사이버 도우미 118

제15회 해킹방어대회(HDCON) 문제

2018. 10.

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Ⅰ 유의사항

- 귀하는 아래 문제에서 제시된 각 분야에서 제시된 **기업의 정보보호를 맡고 있는 담당자**의 입장에서 해법을 제시
  ※ 문제의 상황을 잘 파악하고, 단편적이 아닌 종합적인 해법을 제시
- 각 팀은 다음 문제들 중 **하나 이상에 대해 응모**할 수 있음
  ※ 복수의 문제에 응모하는 경우 각 문제 별로 해법을 별도의 파일로 제출
- 「제약조건」 안에서 「전제사항」을 감안하여 현재 귀사에서 가장 만족스러운 결과를 얻을 수 있도록 **주어진 문제에 대한 해법**을 작성
- 「제약조건」 및 「전제사항」에 주어지지 않은 사항에 대해서는 임의로 가정을 하고 접근할 수 있으나, 가정한 사항에 대한 현실성 및 타당성이 떨어질 경우, 채점과정에서 불이익을 받을 수 있음.
- 제출하는 해법 자체에는 팀명을 제외한 참가팀의 소속, 이름 등 **인적사항이 드러나지 않도록** 유의
- 응모작은의 제출기한은 2018. 10. 19.(금) 17:00까지, 이메일(hdcon2018@concert.or.kr)로 제출
- 제출물은 아래와 같은 형식으로 제출
  * **메일 제목 : 2018 HDCON 참가신청(팀명)**
  * **파일 제목 : 팀명_분야_제출일.pdf** (예 : 만능컨설턴트_계정도용_181001.pdf)
  * **메일 주소 : hdcon2018@concert.or.kr**
- 문제에 드러난 상황 및 사실관계는 HDCON해킹방어대회를 위하여 만들어진 가상의 것으로, 실존하는 특정 인물, 기업, 단체 등과 관계 無
- 제출하는 해법의 분량은 전체 10장 이내
  ※ 폰트 맑은고딕, 크기 10pt, 줄간격 160% 기준

II 문 제

[1] Supply Chain Security

<배경 설명>

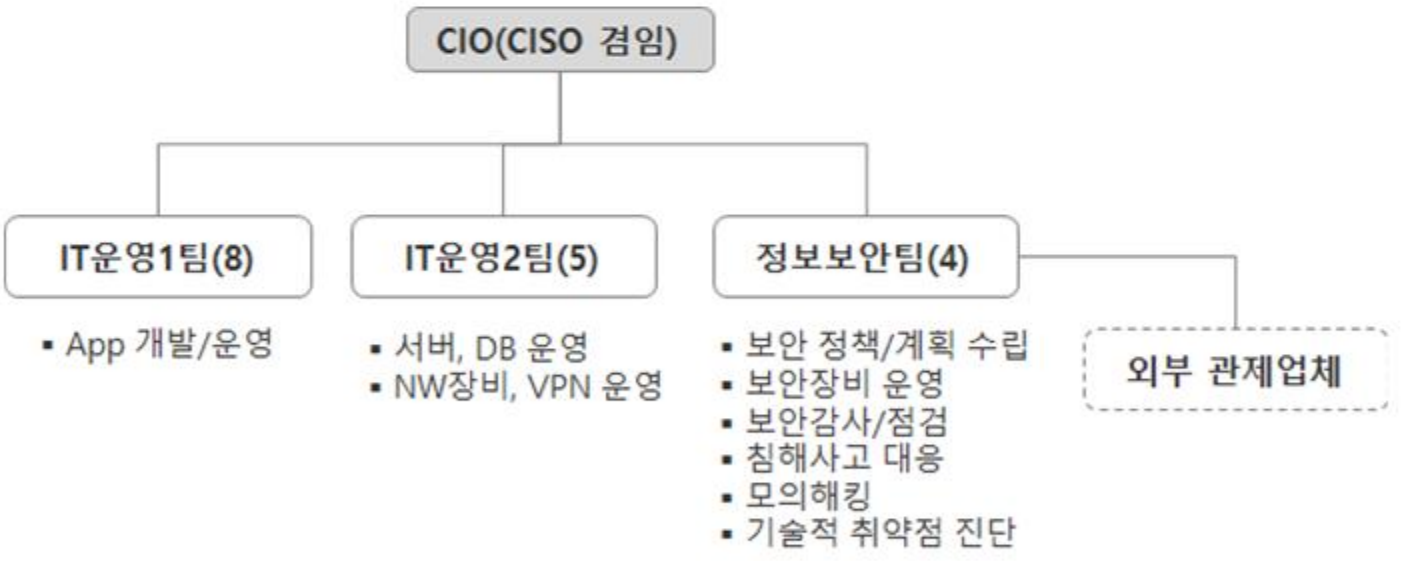
중견제조업체 A사는 최근 개발한 신기술이 글로벌 시장에서 경쟁하는 중국 업체로 유출된 정황이 확인되었으며 정보보안 담당자가 의심하는 정황은 아래와 같다.

