4차 산업혁명 시대에 정보보안의 위협요인과 대응방안에 대한 연구

조 성 필*

〈요 약〉

누구도 예상 할 수 없는 기술 혁명을 통해 이제 정보화 및 공장 자동화로 일컬어지는 3차 산업혁명에서 기술이 융합되고 데이터가 힘을 갖는 초지능·초연결의 시대인 4차 산업혁명 사회로 나아가고 있다. 이러한 제4차 산업혁명의 시대에 무엇보다도 가장 중요한 자원은 정보나 데이터라고 볼 수 있다. 과거 3차 산업혁명 때보다도 더욱 방대한 양의 정보가 실시간으로 활용, 공유 그리고 전달되면서 이러한 정보의 관리 및 보안의 중요성이 커지고 있다고 볼 수 있다. 이처럼 4차 산업혁명의 가장 핵심이 되는 정보자산의 관리와 보안의 중요성은 증대해 가고 있는 동시에 위협요인 또한 증가해서 많은 정보 침해 사고와 유출사례들이 늘어나고 있다. 이러한 정보 침해와 유출 사고로 인해 조직체나 회사는 금전적으로나 대외적으로 큰 손해를 볼 수 있는데 이에 대한 철저한 해결 방안을 마련하는 것이 필요하다고 볼 수 있다. 따라서 본 논문에서는 위협요인과 관련해 데이터 사고나 유출에 대한 전반적인 추이를 알아보고 구체적으로 어떤 산업분야에서 가장 많은 피해를 입었는지도 알아보고자 한다. 다음으로 이러한 데이터 사고나 유출을 일으키는 요인들과 9가지 공격패턴을 각각의 특징에 따라 설명하고 이러한 위협요인과 공격에 어떻게 대응해 나갈지도 논의해 보기로 한다.

주제어 : 4차 산업혁명, 정보보안, 위협요인, 대응방안

* 중앙대학교 융합보안학과 연구교수 (제1저자)

목 차

Ⅰ. 서 론
Ⅱ. 4차 산업혁명과 정보보안
Ⅲ. 정보보안 위협요인들
Ⅳ. 대응방안 및 제안
Ⅴ. 결 론

Ⅰ. 서 론

컴퓨터와 인터넷 발달로 인한 정보화 및 공장 자동화로 일컬어지는 3차 산업혁명에서 이제는 인간을 훨씬 뛰어넘는 인공지능(AI)과 로봇 등장을 예견하고 모든 사물에 인터넷이 연결되는 사물 인터넷(IoT)이 보편화 되는 4차 산업혁명 시대로 들어가고 있다고 볼 수 있다. 이러한 초지능과 초연결이 보편화된 세계에서 과거에 비해 정보나 데이터의 중요성은 훨씬 더 증대 될 것이고 더 많은 양의 정보들이 교환되고 이용되어 질 것이다. 이러한 정보이용이나 유용성 증대에 따라 정보유출이나 침해 그리고 관련 범죄도 늘어나고 있는 것이 지금의 현실이다. 예를 들어 조직체의 내부들이나 외부 범죄 조직에 의해 조직의 중요 정보가 기밀들이 유출되거나 다른 조직체에 팔려 나감으로 해서 금전적으로 막대한 손실을 입히고 기업 이미지에도 커다란 타격을 줄 수 있다. 또한 해커들이나 공격자들에 의한 다양한 공격에 의해 조직체의 시스템이 통제 불능상태가 되면 다시 원상복구를 하는데도 많은 시간과 노력이 필요하고 어떤 경우에는 관련 정보자원과 시스템을 영영 사용할 수 없게 될 수 있다. 더욱 더 큰 문제는 이러한 정보사고나 유출관련 범죄 행위가 다양화 되고 더욱 치밀해져 가고 있다는 점이다. 이런 점에서 정보 관련 사고나 범죄 예방을 위한 정보보안의 중요성이 앞으로 계속 증대될 것이며 새로운 정보보안 기법이나 관련 소프트웨어

개발의 필요성도 제기 될 것이다. 그래서 이 연구는 이러한 4차 산업혁명의 진입점에 선 상황에서 정보보안의 역할에 대해 알아보고 에에 따른 관련 위협요인들이나 관련 위반 등을 알아보고자 한다. 특히 본문에서 언급될 위협요인 중에서도 최근에 드러나는 9가지 공격패턴에 대해 중점적으로 다룰 예정인데 이러한 공격패턴들이 정보 유출이나 위반에 많은 부분을 차지하고 있기 때문에 4차 산업혁명 시대의 발전에 있어서 심각한 저해 요인으로 작용할 수 있고 더 나아가 국가적으로도 막대한 손해를 끼칠 수가 있다. 마지막으로 이러한 위협요인들 특히 9가지 공격패턴을 경감시키거나 제거하기 위한 대응 방안을 제시하여 4차 산업혁명 내에서 정보의 안정적인 사용을 위해 기여를 할 수 있는 방법을 찾아보도록 한다.

Ⅱ. 4차 산업혁명과 정보보안

1. 4차 산업혁명과 정보보안

스위스 다보스포럼 의장인 클라우스 슈밥 (Klaus Schwab)은 2016년 그의 저서 ≪제4차 산업혁명(The Fourth Industrial Revolution)≫을 통해 “현재 인류는 지금까지 아무도 미리 내다보지 못할 정도의 빠른 기술혁신에 따른 ‘제4차 산업혁명’ 시대를 맞이하고 있다”고 선언했다. 산업의 혁명적 변화는 1760년대의 증기기관의 발명에 따른 1차 산업혁명의 시작으로부터 촉발된 산업혁명은 110년 이후 전기를 중심으로 한 에너지 혁명으로 인한 2차 산업혁명의 시작, 그 후 약 100년 후 IT 산업의 시작으로 인한 3차 산업혁명이 전개된 후 미처 50년이 되기도 전에 새로운 산업혁명의 모습으로 우리들 앞에 나타나고 있다.

증기, 에너지, IT에 이은 제4차 산업의 핵심은 인공지능(Artificial Intelligence; AI)과 모든 사물을 네트워크로 연결한 사물인터넷(Internet of Things; IoT)이라고 할 수 있다. 초지능과 초연결(super networking)은 지구상의 수십억의 인구와 그 보다 더 많은 기기들이 모바일로 연결되는 새로운 환경을 제공해주게 된다. AI와 IoT를 통해 로봇공학, 자율주행자동차, 3D프린팅, 나노기술, 생명공학, 재료공학, 에너지저장기술, 퀀텀 컴퓨터(quantum computing) 등 산업과 생활 전반에 걸친 혁명적 변화를 가져오게 된다. 이와 같은 혁신은 물리학, 디지털, 생물학 등의 분야의 경계를

없애고 새로운 융합(convergence) 시대를 만들어 나갈 것이다.

초연결의 시대에 도달하면서 가장 큰 우려 사항 중 하나는 정보 보안(information security)이다. Schwab(2015)은 마이클 샌델(Michael J. Sandel)의 경고를 받아들여 “우리는 일상적으로 사용하는 여러 기기를 통해 편리함을 대가로 기꺼이 사생활을 제공하려는 경향을 점점 보이고 있다”는 것을 지적하고 있다. 문제는 이런 자발적 정보 제공만이 아니라 자기도 모르는, 비의도적인 정보누출(information leakage)이 횡행해지고 있다는 점이다. 특히 악의적 의도에 의한 대량의 정보 데이터의 누출은 단순히 개인 정보의 누출을 넘어 재산과 신체에 심각한 위협으로 작용될 수 있다는 것이다.

