대규모 NATE 해킹과 그에 대한 분석

NATE 개인정보 유출을 통한 대응방안 모색과 보안인의 포부

2019 NOVEMBER 4

정보보호개론 보고서

경영학과 20180494 김지원

목차

1) 주제

1.1 주제 및 주제선정이유

보고서의 주제는 대규모 NATE해킹과 그에 대한 분석으로, NATE 개인정보 유출을 통한 대응방안 모색과 보안인으로써 나의 포부로 내용을 구성했다. 이를 주제로 선정한 이유는 과거 NATE, 싸이월드가 최초의 SNS 대규모 개인정보 유출사건으로 기록되어 있으며, 이를 토대로 해커의 측면에서 그들의 포탈을 통해 이용자에게 어떤 공격을 가했는지, 포탈측면에서는 어떠한 대처를 했고 어떠한 점이 원인이 되었는지, 마지막으로는 이용자 측면에서 어떠한 피해를 당했는지를 조사하고 보안인으로써 나의 포부를 다짐하는 것이 의미가 있을 것이라 판단했기 때문이다.

2) NATE 대규모 개인정보 유출사건

2.1 공격기법

2011 년 7 월 26 일 중국 IP 의 악성코드로 인하여 싸이월드와 네이트의 3500 만여명의 개인정보가 해킹당했다. 해커는 이스트소프트의 알툴즈 업데이트 서버에 악성코드를 설치하여 알툴즈가 설치된 SK 커뮤니케이션즈 직원의 PC 에 악성코드를 유포한다음 감염된 좀비 PC 가 서버를 해킹하여 SK 커뮤니케이션즈 데이터베이스를 해킹하여 개인정보를 유출하는 방식으로 진행되었다. 또한, 해커는 SK 커뮤니케이션즈 직원의 PC 접근권한을 확보하고 장기간에 걸쳐 정보를 모아서 해킹하는 APT 방식으로 네이트와 싸이월드의 DB 를 해킹한 것으로 추정했다.

2.2 발생원인

알툴즈를 사용하는 이용자들의 경우 프로그램을 실행시키면 자동으로 버전이 업데이트된다. 모든 알툴즈 제품에 공통으로 사용되는 모듈이므로 여러 제품을 쓰더라도 한 번만 업데이트를 하면 된다. 내부 PC 관리를 제대로 하지 못한 사실이 드러남과 동시에 해킹 원인이 발견되었다.

<출처: 메일경제>

2.3 대처방법

SK커뮤니케이션즈 측의 대처는 고객들에게 큰 실망을 안겨주었다. 발생 초기의 SK커뮤니케이션즈는 자신들의 대처를 해명하기에 급급했다. 또한, 네티즌에 대한 직접적 조치는 개인정보 유출 여부와 비밀번호 변경 안내 서비스뿐이었다. 그러나 곧이어 개인정보 유출 여부를 확인하는 것이 더 위험하다는 내용의 기사가 나오며 네티즌들을 혼란에 빠뜨리기도 했다. 고객 정보 유출이 중국발 IP 악성코드에 의한 것이고, 현재까지 확인되어진 유출된 개인정보는 암호화된 개인정보이기에 안전하다고 해명했다. 하지만 피해규모는 약 3500만명으로 고객의 70%이며, 전문가들은 사용자들이 대개 비밀번호 같은 것들을 자신의 신상정보를 조합해서 만드는 경우가 많기 때문에, 네이트에서 사용하는 계정과 패스워드를 쓰는 다른 사이트도 위험에 처할 가능성을 면치못한다고 말했다. 이로써 네이트 해킹으로 인한 피해는 개인 차원의 노력으로 예방될 수 있는 문제의 범위를 넘어섰다.

2.4 피해결과

한 사용자는 2~3곳의 카드사에서 자신의 명의로 신용카드 추가 발급 신청이 이뤄졌다는 사실을 확인하여 카드 발급을 취소시켰고, 누군가에 의해 변경된 비밀번호를 발견하기도 했다. 또한, 네이트와 싸이월드 해킹사건 이후 신용카드 추가 발급을 신청했다가 개인정보 불일치로 중단된 사례가 3배 가량 증가하기도 했다. 범인들은 신용카드 신규발급과 달리 추가발급은 이메일, 카드결제은행과 결제일, 연락처 등 개인정보만 알면 전화로 신청할 수 있다는 점을 노려, 이메일과 주민등록번호 등 유출 정보를 통해 피해자의 네이트 메일 계정에 들어가 카드 명세서를 열람하고 카드 추가 발급을 시도했기 때문이다.

