특집 06

데이터 유출 발생 이유와 그 대처 방법

목 차

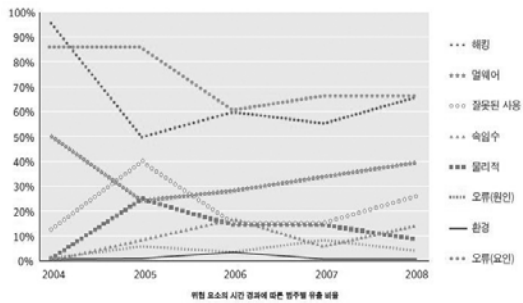
윤 광 택
(시만텍코리아)

1. 서 론

고객 데이터, 지적 재산, 영업 기밀, 독점 소유 데이터 등 중요한 정보 자산을 보유한 기업의 데이터 유출 위험성이 과거 어느 때보다도 높아지고 있다. 2008년에 발생한 전자 기록 유출 건수가 지난 4년간 발생한 총 건수보다 많을 정도다.

데이터가 도처에 존재하는 지금, 기업이 기밀 정보를 보호하는 일은 갈수록 어려워지고 있으며, 복잡한 이기종 IT 환경에서 데이터를 보호하고 위협 요소에 대처하기는 쉽지 않다. 그러나 오늘날 기업은 점차 증가하는 모바일 오피스 환경에서의 안전한 협업과 공유를 지원하고 보안을 보장하는 책임을 전적으로 보안 팀에게 맡기고 있는 상황이다.

끊임없이 발생하는 데이터 유출의 폐해는 지속적으로 강조되고 있으나 데이터 유출이 발생하는 이유 및 이를 방지하기 위한 조치에 관해서는 이해가 부족한 상황이다. 여기서는 데이터 유출의 대표적인 원인 세 가지, 즉 선의의 내부자, 외부로부터의 대상 지정 공격 및 악의적 내부자에 대해 소개하고 각 원인이 어떻게 데이터 유출로 이어질 수 있는지 조명한다. 또한 거시적 관점에서 데이터 유출을 막기 위한 대책과 예방 조치에 대해 알아본다.



(그림 1) 위협 요소의 시간 경과에 따른 범주별 유출 비율

2. 데이터 유출 및 그 영향

최근 기업이 보유한 고객상세정보나 기업 기밀 데이터와 같은 민감한 정보를 확보하려는 시도가 급증하고 있다. 2008년 시만텍은 고객 네트워크에 대한 바이러스 접근을 차단하기 위해 전 세계적으로160만개의 악성코드 시그니처를 생성했다. 바이러스는 대부분 정보를 빼돌려 금전적 이득을 취하기 위한 목적으로 개발된 것으로, 2008년에 시만텍이 생성한 시그니처 수는 지난

17년간 생성된 시그니처를 합한 것보다 더 많았다. 또한 새로 발견한 악성 프로그램 가운데 절반 이상이 기밀정보를 빼내기 위해 만들어진 것으로 분석됐다.

이와 함께 시만텍이 2009년 4월 발표한 '인터넷 보안 위협 보고서 제 14호'에 따르면 보안침해 및 온라인 범죄행위는 우려할만한 수준으로 증가했다. 2008년 한해 조직범죄단이 연루된 보안침해 사건 가운데 10건당 9건이 기업정보를 겨냥한 것으로 총 2억8500만 건으로 조사됐다. 이는 2004~2007년 2억3천만 건보다 증가한 것이다. 보안침해 사건 중 88%는 내부직원의 부주의 때문에 발생한 것으로 기업에 상당한 손실을 입힌 경우도 있었다. 지적재산권 도용으로 인한 피해액은 6억 달러에 달했다.

데이터 유출 위협이 기업에 미치는 영향을 파악하기 위해 IT 및 비즈니스 관리자들은 누가 어떻게 정보를 유출시켰고 그로 인한 피해규모는 어느 정도인지 알아야 한다. 예를 들어, 기업은 제대로 된 보안 정책을 수립했는지의 여부를 떠나서 직원들이 기밀 정보 보안의 중요성을 인식하고 있고, 그에 따라 행동하고 있을 것이라고 편하게 생각해서는 안된다. 한 조사기관에 따르면 2008년 데이터 유출사건의 3분의 2가 내부 직원의 고의성이 없는 '중대한 실수'로 인해 발생했다.

