보안담당자가 겪는 실무적 이슈와 법률적 검토

구 태 언

테크앤로 법률사무소 대표변호사
taeeon.koo@teknlaw.com

TEK&LAW

연사 소개

구 태 언 대 표 변 호 사

- 제34회 사법시험 합격, 사법연수원 제24기 수료
- 서울중앙지방검찰청 첨단범죄수사부 검사
- 김앤장법률사무소 변호사 (정보보호·부정조사 팀장)
- 안전행정부·방송통신위원회·개인정보보호위원회·미래창조과학부·대검찰청 디지털수사·특허정보원 영업비밀보호센터 등 자문변호사
- 한국정보보호학회·한국정보처리학회 이사
- 2012 정보보호대상 수상
- 2013 개인정보보호대상 수상
- 2014 개인정보보호위원회 위원 위촉
- 2015 특허청 산업재산권 법제위원회 위원 위촉
- 2015 한국정보처리학회 이사 위촉
- 2015 금융위원회 법령해석심의위원회 위원 위촉
- **현) 테크앤로 법률사무소 대표변호사**

- 고려대학교 법과대학 (법학사)
- 고려대학교 정보보호대학원 (공학석사)
- Santa Clara University Law School (Visiting Scholar)

사고 대응 및 보안담당자가 겪는 실무적 이슈

정보통신망 침해 관련 이슈

질의의 내용

침해사고를 분석하던 중 악성코드를 발견하여 역공학(리버싱 엔지니어링)을 해본 결과, 국내에서 호스팅되고 있는 서버에서 추가적인 악성코드를 다운받는 것을 확인하였습니다. 현재 추가적인 악성코드는 삭제되어 해당 시스템에서 어떤 기능을 수행했는지 알 수 없는 상태입니다. 분석가는 이에 악성코드를 분석하여 알아낸 국내 호스팅 서버에 접근하여 추가적인 악성코드를 다운받았습니다. 이 행위가 정당한가요? 정당하지 않다면 어떤 식으로 해결해야 할까요?

위와 같은 상황에서 국내 호스팅되고 있는 서버가 ID/PASS로 제한되어 서비스가 제공되는 경우, 악성코드 분석으로 해당 서버의 주소, ID, PASS를 모두 알아내어 이를 통해 국내 서버에 로그인하여 추가 악성코드를 다운받은 경우, 이 행위가 정당한가요? 정당하지 않다면 어떤 식으로 해결해야 할까요?

정보통신망 침해 관련 이슈

악성코드의 수집과 정보통신망의 침해

해커	• 해커는 범죄인 ✓ 언제든 법 위반 가능
보안 담당자	• 정보통신망법 제48조 제1항(정보통신망 침해행위 등의 금지) • 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다 • 정보통신망법 제49조(비밀등의 보호) • 악성코드는 비밀에 해당하지 아니함

정보통신망 침해 관련 이슈

질의의 내용

웹사이트에서 유포되고 있는 악성코드의 현황을 살펴보고 악성코드 샘플을 얻기 위해 국내 호스팅되고 있는 웹사이트를 크롤링(Crawling)한 경우 이것이 정당한가요? 정당하지 않다면 어느 선에서 크롤링이 이루어져야 하나요?

- 크롤링 과정 중에 특정 웹사이트가 robots.txt 파일로 크롤링을 제한시켜 두었는데 이를 무시하고 크롤링하여 해당 웹사이트의 파일을 다운받은 경우 정당한가요?

정보통신망 침해 관련 이슈

크롤링(Crawling)의 허용 범위

	일반적 접근 허용	특정인 접근 허용
백화점 등 대중이용시설	물건 파는 곳/공중 화장실 등 일반인의 접근이 허용된 장소	STAFF ONLY 등 직원 전용 시설
정보통신망	1. 일반인에게 접근이 허용된 웹 페이지 2. Robots.txt 파일이 없는 경우 3. Robots.txt 파일에서 접근을 제한하지 않는 디렉토리/웹 페이지	1. Robots.txt로 크롤링 전부를 제한하는 경우 2. Robots.txt로 특정 디렉토리만을 제한한 경우 그 디렉토리
대법원 판례	• 접근권한을 부여하거나 허용되는 범위를 설정하는 주체는 서비스제공자 • 권한을 부여 받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단 (대법원 2005. 11. 25. 선고 2005도870 판결)	

개인정보 관련 이슈

질의의 내용

우리 회사의 개인정보가 중국의 모사이트에서 유료로 거래되고 있다는 기사가 나왔습니다. 이에 보안담당자는 자사의 정보가 맞는지 확인하기 위해 기자를 통해 정보를 얻고자 했으나 기자가 제공해 주지 않자, 중국의 모사이트에 가입하여 유료로 개인정보를 구입하였습니다. 이 행위가 정당한가요? 정당하지 않다면 어떤 식으로 해결해야 할까요?

