2013년 9월 전자공학회 논문지 제 50 권 제 9 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 9, September 2013 http://dx.doi.org/10.5573/ieek.2013.50.9.092

논문 2013-50-9-11

지능형 지속 위협에 대한 차세대 융합 보안 프레임워크

(Next Generation Convergence Security Framework for Advanced Persistent Threat)

이 문 구*, 배 춘 석**

(Moongoo Lee© and Chunsock Bae)

요 약

최근 사이버 공격은 명확한 목적과 특정화된 대상에 대해 지능적이고 지속적이며 복잡한 공격 특성을 가짐으로써 사전에 인지하거나 사고 발생 시 대응하기에 상당히 어려워지고 있다. 또한 피해규모도 상당히 크기 때문에 이에 대한 대응체계가 국가적인 측면에서 시급한 상황이다. 기존의 데이터센터 및 전산실의 통합보안체계는 이러한 최근의 사이버 공격에 대응하기에는 시대에 뒤떨어진 면이 많다고 판단된다. 그러므로 본 연구에서는 지능형지속위협(APT)기반의 공격에 대비해 보다 고도화된 차세대 융합형 보안 프레임워크를 제안한다. 제안한 차세대 융합형 보안 프레임워크는 영역별 보안계층, 영역별 연계계층, 행위가시화 계층, 행위통제계층, 융합대응계층의 5단계 계층적 구성으로 APT 공격에 대한 선제적 대응이 가능하도록 설계하였다. 영역별 보안계층은 관리적, 물리적, 기술적 보안영역별로 보안 지침과 방향을 제시한다. 영역별 연계계층은 보안 도메인 간의 상태정보가 일관성을 갖도록 한다. 지능화된 공격 행위의 가시화 계층은 데이터 취합, 비교, 판단, 통보의 수명주기로 구성된다. 행위 통제계층에서는 가시화된 행위를 통제하는 계층이다. 마지막으로 융합대응계층은 APT공격 전과 후의 대응체계를 제안하였다. 제안하는 차세대 융합 보안 프레임워크의 도입은 지속적이고 지능적인 보안위협에 대해 보다 향상된 보안관리를 수행하게 될 것이다.

Abstract

As a recent cyber attack has a characteristic that is intellectual, advanced, and complicated attack against precise purpose and specified object, it becomes extremely hard to recognize or respond when accidents happen. Since a scale of damage is very large, a corresponding system about this situation is urgent in national aspect. Existing data center or integration security framework of computer lab is evaluated to be a behind system when it corresponds to cyber attack. Therefore, this study suggests a better sophisticated next generation convergence security framework in order to prevent from attacks based on advanced persistent threat. Suggested next generation convergence security framework is designed to have preemptive responses possibly against APT attack consisting of five hierarchical steps in domain security layer, domain connection layer, action visibility layer, action control layer and convergence correspondence layer. In domain connection layer suggests security instruction and direction in domain of administration, physical and technical security. Domain security layer have consistency of status information among security domain. A visibility layer of Intellectual attack action consists of data gathering, comparison, decision, lifespan cycle. Action visibility layer is a layer to control visibility action. Lastly, convergence correspond layer suggests a corresponding system of before and after APT attack. An introduction of suggested next generation convergence security framework will execute a better improved security control about continuous, intellectual security threat.

Keywords: 지능형지속위협 : Advanced Persistent Threat, 행위 가시화 : Action Visibility, 행위 제어 : Action Control, 융합대응계층 : Convergence Correspondence Layer

* 평생회원, 김포대학교 모바일환경공학부 인터넷정보과
(School of Mobile &Environmental Engineering, Dept. of Internet Information, Kimpo College)
** 정회원, LG CNS, 정보관리기술사
(Cloud Group, Global Infra Service Unit, LG CNS Co.)
© Corresponding Author(E-mail: yeon0330@kimpo.ac.kr)
※ 이 논문은 2013학년도 김포대학교의 연구비 지원에 의하여 연구되었음.
접수일자: 2013년7월22일, 수정완료일: 2013년8월26일

Ⅰ. 서 론

인터넷의 급속한 확산과 함께 국내 데이터 센터의 신규 구축도 늘어났다. 대규모 전산장비를 운영하고 있는 데이터센터에서의 서비스 중단, 해킹, 정보유출 사고의 부정적인 영향은 국가적, 사회적으로 심각한 수준에 이른다. 본 연구에서는 국내 데이터센터에서 기본적으로 적용되고 있는 통합 보안 프레임워크에 대해 알아보고, 더욱더 지능화 되어가고 있는 사이버 위협의 형태인 지능형 지속위협(APT, Advanced Persistent Threat)에 대응하기 위해 기존의 통합형 보안 프레임워크의 한계를 극복하기 위해 할 수 있는 차세대 융합형 보안 프레임워크를 제시하였다.