또한, 해킹을 의례히 심신이 성숙하지 못한 어설픈 십대들이 자기만족을 위해 기업 네트워크를 침범하는 행위로 인식하는 것은 지극히 위험한 구시대적 발상이다. 최근에는 기업의 기밀 정보를 빼내기 위해 사이버범죄자들이 조직적으로 공격에 가담하는 양상을 보이고 있다. 이 같은 지능형 공격은 기업의 감시망을 뚫고 정보를 해커사이트로 빼내는 악성 코드를 사용해 자동으로 실행될 수 있다.

3. 데이터 유출이 발생하는 이유

데이터 유출을 방지하려면 먼저 데이터 유출이 발생하는 원인을 규명할 필요가 있다. 데이터가 유출되는 근본 원인은 크게 선의의 내부자, 대상 지정 공격 및 악의적인 내부자 세 가지 유형으로 나뉜다. 대다수의 경우 이러한 요인들이 합쳐진 결과 데이터 유출이 발생한다. 예를 들어, 선의의 내부자가 실수로 보안 정책을 지키지 못해 대상 지정 공격이 가능해지고 그로 인해 데이터가 유출될 수 있다.

3.1 선의의 내부자

회사 직원이 실수로 데이터 보안 정책을 위반하는 경우가 여전히 데이터 유출 사고 중 상당 부분을 차지한다. 포네몬 인스티튜(Ponemon Institute)에서 데이터 유출 사고를 겪은 기업 43곳을 대상으로 실시한 설문조사에 따르면, 전체 사고 중 88% 이상이 직원 부주의에서 비롯되었다. 이 같은 선의의 내부자로 인한 데이터 유출은 크게 5가지 유형으로 나뉜다.

3.1.1 서버 및 데스크탑에서 노출된 데이터

제대로 보호받지 못한 서버, 데스크탑 및 랩탑에도 매일 기밀 정보가 급증하기 마련이다. 아마도 가장 보편적으로 발생하는 데이터 유출 유형은 데이터 보안정책을 숙지하지 못한 선의의 내부자가 암호화되지 않은 기밀 데이터를 저장, 전송하거나 복사하고 이를 해커가 포착하는 경우이다. 이 공격 유형에서는 바로 이러한 데이터를 악용한다. 데이터의 폭발적인 증가로 인해 오늘날 대부분의 기업은 해당 시스템에 얼마만큼의 기밀 데이터가 저장되었는지조차 알지 못한다. 해당 기업에서 미처 파악하지 못한 데이터가 저장된 시스템이 2008년의 전체 데이터 유출 중 38%를 차지했으며, 해당 레코드 중 67%가 유출되었다.

3.1.2 랩탑 분실 및 도난

2008년 포네몬 인스티튜트에서 실시한 조사에 따르면, 랩탑 분실이 데이터 유출 원인 중 1위를 기록했다.(조사대상 기업 중 35%) 랩탑 분실이

신원 도용으로 이어지지 않더라도 데이터 유출로 인해 기업의 이미지가 실추되고 상당한 비용 부담이 발생할 수 있다.

3.1.3 이메일, 웹 메일 및 이동식 장치

시만텍이 잠재 고객을 대상으로 실시한 리스크 평가에 따르면, 평균적으로 이메일 400개 중 1개에는 암호화되지 않은 기밀 데이터가 포함되어 있었다. 이 같은 네트워크를 통한 전송은 중대한 데이터 손실 위험을 초래한다. 전형적인 시나리오는 직원이 개인 이메일 계정으로 기밀 데이터를 전송하거나 주말에 작업하기 위해 메모리 스틱 또는 CD/DVD로 복사하는 것이다. 이 경우 전송 과정에서 그리고 제대로 보호받지 못한 가정용 시스템에서 데이터가 공격에 노출될 가능성이 있다.

3.1.4 써드파티 데이터 손실 사고

써드파티 비즈니스 파트너 및 벤더와의 비즈니스 관계상아웃소싱 지급 처리, 공급망 주문 관리와 같은 다양한 유형의 운영 데이터를 비롯한 기밀 정보를 주고받아야 하는 경우가 많다. 데이터 공유의 범위가 지나치게 넓거나 파트너가 데이터 보안 정책을 준수하지 않을 경우 데이터 유출의 위험성이 증가한다.

3.1.5 비즈니스 프로세스로 인한 기밀 데이터 자동 배포

기밀 데이터의 양이 급증하는 이유 중 하나는 적합하지 않거나 오래된 비즈니스 프로세스로 인해 권한 없는 개인 사용자 또는 보호되지 않는 시스템으로 데이터가 자동 배포되기 때문이다. 이렇게 배포된 데이터는 해커가 손쉽게 수집하거나 악의적인 내부자가 도용할 수 있다. 시만텍에서 실시한 리스크 평가에 따르면, 위와 같은 사례 중 절반 가량은 오래되었거나 허가받지 않은 비즈니스 프로세스를 통해 기밀 데이터가 노출될 수 있다.