1. 연구소 내에서 사용하는 복합기에서 매주 월요일 새벽에 외부 전송 트래픽이 급증하였다 사라지는 현상이 발견되었으며 해당 복합기의 이상 현상은 6개월 전 유지보수 업체를 통해 패치를 실시한 후부터 발생되었으며 이전에는 발견되지 않은 현상으로 확인됨
2. 본사/공장/연구소에서 사용하는 백신은 국내 백신업체의 제품을 사용하고 있으며, 해당 업체는 2년 전 해킹을 당한 이력이 있으나 해당 백신 소프트웨어는 그 이후 개발된 것으로 문제가 없다고 답변 받은 바 있으나 최근에 동일한 제품을 사용하는 타 기관에서 해킹 정황이 있다는 언론보도가 있었음
3. 공장 내 일부 설비는 글로벌 업체의 제품으로 유지보수/원격점검/원격패치 등의 목적으로 포트가 오픈되어 있으며 해당 업체의 유지보수 사무소는 중국에 있음, 해당 제품은 관리를 위해 Windows 기반의 PC가 있으며 원격패치 이후 악성코드에 감염되어 백신으로 조치한 사례가 있음.

정보보안 책임자는 CISO 교육을 통해 이러한 문제가 공급망 보안에 대한 체계가 없어서 발생한 것으로 보고 정보보안 담당자인 귀하에게 근본적으로 해결할 수 있는 방안을 수립하여 보고하도록 하였다.

<전제 사항>

1. A사의 IT 및 정보보안 조직(괄호 안은 인원 수)



2. 운영 중인 보안장비는 아래와 같다.
   - 방화벽, IPS, DDoS 대응장비, NDLP, DRM, PC보안, 백신
3. 내부망과 공장망은 방화벽을 통해 분리하고 있으며 방화벽 정책에 대한 점검 및 불필요한 정책의 삭제 등은 실시되지 않음
4. 내부망 내 사용자 중 승인을 받은 사용자는 공장망으로 제한 없이 접근이 가능함

5. 정보보안팀은 기술적 취약점 진단 및 웹 어플리케이션에 대한 모의해킹이 가능한 인력이 있으나 전반적인 모의해킹은 년 1회 외부 전문업체를 통해 모의해킹을 실시함
6. 전사 정보보안 규정 중 '어플리케이션 개발/운영 보안지침'이 수립되어 있으며 주요 언어별 보안가이드 또한 KISA 자료를 참고하여 작성하여 운영하고 있음
7. 외주 개발 시 개발자는 내부 또는 외부에서 개발이 가능하며 외부 개발 시 별도의 보안점검은 실시하지 않음(보안서약서는 작성함)
8. 자체 또는 외부 개발된 어플리케이션은 보안 취약점 점검을 실시한 후 조치가 완료된 경우에만 운영으로 이관이 가능하나 상용 제품 및 어플라이언스 제품 등에 대한 보안 점검은 실시하지 않음
9. 패치 파일 반입 시 외부 USB의 반입은 불가하며 패치 파일은 악성코드 감염여부 등에 대해서만 점검을 실시함

<제약 조건>

o 3가지 정황을 모두 고려하여 관리적/기술적 관리체계 및 대응방안을 수립하여야 합니다.

위 상황을 해결할 수 있는 해법을 제시해주세요.

[2] 계정 도용

<배경 설명>

B사는 최근 고객의 운동량에 따라 코인을 지급하고 그것으로 물건을 살 수 있도록 하는 서비스의 상용화를 앞두고 있는 중소 IT개발사임. 현재 서비스의 완성도 및 대외 고객들의 반응을 확인하기 위해 최종 마지막 Beta Test를 진행하고 있음

