CONCERT FORECAST 2014

기업 정보보호 이슈 전망

(사)한국침해사고대응팀협의회

정보보호 사용자 그룹인 한국침해사고대응팀협의회(이하 CONCERT)가 벤더가 아닌 사용자의 입장에서 현안이 되고 있는 정보보호 이슈를 선정, 「CONCERT FORECAST - 기업 정보보호 이슈 전망 보고서」를 2007년 처음 발간한 이래 올해로 여덟 번째 보고서를 발간하게 됐다. 매년 그렇듯이 CONCERT FORECAST 보고서는 제품/서비스 공급자나 학계, 연구기관 등의 의견이 아닌 순수 유저들의 입장에서 기업 실무와 직접적으로 연관된 이슈들만을 추려냈다는 점에서 타 전망자료들과는 그 내용을 달리하며, 기업 실무자의 입장에서 가장 흥미롭고 유용한 참고자료 중의 하나로 이용되어 왔다.

CONCERT 정회원사란 현재 보안전담팀을 구성, 운영하고 있는 기업, 즉 정보보호를 위한 노력에 있어 상대적 우위를 지니고 있는 기업들을 의미하기에, 이들을 대상으로 한 본 설문결과 보고서는 사실상 우리나라 기업 정보보호 우등생들의 트렌드라고 봐도 무방할 것이다.

기업의 내부 사업계획을 외부에서 접하기는 쉽지 않고 특히 그것이 보안과 관련한 영역이라면 더욱 그러한게 현실이다. 하지만 CONCERT 정회원사라는 이름으로 사업계획을 공유하고 이를 통해 정보보호 트렌드를 분석하여 CONCERT 회원사 뿐만 아닌 우리나라 기업의 보안수준을 높이는 데 일조하는 것, 이것이 CONCERT의 존재 가치가 아닌가 한다.

조사는 지난 1월 7일부터 31일까지 약 4주간에 걸쳐 CONCERT 433개 회원사 중 152개 정회원사를 대상으로 실시되었으며, '정보보호 부서의 올해 주요 사업계획'과 '보안담당자로서의 고민' 두 가지의 질문을 이메일을 통해 조사하고, 이후 추가 인터뷰를 통해 답변의 세부적 의미를 파악, 보고서에 보충하는 순서로 진행됐다.

올해 보고서는 예년과 마찬가지로 회원사들을 대상으로 물었던 2개의 질문을 토대로 2개의 파트, 즉 '계획'과 '고민'으로 구성했다. '계획'은 해당 사안에 대한 솔루션을 찾고 구체적인 실행단계에 이른 것을 의미하는 반면, '고민'은 사실상 아직까지 이렇다 할 솔루션을 찾아내지 못한 것을 의미한다. 따라서 계획 보다는 고민이 우리 보안 담당자들을 훨씬 더 크게 괴롭히고 있는 부분일 것이다.

심상현 | 한국침해사고대응팀협의회 사무국장

Part 0 "靜中動"

신용카드사 사고이후 기업 대책

앞서 언급했듯 금번 설문은 1월에 시행됐기 때문에, 보안정책과 계획에 영향을 줄 수 있는 신용카드사 정보유출 '대란' 이후의 정책변화가 있었는지, 즉 CONCERT 회원사에 사고 발생 이후에 강화되거나 변경된 보안 정책/조치가 있었는지에 대한 추가 조사가 필요했고, 그것이 예년에 비해 보고서 발간이 다소 늦어진 이유가 됐다.

대형사고가 발생하면 언론과 기관은 연일 문제점과 대책을 쏟아내고 기업은 언론을 통해 노출된 정보와 나름 정보력을 동원하여 얻은 정보를 바탕으로 원인분석을 하고 동일 문제가 자사에 발생할 가능성이 없는지에 대해 가능성 검토와 발견된 문제점을 보완하는 정책/솔루션 도입을 추진하느라 동분서주하는 모양새를 보이는 것이 보통이다.

그런데 이번 사고는 그 규모로 볼 때 초대형사고임에는 틀림없지만 기업의 움직임은 기존의 사고와는 조금 다른 움직임을 보인다. 사고발표가 나고 40여일이 경과되었지만, 회원사 조사에서도 뚜렷한 움직임을 보이기보다는 기존에 계획했던 정책/솔루션 도입등을 예정대로 – 시기는 예정보다 조금 빨리 - 진행하겠다는 반응이 가장 많이 관측되고 있다.