3.2 대상 지정 공격

오늘날처럼 모든 곳에 데이터가 존재하고 어디서나 연결되는 네트워크 환경에서 지능적인 해킹 기술로부터 정보 자산을 보호하기란 결코 쉽지 않다. 조직적인 사이버 범죄가 기승을 부리는 가운데 신원 도용 목적으로 정보를 훔쳐내는 대상 지정 공격이 늘고 있다. 이러한 공격은 제대로 보호받지 못하는 기업에 침투하여 데이터를 해커 사이트로 보내는 악성 코드에 의해 자동으로 이루어지곤 한다. 2008년에 시만텍은 160만 개가 넘는 악성 코드 시그니처를 새로 작성했으며, 이는 지난 17년간 작성한 것보다 많은 양이다. 또한 전 세계에서 매월 평균 2억 4,500만 건이 넘는 악성 코드 공격 시도를 차단했다.

손상된 레코드 수를 기준으로 할 때, 가장 자주 발생한 해킹 유형은 기본 또는 공유 인증 정보를 이용한 무단 액세스, 부적절하게 제한된 액세스 제어 목록(ACL) 및 SQL 인젝션 공격이었다. 뿐만 아니라 손실된 레코드의 90%는 멀웨어 감염이 주 원인이었다. 공격의 첫 단계인 초기 침투는 주로 다음 세 가지 방법을 통해 이루어진다.

3.2.1 부적절한 인증 정보

이메일, 웹 또는 FTP 서버와 같은 인터넷 연결 시스템의 암호가 초기 설정값 그대로 남아 있는 경우가 많으며, 이 경우 해커가 이를 손쉽게 획득할 수 있다. 제대로 제한되지 않거나 오래된 ACL은 해커와 악의적인 내부자 모두에게 절호의 기회를 제공한다.

3.2.2 SQL 인젝션

해커는 대상이 된 웹 사이트의 URL 구문을 분석하여 멀웨어를 업로드하는 명령을 포함시킴으로써 대상 서버를 원격으로 액세스할 수 있게 된다.

3.2.3 대상 지정된 멀웨어

해커는 알려진 기업에서 보낸 합법적인 통신으로 가장하여 이메일을 전송하지만, 실제로는 사용자를 다른 사이트로 연결시켜 자동으로 멀웨어를 다운로드하게 한다. 이 멀웨어에는 원격 액세스 툴이 포함되어 해커가 사용자 컴퓨터를 원격 제어할 수 있게 된다.

대부분 보안 팀은 오직 침투를 차단하여 데이터를 보호하려고 한다. 그러나 침투는 대상 지정 공격에 의한 데이터 유출의 첫 단계일 뿐이다. 철저한 데이터 보호를 위해서는 다음의 4단계를 모두 해결해야 한다.

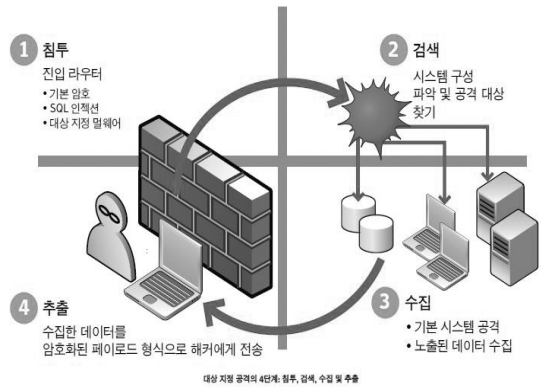
1단계: 침투 - 해커가 기본 암호 해독, SQL 인젝션 또는 대상 지정 멀웨어를 사용하여 회사의 네트워크에 침투

2단계: 검색 - 해커 팀이 회사의 시스템 구성을 파악하고 자동으로 기밀 데이터를 검사

3단계: 수집 - 선의의 내부자가 보호되지 않는 시스템에 저장한 데이터 즉시 수집. 또한 루트킷이라는 구성요소가 대상 시스템 및 네트워크 액세스 지점에 비밀리에 설치되어 사내를 돌아다니면서 기밀 데이터를 수집

4단계: 추출 - 기밀 데이터가 일반적인 형태(예: 웹 메일)나 암호화된 패킷 또는 암호로 보호되는 압축 파일에 통합된 형태로 해커 팀에게 전송

다행히 기밀 데이터에 대한 대상 지정 공격은 이 네 단계 중 어느 한 단계에서만 방어하면 된다. 침투 단계에만 주력하는 보안 전문가는 모 아니면 도 식의 내기를 하는 셈이며, 오늘날처럼 모든 것이 열려있는 정보 환경을 감안할 때 언젠가는 실패할 수 밖에 없다. 반면 데이터 검색, 수집 및 추출 단계에 대한 예방 조치를 취한다면 대상 지정 공격에 대한 방어 체계를 크게 강화할 수 있다.