대규모 온라인 운영자는 규모가 큰 데이터 세트(data set)의 집적을 통해 사용자가 제공하는 정보보다 훨씬 더 많은 정보를 생성할 수 있게 된다. 빅 데이터의 분석과 추론기술(inference technique)을 통해 유추된 추가 정보는 ‘나도 모르는 나’에 대한 정보가 만들어 지고, 이에 대한 비의도적 유출은 심각한 문제를 야기할 경우가 생기게 된다. 실질적인 위험은 금융기관에서 일어나는 정보유출이다. 개인의 대부분의 자산이 금융기관에 보관되어지는 환경에서 금융기관에 대한 공격의 후유증은 매우 크다고 할 수 밖에 없다. 결국 제4차 산업의 ‘초연결’은 ‘초보안(super security)’의 필요성을 강조할 수밖에 없는 환경을 만들게 된다.

2. 정보보안 개념 및 역할

정보보안은 사용자, 국가, 또는 기관에 따라 다양하게 정의되고 있다. 국제표준 ISO/IEC 17799에서는 정보보안을 ‘정보를 다른 중요한 비즈니스 자산과 같이 비즈니스에 필수적이며, 따라서 적절하게 보호될 필요가 있는 자산이며 비즈니스 연속성을 보장하고, 위험을 최소화하며, 투자와 기회를 극대화하기 위하여 광범위한 위협으로부터 정보를 보호하는 것이라고 정의하고 있다(ISO/IEC 2005).

OECD(2002)에서 발표한 정보보안 가이드라인에 따르면 정보보안은 ‘기밀성(confidentiality)’, ‘무결성(integrity)’, ‘가용성(availability)’ 등의 세 가지 요소를 관리하는 것이라고 정의하고 있다. 여기에서 ‘기밀성’은 보안공격으로부터 전송자료를 보호하기 위하여 전송 또는 보관 중인 정보를 인가되지 않은 사용자가 부정한 방법으로 입수하더라도 그 내용을 알 수 없도록 보호하는 것이므로 정보가 접근이 인가

된 자만 접근할 수 있도록 보장하는 것을 말하고, '무결성'은 전송 또는 보관중인 정보가 인가되는 방법으로 위조 또는 변조할 수 없도록 보호하는 것으로서 메시지 스트림, 단일메시지, 또는 메시지 특정 필드에 적용할 수 있으며, '가용성'은 인가된 사용자만 필요할 때에 적절히 그 정보 또는 자산에 접근하도록 보장하는 것을 말한다(조찬식, 2000).

Eloff(2000)는 관찰 또는 측정 등을 통해 수집된 자료를 분석하여 정리된 지식을 외부의 위협으로부터 안전하게 지키는 활동으로 정의하고 있다. 미국 표준 기술원은 정보보안을 '조직의 정보 및 정보시스템을 보호하기 위하여 정보보안이 기밀성, 무결성, 가용성을 통해 비 인가자의 접근, 사용, 변조, 공개, 혼란, 공격을 방어하기 위한 일련의 보안활동' 이라고 정의하였다(Kissel 2013). 국내에서는 '정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강화하는 것' 이라고 정보화촉진기본법 제2조에서 정의 하고 있다.

정보보안의 중요성은 고대부터 지금까지 끊임없이 지적된 문제이다. 특히 국가간 전쟁의 수행이 당연하게 인정되었던 근대 이전에는 정치적·군사적 목적에 의한 정보 정보이 중요했다. 정보 보안의 개념이 획기적으로 변화하게 된 시점은 디지털 시대의 출발에 의해서다. 제3차 산업혁명의 출범인 IT산업의 발전은 디지털 정보 보안의 필요성을 확대시키는 결과를 초래하게 된다. 공간적 차이를 극복한 네트워크의 발전은 정보 유출의 새로운 패러다임이 나타나게 되었다.

Loch et al(1992)은 정보보안을 위협하는 요소로 내부적 위협과 외부적 위협으로 나누고 이를 위협을 가하는 대상을 기준으로 인간과 비인간으로 구분하고 있다. 이러한 분류에 따르면 외부에서 위협을 가하는 위협은 인간을 기준으로 할 때 해커와 경쟁자이며 비인간 위협으로 자연 재해와 컴퓨터 바이러스를 들고 있다. 또한 내부적 위협으로 직원의 행위와 절차, 기계적, 전기적 장애 그리고 프로그램 문제라고 정의하고 있다. 그리고 이 모든 경우는 의도적인 위협과 비의도적인 위협으로 구분된다고 하고 있다.

'초연결'의 4차 산업혁명시대에서의 정보보안은 그 중요성이 더 중요해 지고 있다. 2015년 발표된 '세계경제포럼보고서'에 따르면 2025년 예상되는 사회의 변화 중 60% 이상의 확률을 가진 변화는 다음과 같다.

인구 10% 이상이 인터넷에 연결된 의류를 입고(91.2% 확률), 인구 90% 이상이 무한 용량의 무료 저장소를 사용하고(91.0% 확률), 1조 개의 센서가 인터넷에 연결

되고(89.2% 확률), 로봇 약사가 등장하고(86.5% 확률), 10%의 인구가 인터넷이 연결된 안경을 쓰고(85.5% 확률), 인구 80%가 인터넷상 디지털 정체성을 갖게 되고(84.4% 확률), 3D로 제작된 자동차가 처음 생산되고(84.1% 확률), 인구 센서스 대신 빅 데이터를 활용하는 최초의 정부가 등장하고(82.9% 확률), 상업화 된 인체 삽입형 휴대폰이 등장하고(81.7% 확률), 미국 도로를 달리는 차 중 10%가 자율주행자동라가 되고(78.2% 확률), 3D로 제작된 간이 최초로 이식되고(76.4% 확률), 인공지능이 기업 강사의 30%을 차지하고(75.4% 확률), 가정용 기기에 50% 이상이 인터넷 트래픽이 몰리게 된다(69.9% 확률) (세계경제포럼보고서, 2015).

이상의 변화의 시대에서 보안의 중요성은 어떨 것인가? 초연결은 재산은 물론 신체적 위협에 까지 무방비로 연결되게 되며 이를 예방할 수 있는 것은 결국 정보보안이며 이의 중요성은 더욱 높아 질 수밖에 없는 것이다.

Ⅲ. 정보보안 위협 요인들

82개국 조직체들과 관련 무수한 산업들의 데이터 유출과 사고들을 정리한 Verizon (2016)에 따르면 금전적인 동기를 가진 악의적인 공격자나 해커들에 의해 이러한 데이터 유출이나 사고들이 일어나고 있다는 것을 알 수 있다. 여기서 데이터 유출과 사고의 차이점은 데이터 유출은 인증되지 않는 당사자들에게 정보노출이나 유출의 결과를 유발할 수 있는 사고들 말하고 데이터 사고는 정보 자산의 완전성, 기밀성 그리고 유용성을 손상시키는 보안 사건을 말한다. 정보보안을 위협하는 요소로서 위에서 언급한 데이터 유출, 보안 취약성, 피싱 그리고 특히 9가지로 유형화 될 수 있는 공격 패턴에 대한 자세한 설명을 해보고자 한다.

1. 데이터 유출

문가용(2016)에 따르면 <표 1>에 나타난 것처럼 2015년 가장 많은 공격을 받은 건 금융기관들이었다. 데이터 유출 사건만 795건이 있었다. 다음은 호텔 및 숙박업으로 총 282건, 정보 산업이 194건, 공공 기관이 193건, 도소매가 137건, 의료 및 건강 산업이 115건이었다. POS 공격에 대한 보안인식이 높아짐에 따라 도소매업에

서 발생한 정보 유출 사건은 2014년에 비해 줄어들었고, 해커들은 호텔 및 숙박업으로 눈길을 돌려, 이 부분에서는 공격이 늘어났다.