대다수의 회원사와는 다른 법률을 적용받고 있는 금융회사의 사고이다 보니 사고대책 또한 금융권에 초점이 맞춰진 경우가 많아 회원사에서 받아들이는 정서적 공감대가 조금 다른 것도 한 이유라고 할 수 있겠다.

사고 이후 위탁업체에 대한 관리감독, 외주인력에 대한 통제를 강화하겠다는 회원사도 있지만, 구체적인 계획이 세워진 단계라기 보다는 지금 기준에서 보안감사/점검을 추가 수행하는 정도로만 관측되고 있다. 이번 사고가 대단한 기술이나 고도의 해킹에 의한 것이 아니라 내부 정보에 접근 가능한 인력에 의한 기본적인 방법에 의한 유출이기 때문에 기술적인 보완조치가 불필요하다고 생각하고 있는 것이 아닌지 하는 인상까지 준다. 외주인력이나 내부인력에 대한 정보 통제방안을 이미 가지고 있고, 시행하고 있는 회원사가 많다 보니, 어느 정도 자신감을 가지고 있어 추가적인 보안강화 조치보다는 예외사항에 대한 보다 엄격한 관리, 직원/외주인력에 대한 정보보호 교육강화 등에서 해법을 찾는 모습도 보이고 있다.

Part Ⅰ. 계 획

Part I 1

“보험을 드는 심정으로…”
정보보호관리체계(ISMS/PIMS/PIPL) 인증

2013년 ISMS 인증 의무화가 되면서 많은 기업이 인증을 받았거나 인증심사 중에 있다. 또 PIMS는 기업이 자율적으로 인증을 신청할 수 있고, 지난해 11월 시행된 PIPL은 시행 첫 해를 맞아 기존에 ISMS나 PIMS인증을 보유한 기업들로부터 관심을 받고 있다. 2014년부터는 기존의 ISMS인증을 3년 이상 유지한 기업을 대상으로 정보보호 관리등급제를 시행한다.

기업의 입장에서는 법에서 규정하는 요건을 모두 충족한 이후에 더 잘하고 있는지를 판단하기 위해 인증을 신청하는 것이다. 보안담당자 입장에서도 인증취득이야 말로 보안부서가 열심히 일하고 있고 무언가 가치 있는 일을 하고 있다는 것을 보여주는 가장 확실한 방법이 아닐 수 없다. 게다가 일부 인증은 인증을 취득하면 추후 정보유출 사고가 났을 때 과태료/과징금을 감경 받을 가능성도 있으니 일단 받아두고 보자는 분위기도 감지되고 있다. 하지만 인증취득만 하면 기업의 보안수준이 강화되는 것일까. 인증을 받는 것보다 더 중요한 것은 인증을 취득한 이후에 사후관리가 인증심사 시와 동일한 수준으로 되고 있는지 여부이다. 매년 사후심사를 받을 때마다 외부 컨설팅을 받아야만 하는 상황이라면 인증취득의 의미가 있다고 할 수 있을까.

정보보호와 개인정보보호 정책기관이 미래창조과학부, 방송통신위원회, 안전행정부로 분산되어 있다 보니 정책기관별로 개별 정보보호인증을 운영하고 있는데 이 인증들이 서로 유사한 부분이 많아 하나의 인증을 취득한 이후 타 인증을 취득할 때 도움이 되는 점은 있지만, 중복되는 부분에 대해 다시 심사를 받아야 하는 점에 대해서는 기업의 부담이 존재한다. 동일 항목에 대한 상호인정 또는 장기적인 관점에서 인증의 통합에 대한 논의가 있어온지 오래되었지만 현재까지는 G-ISMS의 ISMS로의 통합 정도만 겉으로 드러난 상황이다. 각각의 인증마다 목적과 범위가 다르고 정책기관이 다르기 때문에 어쩔 수 없는 부분도 있겠지만, 빠른 시일 내에 가시적인 결과물이 나와야 한다는 목소리가 커지고 있다. 방송 3사 맛 집 프로그램에 한번도 나가지 않은 맛 집을 찾기가 더 어려운 것처럼 인증의 홍수에 빠지지 않기 위해서는 인증의 효과와 차별성에 대해 심사숙고가 필요한 시기이다.

