네트워크 보안 및 개인정보 보호

목차

네트워크 보안

1. 네트워크 보안이란?

▶ 조직의 네트워크 및 네트워크에 접근 가능한 리소스에 대한 공격을 방지하는 정책, 실행, 기술 등을 의미한다.

보안의 필요성

1. 허가받지 않은 외부 침입자에게 정보가 유출되지 않기 위해서
2. 외부 침입자가 보안 데이터의 내용을 조작하지 않도록 하기 위해서

네트워크 보안

2. 네트워크 보안의 3원칙

기밀성	정보의 비밀 유지
무결성	비인가된 변경으로부터 안전
가용성	필요할 때 언제든지 사용

이 원칙들 간에는 의존관계를 가지고 있다

네트워크 보안

3. 네트워크 공격 기술

공격유형

- **정상적**
- **1.전송차단**
- **2.가로채기**
- **3.변조**
- **4.위조**

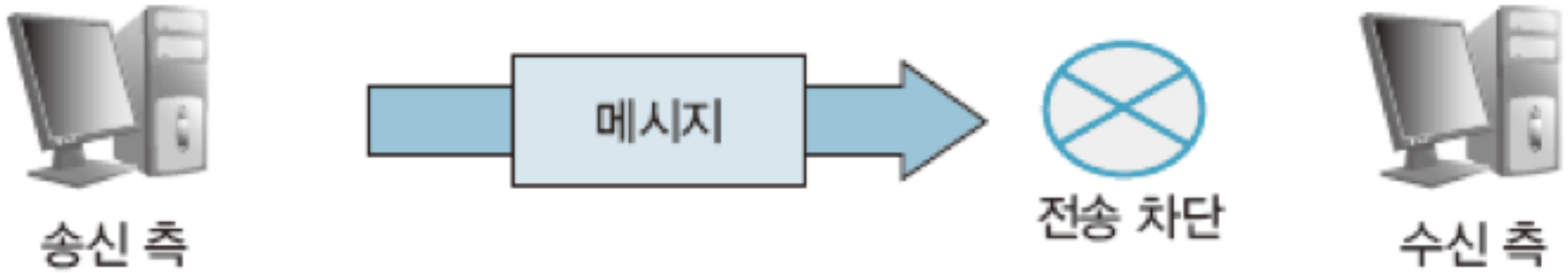
정상적으로 데이터를 전송할 경우의 모습

네트워크 보안

3. 네트워크 공격 기술

공격유형

- 정상적
- **1.전송차단**
- 2.가로채기
- 3.변조
- 4.위조



공격자가 송신 측이 수신 측과 연결할 수 없도록

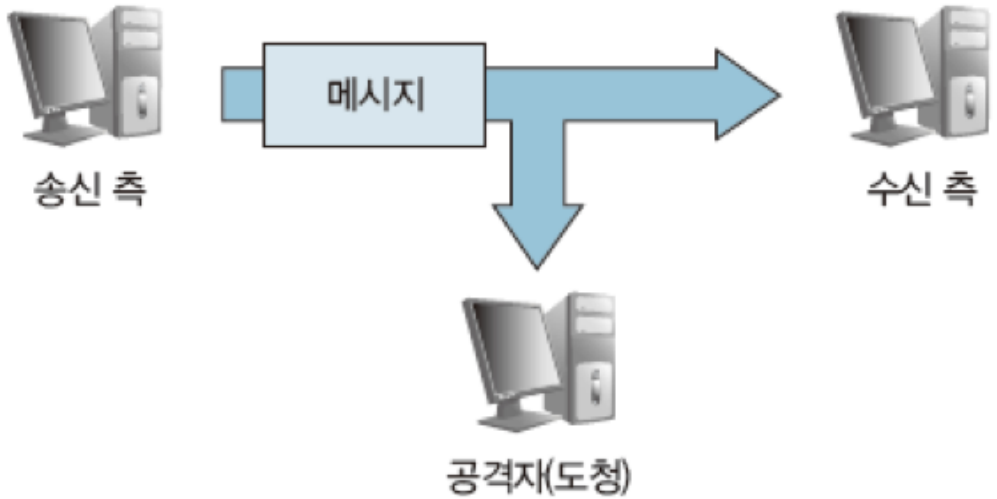
데이터 전송을 차단한다.

