## 신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안
# 학습정리

### 1차시 개인정보의 중요성 이해

**[개념학습] A기업 개인정보 인질사건**

A기업 개인정보 유출사건은 허술한 개인정보 관리로 인해 발생할 수 있는 전형적인 사례로, 수탁업체 직원에 대한 관리감독 미흡, 안전성확보조치 미이행, 주민등록번호와 여권번호 암호화 보관 미 이행이 원인이었다.

**1. 개인정보의 이해**

- 정보통신망법, 신용정보법 등 개별법을 적용받는 자(회사)라고 해서 개인정보보호법의 적용이 면제되는 것이 아니고, 법률의 내용이 상충되는 경우에 해당 개별법의 규정이 우선 적용된다.
- 개인정보란 ① '살아있는' 개인에 관한 정보여야 하며 ② '특정 개인에 관한 정보'이면서 ③ 개인을 '식별할 수 있는' 정보여야 한다. 또한 ④ '해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'도 개인정보이다.
- 그밖에 민감정보도 개인정보이므로 반드시 정보주체의 동의를 받은 후 수집해야 한다.

**2. 개인정보의 처리**

- 개인정보의 수집에서 제공, 파기까지의 전반적인 단계를 총칭하여 개인정보 생명주기(Life cycle)라 부르며, 법령에서는 수집, 이용, 제공, 파기에 관한 의무조치 사항을 규정하고 있으므로 처리 시 주의를 기울여야 한다.

**3. 개인정보처리자와 개인정보취급자**

- 개인정보처리자는 개인정보 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
- 회사의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 개인정보취급자로 정의한다.

**4. 개인정보의 안전한 보호는 사업의 성패를 가를 수 있다.**

- 정보통신기술의 급속한 발달 속에서 개인정보보호는 이제 사업의 성패를 가를 수 있는 중요한 부분이 되었다.

# 신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안
# 학습정리

## 2차시 개인정보의 생명주기

### [개념학습] 인기어플 개인정보 해킹사건

모 인기어플의 개인정보유출 사건은 해킹을 의뢰받은 중국인 해커가 웹페이지의 취약점을 이용해 SQL 인젝션 공격을 통해 개인정보를 탈취한 사건이다. SQL 인젝션 공격은 아주 초보적인 수준의 해킹 공격으로 홈페이지 보안만 제대로 되어 있어도 절대 일어나지 않을 사고였다.

### 1. 개인정보의 수집 및 이용

- 개인정보처리자는 반드시 정보주체에게 ① 수집 및 이용목적, ② 수집항목, ③ 보유 및 이용기간, ④ 동의 거부 권리 및 동의 거부 시 불이익에 대한 사항을 알리고, 동의를 받아야 한다.
- 명시적인 정보주체의 동의 없이 개인정보 수집이 가능한 경우는 ① 법률의 특별한 규정 또는 법령상 의무 준수, ② 공공기관이 법령 등에서 정한 소관업무 수행, ③ 정보주체와의 계약 체결·이행, ④ 정보주체 등의 생명, 신체, 재산의 이익 보호, ⑤ 개인정보처리자의 정당한 이익 달성이 필요한 경우이다.

### 2. 개인정보의 최소수집

- 개인정보처리자는 법령에 따라 목적에 필요한 최소한의 개인정보를 수집해야 하며, 최소한의 개인정보 수집이라는 것을 입증해야 할 책임을 가진다. 또한, 동의를 요하는 수집의 경우 필요최소한의 정보 외에 동의하지 아니할 수 있다는 사실 고지해야 하며, 동의를 하지 않는 경우 필요최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부해서는 안 된다.

