정보통신분야
침해사고 대응 안내서

2025. 08.

과학기술정보통신부

KISA 한국인터넷진흥원

목 차

제1장 개요

제2장 침해사고 신고

제3장 침해사고 조치 가이드

부록

제1장
개요

제1장 개요

1. 배경

경제협력개발기구(OECD)가 발간한 디지털경제전망보고서2024에 따르면 우리나라는 OECD 국가 중 사물인터넷(IoT), 빅데이터, 인공지능(AI) 등 혁신 기술 분야에서 가장 빠른 도입률을 나타내며 세계적인 ICT 강국임을 입증했다.

또한 코로나19 이후 디지털 전환이 가속화되면서 2023년 우리나라 가구 인터넷 접속률은 99.9%, 인터넷 이용자 수는 94%, 모바일 인터넷 이용률은 93.5%로 모든 국민이 언제 어디서나 인터넷과 연결되는 초연결 시대로 진입했다.

이제 인터넷을 기반으로 한 정보통신은 선택이 아닌 우리 생활과 밀접한 생존에 직결되는 영역이며, 오늘날 국가경쟁력을 좌우하고 있다고 해도 과언이 아니다.

이와 같은 인터넷의 생활화와 함께 해킹, 악성코드, 서비스 거부(DDoS) 등침해사고의 공격 유형도 갈수록 지능화·고도화되고 있으며 매년 증가추세를 보이고 있다. 또한, 개인정보 침해, 산업기밀 유출, 사이버 범죄, 사이버 테러 등 사이버공간에 대한 위험은 다양해지고, 그에 따른 피해도 커지고 있다.

침해사고는 이제 특정 개인, 기업의 문제가 아닌 사회적, 국가적, 세계적 이슈가 되고 있다. 이처럼 인터넷 등 정보통신의 발달에 따른 생활의 편리함 등 순기능과 함께 해킹 등과 같은 역기능도 피할 수 없는 상황이다. 날로 증가하는 사이버 위협에 지속적으로 대비하고, 현재의 침해사고 예방 및 대응 수준을 더욱 높여 개인, 기업, 국가의 안전을 보장해야 할 것이다.

2. 목적 및 구성

본 안내서는 기업이나 개인 인터넷 이용자가 알아야 할 침해사고 예방 및 대응요령을 제공한다.

<제1장 개요>는 안내서의 이해를 돕기 위해 배경, 목적 및 구성을 설명하였다.

<제2장 침해사고 신고>는 첫 번째로 정보통신망법에 근거한 정보통신서비스 제공자, 기업의 정보보호담당자 등이 알아야 할 침해사고 신고의무를 설명하고, 두 번째로 개인정보보호법에 근거한 개인정보처리자가가 알아야 할 개인정보 유출 발생 시 신고 및 통지의무를 설명하였다.

<제3장 침해사고 조치 가이드> 부분에서는 구체적으로 침해사고 발생 시 대응절차, 사고 유형별 시스템 점검항목 및 조치 방안, 웹 서버 취약점 조치 방안, 네트워크 취약점 조치 방안, DB 취약점 조치 방안, 어플리케이션 취약점 조치 방안에 대한 정보를 제공하는데 주안점을 두었다.

부록에서는 인터넷 침해 관련 주요 용어를 별도로 수록하였다.

제2장

침해사고 신고

제2장 침해사고 신고

1. 침해사고 발생 시 신고

가. 침해사고 정의

정보통신망법 제2조 정의 규정에 따라, “침해사고”란 “해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법(나목)으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다”을 의미한다.

예를 들어 DDoS 공격에 의한 운영 서비스의 지연 또는 장애 발생, 해킹 공격 및 악성코드 감염에 의한 정보 유출, 시스템 파괴, 공격 경유지 악용, 홈페이지 위변조 등 피해가 발생한 모든 사고를 침해사고로 볼 수 있다.

나. 관련 법률

정보통신망법 제48조의3(침해사고의 신고 등) 및 동법 시행령 제58조의 2(침해사고 신고의 시기, 방법 및 절차 등)에 따라 정보통신서비스 제공자는 해킹, 악성코드, 서비스 거부(DDoS) 등의 사이버 공격으로 인한 침해사고 발생을 알게 된 때, 그 사실을 24시간 이내 과학기술정보통신부나 한국인터넷진흥원에 신고해야 한다.

<정보통신망법>
제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고해야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.
(생략)
③ 제1항 후단에 따라 침해사고의 통지 또는 신고를 받은 관계 기관의 장은 이와 관련된 정보를 과학기술정보통신부장관 또는 한국인터넷진흥원에 지체 없이 공유해야 한다.

<정보통신망법 시행령>
제58조의2(침해사고 신고의 시기, 방법 및 절차) ① 정보통신서비스 제공자는 법 제48조의3제1항 전단에 따라 침해사고를 신고하려는 경우에는 침해사고의 발생을 알게 된

때부터 24시간 이내에 다음 각 호의 사항을 과학기술정보통신부장관 또는 한국인터넷진흥원에 신고해야 한다.

1. 침해사고의 발생 일시, 원인 및 피해내용
2. 침해사고에 대한 조치사항 등 대응 현황
3. 침해사고 대응업무를 담당하는 부서 및 연락처

② 정보통신서비스 제공자는 제1항에 따라 신고한 후 침해사고에 관하여 추가로 확인되는 사실이 있는 경우에는 확인한 때부터 24시간 이내에 신고해야 한다.

③ 제1항 및 제2항에 따른 신고는 서면, 전자우편, 전화, 인터넷 홈페이지 입력 등의 방법으로 할 수 있다.

정보통신서비스 제공자가 이미 다른 법률*에 따른 침해사고 통지 또는 신고를 했다면, 침해사고 신고를 한 것으로 인정한다. 이 때, 해당 정보통신서비스 제공자의 침해사고를 신고 받은 관계기관은 즉시 과학기술정보통신부나 한국인터넷진흥원에 신고정보를 공유해야 한다.

침해사고 발생을 알게 된 때로부터 24시간을 초과하여 신고하거나 침해사고 사실을 알고도 과학기술정보통신부나 한국인터넷진흥원에 신고하지 않을 경우, 정보통신망법 위반으로 3천만원 이하의 과태료가 부과되므로 반드시 신고해야 한다.

<정보통신망법>

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

(생략)

6의6. 제48조의3제1항을 위반하여 침해사고의 신고를 하지 아니한 자

(생략)

다. 침해사고 신고 의무 대상

침해사고 신고 의무 대상은 정보통신서비스 제공자로 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

또한, 정보통신망법 제5조의2(국외행위에 대한 적용)에 근거하여 국내 시장 또는 이용자에게 영향을 미치는 경우, 해외법인의 정보통신서비스 제공자도 침해사고 신고 의무 대상에 해당된다.

라. 신고 시기 및 내용

정보통신서비스 제공자는 침해사고 발생을 알게 된 때, 그 사실을 24시간 이내 과학기술정보통신부나 한국인터넷진흥원에 신고해야 한다.

‘침해사고 발생을 알게 된 때’는 정보보호 담당자, 정보보호 담당부서의 장, 정보보호 최고책임자, 기업 대표자 등이 정보통신망법 제2조에 정의된 “침해사고”의 발생을 알게 된 때를 말한다.

정보통신서비스 제공자는 조직 규모나 업무 환경 등에 따라 침해사고 발생을 확인하는 절차, 침해사고 신고 및 초동대응 절차 등을 포함한 침해사고 대응체계를 수립하여야 한다. 그리고 침해사고를 확인하거나 대응조치 과정에서의 기록은 명확히 관리할 필요가 있다.

침해사고를 신고하려는 경우에는 다음 각 호의 사항 중 확인된 내용을 신고해야 한다. 이후, 침해사고에 관하여 추가로 확인되는 사실이 있는 경우에는 확인한 때부터 24시간 이내에 신고해야 한다.

<정보통신망법 시행령>
제58조의2(침해사고 신고의 시기, 방법 및 절차) ① (생략)
1. 침해사고의 발생 일시, 원인 및 피해내용
2. 침해사고에 대한 조치사항 등 대응 현황
3. 침해사고 대응업무를 담당하는 부서 및 연락처

정보통신서비스 제공자는 최초신고 이후 작성 오류나 사실확인 과정에서 잘못된 내용 등을 확인한 경우, 해당 부분을 정정하여 다시 신고해야 한다.

마. 신고 방법

침해사고 신고는 인터넷 홈페이지 입력, 전자우편, 전화, 서면 등의 방법으로 할 수 있다.

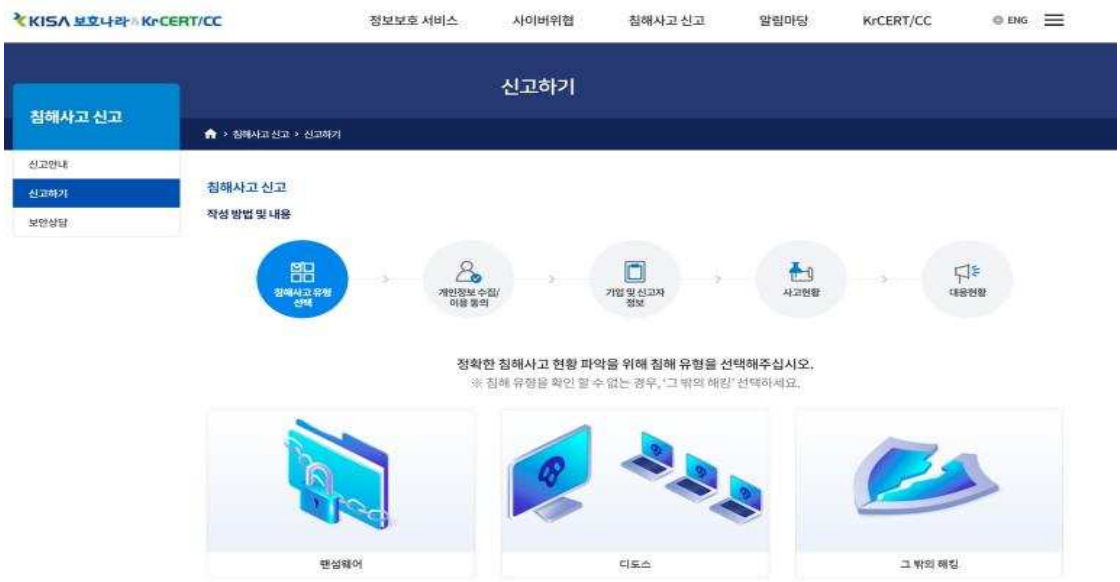
- **한국인터넷진흥원 보호나라&KrCERT 홈페이지 신고(http://www.boho.or.kr)**

① 보호나라&KrCERT 홈페이지에 접속하여, '침해사고 신고' → '신고하기' 메뉴를 클릭한다.