사건 이후 네이버와 다음 등 각 포탈 사이트에는 SK커뮤니케이션즈에 보안상 관리 책임을 묻고 피해보상을 요구하는 집단 소송 카페가 개설되었고, 전국 법원에서는 수십건의 소송이 진행되었다. 하지만, 2018년 7월 12일 기사에 따르면 대법원이 SK가 손해를 배상할 책임이 없다고 판단하였고 이전에 배상책임을 인정했던 2심을 파기환송하였다. 재판부는 "해킹사고 당시 보편적으로 알려진 정보보안의 기술 수준 등을 종합적으로 살펴보면 SK가 개인정보 유출을 탐지하지 못했더라도 사회 통념상 합리적으로 기대 가능한 정도의 보호조치를 다 하지 않았다고 볼 수 없다"고 판단했기 때문이다.

3) 보안 전공자로서의 포부

대규모 해킹사건을 조사해보고 난 이후, 기업에서의 초기대처와 개인의 적극적인 예방이 중요하다고 생각했다. 하지만, 위의 예시처럼 개인의 적극적인 행동에도 어려운 APT(지능형지속공격)와 같은 경우에는 기업의 보안 능력이 필수적이다. 그래서 NATE의 대처방식을 보면 아쉬운 부분이 많이 남는데, 나의 주전공인 경영학과와 복수전공으로 수강하고 있는 융합보안공학과의 메리트를 섞는다면 이런 문제를 더 잘 해결할 수 있을 것이다. 현재 높은 직급에 있는 경영인들도 보안에 대한 기초적인 상식이 있다면 대응하기에 훨씬 수월할 것으로 보이기에 나는 보안 지식을 감미하고 있는 경영학도가 될 것이다.

나는 보안이 SNS뿐만아니라, 모든 분야에서 중요하다고 생각한다. 그만큼 해커들이 언제, 어디서, 어떻게 공격할 것인지 아무도 예측할 수 없기 때문이고, 개인정보는 어떤 형태로든지 중요한 자산이 될 수 있기 때문이다. 사용자는 서비스제공자에 대한 신뢰를 바탕으로 서비스를 이용하고, 서비스 제공자는 개인정보라는 자산을 담보로 한 이용자에게 서비스를 제공한다. 그렇기 때문에 보안을 전공한 나는, 기업이나 서비스제공자서비스 취약점을 점차적으로 보안해야 이용자 수 감소를 면할 수 있을 것이라 생각한다.

나는 FINTECH 분야에서의 보안인을 꿈꾸고 있고 작년과 이번 년에 블록체인에 대한 수업과 특강을 많이 들었다. 블록체인은 보안에 강하다고 알려져 있는 대표적인 기술 중 하나이지만, 현재는 블록체인 또한 완전히 안전한 기술은 아니라는 의견도 점점 생겨나고 있다. 이에 대비하여 현재는 블록체인기술에만 사용할 수 있는 블록체인 신분증이 나타난다고 하는데, 이 또한 기술이 발달함에 따라 강했던 보안도 취약해질 수 밖에 없는 터이기에 더 나은 보안 대책을 강구해야 한다고 생각하며, 이용자 관점에서의 보안을 중요시 하는 보안인이 될 것이다.

몇 주전, 융합보안공학과에서 주관한 특강에서 티몬 정보보안담당자님에 대한 이야기를 들었고 그 중에서 가장 기억에 남는 이야기가 하나 있다. "마케팅 같은 경우에는 성과가 눈에 그대로 드러나지만, 보안은 아무 일도 일어나지 않는 것이 제일 좋은 것이다. 점점 보안이 중요해지고 있는 추세이지만 보안의 성과가 눈에 드러나기에는 쉽지 않은 일인 것 같다. 하지만 여성 보안인으로서의 삶은 전문성을 인정받을 수 있기에 추천한다."라고 말씀하셨다. 그 분 말씀처럼 보안의 성과가 뚜렷하게 드러나는 것은 어려운 일이지만, 최근 신기술 어디에나 중요하게 여기는 것이 보안이므로 끊임없이 보안에 대해 연구하고 공부하여 실력을 겸비한 보안인이 될 것이다.

4) 출처

https://www.yna.co.kr/view/AKR20180711147800004 연합뉴스 2018.07.12

http://www.donga.com/news/article/all/20110729/39163516/1 동아일보 2011.07.29

https://www.hankyung.com/it/article/201107290963g 한국경제 2011.07.29

http://www.e-patentnews.com/3335 특허뉴스 2011.09.06

http://www.snujn.com/news/2218

https://www.mk.co.kr/news/business/view/2011/08/507141/

https://news.joins.com/article/22324512