〈표 1〉 2015년 데이터 유출 피해를 받은 산업에서의 보안 사고 수

산업	작은 조직	큰 조직	기타	합계
숙박업(72)	136	10	136	282
행정 · 관리업(56)	6	2	10	18
농업(11)	0	0	1	1
건설업(23)	0	1	3	4
교육업(61)	3	8	18	29
예능 산업(71)	18	1	19	38
금융업(52)	14	94	687	795
의료업(62)	18	20	77	115
정보 산업(51)	12	12	170	194
경영(55)	0	0	0	0
제조업(31 - 33)	5	11	21	37
광산업(21)	0	6	1	7
다른 서비스들(81)	5	2	4	11
전문업(54)	10	4	39	53
공공 부문(92)	4	122	67	193
부동산업(53)	3	0	2	5
소매업(44 - 45)	101	14	67	182
무역(42)	2	2	0	4
운송(48 - 49)	1	3	11	15
공익사업(22)	0	0	7	7
기타	109	0	161	270
합계	447	312	1501	2,2260

출처 : Verizon(2016)

데이터 유출 행위는 내부나 파트너들에 의한 것보다 대부분 외부 공격자나 조직에 의한 것들이고 금전적인 동기에 의해서 이런 행위들을 하게 된다. 금전적인 목적

인 경우가 대부분이지만 스파이나 재미를 목적으로 이런 위반 행위가 이루어지기도 한다. 이러한 데이터 유출을 하는데 멀웨어(malware), 스파이웨어(spyware), 해킹 그리고 피싱(phishing) 등의 소프트웨어나 방법들이 이용되는데 해커들이나 공격자들은 이런 공격 방법들을 서버, 유저 디바이스(user devices), 인적 자산 그리고 네트워크 등의 매개체를 통해 실행한다. 과거 몇 년 전까지 서버를 이용하는 비중이 높았지만 요즘에 들어서 유저 디바이스의 비중이 계속적으로 증가하고 있다.

정보의 유비쿼터스적(ubiquitous)인 성격으로 인해 데이터를 손상시켜 유출시키는데 걸리는 시간이 매우 짧은데 더욱 심각한 점은 해가 갈수록 데이터를 손상시키는데 걸리는 시간은 짧아지지만 이것을 찾는데 걸리는 시간은 변함이 없거나 늘어난다는 점이다. 데이터 손상이나 유출에 대한 탐지 성공 능력이 증가되지 않음으로 인해 공격자들이 더욱 쉽게 그들의 피해자들을 공격하고 발견되지 않고 있다. 데이터 유출에 대한 발견이나 탐지에 어려운 점이 있지만 대부분이 유출에 대한 법집행 신고나 부정행위 적발 시 이루어지는 경우가 대부분이다.

2. 보안 취약점

해커나 공격자의 숫자는 늘어나고 공격코드는 자동화됨에 따라서 새로운 데이터 취약점은 매일 나타나게 되었는데 이에 따라 기업에서는 이러한 취약점을 없애고 줄이기 위해 취약점 관리를 실행하게 되었다. 신성윤과 이윤창(2015)는 취약점 관리란 IT 환경을 보다 더 안정적으로 운영하고 기업체들이 개별 보안 정책을 지키는지를 계속해서 감시하고 대응하여 위협을 완화시켜 사업의 연속성과 가용성을 가능하도록 하는 것이다. 여기에서 취약점이란 보유하고 있는 정보 시스템(하드웨어(PC 포함), 네트워크 장비, 운영체제, 소프트웨어, 등)의 탑재하고 있는 소프트웨어의 오류와 결함이나 설치하는데 있어서의 오류 등을 말한다.

해커나 공격자들에 의해 행해지는 시스템 보안 취약점을 이용한 공격의 반 정도는 보안 취약점 관련 리포트 나온 후 10일과 100일사이에 이루어지고 지는데 평균적으로는 30일 정도에 행해지게 된다. 새로운 소프트웨어나 시스템 등장으로 보안 취약성이 증대되면 해커나 공격자들로부터의 공격을 막기 위해 일부 프로그램을 수정 및 변경하게 되는데 이러한 과정이 올바르게 수행되지 않으면 데이터 유출이나 사고를 막을 수 없게 된다. 따라서 보안 취약점 관리에서 중요한 점은 관련된 프로그램의

올바른 수정과 변경에 달려 있다고 볼 수 있다.

보안 취약점을 관리하는데 있어서 보편적으로 2가지 방법이 있는데 프로그램의 수정이나 변경을 통한 치료와 취약점을 경감시키는 방향으로의 방법이 있는데 완벽한 치료가 불가능할 경우 취약점 경감도 치료처럼 유용하고 때때로 당신의 유일한 옵션이 될 수 있다.

3. 피싱

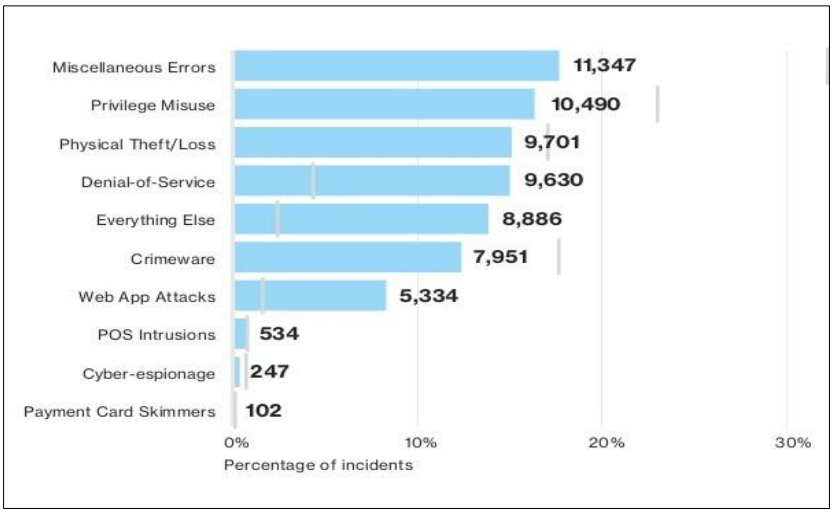
이제 일반적인 용어로 사용되고 있는 피싱이란 용어는 메일을 사용하여 인터넷 사용자의 비밀번호나 금융정보를 낚아채는 형태의 초기 인터넷 범죄를 의미하는 피쉬(phish)에서 유래하고 있는데 이 피쉬는 “Ph” 와 “Fish”의 합성어로 “Ph”의 사용은 부분적으로 연대기를 잃었지만, 전화 시스템을 해킹(프리킹, Phreaking)하는 초창기의 해커(phreaks)와 같이 인기 있는 해커 명명 규칙과 연관을 지을 수 있다 (김성재, 2013). 이러한 피싱은 현재의 통용되는 가장 성공적인 사회 공학적(social engineering) 공격인데 악성적인 첨부파일과 링크를 가진 메시지나 메일을 보내 희생양이 열어보게 해서 사기를 치거나 정보를 탈취하는 행위를 말한다. 가장 기본적인 피싱 공격의 프로세스는 아무 것도 모르는 사용자가 클릭을 하고 이 과정에서 멀웨어같은 악성 소프트웨어가 설치되고 침투 기반이 마련이 되는데 이와 달리 피싱 이메일이 사용자들로 하여금 가짜 사이트들에 끌어들여 사용자 입력 데이터를 얻는데 이용되기도 한다. 하지만 대부분의 피싱관련 사건들에서 피싱의 목적은 지속적인 악성 소프트웨어를 설치해서 사용자의 정보를 빼내거나 사기를 저지르는데 사용되고 있다.

피싱 공격을 하는 주요 범죄자들은 조직화된 범죄 조직단이 89%이고 국가산하 공격자들이 8%인데 이들이 훔치는 대부분은 회사나 정부의 기밀(confidential) 정보나 서류이고 다음으로는 영업 비밀관련 정보들이다.