본 논문의 구성은 다음과 같다. Ⅰ장 서론에서는 연구목적을 기술하고, Ⅱ장 최근 보안위협의 특징을 기술하고, Ⅲ장 기존의 통합 보안프레임워크를 공공 및 민간분야에 대한 사례와 고려사항을 제시하고, Ⅳ장에서는 본 연구에서 제안하는 차세대 융합 보안 프레임워크를 제안 하였으며, Ⅴ장에서는 결론과 향후 연구방향을 제시하였다.

Ⅱ. 최근 보안 위협의 특징

최근의 보안위협은 지속적으로 증가 및 진화 해 오고 있으며, 주목할 것은 공격방법이 더욱 지능적이며, 지속적으로 이루어지고 있다는 것이다.

1. APT의 정의와 특징

APT는 해킹을 시도하는 개인이나 그룹이 명확한 목적을 가지고 특정 대상을 겨냥하여 지능적이고 복합적인 방법을 동원하여 지속적으로 공격하는 위협형태를 말한다[1]. 이러한 APT의 특징은 지능형, 지속형, 복합형 공격으로 분류할 수 있다[6~7].

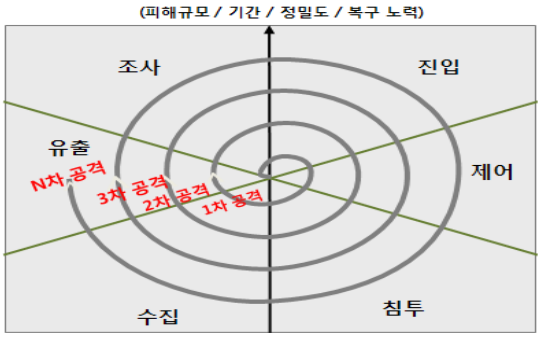

그림 1. APT 공격 개념도
Fig. 1. Diagram of APT Attacks Concept.

가. 지능형 공격

APT의 전체 공격 시나리오는 상당한 기간과 노력을 거쳐 조직화된 '지능형'으로 단편적인 탐지로는 최종 목적이 무엇인지 간파하기가 어렵다.

나. 지속형 공격

목적달성을 위해 긴 시간을 두고 공격대상 조직의 내·외부에서 조용하고 은밀하게 여섯 단계의 주기가 나선형의 수명주기를 갖고 반복되며, 수명주기가 6개월 내지 1년의 기간 동안 반복될 때 이에 비례하여 공격기술은 정교해지고 피해의 규모는 확대된다.

다. 복합형 공격

기술적 공격수단의 사용뿐만 아니라 회사의 주차장에 USB를 흘려두어 이를 습득한 내부 직원이 호기심으로 PC에 삽입하도록 유도하는 등 사회공학적인 기법과 기술적인 공격을 결합한 '복합형' 공격기법의 특징을 갖는다.

Ⅲ. 지능형 지속위협에 대한 통합보안프레임워크의 사례와 고려사항

1. 공공분야 사례

공공분야 통합보안 프레임워크 사례 [그림 2]를 보면 외부 인터넷 접점으로부터 데이터베이스에 이르는 정보시스템 서비스 구간을 8단계로 나누고 각 단계에 대응하여 DDoS대응시스템, 스팸/바이러스차단시스템, 침입차단시스템(IPS) 침입탐지시스템(IDS), 방화벽(Firewall), DDoS대피소, 웹방화벽, 서버보안시스템, DB

그림 2. 공공분야 통합 보안 프레임워크 사례
Fig. 2. The Example of Integration Security Framework for Public Institution.

보안시스템의 8개 관제/대응 시스템으로 구성된다. 이로부터 수집된 정보들을 분석하는 유해트래픽분석시스템, 취약점분석시스템, 악성코드분석시스템, 종합분석시스템의 4개 분석시스템을 통해 사후 분석 및 대응까지 가능하도록 지원한다[2].

기술적인 보안요소를 계층적 구조로 체계화하고 통합 운영하고 있으며, 24시간 365일 동안 중단이 없는 관제, 분석활동 수행으로 효과적인 공격 대응이 가능하며, 기술적 보안을 위한 시스템에 지속적인 투자를 통해 필요한 방어시스템을 골고루 갖추고 있으나 공격 및 이상 징후에 대하여 수동적인 대응에 집중되어 있어서 복합적인 공격에 대응하기에는 부족하며, 위협의 관점을 외부요소에 치중하고 있어서 내부위협, 즉 내부 사용자와 PC, 서버들 또한 공격을 수행하는 주체 혹은 공격에 이용될 수 있다는 것을 고려할 필요가 있다.