<그림 2-1> KISA 보호나라 & KrCERT 홈페이지 침해사고 신고 메뉴

② 침해사고 신고 메뉴에서 침해 유형(랜섬웨어, 디도스, 그 밖의 해킹)을 선택한다.

<그림 2-2> KISA 보호나라 & KrCERT 홈페이지 신고할 침해사고 유형 선택



③ 신고기업 및 신고자 정보를 입력한다. 단, 사업자 조회 시 기업정보 조회가 되지 않을 경우, 하단의 신고서 다운로드(한글, 워드)하여 침해사고 신고서를 작성한 후 전자우편(certgen@krcert.or.kr)으로 제출한다.

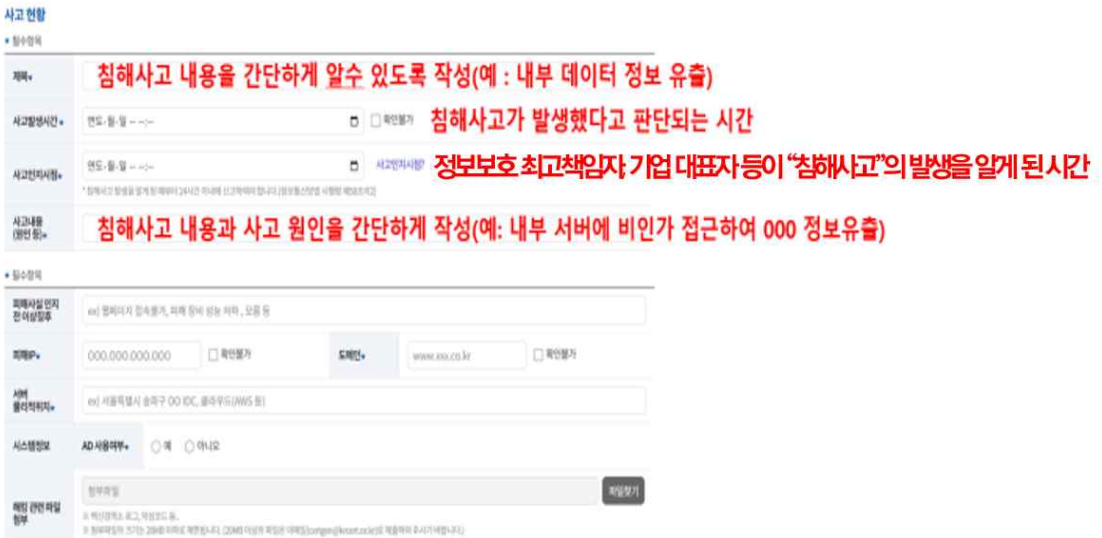
<그림 2-3> 사업자(신고기업) 정보 조회

④ 신고기업 및 신고 자 정보를 작성한 후 '다음' 버튼을 클릭한다. 이때, 침해사고 발생 원인 파악 및 재발방지를 위해 기술지원 서비스 동의 여부를 선택할 수 있다.

<그림 2-4> 침해사고 신고 기업 및 신고자 정보 입력(기술지원 여부 선택)

⑤ 침해사고 현황을 작성한 후 '다음' 버튼을 클릭한다.

<그림 2-5> 침해사고 신고 사고현황 입력



⑥ 침해사고 대응현황을 작성한 후 '제출하기' 버튼을 클릭한다.

<그림 2-6> 침해사고 신고 대응현황 입력

• 전자우편 신고(certgen@krcert.or.kr)

① 보호나라&KrCERT 홈페이지에 접속하여, '침해사고 신고' → '신고하기' → '침해사고 유형 선택' → 기업 및 신고자 정보 조회 메뉴에서 침해사고 신고서를 다운로드 한다.

<그림 2-7> 침해사고 신고서 다운로드

② 다운로드 받은 KISA 침해사고 신고서에 침해 유형(랜섬웨어, 디도스, 그 밖의 해킹)에 맞는 내용을 작성한 후 전자우편(certgen@krcert.or.kr)으로 제출한다.

<그림 2-8> KISA 침해사고 신고서 – 개인정보 수집 및 제공 동의 여부 확인

KISA 침해사고 신고서

과학기술정보통신부와 한국인터넷진흥원은 아래와 같이 『정보통신망 이용 촉진 및 정보보호 등에 관한 법률』(이하, 정보통신망법) 에 근거하여 민간분야 인터넷 침해사고 예방 및 대응 활동을 수행하고 있습니다.

☞ **제48조의3(침해사고의 신고 등):** 정보통신서비스 제공자의 침해사고 신고 접수

* 침해사고 신고는 동법 시행령 제58조의2(침해사고 신고의 시기, 방법 및 절차 등)에 근거하여 침해사고의 발생을 알게 된 때부터 24시간 이내에 신고
* 침해사고의 **발생을 알게 된 때부터 24시간 이후에 신고하거나** 신고를 아니할 시, 동법 제76조(과태료)에 근거하여 **3천만원 이하의** 과태료 부과

☞ **제48조의4(침해사고의 원인 분석 등):** 정보통신서비스 제공자의 침해사고 관련 자료 보전 및 제출 요구, 현장조사 등

* 침해사고 관련 자료 보전 명령을 위반할 시, 동법 제73조(벌칙)에 근거하여 2년 이하의 징역 또는 2천만원 이하의 벌금 부과
* 침해사고 관련 자료를 제출하지 아니하거나 거짓으로 제출할 시, 동법 제76조(과태료)에 근거하여 1천만원 이하의 과태료 부과

정보통신서비스 제공자는 침해사고 발생 즉시 정보통신망법 제48조의3(침해사고의 신고 등)에 따라 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 하며, 제48조의4(침해사고의 원인 분석 등)에 따라 피해확산 방지를 위하여 사고대응, 복구 및 재발방지에 필요한 조치를 하여야 합니다.

o 개인정보 수집·이용 동의(필수)

o 개인정보 수집 이용 목적: 침해사고의 사실 확인 및 원인분석, 대응체계 운영의 업무처리
o 수집하는 개인정보 항목: 신고자 이름, 메일, 연락처
o 수집 및 이용기간: 정보통신기반보호법 등 관련 법령에 따른 보유기간(5년)

* 개인정보 수집 이용에 동의하지 않을 수 있으나, 동의 거부 시 침해사고 신고 접수가 불가합니다.

☞ **개인정보 수집·이용에 동의하십니까?** ☐동의 ☐미동의

o 침해사고 신고 기업의 KISA 지원사업 안내를 위한 개인정보 제공 동의(선택)

o 개인정보 제공 목적 : 침해사고 신고 기업의 정보보호 수준 향상 등을 위한 KISA 지원사업 안내

구분	세부 내용	동의	미동의
ICT 중소기업 정보보호 지원	정보보호 컨설팅(정책, 인프라 취약점 점검 등) 및 컨설팅 기반 보안솔루션 지원과 클라우드 기반 보안 기능을 제공하는 SECaaS 지원 사업에 대한 안내	☐	☐
사이버 위협정보 분석공유 시스템(C-TAS)	사이버 위협정보 분석공유 시스템(C-TAS) 가입에 대한 안내	☐	☐

o 제공하는 개인정보 항목: 신고자 이름, 메일, 연락처
o 제공 및 이용기간: 이용 목적 달성(안내) 후 즉시 파기

* 개인정보 제공에 동의하지 않을 수 있으나, 동의 거부 시 KISA 지원 사업 안내가 불가합니다.

☞ **개인정보 제공에 동의하십니까?** ☐전체동의 ☐전체미동의

기타 문의사항은 인터넷침해대응센터 종합상황실(02-405-4911~6, certgen@krcert.or.kr)로 연락 주시기 바랍니다.

<그림 2-9> KISA 침해사고 신고서 – 랜섬웨어

☐ 랜섬웨어

· 필수항목

구 분		내 용
기업 및 신고자 정보	기업정보*	- 기업명 : - 사업자번호 : - 업종 : - 규모 : ☐ 대기업 ☐ 중견기업 ☐ 중소기업 ☐ 비영리 - 회사주소 :
	정보통신기반시설 대상여부*	☐ 예 (▫ 기반시설 내 침해사고 / ▫ 기반시설 외 침해사고) ☐ 아니오
	CISO 지정여부*	☐ 지정 ☐ 미지정
	신고자 정보*	- 이름 : - 메일 : - 연락처 : ※ 비상 연락이 가능한 번호를 기재해주십시오.
	기술지원 여부*	☐ 예 (▫ 침해사고 피해지원 서비스 / ▫ 침해사고 후속조치 지원) ☐ 아니오
사고현황	제목*	
	사고발생시간*	☐ OO년 OO월 OO일 OO시 OO분 ☐ 확인불가
	사고인지시점*	☐ OO년 OO월 OO일 OO시 OO분 ※ 침해사고 발생을 알게 된 때부터 24시간 이내에 신고하여야 합니다. (정보통신망법 시행령 제58조의2)
	피해내역*	☐ 단순 업무 장애 ☐ 주요 서비스 장애 ☐ 개인정보 유출 ☐ 기타(_____) ※ 예시 : 제조설비 가동 지연 등 - 서버 총 OO대 중 OO대 - PC 총 OO대 중 OO대
	사고내용(원인 등)*	(자유롭게 작성) ※ 예시 : 출처 불명의 이메일 열람, 의심스러운 사이트 접속, 계정유출로 인한 내부 서버 침투, 확인불가 등
	암호화파일 확장자명*	※ 예시 : '.makop', '.UWTJF', '.locked', 모름 등
	협박유무*	☐ 있음 ☐ 없음 - 해커 요구금액 : _____(원화, 코인, 달러 등) - 예상 피해금액 : _____(원화, 코인, 달러 등)
	피해사실 인지 전 이상징후	※ 예시 : 웹페이지 접속 불가, 피해 장비 성능 저하, 모름 등
	랜섬웨어 종류	※ 예시 : Makop, Conti, Hive, Ragnar, Darkside, 모름 등
	AD 사용여부*	☐ 사용 ☐ 미사용
	피해 IP*	☐ OOO.OOO.OOO.OOO ☐ 확인불가
	피해 도메인*	☐ www.xxx.co.kr ☐ 확인불가
	서버 물리적 위치*	※ 예시 : 서울특별시 송파구 OO IDC, 전라남도 나주시 등 또는 클라우드(AWS 등)
	※ 랜섬노트, 백신 검역소 로그, 악성코드 등 침해사고 관련 파일을 신고서와 함께 보내주십시오. ※ 대응현황 자료, 내부보고자료, 증상(화면 캡처 등)	
대응현황	백업유무*	☐ 전체 백업 ☐ 일부 백업 ☐ 백업이 있으나 감염 ☐ 백업 없음 ☐ 기타
	조치사항*	① (자유롭게 작성) ② ※ 예시 : 피해 대상 네트워크 분리, 복구업체를 통한 복구시도 중
	경찰 신고여부*	☐ 예 ☐ 아니오

