개인정보보호위원회 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2024. 10. 24.(목) 12:00 (2024. 10. 24.(목) 석간) 배포 2024. 10. 23.(수) 17:00

개인정보위, 안전조치 의무를 위반한 2개 사업자 제재

- 데이터베이스와 연동된 웹 관리자페이지 주기적 계정 관리, 보안 점검 등 당부
- 에스큐엘(SQL) 인젝션(악의적 데이터베이스 구문 주입) 공격 예방을 위한 웹 취약점 점검·조치 등 강조

개인정보보호위원회(위원장 고학수, 이하 '개인정보위')는 10월 23일(수) 제17회 전체회의를 열고, **개인정보보호 법규**를 **위반**한 **2개 사업자***에 대해 **총 1억 2,317만 원의 과징금**과 **1,080만 원의 과태료를 부과**하기로 **의결**하였다.

* ㈜네오팜 : 화장품 등 판매 온라인 쇼핑몰 웹사이트 운영 사업자
㈜일학 : 낚시용품 등 판매 온라인 쇼핑몰 웹사이트 운영 사업자

개인정보 유출 신고에 따라 조사가 이루어진 이들 2개 사업자의 **구체적인 위반 내용**과 **처분 결과**는 다음과 같다.

1 ㈜네오팜 : 과징금 1억 517만 원과 과태료 720만 원 부과, 결과 공표

조사 결과, 해커는 사전에 획득한 ㈜네오팜이 운영 중인 쇼핑몰 **관리자 계정 정보**를 통해 쇼핑몰의 **웹 관리자 페이지**에 **접속**하여, 쇼핑몰 전체 **회원**인 **293,723명**의 **개인정보**를 **탈취**하였다. 특히, 해커는 '23. 8. 5.부터 약 2주 동안 쇼핑몰 **웹 관리자 페이지**에 750여 회 접근해 **회원정보**를 **조회**하고 **내려받았으며**, **약 44만 건**의 **불법 문자**도 **발송**하였다.

이렇게 **대규모 유출사고**가 발생하게 된 것은 ㈜네오팜의 개인정보처리 시스템인 **웹 관리자 페이지**가 추가 인증수단 없이 **아이디와 비밀번호만**으로도 **로그인**이 **가능**하게 **운영**되고 있었고, **웹 관리자 페이지**에 접속할 수 있는 **아이피(IP) 주소 등**을 **제한하지 않는** 등 **안전조치의무**를 **위반**했기 때문이다.

아울러, ㈜네오팜이 **개인정보취급자별**로 **계정**을 **부여하지 않고 부서별**로 **계정**을 **공유**하는 등 **접근권한**에 대한 **관리**도 **소홀**한 사실과, 유출된 이용자 대상으로 **개인정보 유출 통지**를 **지연**한 사실도 확인하였다.

이에 개인정보위는 과징금 1억 517만 원과 과태료 720만 원을 부과하고, 개인정보위 홈페이지에 그 결과를 공표하기로 하였다.

2 ㈜일학 : 과징금 1,800만 원과 과태료 360만 원 부과, 공표 명령

㈜일학은 '23. 12. 17.부터 이틀간 해커의 **에스큐엘(SQL) 삽입 공격***을 받아 **개인정보**가 **유출**되었는데, 개인정보를 유출한 해커는 ㈜일학의 쇼핑몰 **게시판**에 **10,000명**의 **개인정보**를 **게시**하기도 하였다.

* **에스큐엘(SQL, Structured Query Language) 삽입 공격** : 웹사이트 취약점을 이용해 악의적인 에스큐엘(SQL, 데이터베이스 조회 등을 위해 사용하는 프로그램 언어)문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 공격 기법

조사 결과, ㈜일학은 낚시용품 쇼핑몰을 운영하면서 **웹 관리자 페이지**에 로그인 시 **안전한 인증수단**을 **적용하지 않았고**, 외부로부터 불법적인 접근을 방지하기 위한 **침입 탐지·차단 시스템 운영**도 **부실**했던 것으로 확인되었다.

아울러, **에스큐엘(SQL) 삽입 공격**을 **예방**하기 위한 **이용자 입력값 검증 절차 부재**, **비밀번호 암호화 미조치** 등의 **안전조치의무**도 **위반**한 것으로 확인되었다.

이에 개인정보위는 과징금 1,800만 원과 과태료 360만 원을 부과하고, 사업자 홈페이지에 그 사실을 공표하도록 명령하였다.

웹사이트를 통해 서비스를 제공하고 개인정보를 처리하는 사업자는 **회원 데이터베이스**와 **연동**된 **웹 관리자 페이지 운영** 시 **개인정보취급자 계정 관리**, **보안 취약점**에 대한 **점검** 등을 **주기적**으로 **실시**해야 하며, **에스큐엘(SQL) 삽입 공격**처럼 **잘 알려진 웹 취약점 공격**에 대해서는 **적절한 보안조치** 등 **지속적인 주의**가 **필요**하다고 개인정보위는 밝혔다.

[붙임] 사업자별 위반 및 시정조치 내역(종합)

담당 부서 <총괄>	개인정보보호위원회 조사2과	책임자	과 장	김해숙 (02-2100-3151)
		담당자	조사관	허재형 (02-2100-3129)
<공동>	한국인터넷진흥원 플랫폼조사팀	책임자	팀 장	문봉주 (061-820-1496)
		담당자	책 임	김민수 (061-820-1472)

대한민국 정책브리핑
더 아픈 환자에게 양보해 주셔서 감사합니다
가벼운 증상은 동네 병·의원으로
OPEN 출처표시
공공누리 공공저작물 자유이용허락

붙임 | **사업자별 위반 및 시정조치 내역(종합)**

사업자명	위반 내용	위반 조항	시정조치(안)
㈜네오팜	• 안전조치의무 (접근통제, 접속기록) • 개인정보 유출통지·신고 특례 위반	舊 보호법* §29 §39의4①	• 과징금 1억 517만 원 • 과태료 720만 원 • 결과 공표
㈜일학	• 안전조치의무 (접근통제, 암호화, 접속기록)	보호법 §29	• 과징금 1,800만 원 • 과태료 360만 원 • 공표 명령

* ‘23.9.15. 이전 발생한 유출 사건은 舊 보호법(‘20.8.5. 시행, 법률 제16930호) 적용