한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

무역 산업에서의 비즈니스 스캠(Business Scam) 대응 문제점과 대책 방안

이은경[O], 조용현[*]
[O*]소셜정보안전센터
e-mail: divayeyo@nposecurity.kr[O], yhjo@nposecurity.kr[*]

Corresponds problems to Business scam and measures in the trade industry

Eun-Kyoung Lee[O], Young-Hyun Jo[*]
[O*]NPO Security Center

● 요 약 ●

우리나라의 무역 교역량이 '11년부터 3년 연속 1조 달러를 돌파하면서 인터넷 무역도 활성화 되고 있으나 인터넷 무역의 특징인 비대면 거래과정을 악용한 사기 행위가 급증하여 기업의 피해가 증가하고 있는 실정이다. 이메일을 해킹하여 거래처로 위장해 무역 거래대금을 가로채는 사이버범죄 수법인 비즈니즈 스캠(Business Scam)은 건전한 무역 활동에 위협적인 요소로 작용하고 있다.

이와 같이 무역 산업의 위협이 증가하고 있는 현재 상황에서 본 연구는 정보보호 관점에서 기술, 정책, 제도, 법률, 관련 사례를 조사 분석하여 비즈니스 스캠의 효율적인 피해방지 방안을 제시하고자 한다.

키워드: 산업보안, 기업보안, 비즈니스스캠, 정보보호, 사이버범죄, 이메일피싱

I. Introduction

인터넷 무역은 인터넷을 이용하여 거래 및 일선 관계를 성립시키고, 이에 따라 발생하는 대금결제와 선적, 보험 및 통관절차는 전자문서교환(EDI: Electronic Data Interchange)을 통해 이뤄지는 무역거래의 한 형태이다(산업통상자원부[1]). 전 세계적으로 인터넷 환경의 확산에 따라 무역거래가 인터넷 기반으로 이동하고 있으며, 인터넷 무역이 당사자와 거래자의 비대면 거래를 통하기 때문에 이에 따르는 위험도 함께 증가 하고 있다. 최근 이메일을 해킹하여 거래처로 위장해 무역 거래대금을 가로채는 사이버범죄 수법인 비즈니스 스캠은 인터넷 무역 활동에 위협적인 요소로 작용하고 있어, 정보보호 관점에서의 방지 대책이 필요하다.

II. Preliminaries

1. Related works

최근의 연구[2](원륭비, 2014)에서 인터넷 무역상의 위협을 정보보호 관리체계상의 주요 위협요인과 비교 하였을 때 ①경영전략 및 정보화 전략 수립 시 인터넷 무역을 안전하게 보호하기 위한 시스템 및 사용자 보호를 위한 전략 미수립 ②인터넷 기반의 비즈니스 환경인 인터넷 무역 사용상에 중요 무역문서 및 거래정보 등이 내부자에 의해 유출되는 방지대책 미수립 ③거래 알선 및 기업·신용정보 조회 사이트의 피싱(phishing)·파밍(pharming) 에 의한 인터넷 금융사기 피해 ④전자무역시스템의 인프라에 대한 외부 침입으로 인한 무역시스템의 파괴, 도난, 위·변조에 의한 피해 등으로 구분할 수 있다.

대한무역진흥공사(2015)[3]의 조사에 따르면 무역사기 피해규모는 지난 3년간 약 1,000억에 달하고 무역사기 피해의 발생 대상지역은 아프리카 및 유럽 지역에서 3개년 간 325건(61.3%)이 발생하였다. 인터넷 보급이 활성화 된 이후 무역 사기에 이메일을 적극 활용하고 있다. 비즈니스 스캠에 이용되는 이메일 해킹은 인터넷 환경의 전파성으로 인하여 대규모 피해가 발생할 소지가 높고, 악성코드를 동반할 경우 피해원인 분석과 복구 대책을 마련하기가 매우 어렵다는 특징을 가지고 있다.

