Hanbit RealTime 102

Max의 해킹과 보안 시리즈

네트워크 보안 시스템 구축과 보안 관제

장상근 지음

– 시스템 구축편 –

한빛미디어 Hanbit Media, Inc.

Max의 해킹과 보안 시리즈

네트워크 보안 시스템 구축과 보안 관제

장상근 지음

– 시스템 구축편 –

한빛미디어 Hanbit Media, Inc.

Max의 해킹과 보안 시리즈 **네트워크 보안 시스템 구축과 보안 관제** – 시스템 구축편 –

초판발행 2015년 5월 29일

지은이 장상근 / **펴낸이** 김태헌
펴낸곳 한빛미디어(주) / **주소** 서울시 마포구 양화로 7길 83 한빛미디어(주) IT출판부
전화 02-325-5544 / **팩스** 02-336-7124
등록 1999년 6월 24일 제10-1779호
ISBN 978-89-6848-763-7 15000 / **정가** 12,000원

총괄 배용석 / **책임편집** 김창수 / **기획·편집** 정지연 / **교정** 이미연
디자인 표지/내지 여동일, 조판 최송실
마케팅 박상용 / **영업** 김형진, 김진불, 조유미

이 책에 대한 의견이나 오탈자 및 잘못된 내용에 대한 수정 정보는 한빛미디어(주)의 홈페이지나 아래 이메일로 알려주십시오.
한빛미디어 홈페이지 www.hanbit.co.kr / **이메일** ask@hanbit.co.kr

Published by HANBIT Media, Inc. Printed in Korea

지금 하지 않으면 할 수 없는 일이 있습니다.
책으로 펴내고 싶은 아이디어나 원고를 메일(ebookwriter@hanbit.co.kr)로 보내주세요.
한빛미디어(주)는 여러분의 소중한 경험과 지식을 기다리고 있습니다.

저자 소개

지은이_ **장상근(맥스)**

현재, KBS(한국방송공사)에서 정보보호 업무를 하고 있다. 1998년 중학교 시절부터 해킹&보안 분야에 관심을 가졌으며 고등학교 때에는 충북 지역 정보보안 연구 모임(충북 해커스랩)에서 활동하였다. 대학에 입학해서는 세종대 정보보안 소모임(S.S.G)에서 활동하였으며 그 와중에 육군 정보보호기술CERT병 및 자이툰 파병으로 군 복무를 했다. 제대 후 2008년도 대학정보보호동아리 연합회(KUCIS) 회장을 하였고 국내 보안 업체들에서 악성코드 분석, 모바일 보안 및 보안 취약점 분석 등 선행 보안 기술 연구 활동을 하였다. 그 외 활동으로 해킹&보안 커뮤니티(Haru) 및 SECUINSIDE 보안 컨퍼런스 등에도 참여하고 있다.

최근 출판된 해킹&보안 관련 책은 웹 해킹, 리버스 엔지니어링, 모의 해킹 등 공격 및 분석에 초점이 맞춰 있는 반면 방어의 입장에서 저술된 책은 상대적으로 적다는 생각이 문득 들었습니다. 사실, 보안 업체 및 일반 기업에서는 공격을 목표로 하고 있는 것이 아니라 어떻게 하면 서버, 네트워크, PC 등 자신의 자산을 안전하게 보호할 수 있는지를 목표로 하고 있습니다. 하지만 자체적으로 보안 조직을 구성하여 보안 시스템을 운영 및 유지보수하고 보안 관제를 하면서 사이버 침해사고에 대응할 수 있는 능력을 갖춘 곳은 생각보다 많지 않습니다.

이 책은 중소기업, 스타트업, 학교, 게임방 등 소규모 조직에서 오픈소스를 활용하여 적은 예산을 가지고도 자체적으로 보안 시스템을 구축할 수 있도록 내용을 구성하였습니다. 보안 관제를 통해 다양한 사이버 공격에 대응할 수 있는 능력을 갖출 수 있도록 이 책이 작지만 큰 도움이 되었으면 합니다.

이 책이 나오는 데 많은 도움을 주신 한빛미디어 관계자분들께 감사의 말씀을 드리며 항상 응원하고 격려해 주시는 부모님과 가족, 동료, 친구들에게 감사의 말을 전합니다. 마지막으로 책을 쓰는 동안 중간중간 책의 내용을 검토해 주는 등 세심하게 배려해 준 여자 친구에게 사랑한다는 말을 전합니다.

대상 독자 및 참고사항

이 책은 보안 시스템을 구축하고 보안 관제를 하려는 기업 및 공공기관 등의 보안 담당자, 보안 시스템 구축과 보안 관제를 배우고자 하는 학생을 대상으로 합니다. 이 책은 네트워크와 운영체제(Linux)에 대한 기본적인 내용을 알면 좀 더 쉽게 이해할 수 있습니다. 또한, 이 책은 어떻게 보안 조직과 보안 관제 센터를 만들어야 할지에 대한 것, 보안 관제 시스템 구축과 운용에 대한 기본적인 것 등을 이해하고 실제 보안 관제 업무에 도움을 주는 것을 목표로 합니다.

이 책과 관련하여 궁금한 점은 다음의 저자 사이트 또는 E-Mail로 문의해 주기 바랍니다.

- 홈페이지: http://www.maxoverpro.org
- E-Mail: maxoverpro@gmail.com

한빛 리얼타임

한빛 리얼타임은 IT 개발자를 위한 eBook입니다.

요즘 IT 업계에는 하루가 멀다 하고 수많은 기술이 나타나고 사라져 갑니다. 인터넷을 아무리 뒤져도 조금이나마 정리된 정보를 찾기도 쉽지 않습니다. 또한, 잘 정리되어 책으로 나오기까지는 오랜 시간이 걸립니다. 어떻게 하면 조금이라도 더 유용한 정보를 빠르게 얻을 수 있을까요? 어떻게 하면 남보다 조금 더 빨리 경험하고 습득한 지식을 공유하고 발전시켜 나갈 수 있을까요? 세상에는 수많은 종이책이 있습니다. 그리고 그 종이책을 그대로 옮긴 전자책도 많습니다. 전자책에는 전자책에 적합한 콘텐츠와 전자책의 특성을 살린 형식이 있다고 생각합니다.

한빛이 지금 생각하고 추구하는, 개발자를 위한 리얼타임 전자책은 이렇습니다.

1 eBook First – 빠르게 변화하는 IT 기술에 대해 핵심적인 정보를 신속하게 제공합니다

500페이지 가까운 분량의 잘 정리된 도서(종이책)가 아니라, 핵심적인 내용을 빠르게 전달하기 위해 조금은 거칠지만 100페이지 내외의 전자책 전용으로 개발한 서비스입니다. 독자에게는 새로운 정보를 빨리 얻을 기회가 되고, 자신이 먼저 경험한 지식과 정보를 책으로 펴내고 싶지만 너무 바빠서 엄두를 못 내는 선배, 전문가, 고수 분에게는 좀 더 쉽게 집필할 수 있는 기회가 될 수 있으리라 생각합니다. 또한, 새로운 정보와 지식을 빠르게 전달하기 위해 O'Reilly의 전자책 번역 서비스도 하고 있습니다.