Part I 2

“견고한 방패와 촘촘한 그물망”
APT & DLP

더 치밀하고, 더 끈기 있게, 그리고 더 은밀한 방식으로 침입 방법은 계속 진화하고 있다. 기존에 훌륭한 방패역할을 하던 백신이나 패턴매칭, 시그니처기반의 보안 장비로는 통상적인 공격은 방어할 수 있지만 APT 공격을 막기에는 역부족이다. 기존의 보안 솔루션과 더불어 VM을 이용해 행위기반으로 악성행위를 판단하고 차단하는 APT 대응 솔루션이 등장하면서 한숨 돌리나 싶었는데, VM을 회피하거나 패킹이나 암호화, 난독화를 통해 VM에서 분석이 어렵게 하는 우회기법이 등장하자 기존의 검사기법 외에 학습 기반(Heuristic), 평판 기반(Reputation)을 병행해 오탐과 미탐을 개선한 제품이 소개되고 있다. 새로운 보안솔루션이 시장에 등장하면 보통 2~3년의 시장형성기를 거치면서 어느 정도 레퍼런스를 쌓은 다음 본격적인 시장이 열리는데 APT는 그 위협이 실제적이고 이로 인한 대형사고가 빈발하자 기업에서는 통상적인 보안 솔루션보다 도입을 서두르고 있는 모습이 관찰되고 있다. 그만큼 APT 공격에 대한 기업의 고민이 깊다고 하겠다.

보안 초창기에는 외부로부터의 침입방어가 목적이었다고 한다면 이제는 외부 위협만큼이나 내부 데이터 유출이 주된 관심사로 떠올랐다. 과거에는 직원들이 모니터링에 대해 가지는 거부감 때문에 도입이 쉽지 않았지만 최근에 잇따른 사고로 인해 정보보호의 중요성과 필요성에 대한 내부인식이 많이 개선되었고 - 거부감은 아직도 상대적으로 덜 개선되었지만- 데이터관리를 직원들에 대한 정보보호 교육에만 맡겨놓을 수 없다는 추세 때문에 DLP 솔루션의 도입 검토에 나서고 있다. 또 이미 DLP를 도입하여 운용하고 있는 기업들은 보다 강화된 보안을 위해 암호화 통신에 대한 모니터링 등 DLP의 기능 고도화를 추진하는 모습도 보인다.

공격을 막아내는 방패는 갈수록 견고해지고 있고, 내부정보유출을 막는 그물은 갈수록 촘촘해지고 있다. 어느 하나만 잘 해서는 충분하지 않다.

Part I 3 "기술/장비가 진화하면 시야는 넓어진다." 차세대 방화벽 & 통합로그관리

보안 기술/장비에도 유행이 존재한다. 방화벽을 필두로 VPN, IDS, IPS, UTM, DLP, 웹방화벽, NAC, MDM 등 일련의 흐름이 있어왔으며, 최근에는 빅데이터 분석기술을 장착한 장비도 등장했다.

보안 장비마다 엄청난 수의 로그를 쏟아내는데, 과거에는 이 로그를 정기적/실시간으로 분석할 엄두를 내지 못하고 단순한 증적으로 남기기만 하다가 사고나 특이사항 발생 시에만 로그를 분석하곤 했다. 로그분석에 들어가는 품이 너무 크다 보니 로그분석을 통해 장비에서 걸러지지 않은 보안위협을 찾을 수 있다는 것을 알고서도 포기한 것이다. 분석기술이 발전하고 빅데이터 처리기술

이 등장하면서 보안장비 로그는 더 이상 감당하기 힘들어 한 쪽에 쌓아 둔 골칫덩어리가 아니라 보안을 강화할 원석으로 탈바꿈하게 됐다.

트래픽이 증가하고 이전에 도입했던 보안 장비들이 노후화되면서 기존 장비의 대체수요가 늘어나고 있다. 더 큰 트래픽을 처리할 수 있지만 결국 같은 기능을 하는 교체장비를 도입하는 것보다 1+1 기능을 장착한 신규장비를 도입하려는 추세가 보인다. 애플리케이션 레벨에서 트래픽을 제어할 수 있는 기능을 갖춘 차세대방화벽을 포함해 보안장비에서 발견된 이상징후를 한눈에 통합적으로 보여줄 수 있는 ESM, SIEM 등의 솔루션이 이것인데, 단순히 기존 네트워크에 이들 솔루션을 도입해서 운용하기보다 기존 네트워크를 운용하면서 쌓은 경험과 새로운 솔루션들을 이용해 차세대 보안 네트워크를 새로 구축하려는 움직임도 관측된다.