### 3. 개인정보의 목적내 제공

- 개인정보처리자는 수집된 개인정보를 정보주체의 동의를 받거나, 수집한 목적 범위 내에서 개인정보를 제공하는 경우 개인정보를 제3자에게 제공할 수 있다.
- 처리위탁은 위탁자(개인정보처리자)의 업무처리 범위 내에서 개읶정보 처리가 행해지고, 위탁자의 관리·감독을 받게 되어 있다.
- 제3자 제공은 제3자의 이익을 위해서 개인정보가 처리되고, 제3자가 자신의 책임 하에 개인정보를 처리하고, 유출사고 발생에 따른 민형사상 책임을 지는 법적 구조를 가진다.

## 4. 개인정보의 목적외 이용 및 제공 제한

- 정보주체로부터 별도의 동의를 받은 경우
- 다른 법률에 특별한 규정이 있는 경우
- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
- 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

## 5. 정보주체 이외로부터 수집한 개인정보의 처리 제한

- 정보주체 이외로부터 개인정보를 수집하여 처리할 경우 개인정보처리자는 정보주체가 해당 사실을 인지하고, 개인정보 수집출처, 처리목적 등을 요구할 권리가 있다는 사실을 즉시 알려줘야 하는 고지의 의무를 가지고 있다.
- 개인정보처리자는 정보주체의 요구가 있을 경우 해당 요구가 발생할 날로부터 3일 이내 ① 개인정보의 수집 출처, ② 개인정보의 처리목적, ③ 개인정보 처리정지를 요구할 권리가 있다는 사실 등에 대해 반드시 고지해야 한다.

## 6. 개인정보의 파기

- 파기시기는 통상적으로 개인정보의 보유기간이 경과된 경우, 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내이며, 개인정보 처리목적 달성, 해당 서비시의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5일 이내로 파기해야 한다.

신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안

# 학습정리

## 3차시 개인정보의 보호조치

**[개념학습] 매우 미흡한 가상화폐거래소의 개인정보보호 수준**

인공지능, 사물인터넷, 클라우드, 빅데이터, 로봇, 블록체인, 비트코인…

4차 산업혁명시대의 기술들이 하루가 다르게 변하고 있으며 2020년에는 전세계 50억 명 이상이 네트워크에 연결될 것으로 예상된다. 4차 산업혁명시대 기술의 발전이 제대로 이루어지기 위해서는 보안과 개인정보보호가 반드시 뒷받침되어야 한다.

### 1. 개인정보의 안전성 확보조치의 개요

- 개인정보보호법과 개인정보보호법 시행령에서는 개인정보처리자가 개인정보보호를 위해 적절한 보호조치를 이행할 수 있도록 대통령령에 따른 안전성 확보에 필요한 기술적, 관리적 보호조치가 가능하도록 근거를 제시하고 있다.

### 2. 안전성 확보조치의 실천

#### 1) 내부관리계획의 수립 및 시행

- 내부관리계획은 개인정보처리자가 정보주체의 개인정보를 보호하기 위한 조치를 시행하기 위해 수립되어진 회사 전체에서 적용되는 내부규정(정책, 지침, 가이드 등)을 의미한다.

#### 2) 접근권한의 관리

- 개인정보처리시스템에 대한 접근통제를 실시하기 위해 접근이 가능한 권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여해야 한다. 또한, 권한의 부여뿐만 아니라 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경될 경우에는 해당 취급자의 시스템 접근권한을 지체 없이 변경 또는 말소해야 한다. 이때 해당 내역에 대해 최소 3년간 보관해야 한다.

#### 3) 비밀번호 설정

- 접근권한이 부여된 개인정보취급자와 정보주체가 안전한 비밀번호를 설정하여, 개인정보처리시스템에 접근할 수 있도록 비밀번호 작성규칙을 수립하여 적용해야 한다.

### 4) 접근통제

- 개인정보처리시스템에는 승인된 권한자 이외에 불법적 접근 및 유출시도 등을 탐지하고 방지하기 위해 관련 시스템을 설치 운영하도록 해야 한다. 개인정보처리시스템의 보호시스템은 접속권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응하도록 설정해야 한다.