2. 민간분야 사례

민간분야 통합보안 프레임워크 사례 [그림 3]을 보면 개별 사용자의 행위를 전사적이고 실시간으로 모니터링하고 이력을 관리함으로써, 예상되는 위험을 사전에 탐지하고 조치하는 것이 목표이다. 구현의 핵심은 사용자별 단일 ID카드이다. 데이터센터 시설 내 또는 전산실 내의 각종 단말기와 시스템을 통해 사용자의 ID카드를 인식하고 이벤트를 발생시킨다. 즉, 사용자의 출근부터 컴퓨터 로그인, 네트워크 접속 그리고 시스템 접속과 사용내역을 빈틈없이 기록하고 관리하며, 이에 대한 분석으로 위협을 식별한다.

민간분야 프레임워크 사례의 특징은 사용자 행위중심으로 위험을 식별한다는 것이다. 사용자의 물리적 동선과 시스템 사용 등의 논리적 행위를 가시화하여 모니터링 할 수 있다. 외부 사용자 뿐 아니라 내부 사용자 역시 감시대상에 포함되며, 이는 내·외부의 사용자 모두를 위험요소로 인식하여 분석을 수행할 수 있도록 지원한다[3].

사용자의 논리적, 물리적 행위를 연관하여 분석하는 것은 APT위협에 대응할 수 있는 방안 중의 하나로서 기존의 통합보안체계 대비 한 단계 진일보한 것으로 볼 수 있다. 그러나 본 사례 역시 관리적 보안, 기술적 보안, 물리적 보안의 종합적인 연계와 이를 기반으로 신종 위협에 대응할 수 있는 고려가 아직 미흡하다고 볼 수 있다.

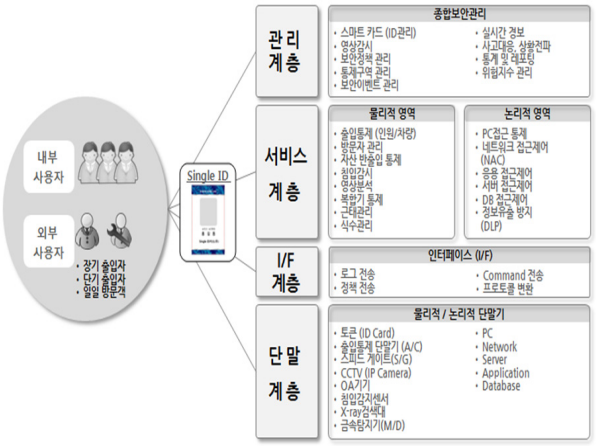

그림 3. 민간분야 통합 보안 프레임워크 사례
Fig. 3. The Example of Integration Security Framework for Private Institution.

3. 통합보안 프레임워크사례의 고려사항

공공분야의 통합보안 프레임워크 사례는 기술적인 방어체계와 사후적인 분석에 치중되어 있으며, 민간분야 사례는 개인의 행위를 중심으로 프레임워크를 구성하여 진일보한 방식을 보이고 있으나 전통적인 방식의 외부공격에 대한 대응체계를 포괄하고 있지는 못하며, 보안의 3대 영역인 관리적 보안, 물리적 보안, 기술적 보안을 모두 포괄하고 있지 못하므로 영역간의 상호 연결 관계가 고려되어 있지 않다[4].

공격 대응에 수동적으로 반응하는 프레임워크라는 점도 한계이다. 또한 작은 위협의 징후들을 통합적으로 수집할 수는 있으나 실질적으로 연관성을 분석하기 위한 방안이 미흡하다. 그러므로 APT와 같은 지능화된 신종 위협이 출현하기 이전에 수립된 프레임워크라고 볼 수 있으며, 보안위협의 변화와 보안 신기술을 반영할 수 있는 지속적인 변화관리가 필요하다.

APT와 같은 신종 보안 위협은 관리적, 기술적, 물리적 보안의 허점을 지능적으로 교묘하게 이용하고 복합적인 공격을 감행하여 인지조차 어렵다.

이에 대응하여 현 공공 및 민간 보안프레임워크의 한계점 극복을 위해서는 단순 통합을 뛰어넘어 융합화 되

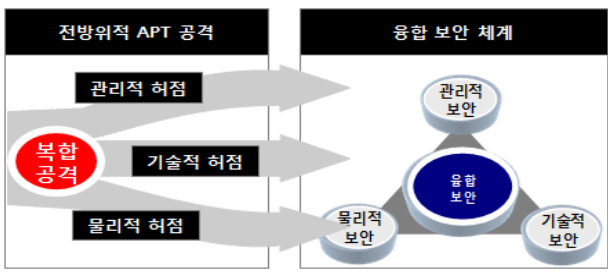

그림 4. 융합 보안 체계 개념
Fig. 4. A Diagram of Convergence Security System.

고 지능화 된 보안프레임워크 수립이 필요하며, [그림 4]는 APT와 같은 공격에 대응하기 위한 융합 보안체계의 개념을 도식화 한 것이다.