2 무료로 업데이트되는 전자책 전용 서비스입니다

종이책으로는 기술의 변화 속도를 따라잡기가 쉽지 않습니다. 책이 일정 분량 이상으로 집필되고 정리되어 나오는 동안 기술은 이미 변해 있습니다. 전자책으로 출간된 이후에도 버전 업을 통해 중요한 기술적 변화가 있거나 저자(역자)와 독자가 소통하면서 보완하여 발전된 노하우가 정리되면 구매하신 분께 무료로 업데이트해 드립니다.

3 독자의 편의를 위해 DRM-Free로 제공합니다

구매한 전자책을 다양한 IT 기기에서 자유롭게 활용할 수 있도록 DRM-Free PDF 포맷으로 제공합니다. 이는 독자 여러분과 한빛이 생각하고 추구하는 전자책을 만들어 나가기 위해 독자 여러분이 언제 어디서 어떤 기기를 사용하더라도 편리하게 전자책을 볼 수 있도록 하기 위함입니다.

4 전자책 환경을 고려한 최적의 형태와 디자인에 담고자 노력했습니다

종이책을 그대로 옮겨 놓아 가독성이 떨어지고 읽기 어려운 전자책이 아니라, 전자책의 환경에 가능한 한 최적화하여 쾌적한 경험을 드리고자 합니다. 링크 등의 기능을 적극적으로 이용할 수 있음은 물론이고 글자 크기나 행간, 여백 등을 전자책에 가장 최적화된 형태로 새롭게 디자인하였습니다.

앞으로도 독자 여러분의 충고에 귀 기울이며 지속해서 발전시켜 나가도록 하겠습니다.

차례

chapter 1

보안 관제 시작하기

1.1 보안 관제란

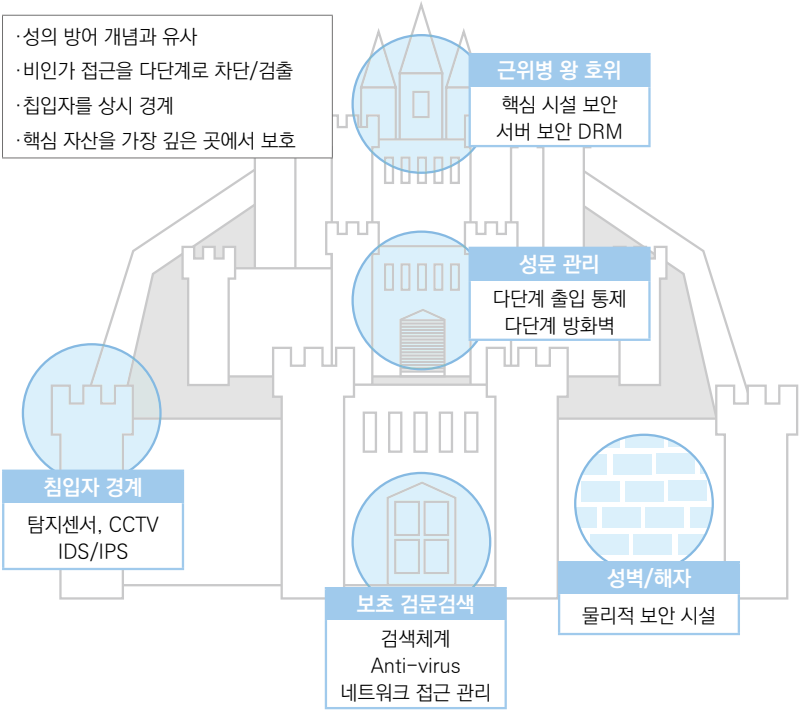
관제의 사전적인 의미는 '필요에 따라 강제적으로 관리하여 통제한다.'라는 것이며, 여기에 보안이라는 단어가 더해지면 '보안을 강제적으로 관리하여 통제한다.'라는 의미가 된다. 그렇다면, 보안 관제는 언제부터 시작된 것일까? 넓은 의미에서의 보안 관제는 우리가 생각했던 것보다 훨씬 오래 전부터 이루어졌다. 선조들이 성곽을 쌓고 성곽 구석구석에 경계병을 두어, 외부 침입자를 탐지하고 대응하여 내부 구성원의 안전을 보호했던 것도 보안 관제이기 때문이다. 그러나 우리가 앞으로 살펴보려는 보안 관제는 사이버 세상에서의 보안 관제를 말하는 것이며 이는 1990년대부터 출발했다.

1980년대로 접어들면서 컴퓨터 기술과 네트워크 기술이 발달했고, 그와 동시에 컴퓨터 범죄들이 발생되기 시작하였다. 대표적인 사례로, 1988년 로버트 모리스가 제작한 모리스 웜에 의해 당시 네트워크에 연결된 컴퓨터들이 감염되어 시스템이 마비된 사태, 1995년 FBI에 체포된 케빈 미트닉이 미국 주요 국가 기관과 기업체 전산망을 해킹한 사건 등이 있다. 이러한 컴퓨터 범죄들의 공통점은 네트워크로 연결되어 있는 곳에서 발생한 사건이라는 점이다.

이러한 문제점을 인식하면서 사이버 보안 관제는 점차 중요해졌으며, 네트워크 보안 관제의 필요성이 대두되었다. 1994년 최초의 상용 방화벽인 체크 포인트

'Firewall-1'이 나오고, 1998년 네트워크 침입 탐지 시스템(IDS)인 'Snort'가 나오면서 다양한 보안 솔루션 업체가 등장하였다. 또한, 다수의 보안 솔루션을 효과적으로 운용하기 위해서 네트워크 보안 관제 업체들도 등장하였다. 국내에도 해커스랩, 코코넛(2007년 안랩으로 인수됨) 등의 보안 관제 업체들이 있으며, 최근에는 보안 관제가 네트워크 보안 관제뿐만 아니라 전 방위적 보안 관제로 발전해 나가고 있다.

