

보도시점 2025. 7. 24.(목) 12:00
(2025. 7. 24.(목) 석간)

배포 2025. 7. 23.(수) 18:00

개인정보위, 랜섬웨어 등으로 개인정보가 유출, 삭제된 2개 사업자 제재

- 개인정보처리자는 운영중인 서비스 취약점 점검 및 보안업데이트 실시 등 필요
- 특히, SSL-VPN 장비 취약점을 악용한 개인정보 유출 증가 추세로 주의 필요

개인정보보호위원회(위원장 고학수, 이하 ‘개인정보위’)는 7월 23일(수)에 제16회 전체회의를 열고, 개인정보 보호 법규를 위반한 (주)해성디에스와 (재)전남테크노파크에 총 4억 4,460만 원의 과징금·과태료를 부과하고 홈페이지 등에 이를 공표하도록 명령하였다.

* (주)해성디에스(반도체 부품 등을 제조하는 회사) : 과징금 3억 4,300만 원, 결과 공표명령
(재)전남테크노파크(중소·중견기업을 지원하기 위해 정부·지자체·민간이 공동 출연하여 설립한 비영리 법인) : 과징금 9,800만 원, 과태료 360만 원, 결과 공표명령

개인정보위는 유출신고에 따라 관련 조사에 착수하였으며, 각 사업자에 대한 구체적인 위반 내용과 처분 결과는 다음과 같다.

< (주)해성디에스 : 과징금 3억 4,300만 원 부과, 공표명령 >

신원 미상의 해커는 (주)해성디에스가 운영 중인 SSL-VPN*장비의 취약점**을 악용하여 VPN에 로그인 후 사내망에 접근('23.10.11.~10.29.)하였다. 이후 내부 파일서버에 저장되어 있던 73,975명의 개인정보(주주 정보, 임직원 정보, 협력사직원 정보)를 외부로 유출하고, 내부 파일서버 등에 랜섬웨어*** 파일을 배포 및 감염시켰다.

* SSL-VPN(Secure Sockets Layer-Virtual Private Network) : 인터넷과 같은 공용 네트워크에서 안전하고 암호화된 연결을 제공하는 가상 사설망 기술

** 인증되지 않은 공격자가 웹에 노출된 SSL-VPN 인터페이스를 통해 원격으로 코드를 실행할 수 있는 취약점

*** 해커가 컴퓨터 시스템이나 데이터 등을 암호화한 뒤 정상적인 사용을 위해 필요한 복호화 키(Key)를 조건으로 일종의 돈을 요구하는 악성코드의 한 종류

조사 결과, (주)해성디에스가 사용하던 SSL-VPN 장비의 취약점이 발견되어 보안 업데이트가 필요하다는 사실이 해당 장비 제조사 및 한국인터넷진흥원 등에 의해 공지되었음('23.6.12.)에도, (주)해성디에스는 해킹 사고 당시까지 취약점에 대한 조치를 하지 않은 사실이 확인되었다. 아울러, 해커가 유출을 진행하던 '23.10.11.~10.29. 기간 동안 (주)해성디에스의 일부 시스템은 백신 동작 이력이 존재하지 않는 등, 악성프로그램 방지·치료 기능 운영 소홀 사실도 확인되었다.

개인정보위는 안전조치 의무 위반으로 개인정보가 유출된 (주)해성디에스에 과징금 3억 4,300만 원을 부과하고, 처분받은 사실을 운영 중인 홈페이지에 공표할 것을 명령하였다.

이번 (주)해성디에스뿐 아니라, SSL-VPN 등 보안장비의 취약점을 악용한 해킹 및 개인정보 유출 사례가 최근 증가하고 있다. VPN 등 보안장비를 이용하는 사업자들은 보안장비 업데이트, 보안설정 점검 등에 유의해야 한다.

<(재)전남테크노파크 : 과징금 9,800만 원, 과태료 360만 원 부과, 공표명령 >

'23.11.23.경 해커는 (재)전남테크노파크(이하 '테크노파크')가 운영하는 전남 과학기술정보시스템(홈페이지) 내 개인정보처리시스템(이하 '처리시스템')에 권한 없이 접근하여 데이터베이스(DB)를 모두 삭제하였고 금전을 요구하는 랜섬노트(협박 메시지)를 남겼다. 공격을 받은 당시 처리시스템에는 약 1,200여 명의 개인정보가 저장되어 있었으며, 성명, 휴대전화번호, 이메일주소, 소속기관 정보 등이 포함되어 있었다.

조사 결과, 테크노파크는 처리시스템 취급자 계정에 유추하기 쉬운 아이디와 비밀번호*를 사용하였다. 또한, 이용자의 비밀번호도 안전하지 않은 암호화(MD5)방식으로 저장하고 로그인 시 전송하는 비밀번호는 암호화하지 않은 사실을 확인하였다.