네트워크 보안

3. 네트워크 공격 기술

공격유형

- 정상적
- 1.전송차단
- **2.가로채기**
- 3.변조
- 4.위조



송신 측과 수신 측이 데이터를 주고 받는 사이

공격자가 데이터를 가로채어 도청을 한다.

네트워크 보안

3. 네트워크 공격 기술

공격유형

- 정상적
- 1.전송차단
- 2.가로채기
- **3.변조**
- 4.위조

공격자가 데이터를 가로채어, 데이터의 일부 또는 전부를 변경하여 잘못된 데이터를 수신 측에 전송한다.

네트워크 보안

3. 네트워크 공격 기술

공격유형

- 정상적
- 1.전송차단
- 2.가로채기
- 3.변조
- **4.위조**

마치 송신 측이 메시지를 전송한 것처럼 위조하여

수신 측에 전송한다.

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- **1.스푸핑**
- 2.스니핑
- 3.백도어
- 4.버퍼 오버플로우
- 5.DOS / DDOS
- 6.죽음의 핑

1. 스푸핑 (Spoofing)

스푸핑은 '속이다 ' 의 의미로, 속임을 이용한 공격의 총칭

- **엑세스 제어** : 내부 네트워크에 있는 송신지 주소를 가진 외부 네트워크 패킷을 모두 거부
- **필터링** : 송신지 주소를 보유하지 않은 패킷이 외부로 나가는 것을 차단
- **암호화** : ip스푸핑을 차단하는 가장 좋은 방법은 패킷을 암호화 하는 것

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- 1.스푸핑
- 2.스니핑
- 3.백도어
- 4.버퍼 오버플로우
- 5.DOS / DDOS
- 6.죽음의 핑

2. 스니핑 (Sniffing)

'코를 킁킁거리다 ' 또는 '냄새를 맡다 ' 는 뜻

네트워크를 이용하여 전송하는 데이터를 엿듣는 도청행위

네트워크 내 암호화 되지 않은 패킷들을 수집 후 재조합

- **암호화** : 패킷을 암호화하여 스니핑을 당하더라도 내용을 볼 수 없게 만든다.

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- 1.스푸핑
- 2.스니핑
- **3.백도어**
- 4.버퍼 오버플로우
- 5.DOS / DDOS
- 6.죽음의 핑

3. 백도어 (Backdoor)

'뒷문 ' 이라는 뜻. 허가받지 않고 우회를 통해 네트워크에 접속하는 권리를 얻는 행위

고의적으로 만든 비밀통로일 수도, 발견 못한 빈틈일 수도

- **취약점 체크** : 네트워크 취약점 점검 도구 등을 사용해 취약점 체크 및 보안

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- 1.스푸핑
- 2.스니핑
- 3.백도어
- **4.버퍼 오버플로우**
- 5.DOS / DDOS
- 6.죽음의 핑

4. 버퍼 오버플로우 (Buffer Overflow)

공격자가 과도한 데이터를 보내 고정된 길이의 버퍼를 흘러넘치게 하여 프로그램이 비정상적으로 동작하게 만드는 행위

- **안전한 함수** : 소프트웨어 개발 시 버퍼 오버플로우에 취약한 함수를 사용하지 않는다.

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- 1.스푸핑
- 2.스니핑
- 3.백도어
- 4.버퍼 오버플로우
- 5.DOS / DDOS
- 6.죽음의 핑

5. DOS/DDOS (Distributed Denial Of Service attack)

'서비스 공격'이라고도 한다.

대량의 접속을 유발해 해당 컴퓨터를 마비시키는 수법.

공격할 서버의 하드/소프트웨어를 무용지물로 만드는 행위

- 대역폭 제한, 시스템 패치, ip차단, 필요한 트래픽만 허용 등 여러가지 방어 대책이 존재

네트워크 보안

3. 네트워크 공격 기술

공격과 방어

- 1.스푸핑
- 2.스니핑
- 3.백도어
- 4.버퍼 오버플로우
- 5.DOS / DDOS
- 6.죽음의 핑

6. 죽음의 핑 (Ping of Death)

