호스팅 서비스 보안 및 백업 권고 가이드라인 (Ver 1.0)

작성일 : 2017년 9월 15일

한국호스팅도메인협회가 이번에 마련한 보안 및 백업 가이드는 대한민국 내에서 호스팅 서비스를 제공하는 사업자가 서비스를 영위하기 위한 최소한의 보안 및 백업 권고사항을 담고 있습니다. 본 가이드는 보안과 백업의 끝이 아니고 최소한의 지켜야 할 사항을 제시한 것으로서, 본 가이드의 목적은 보안과 백업에 대한 협회 회원사 내의 안전하고 안정적인 최소한의 관리 체계를 유지하기 위함이며, 아울러 국내 호스팅 서비스 이용자의 안전하고 쾌적한 서비스 이용 환경을 제공하기 위함입니다.

1. 보안 담당자와 개인 정보 보호 담당자 지정

- 사내 보안 담당자와 개인 정보 보호 담당자를 지정 합니다.

2. 취약점의 관리

- 모든 서버는 보안 취약점이 발표 되었을 경우, 즉시 업데이트해야 합니다.

- 시스템 관리자 권한으로 직접 운영하는 모든 서버의 목록을 정리하고, 서버 별정,부 관리자를 지정합니다. 또한 서버의 사양, 설치한 운영체제, 설치한 프로그램의 목록을 보관하고 있다가, 보안 취약점이 발표되었을 때, 해당하는 서버가 있는지를 점검하도록 합니다.

- 서비스 홈페이지는 프로그래밍이 변경되었을 경우, 변경시마다 그에 대한 취약점이 있는지를 점검 합니다. 또한 분기 1 회 정도는 취약점 스캐너를 이용하여 웹 취약점이 존재하고 있는 지를 점검하고, 취약점이 확인된 부분에 대해 조치 합니다.

- 관리하는 모든 서버는 최소 분기 1 회 최신의 취약점 점검 전용 프로그램을 이용하여 점검하고, 취약한 내용을 기록합니다. (예: 웹스캐너, 시스템스캐너, 루트킷, 웹쉘 등의 탐지 등)

- 발견된 취약점은 프로그램을 수정하거나 업데이트하여 취약점이 존재하지 않는 수준으로 관리하며, 그렇지 못할 상황인 경우 방화벽이나 웹방화벽 등의 방어 프로그램을 운영하여 보완하도록 합니다.

3. 관리서버의 접근 제어

- 관리서버는 서버의 관리자 권한으로 접근하여 관리하는 모든 서버 - 자사 운영서버, 웹호스팅서버, 관리대행서버 - 를 말합니다.

- 관리서버의 종류별, 목적별 실행되는 데몬을 기술하고, 열어야 할 포트 정책을 정의하며, 이에 대한 적정하고 안전한 접근 정책을 정의 합니다.

- 서버의 이용목적, 관리 목적별로 적절한 IP 접근 정책 - 사무실 IP, VPN IP, 협력사 IP 등 - 을 정의 합니다.

- 한 서버에 여러 명의 관리자가 접근 할 경우 서버 내에 필요에 따른 디렉토리별, 실행 범위를 관리자별로 차등의 권한을 부여 합니다.

- 서버의 방화벽 프로그램은 이용 목적상 열어야 할 포트 (예 : 웹서버 80) 를 제외한 , 관리 목적상 열어야 할 포트는 사무실과 관리용 VPN서버 이외에는 접근을 하지 못하도록 합니다.

- 포트를 열고 있는 이용 목적이나 운영 목적에 해당하지 않는 포트를 열고 있는 서비스 데몬이 있다면 실행되지 않도록 설정하며, 만일 보안권고나 취약점이 발견된 서비스 데몬의 포트에 대해서는 평소에는 차단하고, 꼭 필요한 경우에만 포트를 열어서 작업을 하며, 작업완료 후 다시 차단합니다. (예: SAMBA 포트)

- 망 분리 : 데이터베이스 서버 등 외부로 노출될 경우 공격으로부터 위험이 발생할 수 있는 주요 서버는 공인된 IP 망으로부터 직접 접속할 수 없도록 분리하여 운영합니다.

- 로그 파일의 보호 : 로그 파일은 침입 혹은 침입시도 등 보안 문제점을 파악하는데 중요한 정보를 제공하므로 로그 파일이 노출, 변조 혹은 삭제되지 않도록 불필요한 접근으로부터 보호합니다.

4. 패스워드 정책

- 관리 목적상 접근해야 할 서버의 패스워드는 최소 10자리 이상으로 운영하며, 패스워드는 무작위 대입공격으로부터 충분히 방어가 될 수 있도록 숫자, 특수문자, 영문 대소문자를 조합하여 생성합니다.