이런 피싱을 미리 예방하는 것이 피싱을 당한 후의 조치나 치료보도 훨씬 중요하다고 볼 수 있다. 이를 위해서 해야 할 일은 이메일을 필터링함으로서 피싱관련 위협요인들을 미리 제거하고 직원들에게 피싱관련 정보교육 하여 피싱에 대한 정확하고 신속한 인지를 할 수 있도록 해야 한다. 또한 피싱 발생시 빠르게 보고 할 수 있는 체계를 마련해 놔야 한다. 마지막으로 지속적인 모니터링을 통해서 의심스러운 접속이나 신호를 미리에 인지해서 차단함으로서 피싱 공격의 피해를 줄일 수 있다.

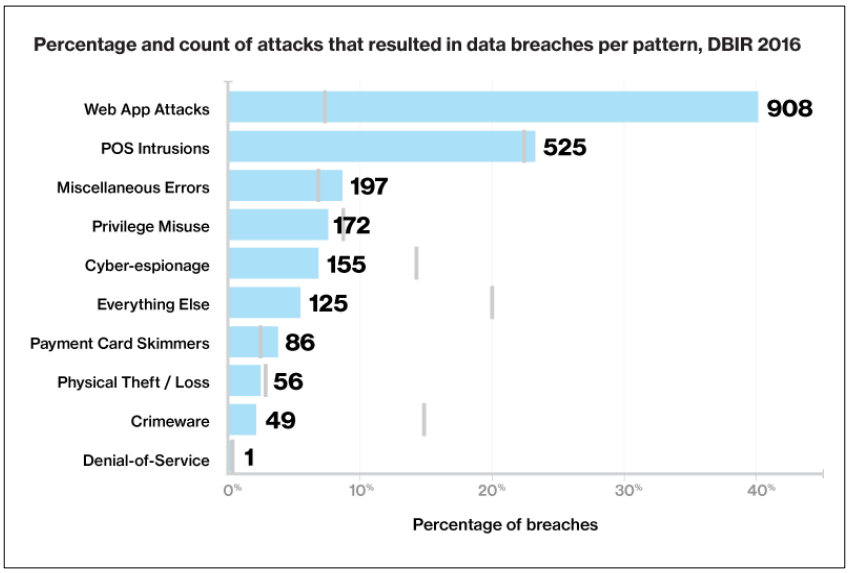
4. 보안 침해 9가지 공격 패턴

Verizon(2014)에 의하면 기업에서 발생할 가능성이 있는 거의 모든 공격은 누가(행위자), 무엇(자산), 어떻게(행위), 그리고 왜(동기)에 따라 9가지 패턴으로 분류된다. 이를 통해 보안위협을 이해하고 보안 관련 업무의 우선 순위를 지정할 수 있다(김태형, 2014). Verizon(2014)에 따르면 데이터 유출에 있어서 90%이상이 9가지 공격 패턴에 의해 행해졌고 Verizon(2016)에서도 특별한 차이점을 보이지는 않았다. Verizon(2016)에 따르면 2015년 발생한 데이터 사고에서 9가지 공격 패턴 중 가장 많이 나타나는 공격 패턴은 [그림 1]에 나타나듯이 다양한 종류의 실수들(miscellaneous errors)이고 그 다음으로 내부자 및 권한의 잘못된 사용(privilege miuse)등으로 나타났다. 데이터 유출에 있어서는 [그림 2]에서 보듯이 웹 앱 공격(web app attacks)이 가장 많이 나타나는 공격 패턴으로 나타났는데 여기서 흥미로운 사실은 웹 앱 공격이 데이터 유출부분에 있어서 급성장하고 있는 공격 패턴인데 특히 금융 분야에서 가장 많이 사용되는 방식이다. 다음으로는 POS 침투(POS Intrusions)로 나타났고 데이터 사고에서 가장 높은 비율을 차지한 다양한 종류의 실수들이 세 번째로 나타났다.



출처 : Verizon(2016)

[그림 1] 데이터 사고에 있어서 9가지 공격 패턴 비율 및 빈도수



출처 : Verizon(2016)

[그림 2] 데이터 유출에 있어서 9가지 공격 패턴 비율 및 빈도수

이상과 같이 9가지 보안위협의 공격 패턴을 분류한 기준은 실제 현장에서 발생된 보안 위협 상황을 바탕으로 행하여 졌다. 이러한 분류가 학문적인 측면에서는 다소 부족할 수 있을지 모르지만 실용적인 측면에서는 매우 가치 있는 일이라고 할 수 있다. 특히 그리고 이 분류를 통해 전체 보안위협 상황의 90%가 포함이 된다는 것은 이번 분류의 타당성을 설명해주고 있다고 할 수 있다.

1) 웹 어플리케이션 공격

인터넷에서 가장 많이 사용하는 애플리케이션이 웹이다. 최근 BYOD(biring your own device)가 확산되면서 다양한 모바일 기기에서 업무를 수행하기 위해 모바일 앱이 다양하게 발전하고 있지만, 모바일 앱도 결국은 웹(모바일 웹)을 통해 연결된다(김선애, 2016). F5네트웍스의 조사에 따르면 인터넷 사용자의 69%가 웹 애플리케이션을 사용하는 것으로 나타났으며, 2020년에는 업무의 71%가 웹 또는 모바일 앱/웹으로 수행될 것으로 예상된다(김선애, 2016). 웹이 일상적으로 사용되면서 웹을 통한 공격도 늘어나고 있는데 이러한 웹 앱 공격은 CMS(콘텐츠 관리 시스템) 또는 전자

상거래 플랫폼 같은 웹 애플리케이션에서 공격자가 훔친 자격 증명을 사용하거나 취약성을 악용하는 경우다. 현재는 대부분의 업종이 웹에 접속하는 애플리케이션을 많이 사용하고 있지만 주요 공격 대상은 정보 유틸리티, 제조 및 소매업체이다(김태형, 2014). 웹 어플리케이션 코드나 기본적인 비즈니스 로직과 같은 웹 인프라가 과거에 비해 더욱 복합해지면 질수록 사용자들이 단순히 웹을 방문해서 단순한 정보를 구하거나 몇 개 정도의 링크 사이트를 가는데 그치지 않고 더욱 많은 상호작용을 하고 보안 취약점을 훨씬 자주 노출하게 되면서 웹서버가 해커나 공격자들의 명백한 타겟이 되고 있다.

웹을 이용한 공격은 비즈니스에 심각한 위협이 되고 있다. 웹서버가 직접 공격을 받는 경우는 직접적인 피해를 입게 되고, 웹을 통해 방문자를 공격한다면 기업/기관의 신뢰도에 타격을 입는다(김태형, 2014).이러한 공격들은 확인된 데이터 유출에 있어서 95%정도가 금적적인 목적에 의해서 행해진다.

2) POS(Point-of-Sale) 침입

POS는 Point Of Sales"의 약어로 판매시점정보 관리를 의미하며 POS 시스템은 매장에서 상품 및 서비스가 판매되는 시간과 장소에서 그와 관련된 모든 정보를 취득 및 처리하여 필요한 일련의 조치가 한 번에 이루어지는 시스템을 의미한다(윤정현 · 문현실 · 김재경 · 최주철, 2015). POS 시스템은 바코드, 광학스캐너, 카드리더 등과 결합되어 있는 PC나 단말기(Terminal)로 구성되며 일련의 판매를 통해 생성 및 수집되는 데이터는 일차적으로 재고관리 등에 활용된다. 또한 판매 활동으로부터 수집되는 고객의 행동에 관한 정보는 적절한 데이터 처리 및 분석을 통해 마케팅 활동에 활용되고 있다(김동훈, 1997).