기존의 보안 프로세스에 감지되지 않는 새로운 보안위협은 계속 등장하고, 그 움직임을 보고 판단해 경보를 울리는 시스템은 계속하여 발전하기 마련이다. 신규 장비의 등장으로 이전에는 보이지 않던 영역까지 레이더망이 넓어졌지만, 그만큼 감시해야 할 영역이 넓어진 셈이다.

Part Ⅱ. 고 민

Part Ⅱ 1 "보안도 좋지만 일 좀 하자구요" 보안/생산성 절충점 찾기

망 분리를 통한 인터넷 망과 내부 망의 차단, USB 사용 금지, 개인 PC 보안장치 강화, MDM을 통한 사내 개인 휴대기기 기능제한 같은 조치를 통해 보안수준은 올라가지만 내부 직원의 불만 섞인 아우성도 터져 나온다. 보안도 좋지만 일은 하게 해주어야 할 것 아니냐는 볼멘 목소리를 보안부서가 듣기 십상이다. 처음부터 강력한 보안수준을 갖추고 일을 해서 원래 그러려니 했으면 모를까, 망치로 못을 박던 사람에게 이제 망치를 쓰지 말고 돌로 못을 박으라고 하는 셈이니 불만이 높아질 수 밖에 없다. 이미 망치의 유용함을 알아버렸는데 망치가 없던 시대로 돌아가라니...

보안부서도 나름 고충이 크다. 보안 자체가 현실과 타협할 수 있는 것이 아니고, 위협은 실제로 존재하는 것이며, 한 순간의 관리소홀이 정보유출로 이어지는 상황이니 말이다. 예방적인 조치라 하더라도 소홀하게 관리했다간 사고 발생시에 치명적으로 다가오기 때문에 어쩔 수 없다. 나무통

이야기나 쇠사슬의 강도 이야기에서도 알 수 있듯 조직의 보안 수준은 각 분야 중 가장 낮은 수준으로 귀결되는 것이고 보안활동은 어쩔 수 없이 약점을 보완하는 활동이 될 수 밖에 없다.

결국 보안강화에 있어 균형점을 찾아야 하며 이는 사내 보안인식 제고로 귀결된다. 불편한 것은 알고 있지만, 보안을 위해 어쩔 수 없이 그 불편함을 감수하게 하는 것이다. 그렇게 하기 위해서는 보안조직의 방침에 경영층이 힘을 실어주는 것도 필요하고, 타사의 사고사례를 제시하며 우리도 같은 사고를 당할 수 있음을 은근히 강조하는 것도 필요하다. 하지만 그 사고가 너무 잦다 보니 위협에 둔감해지는 것이 문제다.

'Security has its price'라는 말이 있다. 물론 일리가 있는 말이지만 그 'Price'가 감당하지 못할 수준으로 올라버리지 않을까 걱정이다.

Part Ⅱ 2 "갈수록 센 놈이 온다" 컴플라이언스

작년에도 3.20, 6.25로 온 나라가 떠들썩하더니 올해는 연초부터 카드사의 개인정보유출 사태로 제대로 발칵 뒤집혔다. 큼지막한 해킹, 정보유출사고가 일어날 때마다 새로운 제도와 규제, 처벌조항이 생긴 전례를 볼 때 이번에도 이 패턴에서 벗어나지 않을 것 같다. 법에서 명시된 기준은 그 내용을 전부 준수하기가 쉽지 않음에도 불구하고 법에서는 법 상 의무조치가 정보보호를 위한 최소한의 기준이라고 밝히고 있어 기업입장에서는 어느 수준까지 보호조치를 취해야 하는지 판단에 어려움을 겪고 있다.