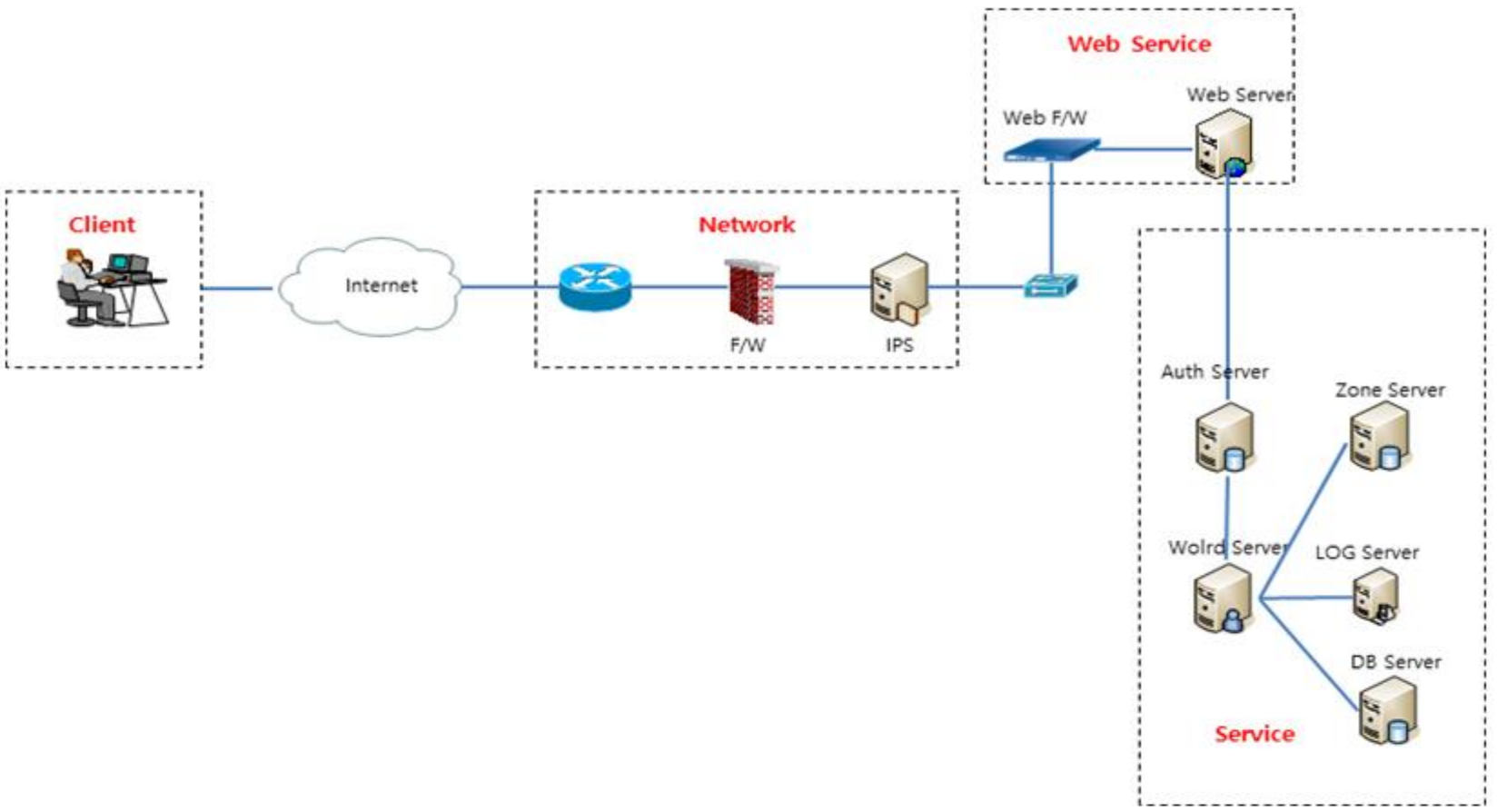
안정성 점검을 위해 접속 관련 로그를 분석하던 중 대량의 계정도용 시도 및 도용 성공 로그가 다수 발생하고 있는 것이 확인되었음. 서비스 특성상 계정 도용을 통해 기존 계정 주인이 보유하고 있던 재화(코인)를 모두 탈취해 부당이득을 취할 수 있기 때문에 비즈니스에 치명적인 영향을 줄 수 있음. 현재 회사에서 계정도용을 방어하기 위한 방어 수단으로 아래와 같은 솔루션을 사용하고 있으나 2차 인증 솔루션은 고객의 불편함 때문에 강제로 적용할 수 없는 상황임. 지속적으로 2차 인증 적용을 유도하고 있으나 사용율이 10% 정도에 그침. 웹 방화벽을 통한 로그인 페이지 임계치 차단은 임시적인 방법이며 임계치 도달 이전 IP변경 등의 우회를 통해 실질적인 대응이 되고 있지 않음.