Ping명령을 실행하면 **ICMP**패킷을 원격 **ip**에 보내는데

이 때, 공격자는 패킷 구조를 크게 어긋나도록 변경시켜

공격 대상의 시스템을 과부화 시키는 것을 의미

- 핑을 이용한 공격은 라우터 수준에서 차단하거나 방화벽을 이용한 방어를 한다

네트워크 보안

4. 네트워크 보안 기술 (1)

보안유형

1.방화벽

2.침입탐지

3.침입방지

4.가상사설망

1. 방화벽 (Firewall)

외부 네트워크에서 내부 네트워크로 접근하려면

반드시 방화벽을 통과하도록 하여 내부 자원/정보 보호

- **패킷 필터링 :** 패킷의 송신지 및 목적지 ip,
  각 서비스의 포트 번호를 이용한 접속 제어

네트워크 보안

4. 네트워크 보안 기술 (1)

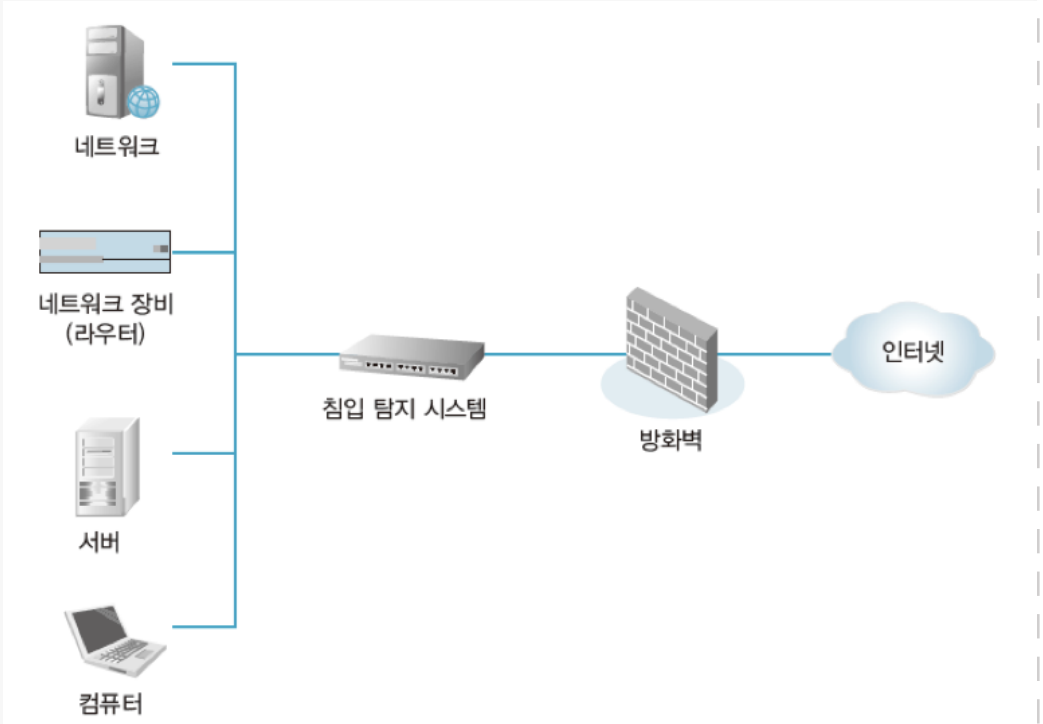
보안유형

- 1.방화벽
- 2.침입탐지
- 3.침입방지
- 4.가상사설망

2. 침입 탐지 시스템 (IDS)

방화벽처럼 단순한 접근 제어 수준의 통제만으로 악의적인 공격에 효과적 대처가 어려움.

→ 네트워크와 시스템 사용을 실시간 모니터링, 침입을 탐지하는 침입 탐지 시스템 등장



네트워크 보안

4. 네트워크 보안 기술 (1)

보안유형

- 1.방화벽
- 2.침입탐지
- **3.침입방지**
- 4.가상사설망

3. 침입 방지 시스템 (IPS)

네트워크에 상주하면서 트래픽을 모니터링하여
악성코드 및 해킹 등의 유해 트래픽 차단,
의심스러운 세션들을 종료시키는 등으로 네트워크 보호

- 보통 인터넷 방화벽 뒤편에 설치하여 방화벽으로
  필터링 할 수 없는 트래픽을 차단하는 형식으로 설치

네트워크 보안

4. 네트워크 보안 기술 (1)

