경영유의사항 등 공개안

1. 금융기관명 : ㈜다날

2. 조치일 : 2018. 6. 14.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 4건

4. 조치대상사실

가. 경영유의사항

(1) 계열사 업무 시스템 분리대책 강화

회사는 OOOO, OOO, OO·OOOOO 등 업무시스템을 망분리 미적용 계열사(OOOOOOOO, OO)와 공유하고 있어 계열사 단말기 등이 악성코드에 노출될 경우 동 업무시스템을 통해 악성코드가 유입될 우려가 있으므로

계열사를 통한 악성코드 유입 등을 방지하기 위하여 상기 업무시스템을 분리·운영하는 등 통신망 보안대책 강화 필요

(2) 기술지원 종료 운영체제 사용에 따른 보안통제 강화

회사는 OO 데이터베이스(DB), OOOO, OOOO 서버, OOOOOOO(OOO) 서버 등 주요 시스템(총OO대)에서 사용 중인 운영체제 Windows2003 및 Windows XP는 기술지원이 종료되어 신규 보안패치 등이 이루어지지 않음에 따라 기존에 알려지지 않은 취약점을 이용한 해킹 및 악성코드 등에 의한 전자적 침해 우려가 있으므로

기술지원이 종료된 주요시스템의 운영체제를 전환하기 위한 구체적인 계획을 수립하고 이행 필요

가. 개선사항

(1) 카드번호 보호대책 불합리

회사는 OOO 거래조회 및 매출내역 등을 관리하기 위한 OOO 관리시스템을 운영하면서 ID·비밀번호 로그인 외에 OTP 등의 추가인증 절차를 마련하고, IP주소를 등록하여 비인가 접근을 제한하는 등 보안조치를 취하고 있으나

수기거래 시 결제가 미완료된 카드는 데이터베이스(DB)에 OOOO가 마스킹 되지 않은 채로 보관되어 있어 OOO 관리시스템의 승인실패 화면에서 OOOO를 평문으로 조회할 수 있고, 데이터베이스(DB) 또는 OOO 관리시스템 해킹시 평문으로 된 OOOO가 유출되어 악용될 수 있으므로

수기거래 시 결제가 미완료된 카드는 데이터베이스(DB)에 OOOO를 마스킹 하여 저장하고 OOO 관리시스템에서 마스킹 처리된 상태로 조회되도록 개선 필요

(2) 정보유출방지 대책 미흡

회사는 정보유출 방지를 위해 매체제어시스템(OOO)을 운영하고, 내부망 PC에서는 등록된 보안 USB만 이용하도록 하는 등 보안대책을 마련하고 있으나

여전히 인터넷망 PC에서는 일반 USB의 읽기권한을 상시 허용하고 있어 이를 통해 바이러스 및 악성코드에 감염될 수 있고, 상용메일(OOOOO 등), 상용메신저(OOOO, OOOO 등) 및 웹하드 등을 차단하지 않아 이를 통해 사내정보가 유출될 경우 사후 추적이 불가능할 우려가 있으며

개발자의 인터넷망 PC에서 과거 프로그램 소스코드 등을 보관하고 있어 관련 자료 유출시 해커가 프로그램 구조를 파악하여 해킹공격을 하거나 파밍사이트 등의 제작에 악용될 우려가 있으므로

인터넷망 PC에서 일반 USB의 읽기권한 및 상용메일, 상용메신저 및 웹하드 등의 사용을 차단하고 개발자의 인터넷망 PC에 보관된 과거 프로그램 소스코드를 삭제하는 등 정보유출방지 대책 마련 필요

(3) 이메일 보안대책 미흡

회사는 이메일(OOOO.OOOOO.OO.OO)을 외부에서도 아이디·패스워드를 이용하여 접속할 수 있도록 운영하고 있고, 관련 웹페이지 등에 대한 점검도 이루어지지 않는

등 이메일 보안대책이 미흡한 수준으로 해킹 또는 아이디·패스워드 도용 등에 대해 취약할 우려가 있으므로

회사 이메일에 대한 접근을 가상사설망(VPN)을 통해 제한하고, 이메일 웹페이지 등에 대해 취약점 점검을 실시하는 등 이메일 보안대책 마련 필요

(4) 백업 및 소산절차 불합리

회사가 제공하는 전자결제 서비스와 관련하여 결제로그 기록을 일, 월, 분기 별로 백업하고 매월 본사로 이를 소산하고 있으나

결제로그 외의 데이터 및 시스템 설정 등에 대해서는 백업하지 않고 본사의 소산 데이터도 일반 캐비넷에 보관하는 등 관련절차가 미흡하여 화재 등의 재해가 발생한 경우 이를 복구하기 어려울 우려가 있으므로

앞으로 결제로그 외의 중요 전산자료에 대해서도 백업하고 내화금고를 도입하여 소산자료를 보관하는 등 백업 및 소산절차 개선 필요