- 패스워드는 별도의 종이 문서로 관리하며, 파일 형태로 관리 하지 않으며 퇴근시 안전 금고에 보관하도록 합니다. 부득이하게 파일 형태로 관리 할 경우 반드시 파일에 암호를 걸어서 관리하고 컴퓨터 하드디스크 이외의 저장 매체를 이용하여 저장합니다. 서버로의 접근이 허용된 IP의 컴퓨터에 보관하거나 저장매체를 연결하여 파일을 열어 보지 않도록 합니다.

- 서버의 관리 목적상 접속할 때 최소 2가지 이상의 별개 방법의 패스워드 로그인 정책을 가지도록 합니다. (공인인증서, OPT (One Time Password) 등)

- VPN을 이용한 접근 제어를 할 경우 (특히 WINDOWS 서버) VPN서버에 최소 2개 이상의 별개의 패스워드 로그인 정책을 가지도록 VPN 서버를 구축합니다. 예) OPEN VPN - OTP 정책 적용

5. 서버의 관리 및 모니터링

- 서비스 구조도, 네트워크 구조도, 서버별 랙 위치도, 스위치 포트별 서버의 위치도 등을 작성하여 보관하고, 물리적 서버에는 서버의 ip 주소, 관리자 등을 라벨링을 하여, 보안사고 발생시 해당 서버의 즉각적인 고립이나 조치 행위를 할 수 있도록 합니다.

- 네트워크는 서비스 목적에 따라 보안 유지 목적에 따라 적정한 VLAN으로 나누어

운영 합니다.

- 관리 권한을 유지하고 있는 모든 서버의 시스템 헬스 상태의 임계치를 설정하여 임계치 초과시 경고할 수 있도록 하는 모니터링 시스템을 구축하여 운영하도록 합니다.

- 운영하는 네트워크 상태 (BPS, PPS, ARP, FLOW등)를 모니터링하며, 보유한 네트워크 장비 상황에 대하여 임계치를 설정, 운영, 경고할 수 있는 원격 모니터링 체계를 구축하고 상시 관제하도록 합니다.

6. 고객 개인 정보 보안

- 고객 패스워드 암호화, 개인 정보 보유의 최소화, 주요 고객 정보의 암호화를 시행하며, 이는 정부의 '개인정보보호 자가진단 체크리스트' (인터넷진흥원 개인정보보호 기술지원센터 2014.12) 에 근거하여 회사의 실정에 맞추어 관리합니다

- 고객의 패스워드는 최소 8자 이상의 숫자와 영문을 섞어서 사용 가능 하도록 하며, 너무 쉽고 유추가 가능한 손쉬운 패스워드는 사용하지 못하도록 홈페이지 프로그램을 설정 합니다.

- 홈페이지 암호 대입공격의 방어를 위하여, 로그인 실패 시 모호한 에러 메세지 실행 및 지정 로그인 횟수 이상의 로그인 실패 시 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) 입력 등의 기본적인 방어 조치를 하도록 합니다.

7. 웹 호스팅 서버의 관리

- 웹 호스팅 서버의 보안은 KISA 에서 배포한 '리눅스 서버용 웹 호스팅 보안 가이드' 및 '윈도우 서버용 웹 호스팅 보안 가이드'를 근거하여 현재의 보안 상황에 근거하여 관리 합니다. http://www.kisa.or.kr/public/library/etc_List.jsp?pageIndex=1&searchType=&searchKeyword=%EC%9B%B9%ED%98%B8%EC%8A%A4%ED%8C%85

- 해지된 고객의 서버 계정 및 해당 데이터는 삭제하고 그 계정으로 접근을 불허하도록 합니다.

- 웹 호스팅 서비스 이용 고객의 계정 접근은 FTP 접근만을 허용하는 것을 원칙으로 합니다, SSH 접속 권한을 요구 하는 고객은 별도의 SSH 사용자들만을 위한 서버로 격리 운영하며, SSH 계정의 보안 허점을 이용한 권한상승 공격으로 인한 피해를 입게 될 경우, 그 책임은 본인에게 있음을 주지시킵니다.

- 고객의 불필요한 파일 업로드는 허용하지 않습니다. 또한 업로드를 허용해야 하는 파일의 종류를 지정하여 그 외 종류의 파일들은 업로드가 불가능하도록 하여 업로드된 파일이 실행 되지 않도록 설정 합니다.

- CGI, PHP, JSP, ASP 등 서버에서 실행될 수 있는 스크립트 파일이 웹 서비스를 통해 업로드 되는 것을 방지하며, 그 파일이 실행 되지 않도록 서버를 설정 합니다.

- 웹 호스팅 서버의 이용 고객이 자신의 모든 데이터 (홈페이지 및 DB)를 손쉽게 다운로드받아 백업할 수 있도록, 1일 1회의 압축된 백업 데이터를 고객이 다운로드받기 가장 쉬운 자리에 제공하며, 홈페이지 그 위치를 공지 합니다.

