이용을 제한하는 개인건강정보보호법, 통신자료 제공의 절차를 더욱 엄격하게 통신비밀보호법, 개인정보 처리시 주의의무를 강조한 공공기관의 개인정보보호에 관한 법률 등이 신규

로 제정되거나 개정되어 '법적 보안'이라는 새로운 영역의 탄생을 마중 나와 있다. 여기에 지적재산권, 음란물, 스팸, 위치정보보호, 그리고 인터넷을 둘러싼 각종 규제들을 모두 숙지해야만 하는 보안담당자들은 이제 준(準) 고시를 준비하는 심정으로 법 공부에 매진해야 한다.

실제로 많은 CONCERT 정회원사들이 이러한 법률 등의 숙지를 위해 효율적인 학습방안들을 고민하고 있었으며, 이런 분위기는 올해 내내 끊이지 않는 이슈가 될 것으로 보인다.

내부자도, 외부자도 아닌 사람들

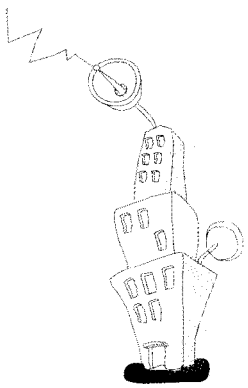
Issue 6

"아웃소서들의 보안관리"

기업의 위협은 통상 두 종류로 나뉜다. 내부로부터의 위협과 외부로부터의 위협이 그것이다. 그런데 그 중간에 내부자도 아닌, 그렇다고 외부자도 아닌 애매한 성격의 존재들이 있다. 바로 기업의 아웃소싱 인력이 그들이다. 지난해 개인정보 유출사건을 한동안 언론지면을 장식했던 GS 칼텍스 사고 역시 이 아웃소싱에 의해 초래된 보안사고였으며 콜센터, 협력업체, 외주업체 등 다양한 이름으로 불리우는 이 아웃소서들에 대한 보안대책이 그 어느 때보다 진지하고 강도 높게 논의되고 있다.

이 아웃소싱의 추이는 경기에 민감하게 반응한다. 인소싱(In-Sourcing)이 아닌 아웃소싱을 채택하는 이유로는 언제나 비용대비 효과가 첫 번째로 꼽히고, 지금 같은 경기 불황 국면에서는 기존보다 많은 기업들이 아웃소싱에 눈을 돌리게 될 것임은 자명하다. 그 형태 또한 발전을 거듭해 아웃소싱은 과거 단순 IT 인프라를 대리 운영해주던 형태에서 이제 기업의 내부 비즈니스 프로세스를 효율화할 수 있는 BPO(Business Processing Outsourcing)와 고객사의 프로세스 자체를 변화시키고 관리하는 BTO(Business Transformation Oursourcing)에 이르기까지 그 폭을 넓혀오고 있다.

문제는 이를 통해 기업 내부망에 접근하는 아웃소싱 업체 직원들에 의해 야기되는 각종 정보보호 문제들이다. 때문에 아웃소싱 비중이 높은 CONCERT 정회원사들은 아웃소싱 업체와의 SLA(Service Level Agreement) 계약에 요구되는 보안수준의 점검과 손질을 준비하고 있으며, 아웃소싱 기획단계에서부터 역할과 책임한계를 명확히 하는 작업을 병행하고 있다. 하지만 걱정은 여기서 끝나지 않는다. 아웃소싱의 확대는 기존에 기업에서 이를 전담하던 인력이 그만큼 축소될 수 있음을 의미하는데, 그 인력에는 보안전담 인력도 포함될 가능성 또한 다분하기 때문이다. **s**



올해 뜰~ 솔루션, 서비스는?

올해 CONCERT 회원사들이 가장 관심 있어 하는 정보보호 솔루션/서비스는 무엇일까?

우선 올해 조사결과를 토대로 도출된 6가지의 이슈들이 사실상 모두 개인정보보호 문제와 무관치 않다는 점을 감안하면, 개인정보보호와 관련한 솔루션/서비스를 가장 먼저 꼽을 수 있다. 지난해의 경우 관련 벤더들이 유저 기업들의 개인정보보호 프로세스에 대한 이해도가 비교적 낮다는 평가를 회원사들로부터 들을 수 있었으나, 최근 들어서는 유저와 벤더 사이의 간극이 많이 줄어들었다는 평이다. DB보안과 DRM 등이 대표적이며, 내부정보유출 방지를 위한 솔루션 또한 여기에 포함된다. 또한, 개인정보를 실제로 담고 있는 서버 관리에 대한 문제가 첨예하게 대두되면서, 이를 아웃소싱을 통해 해결코자 하는 분위기 속에 자연스레 보안관제 서비스가 다시 한번 빛을 발할 수 있을 것으로 CONCERT 회원사들은 예상했다.

아울러, 지난해부터 본격적으로 시장을 형성하기 시작한 Anti-DDoS는 올해 역시 빼놓을 수 없는 정보보호 산업의 기대주로 전망되고 있고, 끊임없이 나타나는 취약점으로 인한 피해를 최소화하기 위한 '진화한 취약점 분석도구'의 등장에 대한 기대도 어느 때보다 높았다.