그림 1-1 과거의 보안 관제

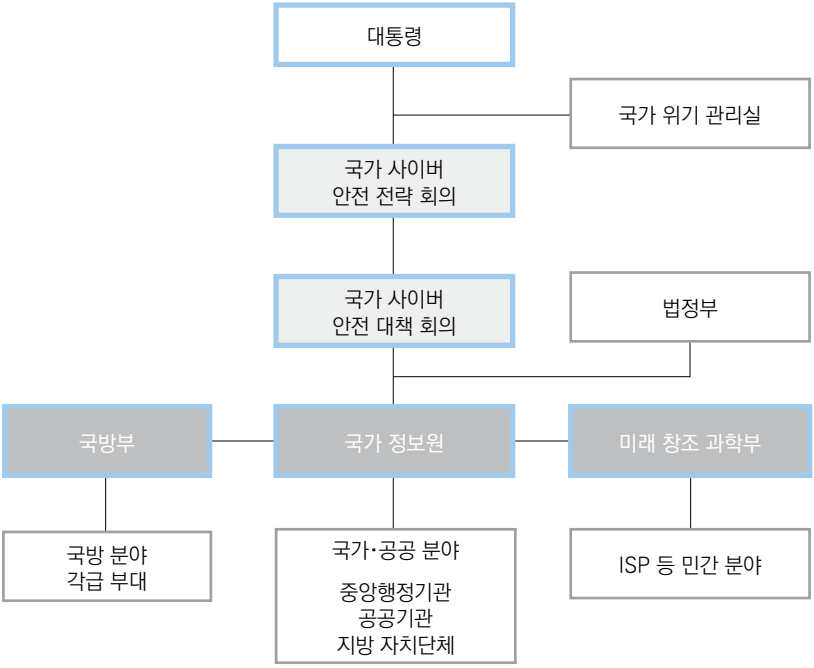


1.2 보안 관제 어떻게 하고 있나

국내에서의 보안 관제가 국가적인 차원에서 다루어지게 된 것은 2003년 '1.25 인터넷 대란'을 겪으면서부터였다. 1.25 인터넷 대란은 슬래머 웜에 감염된 PC들에서 국내 최상에 있는 DNS(혜화전화국 DNS)로 대량의 트래픽을 집중시켜

DNS를 마비시키는 바람에 전국의 모든 인터넷망이 불통되었던 사건을 말한다. 이는 우리나라뿐만 아니라 전 세계에서 동시에 벌어진 사건이었는데, 이 사건 이후 국가적인 차원에서 사이버 공격에 대비한 사이버 안전 보장의 필요성이 제기되었다. 이에 따라 공공, 민간, 군 분야 간의 사이버 안전 체계를 수립하고 상호 협력하여 유사시 대응할 수 있도록 2003년 7월 24일 '국가 사이버테러 대응체계 구축에 관한 기본계획'을 수립하였다. 이에 따라 2004년 2월에는 국가정보원 산하에 국가 사이버 안전을 위한 업무를 수행하는 '국가사이버안전센터'를 설치하여 국가 공공 분야를 담당하게 하였다. 또한, 군 분야는 국방부에 국방 정보전 대응센터를 두었으며, 민간 분야는 한국인터넷진흥원(KISA) 내 인터넷 침해사고 대응센터에서 사이버 보안 관제 업무를 수행하게 하였다.

그림 1-2 국가 사이버 안전 업무 수행 체계도



[그림 1-2]의 국가 사이버 안전 업무 수행 체계도는 정부의 조직 개편에 따라 조금씩 변화하고 있으며 본 체계도는 2010년 1월 기준으로 작성되었다.

이 책에서는 보안 관제 체계가 비교적 잘 운영되고 있는 국가 공공 분야, 국방 분야에 대한 보안 관제 상황은 다루지 않으며, 민간 분야 기업들에서의 보안 관제 상황에 대해 이야기하겠다.

대기업을 제외한 민간 분야에서는 자체적으로 정보보안 조직을 구성하여 보안 관제를 할 수 있는 여건이 되지 않아서 민간 보안 관제 전문 업체들에게 보안 관제 서비스를 받고 있는 상황이다. 하지만 보안 관제 서비스는 주로 네트워크 보안 관제에만 머물러 있으므로 기업 전체의 보안 관제를 맡기는 것에는 한계가 있다.

다음 표는 보안 관제의 유형으로, 크게 자체 보안 관제, 원격 보안 관제, 파견 보안 관제로 나누어져 있다.

표 1-1 보안 관제의 유형

유형	설명
자체 보안 관제	자체적으로 보안 전담 조직을 갖추고 관제 시스템을 구축하여 운영하는 관제 방식으로 국가 기관, 통신사, 대기업 등 보안을 중요시하는 곳이나 자체적으로 내부 네트워크망을 구성해서 운영하는 곳에서 주로 실시한다.
원격 보안 관제	보안 관제 전문 업체와 계약된 범위 내에서 보안 시스템을 구축하고 원격에서 보안 관제를 위탁해서 운영하는 방식으로 자체적으로 보안 관제를 하기 힘들거나 보안 인력이 없는 일반 기업에서 주로 실시한다.
파견 보안 관제	자체적으로 관제 시스템을 구축하였으나 보안 관제를 할 수 있는 전담 조직이나 보안 인력이 없는 경우 보안 관제 전문 업체에서 보안 전문 인력을 파견받아 보안 관제를 운영하는 관제 방식이다.

1.3 보안 관제를 왜 해야 하는가

"정보 보안, 모르는 것과 아는 것의 차이는 크다!"

'1.25 인터넷 대란' 이후 국내에도 끊임없이 굵직한 정보 보안 사고들이 이어지고 있다. 이에 공공 기관, 기업들은 정보 보안 강화를 위해 정보 보안의 예산을 늘리는 등 역량 강화에 노력하고 있다. 하지만 막상 보안 제품만 도입하고 사후 운영이 제대로 되지 않고 있어 정보 보안 사고가 언제든지 발생할 수 있는 위험이 존재하

고 있다. 더욱이 기본적인 보안 시스템조차 없는 중소기업들은 공격을 받고 있는지 아닌지, 공격을 받았다면 어떤 경로를 통해 유입되었는지 등 그 상황 자체도 파악할 수 없는 경우가 많다.

정보 보안 사고를 예방하기 위해서는 보안 시스템을 구축한 이후에도 보안 전담 인력이 보안 관제를 하여 위협을 사전에 탐지할 수 있어야 한다. 또한, 정보 보안 사고를 예방하는 활동과 함께 정보 보안 사고에 대한 대응 활동을 통해 똑같은 공격에 피해를 입지 않도록 대비할 수 있어야 한다.

이 장에서는 보안 시스템을 왜 구축해야 하는지, 보안 관제를 왜 해야 하는지를 보안의 3요소인 기밀성, 가용성, 무결성이 침해된 사건 사례를 통해 알아보도록 하겠다.

1.3.1 기업 기밀 정보 유출 피해

기업에서 어렵게 개발한 핵심 기술이나 영업 노하우 등이 경쟁 업체로 유출되는 경우, 피해 기업은 매출 감소뿐만 아니라 기업의 존폐가 좌우되는 최악의 상황을 맞이할 수도 있다. 그만큼 기업의 기밀 정보가 유출되지 않게 보호하는 일은 중요하다.

기업의 기밀 정보는 주로 퇴직자, 경쟁업체 직원, 협력업체 직원에 의해서 유출되는 경우가 많다. 특히 기술 유출의 경우에는 핵심 인재를 스카우트하는 방식이 가장 많고, 중요 자료를 복사하여 유출하는 사례가 그다음으로 많이 발생하고 있다.