III. The Proposed Scheme

1. The Proposed Scheme

1.1 사례 분석

본 연구에서 비즈니스 스캠에 사용된 공격 특징을 실제 피해사례를 통해 분석하였다. 비즈니스 스캠은 MITM(Man In the Middle attack)의 형태로 이뤄지고 있는 경우가 일반적이다. MITM 공격의 경우는 SELLER와 BUYER의 양측에서 오가는 메시지(무역대금

사기의 경우에는 입금 계좌 번호 변경에 대한 notice)를 위·변조하기 위해 공격자(Hacker)는 둘 중 하나의 이메일 계정을 해킹하고, 해킹된 메일 계정으로 대금을 가로챈다. 다음과 같이 비즈니스 스캠 메일은 불특정 다수에게 발송되거나, 대외 무역회사의 이메일을 타겟으로 발송된다.

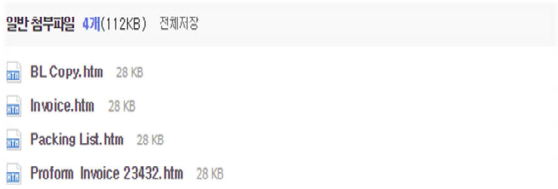

Fig. 1. 첨부 파일 (위장 사례)

<Fig.1>과 같이 첨부된 파일이름이 BL, Invoice, Packing list 등으로 제목으로만 판단할 때는 마치 비즈니스와 관련된 명세서 및 수출입 목록 등으로 위장되어 있지만 모두 <Fig.2>와 같이 포털 로그인 페이지로 위장된 첨부파일이다. 위장된 페이지를 통해 피해자가 입력한 ID와 비밀번호는 해외 소재 호스팅 업체로 전송된다. HTML 언어로만 구성된 이 첨부파일은 소스코드 자체에 의심스런 행위 등 코드가 없기 때문에 안티 바이러스 SW 등으로 탐지가 되지 않는다.

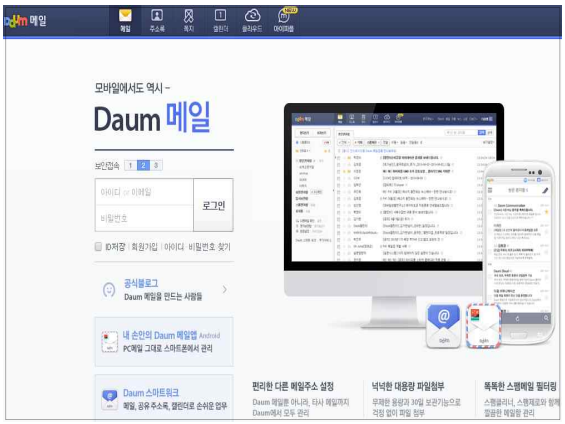

Fig. 2. 포털 로그인 페이지로 위장된 첨부파일

전송된 ID와 비밀번호를 통해 해커가 해당 메일에 로그인하여 SELLER 또는 BUYER에게 계좌변경 등과 같은 이메일을 송신하여 대금을 가로챈다. 이때 피해자는 로그인 비밀번호를 주기적으로 변경하지 않거나, 해외 로그인 차단 서비스를 적용하지 않거나, 무역대금 계좌 변경에 대한 별도의 확인절차를 거치지 피해를 입게 된다.

