역추적 기술개발에 대한 ROI 분석

김종현°,나중찬
한국전자통신연구원 정보보호연구단

The ROI Analysis for developing Traceback Technology

Kim, Jong Hyun, Na, Jung Chan
Electronics and Telecommunications Research Institute
E-mail : jhk@etri.re.kr, njc@etri.re.kr

요 약

최근 들어 TCP/IP(인터넷 프로토콜)기반 역추적의 기술적 한계를 이용해 각종 명의(계정)도용 사건을 비롯해 금융피싱 사고들이 부쩍 늘고 있다. 이 때문에 천문학적인 경제 및 사회적 손실이 초래되고 있음은 물론, 사이버상의 각종 행위에 대한 제약과 발전을 가로막고 있다. 이와 같은 난제를 해결하고 기업 혹은 기관의 보안시스템을 강화하기 위해 실시간 역추적 기술이 등장했다. 과거 정보보호시스템의 가치는 비용 절감, 강력한 보안기술 도입 차원의 맹목적 시도, 구축에 따른 구축 난이도에 초점이 맞추어져 있었다. 하지만 최근에는 정보보호 투자성과 평가에 대해 더욱 설득력 있고 과학적인 결과를 원하고 있으며, 단순한 재무적 시스템 효과보다는 종합적인 비즈니스 효과에 대한 ROI 평가를 중요시하고 있다. 이 논문에서는 역추적 기술의 필요성과 배경에 대하여 살펴보고, 흔히 많이 사용하는 방식인 재무 관점의 비용·효과(Cost-Benefit) 기법을 통해 역추적 기술 개발의 투자수익률(ROI)을 분석할 수 있는 기준을 도출해 본다.

1. 서론

1.1 투자성과 평가(ROI)의 정의

정보보호 투자성과 평가는 '정보보호가 기업이나 조직의 목표 달성에 얼마나 기여하며, 경제적으로 얼마나 공헌하고 있는가를 사업 관점에서 체계적으로 조사하고 분석하는 행위'다[1].

이 과정에서 정보보호의 조직 목표 달성에 대한 경제적 공헌도 및 기여도 분석에 필요한 투자성과 평가의 기본 틀이 정보보호 투자성과 평가 방법론이다.

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력 핵심기술개발사업의 일환으로 수행하였음. [2007-S-022-01, All-IP 환경의 지능형 사이버공격 감시 및 추적 시스템]

이런 측면에서 정보보호 ROI는 체계적인 정보보호 투자성과 평가 방법론을 세워 정보보호 투자를 사업 관점에서 조사하고 분석·평가하는 활동으로 정의될 수 있다.

이것의 궁극적 목적은 정보보호를 통한 비즈니스의 '가치' 창출을 평가하기 위한 것으로, 투자 타당성 및 당위성을 분석해 정보보호 투자가치를 입증하고 현실 타당성 있는 효과를 실현할 목표와 정책을 형성하는 것이다. 즉 투자 실행 이전에는 투자의 의사결정을 합리화하고 투자 실행 이후에는 정보보호에 의한 사업적 이익의 극대화를 통해 궁극적으로 비즈니스 가치 창출자로서 IT보안의 역할을 정립하는 것이다.

예를 들어 어떤 기업이 보안 시스템을 구축하는

경우를 생각해보자. 이런 경우 투자 목표와 그 성과에 미치는 효과를 정량적으로 분석하지 않은 채 개념상 경쟁적 우위나 업무 생산성증대라는 너무 무형적이거나 거시적인 투자 목표를 가지고 정보보호 통제를 느슨하게 하며 시스템 구축에 착수한다면, 새로운 시스템이 결국 기업이나 조직에 기여하는 정도를 초과해 자원을 투입했는지 혹은 구축 이후에도 목표 대비 무엇이 개선됐는지조차 파악할 수 없게 될 것이다.

이는 기업 가치의 극대화라는 기업 목표에 반하는 것이며, 오히려 가치를 훼손할 수도 있는 것이다. 따라서 정보보호 투자도 기업의 다른 투자 활동과 마찬가지로 투자 안의 경제성, 즉 그 투자로 인해 발생하는 미래의 이익이 이를 위해 투입되는 비용을 상회해 가치가 창출되는지 반드시 파악할 필요가 있으며, 이를 파악하는 활동이 바로 정보보호 투자성과 평가 활동이다.

1.2 정보보호 투자성과 평가에 대한 인식 변화

포레스터 리서치의 조사에 따르면, 선진 IT기업들의 최고 경영자들은 정보보안시스템의 가치에 관해 투자회수율을 가장 중요시하는 것으로 나타났다. 즉 선진 IT기업 최고 경영자들의 정보보호시스템 가치에 대한 인식에 변화가 생기고 있다는 것이다.

과거 정보보호시스템의 가치는 비용 절감, 강력한 보안기술 도입 차원의 맹목적 시도, 구축에 따른 구축 난이도에 초점이 맞추어져 있었다. 하지만 최근에는 '투자 이상의 구체적인 효과를 거둘 수 있는가? 그렇다면 얼마나 빨리 투자 회수가 가능한가?', '정보보호시스템을 경영 전략 구현의 도구로 사용할 수 있는가?'와 같이 매우 현실적인 경영 효과에 초점이 맞추어지고 있다.