Ⅳ. 제안하는 차세대 융합보안 프레임워크

1. 차세대 융합보안 프레임워크의 요구사항

융합보안 프레임워크의 설계 요구사항은 다음과 같다[5, 8].

가. 구성의 적절성

보안의 3대 도메인으로 관리적보안, 물리적보안, 기술적보안 도메인을 모두 포함하여야 한다.

나. 계층간 연계성

독립적인 3개의 도메인이 융합관점에서 상호 연계되도록 구성하여야 한다.

다. 선제적 방어의 전환

외부 공격에 대한 수동적 관제 및 사후 대응 차원을 넘어 지능화되어가는 APT 공격에 대한 방어가 가능하도록 선제적인 전략으로 전환하여야 한다.

라. 환경 변화에 유연한 프레임워크

보안 위협은 지속적으로 변화, 진화 하고 있다. 프레임워크 역시 이러한 보안환경의 변화에 대응하여 유연하게 진화, 발전할 수 있어야 한다.

2. 제안하는 차세대 융합보안 프레임워크

제안하는 차세대 융합보안 프레임워크[그림 5]는 영역별 보안계층, 영역별 연계계층, 행위가시화 계층, 행위통제계층, 융합대응계층의 5단계 계층적 구성을 갖는다.

가. 영역별 보안계층

영역별 보안계층은 관리적·물리적·기술적 보안 지침과 방향을 제시한다.

(1) 관리적 보안

관리적 보안은 조직의 정보자산을 보호하기 위한 물리적, 기술적 보안을 포함하는 외연을 구성하고 정보보호와 관련된 국제 표준, 규제(Compliance)에 대응하는 지침과 방향을 제시한다. [그림 6]의 관리적 보안 목표 프레임은 정책·절차·조직·문서의 4개축과 계획(Plan)·실행(Do)·측정·분석(Check)·시정조치(Action)의 관리 주기를 갖도록 설계되었다. 내부자가 의도적·비의도적(미필적 고의 포함) 매개체 역할을 한 것임을 감안

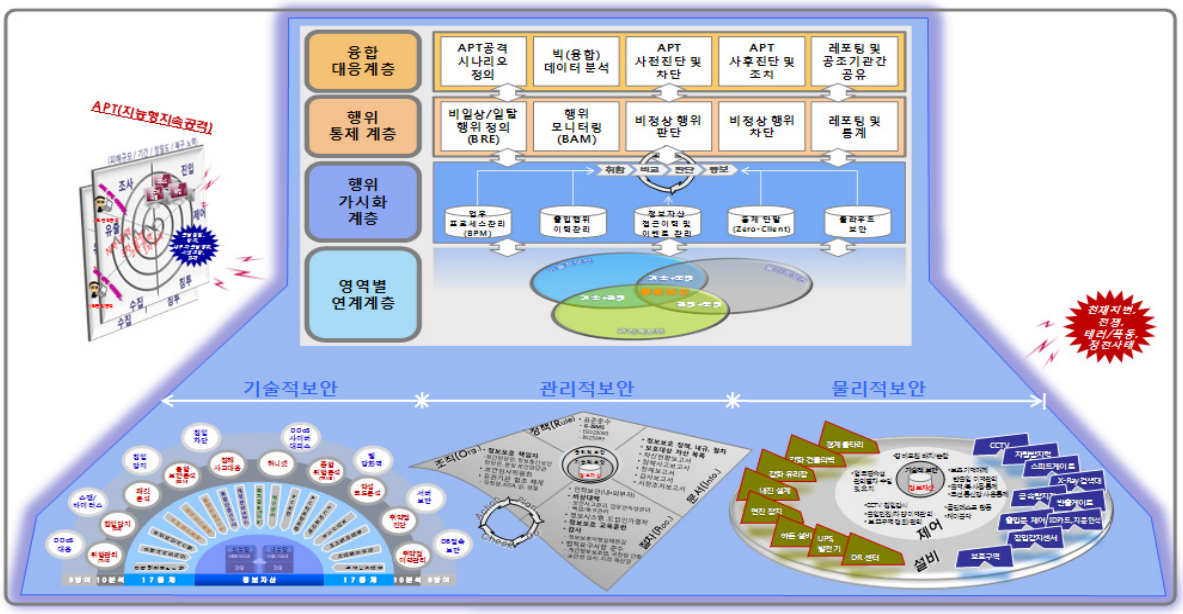

그림 5. 차세대 융합 보안 프레임 워크
Fig. 5. A Next Generation Convergence Security Framework.