카드기반 소매 거래가 많아지면서 공격자가 원격으로 고객의 결제 데이터 유출을 목적으로 POS 애플리케이션을 실행하는 컴퓨터 및 서버를 손상시키는 경우를 POS 침입이라고 하는데 주로 POS 터미널이나 콘트롤러가 공격대상이다. 이러한 POS 장치들은 고객 신용카드 정보를 훔치는데 유용한 자원으로 계속 사용되고 왔는데 가장 많은 POS 장치를 보유하고 있는 접객 및 소매 업체가 당연히 최다 공격 대상이지만 의료 서비스, 결제 처리 등의 다른 업무 부문 역시 위험하다(김태형, 2014).

일반적인 소매업종에 공격자들의 일반적인 POS 침입 프로세스는 인터넷에 POS 서버가 보여지면 이러한 POS가 디폴트 로그인 패스워드 가지고 있기 때문에 쉽게

시스템에 접근 할 수 있다. 여기서 의 디폴트 로그인 패스워드는 장비 제조업체에서 출고 시 설정되어 나오는 기본 로그인 아이디와 패스워드를 말하는데 각 제조사의 장비별 디폴트 로그인 패 스워드 리스트는 인터넷 등을 통해 쉽게 구할 수 있어, 악의인 사용자가 이러한 디폴트 로그인 패스워드를 이용하여 불법으로 네트워크 장비에 근할 수 있다(한국정보보호진흥원, 2015). 위의 과정을 통해 POS 시스템에 침입한 후 악성 소프트웨어를 설치시켜 이를 통해 고객의 신용카드 정보를 빼내게 된다. 작은 규모의 소매 업종과 마찬가지로 큰 규모의 조직체들도 POS 침입으로 인해 데이터 유출로 인한 피해가 급증하고 있다. 이런 큰 업체들은 작은 규모의 소매 업종과는 달리 인증과정이 다소 복잡하고 디폴트 로그인 패스워드를 사용하지는 않지만 공격자들도 이를 손상시키기 위해 더욱 치밀해져 가고 있다.

3) 내부자 및 권한의 잘못된 사용

CA 백서(2011)의 연구에 따르면 기업이 과거에 비해 IT관련 정보자산을 더 많이 사용하게 되면서 외부로 유출되어서는 안 되는 민감한 기밀 정보에 액세스 하거나 주요 시스템에서 전권을 행사하면 모든 작업을 자유롭게 수용하는 내부 관리자나 사용자들의 활동이 늘어나게 되었다. 또한 현재 수행 중인 업무에 필요한 수준 이상의 자격을 부여 받는 일반 사용자들이 있는데 이 모든 요인들로 인해 내부자 보안 및 프라이버시 침해의 위험이 급격하게 증가하고 있다. 이렇게 내부 사용자나 관리자가 조직체의 자원을 허가없이 사용하거나 악용함으로 나타나는 모든 사고에 관련된 행위를 '내부자 및 권한의 잘못된 사용' 이라 하는데 대부분 내부자들에 행해지지만 외부자나 파트너에 의해 행해지기도 한다. 특히 이러한 공격 패턴은 내부자와 외부자 (혹은 파트너) 사이의 공모를 포함하고 있는 몇 안되는 방식 중에 하나이다. 하지만 대부분의 경우 내부 사용자나 관리자에 의해 이루어지는데 이 공격에 참여하는 내부자들은 엔드 유저가 33%로 가장 많고 그 다음으로는 경영자 레벨이 14%로 시스템 개발자 및 관리자들과 같은 비율로 나타났다. 이들은 많은 경우 금전적인 목적에 의해 이러한 행동을 저지르게 되었는데 최근에 들어서 산업 스파이적인 동기에 의해 저질러지는 공격의 수가 늘어나고 있는 추세이다.

'내부자 및 권한의 잘못된 사용'에 공격 패턴에서 가장 많은 것을 차지하는 것은 특권이나 권한의 악용인데 민감하고 허가되지 않은 정보를 얻기 위해 접속하여 이를 얻어내기 위한 공격 행동이라 볼 수 있다. 다음으로는 직원으로 실수나 부주의로

데이터나 정보를 유출시키는 경우를 말한다. 이러한 내부자 위협에 의한 데이터 유출이나 사고는 다른 어떤 공격 패턴보다 가장 탐지하기 어렵고 발견되더라도 한 달이나 1년 정도 걸리게 되는데 이러한 이유는 내부자의 공격 행동이나 위협행동에 대한 탐지가 설문조사 같은 자체보고에 의한 경우가 많기 때문에 방어적인 대답이 많기 때문에 실제 내부자 공격에 비해 탐지되는 경우가 아주 적다고 볼 수 있다(CA 백서, 2010).

4) 기타 실수

모든 사람들은 완벽하지 않기 때문에 어떤 것을 잃어버리는 실수를 하게 되는데 이렇게 의도 되지 않은 행동들이 곧 바로 정보자산의 보안적 속성을 손상시키면서 일어나는 사고를 말하는데 문서나 디지털 형태의 정보가 잘못 전달되는 형태가 가장 일반적인 실수이고 문서 또는 자산을 안전하게 폐기하지 못하는 것 등이 포함된다. 어떤 업계에서 일하든 모든 업무 과정에서 이러한 실수는 일어난다. 그러나 공공부문, 행정, 교육, 의료 서비스처럼 정보전달을 다루는 업종의 피해가 가장 심각하다(김태형, 2014). 하지만 어떤 패치나 타당성 검증의 부족으로 해킹 당할 때 우리는 이것을 실수라고 하지는 않는데 이러한 행동이 직접적인 데이터 유실의 원인이 아니기 때문이다.

여러 종류의 실수 중에 용량부족과 관련된 실수가 가장 많고 그 다음으로는 정보나 문서의 배달착오로 인한 실수이고 잘못된 정보고지나 발표 등이 세 번째로 나타났다. 이러한 다양한 실수들로 인한 데이터 유출시 보편적으로 내부보다 외부에 의해 발견될 가능성이 높은 것으로 드러났다.

5) 물리적 도난 및 분실

정보 자산들이나 데이터들이 잘못 배치하는 실수나 악의적인 목적에 의해서 유실되는 것을 말하는데 일반적으로 노트북·USB 드라이브, 인쇄된 서류 및 기타 정보자산의 분실/도난을 말한다(김태형, 2014). 그중에서도 이 공격 패턴과 관련된 모든 사고에서 노트북이 가장 일반적인 타겟이지만 우리의 연구를 확인된 유출사고로 한정시켰을 때 서류나 문서의 관리 결여로 인해 이를 발견한 사람이나 훔친 사람이 이 문서를 유출시키거나 폭로하는 경우가 대부분이다. 이러한 정보자산의 물리적 도난 및 분실에 있어서 관련 자산 손실이나 유실이 도난보다 100배 많은 것이 일반적

이다. 물리적 도난 및 분실로 일어나는 유출 사고들은 피해자 장소(39%) 혹은 종업원들의 개인 차량(33.9%)에서 일어나는데 이러한 분실물들은 훔쳐진 것보다 잃어버려진 것들이 훨씬 많다.

6) 크라임웨어(Crimeware)

개인정보 유출, 피싱 등 온라인 범죄행위를 용이하게 하는 소프트웨어를 말하는데 이 공격 패턴을 차지하는 사고의 대부분은 기본적으로 우발적이고 금전적이 동기가 숨어있기 때문에 지속적인 금전적 동기를 가진 외부의 조직화된 범죄 그룹에 의해 행해지는 경향이 있다. 크라임웨어 관련 사고 대부분은 통제서버(C2) 숨어있는 악성 소프트웨어나 랜섬웨어(ransomeware) 등을 이용해서 디바이스에 조정을 시작하고 이를 통해 사용자의 인증이나 계정 획득을 목적으로 하거나 봇네트(botnet)계정으로 등록 시키는 것이 대부분을 차지한다. 여기서 봇네트란 악의를 가진 공격자인 봇 마스터(bot master)가 보안이 취약한 PC들을 마음대로 제어할 수 있도록 소프트웨어적 로봇(bot)을 감염시키고, 이렇게 감염된 수천~수만대 이상의 PC들이 네트웨크를 통해 연결되어 제어 권한을 가지 봇 마스터에 의해 원격 조정되는 것을 말한다(한경수 · 임광혁 · 임을규, 2009).