따라서 최근 경영자들은 정보보호 투자성과 평가에 대해 더욱 설득력 있고 과학적인 결과를 원하고 있으며, 단순한 재무적 시스템 효과보다는 종합적인 비즈니스 효과에 대한 ROI 평가를 중요시하고 있다.

이렇듯 각 IT기업의 최고 경영자들도 정보보호 투자성과 평가의 필요성을 절감해가고 있는 실정으로, 최고 경영자의 경영 전략을 지원해줄 수 있는 구체적 근거 없이는 새로운 정보보호 과제의 수행이 어려워지고 있으며, 이를 지원할 수 있는 정보보호 투자성과 평가 방법이 절실히 요구된다고 하겠다.

[표1] 정보화 투자성과 평가에 대한 인식변화 [2]

과거의 인식	현재 변화된 인식
정보시스템 자체에 대한 평가	투자 효과에 대한 평가
직접적인 재무적 효과에 대한 평가	종합적인 비즈니스 효과에 대한 평가
적접 비용에 대한 분석	간접 비용을 포함한 포괄적인 분석
정보기술 관점에서 내린 평가	비즈니스 관점에서 내린 평가
단편적 효과 분석	불확실성과 리스크 요인을 고려한 평가

1.3 정보보호 투자성과 평가의 과제

IT ROI 현황조사서[3]에 따르면 정보보호 투자를 위한 의사결정시 정보보호 투자성과 평가가 대답해야 할 과제는 다음과 같다.

가) 유형적 이익 (44.00%) - 비용절감, 투자수익이 어느 정도인가?

나) 투자비용의 규모 (31.20%) - 어디에 얼마를 언제 투자할 것인가?

다) 무형적 이익 (16.80%) - 고객의 만족도 향상, 기업의 가치 등

라) 투자 위험 (8.00%) - 손실위험, 시장위험 및 개발위험, 추가투자위험 등

결국, 정보보호 투자성과 평가는 투자 의사결정 최적화, 투자 위험도 분석, 투자 타당성 입증, 효과 정량화, 효과의 화폐 가치 전환, 선진 사례 제공 등을 IT보안관리 관점에서 다양한 분석과 방향을 제시할 수 있어야 한다.

2. 역추적 기술 개발의 ROI

2.1 실시간 역추적 기술의 현황

최근 들어 TCP/IP(인터넷 프로토콜)기반 역추적의 기술적 한계를 이용해 각종 명의(계정)도용 사건을 비롯해 금융피싱 사고들이 부쩍 늘고 있다. 이 때문에 천문학적인 경제 및 사회적 손실이 초래되고 있음은 물론, 사이버상의 각종 행위에 대한 제약과 발전을 가로막고 있다. 이와 같은 난제를 해결하고 기업 혹은 기관의 보안시스템을 강화하기 위해 실시간 역추적 기술이 등장했다. 이에 대한 기술적 필요성 및 배경에 대해 살펴본다.

기존 보안해법들은 불법행위자가 인터넷상에서 자신의 접속위치를 세탁(변조 및 우회)할 경우 추적이 사실상 불가능한 문제점을 드러내고 있다. 이에 비해 '실시간 역추적 기술'은 각종 행위에 대한 근원지 색출을 자동으로 수행한다. 역추적 기술의 기술적 가치는 현행 TCP/IP 구조상 IP 우회 및 변조가 이뤄질 경우 불가능했던 역추적을 가능케 한다는 점이다.

현재 보안시스템 환경에서 '로그기반' 역추적 기술은 여러 한계에 직면해 있다. 제한적인 수준 및 범위내에서 운용되는 문제를 비롯해 사이버테러(해킹)의 증가, 은폐 및 위장 기술의 향상으로 책임소재 파악이 어렵고, 대응의 적시성과 정밀도가 떨어지는 등의 난제를 안고 있다. 이러한 문제를 해결하기 위해 '역추적 기술'이 제안되었으며, 이 기술을 적용함으로써 발생되는 기대효과는 다음과 같다.

- 경제성(추적에 소요되는 비용과 시간, 노력) 향상
- 과학적이고 기술적인 원인 규명과 오대응 방지
- 위협의 실체 파악에 따른 신속한 대응안 강구 및 침입 재발 방지
- 심리적 압박을 통한 예방효과 증대
- 사고발생시 분석, 법률적 증거(Forensics) 강화 및 책임 소재 규명

이러한 '역추적 기술'은 기존 제한된 보안시스템(방화벽, IDS, IPS 등)의 구조적 한계를 벗어나 능동적인 대안을 제시하며 발전하고 있다. 이 기술을 적용하면 다양한 이벤트와 변수에 대해 보안체계의 정확성과 대응능력을 한 차원 높일 수 있을 것이다. 특히 애플리케이션 및 웹서비스에 대한 위협의 등장과 함께 이 기술은 더욱 각광받고 있고, 방화벽, 메일 등 적용분야 및 적용사례 또한 매우 다양하다.