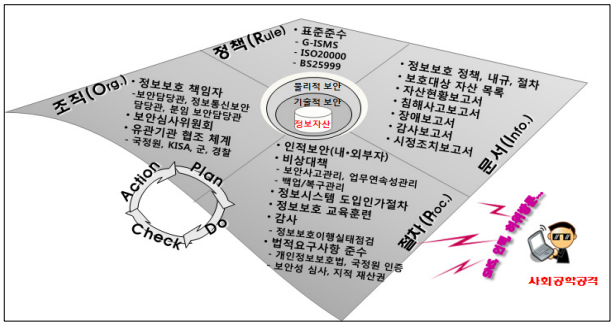

그림 6. 관리적 보안 프레임
Fig. 6. An Administration Security Frame.

할 때 사회공학 공격의 관점에서 관리적 보안 대응방식은 더욱 강화 되어야 하므로 절차 축에서는 인적보안(내·외부자)은 사회공학적 공격유형의 준수여부를 주기적으로 감시 및 시정 조치 할 수 있도록 한다.

(2) 물리적 보안

물리적 보안은 [그림 7]과 같이 설비와 제어 의 2개 축으로 설계하고, 통제가능 위협, 통제불가 위협에 맞추어 구성한다. 통제불가 위협의 대응으로 재난복구센터(DR, Disaster Recovery)구축과 내진설계를 일반화 한다. 통제가능 위협은 불법침입·내부자 불법행위·시설고장·화재 등에 대하여 비인가자의 데이터센터와 전산실 출입에 대한 통제, 출입 인가된 자라 할지라도 권한이 없는 특정보호 구역에는 접근할 수 없도록 통제하고 금속탐지기, X-Ray 검색대 등의 검사장치를 통해 차단하도록 한다.

(3) 기술적 보안

기술적 보안은 정보자산에 논리적인 접근을 통한 분산서비스거부공격(DDoS), 해킹시도, 내부자 공격 시도

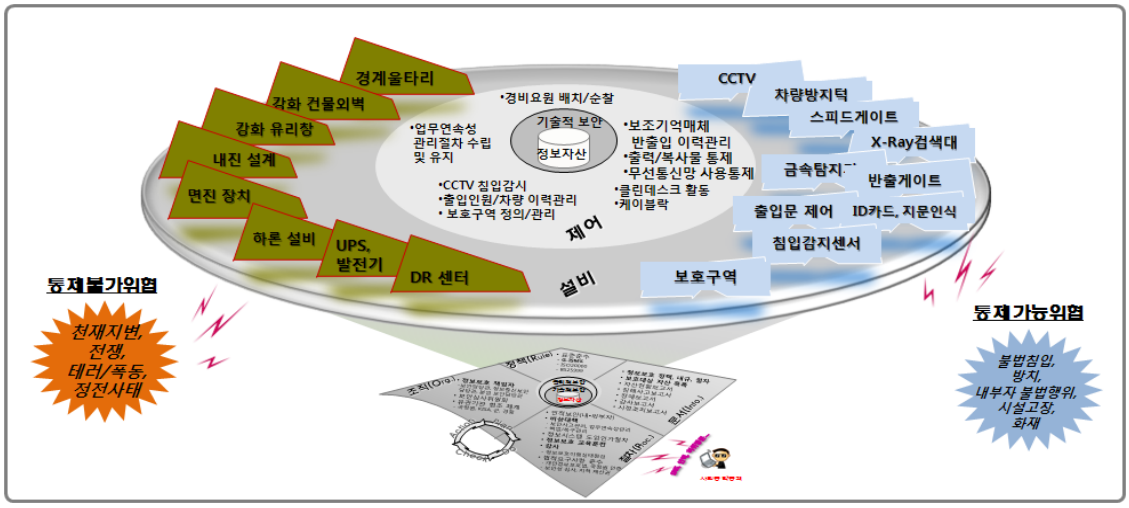

그림 7. 물리적 보안 프레임
Fig. 7. A Physical Security Frame.