표 1-2 2013년도 중소기업 기술보호 매뉴얼(중소기업 기술유출 연도별 현황)

구분	'09년도	'10년도	'11년도
기술 유출 경험 유무	14.7%	13.2%	12.5%
기술 유출 횟수	1.8건	1.6건	1.6건
기술 유출 피해금액(건당)	10.2억 원	14.9억 원	15.8억 원

참고 : [중소기업 기술보호 매뉴얼]

기술 유출에 대한 원인으로는 보안 관리 및 감독이 허술하거나 임직원의 보안 의식이 부족한 경우가 가장 큰 부분을 차지하고 있다. 안타까운 점은 한번 유출된 정보에 대해서 유출 사실을 입증하기가 쉽지 않다는 점이다. 그러므로 정보 유출을 예방하기 위해 보안 강화에 꾸준히 투자하고, 구성원들에게 보안 교육을 실시하며, 수시로 모니터링 하는 것이 중요하다.

1.3.2 개인정보 유출 피해

개인정보는 주로 해킹, 내부 직원 및 협력사 직원을 통해 유출되고 있다. 대표적인 사건으로 2008년 2월에 발생된 옥션(국내 대표적인 오픈 마켓 사이트 중 하나)에서 1,863만 명의 개인정보가 해킹으로 인해 유출된 사건이 있다. 2011년 미니홈피로 사랑받던 Cyworld에서 해킹으로 3,500만 명의 개인정보가 유출되자 많은 사용자들이 해당 사이트에서 탈퇴한 사건도 있다. 이로 인해 Cyworld는 급격하게 매출이 감소하여 기업 경영이 어려운 상황까지 왔으며 해당 사건은 여전히 소송이 진행 중에 있다. 또한, 최근 내부자에 의해 개인정보 유출 피해가 발생한 국민, 롯데, 농협 카드는 영업정지 3개월이라는 처벌을 받았으며, 이 결과 기업의 순이익이 감소하는 상황으로 이어졌다.

표 1-3 국내 주요 개인정보 유출 사례

일시	기업	피해 유형	피해 건수
2008년 2월	옥션	해킹	1,863만명
2011년 7월	SK컴즈(Cyworld)	해킹	3,500만명
2014년 1월	국민,롯데, 농협 카드	내부자 유출(협력 업체 직원)	2,000만명
2014년 3월	KT	해킹	1,200만명

1.3.3 악성코드 감염으로 인한 피해

악성코드 감염은 가장 빈번하게 일어나는 것으로, 위험도가 낮은 악성코드는 피해도가 낮지만 위험도가 높고 지능화된 악성코드는 큰 피해로 이어질 수 있다. 그 대

표적인 사례로 2013년 3월 20일 국내 주요 언론(KBS, MBC, YTN)의 전산망에서 3만 대 이상의 PC가 악성코드에 감염되어 피해를 입은 사건이 있다. 사전에 기업 내 일부 PC를 감염시킨 후 필요한 정보를 수집하고 PMS(패치관리 시스템)을 이용하여 다수의 PC를 동시에 감염시켜 데이터 파일 및 부트 영역을 파괴한 것이었다. 이로 인해 업무를 원활히 진행할 수 없었으며 이것을 복구하는 데에 막대한 시간과 비용이 발생하였다.

최근에 발생된 한국수력원자력공사 해킹 사건은 APT[01] 공격으로, 특정 목표를 대상으로 지속적으로 공격을 수행하여 특정 목표가 위치한 곳까지 악성코드를 침투하는 방식이다. 즉, 특정 목표에 위치한 구성원들에게 지속적으로 악성 E-Mail을 발송하여 누군가 해당 악성 E-Mail을 확인하면, 첨부된 악성코드들을 실행시켜 내부까지 침투해서 공격자가 원하는 자료들을 유출하는 방식이었다. 이러한 악성코드 공격은 쉽게 탐지하기 어려우므로 악성 E-Mail을 확인하는 일이 없도록 기업의 구성원들을 대상으로 지속적으로 보안 교육을 실시하여 정보 보안 의식 강화 활동을 해야 한다.

1.3.4 보안 취약점으로 인한 피해

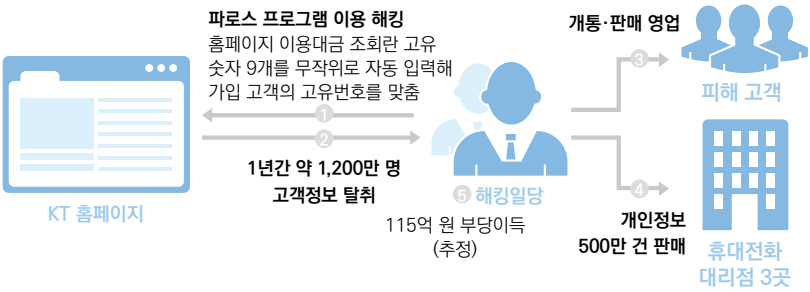
내부 또는 외부를 대상으로 서비스하는 시스템 또는 애플리케이션에 존재하는 취약점을 이용하여 공격자가 시스템 내부에 침투해 해당 데이터베이스에서 원하는 정보의 탈취, 홈페이지 변조, 악성코드 유포지로 활용하는 등의 피해가 발생하고 있다.

지난 2014년 3월 6일, 'KT 1,200만 명 개인정보 유출 사건'은 KT 홈페이지의 이용대금 조회 서비스에서 고객 고유번호 9자리를 무작위로 입력할 수 있도록 도와주는 해킹 프로그램을 이용해 1년 동안 1,200만 명의 이름, 주민등록번호, 전

01 APT(Advanced Persistent Threat) : 지능형 지속 위협

화번호, 집주소, 직업, 은행 계좌 등의 정보를 알아내 텔레마케팅 업체에 팔아넘긴 사건이었다.

그림 1-3 KT 홈페이지 개인정보 유출 흐름도



해당 사건에 이용된 '무작위 대입(Brute Force)' 방식은 취약점을 공략하여 원하는 정보를 획득할 때까지 공격하는 해킹 방식이다. 무작위 대입 공격 방식은 횟수 제한이 없는 이상 정상으로 보이기 때문에, 공격자가 취약점을 가진 페이지를 집중 공략하여 지속적으로 정보를 획득해 가도 해당 공격에 대한 탐지가 어렵다. 그러나 지속적으로 접근하거나 비정상으로 접근하는 횟수를 제한하는 방법을 사용했더라면 공격을 방어할 수 있었던 사건이었다.

KT 사건과 같은 해킹 방법 이외에도 최신 취약점을 이용한 공격들이 계속되고 있으므로 보안을 위해 운영하는 시스템과 서비스에 대해 보안 관제뿐만 아니라 최신 보안 패치 및 보안성 진단 활동을 병행해야 한다.