1)문자메시지(SMS)와 피싱(Phishing)의 합성어로 문자메시지내 인터넷주소 클릭하면 악성코드가 설치되어 피해자가 모르는 사이에 개인·금융정보 탈취하는 수법(출처: 사이버경찰청)

▶ 나이지리아 해킹조직과 공모, 세제 원료를 수출입하는 리비아 거래처의 이메일을 해킹한 후 국내업체에 가짜 이메일(입금계좌 변경)을 보내 거래대금 3,000만원을 편취한 피의자 검거 <'13.10월, 서울 중부서>
▶ 국내 의류업체의 이메일 해킹 후 러시아 거래처에 가짜 이메일(입금계좌 변경)을 보내 6,000만원을 편취한 피의가 검거 <'13. 8월, 서울 남대문서>
▶ 국내 자동차부품 판매회사의 이메일을 해킹한 후 이집트 거래처에 가짜 이메일(입금계좌 변경)을 보내 거래대금 1억 1,000만원을 가로챈 일당 6명 검거 <'13. 2월, 인천 남부서>

Table 1. 경찰청 수사 사례

경제풍월(2013)[4]의 보도 자료에 따르면 <Table1>과 같은 범행에 이용된 계좌는 중국, 영국, 미국, 등 주로 해외 금융회사의 계좌이나 국내 은행계좌도 7건(14.9%)사용되었다.

<Table2>와 같은 범죄 수법으로 우리나라의 무역 업체를 대상으로 하는 이메일 해킹 무역사기는 경찰청 발표(2015)[5]에 따르면 2013년 44건에서 2014년 71건으로 61% 증가하였고 피해금액도 한국무역협회(2015)[6]에 따르면 2013년 370만 달러(약 40억 원)에서 2014년 547만 달러(약 60억 원)로 48%나 증가했다.

▶ **(이메일 해킹)** 해커들은 악성코드에 감염된 수출업체 컴퓨터에 잠복하며, 거래현황을 체크하다가 입금단계에서 수출업체를 사칭하여 바이어에게 결제계좌 변경을 통지하고 거래대금 편취
▶ **(유사 메일 주소 생성)**
① 알파벳 (+) 또는 (-) nuts@apmail.com→nut@apmail.com
② 글자 재정렬 dm383@apmail.com→dm838@apmail.com
③ 글자 변환 sales@apmail.com→sa1es@apmail.com ※ (원래) 'L' 소문자 => (변환) '1' 숫자
④ 메일주소 서버네임 변경 xxx@happy.com -> xxx@hapy.com)

Table 2. 범죄 수법

1.2 문제점

비즈니스 스캠 관련 기존 방지 대책의 한계와 문제점을 제도, 보안수준, 정책 측면에서 살펴보았다.

1) 개인 고객의 금융사기 예방 위주 제도

정부는 금융소비자의 전자금융사기 피해를 예방하고 스미싱(Smishing)[1], 파밍 등 신·변종 전자통신 금융사기에 대응하기 위한 "전자금융사기 예방서비스"를 시행하였다(금융위원회, 2013)[7].

구분	사기유형별 피해건수(단위: 건, 경찰청)			
	'13년	월평균	'14.1~6	월평균
스미싱	29,761	2,480	1,317	220
메모리해킹	463	39	97	16
파밍	3,128	261	1,627	271
총계	33,352	2,780	3,042	507

Table 3. 사기유형별 피해건수 현황 비교

<Table3>과 같이 경찰청 자료(2014)[8]에 따르면 종합대책 시행 이후 월평균 2,700여건에 달하던 금융사기 건수는 500여건으로 급감하였다. 그러나 전자금융사기 예방서비스는 인터넷 뱅킹에 가입된 개인고객을 대상으로 사전에 전자금융이 가능한 PC를 지정하거나, 추가 인증수단을 거쳐야만 거래가 가능한 서비스로 무역대금을 처리하는 법인계좌 이용자는 이와 같은 전자금융사기 예방서비스를 이용할 수 없어 이에 따른 보완 대책이 필요하다.