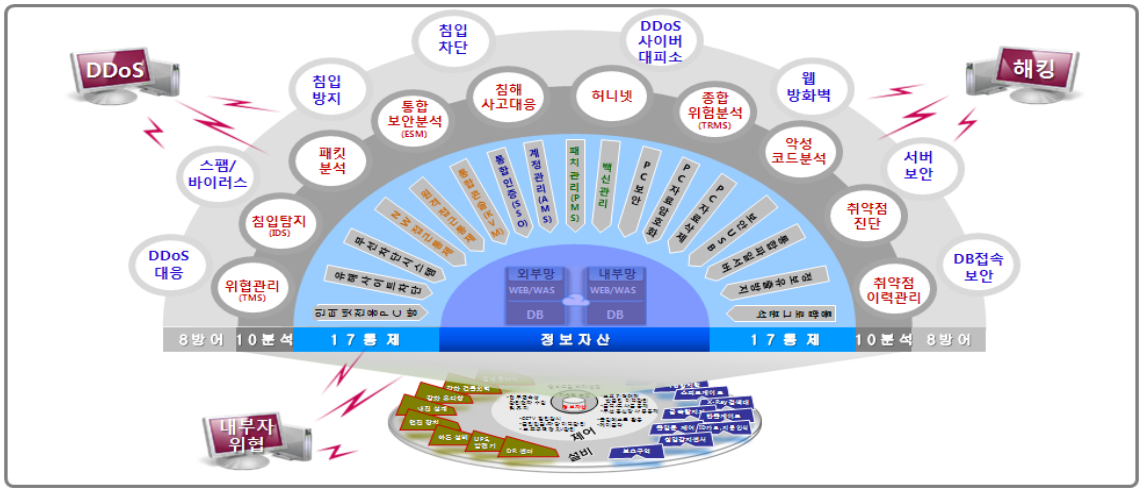

그림 8. 기술적 보안 프레임
Fig. 8. A Technical Security Frame.

등의 위협으로부터 보호하기 위해 [그림 8]과 같이 방어·분석·통제의 3개축으로 설계된다. 방어축은 외부 인터넷망을 통한 공격에서 시작하여 정보시스템의 논리적 계층인 네트워크·서버·데이터베이스에 이르는 각 구간별 방어를 담당한다. DDoS 대응장비, 스팸/바이러스 필터장비, 침입방지장비(Firewall), 침입차단장비(IPS), DDoS사이버대피소(캐싱서버), 웹방화벽, 서버보안솔루션, DB접속보안솔루션을 운영하며, 외부망과 내부망의 망분리는 기본으로 한다.

분석축은 방어축에서 발생된 공격의 2차적인 분석 및 대응을 수행한다. 유해트래픽분석(IDS), 통합보안분석(ESM), 패킷분석, 악성코드분석, 취약점 분석, 침해사고 대응(CERT) 등을 들 수 있다.

통제축은 정보자산에 대한 인가된 접근만을 허용하고, 정보유출 등 불법적인 시도를 기술적인 방법으로 차단하기 위한 것으로서 주로 사무실 및 전산실에서 근무하는 사용자, 개발자, 시스템운영자, 관리자들에 의한 의도적, 비의도적 공격행위를 방지하고자 하는데 중점을 두어야 한다. 유해사이트차단, 무선차단, 원격접근통제, 통합인증(SSO), 통합접근콘솔(KVM), 계정관리, 보안USB, PC보안, PC자료암호화, 통합파일서버, 정보유출방지 등의 솔루션을 활용할 수 있다. 최근에는 클라우드 컴퓨팅이 확산되면서 클라우드 환경에 대한 보안이 중요해지고 있다. 클라우드 환경일지라도 통제축에서 제시되는 보안솔루션들이 적용되는 것은 대동소이하다고 할 것이다.

나. 영역간 연계 계층

제안하는 차세대 융합 보안 프레임워크의 영역간 연계계층은 [그림 9]에서와 같이 관리적·물리적·기술적 보안 도메인간의 교차적 연계를 통한 보안활동을 말한다.

통합보안 관점에서 관리 + 물리 + 기술 보안이 연계되고, 관리 + 기술, 관리 + 물리, 기술 + 물리 보안이 연계되는 형태로 총 4개의 연계가 발생하에 대해 일관

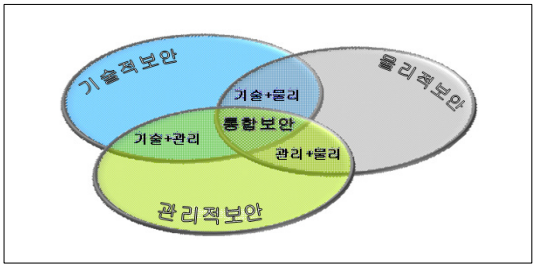

그림 9. 영역별 연계계층 구성도
Fig. 9. A Diagram of Domain Connection Layer.

성있는 보안설계를 한다. 그러므로 각 보안 도메인별 보안관련 이력정보는 데이터베이스화 되어 저장되어야 하며 이러한 정보를 이용하여 보안업무가 수행될 수 있도록 시스템이 구현되어야 한다.

다. 행위 가시화 계층

APT공격의 특성은 장기간의 치밀한 사전준비와 목표를 향한 단계적 접근과 목표 달성 후에 정보자산에 대한 파괴시도를 통해 그간의 흔적을 없애 추적하지 못하도록 한다는 점이다.

그러므로 행위가시화 계층 [그림 10]은 연계계층에서 축적된 데이터를 분석하여 투명성을 제공한다.

행위가시화의 대상이 되는 데이터를 다음과 같이 분류하였다.

(1) 업무프로세스 관리(BPM)기반 데이터

BPM(Business Process Management)은 데이터 센터 및 전산실에서 이루어지는 일체의 업무 프로세스에 대한 가시화를 제공한다. 주요한 업무프로세스는 Cobit 4.0에 정의된 IT기획 및 조직화, 정보시스템 도입 및 구축, 서비스 운영 및 지원, 모니터링 및 평가의 4개 도메인과 하부 34개 통제 프로세스로 표현한다.