크라임웨어에서 기능이나 목적에 따라 5가지로 나누어지는데 C2 말웨어, 랜섬웨어, 스파이웨어/키로거(keylogger), 백도어(back door) 그리고 데이터 가져오기(export data) 등이 있는데 여기서 랜섬웨어란 몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로 사용자의 동의 없이 컴퓨터에 불법으로 설치되어 문서나 스프레드시트, 그림 파일등을 암호화하여 열지 못하도록 한 뒤, 암호화된 파일을 원상복구 시켜주는 조건으로 금품을 요구한다(윤정무 · 조제경 · 류재철, 2016). 이러한 크라임웨어를 설치하게 되는 3가지의 경로가 있는데 첫째로 악의적인 첨부파일을 가지고 있는 이메일을 통해서 둘째로는 각각의 방문마다 드라이브 바이 다운로드(Drive-by download)를 제공하는 웹사이트에 의해서이다. 마지막으로는 위의 두 가지가 결합된 형태인데 예를 들어 드라이브 바이코드 설치를 포함하고 있는 페이지로 링크되는 이메일을 열었을 경우 의도되지 않게 스파이웨어나 악성 소프트웨어가 설치가 된다.

7) 결제카드 조작

정기석(2016) 연구에 따르면 신용카드가 지불수단으로서 현금이나 수표를 대신하는 중요한 경제수단의 하나로 자리 매김하면서 현재 우리사회의 성인 인구 중 90% 이상이 사용하고 있고 또한 신용카드의 개인별 보유비율, 개인별 이용비율, 지급수단별 이용비중이 매년 증가하고 있고 이에 따라 부정사용도 증가하고 있다. 이와 같은 부정사용중에서도 결제카드 조작은 현금자동 입출금기(ATM), 주유기 결제시스템이나 POS 단말기 등을 통해 신용 카드의 마그내틱 정보를 위조 장치인 스키머(skimmer)로 읽어내어 카드를 위·변조하는 것을 말한다. 이 공격 수법에서의 변화는 거의 없고 루마니아 같은 동유럽에서 많이 행해지는 수법인데 이러한 위조 범죄의 70%정도는 조직화된 범죄그룹에 의한 것이다. 이들의 주요 타겟은 ATM기기이지만 주유기 결제시스템도 가끔 이들의 희생양이 된다.

8) 사이버 스파이

정부기관과 관련이 있는 단체나 사람이 스파이 목적으로 승인되지 않는 네트워크나 시스템 접속을 통해 조직의 중요한 정보를 빼내 다른 회사에 팔아넘기거나 유출하는 행위를 하는 사람을 사이버 스파이라고 한다. 따라서 사이버 스파이는 피해자 네트워크에 잠입해서 민감한 내부 데이터나 기업 비밀 등을 찾아내는 외부적 위협 행동으로 볼 수 있다. 이러한 스파이 행위는 대부분의 경우는 정부와 밀접한 연관이 있는 그룹들에 의해 행해지지만 조직화된 범죄 집단들과 경쟁자들 그리고 정부가 같이 공모해서 진행되는 경우도 있다. DBIR(2016) 보고서에 따르면 사이버 스파이의 공격 대상이 되는 상위 피해산업분야들은 공공분야, 생산, 전문서비스나 정보서비스 분야로 나타났다.

사이버 스파이 프로세스는 백도어나 C2 말웨어를 설치시키고 이러한 악성 소프트웨어를 이용해 시발점으로 하는 피싱으로 시작하는데 이러한 피싱은 이러한 사이버 스파이 행위를 주도하는 방법으로서 많은 다른 익스플로잇 (exploit)공격보다 더 많은 장점을 가지고 있는데 여기서 익스플로잇이란 프로그램 과정에서 발생한 취약한 부분을 이용하여 정상 동작이 아니 공격자가 의도한 동작이나 명령을 실행하도록 만드는 행위를 말한다(이홍선, 2013). 예를 들어 손상시키는데 걸리는 시간이 극도로 짧고 공격자들이 조직체의 특정 개인을 타겟으로 할 수 있는 메카니즘을 제공한다.

앞에서 언급한 프로세스를 통해 독점적 정보로 알려진 기업 비밀들이 사이버 스파이에 의해 훔쳐지거나 해킹되어지는 가장 일반적인 데이터인데 90%이상이 이런 케이스이다.

9) DoS(Denial-of-Attacks) 공격

최근 이루어지는 사이버 공격의 목적은 단순히 개인적인 이득에서 벗어나 국가 기간망을 파괴하거나 국가 정보 시스템 마비와 같이 대규모 테러 형태로 범위가 확장되고 있다. 그 중에서도 서비스 거부 공격(Denial of Service: DoS)이 대규모 테러 형태의 사이버 공격에 가장 많이 활용되고 있다. DoS 공격은 네트워크나 시스템의 효용성을 손상시킬 의도로 행해지는 공격인데 시스템에 큰 부하를 줘서 성능저하나 서비스 방해를 일으켜 공격 대상이 되는 시스템이나 네트워크를 마비시키는 목적이 있다. 조성현 · 이택규 · 이선우(2014)의 연구에 따르면 DoS 공격은 MTU(Maximum transmission unit)를 이용하여 큰 사이즈의 Ping 패킷을 서버로 전송하여 재조합하게 만들어 리소스를 많이 소비하도록 만드는 Ping of Death 사례와 같이 특정 서버를 공격하는 형태에서부터 분산 서비스 거부 공격과 홈페이지 변조 및 개인정보를 유출한 6.25사이버 테러 사례와 같이 조직적인 테러 형태의 공격까지 다양한 형태를 보인다고 하였다. 이러한 Dos 공격의 또 다른 특징은 공격하려는 대상이 미리부터 정해져 있기 때문에 이러한 공격 대상이 되는 시스템이나 네크워크의 보안 취약점을 찾아서 공격하기 수주나 수개월부터 철저히 준비해서 이루어지기 때문에 다른 공격 패턴에 비해 더 많은 시간이 걸린다고 볼 수 있다.

Ⅳ. 대응 방안 및 제안

앞서 거론했던 9가지 공격 패턴에 대한 주요 대응 방법은 다음과 같다.

1. 앱어플 공격

웹 어플리케이션 안전화를 위해서는 비밀번호 기반 인증 실시가 가장 중요하고 반복적인 로그인 실패 시 계정이 잠기도록 잠금 정책을 실시하면 무차별 암호 대입 공격을 제지하는데 도움이 되고 아웃바운드 접속 모니터링을 통해 서버에서 수백만

개의 패킷을 외국 정부 시스템에 전송해야 할 이유가 없다면 해당 기능을 잠글 수 있다(김태형, 2014). 이를 통해 사용자의 입력 유용성 검사 및 확인을 철저히 하고 또한 제 3자(third-party) 플러그인에 대한 경계해야 한다.

2. POS침투

POS 침투에 대한 대응으로는 고정적인 하나의 인증 시스템만을 사용 하는 것이 아니라 다채롭고 강력한 인증 시스템을 복합적으로 사용하는 것이 좋다. 때문에 어떤 모니터링 옵션이 좋을지 결정 및 설치하는 것과 POS 환경을 분산 배치하는 것이 중요하다. 또한 POS 작업용 POS 시스템을 별도 확보해 직원이 웹 사이트 검색, 이메일 확인 또는 게임 용도로 사용하는 것을 금해야 한다(김태형, 2014).