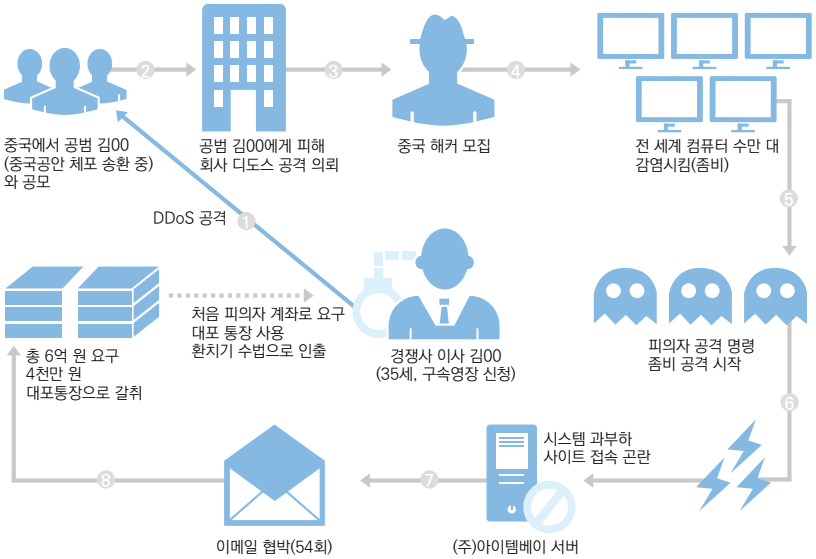
1.3.5 서비스 거부 공격

분산 서비스 거부 공격(DDoS[02])은 악의적인 목적으로 특정 시스템의 자원을 소모하게 하여 정상적으로 서비스할 수 없게 방해하는 공격으로, 공격자가 이미 보유

02 DDoS: Distributed Denial of Service

한 좀비 PC들에 명령을 내려 특정 사이트에 트래픽을 과도하게 보내는 방식과 명령 제어 서버 없이 악성코드가 감염된 네트워크에서 특정 사이트나 네트워크에 과도한 트래픽을 유발시키는 방식이 있다.

그림 1-4 아이템베이 DDoS 공격 금품 요구 사건 개요도

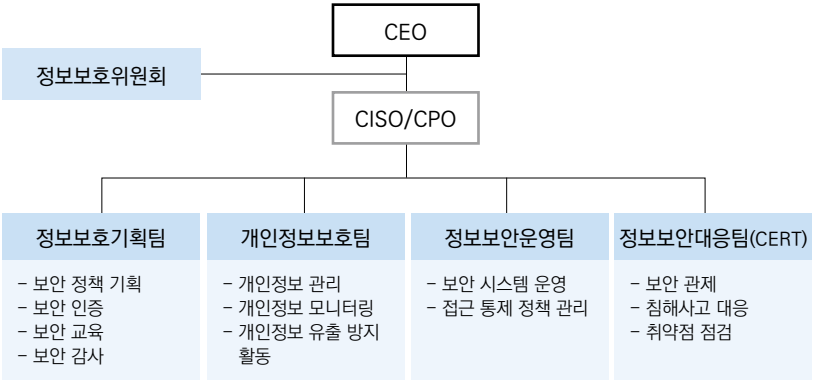


근래에 발생되었던 대표적인 서비스 거부 공격 사건으로는 '7.7 DDoS', '3.4 DDoS'가 있으며, 주요 기관 및 은행 사이트를 공격했다. 이외에도 중소기업이나 인터넷 서비스 업체들을 대상으로 지속적으로 서비스 거부 공격을 시도하였다. 피해를 입은 업체 중에는 정상적인 웹 서비스를 할 수 없게 되어 금전적 피해가 발생한 업체들도 있다. 이와 같은 피해가 발생하지 않도록 보안 관제 활동을 통해 과도한 트래픽이 발생되고 있는지 여부를 판단하고, 별도의 서비스 거부 공격 방어 장비를 이용해 서비스 거부 공격을 방어할 수 있도록 해야 한다.

1.4 보안 조직 구성하기

기업이 정보 보안을 제대로 하기 위해서는 정보 보안 업무를 전담하는 전문 조직을 구성해야 한다. 보안 조직은 상황에 따라 달라질 수 있지만 [그림 1-5]와 같은 형태로 구성하는 것을 권장한다.

그림 1-5 보안 조직 구성도



[그림 1-5]는 CEO 직속으로 CISO[03], CPO[04]를 두고 그 아래 주요 업무 단위로 팀을 구성하여 운영할 수 있는 보안 조직이다. 규모가 작은 기업에서는 정보보호팀으로 통합하여 업무별 보안 담당자를 두어 보안 업무를 수행할 수 있다. 또한, 이 그림에서 CISO/CPO는 CISO로 겸직을 고려한 것이므로 보안 기술과 법률을 잘 이해하고 정책에 반영할 줄 아는 융합형 전문가가 겸직하는 형태가 현실적으로 가장 적합한 보안 조직 형태라 할 수 있다.

보안 조직은 CEO 직속으로 CISO/CPO를 두어 정보 보호 업무를 총괄할 수 있도록 힘을 실어주고, 정보보호위원회를 통해 주요 보안 정책을 결정하도록 한다. CISO/CPO 아래에는 분야별로 팀을 구성한다. 정보보호기획팀은 보안 정책 기

03 CISO(Chief Information Security Officer) : 정보보호 최고책임자
04 CPO(Chief Privacy Officer) : 개인정보보호 책임자

획, 보안 인증, 직원들의 정보 보호 교육, 보안 감사 업무를 수행하며, 개인정보보호팀에서는 개인정보 관리와 개인정보 유출 방지를 위한 모니터링 활동을 수행한다. 정보보안운영팀에서는 방화벽, IDS/IPS 등 보안 시스템을 운영하고 시스템 접근 통제 업무를 수행하며, 정보보안대응팀에서는 보안 관제 활동과 침해사고 발생 시 분석과 대응을 하고 기업 내 정보자산 시스템의 취약점 점검 업무를 수행한다.

1.5 보안 관제 센터 구축하기

"작전에 실패한 지휘관은 용서할 수 있어도 보초 경계에 실패한 지휘관은 용서할 수 없다!"