실례를 살펴보면

- 보안 분야에서 통합 보안관리 시스템과의 연동
- 웹 애플리케이션 보안(웹방화벽)에 적용된 웹 해킹 추적
- 스팸 차단(바운싱백 방식) 및 추적
- 이메일 수신자가 포워딩을 통한 유출시 다단계 추적이 가능한 '이메일 유통 경로 추적'
- 금융피싱 대응 및 추적
- 저작권 침해 대응 및 추적
- 각종 웹서비스 추적(전자결제시스템 보안, 계정보안, 접근 보안 및 포렌식)

등에서 이 기술이 활발히 적용되고 있다.
이외에도 사이버범죄 수사 분야에 적용돼 이메일, 인터넷 게시판, 웹, 메신저 등 용의자를 추적할 수 있는 다양한 수단을 통합해 동작과 관리를 자동화한다. 또 향후 사이버테러 및 사이버전에 대비해 방어와 공격에 필수적인 요소인 정확한 '적'의 위치를 파악하고, 적시에 대응토록 한다. 또 각종 방어(Defence) 수단과 연계해 정밀 타격 수단을 견지할 수 있게 지원하는 등 정보전(Information Warfare)의 핵심요소로 자리잡게 될 전망이다.

결론적으로 역추적 기술은 인터넷 침해행위에 대응해 지속적으로 발전해 왔으며, 앞으로도 진화를 거듭할 것이다. 다만 이러한 발전은 기술적인 한계를 극복함은 물론, 합법적인 수준 내에서 은밀성과 적시성을 보장할 경우에 가능할 것이다.

2.2 역추적 기술 개발에 대한 ROI

정보화 투자분석의 주요 방법론으로는 여러 가지 모델이 있으나, 흔히 가장 많이 사용하는 방식은 재무 관점의 비용·효과(Cost-Benefit) 기법[4]을 통해 투자수익률(ROI)을 도출하는 것이다.

- Cost Benefit Analysis (Financial Approach) - 비용/수익 평가 ROI(Return On Investment)

> ROI(투자수익율)=순 이익/ 총 비용
>
> - 순 이익: 프로젝트로 인한 순이익의 누적적 합
> - 총 비용: 프로젝트에 투자된 혹은 투자될 것으로 예상되는 모든 비용

가) 투자대비 기대효과

① 초기 장비투자 비용 및 운영비용 절감:
IT보안 산업별로 최적화된 템플릿과 방법론으로 프로젝트 기간 및 보안장비의 도입비용 등 초기투자 비용을 최소화하여 투자회수 기간을 단축할 수 있다.

② 전문 인력 및 기술의 투자감축 (인건비 절감):
보안관리 전문인력의 투입인력을 최소화하고 기존 인력의 재배치로 인건비를 절감할 수 있다.

③ 시스템 확장 및 기능의 확대에 대한 비용 절감:
보안시스템 확장, 기능 확대등에 따른 추가비용을 절감할 수 있다.

④ 침입 재발 방지에 따른 비용절감:
위협의 실체 파악에 따른 신속한 대응안을 강구하고 공격자를 격리함으로써 침입 재발을 방지할 수 있다.

⑤ 업무 생산성 향상에 따른 비용절감:
시스템의 가용성, 성능 및 용량, 보안수준 등을 안전한 인프라스트럭처와 관리/운영 프로세스로 관리하여 비용을 크게 절감할 수 있다. 또한, 구축 및 안정화 기간 최소화를 통해 업무생산성이 향상될 것이다.

나) 피해 규모

① 피해대처시간 지연에 따른 손실
② 시스템 장애로 인한 실손실액
③ 업무 생산성 마비로 인한 손실
④ 기업, 조직의 가치 하락에 따른 손실
보안의 특성상 보이지 않는 ROI가 크다. 보안사고 발생시 우려되는 손실비용과 기업 이미지 실추에 따라 영업기회 감소 등을 고려하면 엄청난 ROI가 숨어있다.

3. 결론

본 논문에서는 정보보호 ROI에 대한 개요와 요구사항을 살펴보고, 최근 들어 사이버테러(해킹)의 증가, 은폐 및 위장 공격 등의 출현으로 기존 보안시스템의 구조적 한계를 벗어나 능동적인 대안으로 제시되고 있는 역추적 기술의 필요성과 배경을 언급하였다. 또한, 역추적 기술개발의 투자수익률(ROI)를 분석할 수 있는 기준을 도출하였으며, 이는 역추적 기술개발을 위한 기술변화추이를 분석하여 향후 기술개발 투자 방안 수립에 활용할 수 있을 것이다.

[참고문헌]

[1] 삼성SDS, "정보화 투자성과 평가 솔루션 및 적용 사례", 2002.

[2] 박기한, "정보화 투자성과 평가" LG-CNS,2006

[3] 한국정보산업연합회, "2003 IT ROI 현황조사," 2003

[4] Bierman, H. and Smidt, S., "The capital budgeting decision : economic analysis of investment projects", McMillan Publishing Company, 1993.