2) 중소기업의 낮은 보안수준

무역사기 피해를 입는 대다수의 법인은 중소기업으로 대기업에 대비하여 낮은 정보보호 수준으로 운영되고 있다. 대기업 및 공공기관, 정부기관의 경우 대규모의 보안투자 및 보안인력을 통하여 인터넷 무역사기 공격과 같은 내부 자산(이메일 계정 등 정보자산)을 타겟으로 하는 위협을 보호하기 위하여 다중 보안체계를 구축하고 있다. 중소기업청(2013) 연구에 따르면 중소기업의 기술보호 인프라가 매우 열악한 것으로 파악되었는데 기술보호 수준을 등급별로 보면 취약/위험(71.8%), 보통(20.1%), 양호/우수(8.2%)으로 나타났다. 중소기업의 경우 보안에 대한 기술, 인력 투자에 있어 정부의 지원이 뒤따르지 않는 한 자체 보안기반 투자에 한계가 있다.

3) 사고예방을 위한 정책 미흡

인터넷 무역 사기 증가로 인한 신·변종 전기통신금융사기에 대처하고자 금융위원회, 경찰청 등 관계부처에서는 금융회사를 중심으로 다각적이고 체계적인 사고예방 정책을 수립하여 시행하고 있다.

하지만 무역 관련 부처인 KOTRA(2015)의 무역사기 방지 5계명에 의하면 ①기본정보 확인을 빼먹지 마라 ②평소와 다르면 2중 3중으로 확인하라 ③좋은 조건의 첫 거래를 조심하라 ④바이어 국적으로 신뢰도를 판단마라 ⑤어려울 때일수록 무역사기에 조심하라 등 사용자 주의환기에 맞춰져 있다. 또한 인터넷 무역 사기와 유사한 개념인 보이스 피싱 예방대책도 마련되어 있으나 그 매체를 휴대폰(음성/문자 메시지)에 국한하여 이메일을 이용한 비즈니스 스캠을 예방하기에는 부족하다.

1.3 대책 방안

사례 및 문제점을 통해 살펴본 바와 같이 비즈니스 스캠은 법인 사용자를 대상으로 하고 있으며, 비대면 거래라는 인터넷 무역의 특징을 악용하고 있다. 이러한 특징을 고려한 비즈니스 스캠의 대책 방안을 다음과 같이 제안한다.

1) 정보보호 관리체계상의 대책

대외 무역활동을 하는 기업들이 준수하는 AEO (Authorized Economic Operator)[2]에서는 안전한 무역기업으로의 최소한의 보안 요구사항을 규정하고 있다. 현실적으로 인력예산 부족한 중소 수출기업의 경우 관리적 보안 대책을 수립하기 위해 국내외 정보보호인증제도(KISA ISMS, ISO 27001 등)를 추가적으로 취득하고 유지하기에는 어려운 점이 많다.

관세청 AEO 가이드라인(2013)[9] 정보보호 관련 요구사항으로 정보보호 정책·지침 수립, 사용자 계정 및 패스워드 관리 (1인 1계정), 주기적인 백업 관리, 인적 보안(교육 및 훈련), 부적절한 프로그램(P2P) 설치 금지, 물리적 보안, PC보안(백신) 등을 정의하고 있어 이를 활용한 관리적 보안 대책을 수립하고 보완하는 것이 효과적이다. 특히 교육 및 훈련 과정에 임직원 대상 비즈니스 스캠 (이메일 피싱) 모의 훈련을 포함하여 이메일 보안 수준을 향상시키는 것이 비즈니스 스캠 예방활동에 중요하다.

2) 기업 업무 관리 체계 관점의 대책

비즈니스 스캠을 방지하기 위해서는 기업 내 경영 정책 및 업무 프로세스 상에서의 변화를 통해 능동적인 사고 예방조치와 대책마련이 요구된다.

사회 공학적 공격을 이용한 비즈니스 스캠 공격은 이메일 주소를 유사하게 변조하는 방법을 사용하고 있으므로 ①영문자나 아라비아 숫자와 혼동을 일으키기 쉬운 유사 도메인을 회사가 선점하는 방안, ②구매 시스템 내 중요 거래정보는 메일을 통해서 정보를 교환하지 않고 시스템을 통해 관리할 수 있도록 관리 시스템을 별도로 구축하여 BUYER-SELLER간의 신뢰통신망을 상호 제공하는 방안, ③민감한 구매 정보 (Invoice, Bank Account 등)에 대해서는 등록/변경 프로세스를 표준화 하는 방안이 필요하다.