※ 침해사고 피해지원서비스 : 침해사고 발생 원인 및 침투경로를 분석하여 원인분석 보고서 및 향후 대응방안에 대해 안내

※ 침해사고 후속조치 지원 : 침해사고 피해지원서비스에서 안내한 대응방안의 조치여부를 확인하고 보안강화에 대한 지원을 제공

<그림 2-10> KISA 침해사고 신고서 – 디도스

□ 디도스

· 필수항목

구 분		내 용
기업 및 신고자 정보	기업정보*	- 기업명 : - 사업자번호 : - 업종 : - 규모 : □ 대기업 □ 중견기업 □ 중소기업 □ 비영리 - 회사주소 :
	정보통신기반시설 대상여부*	□ 예 (▫기반시설 내 침해사고 / ▫ 기반시설 외 침해사고) □ 아니오
	CISO 지정여부*	□ 지정 □ 미지정
	신고자 정보*	- 이름 : - 메일 : - 연락처 : *※ 비상 연락이 가능한 번호를 기재해주십시오.*
사고현황	제목*	
	사고발생시간*	□ OO년 OO월 OO일 OO시 OO분 ~ OO시 OO분 □ 현재 지속중 *※ 발생시간 추가 가능*
	공격대상 서버 종류*	*※ 예시 : Apache, Nginx, Microsoft IIS, 기타*
	서비스 장애 유무*	□ 장애가 있었으나 정상화 □ 있음 □ 없음
	공격규모*	- 속도(Mbps) : 약 OOMbps □ 확인불가 - 속도(pps) : 약 OOpps □ 확인불가
	협박유무*	□ 있음 □ 없음
	피해사실 인지 전 이상징후	*※ 예시 : 웹페이지 접속 불가, 피해 장비 성능 저하, 모름 등*
	피해 IP*	□ OOO.OOO.OOO.OOO □ 확인불가
	피해 도메인*	□ www.xxx.co.kr □ 확인불가
	서버 물리적 위치*	*※ 예시 : 서울특별시 송파구 OO IDC, 전라남도 나주시 등 또는 클라우드(AWS 등)*
	서버임대회선 통신사·대역폭	*※ 예시 : xx파워콤, xx브로드밴드, xx호스팅 등*
	공격IP	□ OOO.OOO.OOO.OOO □ 확인불가
	운영체제	□ Win10 □ Win8 □ Win7 □ Win VISTA □ Win Server □ Unix □ Linux □ 기타( )
	웹서버	□ Apache □ Nginx □ Microsoft IIS □ 기타( )
	DB종류	□ MySQL □ Oracle □ MongoDB □ 기타( )
	AD 사용여부	□ 사용 □ 미사용
	※ 백신 검역소 로그, 악성코드 등 침해사고 관련 파일을 신고서와 함께 보내주십시오. ※ 대응현황 자료, 내부보고자료, 증상(화면 캡처 등)	
대응현황	조치사항*	① *(자유롭게 작성)* ② *※ 예시 : KISA 사이버대피소 입주, DDoS 장비를 통한 공격트래픽 차단*
	경찰 신고여부*	□ 예 □ 아니오

<그림 2-11> KISA 침해사고 신고서 – 그 밖의 해킹

□ 그 밖의 해킹

· 필수항목

구 분		내 용
기업 및 신고자 정보	기업정보*	- 기업명 : - 사업자번호 : - 업종 : - 규모 : □ 대기업 □ 중견기업 □ 중소기업 □ 비영리 - 회사주소 :
	정보통신기반시설 대상여부*	□ 예 (▫ 기반시설 내 침해사고 / ▫ 기반시설 외 침해사고) □ 아니오
	CISO 지정여부*	□ 지정 □ 미지정
	신고자 정보*	- 이름 : - 메일 : - 연락처 : ※ 비상 연락이 가능한 번호를 기재해주십시오.
	기술지원 여부*	□ 예 (▫ 침해사고 피해지원 서비스 / ▫ 침해사고 후속조치 지원) □ 아니오
사고현황	제목*	
	사고발생시간*	□ OO년 OO월 OO일 OO시 OO분 □ 확인불가
	사고 인지시점*	□ OO년 OO월 OO일 OO시 OO분 ※ 침해사고 발생을 알게 된 때부터 **24시간 이내에 신고**하여야 합니다(정보통신망법 시행령 제58조의2)
	사고내용(원인 등)*	*(자유롭게 작성)* ※ 예시 : 직원 사칭메일 발송, 해킹경유지로 악용, 기업서버에서 특정 포트로 비인가된 접근 시도
	피해사실 인지 전 이상징후	※ 예시 : 웹페이지 접속 불가, 피해 장비 성능 저하, 오류 등
	AD 사용여부*	□ 사용 □ 미사용
	피해 IP*	□ OOO.OOO.OOO.OOO □ 확인불가
	피해 도메인*	□ www.xxx.co.kr □ 확인불가
	서버 물리적 위치*	※ 예시 : 서울특별시 송파구 OO IDC, 전라남도 나주시 등 또는 클라우드(AWS 등)
	※ 백신 검역소 로그, 악성코드 등 침해사고 관련 파일을 신고서와 함께 보내주십시오. ※ 대응현황 자료, 내부보고자료, 증상(화면 캡처 등)	
대응현황	조치사항*	① *(자유롭게 작성)* ② ※ 예시 : 피해 대상 네트워크 분리, 복구업체를 통한 복구시도 중
	경찰 신고여부*	□ 예 □ 아니오

• **전화 신고(☎118 또는 02-405-4911 ~ 4914)**

① 아래 정보를 포함한 침해사고와 관련된 내용을 유선으로 신고한다.

1. 기업 정보(기업명, 업종 등) 및 신고자 정보(이름, 연락처)
2. 침해사고의 발생 일시, 원인 및 피해내용(사고 인지시점 포함)
3. 침해사고에 대한 조치사항 등 대응 현황
4. 침해사고 대응업무를 담당하는 부서 및 연락처

• **서면 신고(수신 주소 : 서울특별시 송파구 중대로 135 IT벤처타워 서관 5층 종합상황실)**

① 침해사고 신고서에 침해 유형(랜섬웨어, 디도스, 그 밖의 해킹)에 맞는 내용을 작성한 후 수신 주소로 등기 우편을 발송한다.

바. 추가 신고

정보통신망법 시행령 제58조의2(침해사고 신고의 시기, 방법 및 절차 등)에 따라, 신고 후 추가로 확인되는 사실이 있는 경우에는 확인한 때부터 24시간 이내 신고해야 한다.

※ 추가신고 방법은 '마. 신고 방법'와 동일하며, 추가로 확인된 사실에 대해 기재

• **한국인터넷진흥원 보호나라&KrCERT 홈페이지 신고(http://www.boho.or.kr)**
• **전자우편 신고(certgen@krcert.or.kr)**
• **전화 신고(☎118 또는 02-405-4911 ~ 4916)**
• **서면 신고(수신 주소 : 서울특별시 송파구 중대로 135 IT벤처타워 서관 5층 종합상황실)**

2. 개인정보 유출 발생 시 신고 및 통지

가. 관련 법률

개인정보처리자는 개인정보가 분실·도난·유출(이하 유출 등)되었음을 알게 되었을 때에는 개인정보보호위원회 또는 한국인터넷진흥원에 신고하여야 하며, 지체 없이 해당 정보주체에게 통지해야 한다.

※ '개인정보 유출 등'이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자 그 내용을 알 수 있는 상태에 이르게 된 것을 의미(표준 개인정보 보호지침 제25조)

개인정보 보호법 제34조(개인정보 유출 등의 통지·신고) ①개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등의 사항을 지체 없이 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.

개인정보 유출 등의 신고 또는 통지를 72시간 이내 하지 않을 경우 3천만 원 이하의 과태료가 부과될 수 있다.

<개인정보 보호법>

제75조(과태료) ②다음 각호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

17. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
18. 제34조제3항을 위반하여 보호위원회 또는 한국인터넷진흥원에 신고하지 아니한 자

나. 통지 절차

개인정보처리자는 개인정보 유출 등을 알게 되었을 때로부터 72시간 이내 해당 정보주체에게 개인정보 유출 등의 사실을 개별 통지해야 한다.