* (예시) 아이디 : myusername 등 / 비밀번호 : mypassword, 123456789 등

이에 더해, 처리시스템의 접속 권한을 IP 주소 등으로 제한하거나 불법 접근 및 개인정보 유출 시도를 탐지·차단 하지 않았고, 처리시스템의 접속 기록을 보관·관리하지도 않았다.

아울러 테크노파크는 '24.11.23. 해커가 불법 접근해 개인정보를 삭제하여 훼손된 사실을 인지하였으나, 정당한 사유없이 72시간을 경과하여 '24.11.30일 개인정보 유출 신고를 하였고, '24.12.1일 홈페이지에 유출 사실을 게시하였다.

이에 따라 개인정보위는 안전조치 의무를 위반한 테크노파크에 9,800만 원의 과징금과 360만 원의 과태료를 부과하면서, 처분받은 사실을 테크노파크 홈페이지에 공표하도록 명하였다.

< 이번 조사·처분의 의의 >

최근 제조업 등을 중심으로 랜섬웨어 감염 및 개인정보 유출이 증가하고 있다. 개인정보를 처리하는 사업자들은 운영 중인 서비스에 대한 취약점 점검 및 보안 업데이트를 실시하고, 개인정보 데이터베이스 등 주요 파일을 별도 백업·보관하는 등 각별한 주의가 필요하다.

[붙임] 사업자별 위반 및 시정조치 등 내역(종합)

담당 부서	개인정보보호위원회 조사총괄과	책임자	과 장	강대현 (02-2100-3101)
		담당자	조사관	나일청 (02-2100-3162)
담당 부서	개인정보보호위원회 조사1과	책임자	과 장	김해숙 (02-2100-3111)
		담당자	조사관	조근상 (02-2100-3130)
<공동>	한국인터넷진흥원 유출조사팀	책임자	팀 장	조형진 (061-820-2850)
		담당자	주 임	한미정 (061-820-2856)
		담당자	주 임	김윤권 (061-820-2857)

붙임

사업자별 위반 및 시정조치 내역(종합)

사업자명	위반 내용	위반 조항	시정조치(안)
(주)해성디에스	- 고유식별정보 처리 제한 - 안전조치의무	- 법 §24③ - 법 §29	- 과징금 3억 4,300만 원 - 공표명령
(재)전남테크노파크	- 안전조치 의무 위반 - 개인정보 유출 통지·신고 위반	- 법 §29 - 법 §34①·③	- 과징금 9,800만 원 - 과태료 360만 원 - 공표명령

< 랜섬웨어 대응 수칙 >

수칙	내용
최신 보안패치 적용	서버와 SW 등 보안 업데이트·패치를 신속하게 적용 - 보안 업데이트가 제공되는 최신 버전의 운영체제, SW 사용 - 응용소프트웨어 제조사가 제공하는 업데이트 적용
백업 및 복구 체계 마련·운영	일간/주간/월간 백업 계획 수립, 이행 - 회원 정보 등 주요 개인정보 파일은 별도 백업 등 2차 백업
접근 통제 및 권한 관리	개인정보처리시스템 등에 대한 최소 접근권한 적용, 이력 관리 - 업무용 시스템이나 외부에서 접속해야 하는 경우, 접속 가능한 IP주소, 단말기기 제한, 안전한 인증수단 적용 등 * VPN으로 외부에서 접속하더라도, 다중인증 적용 등 - 내부에서 개인정보처리시스템에 접속시에도 접속 허용 IP 주소 등 최소화로 피해 확산 방지
백신 소프트웨어 설치·운영	백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 - 최신 업데이트를 유지하고, 실시간 감시 이용기능 활성화 - 주기적으로 악성코드 검사 수행 등
개인정보 파일 보관시 암호화 또는 DRM 적용	파일 서버, PC 등에 개인정보가 포함된 파일 보관시 암호화 또는 DRM 적용으로 외부 유출에 따른 피해 최소화 * 개인정보 유출 후 랜섬웨어 전파·감염 등 대비

< 주요 랜섬웨어 사고사례* >

- (서버보안) 보안 설정이 미흡하여 랜섬웨어 감염 및 주요 자료(개인정보 등) 유출
사례 기업 Active Directory 등 중앙관리형 솔루션 환경의 사용자 계정, 권한, 보안 정책 관리의 미흡으로 감염
- (PC보안) 보안 수칙을 준용하지 않아 랜섬웨어 감염 및 주요 자료(개인정보 등) 유출
사례 공문, 이력서, 견적서 등으로 위장한 악성메일의 첨부파일(랜섬웨어) 실행
사례 취약한 버전의 브라우저를 이용해 악성코드(랜섬웨어)가 은닉된 웹사이트 방문
- (NAS) 보안 설정이 미흡하여 랜섬웨어 감염 및 주요 자료(개인정보 등) 유출
사례 접근제어 없이 공장 출하 시 설정된 기본 관리자 패스워드를 사용하거나, 보안 업데이트 미적용으로 감염

* 출처: 보호나라 보안공지 “랜섬웨어 악성코드 감염피해 예방을 위한 보안강화 권고”, (‘25.6.11)