(2) 출입행위 이력관리 데이터

데이터 센터 및 전산실을 출입하는 모든 기록들을 유지관리 하며, 이 기록들은 상주 및 비상주 근무자, 방문자를 대상범위로 한다.

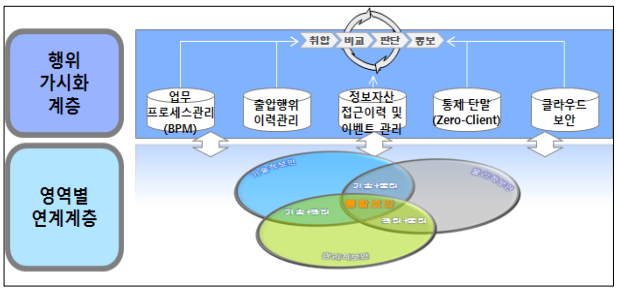

그림 10. 행위 가시화계층 구성도
Fig. 10. A Diagram of Action Visibility Layer.

(3) 정보자산 접근이력 및 이벤트 관리 데이터

정보자산 즉 서버, 데이터베이스, 네트워크, 소프트웨어, 응용프로그램에 접근한 기록들과 정보자산의 운영상태를 모니터링 하는 도구들을 통해 발생된 운영성 이벤트, 보안 모니터링 툴을 통해 발생된 보안이벤트를

대상범위로 한다.

(3) 통제단말(Zero-Client) 데이터

사용자 행위의 직접적인 도구인 데스크톱PC, 노트북PC, 태블릿PC 등과 데이터센터, 전산실, 또는 사외에서의 VPN을 통한 다양한 단말의 접근으로 인한 보안의 위험을 통제하기 위해서는 가상 데스크톱 인프라환경(VDI, Virtual Desktop Infra structure)을 조직 내 도입, 사용자 단말환경의 표준화와 접근 경로를 단순화한다.

(4) 클라우드 보안 데이터

효율적 자원관리, 사용자 편의성 등 다양한 이점으로 클라우드 컴퓨팅 인프라 도입이 늘고 있는 반면, 기존 컴퓨팅환경에서의 보안위협에 추가하여 클라우드 환경의 구조적 특징으로 운영체제, 네트워크, 프로세스, 하이퍼바이저, 관리자 등에 의한 위협에 직면하고 있으므로 TPM(Trusted Platform Module) 기반의 암호화기술로 클라우드 컴퓨팅환경 구축, 클라우드바이저를 통한 접근통제, 인증된 부팅, 안전한 스토리지 구축 등의 관리활동 기록들을 행위 가시화한다.

라. 행위 통제 계층

행위 통제 계층[그림 11]은 가시화된 행위를 통제하기 위해 업무규칙엔진(BRE, Business Rule Engine)을 활용하여 비일상·일탈 행위를 정의하고, 업무행위감시(BAM, Business Activity Monitoring)도구를 활용하여 행위모니터링을 수행하며, 비정상 행위 여부를 판단하고, 통제단말을 가상 데스크톱 인프라환경의 접근경로에서 격리하는 등의 조치를 통해 비정상행위를 차단하는 일련의 통제과정을 수행한다.

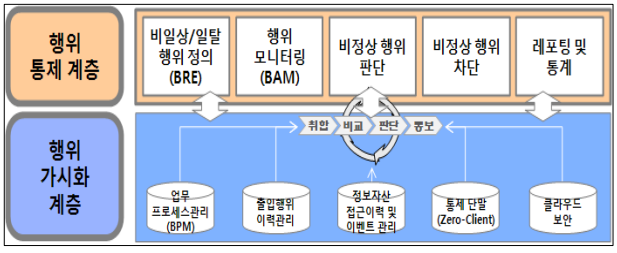

그림 11. 행위 통제계층 구성도
Fig. 11. A Diagram of Action Control Layer.

마. 융합 대응 계층

융합대응 계층 [그림 12]은 APT공격 시나리오를 정의한다. APT 공격시나리오의 정의는 우선적으로 APT

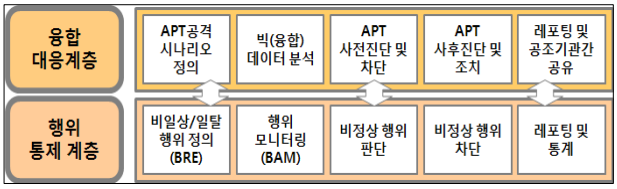

그림 12. 융합 대응계층 구성도
Fig. 12. A Diagram of Convergence Correspondence Layer.