3. 내부자 특권 악용

종업원들을 존중하고 조직의 결속력을 다지는 것은 기업 경영에서 매우 중요한 일임은 분명하나 하지만 조직이나 회사내에서 매일매일 금전적으로 중요한 부분을 책임지는 담당자나 기업에 중요한 데이터나 기밀에 접근할 수 있는 관리자에 대한 모니터하는 것 또한 그에 못지 않게 중요한 일이다. 왜냐하면 보편적으로 '내부자의 특권 악용'의 특징은 중요 정보나 기밀에 접근할 수 있는 이런 내부 관리자나 담당자에 의해 행해지기 때문에 이들에 대한 철저한 관리나 모니터링이 필요하다(Verizon, 2016). 특히 내부자 모니터 활동 중에 중요한 것은 USB를 사용해서 민감한 자료를 빼돌리는 지 확인하고 감시할 필요가 있다는 것이다. 근본적으로 중요 정보가 어디에 위치해 있는지에 대한 정확한 파악과 누구에게 어느 정도로 접근 권한을 줬는지에 대해서 파악하고 있는 것이 중요하다.

4. 여러 종류의 실수들

조직원들이 저지르는 다양한 종류의 실수들은 회사에 타격을 줄 수 있지만 이러한 경험들이 미래에 후배들이나 그들 자신에게 매우 중요한 보안 자산일 될 수 있는데 이러한 다양한 종류의 실수들에 대한 기록들을 보관하고 모아서 나중에 보안 관련한 교육이나 연수 시에 유용한 자료로 사용될 수 있기 때문이다. 잘못된 것들이나

실수들에 대한 자료들을 보관하는 다른 목적은 이런 데이터를 통해서 그들이 일어나는 빈도를 줄이고 일어났을 때 받을 데미지를 경감하는 하는 역할을 할 수 있다. 따라서 데이터 셋이나 데이터 자산들이 처리되거나 해체되기 전에 IT부서에서 이런 자산들이 엄격한 절차에 따라 행해지는 지를 확인해야 한다(Verizon, 2016).

5. 물리적 도난 및 손실

이동식 디바이스의 증가에 따라 도난과 손실은 가장 빈번한 보안 위기 사항을 발생시킬지 모른다. 때문에 모든 모바일 디바이스들과 이동식 미디어들은 완전 암호화해야 한다. 또한 정기적인 백업을 통해 주요 데이터의 손실을 예방하고 다운타임을 줄이며 보안 침해가 발생한 경우 범죄 수사에 도움을 준다(김태형, 2014). 근본적으로는 모든 직원들이 보안 상황에 대한 인식을 확고하게 만드는 일이다. 또한 데이터 분류 작업을 하고 민감한 데이터의 인쇄나 이동에 관한 회사 정책과 이를 위반하는 것에 대한 정확한 규정을 만들고 시행하여야 한다.

6. 크라임 웨어

보안 취약성을 방어하기 위해 판매사가 제공하는 OS 어플리케이션이나 보안 툴 등의 패치를 적극적으로 활용한다. 악의적인 실행을 막기 위해 프로그램이 시크립트나 매크로 실행하는 것을 막고 이메일 서버에 첨부파일을 통해 실행파일이나 파일 확장 등을 제거하는 것이 중요하다. 무엇보다 가장 중요한 것은 자신의 환경에 있는 악의적인 소프트웨어 분석을 정확히 하는 것이다(Verizon, 2016).

7. 지불카드 위조 장치들 & 위조 사고

악의적인 조작 & 조정을 막는 터미널(terminal)을 구입하여 사전적 대처를 실시하여야 하고 악의적으로 조정당하기 쉬운 디자인이나 기계에 대한 조심을 높여야 한다. 승인 없이 기계들이나 디바이스들을 조작하는지 모니터하고 그 증거들을 잡을 수 있게 하여야 하며 ATM 등의 물리적 데이터 완전성을 체크하는 프로세스를 세워야 한다(Verizon, 2016).

소비자들(consumers)관점에서는 개인 비밀번호를 핀홀카메라나 다른 몰래 카메

라가 못 보게 방어하고 조금이라도 미심적인 것이 있거나 조짐이 있으면 그것을 이용하지 말아야 한다.

8. 사이버 스파이

사이버 스파이 범죄는 더욱 복잡한 공격으로 들어가기 전에 단순한 툴들과 테크닉들로 시작을 하는 경향이 있기 때문에 가장 기본적인 보호들이 이런 종류의 위협을 차단하는데 중요하고 특수화된 보호도 필요하다.

첫째, 엔드포인트 보호가 중요하다. 악의적인 소프트웨어가 2016년 사이버 스파이 사고에 90% 연관이 되어있는데 이러한 소프트웨어가 이메일, 웹 드라이브 바이, 직접/원격 설치 등을 통해 전달되기 때문에 엔드포인트 보호가 중요하다. 둘째, 이메일 보호이다. 피싱이 여전히 사이버 스파이행위의 주요 공격 벡터이기 때문에 이러한 전달 매개체를 방어하는 것이 중요하다. 셋째, 네트워크 보호의 중요성이다. 사이버 스파이 범죄의 거점이나 기반이 마련되었다 할지라도 내부 시스템을 보호하기 위해 네트워크 보호는 중요하다. 넷째, 철저한 모니터링/로깅[1]이 중요하다. 모든 해킹들로부터 교훈을 얻기 위해 시스템, 디바이스 그리고 어플리케이션의 내부 모니터가 필요하다(Verizon, 2016).

9. DoS 공격

DoS 공격들의 빈도, 복잡성, 규모들이 계속 진화하고 발전하기 때문에 이것을 인지하고 클라우드 서비스 공급자들은 그들의 서비스와 인프라를 보호하기 위한 솔루션을 가지고 있어야 하며 그를 위해서는 DoS 공격에 대한 방어와 경감 능력에 대한 이해 필요하다. 무엇보다 DoS 공격이 실행되어지는 것을 막기 위해 철저히 핵심 자산을 분리·구분해서 관리할 필요가 있다(Verizon, 2016).

1) 로깅[logging] :시스템을 작동할 때 시스템의 작동 상태의 기록과 보존, 이용자의 습성 조사 및 시스템 동작의 분석 등을 하기 위해 작동중의 각종 정보를 기록해둘 필요가 있다. 이 기록을 만드는 것을 로깅이라 한다. 즉 로그 시스템의 사용에 관계된 일련의 「사건」을 시간의 경과에 따라 기록하는 것이다. 실행한 프로그램의 이름, 콘솔로부터의 키인, 이상 사태 발생, 정지 상태, 컴퓨터의 사용 시간, 입출력 장치의 사용 개시와 사용 종료 시간 등을 기록하는 것으로 이렇게 해서 기록된 것을 로그(log)라고 한다.

Ⅴ. 결 론

4차 산업혁명의 출발점에 선 지금 3차 산업혁명보다도 정보자원의 중요성은 더욱 증대되고 있다. 모든 분야에서 정보의 활용, 공유 그리고 전달 등이 과거에 비해 시공간을 초월해 동시 다발적으로 이루어지며 더욱 많은 양의 정보들이 이용되어지고 있다. 다시 말해 4차 산업혁명의 가장 중요한 자산은 정보자원이라 말할 수 있는데 이런 정보자원을 잘 보호하고 원활히 공유 될 수 있도록 하는 것이 정보보안의 역할이라고 볼 수 있다. 이런 4차 산업혁명에서 정보보안을 위협하는 데이터 침해사고라든가 데이터 유출 등이 기업 내부자나 범죄 집단에 의해 행해지는 빈도가 범죄행위가 증가하고 수법이 진화하면서 이에 대한 대응방법의 마련이 시급하다고 볼 수 있다.

