당신의 정보를 지켜라
개인정보보호기술의 현황과 전망

몇 달 전 발생했던 옥션의 개인정보 해킹 사건 등에서 볼 수 있듯이 개인정보는 한번 유출되면 명의도용 등으로 악용될 수 있어 기업뿐만 아니라 해당 정보의 주체인 일반 이용자에게까지 정신적·경제적 피해를 야기할 수 있다. 최근 개인정보 유출 사고는 내부자의 고의적 범죄, 관리 부주의 등에서 외부인의 악의적 해킹에 의한 기술적 침해로 진화하고 있다. 이에 따라 개인정보보호 기술(PET, Privacy Enhancing Technologies)이 그 어느 때보다 중요해지고 있다.

개인정보보호 기술의 중요성

전통적으로 프라이버시는 타인의 방해를 받지 않고 개인의 사적 영역을 유지하고자 하는 이익 또는 권리를 의미한다. 프라이버시가 남에게 알리고 싶지 않은 사적 사항 전체의 보호를 의미하는 광의의 개념이라면, 개인정보보호는 개인의 정신, 신체, 재산, 지위, 신분 등 개인에 관한 구체적 정보를 보호하는 협의의 개념을 지칭한다. 최근 IT의 급속한 발전과 함께 인터넷 등 정보통신망에서 처리·관리·유통되는 개인의 성명, 주민번호, 전화번호, 계좌번호 등 개인정보를 안전하게 보호하기 위한 기술적 방안들이 도입되고 있으나 개인정보보호가 본질적으로 기업보다는 개인정보의 주체인 이용자를 보호하기 위한 목적이 더 큰 만큼 그 동안 기술보다는 법·제도적 보호방안의 비중이 더 컸던 것이 사실이다. 하지만, 최근 들어 급증하고 있는 개인정보 해킹사고로 인하여 개인정보보호 영역에서도 기술적인 보호수단의 중요성이 점차 커지고 있다.

일반적인 정보보호 기술이 기업의 중요 자원인 정보(information)를 안전하게 보호하고 활용하기 위한 기밀성, 무결성, 가용성을 보장하기 위한 것인데 반해 개인정보보호 기술은 기업이 아니라 정보 주체인 이용자의 권익을 보호하는 것을 목적으로 한다. 따라서 개인정보보호 기술은 이용자의 자기정보 통제권을 보장하기 위한 법·제도적 정책을 바탕으로 발전되고 있다고 볼 수 있다. 아울러, 기술적인 측면에서 기존의 정보보호 기술이 개인정보의 보호를 위해 사용되면서 제도와 기술이 융합된 형태의 개인정보보호 기술들이 속속 등장하고 있다. 최근 주목받고 있는 개인정보보호 관련 대표적 기술들을 소개하면 다음과 같다.

▶▶ 주민등록번호 대체수단

우리나라 국민이라면 누구나 가지고 있는 고유불변, 일신종속적인 정보가 바로 주민등록번호이다. 그러다 보니 주민등록번호 유출로 인한 각종 명의도용, 신분증 위조, 대포폰 등 크고 작은 침해사고가 끊이지 않고 있다. 이러한 주민등록번호를 최소한 인터넷 환경에서라도 사용하지 않도록 보호하기 위한 기술이 바로 주민등록번호 대체수단이다. 현재 민간분야의 주민등록번호 대체수단으로 i-PIN(아이핀)이 시행 중에 있는데 i-PIN은 미리 지정된 대체수단 발급기관으로부터 공인인증서, 휴대전화 인증 등을 통해 본인확인 절차를 거친 뒤 주민번호와 같은 길이인 13자리의 가상 식별번호를 발급받아 사용하는 것을 말한다. i-PIN은 주민등록번호와 달리 원하는 경우에 얼마든지 변경할 수 있어 유출로 인한 추가 피해를 방지할 수 있다는 장점이 있다. 공공분야에서는 이와 유사한 G-PIN 제도가 시행 중에 있다.

▶▶ 개인정보취급방침의 전자적 표시

인터넷사업자 등 정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우에 그 목적, 보유기간 등에 관한 내용을 포함한 개인정보취급방침을 이용자에게 반드시 고지하여야 한다. 그러나 텍스트 형태의 기존 고지 방식은 분량이 많아 이용자가 내용을 정확히 읽지 않는 경우가 대부분이었다. "개인정보취급방침의 전자적 표시"는 이러한 문제점을 개선하기 위한 기술이다. 인터넷사업자는 "개인정보취급방침의 전자적 표시" 소프트웨어를 통해 개인정보취급방침의 내용과 형식을 표준화하여 고지하고 웹사이트 이용자는 전자적 표시를 자동 인식하는 에이전트 소프트웨어를

네이버는 바이러스 및 악성코드의 실시간 탐지 및 검사, 치료 기능을 제공하는 무료 보안 서비스 'PC그린'을 시작했다.