3) 법 · 제도적 대책

관련 법률 조사결과 전자무역 촉진에 관한 법률(법률 제13155호, 2015.8.4. 시행), 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법에서는 전자무역 정보 및 시스템에 대한 전자적 침해, 해킹사고에 대한 보호 사항이 마련되어 있지 않다. 전자무역 촉진에 관한 법률의 경우 전자무역에 관한 시스템 및 문서를 보호대상으로 정의하고 있으나 전자무역문서 및 무역정보에 관한 일반적인 보안관리 사항만 명시되어 있다. 이에 전자무역산업의 안전성 확보를 위해 정보통신기반보호법[10]을 준용한 기술적 취약점 분석·평가 방법과 보호대책 수립, 사이버 보안 위협에 대한 무역산업 보안정보 공유체계, 침해사고 예방 및 복구 등의 종합적인 보호제도가 전자무역 촉진에 관한 법률 개정을 통해 마련되어야 한다.

2) 수출기업이 일정수준 이상의 기준을 충족할 경우 통관절차를 간소화하는 제도

IV. Conclusions

기업의 무역거래 활동을 대상으로 한 사기는 날로 증가하고 있으며 특히 비즈니스 스캠은 기업의 금전적 손실을 유발 할 수 있다는 점에서 경제, 사회적으로 문제점이 크다.

본 연구에서는 기업의 비즈니스 스캠을 예방하기 위하여 정보보호 관점에서 기술, 정책, 제도 등에 관한 연구를 진행하였다. 특히 본 연구는 정보보호 관리체계 관점에서 AEO를 통한 보안 수준 확보, 무역 기업 종사자들의 비즈니스 스캠 대응 훈련 등을 제시하였고, 기업 업무 관리체계 관점에서 스캠 피해를 방지하는 방안을 제시하였고, 법·제도적인 관점에서 전자무역 촉진에 관한 법률 개정을 통해 무역산업에서의 보안 정보 공유 체계를 수립하는 등의 방안을 제시하였다.

지금까지의 사이버범죄는 날로 고도화, 지능화 되고 있음을 살펴볼 때 비즈니스 스캠도 다양한 신·변종 형태로 진화할 것이다. 이에 국내 무역산업을 보호하고 인력·예산 부족한 중소 수출기업의 경영 안전성을 확보하기 위한 제도적 지원 방안에 관한 연구가 필요하다.

References

[1] Ministry Of Trade, Industry and Energy , “electronic trade (e - Trade comprehensive development programs)” , press release, 2001.

[2] RyonbiWon, “Research on China Electronic trade activation scheme”, Pai Chai University, 2014.

[3] Korea Trade-Investment Promotion Agency, “trade fraud occurrence and Countermeasures”, 2015.

[4] The EconoTalking newspaper, “http://www.econotalking.kr/news/articleView.html?idxno=112654”, 2013.

[5] National Police Agency, “Overturn mail came from Nigeria , the small and medium-sized enterprises haircut”, The Hankook-ilbo, p. A22, 2015.

[6] Korea International Trade Association, “E-mail of the hacking trade fraud surge” , the press release, 2015.

[7] Financial Services Commission, “Electronic financial fraud prevention services full enforcement” , the press release, 2013.

[8] National Police Agency, “The attention to small and medium-sized trading company aim mail hacking trade fraud”, the press release, 2014.

[9] Korea Customs Service, “AEO Guidelines”, 2013.

[10] Ministry of the Interior, “Detailed guide of technical vulnerability analysis and evaluation method of the main information and communication infrastructure”, 2014.