### 5) 모바일 기기와 관리용 단말기 통제

- 개인정보처리자는 개인정보취급자가 모바일 기기와 관리용 단말기를 통해 개인정보처리시스템에 접속한다면 해당 단말기에서 P2P 프로그램을 사용하지 않도록 조치해야 하는 것이 적절하다. 특히, P2P 프로그램의 단순 사용금지 뿐만 아니라 시스템 상에서 해당 포트를 차단하는 등의 조치를 취하도록 해야 한다.

### 6) 개인정보의 암호화

- 개인정보처리자는 개인정보처리시스템에서 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에 반드시 암호화해야 한다. 개인정보 저장시 암호화 대상은 비밀번호 및 바이오 정보로 개인정보취급자의 단말기, 모바일 기기 등에 파일로 저장할 때 적절한 암호화 방식으로 암호화해야 한다.

### 7) 접속기록의 위·변조 방지

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관.관리하여야 하며, 개인정보의 분실.도난.유출.위조.변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 필수적으로 점검하여야 한다. 더욱이 개인정보취급자의 접속기록이 위.변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

### 8) 악성프로그램 방지

- 개인정보처리자는 악성프로그램 등을 통해 발생할 수 있는 감염을 방지하기 위해 이를 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태를 유지하도록 한다.

### 9) 물리적 안전조치

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에 개인정보 유출에 대비하여 출입통제 절차를 수립·운영하여야 한다.

### 10) 개인정보의 파기

- 개인정보처리자는 이용목적이 달성된 개인정보 파일을 완전 파기할 경우 ① 완전파괴 (소각·파쇄 등), ② 전용 소자장비를 이용하여 삭제, ③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기를 수행해야 한다.

### 11) 기타 보호조치

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에 개인정보 유출에 대비하여 출입통제 절차를 수립·운영하여야 한개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치하던지, 본래 목적 외로 사용되지 않도록 조치해야 한다. 또한 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안

# 학습정리

## 4차시 개인정보의 처리제한

**[개념학습] 최근 5년간 개인정보보호 위반 행정처분 증가세**

랜섬웨어, 스피어피싱(spearphishing), IoT 기반 공격에 자동화가 더해지면서 공격은 더욱 정교해지고 곧 AI가 동원된 공격도 등장할 것이으로 예상된다. 우리나라에서도 개인정보보호법 위반에 따른 행정처분 건수가 계속 증가하고 있는데, 이는 정부 차원에서 현장점검 강화 등 단속이 강화하고 있기 때문이다.

### 1. 처리하면 안 되는 정보들

#### (1) 민감정보의 처리제한

- 민감정보는 다르게 사생활 정보로 불리어지며, 개인정보보호법 상에서
  ① 사상 및 신념, ② 노동조합 및 정당의 가입 및 탈퇴, ③ 정치적 견해, ④ 건강, 성생활 등에 관한 정보, ⑤ 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 지칭하고 있다.

#### (2) 고유식별정보의 처리제한

- 고유식별정보란 개인을 공유하게 구별하기 위해 부여된 식별정보로써, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 4가지를 의미한다. 정보주체에게 유일하게 부여된 정보임에 따라 유출 시 큰 피해가 발생할 수 있기 때문에 고유식별정보도 민감정보와 같이 원칙적으로 수집을 금지하고 있다.

#### (3) 주민등록번호 처리제한

- 2014년 8월 이후 주민등록번호에 대한 처리기준이 보다 엄격해짐에 따라 법률, 대통령령, 국회규칙, 대법원규칙 등에 근거 없이는 주민등록번호를 요구하거나 수집할 수 없으며, 해당 사항을 위반할 경우 3천만원 이하의 과태료가 부과된다.

## 2. 개인정보가 옮겨질 때

### (1) 개인정보 처리 업무 위탁

- 개인정보처리자가 정보주체의 개인정보를 제3자에게 개인정보 처리업무를 위탁하는 경우에는 반드시 문서에 의해 처리되어야 한다. 이때 처리와 처리 업무위탁은 구분되어야 하는 정의로 개인정보보호법 제2조에서는 "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위로 정의하고 있다. 또한, 처리 업무위탁은 개인정보처리를 대신 수행할 수 있도록 하는 행위에 해당하는 정의로 볼 수 있다.