침해공격 사례를 기반으로 알려진 공격시나리오를 정의하고 조직의 정보자산 특성에 따라 시뮬레이션 과정을 거쳐 특화된 공격시나리오를 추출한다. 다양한 공격시나리오가 가능하고 시나리오 전체 단계뿐만 아니라 중간단계 구간별로도 탐지를 위한 시나리오로 정의한다. 빅(융합)데이터 분석을 위해 대용량 분산파일 시스템을 도입하고 정보보호데이터웨어하우스(SDW, Security Data Warehouse)를 구성한다. 이를 기반으로 정형·비정형 데이터 분석을 수행한다. 또한 SDW를 기반으로 정보보호 데이터마이닝을 수행하여 APT 공격 시나리오를 주기적으로 추출하는 활동을 수행한다. 정보보호 인텔리전스(SBI, Security Business Intelligence) 구현을 통해 진행중인 APT 공격의 탐지 및 차단, 기 침해시도가 성공한 APT 공격에 대한 사후조치를 수행할 수 있다. 융합대응계층까지 도입된다면, 조직은 기존의 통합보안관제 체계에서 한 단계 상향된 융합보안관제 체계로 전환하기 위한 변화관리를 수행하게 된다.

V. 결론 및 향후 연구방향

클라우드 컴퓨팅, 빅데이터, 스마트 디바이스로 대변되는 현재의 진화중인 IT와 이에 기반 한 컨버전스 비즈니스는 새로운 문화와 경제적 부가가치 창출에 지대한 영향을 미치고 있다. 더불어 IT기술에 내재된 취약점 역시 더욱 많이 노출되고 있으며 이에 대응하기 위한 보안투자는 너무나 부족한 실정이다. 이에 본 연구에서는 지능형지속위협(APT, Advanced Persistent Threat)기반의 공격에 대비한 차세대 융합 보안 프레임워크를 제안하였으며, 영역별 보안계층, 영역별 연계계층, 행위가시화 계층, 행위통제계층, 융합대응계층의 5단계 계층적 구성을 갖도록 설계하였다. 제안한 융합보안 프레임워크는 기존의 통합보안관제 체계에서 한 단계 상향된 융합보안관제 체계로 전환하기 위한 변화관리를 수행할 수 있도록 단계별, 영역별, 연계성 등을 고려하여 설계하였다. 차후에는 본 연구에서 제시한 차세대 융합 보안 프레임워크가 실무에서 적용할 수 있도

록 세부 가이드와 중소규모 전산실 적용을 위한 맞춤적용을 위한 테일러링 가이드를 제시할 계획이다.

REFERENCES

[1] Strategies for Dealing With Advanced Targeted Threats, GARTNER Aug. 2011.
[2] http://isis.kisa.or.kr/ 2011. 2012, 2013.
[3] Safezone ID Provisioning, LG CNS, http://safezone.lgcns.com/solu/solu_idpro_intro.asp, Mar. 2013.
[4] Blue Coat Labs Report: Advanced Persistent Threats, BlueCoat, BlueCoat, 2011.
[5] 김현성, "인지무선네트워크를 위한 회전자 기반 적응형 보안프레임워크 설계", 대한전자공학회, 전자공학회논문지 제 50권 제 5호, 2013.5, 165-171 (7 pages)
[6] 최종욱, 김인기, 유지연, 조주원, "APT공격에 대한 E-DRM기반의 효율적 대응방안", 한국지역정보화학회, 한국지역정보화학회지 15(3), 2012.9, 29-54 (26 pages)
[7] 한성백, 홍성권, "APT공격에 대한 금융권에서의 대응방안", 한국정보보호학회, 정보보호학회지 23(1), 2013.2, 44-53 (10 pages)
[8] 최대선, 김승현, 진승헌, 이윤호, "스마트폰 환경에서 응용 보안을 위한 플랫폼 독립적인 보안 프레임워크" 한국정보과학회, 정보과학회논문지 : 정보통신 39(1), 2012.2, 102-107 (6 pages)

저 자 소 개

이 문 구(평생회원)
1984년 숭실대학교전자계산학 (학사)
1993년 이화여자대학교 대학원 전산교육학 (석사)
2000년 숭실대학교 대학원 컴퓨터시스템 (공학 박사)
2000년 3월~현재 김포대학교 모바일환경공학부 인터넷정보과 부교수
<주관심분야 : 인터넷 보안, 암호화 알고리즘, 전자상거래 보안, 멀티미디어 콘텐츠 보안>

배 춘 석(정회원)
1993년 전남대학교 경영학(학사)
1993년 4월~현재 (주)STM(현 LG CNS) 공공 및 금융분야 컨설팅, SI, SM 등 다수 프로젝트관리자 역임
2008년 12월 정보관리기술사
2009년 지식경제부장관 임명 IT멘토
<주관심분야 : 데이터센터 보안, 데이터센터 구축 및 운영 >