(그림 2) 대상 지정 공격의 4단계: 침투, 검색, 수집 및 추출

3.3 악의적인 내부자

악의적인 내부자로 인한 데이터 유출이 크게 늘어나는 가운데 그러한 유출 사고로 기업이 부담하는 비용 또한 증가하고 있다. 포네몬의 조사에 따르면, 직원의 부주의로 인한 데이터 유출은 레코드당 199달러의 비용을 발생시키는 데 비해, 악의적 행동에서 비롯된 유출은 레코드당 225달러의 비용을 발생시킨다. 정보를 도용할 목적으로 내부자가 저지르는 데이터 유출은 다음 네 범주로 나눌 수 있다.

3.3.1 화이트 칼라 범죄

신원 도용 조직에 가담한 직원이 고의로 데이터를 훔치는 경우로, 대표적인 화이트 칼라 범죄 중 하나로 자리잡았다. 이러한 범죄는 회사 내부자가 사적인 이익을 위해 정보 접근 권한을 남용하면서 발생한다.

3.3.2 해고된 직원

경제 위기로 해고가 늘어나면서 불만을 품은 퇴사자가 데이터를 유출하는 경우도 늘어났다. 메일 계정 접근권한이 종료되기 전에 해고가 통보되는 경우 해고된 직원이 기밀데이터에 액세스하여 개인 이메일 계정으로 보내거나 이동식

미디어에 복사할 기회가 생긴다. 최근 직원 해고가 데이터 보안에 미치는 영향을 분석한 포네몬 조사 결과에 따르면, 퇴사자 중 59%는 고객 목록, 직원 기록과 같은 회사 데이터를 유출했다.

3.3.3 경력 개발에 회사 데이터 이용

직원이 향후 경력 기회에 활용하고자 회사 데이터를 홈 시스템에 저장하는 경우가 빈번하다. 그러한 행위를 신원 도용처럼 심각한 악의적 의도로 간주하지는 않더라도 만만치 않은 피해를 가져올 수 있다.

3.3.4 산업 스파이

악의적 내부자의 마지막 유형은 불만을 품거나 실적이 좋지 않은 직원이 경쟁사로 이직하기 위해 본인의 작업 파일을 경쟁사에 전달하는 것이다. 제품 정보, 마케팅 계획, 고객 목록 및 재무 데이터가 이런 방식으로 악용될 수 있다.

데이터 유출 사고 소식이 거의 매일 헤드라인을 장식하는 가운데, 데이터 유출을 네트워크 환경의 필연적인 부산물, 즉 비즈니스 활동에서 반드시 치러야 하는 비용으로 간주하는 사람들도 있지만 데이터 유출은 충분히 예방할 수 있다. 앞서 소개한 데이터 유출 시나리오 각각에는 주요 개입 지점이 존재하며, 그러한 지점에서 대응책이 마련되어 있었다면 유출을 막을 수 있었을 것이다.

4. 데이터 유출을 막는 방법

IT 인프라스트럭처 전반에서 사내외 위협 요소로부터 정보를 보호하고 시스템을 모니터링하려면 운영 보안 모델 기반 솔루션, 즉 리스크를 기초로 컨텐트를 인식하면서 실시간으로 위협 요소에 대응하며, 워크플로에 기반하여 데이터 보안 프로세스를 자동화하는 솔루션을 선택해야 한다. 조직은 검증된 솔루션을 사용하여 다음 6단계를 거쳐 데이터 유출의 위험성을 크게 줄일 수 있다.

1단계: 정보를 사전에 보호 - 오늘날의 네트워크 환경에서 더 이상 주변부 방어만으로는 충분하지 않다. 이제는 가장 중요한 정보가 어디에 저장 또는 전송되거나 사용되든지 간에 그 정보를 정확하게 파악하고 사전에 보호해야 한다. 전사적으로 서버, 네트워크 및 엔드포인트 전반에 걸쳐 통합 데이터 보호 정책을 시행함으로써 데이터 유출의 위험성을 점진적으로 줄일 수 있다. DLP(Data Loss Prevention) 솔루션은 이러한 통합적인 방식을 실현시킬 수 있는 데이터손실방지 솔루션이다.