싸이월드가 개인정보 보호 기능을 한층 강화하기 위해 로그인시 휴대폰으로 매번 새로운 1회용 비밀번호를 부여받는 '모바일 OTP(비밀번호생성)' 서비스를 시작했다.

통해 개인정보취급방침 내용을 일일이 읽지 않더라도 핵심적인 사항들을 이미지 등으로 손쉽게 확인할 수 있다. 정부는 "개인정보취급방침의 전자적 표시" 제도 도입의 안정화를 위해 2007년 7월부터 웹사이트를 통해 개인정보취급방침 고지 시 전자적 표시를 반드시 병행하도록 법적 근거를 마련하였다. 국제적으로는 W3C(World Wide Web Consortium)에서 유사한 기술을 P3P(Platform for Privacy Preferences)라는 명칭으로 표준화하여 보급 중에 있다.

▶▶ 개인정보 전송구간 암호화

인터넷 등 정보통신망을 통해 개인정보를 전송하거나 전송받는 경우 패킷스니핑(Packet Sniffing)이나 MITM(Man In The Middle) 등 가로채기 공격을 당할 수 있다. 이러한 사고를 예방하기 위해 전송구간에서 개인정보를 암호화함으로써 가로채기로 인한 유출 시에도 개인정보 식별이 불가능하도록 하는 기술이며 통상 보안서버를 통해 이를 수행하게 된다. 보안서버는 별도의 하드웨어 장치가 아니라 기존에 운영 중인 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나 별도의 암호화 기능을 추가하는 소프트웨어적인 방식으로 구축하게 된다. 보안서버는 인터넷상에서 개인정보를 암호화하여 안전하게 전송하기 위한 기본적 수단으로서 정부는 법제화를 통해 개인정보를 수집하는 모든 웹사이트에 보안서버 설치를 의무화하고 있다.

▶▶ 피싱 탐지 및 차단 기술

피싱(Phishing)이란 "개인정보(private data)를 낚시(fishing)하듯 낚아챈다"는 의미에서 유래되었다. 피싱은 보통 유명한 금융기관 등을 사칭하여 메일을 보내 수신자들로부터 개인정보나 금융정보를 얻어내 금전적 이득을 목적으로 악용하는 범죄행위이다. 피싱 대응 기법은 피싱메일 내부에 존재하는 하이퍼링크를 불허하는 방법이 기본적이었으나 최근 악성코드를 이용해 이용자 PC의 도메인 정보를 조작하는 파밍(Pharming)이나 VoIP를 이용한 비싱(Vishing) 등 지능적인 공격기법이 등장하고 있어 이에 대한 대응 기술들이 연구되고 있다.

▶▶ 원타임 패스워드(OTP : One Time Password) 인증

해킹이나 악성코드에 의해 패스워드가 유출되는 경우 악의적인 접근 및 개인정보 유출 등이 가능해진다는 문제점이 있다. 원타임 패스워드 인증은 로그인 시 매 회 패스워드를 변경하는 일회용 암호 방식으로서 패스워드가 유출되더라도 악의적 접근을 방지할 수 있는 보다 안전한 패스워드 체계이다. 현재 국내에서는 금융권을 중심으로 계좌이체 등에 보안카드 대신 원타임 패스워드 활용이 증가하고 있으며 일부 온라인게임 등에서도 원타임 패스워드 인증 서비스를 지원하고 있다. 원타임 패스워드 솔루션은 서버와 클라이언트 간의 암호화 동기방식에 따라 시간 동기화 방식, 이벤트 동기화 방식, 질의응답 방식, 혼합 방식 등 크게 4가지로 구분이 가능하다.

▶▶ 이동식 저장매체를 통한 유출 방지

이동식 저장매체란 USB, PDA, 이동식디스크 등 휴대할 수 있는 저장매체를 말한다. 이동식 저장매체를 통한 정보 유출 방지를 위해서는 일반적으로 프로그램이 메모리에 상주하고 있다가 복사가 이뤄지는 것을 모니터링하여 이를 중단시키거나 관리자에게 복사 행위를 통보하게 된다. 또는 하드웨어적으로 저장매체의 착탈을 감시하는 시스템도 있다.

▶▶ 키보드 보안 기술

키보드 보안은 전자상거래 등 온라인 정보 교환 시 PC의 키보드로 이용자가 입력하는 패스워드 등 입력정보를 키로거(keylogger) 등 키보드 해킹을 통해 가로채는 것을 막기 위한 기술이다. 키보드 보안은 기존의 SSL(Secure Socket Layer) 기술을 키보드에까지 연장시킨 기술로서 금융권 등을 중심으로 널리 사용 중에 있다. 주요 기능은 키로거 공격 무력화, 스파이웨어 무력화, 키보드 입력 유출모듈 동작 시 자동 알림 등이 있다.