개인정보 관련 이슈

개인정보의 수집 이용 근거

- 회사는 개인정보의 취급권한 보유
- 수집이용근거
  - 개인정보주체의 동의
  - 개인정보 보호법 제15조
  - 정보통신망법 제22조
- 오히려 개인정보 “보호활동”으로 볼 수 있음
  - 계약상 의무이행
  - 개인정보 보호법 제15조 제1항 제4호
  - 정보통신망법 제22조 제2항 제1호

개인정보 관련 이슈

질의의 내용(1)

'A' 사용자는 'B' 회사의 카드를 사용하고 있었습니다.
'B' 회사의 카드는 친구에게 마일리지를 선물하는 기능이 있습니다.
어느 날 'A' 사용자의 카드 마일리지 10만이 모르는 사람에게 선물되어 'A' 사용자는 현금 10만원 상당의 피해를 입었습니다.
'A' 사용자는 'B' 회사에게 자신은 마일리지를 선물한 적이 없다며 'B' 회사에게 이와 같은 사실을 문의하였고, 'B' 회사는 문의를 접수하여 결제 시스템 등을 살펴 보았지만 해당 마일리지 선물거래는 정상적인 거래여서 사용자에게 정상적인 거래였다는 통보를 합니다.
그리고 'B'사는 'A' 사용자 스마트폰에 악성 앱이 설치되었을 수 있다는 의심을 합니다.

개인정보 관련 이슈

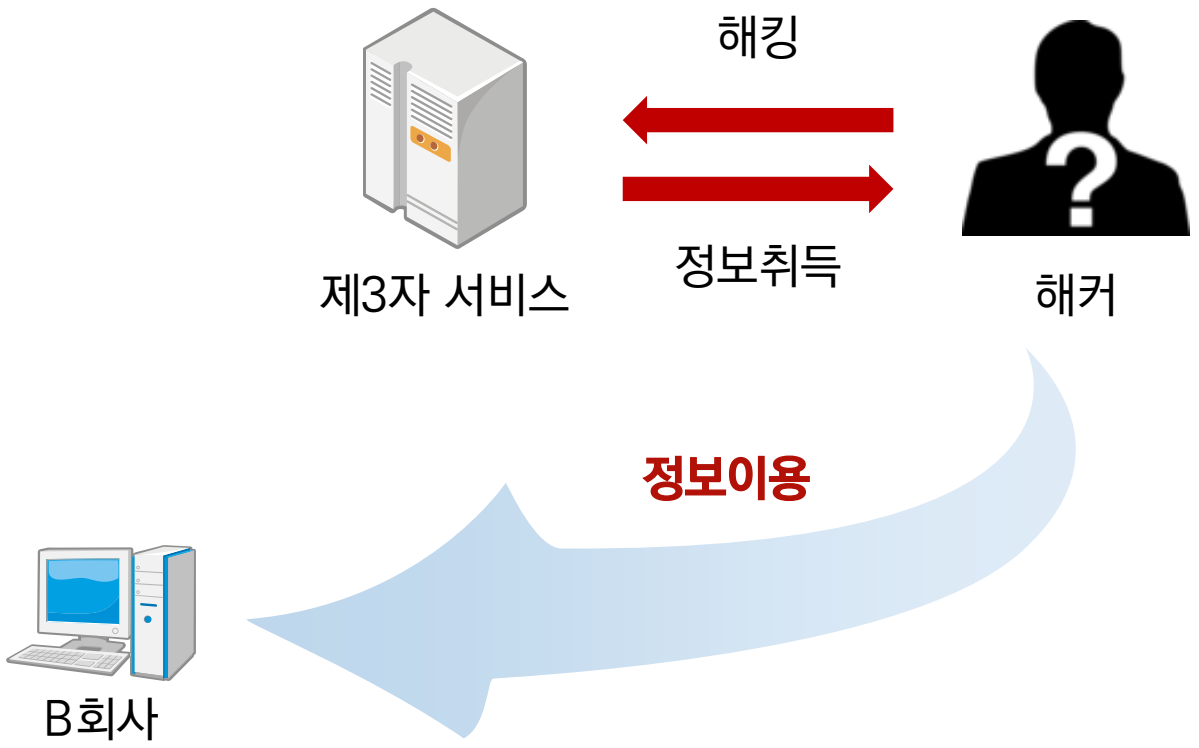
질의의 내용(2)