o 현재 대응책
- 2차 인증 솔루션 제공
  : 2차인증 솔루션(2차 비밀번호, OTP, 지정단말, 전화인증) 제공 (유저선택)
- 임계치 기반 보안 솔루션을 통한 차단
  : 웹방화벽의 임계치 차단기능을 이용하여 로그인 페이지 등의 접속IP 임계치 차단
- 인증서버에서 계정도용 필터링 시스템 구축
  : 해커의 공격 패턴을 분석하여 로그인 단에서 계정도용 필터링 시스템 구축
  : 동일IP에서 지속적으로 공격이 들어 올 경우 해당IP를 차단하고 해당 IP에서 로그인 성공한 계정에 대한 본인인증 시행
  : 블랙리스트 DB를 구축하여 탐지된 IP 및 악성IP에 대한 차단
- 로그 분석을 통한 차단 및 제제
  : 로그를 분석하여 이상로그인 계정에 대한 차단
  : 로그 분석을 통한 계정도용 행위 계정 추출 및 제제

<전제 사항>

o 임직원 수는 400명 정도 되는 중견규모 IT개발사임.
o 정보보호 예산은 2억 정도 보유하고 있으며, 보안조직은 5명으로 구성됨
o IT개발사 특성상 실력 있는 개발자가 많기 때문에 좋은 아이디어가 있다면 자체 구축할 수 있음.

1.서비스 구성도



2. 계정도용 방지를 위해 적용된 보안시스템
- IPS, 웹방화벽
- OTP, 지정단말

<제약 조건>

- o 해커가 대량으로 계정도용 공격을 시도할 때 자신의 IP를 속이기 위하여 VPN 서비스를 이용
- o 운동량은 모바일 디바이스를 통해 측정하며, 계정관리 및 코인을 이용한 구매 등은 웹페이지를 통해 제공하고 있음.(운동량 측정 단에서의 보안 문제는 없다고 가정함)
- o 서비스의 특성상 금융권 서비스처럼 로그인 시마다 본인인증 등을 일괄적으로 적용하여 의무화 할 경우 이용자의 이탈이 발생 할 수 있음(서비스의 비즈니스모델은 고객의 수를 기반으로 마케팅을 하여 수익을 얻는 구조임)
- o 모바일 웹/앱 통합 등의 비즈니스 로직 변경은 불가함. 유저들의 서비스 이용에 불편함을 주지 않으면서 보안을 강화할 수 있는 방안이 필요함

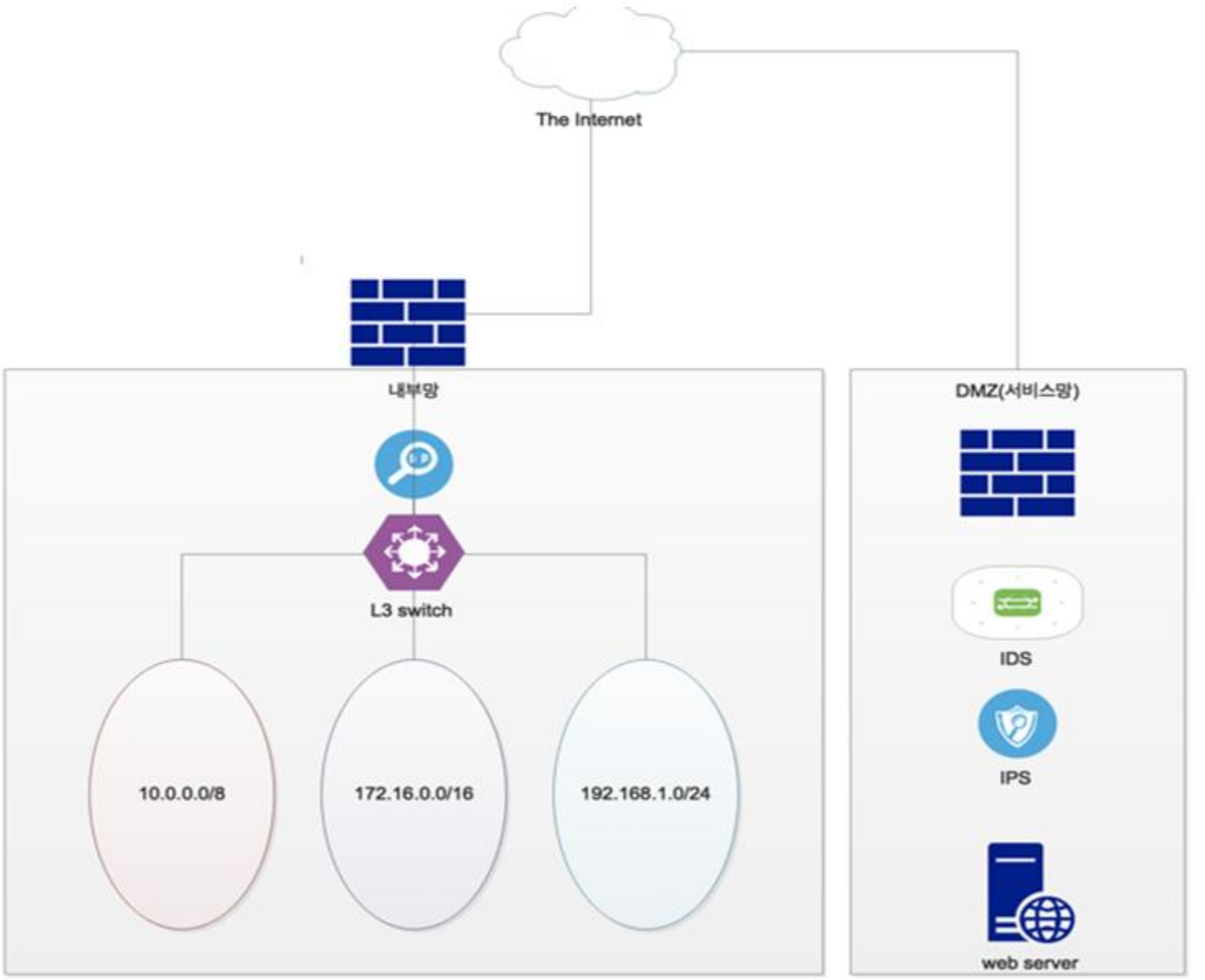
귀하는 B사의 정보보호 팀을 이끌고 있는 팀장으로서 위 대응방안을 포함하여 계정도용을 효과적으로 차단할 수 있는 종합대책을 수립해야 함.