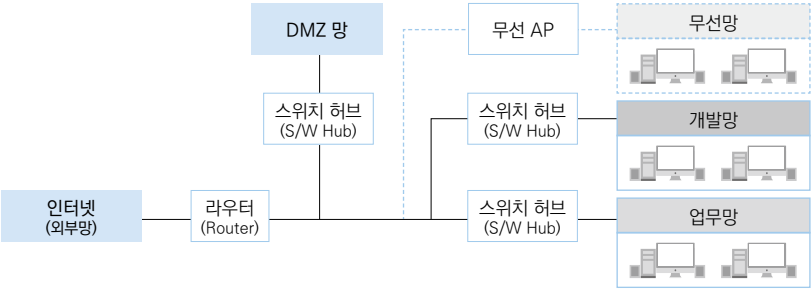
더글라스 맥아더

견고한 성곽을 쌓아 두었어도 성을 지키는 병사들이 없다면 어떻게 될까? 어렵게 만든 성이 공격자들에 의해 쉽게 함락될 수 있을 것이다. 이 말은 많은 예산을 들여 다양한 보안 시스템을 구축하였다 하더라도 보안 관제를 하지 않는다면 공격자가 내부로 침투해 내부의 중요 정보를 유출하거나 파괴시키는 상황에 속수무책으로 당할 수 있음을 뜻한다. 따라서 '성을 지키는 병사들'에 해당하는 보안 관제는 정보 보호에 있어 필수라고 할 수 있다.

1.5.1 무엇을 보안 관제해야 하는가

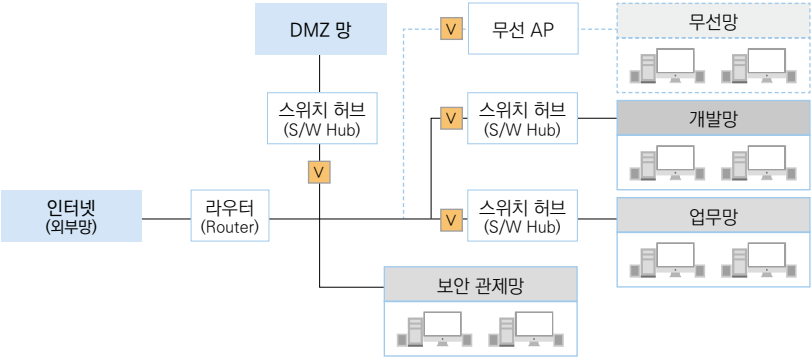
보안 관제의 주요 대상은 네트워크망을 기준으로 분류하여 각각의 네트워크망에서 발생되는 이벤트들이며, 네트워크 보안 장비 이외에 보안 소프트웨어들에서도 수집되는 각종 정보(악성코드 감염 정보, 각종 보안 에이전트 소프트웨어)들도 보안 관제의 대상이 된다. [그림 1-6]은 이 책에서 정의한 가상의 기업인 맥스 연구소의 네트워크 구성도다.

그림 1-6 맥스 연구소의 네트워크 구성도



이 그림을 보면, 맥스 연구소에서는 외부 서비스를 위해 DMZ 망을 운영하고 노트북이나 스마트폰을 위한 무선망, 업무를 위한 유선의 업무망, 제품 개발을 위해 폐쇄망으로 개발망을 운영하고 있다. 하지만 아직까지 맥스 연구소는 네트워크만 갖추어 놓고 보안은 하나도 되어 있지 않은 상황이다. 맥스 연구소의 네트워크 구성도를 보고 무엇을 어디에 놓고 보안 관제를 할 수 있을지 생각해 보자.

그림 1-7 맥스 연구소의 보안 관제 대상

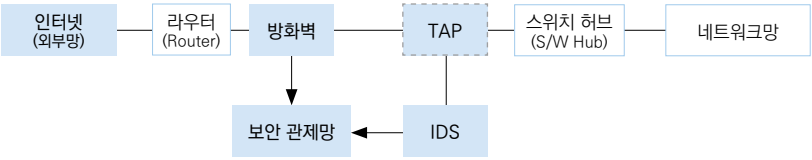


[그림 1-7]은 맥스 연구소의 네트워크 구성도에서 보안 관제를 하고자 하는 곳을 표기한 것이다. [V]로 표기한 부분은 보안 시스템들이 위치하여 각 망에서 수집된 보안 이벤트를 보안 관제망으로 전송하는 지점이자 보안 담당자들에 의해 보안 관제가 되고 보안 이벤트에 대응이 가능한 지점이 된다.

1.5.2 어떻게 보안 관제를 해야 하는가

무엇을 보안할지 대상을 정했다면 어떻게 보안 관제를 해야 하는지에 대해 고민해야 한다. 기본적으로 네트워크가 구축된 상태에서 무엇을 보안 관제할지 정했다면 이제는 어떤 보안 시스템을 구축해야 효과적인지 고려하여 보안 시스템들을 설치해야 한다.

그림 1-8 네트워크 보안 기본 흐름도



네트워크 보안의 외부망과 내부 네트워크를 구분해 주는 방화벽으로 1차적으로 필터링하고 2차적으로 IDS를 통해 공격을 탐지해 내도록 한다. IDS를 통해 트래픽을 모니터링 하는 방법으로는 미러링 방식과 인라인 방식이 있다. 미러링 방식은 TAP 장비나 네트워크 장비의 미러닝 포트 기능 설정을 통해 네트워크 트래픽 사본을 받아 모니터링 하는 방식이다. 인라인 방식은 방화벽과 동일하게 위치하여 모든 트래픽이 IDS를 거쳐갈 수 있도록 하는 방식이다. 하지만 인라인 방식으로 구성하는 경우 네트워크 성능이 저하되고 하드웨어에 장애가 발생하는 현상으로 인해 가용성을 보장할 수 없다는 문제가 있다.

보안 관제망에서는 통합 보안 관리(ESM) 시스템을 통해 수집된 보안 이벤트들을 분석할 수 있는 분석기와 분석된 이벤트들을 확인할 수 있다.

1.5.3 보안 관제 센터 구축 시 무엇을 고려해야 하는가

보안 관제 센터는 멋진 관제 상황판이 전부가 아니다. 얼마나 효율적으로 보안 시스템들을 관리하고 분석할 수 있는지에 초점을 맞춰 보안 시스템 도입 계획을 수립한 후 보안 관제 센터를 구축해야 한다.

표 1-4 보안 관제 센터 구축 시 고려 사항

구분	고려 사항
관제 상황실 (Control Center)	관제 상황판 구성 및 인테리어 공사 디자인 공조 시설, 소방 시설, 전기 및 통신 시설 배치 출입 통제 프로세스 확립, CCTV, 관제 시스템 운영 장비
통합 보안 관리 시스템 (ESM)	보안 시스템 현황 및 모니터링 대상 파악 향후 기능을 확장하여 운용 가능 여부 확인
통합 로그 분석 시스템 (SIEM)	로그 수집이 필요한 대상 시스템 파악 보안 이벤트를 수집·저장할 수 있는 스토리지 확보 보안 이벤트 분석을 위한 분석 시스템 확보
방화벽(Firewall)	네트워크 트래픽의 부하량을 측정해서 방화벽 도입
침입 탐지 차단 시스템 (IDS/IPS)	네트워크의 어느 부분에 넣어야 효과적으로 침입 탐지/차단이 가능한지
네트워크 접근 제어 시스템 (NAC)	사용자 및 장비에 대한 네트워크 접근 통제 방식 확인

이외에도 여러 보안 솔루션의 도입 후 원활한 유지보수 계약을 통해 보안 관제 체계에 안정성을 확보하고, 충분한 관제 운용 테스트를 통해 24시간 보안 관제의 연속성을 확보해야 한다.