이를 듣고 'A' 사용자는 사이버수사대에 악성 앱 설치 여부 판단을 의뢰합니다.
하지만 분석결과 이상 없음을 통보 받습니다.

이에 'A' 사용자는 악성 앱 설치도 없고 자신은 결제한 적이 없다며 'B' 회사에게 법적 책임을 묻겠다는 이야기를 합니다.
이에 'B' 회사는 자신들에게 문제가 없다는 것을 증명하고자 침해사고 분석업체에게 이와 같은 사건으로 분석을 의뢰하며 분석업체는 마일리지를 무단으로 선물한 공격자가 제3의 서비스에서 유출된 계정정보를 이용하여 'A' 사용자의 마일리지를 무단으로 사용했다는 결과를 내놓습니다.
이와 같은 사건에서 누구의 책임이 더 큰 것인가요? 부정거래에 대한 최소안전대책을 강구하지 않은 'B' 회사에게 책임이 있는 것인지, 계정/패스워드 등을 동일하게 사용한 'A' 사용자에게 책임이 있는 것인지 궁금합니다.

개인정보 관련 이슈

개인정보 유출과 법적 책임의 소재



개인정보 유출과 법적 책임의 소재

법적 책임

- A 사용자
  - ✓ 책임 없음

- B 회사
  - ✓ 정보통신서비스 제공자가 모든 해킹을 방어하는 것은 사실상 불가능
  - ✓ 최소한의 안전 대책 강구 여부를 판단
  - ✓ 정보통신망법 제29조(안전조치의무) : 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다

- 제3자
  - ✓ 정보통신망법상 기술적/관리적/물리적 조치를 취하지 아니한 것으로 보임
  - ✓ 해커와 연대하여 손해배상

형법/저작권법 관련 이슈

질의의 내용

보안업체에서 사용자 방문기록을 추적하여 특정 광고창을 생성하는 플러그인을 '악성프로그램'으로 정하고 진단 · 삭제하였습니다. 그러자 해당 플러그인 제작사로부터 업무방해 명목의 고소를 당하였습니다. 이런 경우 보안업체를 보호하기 위한 법적 장치가 있는가요?

형법/저작권법 관련 이슈

악성프로그램의 진단/삭제

동의 받아 설치된 경우	• 광고프로그램이 이용자의 동의를 받아 설치된 경우 ✓ 해당 악성프로그램을 진단/삭제한 것은 오탐지에 해당 ✓ 적법한 광고 업무 방해시, 형법상 업무방해죄 성립 ✓ 민사상 불법행위로 인한 손해배상 의무 부담
동의 없이 설치된 경우	• 광고프로그램이 이용자의 동의를 받지 아니하고 설치된 경우 ✓ 정보통신망법 제48조 제2항(악성프로그램) 해당 여부 검토 ✓ '업무'의 위법의 정도가 중하여 사회생활상 도저히 용인될 수 없는 정도로 반사회성을 띠는 경우에는 업무방해죄 보호대상이 되는 '업무'에 해당한다고 볼 수 없음(대법원 2011. 10. 13. 선고 2011도7081 판결)

형법/저작권법 관련 이슈

질의의 내용

취약점을 진단하기 위해 자신이 구입한 S/W나 H/W를 분석(리버싱)하는 행위는 어디까지 정당할까요? 그리고 발견한 취약점을 외부로 보고(언론기고 등)하는 행위는 도덕적인 규제인가요? 아니면 법적인 책임이 주어질 수 있나요?