2단계: 중요한 데이터에 대한 액세스 권한 검토 절차를 자동화 - 데이터 유출은 종종 멀웨어를 이용하여 데이터를 찾아내고 내보내는 대상 지정 공격에서 발생한다. 또한 부적절한 인증 정보 사용은 그러한 공격을 가능하게 하는 대표적인 원인이다. 암호 및 기타 권한 제어 수단을 정기적으로 자동 점검함으로써 그러한 유출의 위험성을 줄일 수 있다. 뿐만 아니라 퇴사하는 직원의 권한을 적시에 해제하지 못하는 것도 악의적 내부자에 의한 데이터 유출을 일으키는 대표적인 원인이다. 액세스 권한 검토 과정을 자동화한다면 그러한 유출을 사전에 방지할 수 있다. 설문 조사 도구, 제어 수단 평가 자동화 및 보안 이벤트 관리 솔루션을 활용하면 액세스 권한 남용으로 인한 데이터 유출을 막을 수 있다.

3단계: 실시간 알림과 글로벌 보안 인텔리전스를 연계하여 위협 요소 파악 - 대상 지정 공격 위협요소를 식별하고 대처하기 위해 보안 정보 및 이벤트 관리 시스템에서 의심스러운 네트워크 활동을 조사 대상으로 지정할 수 있다. 그러한 실시간 알림은 특히 해당 정보가 실제로 알려진 위협 요소 관련 지식과 연계될 때 더욱 진가를 발휘한다. 전 세계의 보안 위협 요소에 관한 최신 정보와 분석 결과를 실시간으로 활용할 수 있다면 보안 팀이 외부 위협

요소를 퇴치하는 데 큰 보탬이 될 것이다.

4단계: 대상 지정 공격에 의한 침투를 차단: 해커들이 회사 네트워크 침투에 가장 많이 이용하는 세 가지 방법은 기본 암호해독, SQL 인젝션 및 대상 지정 멀웨어다. 침투를 방지하려면 기업 정보 자산을 노리는 이러한 각각의 수법을 차단해야 한다. 제어 평가 자동화, 코어 시스템 보호 및 메시징 보안 솔루션을 결합하여 활용함으로써 대상 지정 공격을 막을 수 있다. 또한 엔드포인트를 중앙에서 관리하면서 보안 정책, 암호화 기능 및 정보 액세스를 일관성 있게 배포해야 한다.

5단계: 데이터 추출 방지 - 해커의 침투가 성공했더라도 네트워크 소프트웨어에서 기밀 데이터 추출을 탐지하여 이를 차단한다면 데이터 유출을 막을 수 있다. 내부자의 유출도 파악하여 차단할 수 있다. DLP 및 보안 이벤트 관리 솔루션을 결합하여 아웃바운드 전송 단계에서 데이터 유출을 방지할 수 있다.

6단계: 예방 및 대응 전략을 통합하여 보안 운영에 적용 - 데이터 유출을 방지하려면 보안 팀의 일상 업무에 유출 방지 및 대응 계획을 통합시켜야 한다. 보안 팀은 정보 모니터 및 보호 기술을 활용하면서 끊임없이 계획을 업그레이드하고, 지속적으로 확장되는 위협 요소 및 취약점 관련 지식 기반에 기초하여 점진적으로 리스크를 줄일 수 있어야 한다.

5. 결 론

지금까지 살펴본 것처럼 데이터 유출을 예방하고 대응 계획을 수립하기 위해서는 먼저 보호해야 할 기밀 데이터의 유형을 파악하고 그 정보를 바탕으로 보안 리스크를 평가해야 한다. 대부분의 기업에서 이 프로세스는 리스크 평가부터 시작된다. 이때 시만텍 데이터 손실 리스크 평가와 같은 서비스를 이용하면 기밀 정보를 신속하게 파악하고 데이터 유출 리스크를 정확하게 분석하여 리스크의 우선순위를 결정하고 데이터 유출방지 및 대응계획을 수립하는데 도움이 될 것이다.

참고문헌

[1] 2009 Data Breach Investigations Report (2009 데이터 유출 조사 리포트)

[2] Ponemon Institute 2008 Annual Study (포네몬 인스티튜트 2008 연간 보고서)

[3] Symantec Internet Threat Report v.14 (시만텍 인터넷 위협 보고서 14호)

[4] Symantec Data Loss Prevention Risk Assessments (시만텍 데이터 손실 방지 리스크 평가)

저자약력

윤 광 택

1996년 단국대학교 졸업
1996년~2000년 한라건설 해외영업부
2000년~2004년 데이타게이트 엔지니어
2004년~현재 시만텍 보안 전문가
관심분야 : 정보 보안
이 메 일 : patrick_youn@symantec.com