### (2) 영업 양도에 따른 개인정보의 이전 제한

- 개인정보처리자는 영업의 전부 또는 일부의 양도 및 합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 해당 정보주체에게 반드시 알려야 한다. 이때 개인정보의 이전을 받은 영업양수자 등은 개인정보를 이전 받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야 할 고지의 의무가 있다.

## 3. 정보주체의 권리보장

- 정보주체는 자신의 개인정보에 대해 직접 제공한 개인정보 외에도 제 3 자 또는 공개된 소스로부터 수집한 개인정보 열람을 요구할 수 있으며, 만 14 세 미만 아동의 경우 법정대리인을 통해 가능하다 열람을 요구할 경우 행정안전부령으로 정하는 바에 따라 열람하려는 사항을 표시한 ‘개인정보 열람요구서’를 개인정보처리자에게 제출하여 자신의 권리를 보장받을 수 있다.

## 4. CCTV 등에 따른 영상정보처리 제한

- 개인정보보호법에서는 우리가 백화점, 길거리, 주차장 등에서 자주 접하고 있는 영상정보처리기기에 의하여 촬영 및 처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상에 대해 해당 권리를 보호할 수 있도록 CCTV 등에 따른 영상정보처리의 제한을 규율하고 있다.

## 신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안
# 학습정리

### 5차시 최근 정보보안 사고 사례

**[개념학습] 숙박앱 W사의 해킹사고 및 개인정보 유출**

업계에서 세계 1위로 유명한 국내 모 기업은 특히 서비스평가에서 10년째 세계 1위를 이어가고 있는 중 출입보안에 구멍이 생겼고 절차를 밟지 않은 고객이 무단으로 출입금지지역에 들어가는 CCTV영상이 언론에 보도되며 크게 평판이 훼손되고 말았습니다. 당장의 성과에 급해 보안에 투자를 하지 못한 결과였습니다.

**1. CASE1. 랜섬웨어 유포 사례**

- 2018년 3월부터, 한국어로 작성된 이메일을 통해 갠드크랩(GandCrab) 랜섬웨어(Ransomware) 유포가 지속적으로 발생하고 있다. 유포자는 악성코드가 포함된 이메일을 통해 수신자의 PC를 공격하였으며, 파일 복구의 대가로 200만원 상당의 금액을 요구하고 있는 실정이다.

**2. CASE2. 웹 호스팅 업체 N사 보안 사고 사례**

- 2017년 6월 국내 유명 웹 호스팅 업체인 N가 랜섬웨어에 감영되는 해킹사고가 발생되었다. N사의 서버 153대가 랜섬웨어에 감염되면서 5,496개의 홈페이지 서비스에 장애가 발생하였다. 사고원인은 웹·백업서버 등 주요 서버에 접속할 수 있는 관리자PC가 인터넷에 접속 가능하여 취약하였고 ID·비밀번호만으로 서버 접근을 허용해 계정탈취에 대한 대책이 미흡하였다.

**3. CASE3. 평창 동계올림픽 APT공격 사례**

- 2018년 2월 평창 동계올림픽 개막일에 미상의 해커 그룹이 장기간에 걸쳐 치밀하게 준비한 지능형지속공격(APT)이 발생되었다. 평창 동계올림픽 조직위원회에 따르면, 공격에 쓰인 악성코드 41종을 확보해 분석한 결과 25개가 실제 평창 동계올림픽 시스템 파괴에 활용됐다.

**4. 소셜 커머스 업체 W사 보안 사고 사례**

- 2017년 6월 소셜 커머스 업체인 W사의 홈페이지에서 수만건의 고객 계좌번호와 환급내역 등 개인정보가 무방비하게 노출되었다. 이는 홈페이지를 업데이트하는 과정에서 내부직원의 실수로 인하여 발생된 것으로 총 35,000건의 개인정보가 유출되었다. W사의 위반 사항은 개인정보 유출신고를 지연시켰으며, 개인정보에 대한 접근통제가 미흡했다.