보안유형

- 1.방화벽
- 2.침입탐지
- 3.침입방지
- 4.가상사설망

4. 가상사설명 (VPN)

네트워크에 상주하면서 트래픽을 모니터링하여
악성코드 및 해킹 등의 유해 트래픽 차단,
의심스러운 세션들을 종료시키는 등으로 네트워크 보호

- 보통 인터넷 방화벽 뒤편에 설치하여 방화벽으로 필터링 할 수 없는 트래픽을 차단하는 형식으로 설치

네트워크 보안

4. 네트워크 보안 기술 (2)

보안유형

5.안티 바이러스

6.통합 위험관리

7.웹 방화벽

8.네트워크 접근제어

5. 안티 바이러스

보통 바이러스 진단 및 치료하는 컴퓨터 백신 의미.

그러나 네트워크 안티 바이러스는 유입되는 바이러스 차단.

- 치료가 목적이 아닌 네트워크 레벨에서 차단이 목적

네트워크 보안

4. 네트워크 보안 기술 (2)

보안유형

5.안티 바이러스

6.통합 위험관리

7.웹 방화벽

8.네트워크 접근제어

6. 통합 위험 관리 (UTM)

기존의 다양한 보안기술 (방화벽, **IDS, IPS, VPN,** 안티바이러스 등)을 하나로 통합한 기술과 장비

네트워크 보안

4. 네트워크 보안 기술 (2)

보안유형

- 5.안티 바이러스
- 6.통합 위험관리
- 7.웹 방화벽
- 8.네트워크 접근제어

7. 웹 방화벽 (WAF)

일반적인 네트워크 방화벽과 달리 웹 어플리케이션 보안에 특화.

웹 서버의 취약점을 악용한 네트워크 공격을 탐지/차단

네트워크 보안

4. 네트워크 보안 기술 (2)

보안유형

- 5.안티 바이러스
- 6.통합 위험관리
- 7.웹 방화벽
- 8.네트워크 접근제어

8. 네크워크 접근 제어 (NAC)

사내망에 접근하는 모든 기기 검사 후

악성코드 감염, 기업 보안 정책에 따르지 않는 기기를 차단.

개인 정보 보호

1. 개인정보 의미

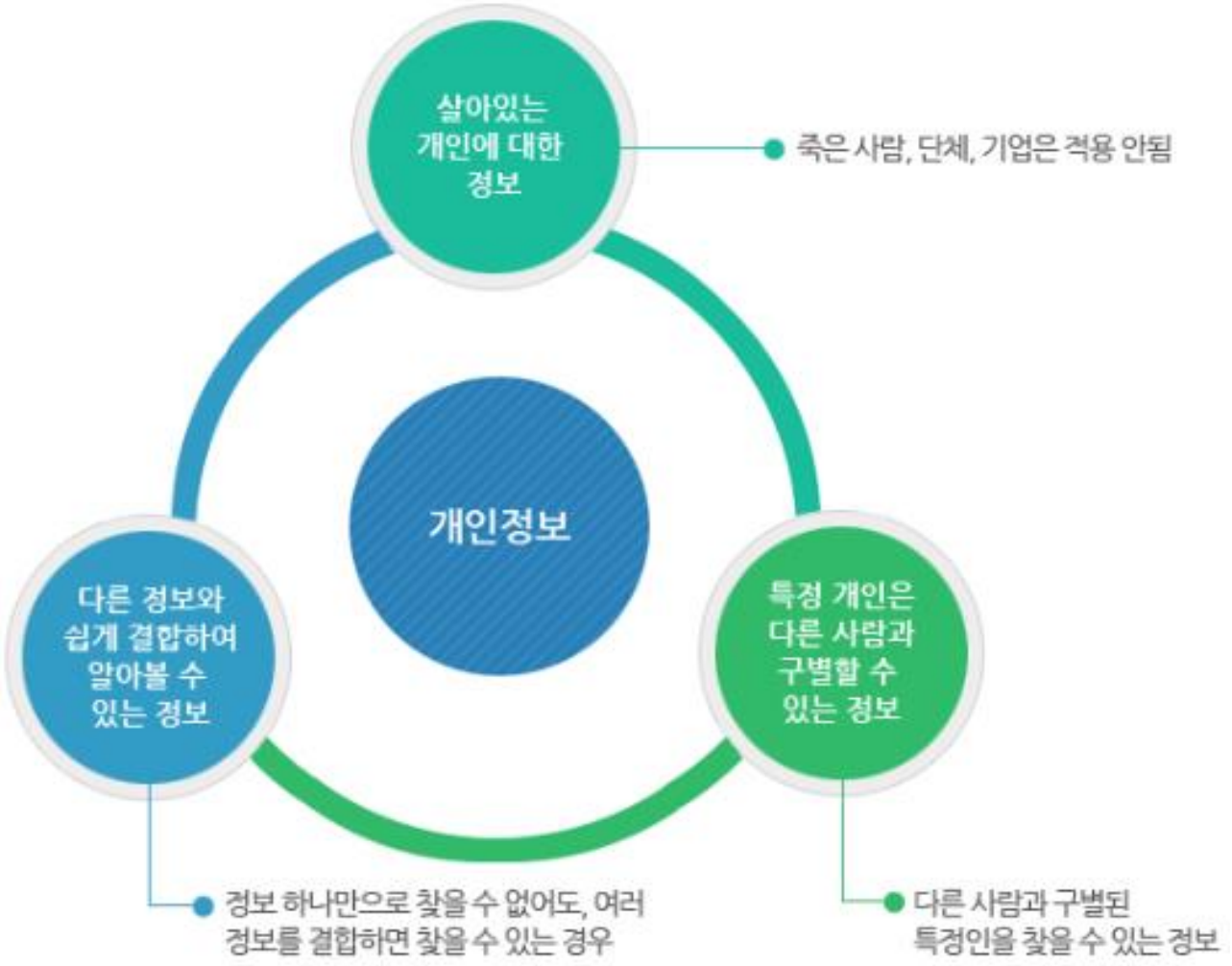
개인정보란?