8. 서버의 백업

- 별도의 백업 서비스를 받지 않는 한, 데이터 백업의 모든 책임은 고객에게 있고, 데이터 망실시 이에 대하여 회사에 책임을 물을 수 없음을 주지시키며, 이 내용을 홈페이지의 가장 잘 보이는 자리에 고지합니다

- 서버 망실시 백업하여 보관된 데이터로 서비스를 복구할 경우, 서비스를 이용을 하지 못하는 장애 시간에 대한 보상에 대하여 이 내용을 홈페이지 상품 페이지에 고지합니다.

- 위의 두가지 사항에 대한 내용을 호스팅 상품을 신청할 때 한국호스팅도메인협회 호스팅서비스 공동 이용약관과 SLA (Service Level Agreement) 를 통해 동의하는 절차를 가지도록 합니다.

- 웹 호스팅 서버는 active – stand by 형태로 서비스 체계로 운영되어야 하며, active 서버의 장애시 stand by 서버에서 즉시 서버를 개통할 수 있도록 합니다.

- 웹 호스팅 서버는 기간에 따라 최소 2단계 이상의 백업 - 단기와 장기의 백업을 유지하도록 하며, 각 단계의 백업 서버는 각각 별도의 서버와 별도의 스토리지에서 운영 하도록 구성 합니다. 가급적 장기 백업본은 서비스 하고 있는 서버가 소재한 데이터센터 이외의 장소에 최소 주 일회 백업 할 것을 권장 합니다.

- 백업 서버는 현재 서비스에 사용 하는 서버를 이용 하지 않고 별도의 서버로 구성 합니다. active - stand by 서버를 구성하기 위하여 서비스 서버끼리 교차 백업을 하는 경우, 별도의 단기 백업 서버를 운영하는 것을 원칙으로 합니다.

- 데이터의 백업은 백업 서버에서 데이터가 있는 서버로 접근하여 백업 하는 것을 원칙으로 하며, 서버가 스토리지를 마운팅하여 데이터를 저장 하는 방식은 백업으로 인정하지 않습니다.

- 백업이 마무리 될 경우 서버 간의 연결은 그 즉시 중단하는 것을 원칙으로 합니다.

- 백업 서버로의 접근은 허용 되는 IP 이외의 접근이 불가능하도록 관리 합니다.

9. 사무실 컴퓨터 및 네트워크의 보안

- 서버 관리 부서는 다른 부서와 네트워크를 별도의 네트워크로 분리하여 운영 합니다.

- 서버 관리 부서는 일반 사무용 컴퓨터와 서버 관리용 컴퓨터는 별도로 분리 하여 이용 하는 것을 원칙으로 합니다.

- 서버 관리용 컴퓨터에서는 부득이한 경우가 아니면 웹 서핑, 메일 읽기등을 자제하도록 합니다.

- 서버 관리용 컴퓨터는 상시 보안 업데이트를 합니다

- 서버 관리용 컴퓨터 악성 코드 공격- 특히 키보드 로깅 공격으로부터 대비 하도록 합니다.

- 서버 관리 부서의 컴퓨터는 퇴근시간 이후 자동으로 꺼지도록 운영 합니다.

- 사무실 이외에서 환경에서 운영서버에 VPN 서버를 경유하여 접속하도록 허용하는 경우, 악성 코드로 오염될 수 있는 PC 방이나 가정용 컴퓨터 등을 이용한 접근은 불가능하도록 하는 대책을 수립하여야 합니다. 예) 특정 노트북을 지정하여 VPN 계정 세팅은 보안 담당자만 하도록 운영 합니다.

10. 보안 사고시 대응

- 관계기관, 데이터센터, 통신사, 사내 엔지니어 등 임직원 등의 비상 연락망을 가장 최신 상태로 운영 유지하고 연 1회 이상 비상 전파 훈련을 하도록 합니다.

- 서버와 매칭되도록 고객 정보를 관리하여 장애 시 해당서버의 이용 고객에게 현재의 장애 상황을 통보 하도록 합니다.

- 파장이 큰 보안 사고 발생 혹은 발견 시 관계 기관 침해사고대응센터에 신고하고, 필요시 협회로 통보하도록 합니다.

- 동료 호스팅 회사에 보안 사고 발생시 발생 규모가 클 경우 조기에 위기를 극복할 수 있도록 상호 협조하도록 합니다.

11. 교육 및 보안의 날 행사 및 기타

- 분기 1회 사내 보안 교육 서버교육을 실시 합니다.

- 최소 연 2회 보안 및 서버 관련 외부 교욱을 실시 합니다.

- 보안의 날 행사 : 분기 1회 보안의 날 행사를 합니다

- 보안 체크리스트의 운영하여 백업 사항 컴퓨터 관리, 보안 업데이트 여부등을 점검 사항 목록화 하여 자체 점검 합니다.

- 주요 보안 업데이트 취약점이 나올 경우 해당 고객에게 이를 전파 합니다.

- 정부의 보안 관련 알림 사항이나 요구 사항이 있을 때 즉시 고객에게 이를 전파 합니다.