## 신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안
# 학습정리

### 6차시 정보보안 실천수칙

**[개념학습] 적은 내부에 있다.**

A기업과 드럼 세탁기 모터기술의 세계 1위 기업의 경우 내부 직원이 고액을 받는 조건으로 중국업체에 내부 기술을 불법 유출하여 상당한 영업손실을 입었다. 많은 기업들이 정보보호를 위해 가장 중요하게 여기는 것이 바로 내부보안이며, 상당수의 정보유출이 내부자의 고의 또는 실수로 발생한다.

**1. 정보보호 실천수칙(기업편)**

- 2017년 11월 생활 정보신문 I사의 서버 15대 계정정보가 해킹당해 랜섬웨어에 감염되는 사고가 발생하여 전국 사이트가 며칠 동안 서비스가 중단되었다. 조사 결과 I사는 계정관리 보안이 미흡한 점이 밝혀졌고, 이에 대한 보호 대책이 시급하였다. 반면, I사는 매일 백업을 수행하고 주 1회 물리적 백업을 진행하여, 이번 사고에서 큰 피해 없이 복구시킬 수 있었다. 이러한 크고 작은 보안사고에 기업이 대응하기 위하여 기업은 정보보호 실천수칙을 인지하여 정보보안에 힘써야 한다.

**2. 정보보호 실천수칙(개인편)**

- 국내 파일공유사이트를 통해 한글 소프트웨어로 위장한 해킹프로그램이 유포되었는데, 해당 해킹프로그램은 한글 소프트웨어의 최신버전인 '한글 2018'을 모방하여, '한글 2018' 무설치 인증판이라는 이름으로 실제 한글파일과 같은 1.3GB의 대용량 파일크기로 만들어졌다. 공식적인 경로로 다운받지 않은 불법 소프트웨어는 보안 위협에 노출될 수 있으므로, 반드시 정품 소프트웨어를 사용해야 한다. 개인 PC를 지키기 위한 정보보호 실천 10가지 수칙을 인지하여 정보보안을 생활화 해야 한다.

**3. 정보보호 실천수칙(스마트폰)**

- 개인정보 뿐만 아니라 금융정보도 담겨 있는 스마트폰은 분실하거나 도용될 경우 범죄에 악용되기 쉽다. 스마트폰 범죄를 예방하기 위해서는 주기적으로 메신저나 SNS 비밀번호를 변경하고 바이러스 검사를 하여야 하며, 출처가 불분명한 문자메시지 등은 보는 즉시 바로 삭제해야 한다. 가족 및 지인 등이 메신저로 금전을 요구하는 경우와 소액결제를 사칭하는 문자메시지의 경우 반드시 결제서비스 업체 공식 대표번호 또는 통신사에 전화하여 사실여부를 확인해야 한다.

신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안

# 학습정리

## 7차시 정보보안 실천수칙

### [개념학습] 가상화폐 도난사건

최근 가상화폐에 대한 관심이 커지면서 가상화폐와 관련된 다양한 해킹 수법이 발견되고 있다. 2018년 1월, 일본에서는 5천6백억원 규모의 가상화폐가 사라지는 사상 최대의 가상화폐 해킹사건이 발생했다. 그로부터 얼마 후 이탈리아의 가상화폐 거래소에서 1850억원 상당의 가상화폐가 무단 인출되었으며 우리나라에서도 가상화폐 운영회사가 해킹 공격으로 전체 자산의 20% 정도를 잃고 파산절차에 들어가기도 했다.

### 1. 악성코드의 정의

맬웨어(Malware) 또는 악성 프로그램이라고도 불리는 악성코드는 악의적인 목적을 위해 작성된 실행 가능한 코드를 총칭한다.