형법/저작권법 관련 이슈

역분석 행위의 위법 여부

저작권법 제101조의4(프로그램코드역분석)

① 정당한 권한에 의하여 프로그램을 이용하는 자 또는 그의 허락을 받은 자는 호환에 필요한 정보를 쉽게 얻을 수 없고 그 획득이 불가피한 경우에는 해당 프로그램의 호환에 필요한 부분에 한하여 프로그램의 저작재산권자의 허락을 받지 아니하고 프로그램코드역분석을 할 수 있다.

② 제1항에 따른 프로그램코드역분석을 통하여 얻은 정보는 다음 각 호의 어느 하나에 해당하는 경우에는 이를 이용할 수 없다.

1. 호환 목적 외의 다른 목적을 위하여 이용하거나 제3자에게 제공하는 경우
2. 프로그램코드역분석의 대상이 되는 프로그램과 표현이 실질적으로 유사한 프로그램을 개발•제작•판매하거나 그 밖에 프로그램의 저작권을 침해하는 행위에 이용하는 경우

형법/저작권법 관련 이슈

역분석 행위의 위법 여부

형법상 위법성 조각사유

제21조(정당방위) ① 자기 또는 타인의 법익에 대한 현재의 부당한 침해를 방위하기 위한 행위는 상당한 이유가 있는 때에는 벌하지 아니한다.

제22조(긴급피난) ① 자기 또는 타인의 법익에 대한 현재의 위난을 피하기 위한 행위는 상당한 이유가 있는 때에는 벌하지 아니한다.

- ✓ 정당방위는 “현재”의 “부당한 침해”를 방위하기 위한 것
- ✓ 긴급피난은 위난의 원인이 위법이든 적법이든 불문
- ✓ S/W나 H/W를 분석(리버싱)하는 행위가 저작권 침해의 구성요건에 해당한다 하더라도, 위법성 조각 가능성

조직 운영에서 겪는 실무적 이슈

근로자의 이메일 모니터링

질의의 내용

스피어 피싱 메일방지, 기업의 기밀 유출 차단 등의 목적을 위해 프록시 서버로 직원들의 이메일을 모니터링한 행위는 정당한가요?
모니터링 등 정보보안정책에 대한 동의 절차를 입사시 작성해야만 했다면 이것이 정당한가요?
직원의 동의를 받았을 때 허용된다면 어떤 동의절차가 필요한가요?
그리고 만약 정당하지 않다면 어떤 식으로 해결해야 할까요?

기술유출 혐의가 있는 직원이 있어 내부감사팀이 조사과정에서 해당 직원의 이메일을 열람하였습니다. 이 경우는 정당한가요?

근로자의 이메일 모니터링

일반적인 경우의 근로자 이메일 모니터링

원칙 : 근로자의 구체적 동의

i) 근로계약 또는 취업규칙 등을 통해 모든 이메일은 업무용으로만 사용할 수 있다는 점을 명시

ii) 특정 이메일 열람에 대해 근로자들의 구체적인 사전 동의 획득

iii) 전자우편의 보존목적, 보존기간, 보존에 대한 책임부서 및 책임자, 보존 방법 및 처리과정, 보존장소, 보존된 전자우편의 이용목적과 사용범위 등의 사항을 서면으로 근로자에게 명확하게 고지

iv) 전자우편을 열람한 경우, 전자우편의 수신자인 근로자에게 그 검색결과와 열람사실을 통지

근로자의 이메일 모니터링

일반적인 경우의 근로자 이메일 모니터링

- 사용자의 감독권과 근로자의 프라이버시권의 충돌

  ✓ 근로자는 사용자에게 노무를 제공하고 사용자의 지시·감독권에 복종해야 할 의무를 부담

  ✓ 직장 내에서 근로자가 행사할 수 있는 프라이버시권의 범위는 제한

  ✓ 정보보안은 근로계약의 부수적 의무로 볼 수 있음(정보 유출시 업무상 배임 가능성)

근로자의 이메일 모니터링

기술유출 혐의가 있는 경우 근로자 이메일 모니터링

형법
제20조(정당행위) 법령에 의한 행위 또는 업무로 인한 행위 기타 사회상규에 위배되지 아니하는 행위는 벌하지 아니한다.

제21조(정당방위) ① 자기 또는 타인의 법익에 대한 현재의 부당한 침해를 방위하기 위한 행위는 상당한 이유가 있는 때에는 벌하지 아니한다.