-생존하는 개인에 관한 정보.

-개인을 식별할 수 있는 정보.

-식별할 수 없더라도 다른 정보와

용이하게 결합하여 식별할 수 있는 것 포함



https://www.pipc.go.kr/cmt/not/inf/notPerInfo.do

개인 정보 보호

1. 개인정보 의미

관련 법률

개인정보 보호법

"개인정보란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보"

정보통신망 이용 촉진 및 정보보호 등에 관한 법률

"개인정보란 생존하는 개인에 관한 정보로서 ... 특정한 개인을 알아볼 수 있는 부호,문자,음성,음향 및 영상등의 정보"

개인 정보 보호

2. 개인정보 보호의 원칙

OECD의 프라이버시 보호 8원칙	개인정보 보호법의 개인정보 보호 원칙
수집제한의 원칙	익명처리의 원칙
정보정확성의 원칙	처리목적 내 명확성,완전성,최신성 보장
목적 명확화의 원칙	처리목적의 명확화
이용제한의 원칙	목적범위 내에서 적법하게 처리, 목적외 활용금지
안정성 확보의 원칙	권리침해 가능성을 고려해 안전한 처리
처리방침 공개의 원칙	개인정보 처리방침 등 공개
정보주체 참여의 원칙	정보주체의 권리 보장
책임의 원칙	개인정보처리자의 책임준수,신뢰확보