#### 1) 바이러스

- 바이러스란 프로그램 또는 실행 가능한 부분을 변형해 자기 자신이나 변형된 자신을 복사하는 프로그램이다. 감염대상을 복제해 감염시키고 다른 대상을 감염시킴으로써 확산된다.

#### 2) 웜

- 다른 프로그램의 감염없이 자신 혹은 변형된 자신을 복사하는 프로그램이다. 기억장소에 코드 형태나 실행파일로 존재하며, 실행되면 파일이나 코드 자체를 다른 시스템으로 복사한다.

#### 3) 트로이목마

- 트로이목마는 컴퓨터 사용자는 알 수 없도록 프로그래머가 고의로 포함시킨 자기 자신을 복사하지 않는 프로그램이다.

### 2. 악성코드 최신 동향

- 매일 새로운 악성코드가 만들어지고 있으며, 많은 PC 및 서버에 피해를 입히고 있다. 2017년 기준 악성코드 동향을 분석한 결과, 가장 많이 발견된 랜섬웨어에 이어 정보탈취 등 다양한 유형의 악성코드가 확인되었다. 또한 기타 해킹도구가 46건 (7%)이 수집되어 악성프로그램을 이용한 해킹공격이 현재도 증가하고 있음을 알 수 있다.

### 3. 악성코드 해킹 사례

### 1) 랜섬웨어

- 2017년 5월 교통범칙금 인터넷 납부 및 교통조사예약 시스템인 ‘eFINE’을 사칭한 메일에 첨부된 랜섬웨어가 발견되었는데, 이전에 발견된 ‘OO경찰서’를 사칭한 교통위반고지 랜섬웨어와 동일한 수법을 사용한 또 다른 버전으로 확인되었다. 유포된 ‘[eFINE]위반사실 통지 및 과태료 부과 사전통지서’란 이름의 해당 이메일은 ‘eFINE 교통범칙금 인터넷 납부’에서 보낸 것으로 위장하고 있다.

### 2) 가상화폐 채굴 악성코드

- 2017년 12월 디그마인(Digmne)이라는 악성코드가 페이스북 메신저를 통해 무차별하게 유포되었고, 암호화폐 모네로(Monero) 채굴기를 설치하고 추가 전파를 돕는 악성 크롬 확장프로그램까지 설치하였다.

### 3) 메모리 해킹 악성코드

- 2017년 2월 메모리 해킹 악성코드가 광고, 쇼핑 도우미, 검색 도우미 등의 애드웨어 프로그램 업데이트 기능을 악용하여 설치되었다. 악성코드가 동작하면 우선 백신을 무력화시키고, 이후 메모리 해킹을 통해 금융 보안 모듈의 정상 작동을 막았다.

### 4) 이력서로 위장한 악성코드

- 국내 대표 채용사이트에서 발송된 것처럼 위장한 메일로 악성코드가 유포되었다. 메일에는 금융권 입사지원에 대한 내용이 포함되어 있었으며, 채용 사이트로 연결을 유도하는 가짜 링크를 통해 이력서 파일이 다운로드 된다.

신기한 보안사전, 알고 보면 더 잘 보이는 개인정보보호와 정보보안

# 학습정리

## 8차시 정보보안 전망과 대응

### [개념학습] 아무도 접근할 수 없는 정보의 철옹성

에어갭(air gap) 즉, 망분리 시스템은 단 한 번의 해킹도 허용하면 안되는 시스템의 마지막 대피소로 랜선을 뽑아 오프라인을 만들면 원격 해커가 접근할 수 없는 물리적인 접근이 불가능해진다. 하지만 망분리 시스템이라고 해도 USB를 꼽거나 CPU의 전자기 신호를 사용하거나 하는 다양한 방법이 나오기 시작했다.

### 1. 커져만 가는 보안위협

- 매년 해킹사고, 진화된 악성코드, 새로운 취약점 등 보안위협은 변함없이 진화를 거듭하며 커져만 가고 있다. 지난해 보안사고 사례를 통한 트렌드를 분석한 결과, 지능형 랜섬웨어의 공격 진화, 가상화폐 등 금전적 이익을 목적으로 하는 공격 증가, Iot 기기 해킹 등 총 7가지의 사이버 공격이 대세를 이룰 것으로 전망했다.