[3] 내부망 침투

<배경 설명>

- o C사는 민감한 국가기술정보를 생산/관리하는 업체
- o C사는 사용자 망과는 별도의 DMZ망을 구축하여 자체 홈페이지를 운영
- o 서비스망 보호를 위해 외부업체의 관제를 받고 있으며 방화벽, 웹방화벽 및 침입차단장치 등의 보안장치를 운영
- o 내부망 보안을 위해서는 백신, DLP/DRM 및 NAC 등의 침해사고탐지 및 대응장치를 운영

이러한 일련의 예방체계 운용에도 불구하고 해당 사업장을 목표로 한 국가기반 공격자는 불상의 방법으로 운영 중인 예방체계를 우회하여 내부망에 초기거점을 마련하고 이를 기점으로 외부와 통신이 가능한 비콘형 명령제어 채널을 구성했음. 이후 공격자는 내부정보 수집과정을 통해 사용자망 컴퓨터의 운영취약점을 파악하고 이를 이용한 내부이동 작업을 통해 100여개의 내부 컴퓨터에 접근할 수 있는 체인형 백도어를 구성한 뒤 각 호스트에서 수집된 내부정보를 탈취된 다수의 내부 호스트를 이용하여 해외에 위치한 웹메일 서버에 5M 이하의 첨부파일 형태로 지속적으로 유출하고 있음.



<전제 사항>

해당 사업장은 약 5,000 대 이상의 호스트가 3개의 서브네트워크로 나뉘어 운영되고 있으며 침해사고대응팀은 유입되는 모든 악성파일에 대한 샌드박스 검사, 10M 이상의 데이터 외부 전송 시 자동차단 등 알려진 보안위협에 대응하기 위한 강력한 보안정책을 집행 중이나 대부분의 보안업무는 장비에서 탐지된 탐지 이벤트 대응으로 이루어지고 있다.

<제약 조건>

- o 방어자는 본 위협을 탐지하기 위해 새로운 시그니처 기반 보안장치를 구매하거나 외부 전문가에 문제 해결을 의뢰 할 수 없음
- o 방어자는 내부보안장치 로그 및 네트워크 플로우(Netflow) 등에 접근할 수 있음
- o 특수한 공격에 대한 모델링이 아닌 운영 중인 방어체계에 따라 변화하는 공격자에게 대응할 수 있는 보안아키텍처, 위협모델링 및 이에 근거한 탐지/대응 방법을 명확한 인과관계에 의해 기술적으로 명확하게 제시하여야 함

귀하는 C사의 침해사고대응팀의 팀원으로 상기 위협에 대한 탐지/대응 방법을 수립하여야 합니다.