정보보호 필요성

-정보화 사회 필수적 요소

-기업의 입장에서 자산적 가치 높음

-개인의 입장에서 안전과 재산 보호

https://blog.naver.com/kibani/220178527111

개인 정보 보호

3. 개인정보 해킹사례와 대응사례

국내

1. ‘여기어때’ 해킹 사건

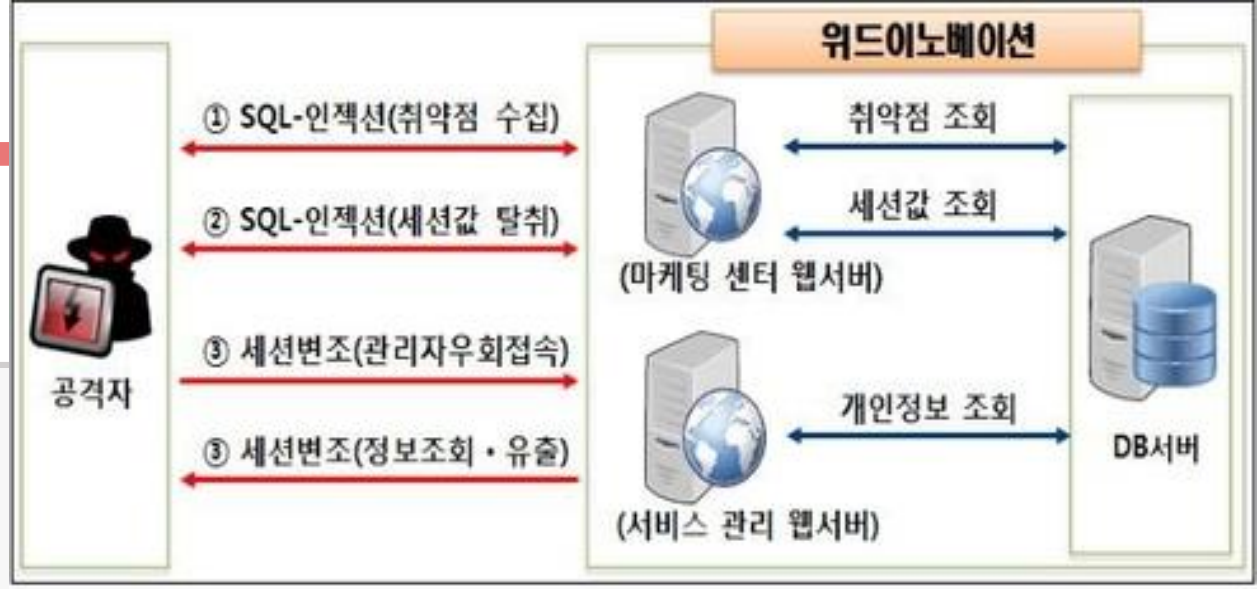
-숙박 O2O 서비스 ‘여기어때’를 서비스하는 위드이노베이션이 해킹으로 회원 91만명의 숙박정보 323건을 유출

-경찰 사이버 수사과는 6월 여기어때 해킹을 모의한 한국인 피의자 5명중 4명 검거

-해킹해 돈을 뜯어내기로 공모하고 중국인 해커를 고용해 행동으로 옮긴 것으로 드러남

개인 정보 보호

3. 개인정보 해킹사례와 대응사례



국내

1. '여기어때' 해킹 사건

- 방법

→ 여기어때 웹 사이트의 데이터베이스 취약점을 악용하는 인젝션 공격으로 관리자 고유 식별 값 탈취.

→ 이 관리자 고유 식별 값으로 외부에 노출된 관리 웹 페이지를 관리자 권한으로 우회접속해 유출

- 피해

→ 회원에게 성적 수치심을 주는 등의 문자 메시지 발송

-대응

→ 정부는 사생활 등 민감한 정보를 다루는 O2O서비스에 대한 보안 실태 점검 실시

개인 정보 보호

3. 개인정보 해킹사례와 대응사례

국내

2. '나야나' 해킹 사건

- 방법
→ 사용된 랜섬웨어 일종인 에레버스는 원래 윈도우 서버 타킷.
→ 그러나 윈도우는 공격하지 않고 리눅스 서버만 공격하는 변종.

- 피해
→ 한국 호스팅 업체가 랜섬웨어에 감염된 것은 인터넷 나야나가 최초
→ 피해 웹 사이트가 3400여개에 이르며 언론에 보도되지 않은 중소 쇼핑몰, 웹사이트의 자료/데이터베이스 유실, 신뢰도 저하 등 천문학적인 피해

-대응
→ 한국 인터넷 진흥원과의 상세 취약점 점검을 통해 추가 피해 예방을 위한 보안 지도와 기술 지원 제공
→ 유사한 피해가 발생하지 않게 사고 원인 분석, 타 호스팅 업체들에게 안내, 지원 계획

개인 정보 보호

3. 개인정보 해킹사례와 대응사례

해외

1. '앤섬' 해킹 사건

- 방법
→ 2015년 1차해킹에서는 워터링 홀 공격을 통해 관리자 비밀번호 유출
→ 2017년 2차 해킹에서는 서드파티 업체 직원이 개인정보가 담긴 파일을 계속해서 자신의 개인 이메일 계정으로 전송

- 피해
→ 2015년 건강 보험사 고객 및 직원 8000만명의 소셜 시큐리티 번호와 생년월일, 주소, 의료기록 등 신상정보 해킹 당함.