제22조(긴급피난) ① 자기 또는 타인의 법익에 대한 현재의 위난을 피하기 위한 행위는 상당한 이유가 있는 때에는 벌하지 아니한다.

개인정보 보호법
제15조 제1항 제5호 “정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우”

직원 개인 노트북의 열람/조사

질의의 내용

기업의 보안관제센터에서 악성코드에 감염된 PC가 확인되었다. 회사PC가 아닌 개인 노트북일 경우 기업에서 해당 노트북을 조사하기 위한 과정은 어떻게 되나요?

직원 개인 노트북의 열람/조사

조사 목적 개인 PC의 조사 및 반출 제한

관련 규정 : 개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 **동의**를 받은 경우
2. 법률에 특별한 규정이 있거나 **법령상 의무를 준수**하기 위하여 불가피한 경우
3. **공공기관이 법령 등에서 정하는 소관 업무의 수행**을 위하여 불가피한 경우
4. 정보주체와의 **계약의 체결 및 이행을 위하여 불가피하게 필요**한 경우
5. 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**
6. **개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우**로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

직원 개인 노트북의 열람/조사

조사 목적 개인 PC의 조사 및 반출 제한

원 칙	• PC/노트북 소유자의 동의 필요
예 외	• 기업의 개인정보 보호의무를 다하기 위하여 급박한 경우 • 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우 • 급박한 생명, 신체, “재산”의 이익을 위하여 필요하다고 인정되는 경우 • 기업의 증거확보를 통한 재판청구권 보장 관점에서 필요한 경우(정당방위 등)

기타 그 밖의 이슈

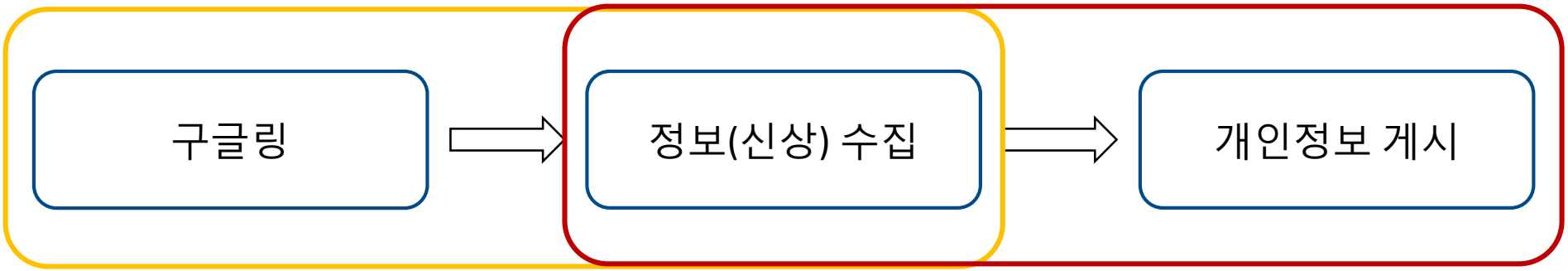
구글링 등을 통한 특정 개인의 신상 털이

질의의 내용

최근 인터넷을 통한 신상털이가 아무렇지 않게 일어나고 있는데 유명인사를 비롯해 일반인의 신상을 인터넷을 통해 수집하는 것이 정당한 행위인가요? 신상털이는 어디까지 허용될 수 있을까요?

구글링 등을 통한 특정 개인의 신상 털이

통신의 자유와 명예훼손/모욕죄 성립 가능성



- 일반적인 네티즌은 개인정보 처리자/정보통신서비스 제공자가 아님
  - ✓ 개인정보 보호법 및 정보통신망법상 개인정보 보호 규정이 적용되지 아니함
- 구글링을 통한 정보수집/신상털이는 헌법 제18조 통신의 자유 등으로 보호
- 신상정보/개인정보를 인터넷 게시판 등에 게시
  - ✓ 형법/정보통신망법상 명예훼손 또는 형법상 모욕죄에 해당할 가능성 존재
  - ✓ 사실의 적시/허위 사실의 적시인 경우 명예훼손죄
  - ✓ 경멸적 감정의 표현인 경우 모욕죄

Q & A

감사합니다