개인정보보호 기술의 향후 전망

현재까지 국내외적으로 다양한 형태의 개인정보보호 기술 연구가 진행되어 왔으나 개인정보보호 기술에 대한 본격적 · 체계적 분석은 거의 이루어지지 않고 있는 것이 현실이다. 이는 앞서 지적했듯이 개인정보보호 기술이 법제도 등 정책에 후행한다는 특징과 일반적인 정보보호 기술을 근간으로 하고 있어 따로 구별하기 어렵다는 점 등에 기인한다고 할 수 있다. 하지만, 최근의 해킹 등 침해사고 경향이 개인정보 탈취를 통한 금전적 이득 목적인 경우가 증가하고 있어 개인정보보호를 위한 기술 분석 등 점차 그 영역이 구체화되고 있다. 향후에는 개인정보의 생명주기(수집 · 저장 · 이용 · 제공 · 파기 등 일련의 과정)별로 보호기술이 체계적으로 정리되고 이에 따른 개인정보보호 기술이 개발되어 점차 독자적 영역을 형성해 나갈 것으로 예상된다.

개인정보를 안전하게 지키기 위한 주의사항

앞서 예로 든 옥션의 개인정보 유출 규모는 1천만 건 이상인 것으로 알려져 있다. 이 정도면 국내 인터넷 이용인구를 약 3천4백만 명으로 추정했을 때(2007 한국인터넷백서, 한국인터넷진흥원) 약 3분의 1에 육박하는 어마어마한 규모다. 현재, 피해자들을 중심으로 대규모 손해배상 소송이 진행 중이라고 하니 해당 기업에 미치는 유무형의 손실이 엄청날 것으로 예상된다. 사실 이번 사건 뿐만 아니라 그간 국내 기업들이 이용자 개인정보를 사유재산처럼 취급하고 소홀히 다루어 왔던 면이 컸다는 점을 생각해 보면 앞으로는 개인정보를 우습게보다가 그야말로 큰 코 다칠 수 있는 현실이 온 것이다.

기업 입장에서는 위에서 소개했던 여러 기술 외에도 기본적인 정보보호에 대한 기술적 · 관리적 보호체계를 이번 기회에 재정비하는 것도 필요할 것이다. 하지만, 보다 근본적인 처방은 개인정보가 기본적으로 기업의 자산이 아님을 깨닫는 것이다. 개인정보는 기업이 이용자로부터 잠시 빌려서 쓰고 있는 것일 뿐 결코 기업의 자산이 아니다. 빌린 물건을 안전하게 보호하고 다 쓰고 나면 원래 주인에게 돌려주는 것(수집목적을 달성했거나 서비스 계약이 끝난 경우 해당 개인정보는 반드시 파기하여야 함)은 당연한 일이다. 그보다 더 좋은 일은 개인정보를 가급적 많이 빌리지 않는 것이다. 우리나라의 인터넷사업자들은 유독 많은 개인정보를 요구한다. 주민등록번호는 기본이고 심지어 결혼유무, 연봉수준까지 요구하기도 한다. 외국의 유명 포털사이트가 이메일 주소와 비밀번호 정도만을 요구하는 것에 비하면 과도해도 한참 과도하다. 과도한 개인정보 수집은 사실 관행적으로 이뤄져 왔던 측면이 큰 만큼 지금부터라도 개선되어야 할 것이다.

이용자 입장에서는 무분별한 웹사이트 가입을 자제해야 할 것이다. 특히, 인터넷상에서 벌어지는 각종 이벤트와 경품행사 등에 함부로 응하는 일이 없어야 한다. 대개 개인정보의 무단 수집이나 제3자 제공은 경품행사 등으로 이용자를 현혹하여 벌어지는 일이 많다. 아울러, 위에서 소개한 주민등록번호 대체수단, 개인정보취급방침의 전자적 표시, 원타임 패스워드 등을 적절히 활용하는 지혜가 필요하다.

안철수연구소

AhnLab

국내 보안 업계 선두주자

안철수연구소(대표 오석주, www.ahnlab.com)는 1995년 3월 창립된 국내 백신 전문 기업으로 최근들어 글로벌 통합보안 솔루션 개발 기업으로 성장하고 있다. 통합보안솔루션과 통합보안 관리 솔루션을 비롯해 안티바이러스 V3 제품군, 악성 코드 사전 방역 서비스, 보안 ASP 등 정보 네트워크 시대 최적의 보안솔루션을 개발 공급한다. 또한 정보통신부지정 정보보호 컨설팅 전문업체로서 보안컨설팅도 제공하고 있다.