### 2. 주목해야 하는 위협들

#### 1) 지능형 공격과 결합한 랜섬웨어 공격 진화

- 인터넷 웹 호스팅 업체의 랜섬웨어 공격 이후, 전 세계를 대상으로 무작위로 유포되던 랜섬웨어가 특정 국가인 한국(한글 윈도우 운영체제)을 대상으로 하여 올크라이 랜섬웨어, 마이랜섬, 에레버스 등 다양한 랜섬웨어가 등장하였다.

#### 2) 가상화폐 관련 서비스와 금전적 이익을 노리는 공격 증가

- 최근 금전적 이득 목적의 공격들이 많이 발생하면서 사행성 게임 이용자들 정보를 탈취해 금전을 탈취하거나, 가상화폐 소유자를 대상으로 한 피싱공격과 랜섬웨어 공격이 발생되는가 하면, ATM이 해킹되어 감염된 ATM을 통한 금융거래정보가 탈취 및 유통되었다.

#### 3) S/W 개발체계 해킹을 통한 대규모 악성코드 감염

- 소프트웨어 개발업체를 직접 해킹하여, 개발단계부터 악성코드를 백도어로 심어서 배포하는 형태의 공격이 증가하고 있다. 또한 소프트웨어 개발업체의 업데이트 서버와 같은 공급망을 장악해 정보를 유출하는 공격망 공격(Supply Chain Attack)도 발생하였다. 가장 최근에 일어난 공급망 공격의 사례로는 골든아이(GoldenEye) 랜섬웨어 사건이 있다.

#### 4) 취약한 Iot 기기의 오프라인 범죄 악용

- Iot 기기(Internet of Things, 사물인터넷)의 취약점을 악용한 범죄가 발생하면서 최근 Iot 기기 쪽에서 가장 큰 키워드를 꼽자면 봇넷(Botnet)으로 사물인터넷 기기들의 취약점(디폴트 암호)을 통해 기기 통제권을 장악한 다음, 다량의 트래픽을 발생시켜 주요 웹 서비스들을 마비시킨 악성코드인 미라이봇넷(Mirai Botnet) 등 여러 변종들이 발견되었다.

### 5) 사회적 이슈 관련 대규모 공격 위험

- 사회적 이슈를 바탕으로 사용자로부터 접근하도록 유도하여 악성코드 감염을 시도하는 방식이다. 기업 및 정치 관련 뉴스는 물론 가짜뉴스를 생산하여 공격에 이용한다. 그 결과 사드 보복성 해킹 공격뿐만 아니라, 서울시 38세금징수과 및 eFine 교통범칙금 사칭 이메일 악성코드 공격도 발생하였다. 최근에 가장 큰 이슈였던 평창 동계올림픽을 이용한 다양한 공격이 시도되었다.

### 6) 악성코드 감염 및 유포 방법의 다양화

- 네이버 계정정보 탈취 사칭사이트 등 가짜 사이트를 만들어 상당히 많은 악성코드들이 유포되고 있으며 유명 웹하드 P2P사이트를 통해 불특정 다수에게 악성코드도 유포되고 있다.

### 7) 중앙관리 S/W 취약점 및 관리 미흡을 통한 표적공격 지속

- 최근 중앙관리 소프트웨어 취약점을 이용해 군 정보가 해킹된 사고가 있었다. 이 공격은 외부적 소프트웨어 취약점을 이용해 들어오는 경우와 내부적 관리자들의 관리 미흡 등 여러가지 요인에 의해 발생하였다. 2018년에는 스마트폰 모바일 단말관리 소프트웨어 등을 통해 Iot 기기 봇넷 공격이 이루어지거나, 주요 인사들 스마트폰에서 정보 유출 등의 공격이 이루어질 수 있다.