보안 관제 센터는 어떻게 만들고 운영해야 하는가?

보안 조직을 갖춘 후 효과적으로 보안 관제하기 위해서는 보안 관제 센터 상황실을 구축하여 24시간 365일 체제로 운영해야 한다. 따라서 최대한 피로감을 줄여줄 수 있는 환경으로 구성하되 소음을 방지하여 관제 업무에 집중할 수 있도록 하고, 방염 처리된 벽체를 사용하여 소방 시설 및 공조 시설에 신경을 써야 한다.

보안 관제 상황실은 운영자에게 주어진 공간이 각기 다르기 때문에 관제 시설을 고려하여 최적의 공간이 될 수 있도록 배치해야 한다. 관제 영상 장비를 장착할 벽면에는 배선 및 배관이 보이지 않도록 벽체 뒤쪽으로 케이블 배선을 할 공간을 남겨두어야 한다.

그림 1-9 관제 센터 상황실 구성도

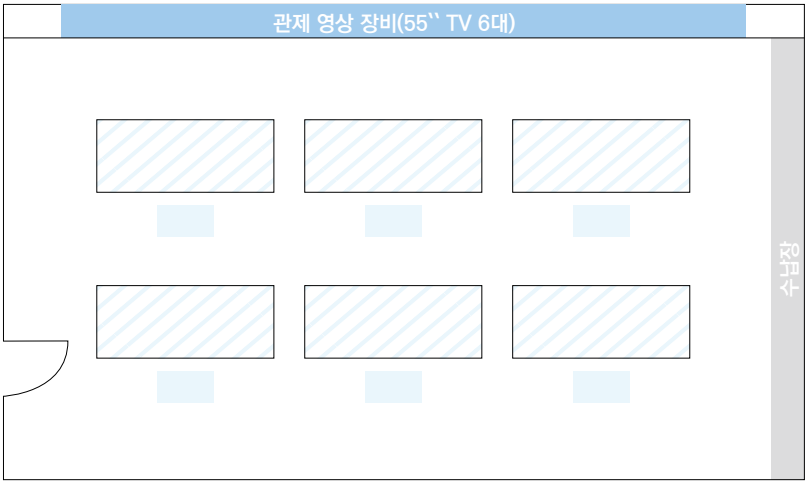
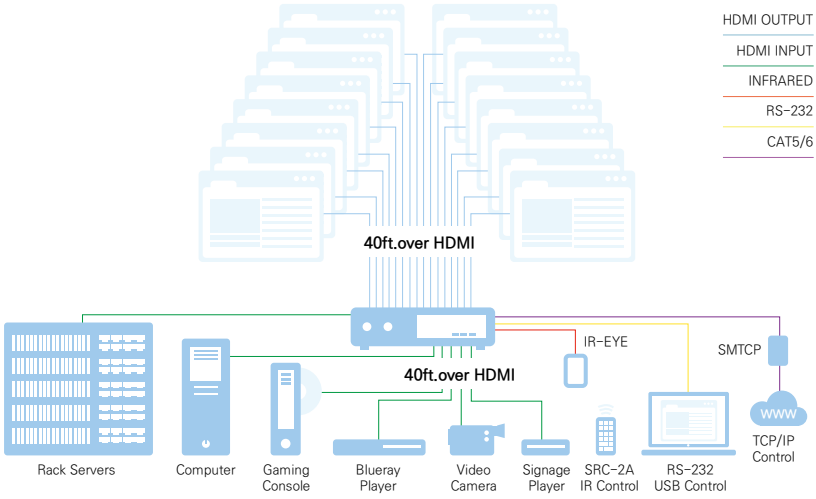


그림 1-10 관제 영상 장비 배치도

관제를 위한 영상 장비는 42인치 이상의 TV를 활용하고 있으므로, FULL HD(1920x1080)의 해상도를 지원하고 컴퓨터와 연결할 수 있는 HDMI 단자 및 다양한 입·출력 단자를 지원하는 것이어야 한다. 또한, 관제 영상 장비는 벽체에 달기 때문에 TV를 고정시켜 주는 Wall Bracket은 장착하기 쉽고 각도 조절이 자유로운 것을 선택하도록 해야 한다. 1대의 통합 보안 관제 제어 PC에서 여러 대의 TV로 영상 신호를 보낼 수 없으므로 영상 출력이 가능한 그래픽 카드를 4개 정도 장착하여 해결하거나 영상 장비가 많은 경우 Video Matrix Switcher,

RGB Matrix Switcher 등을 사용해야 한다.

그림 1-11 Video Matrix Switcher 장비



이외에도 관제 중에 내부로 연결된 보안 위협을 사전에 테스트해 볼 수 있도록 별도의 외부 인터넷망(ADSL)을 따로 연결시켜 주는 것을 권장한다.

보안 관제를 위한 보안 솔루션들은 무엇이 있는가?

기본적으로 방화벽, IDS/IPS에서 발생되는 네트워크 이벤트는 ESM[05] 솔루션을 통해 효율적으로 관리할 수 있다. ESM은 방화벽, IDS/IPS 이외에도 VPN, 서버, 라우터까지 상호 연동되어 다양한 보안 위협에 대해 사전·사후 대응하도록 관리할 수 있어 정보 보안 업무를 좀 더 신속하고 체계화된 프로세스를 통해 처리할 수 있다. 최근 ESM에서는 서버까지 보안 관리를 할 수 있도록 확장하고 있다.

또한, 능동적 통합 보안 관리를 돕는 RMS[06], TMS[07] 등의 보안 솔루션들도 있다.

05 ESM(Enterprise Security Management) : 통합 보안 관리
06 RMS(Risk Management System) : 위험 관리 시스템
07 TMS(Threat Management System) : 위협 관리 시스템

RMS는 보안 조직이 작고, 스캐너를 기반으로 위협 분석, 취약점 인지 및 각종 자산들에 대한 위험 요소를 평가하여 효율적으로 시스템을 운영해 주는 보안 솔루션이다. 반면 TMS는 제로데이와 같은 신규 공격 및 정규화된 보안 이벤트만 처리할 수 있는 ESM의 한계점을 보완하여 각종 사이버 공격을 탐지하고 네트워크 트래픽 모니터링 및 분석 기능을 제공하는 동시에 외부 위협 정보와 비교하여 위협 단계별로 대응할 수 있도록 하여 공격에 의한 피해 확산을 줄이는 목적을 갖춘 보안 관제 솔루션이다.