구분	내용
통지 주체	개인정보처리자
통지 기준	1명 이상
통지 내용	1. 유출 등이 된 개인정보의 항목과 규모 2. 유출 등이 된 시점과 경위 3. 정보주체가 취할 수 있는 피해 최소화 조치 4. 개인정보처리자 대응조치 및 피해 구제 절차 5. 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처
통지 시점	개인정보의 유출 등 사실을 알게 되었을 때로부터 72시간 이내
통지 방법	서면 등의 방법을 통한 개별 통지가 원칙 ※ 다만 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우, 인터넷 홈페이지에 30일 이상 게시 ※ 대규모 유출 등으로 72시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 통해 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출 등 사실을 게시를 하고 나서 추가적으로 해당 정보주체에게 개별적으로 통지

다. 신고 절차

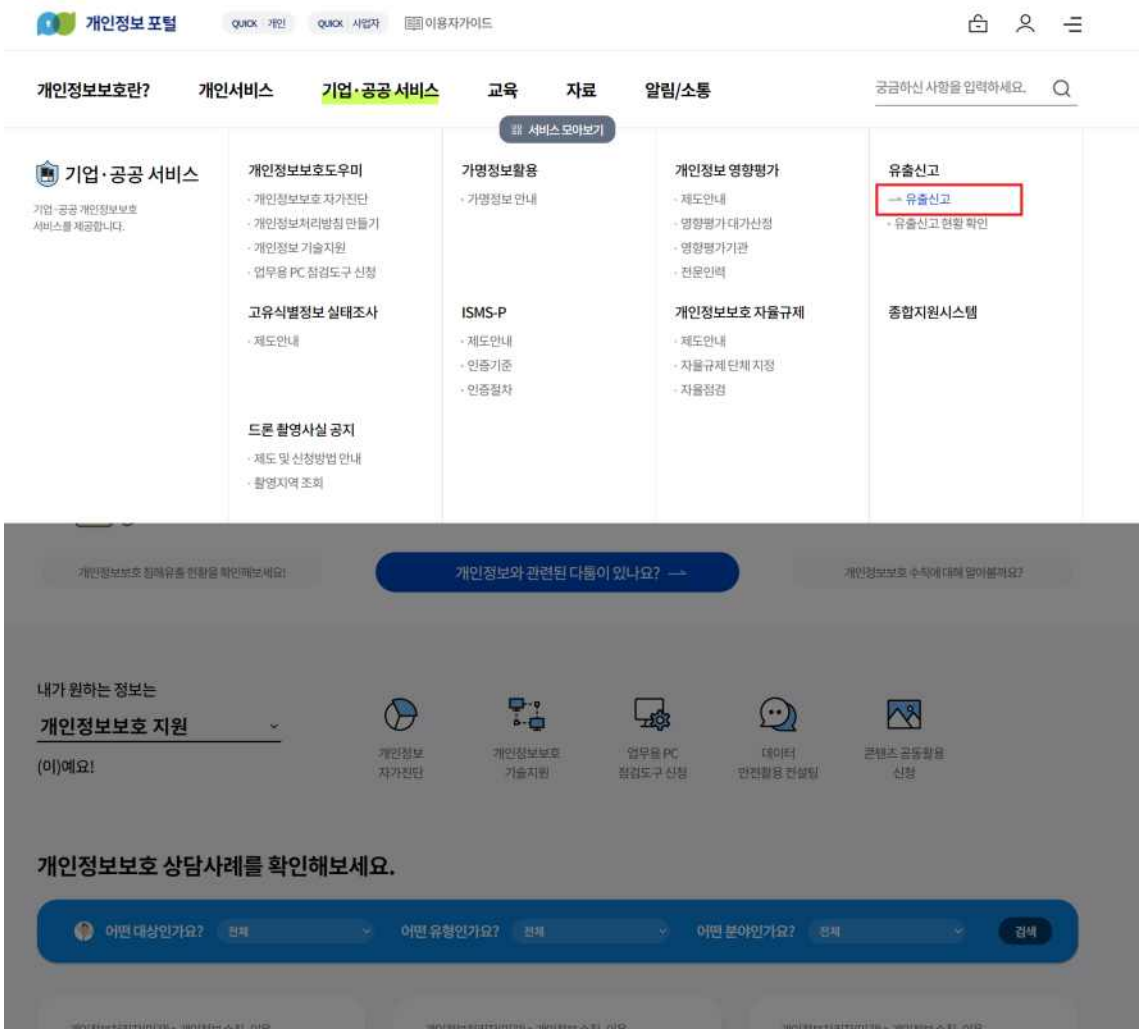
개인정보처리자는 개인정보 유출 등을 알게 되었을 때로부터 72시간 이내 개인정보 포털 홈페이지를 통해 신고해야 한다.

· 개인정보 포털 : https://www.privacy.go.kr

구분	내용
신고기준	※ 아래 어느 하나에 해당하는 경우에 신고하여야 함 - 1천명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우 - 민감정보 또는 고유식별정보가 유출 등이 된 경우 - 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우
신고내용	1. 정보주체에의 통지 여부 2. 유출 등이 된 개인정보의 항목과 규모 3. 유출 등이 된 시점과 경위 4. 유출 등에 따른 피해 최소화 대책·조치 및 결과 5. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차 6. 담당부서·담당자 및 연락처
신고기한	개인정보의 유출 등 사실을 알게 되었을 때로부터 72시간 이내
신고 유의사항	유출사고의 원인 분석을 위해 관련 자료의 보존 · PC : 네트워크 분리 후 전원 차단, 디스크 분리 후 별도 보관 · 일반서버 : dd명령어를 사용한 디스크 백업 수행 · 가상 서버 : 스냅샷 생성 및 가상디스크 파일 형태 보존 · 모니터링 및 보안장비 등 : 생성로그 등 관련자료 일체의 별도 백업 수행 · 악성코드 격리 보존(암호압축 보관)

① 개인정보 포털 사이트에 접속하여 '기업·공공 서비스' → '유출신고' 메뉴를 클릭한다.

<그림 2-7> 개인정보 포털 신고 메뉴



② 신고 양식에 따라 내용을 작성한 후 ‘신고하기’를 클릭한다.

<그림 2-8> 신고 양식

라. 침해사고에 대한 수사 의뢰

해킹, 인터넷을 이용한 사기, 주민등록번호의 도용 등 침해 행위에 대하여 침해 행위자에 대한 수사 등 법적인 처리를 고려하는 경우에는 경찰청 사이버안전지킴이에 신고하여 지원을 받을 수 있다.

· 경찰청 사이버안전지킴이 사이버범죄 신고시스템 : http://ecrm.police.go.kr,
☎ (국번없이) 182

<그림 2-9> 경찰청 사이버안전지킴이 사이버범죄 신고시스템(ECRM) 침해사고 신고

제3장
침해사고 조치 가이드

제3장 침해사고 조치 가이드

1. 침해사고 유형

가. 침해사고 정의

- **정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 1항 7호**
  - '침해사고'란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

나. 침해사고 대응 7단계

특히, 침해사고가 발생하거나 인지한 경우, 정보통신망법에 의거하여 그 사실을 즉시(24시간 이내) 과학기술정보통신부나 한국인터넷진흥원에 신고해야 한다. 신고 대상 및 절차 등 세부 내용은 '제2장 침해사고 신고' 부분을 참고하도록 한다.

2. 침해사고 점검항목 및 조치방안(개인)

가. 점검항목

- **금융관련 홈페이지 방문 시 전체 보안카드 입력 안내 발생**
  - 금융관련 홈페이지에서는 보안카드의 전체 번호를 요구하는 경우가 없으므로, 해당 페이지가 나타날 경우, PC에 악성코드 감염 등을 의심

- **포털사이트 및 메일 서비스 로그인시 해킹의심 알람 수신**
  - 포털 서비스로부터 해킹의심 주의 알람을 받을 경우, 키로그 등을 수행하는 악성코드 감염을 통한 계정정보가 탈취 등을 의심

- **컴퓨터 및 인터넷 속도가 특별한 이유 없이 급감**
  - 평소보다 컴퓨터 자원(CPU, 메모리)사용량이 급증하거나, 인터넷 속도가 급감할 경우 비트코인 채굴이나 DDoS 기능을 수행하는 악성코드 감염 의심

나. 조치방안

- **정품 소프트웨어 사용**
  - 신뢰할 수 없는 경로에서 획득한 운영체제, 유틸리티, 정품 소프트웨어 인증우회 프로그램 등을 설치하지 않는다.

- **운영체제 및 기타 소프트웨어에 대한 최신 패치 적용**
  - 운영체제 및 기타 소프트웨어 대한 자동 보안패치 기능을 사용한다.
  - 자동 보안패치를 지원하지 않는 소프트웨어의 경우, 주기적으로 최신 버전을 확인하여 수동패치를 수행한다

- **백신 소프트웨어 설치**
  - 한 개 이상의 백신 소프트웨어를 설치하여 실시간 감시 수행 및 정기적인 전체 검사를 수행한다

- **신뢰할 수 있는 페이지 방문**
  - 공격자는 취약점을 공격하는 코드를 사용하여 웹 페이지 단순방문 만으로도 악성코드를 감염시킬 수 있으므로 신뢰할 수 없는 웹페이지 접속 자제, 파일 다운로드 및 실행을 하지 않는다
  - 신뢰할 수 없는 발송자가 전송한 이메일은 열람하지 않는다.

• **중요 데이터 백업 수행**

- 랜섬웨어 등과 같은 자료 파괴형 악성코드 피해를 대비하기 위해, 중요 데이터의 경우 주기적으로 PC와 분리된 별도의 저장매체(외장하드 등) 또는 클라우드 서비스를 통해 데이터 백업을 수행한다.

• **인터넷 공유기 관리자 기본 패스워드 변경 및 WIFI 비밀번호 설정**

- 인터넷 공유기의 관리자 기본 패스워드를 변경하지 않을 경우, 공격자는 동일한 기본 패스워드를 사용하여 인터넷 공유기를 해킹할 수 있으므로 관리자 및 WIFI 비밀번호 변경을 수행한다.
- 공격자는 취약점을 악용하여 인터넷 공유기 해킹이 가능하므로, 최신 펌웨어 패치 수행한다.

• **회원가입 사이트 마다 별개 아이디 · 패스워드 사용**

- 아이디, 패스워드를 여러 홈페이지 대상으로 동일하게 사용하게 되면 계정 정보가 유출될 경우, 피해가 확산될 수 있으므로 사용하는 홈페이지마다 별개의 인증정보를 설정하여 사용한다.