또한 정보통신망법과 개인정보보호법 이외에도 통신비밀보호법, 신용정보법 등 정보보호와 관련된 다수의 법들이 존재하고 비슷한 내용에 대해 여러 법의 규제를 받는 중복규제의 문제도 상존하고 있기에 기업담당자들은 각 법에 대해 명확한 이해가 선행되지 않은 상태에서는 같은 일을 여러 번 반복하게 되는 상황에 직면하게 된다. 개인정보보호와 관련하여 일반법인 개인정보보호법이 제정되고 시행 된지 2년이 지났지만, 현장에서는 정보통신망법과 개인정보보호법의 차이에 대해 아직도 혼란스러워 하고 있다. 동일한 사안에 대해 서로 다른 기준을 제시하거나 동일한 위법사항에 대해 처벌수위가 다른 경우가 있어 개선 필요성이 계속 제기되었고, 실제로 두 법은 개정을 거듭하면서 서로 닮아가고 있는 중이다. 개정방향은 물론 규제/처벌 강화 쪽이다. 과징금 상한선을 올리고, 해킹으로 개인정보 유출사고 발생시 기술적·관리적 보호조치 미비가 발견되면 해킹과 인과관계가 확인되지 않더라도 과징금을 부과할 것이라는 방침 등이 그것인데 이 외에도 개인정보유출사고 발생시 정보보호 책임자뿐만 아니라 사안의 경중에 따라 아래로는 담당자, 위로

는 CEO까지 문책할 것이라 하니 보안담당자들은 바짝 긴장하고 있다.

규제일변도에서 벗어나 개인정보의 안전하고 가치 있는 활용을 목적으로 하는 빅데이터 산업을 발전시키겠다는 청사진이 나온 지 얼마 되지 않았는데 다시 찬바람이 불어오지 않을까 걱정된다. 꽃샘추위로 그치면 좋겠지만, 빙하기가 다가오는 것일지도 모르겠다.

Part Ⅱ 3 "내가 너를 어디까지 믿어야 할까?" 외주업체보안

2014년 정초부터 온 나라를 들었다 놨다 했던 신용카드사 개인정보유출사건. 금융권의 개인정보유출사고가 처음 발생한 것도 아니고, 외주인력에 의한 정보유출사고는 심심찮게 접해보았지만, 유출규모로만 세계 3위라고 하니 규모가 엄청나다.

외주업체보안은 정보보호 분야에서는 고질적인 고민에 해당한다. 이미 해킹방지워크샵과 같은 보안 컨퍼런스에서도 여러 번 다루어졌고 시시때때로 보안담당자들이 모여 어떻게 하면 외주/수탁업체로 인한 정보유출을 막을 것인지 고민에 고민을 거듭하지만 딱히 이거다 싶은 해답은 나오지 않는다. 법에 따르면 수탁업체의 과실로 정보유출사고가 발생하면 해당 직원을 위탁업체의 직원으로 간주한다고 하지만, 이것은 손해배상의 책임에 관한 규정일 뿐 수탁업체는 수탁업체이지 위탁업체의 내부조직이 아닌 것이다. 계약서나 SLA에 정보보호와 관련된 사항을 명시하고 주기적으로 정보보호 감사활동을 하는 것이 그나마 잘 하고 있는 경우에 해당하지만 이마저도 누수가 발생할 수 있는 포인트가 많은 것이 현실이다.

개인정보처리위탁이나 제3자 제공인 경우에 이용목적을 달성한 경우 지체 없이 해당 개인정보를 파기해야 하지만 위탁업체의 관리영역 밖에서 이루어지는 데이터 회수/파기를 어떻게 확신할 수 있을까. 보안점검을 나가도 서류점검을 실시하는 것 외에 실제 데이터가 파기된 것을 확인할 수 있을까? 전산을 들여다본다 해도 수탁사의 시스템을 꿰고 있지 않은 다음에는 어딘가 숨겨놓은 데이터를 찾아낼 리 만무하다. 또 해당 수탁사가 여러 위탁업체로부터 수탁을 받는 경우에는 타사의 정보가 노출될 수 있음을 이유로 제한적인 열람만을 허용할 경우도 있다. 수탁사가 위탁사보다 더 큰 규모의 기업인 경우 통상적인 갑을 관계가 성립하지 않을 수도 있다.

개발 외주의 경우에는 외주인력에 대한 최소작업권한 부여, 전산장비 반출입통제, 테스트 시 가상자료 사용 및 종료 시 자료삭제, 고객정보유출금지 등 비교적 잘 규정되어 있으나, 촉박한 프로젝트 일정, 실제상황과 비슷한 테스트 등을 위해 규정대로 적용되고 있지는 못한 실정이다.

이 모든 고민을 한 방에 해결해 줄 수 있는 방법은 앞으로도 나오지 않을 것이다. 하지만 보안담당자들이 자주 만나 함께 고민을 나누다 보면 더 나은 방법을 찾게 되고 그로 인해 조금씩이나마

개선될 수 있지 않을까.