따라서 본 연구는 이러한 정보보안의 위협요인들을 피싱, 보안 취약점 그리고 9가지 공격 패턴으로 나눠서 살펴보았고 이에 대한 대응방법에 대해서도 각각의 공격의 특징이나 성격에 따라 제시하였다.

무엇보다도 선행되어야 하는 것은 정보보안의 위협요인을 파악하고 이런 공격들을 미리 예방하기 위한 구체적인 대책이나 방법을 마련하고 필요한 교육을 조직체 전반적으로 실시하는 것이다. 해커나 공격자에게 악의적인 공격을 당한 후에 후속적인 조치를 취해도 완전한 원상복구를 하는데도 많은 시간과 노력이 들어가고 입은 피해에 대한 보상도 받기 어렵기 때문이다. 이러한 예방활동과 직원교육을 통해 공격에 대한 방어를 철저히 하고 실수를 통한 데이터나 정보 유실을 막을 수 있을뿐더러 사이버 스파이나 내부자의 권한 남용같은 비윤리적인 정보관련 범죄 행위도 줄일수 있다고 볼 수 있다. 또한 정보 유출이나 지능화된 사이버범죄가 급증하면서 이를 예방하고 대비하기 위한 국경을 초월한 고도의 전문적인 조사 및 협력 등이 요구되고 있다(신현주, 2016).

본 연구는 기업 현장에서 나타나고 있는 정보보안의 위협요인에 대한 사례 분석을 통해 발견된 9가지 정보보안 위협사항의 유형화와 그에 대한 대응방안 모색을 중심으로 전개되었다. 다만 본 연구에 기초 자료가 Verizon(2016)을 중심으로 한 것으로서 우리나라에서도 유사하다고 추정될 수 있으나 반드시 똑 같다고는 볼 수 없을 것이다. 예를 들어 우리나라의 경우 발생 빈도는 낮으나 그동안 보안침해에 가장

큰 피해를 본 유형은 DoS 공격이라고 할 수 있는데 이러한 DoS 공격이 위험한 이유는 발생 시 예상되는 피해의 규모가 다른 어떤 위협보다 크고 광범위하기 때문이다(김진열, 2015). 따라서 이의 방지를 위한 전문적인 솔루션의 확보가 무엇보다 중요하며 핵심 자산에 대한 분산 배치의 필요성이 강조되고 있다. 이처럼 Verizon(2016)에 연구된 내용이 모든 측면에서 우리나라에 적용될 수 없기 때문에 후속 연구에서는 이상의 유형화를 바탕으로 우리나라 상황에 맞춘 정보보안 위협요인에 대한 독자적이고 구체적인 연구가 이루어지기를 기대해 본다.

참고문헌

김동훈 (1997). POS 데이타의 중요성과 전략적 활용방안, 마케팅 제31권 제9호, 26-30.

김선애 (2014). '에브리웨어 웹', 공격도 에브리웨어 [데이타넷]. http://www.datanet.co.kr/news/articleView.html?idxno=102370 에서 검색

김성재 (2013). 유사 도메인 검색을 이용한 피싱 사이트 탐지 방안 연구, 성균관대학교 일반대학원 석사학위논문.

김진열 (2015), 가상화 봇넷을 이용한 DDos 공격 영향평가 방법론에 관한 연구, 한세대학교 대학원 박사학위논문.

김태형 (2014, 8, 26). 기업 데이터 보안 침해 9가지 패턴과 대응법 [보안뉴스]. http://www.boannews.com/media/view.asp?idx=42679&kind=3에서 검색

문가용 (2016, 7, 29). 모바일과 사물인터넷 위기론? 암호가 더 큰 문제 [보안뉴스]. http://www.boannews.com/media/view.asp?idx=50437&kind=4 에서 검색

신성윤·이윤창 (2015). 분석단계에서 취약점 관리의 보안 요건 정의에 관한 연구, **한국컴퓨터정보학회논문지 제20권 제3호**, 75-80.

신현주 (2016). 사이버범죄의 효과적인 대응을 위한 민간조사제도의 도입방안, 한국경호경비학회지 제46호, 63-86.

윤정현·문현실·김재경·최주철 (2015). 소셜 네트워크 서비스 기반의 POS 시스템 설계 및 개발, 한국IT서비스학회지 제14권 제2호, 143-158.

윤정무·조재경·유재철 (2016). 파일 I/O Interval을 이용한 랜섬웨어 공격 차단 방법론, **한국정보보호학회지논문지 제26권 제3호**, 645-653.

정기석 (2016). 신용카드 부정사용 방지 방안에 관한 연구, 정보·보안논문지 **제16권 제5호**, 33-40.

조성현·이택규·이선우 (2014). TCP/IP 네트워크 프로토콜의 DoS 공격 취약점 및 DoS 공격사례 분석, 정보보호학회논문지 제24권 제1호, 45-52.

조찬식 (2000). 정보사회에서의 정보보안에 관한 연구. 한국문헌정보학회지 제34권 제1호, 155-180.

한경수·임광혁·임을규 (2014). 하나넷을 이용한 P2P 기반 Storm 봇넷의 트래픽 분석, 한국정보보호학회논문지 제19권 제4호, 51-61.

한국정보보호진흥원 (2005). 네트워크 장비의 디폴트 로그인 패스워드 취약점 및 대책, **한국방재학회지 제4권 제2호**, 한국정보보호진흥원.

CA 백서 (2011). 내부자 위협 차단을 통한 IT 리스크 감소.. http://www.arcserve.com/kr/~/media/files/whitepapers/insider-threat-kr-wp.aspx 에서 검색

Eloff, M. M., and von Solms, S. H. (2000). Information Security Management: A Hierarchical Framework for Various Approaches. Computers & Security, 19(3), 243-256.

ISO/IEC 17799. (2005). Information technology-Security techniques-Code of practice for information security management. Retrieved from https://webstore.iec.ch/p-preview/info_isoiec17799%7Bed2.0%7Den.pdf

Kissel, R. (2013). Glossary of Key Information Security Terms. NIST Interagency/Internal Report (NISTIR)-7298rev2, 5 Jun.

Loch, K. D., Houston, H. C., and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 16(2), 173-186.

OECD (2002). OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD.

Schwab, Klaus. (2016). 클라우스 슈밥의 제4차 산업혁명 (송경진 역). 새로운 현재. (원전은 2016년에 출판).

Verizon. (2014). 2014 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp Verizon-DBIR-2014 en xg.pdf

Verizon. (2016). 2016 Data Breach Investigations Report. Retrieved from http://www.verzionenterprise.com/verizon-insights-lab/dbir/2016/

World Economic Forum. (2015). Deep Shift Technology Tipping Points and Societal Impact. Retrieved from http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_ Points_report_2015.pdf

【Abstract】

The Study on Threats of Information Security and Their Solutions in the Fourth Industrial Revolution

Cho, Sung-Phil

The third industrial revolution, characterized by factory automation and informatization, are moving toward the fourth industrial revolution which is the era of superintelligence and supernetworking through rapid technology innovation. The most important resources in the fourth industrial revolution are information or data since the most of industrial and economic activities will be affected by information in the fourth industrial revolution. Therefore we can expect that more information will be utilized, shared and transfered through the networks or systems in real time than before so the significance of information management and security will also increase. As the importance of information resource management and security which is the core of the fourth industrial revolution increases, the threats on information security are also growing so security incidents such as data breeches and accidents take place more often. Various and thorough solutions are highly needed to protect information resources from security risks because information accidents or breaches seriously damage brand image and cause huge financial damage to organization.

The purpose of this study is to research general trends on data breaches and accident that can be serious threat of information security. Also, we will provide resonable solutions to protect data from nine attack patterns or other risk factors after figuring out each characteristic of nin attack patterns in data breaches and accidents.

Keywords: The Fourth Industrial Revolution, Information Security, Security Risks, Solutions