3. 침해사고 점검항목 및 조치방안(기업)

가. 한국인터넷진흥원에 분석을 요청할 경우 유의 사항

- 침해사고 관련 파일(악성코드, 프로세스)등을 제거하지 않은 상태에서 분석요청
- 불가피하게 제거해야 할 경우 악성파일은 경로와 MAC time(생성 • 접근 • 수정 시간)을 확보하고, 프로세스는 해당 프로세스와 관련된 디렉토리 또는 파일 경로와 MAC time을 확보해야 함(악성파일 백업 필수)

  ※ 리눅스의 경우 stat 명령문과 lsot 명령문 활용

사고 유형 >> 공통

점검내용	조치사항
계정 • 사용하지 않는 계정 및 숨겨진 계정 확인 ▶ Window : [관리도구] → [컴퓨터 관리] → [로컬사용자 및 그룹] → [사용자] 정보 확인 ▶ Linux : /etc/passwd 확인 --- • $ 문자가 포함된 계정 확인 • 패스워드 미설정 계정 확인 • /bin/bash 점검	• 사용하지 않는 계정과 숨겨진 계정 삭제
로그파일 • 사용하지 않는 계정 및 숨겨진 계정 확인 ▶ Window : [관리도구]→[컴퓨터 관리]→[이벤트뷰어] 확인 ▶ Linux : /var/log/secure, message 등 확인 • 웹로그 경로 및 변조 유무 확인 ▶ [관리도구] > 인터넷정보서비스(IIS)에서 관리에서 • 웹로그 경로 확인 ▶ Linux : /usr/local/apache/logs 확인 --- • 웹로그 생성/수정 시간 확인	
웹셸 • 사용하지 않는 계정 및 숨겨진 계정 확인 ▶ Window : [관리도구]→[컴퓨터 관리]→[이벤트뷰어] 확인	• 웹셸 발견 시 업로드 된 경로를 파악하여 해당 취약점 제거
백도어 • 네트워크 상태확인 ▶ map-sw 서버IP (원격에서 실행) • 비정상 포트 및 외부연결 확인 ▶ Window : netstat, TCPView 등 사용 ▶ Linux : netstat –nip, lsof –I --- • 의심 Port 확인 • 의심 Port를 사용하는 프로세스 확인	• 백도어 포트가 발견될 경우 해당 port에 대한 차단 정책을 적용하고 백도어 서비스와 관련된 파일을 확인하여 삭제(차단 정책 적용을 위해 서버내 방화벽 iptables, hosts, allow/deny 활용 가능)
루트킷 • 숨겨진 프로세스 및 비정상 프로세스 확인 • 변조된 파일 및 시스템 명령어 확인 ▶ Window : IceSword, GMER 등 사용 ▶ Linux : Rootkit Hunter, Check RootKit 등 사용 --- • RootKit Hunter 업데이트 필수 ▶ rkhunter-update	• 루트킷의 경우 일부 시스템 명령어만 변조된 경우는 무결성이 보장된 명령어로 교체 가능하나 다수의 라이브러리들이 변조되었을 경우는 시스템 재설치 필요

사고 유형 >> 웹변조

점검내용

웹페이지 확인

- 공통 : index.html,main.html,default.html,index.pho,main.pho
- Window : index, asp, main, asp, default, asp

- 기타 메인페이지로 설정된 파일 확인

HTTP 메소드

- Windows : WebDAV 활성화 확인
  ▶ [관리도구] → [인터넷정보서비스(IIS)관리] → [웹서비스 확장] 허용 여부 확인
- Linux : Apache 웹서버의 httpd, Conf 확인
- 웹로그 경로 및 변조 유무 확인
  ▶ <Directory/>에서 MOME, PUT 메소드 allow 설정 여부 확인

- Windows : [사용금지]로 설정 • Linux : deny로 설정

웹로그 분석

- MOME, PUT 메소드 공격 여부 확인
  ▶ grep MOME 웹로그 : grep –v 404

- Linux : grep 기본 제공 • Window : grep.exe 사용

조치사항

- 웹페이지 내용이 변경되었을 경우 웹셸 감염여부를 확인하고 발견될 경우 삭제 조치
- 리눅스 아파치 웹 서버의 설정 파일에서 사용하지 않는 HTTP 메소드에 대해 허용 금지
- IS 웹서버 또는 아파치 웹서버의 설정이 변경되었을 경우 관리자 계정 변경 필수
- 웹셸이 발견될 경우 웹 접속로그를 통해 웹셸에 접근한 IP를 확인하고 방화벽을 통해 접근 제한 정책 적용

사고 유형 >> 악성코드 경유지/유포지

점검내용

웹페이지 확인

- 사용하지 않는 계정 및 숨겨진 계정 확인
- 악성코드 유포 URL 삽입 페이지 검출
  ▶ grep -r "유포지 URL" 웹페이지 Path
- 웹페이지 생성 및 수정 시간 확인

접속 IP 확인

- 악성코드 유포/경유 페이지 접속 IP 추출
  ▶ grep "유포/경유 페이지 Path" 웹로그 Path
  ※ 추출된 IP는 악성코드에 감염된 좀비PC를 확보하는데 매우 중요

조치사항

- 악성코드 유포 페이지에 대한 파일 생성 및 수정시간 확인
- 유포 페이지 생성 시점 기준으로 웹 접속로그 및 시스템 로그를 분석하여 또 다른 침해 여부 확인
- 웹셸이 발견될 경우 웹접속로그를 통해 웹셸에 접근한 ip를 확인하고 방화벽을 통해 접근 제한 정책 적용

사고 유형 >> 봇넷 C&C

점검내용

네트워크 연결

- 외부 네트워크 연결 확인
  - ▶ Windows : - netstat –na를 통해 확인 후 의심 Port에 연결된 IP를 확인
  - ▶ Linux : -netstat –na 또는 lsof –i -Window와 동일하게 확인
- 네트워크 트래픽 분석
  - ▶ Windows : Wireshark를 사용하여 패킷 분석
  - ▶ Linux :TCPDUMP를 사용하여 패킷 분석

조치사항

- 외부 네트워크와 연결된 백도어 포트 발견시 방화벽을 통해 해당 포트 접근 제한 정책 적용
- 백도어 포트 서비스를 실행중인 파일 확인 및 삭제

사고 유형 >> 해킹 경유지

점검내용

네트워크

- 공통 : Nmap, netstat 사용하여 의심 Port 확인
  - ▶ nmap –sV 서버IP ▶ 의심 Port 확인
- Windows : RRAS 서비스 설정 확인
  - ▶ [컴퓨터 관리] → [서비스 및 응용프로그램] → [서비스]의 Routing and Remote Access 서비스 시작 유형(사용안함) 확인
- Linux : PPTP 서비스 실행 확인
  - ▶ ps –ef 명령 실행 후 pptpd 프로세스 확인
  - ※ RRAS 및 PPTP 프로세스는 VPN 서비스

네트워크

- Windows : CCProxy, RealVNC 등 설치 확인
  - ▶ [제어판] → [프로그램 추가/제거] 에서 설치 여부 확인
- Linux : Rootkit Hunter, Check RootKit 검사를 통해 악성 프로그램 설치 여부 확인
- Rootkit Hunter 업데이트 필수 ▶ rkhunter –update

조치사항

- 윈도우 서버의 RRAS 서비스가 실행중일 경우 해당 서비스 중지
- 윈도우 서버의 이벤트 로그를 통해 RRAS서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용
- 리눅스 서버의 PPTP 서비스가 실행중일 경우 해당 프로세스 중지
- 리눅스 서버의 시스템 로그를 통해 PPTP 서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용

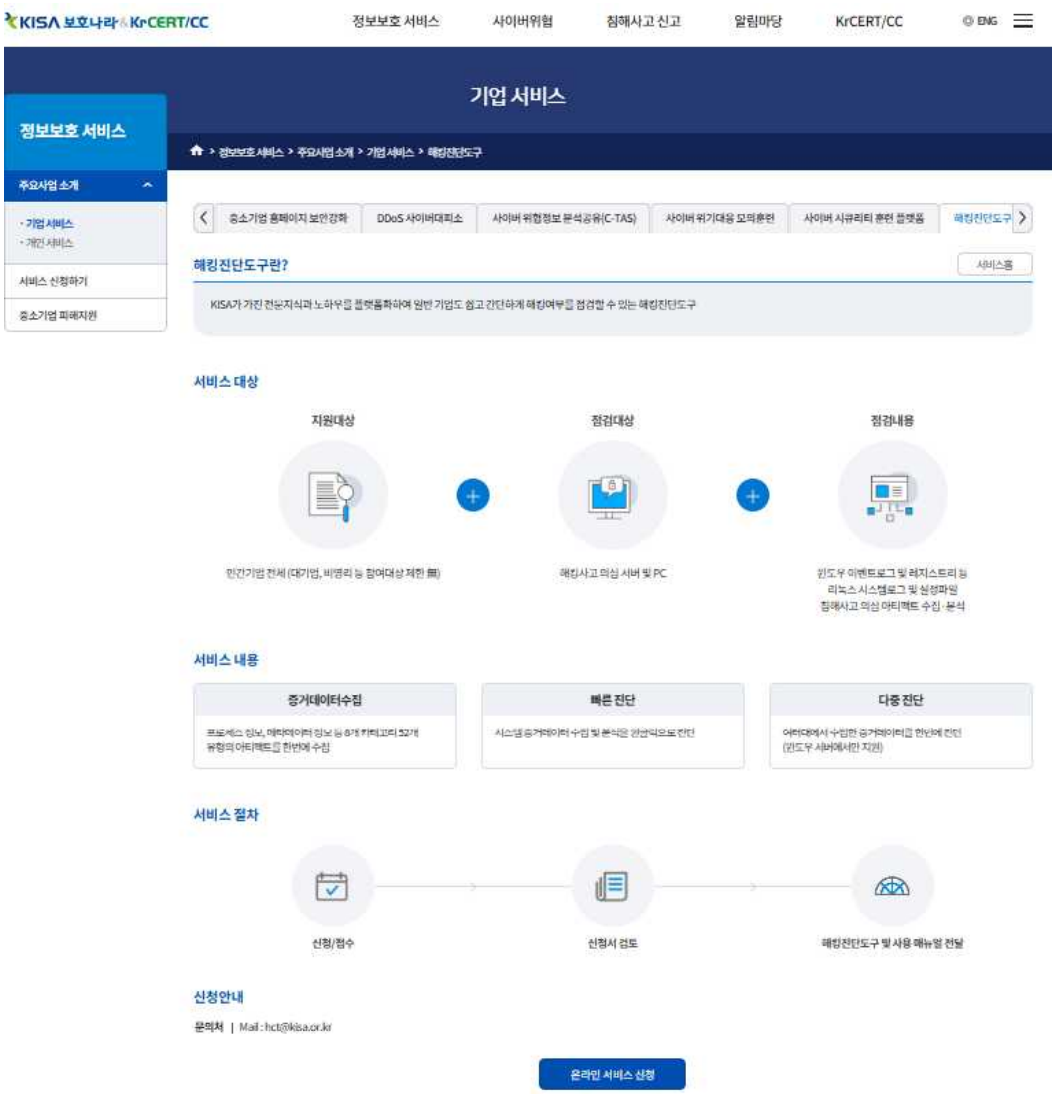

사고 유형 >> DDoS
점검내용
네트워크 연결
• 홈페이지 접속 상태 및 응답 지연시간 확인
▶ ping "홈페이지주소"
• 시스템에 접속한 IP를 확인하여 트래픽 이상 징후 확인
▶ Windows : netstat -na
▶ Linux : netstat –na 또는 lsof -I
• 네트워크 트래픽 분석
▶ Window : Wireshark를 사용하여 패킷 분석
▶ Linux : TCPDump를 사용하여 패킷 분석
조치사항
• KISA 사이버 대피소 또는 ISP에서 운영중인 DDoS 방어서비스 적용 신청
• 보안장비를 통해 DDoS를 유발하는 IP에 대한 접근차단
※ ISP를 통해 공격 로그 제공 요청