1.6 보안 관제 실무

보안 관제는 보안 솔루션들을 구축해 놓는 것이 끝이 아니라 시작임을 분명히 알아야 한다. 예를 들어, 공항의 관제탑에 비행기의 이·착륙을 돕기 위한 매뉴얼이 잘 갖추어져 있다 하더라도 관제사가 관제를 제대로 하지 않는 경우 언제든지 비행 사고가 발생할 수 있다. 사이버 보안 관제 또한 마찬가지다. 그러므로 사이버 공격에 대비하여 실제 보안 관제 중 발생할 수 있는 상황에 대해 프로세스를 적립해야 한다.

1.6.1 사이버 보안 침해사고 대응 프로세스

하나의 보안 솔루션으로 모든 사이버 공격을 막을 수는 없다. 따라서 각각의 상황에 적절한 보안 솔루션을 계층형으로 배치하여 보안 조치 활동을 해야 한다.

첫째, 예방(Protect) 단계는 명확하게 인지될 수 있는 공격을 사전에 막는 단계다. 방화벽을 통해 외부로부터 유입되는 공격을 막아내는 것이 가장 대표적이며, 지속적으로 구성원들에게 정보보호 교육을 시행하여 조직 전체의 보안 의식을 높이도록 해야 한다.

둘째, 탐지 및 분석(Detection/Analysis) 단계는 방화벽을 통과한 공격을 모니터링

하여 탐지하고 분석하는 단계다. IDS(침입 탐지 시스템)이 대표적인 제품이며 최근에는 APT 솔루션들이 이 계층부터 파일 단위까지 위협을 탐지하고 분석할 수 있어야 한다.

셋째, 대응(Response) 단계는 예방, 탐지/분석 단계를 통과하여 공격을 당한 경우 공격을 받은 위치를 찾아내서 분석하고 공격자를 확인하고 차단하는 등의 보안 조치를 하는 단계다. IPS(침입방어 시스템)을 통해 공격 데이터를 막거나 보안 솔루션이 사이버 침해사고 대응이 가능한 보안 전문가를 통해 대응할 수 있어야 한다.

넷째, 포렌식(Forensics) 단계는 침해사고를 당한 시스템에 존재하고 있는 디지털 증거를 수집하고 보존함으로써 향후 공격자의 의도를 파악하고 법적 증거물을 확보할 수 있도록 조치하는 단계다. 다양한 디지털 포렌식 도구들을 통해 침해사고의 증거물을 확보할 수 있어야 한다.

1.6.2 사이버 위협 경보 단계별 업무 대응

사이버 공격의 수준을 평가하여 단계적으로 경보를 발령하고, 그에 맞는 대응 체계를 갖추게 하는 것을 사이버 위협 경보의 목표로 하고 있다. [표 1-5]는 국가사이버안전센터의 '사이버위기 경보단계', 한국인터넷진흥원 인터넷침해대응센터의 '인터넷침해사고 경보단계'를 참고하여 내부 사이버 위협 단계 수준을 '정상 → 관심 → 주의 → 경계 → 심각' 5단계로 정하고 각 단계에 맞는 활동을 정리한 것이다.

표 1-5 사이버 위협 경보의 단계

단계	설명
정상 (그린)	위험도가 낮은 악성코드와 보안 취약점이 탐지되고 있는 상태다. 서버, 네트워크, 보안 장비의 보안 정책을 점검하여 위협요소를 차단하고 최신 보안 패치, 백신 업데이트를 유지하고 지속적으로 보안 모니터링 한다.
관심 (블루)	위험도가 높은 악성코드 및 보안 취약점이 출현하여 공격이 예상되는 상태다. 내부 구성원들에게 공지하여 상황을 전파하고 내부 시스템에 장애가 발생되지 않는 수준에서 포트 차단 및 해당 위협에 대한 점검 및 보안 패치를 수행한다.

단계	설명
주의 (노랑)	위험도가 높은 악성코드 및 보안 취약점으로 피해가 발생되는 상태다. 내부 구성원들에게 공지로 상황을 전파하고 내부 시스템에 장애가 발생되지 않는 수준에서 포트 차단 및 모든 시스템들의 보안 점검 및 보안 패치를 수행한다. 또한, 사이버 보안 관련 기관들에게 협조를 받아 위협제거 활동을 수행한다.
경계 (주황)	위험도가 높은 악성코드 및 보안 취약점으로 피해가 커져가는 상태다. 내부 구성원들에게 다양한 채널로 '경계' 단계를 전파하고 모든 정보 자산에 대해 지속적으로 점검을 실시하며 정보 자산을 최소화하여 운영한다.
심각 (빨강)	국가 및 다수의 국가 기관 등의 주요 정보 통신망에서 장애가 생긴 경우 심각 단계가 발령될 수 있다. 내부 구성원들에게 다양한 채널로 '심각' 단계를 전파하고 모든 정보 자산에 대해 점검하고, 감염된 시스템을 물리적으로 네트워크에서 분리하는 등 즉각적인 보안 조치를 취해야 한다.

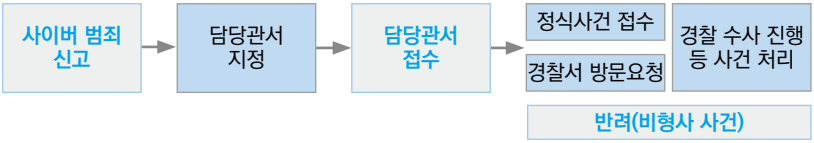
이 사이버 위협 경보 단계를 수행하기 위해서는 보안 전담 조직을 구성하여 보안 담당자 및 책임자를 지정하고 정기적으로 비상 연락망을 점검해야 한다. 또한, 관련 기관들과의 긴밀한 협조 체계를 갖추어 침해사고를 최소화할 수 있도록 노력해야 한다.

1.6.3 사이버 침해사고 대응 프로세스

사이버 침해사고가 발생되면 해당 사고에 대해 감추려고 애를 쓰지만 정보통신망법 및 개인정보보호법에 의해 처벌받을 수 있으므로 피해 유형에 따라 사건을 처리해야 한다.

국내에서는 국가 기관 및 공공기관에서 침해사고가 발생되는 경우 국가사이버안전센터에 침해사고 신고를 접수하여 절차에 따라 처리할 수 있으며 민간에서 침해사고가 발생되는 경우 한국인터넷진흥원(KISA), 인터넷침해대응센터(KR-CERT)에 신고 접수하여 침해사고 처리 지원을 받을 수 있다. 사이버 범죄와 같이 피해가 발생되어 조사가 필요하다면 경찰청 사이버 안전국 사이버 범죄 신고/상담을 통해 사고를 접수하여 절차에 따라 침해사고에 대한 처리와 피해가 발생된 부분에 대한 법적 조치를 할 수 있도록 한다.

그림 1-12 사이버 범죄 사건 처리 절차(경찰청 사이버 안전국)



개인정보를 취급하고 있다면 KISA 개인정보보호침해신고센터에 신고하여 사실 확인을 받고 법 위반 사실을 증명받도록 한다.

그림 1-13 개인정보 침해사고 대응 흐름도(KISA 개인정보침해신고센터)