-대응
→ 2015년 유출로 보험사 앤섬은 고객들에게 2년간 무료 크레딧 모니터 및 신분도용 보호 서비스 제공 및 1억1500만달러(약 1254억원)을 지급하기로 합의
→ 2017년 유출로 정보가 거래되었거나 악용된 사례는 없으나 2년전 제공 서비스 동일제공

개인 정보 보호

3. 개인정보 해킹사례와 대응사례

해외

2. '에퀴팩스' 해킹 사건

- 방법
→ 해킹에 이용된 아파티 스프럿츠는 자바 기반 웹 어플리케이션 개발에 사용되는 오픈소스 프레임워크.
→ 이 프레임워크의 약점은 이미 발표되었지만 에퀴펙츠는 패치를 적용하지 않음.

- 피해
→ 자사 고객 1억4300만명의 개인정보 유출
→ 규모도 크지만,기본정보외 중요정보도 유출 돼 은행계좌탈취, 신용도용등 범죄악용 우려

-대응
→ 약 40억달러의 손실로 CIO와 CSO에 이어 CEO까지 사퇴
→ 보안 취약점을 방치해 개인정보 침해를 초래함에 따라 미국 내에 에퀴팩스를 대상으로 한 700억달러(한화 79조원)에 해당하는 집단소송 진행 중

개인 정보 보호

4. 개인정보 보편적 대응 방법

개인

1. 계정정보 도용 – 아이디와 비밀번호 변경
2. 명의도용 – 휴대폰 명의도용 방지 무료 서비스 가입, 명의 도용 방지 서비스 신청

기업

1. 경영진부터 일반 직원까지 보안 필요성 인식
2. 보안 전담 팀 구축
3. 핵심 자산의 접근은 최소 인원만 허가하고 관리
4. 필요한 경우 망을 분리
5. 보안 업데이트, 최신 백신을 설치하고 악성코드 침투를 예방

참고자료

- (모든 사진) 네트워크개론(한빛아카데미, 진혜진) Chapter09. 네트워크 보안
- (네트워크 보안이란?) 코드엔진 네트워크 보안 https://codeengn.com/archive/Network/
- (보안의 3원칙) 올드멍 블로그http://dyaniworld.tistory.com/13
- (보안의 3원칙) 시크릿츠 블로그
- https://m.blog.naver.com/PostView.nhn?blogId=xcripts&logNo=70093250812&proxyReferer=https%3A%2F%2Fwww.google.com%2F
- (스니핑) 중소기업융합학회 논문지 제 6권 제 2호 효율적인 스니핑 공격 대응방안 연구
- (Dos / DDOS) 나무위키 서비스 공격 https://ko.wikipedia.org/wiki/서비스_거부_공격#DoS_공격의_예방과_대응
- (IDS) Red Hat Enterprise Linux 4 보안가이드
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-ko-4/ch-detection.html
- (UTM) 코마스
- **http://fortistore.co.kr/file_pds/4_29_a/Fortigate-QnA.PDF**
- (WAF) 펜타 시큐리티
- https://www.pentasecurity.co.kr/resource/웹보안/웹방화벽이란/

참고자료

- http://cppg.tistory.com/entry/2-개인정보보호-원칙과-의무?category=639945
- 개인정보 사진 - https://www.pipc.go.kr/cmt/not/inf/notPerInfo.do
- 앤섬 해킹 사례 - http://www.boannews.com/media/view.asp?idx=65749
- 여기어때 해킹 사례 - http://it.chosun.com/news/article.html?no=2837409
- 에퀴팩스 해킹 사례 - http://www.ddaily.co.kr/news/article.html?no=160674
- 나야나 해킹사례 - https://byline.network/2017/06/1-792/
- 나야나 해킹 사례 - https://namu.wiki/w/%EC%9D%B8%ED%84%B0%EB%84%B7%EB%82%98%EC%95%BC%EB%82%98%20%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%20%EA%B0%90%EC%97%BC%20%EC%82%AC%ED%83%9C

감사합니다