4. 시스템 유형별 보안 조치방안

가. 웹 서버 취약점 조치 방안

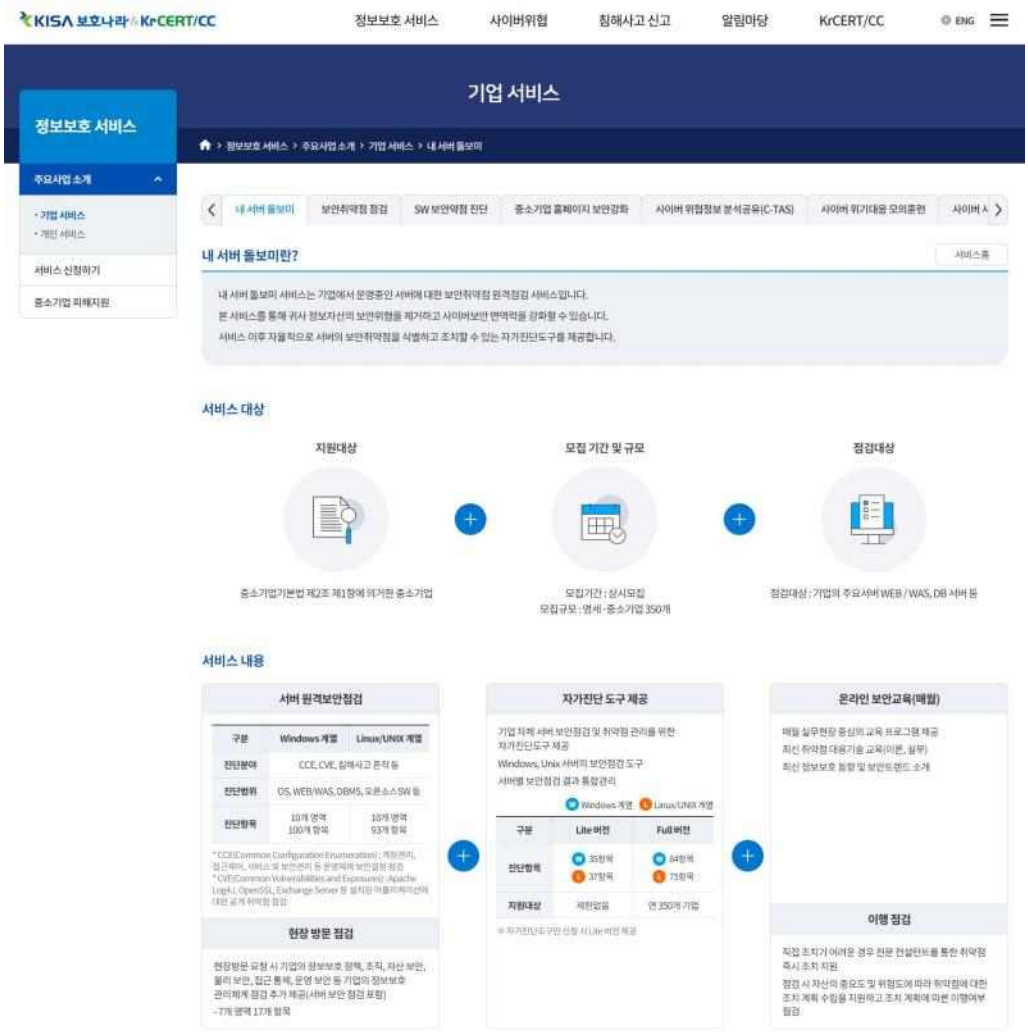
• 해킹진단도구 서비스 수행(http://www.boho.or.kr)

- 기업에서 운영 중인 서버(윈도우, 리눅스)의 해킹여부를 점검, 결과 제공



• 내 서버 돌보미 서비스 수행(http://www.boho.or.kr)

- 기업에서 운영 중인 서버에 대한 보안 취약점 원격 점검, 점검 결과 제공



• OS에 대한 최신 패치 적용

- OS 벤더사이트나 보안 취약점 정보 사이트를 주기적으로 방문하여 현재 사용하고 있는 OS에 대한 최신 취약점 정보획득 및 패치

- 정기적으로 취약점 점검 도구와 보안 체크리스트를 사용하여 호스트 OS의 보안 취약 점검

• 웹 서버 전용 호스트로 구성

- 웹 서비스 운영에 필요한 최소한의 프로그램들만 남겨두고 불필요한 서비스들은 반드시 제거

- 시스템 사용을 목적으로 하는 일반 사용자 계정은 모두 삭제하거나 최소한의 권한만 할당

- 오직 관리자만이 로그인 가능하도록 설정

• **서버에 대한 접근 제어**

- 관리목적의 웹 서버 접근은 콘솔 접근만을 허용
- 위 사항이 불가능할 경우 관리자가 사용하는 PC의 IP만 접근이 가능하도록 접근제어 수행

• **DMZ 영역에 위치**

- 웹 서버를 방화벽에 의해서 보호 받도록 하고, 웹 서버가 침해당하더라도 웹 서버를 경유해서 내부 네트워크로의 침입은 불가능하도록 구성

• **강력한 관리자 계정 패스워드 사용**

- 관리자 계정 패스워드는 유추가 불가능하고 패스워드 크랙으로도 쉽게 알아낼 수 없는 강력한 패스워드 사용
- 문자, 숫자, 특수문자, 기호 2종류 및 8자리 이상으로 구성하거나 10자리 이상의 문자열로 구성
- 사전에 없는 단어를 사용하고 기호를 최소 한 개 이상 포함

• **파일 접근권한 설정**

- 관리자 계정이 아닌 일반 사용자 계정으로 관리자 계정이 사용하는 파일들을 변경할 수 없도록 구성

• **웹 프로세스의 권한 제한**

- 시스템 전체적인 관점에서 웹 프로세스가 웹 서비스 운영에 필요한 최소한의 권한만을 갖도록 제한
- 웹 서버 관리시에는 일반적으로 사용되는 nobody 권한으로 웹 프로세스가 동작하도록 구성

• **로그 파일의 보호**

- 침입 혹은 침입시도 등 보안 문제점 파악을 위해 로그 파일이 노출, 변조 혹은 삭제되지 않도록 불필요한 접근으로부터 보호
- 불필요한 접근으로부터 보호하기 위해 로그파일을 별도의 서버에 백업하여 관리하는 것이 필요
- 로그파일은 최소 6개월 이상의 로그를 확보하는 것이 필요

• **웹 서비스 영역의 분리**

- 웹 서비스 영역과 시스템(OS)영역을 분리시켜서 웹 서비스의 침해가 시스템 영역으로 확장될 가능성을 최소화
- 웹 서버의 루트 디렉토리와 OS의 루트 디렉토리를 다르게 지정

• **설정파일 백업**

- 초기 설정 파일을 백업 받아서 보관해 두고, 변경이 있을 때마다 설정 파일을 백업함으로써 해킹사고 발생 시 빠르게 복구

• **Inbound 트래픽 제한**

- 공개용 침입차단시스템을 이용하여 트래픽을 제한

※ 리눅스 커널에서는 iptables 또는 ipchains 침입차단 시스템이 기본으로 제공됨

- 전체 서비스(포트)에 대해 차단 설정 후 고객이 필요로 하는 서비스(포트)에 대해 선별적으로 접속 제한을 해제

※ 필요 서비스(포트) 예 : FTP(21), SSH(22), SMTP(25), DNS(53), SSL(443)등

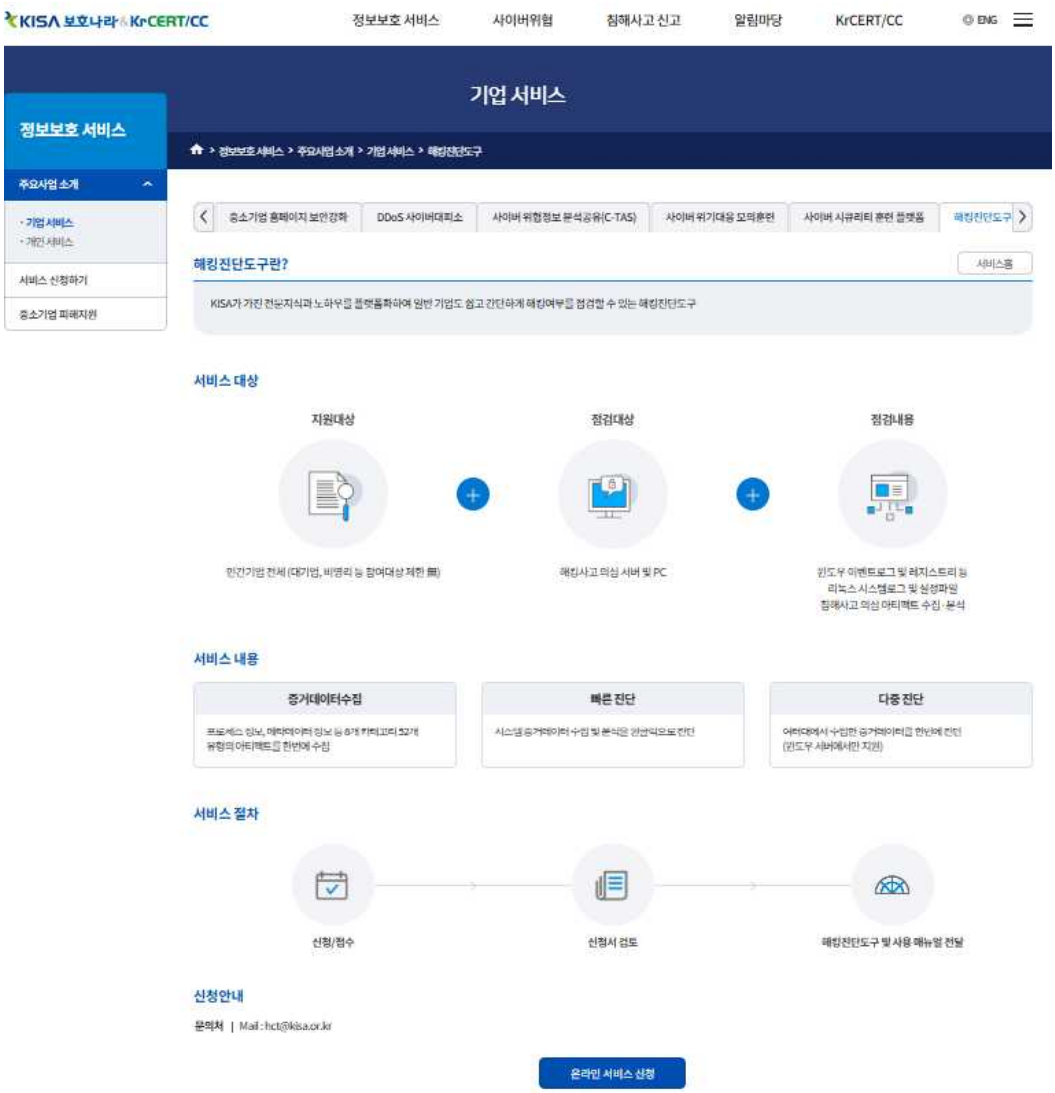
- 필요할 경우 아래와 같이 iptables를 사용하여 특정 포트에 대한 Inbound 트래픽을 제한