최근 개인 정보 유출 등 사용자의 안전과 재산을 위협하는 등의 보안 문제가 사회적 이슈로 대두되면서 안철수연구소는 이에 발맞춰 '종합주치의' 개념의 고품격 온라인 보안 서비스(V3 365 클리닉)를 세계 최초로 선보였다. 종합적인 보안소프트웨어와 서비스를 웹 기술을 통해 고객 밀착형 플랫폼으로 제공한다는 면에서 세계 최초의 모델이다.

소프트웨어로 개인정보보호, 바이러스 스파이웨어 해킹 등 보안 문제 해결은 물론 장애 조치, 문서 편집 등 초보 수준의 PC 활용법까지 서비스를 받을 수 있다. 또한 신종 보안 공격에 실시간 대응할 수 있는 24시간 365일 긴급 대응 인프라에 의해 서비스된다는 점이 장점이다.

안철수연구소는 세계적 수준의 보안 전문가들로 구성된 전담 조직이 전 세계의 보안 위협 발생 현황을 모니터링하고 대응 기술을 개발하고 있다.

잉카인터넷

게임 보안 솔루션 1위 업체

잉카인터넷(대표 주영흠, www.inca.co.kr)은 온라인 보안 솔루션 엔프로텍트(nProtect)를 개발해 지난 2006년 회사설립 6년 만에 100억 원의 매출을 돌파하는 등 고공 성장을 계속하고 있다. 엔프로텍트 제품군은 인터넷뱅킹과 쇼핑몰, 게임 등 인터넷서비스 사용자 보호를 위한 대표적인 제품으로 유명하다. 주요 제품은 '엔프로텍트 네티즌'과 '엔프로텍트 게임가드', '엔프로텍트 엔터프라이즈'를 들 수 있다.

엔프로텍트 네티즌은 바이러스·해킹툴 등 각종 악성프로그램을 자동 진단·치단하고, PC 보안을 위한 기능을 제공한다. 현재 국민은행을 비롯 13개 금융사이트에서 제공되고 있다.

엔프로텍트 게임가드는 악성프로그램, 해킹툴 등 정보해킹위협을 차단, 게임데이터를 보호하는 온라인게임보안솔루션이다. 엔씨소프트의 '리니지', 웹젠의 '뮤 온라인', 그라비티의 '라그나로크' 등 게임에 적용, 게임보안분야 대표 솔루션으로 자리잡았다.

이밖에 기업용통합 PC보안 솔루션인 '엔프로텍트 엔터프라이즈'를 통해 시장 공략에 나서고 있다. 잉카인터넷은 올해 게임보안, PC통합보안솔루션을 통해 넓힌 인지도를 바탕으로 해외 시장을 적극 개척하는 데 총력을 기울일 계획이다. 이미 일본 금융 시장에 40여 개의 레퍼런스를 확보한 상태이며 올 하반기 구체적인 모델을 선보일 예정이다.

미래테크놀로지

금융권 OTP 전문업체

OTP(일회용비밀번호)는 1회에 한해 사용할 수 있는 비밀번호 시스템으로 매번 다른 비밀번호를 이용하여 사용자를 인증하는 방식이다. 주요 시중 은행들은 인터넷뱅킹 사용자 보안 강화를 위해 단말기(토큰형, 카드형) 형태의 OTP 서비스를 실시하고 있다. OTP 전문업체 미래테크놀로지(대표 정균태)는 이같은 OTP 단말기를 개발·공급하는 회사로 이 분야에서 정상을 달리고 있다. 지난 7년간 150만개의 OTP를 금융권에 공급했고 특허만 17개를 보유하고 있다.

이 회사는 현재 타임방식의 OTP 카드를 공급하는 유일한 업체이다. 이를 기반으로 만들어진 카드형 OTP는 제품 소형화, LCD화면 및 글자 크기의 확대, 연결고리 부착 등 사용자의 편의성을 고려한 최상의 제품이다. 지난해 금융권 OTP 시장에서 기존 은행권 고객들을 기반으로 14개의 은행에 OTP솔루션을 공급했다. 또 8곳의 증권사를 포함, 총 22곳으로 가장 많은 사이트를 확보하며 시장 주도권을 잡았다. 이 같은 금융권의 OTP 수요증가로 미래테크놀로지는 올해에도 신제품을 내세워 적극 공략할 계획이다.

최근 개인정보보안을 더욱 강화하는 기술(HSM+OTP)을 개발해 특허 등록을 마쳤다. 또한 지난해 OTP가 메모리 해킹에 취약한 사실이 밝혀진 이후, 메모리해킹을 막기 위한 기술 관련 특허도 출원했다.