※ iptables는 테이블 형식으로 관리되며, 먼저 등록된 것이 효력을 발생하기 때문에 허용하는 정책이 거부하는 정책보다 먼저 위치해야 함

```
· iptables -A INPUT -p TCP --dport 22 -s ip앞 세자리.0/24 -j ACCEPT

· iptables -A INPUT -p TCP --dport 22 -s 192.168.0.0/24 -j ACCEPT

· iptables -A INPUT -p TCP --dport 22 -j DROP

→ ssh 포트에 대해 특정 ip군과 사설ip만 허용하고 나머지는 Drop
```

• 해킹진단도구 서비스 수행(http://www.boho.or.kr)

- 기업에서 운영 중인 서버(윈도우, 리눅스)의 해킹여부를 점검, 결과 제공



나. 네트워크 취약점 조치 방안

- **네트워크 장비의 원격 접근 제한 설정**

  - 허용된 ip 외에는 telnet이나 ssh를 통해 네트워크 장비에 원격 접속할 수 없도록 제한

- **SNMP 접근 제한 설정**

  - 패스워드 역할을 하는 community 문자열의 default 값(public)을 추측하기 어렵고 의미 없는 문자열로 변경
  - 네트워크 장비에서 ACL(access-list) 기능을 이용하여 SNMP에 대한 접근 제한

- **불필요한 서비스 중단**

  - 네트워크 장비를 처음 설치하거나 네트워크 장비의 OS등을 업그레이드 한 후에는 사용하지 않거나 보안상 불필요한 서비스를 반드시 중지

- **설정을 통한 로그인시간 제한**

  - 로그인 한 후 일정 시간 동안 아무런 명령어를 입력하지 않으면 자동으로 접속을 종료하도록 설정

- **로그 관리**

  - 시스템 자체적으로 access-list와 같은 특정한 룰에 매칭되는 로그를 남기도록 설정

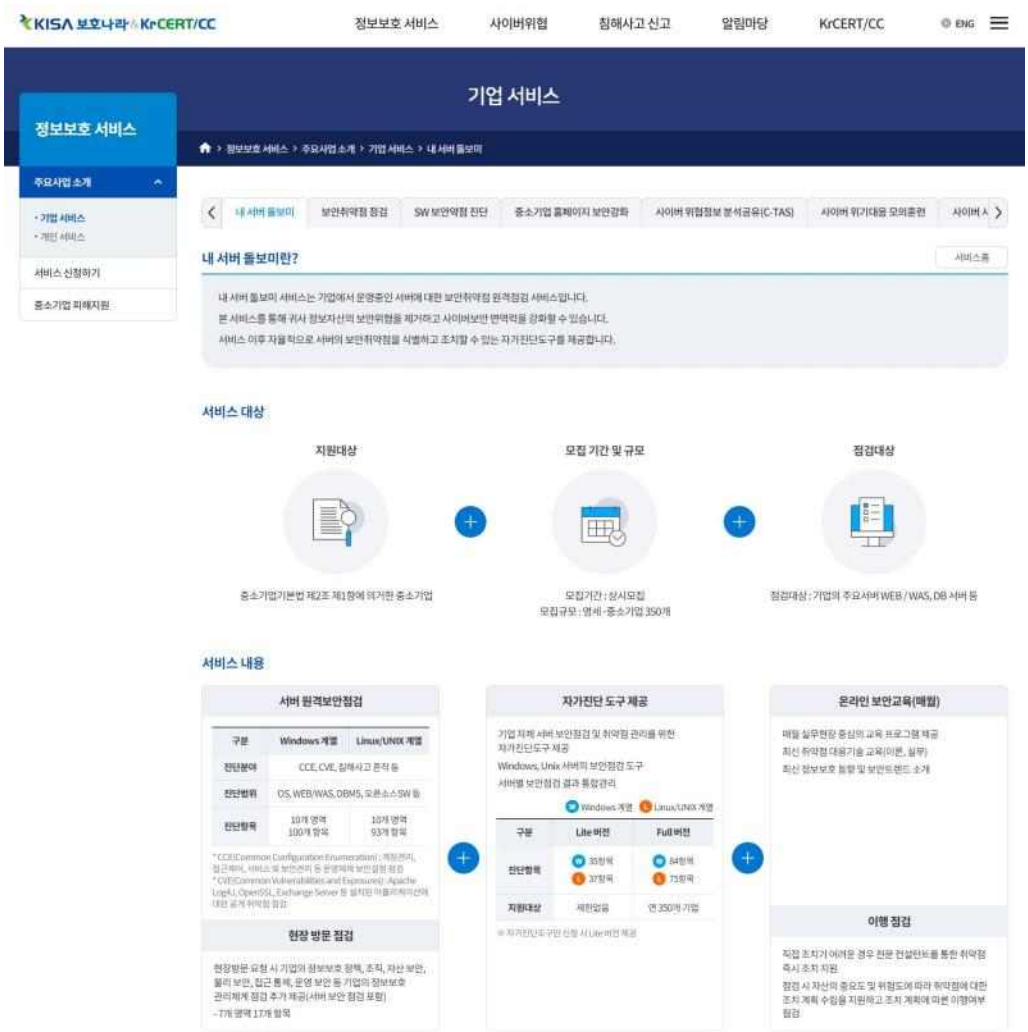
- **보안 패치 적용**

  - 네트워크 보안 취약점 정보 사이트를 주기적으로 방문하여 최신 패치 적용

다. DB 취약점 조치방안

• 내 서버 돌보미 서비스 수행(http://www.boho.or.kr)

- 기업에서 운영 중인 서버에 대한 보안 취약점 원격 점검, 점검 결과 제공



DB 구분 ⟩⟩ My SQL

• DB 시스템 보안패치 적용

- My-SQL이 동작하는 시스템에 대한 기본적인 보안패치 적용

• **DBMS 계정 확인**

- My-SQL 디폴트 설치 시 설정되지 않은 채 비어있는 데이터베이스 관리자 패스워드 변경

※ My-SQL의 관리자인 root는 기본 설치 시 비밀번호가 NULL로 설정됨

- My-SQL 설치 시 기본적으로 생성되어 있는 'test' 계정 삭제

• **원격으로부터의 접속 차단**

- My-SQL이 디폴트로 리스닝하는 3306/tcp 포트를 차단함으로써 데이터베이스가 인가된 어플리케이션에 의해서만 사용되도록 설정

• **데이터베이스내의 사용자별 접속/권한 설정 확인**

- DB 생성 후 사용자 접근 권한 설정 시 일반 사용자에게는 최소한의 권한만을 부여

• **데이터 디렉토리 보호**

- My-SQL 데몬을 mysql이라는 시스템 계정으로 구동할 경우, mysql 디렉토리 이하에 대한 읽기, 쓰기 권한을 제한함으로써 데이터 파일 및 로그파일 보호

• **DB 시스템 보안패치 적용**

- MS에서 제공되는 서비스 팩과 수시로 발표되는 보안패치 설치

• **인증 및 계정관리 확인**

- 윈도우 인증모드 사용을 통해, SQL 사용 권한이 없는 도메인 사용자 또는 윈도우 사용자로부터 윈도우 비밀번호 정책을 사용하여 보안 강화
- 게스트 계정 비활성화
- sysadmin은 데이터베이스에 대한 완전한 관리 권한을 필요로 하는 사용자를 위해 만들어진 역할이므로, 이 역할에 인증되지 않은 사용자는 삭제

• **외부로부터의 SQL Server 포트 접속 차단**

- SQL Server의 디폴트 포트인 1433/tcp, 1434/tcp를 임의의 다른 포트로 설정하여 운영하고, 인가된 시스템에서만 접근이 가능하도록 설정

• **확장 프로시저 제거**

- 서버의 유지관리를 위해 제공하는 확장 프로시저 중 공격에 자주 이용되고 있는 특정 프로시저(xp_cmdshell) 제거 되도록 설정
- 데이터 백업 등의 이유로 데이터베이스로 원격에서 접속해야 하는 경우 SSH 프로토콜 사용

라. 어플리케이션 취약점 조치 방안

• 접근통제 취약점에 대한 조치

설명 - /admin, /admin_login 등과 같이 보편적으로 사용되는 관리자 페이지 주소를 입력하여 해당 페이지로 접근이 가능한 취약점
· 관리자 페이지를 유추하기 어려운 주소로 변경하고 관리자 호스트 IP만 접근 가능하도록 설정

• 부적절한 파라미터 취약점에 대한 조치

설명 - URL, 쿼리 문자열, HTTP 헤더, 쿠키, HTML 폼 인자, HTML hidden 필드 등의 HTTP 요청을 변조하여 웹사이트의 보안 메커니즘을 우회하는 취약점
· 모든 입력 값에 대해 중앙에서 집중적으로 처리하는 하나의 컴포넌트나 라이브러리를 사용하여 모든 인자에 대해 사용 전에 입력 값 검증을 수행하도록 구성 · 파일 다운로드 시 파일명을 직접 URL에서 사용하거나 입력받지 않도록 하며 게시판 이름과 게시물 번호를 이용하여 서버 측에서 데이터베이스 재검색을 통하여 해당 파일을 다운로드 할 수 있도록 수정 · 다운로드 위치는 지정된 데이터 저장소를 지정하여 사용하고, 데이터 저장소 상위 디렉토리로 이동되지 않도록 설정

• Cookie Injection 취약점에 대한 조치

설명 - 쿠키 값 변조를 통해 다른 사용자로의 위장 및 권한상승을 수행할 수 있는 취약점
· Client Side Session 방식인 Cookie는 구조상 다양한 취약점에 노출될 수 있으므로 웹서버에서 제공되는 Server Side Session을 사용 · SSL과 같은 기술을 사용하여 로그인 트랜잭션 전체를 암호화

• SQL Injection(악의적인 명령어 주입) 취약점에 대한 조치

설명 - 데이터베이스 접근을 위해 사용되는 SQL Query문을 비정상적으로 조작하여 사용자 인증 우회, DB에 저장된 데이터 열람, DB의 시스템 명령어를 이용하여 시스템 조작 등의 행위를 할 수 있는 취약점

· 데이터베이스와 연동하는 스크립트의 모든 파라미터를 점검하여 사용자의 입력 값이 SQL Injection을 일으키지 않도록 수정

※ 사용자 입력값 및 URL 인자값에 대해 특수문자(‘, “, ’, ;, :, %, Space, -, +, <, >, (,), #, & 등)와 SQL 구문 (Insert, Select 등)이 포함되어 있는지 검사 후 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리

· SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정

· 웹 어플리케이션이 사용하는 데이터베이스 사용자의 권한을 제한하여 일반 사용자 권한으로는 모든 system stored procedures에 접근하지 못하도록 설정함으로써 SQL Injection 취약점을 이용하여 데이터베이스 전체에 대한 제어권을 얻거나 데이터베이스를 운용중인 서버에 접근이 불가능하도록 설정

· php.ini 설정 중 magic_quotes_gpc 값을 On으로 설정

· Upload 파일을 위한 전용 디렉토리를 별로 생성하여 httpd.conf와 같은 웹 서버 데몬 설정 파일에서 실행 설정을 제거함으로써, Server Side Script가 Upload 되더라도 웹 엔진이 실행하지 않게 환경을 설정

※ IIS 보안 설정

설정 → 제어판 → 관리도구 → 인터넷 서비스 관리자 선택 → 해당 Upload 폴더에 오른쪽 클릭을 하고 등록 정보 → 디렉터리 → 실행권한을 ‘없음’으로 설정

※ Apache 설정

Apache 설정 파일인 httpd.conf의 해당 디렉토리에 대한 문서 타입을 컨트롤하기 위해 Directory 세션의 AllowOverride 지시자에서 FileInfo 또는 All 추가

```
<Directory “/usr/local/apache”>
AllowOverride FileInfo(또는 All)
</Directory>
```

· 파일 업로드 디렉토리에 .htaccess 파일을 만들고 AddType 지시자를 이용, 현재 서버에서 운영되는 Server Side Script 확장자를 text/html로 MIME Type을 재조정하여 업로드된 Server Side Script가 실행되지 않도록 설정

```
<.htaccess>
<FilesMatch “₩.(ph|inc|lib)“>
Order allow.deny
Deny from all
</FilesMatch>
AddType text/html .html .htm .php .php3 .php4 .phtml .phps .in .cgi .pl .shtml .jsp
```

· 설정 후 데몬 재시작

※ 모든 확장자를 제한하고 허용하는 일부 확장자만 업로드 되도록 제한 확장자 검사 우회 (ex, shell.gif.jsp, shell.jpg.jsp)를 막기 위해 뒤에서부터 검사하도록 수정

• XSS(크로스사이트 스크립팅) 취약점에 대한 조치

설명 – 자바스크립트처럼 클라이언트 측에서 실행되는 언어로 작성된 악성 스크립트 코드를 웹 페이지, 웹 게시판 또는 이메일에 포함시켜 사용자에게 전달하면, 해당 웹 페이지나 이메일을 사용자가 클릭하거나 읽을 경우 악성 스크립트 코드가 웹 브라우저에서 실행되는 취약점
· 사용자로부터 입력받는 모든 값을 서버에서 검증 후 입력 받도록 수정 · 스크립트 문장에 존재할 수 있는 아래와 같은 특수 문자를 다른 문자로 변환하도록 소스를 수정 ※ 특수 문자 치환 예 < → &lt > → &gt (→ &#40) → &#41 # → &#35 & → &#38 · 특수 문자 변환을 위해서는 Server Side 언어별로 아래와 같은 함수 이용 가능 ※ ASP : Server.HTMLEncode() PHP : htmlspecialchars() 또는 strip_tags() 또는 strip_replace()

• 버퍼 오버플로우 취약점에 대한 조치

설명 – 지정된 버퍼의 크기보다 큰 데이터를 저장함으로써 실행 시 오류를 발생시키는 취약점
· 서버 제품군과 라이브러리의 경우, 사용하고 있는 제품군에 대한 최신 버그 리포트를 지속적으로 참고하여 최신 패치를 적용 · 자체 제작한 어플리케이션의 경우 HTTP 요청을 통해 사용자의 입력을 받아들이는 모든 코드를 검토하여 입력 값에 대해 적절한 크기를 점검하는지 확인

• CSRF(스크립트 요청 참조) 취약점에 대한 조치

설명 – 공격자가 사용자의 Cookie 값이나 Session 정보를 의도한 사이트로 보내거나 특정한 동작을 유발하는 스크립트를 글에 삽입하여 사용자가 게시물 등을 클릭할 경우 공격자가 원하는 동작이 실행되게 하는 취약점
· 헤더, 쿠키, 질의문, 폼 필드, 숨겨진 필드 등과 같은 모든 파라미터들을 엄격한 규칙에 의해서 검증하여 HTML을 사용할 경우 태그 내에 html, ?, & 등이 포함되지 않도록 수정

• FI(Remote File Inclusion) 취약점에 대한 조치

설명 – 데이터베이스 접근을 위해 사용되는 SQL Query문을 비정상적으로 조작하여 사용자 인증 우회, DB에 저장된 데이터 열람, DB의 시스템 명령어를 이용하여 시스템 조작 등의 행위를 할 수 있는 취약점
· PHP 환경설정 파일 수정 ※ PHP 4.x 이하 버전 : 'allow_url_fopen' 항목을 'off'로 변경 PHP 5.x 이하 버전 : 'allow_url_fopen' 항목과 'allow_url_include'항목을 'off'로 변경 · 외부 사이트의 소스 실행이 반드시 필요한 홈페이지에 대해서는 선별적으로 해당 기능을 허용

```
<VirtualHost www.abc.co.kr>
ServerAdmin webmaster@abc.co.kr
DocumentRoot /home/abc/public_html
ServerName www.abc.co.kr
php_admin_flag allow_url_fopen On ← 추가
</VirtualHost>
```

• 파일 다운로드 취약점에 대한 조치

설명 – 웹 어플리케이션에서 상대경로를 사용할 수 있도록 설정되어 있는 경우, 상대경로 표시 문자열인 "../"를 통해 허가되지 않은 상위경로로 이동하여 시스템 주요 파일, 소스코드 등 중요 자료의 열람이 가능한 취약점
· 파일 다운로드 시 파일명을 직접 URL에서 사용하거나 입력받지 않도록 하며 게시판 이름과 게시물 번호를 이용하여 서버 측에서 데이터베이스 재검색을 통하여 해당 파일을 다운로드 할 수 있도록 수정 · 다운로드 위치는 지정된 데이터 저장소를 지정하여 사용하고 데이터 저장소 상위 디렉토리로 이동되지 않도록 설정 · PHP를 사용하는 경우 php.ini에서 magic_quotes_gpc를 On으로 설정하여 ".₩./"와 같은 역 슬래시 문자에 대응할 수 있도록 설정

• 백업 파일 노출 취약점에 대한 조치

설명 – 관리자가 홈페이지 상에서 작은 수정을 위해 기존 홈페이지 파일의 원본을 특정 확장자를 사용하여 저장할 수 있는데, 이러한 특정 확장자의 파일들이 서버에서 적절하게 처리되지 못할 경우 소스가 유출 될 수 있는 취약점
· 백업파일이 웹 서버에 존재하는 것은 소스 노출이나 DB정보 노출 등의 문제가 발생할 수 있으므로 웹 서버상의 불필요한 백업 파일들은 모두 삭제 · 홈페이지 서비스와 관련 없는 디렉토리(백업디렉토리 등)는 일반 사용자 접근이 불가능하도록 권한 설정

```
<Files~"₩.bak$">
Order allow.deny
Deny from all
</Files>
```

•• 디렉토리 리스팅 취약점에 대한 조치

설명 – 웹 서버에는 현재 브라우징 하는 디렉토리의 모든 파일들을 사용자에게 보여 줄 수 있는 디렉토리 인덱스 기능이 존재하는데, 이런 설정이 활성화되어 있는 경우 공격자가 웹 어플리케이션의 구조를 파악할 수 있는 기회를 제공하게 되는 취약점
· 아파치 웹서버 : httpd.conf 파일에서 DocumnetRoot 항목을 아래와 같이 수정 <Files~"₩.bak$">

```
...
<Directory "/usr/local/www">
Options Indexes ← 제거한다
</Directory>
```

· IIS 웹서버 : IIS 관리메뉴의 기본웹사이트 등록정보에서 홈 디렉토리 검색부분 체크 해제

• 설정파일 및 환경변수 노출 취약점에 대한 조치

설명 – 웹 어플리케이션을 설정하기 위해 위치하는 파일들은 시스템이나 DB에 관련 한 많은 정보를 포함하고 있는데, 이 파일들이 공격자에게 노출될 경우 공격자에게 시스템의 많은 정보를 제공하게 되는 취약점
· 홈페이지 서비스와 관련없는 파일은 일반 사용자 접근이 불가능하도록 권한 설정

• 부적절한 HTTP Method 사용 취약점에 대한 조치

설명 – 원격 사용자가 DocumentRoot 디렉토리에 파일을 업로드하거나 수정하는 등의 행위를 하는 것을 제한해야 하는데, 이러한 제한이 적절히 이루어지지 않을 경우 홈페이지가 변조되거나 침해를 입을 수 있는 취약점

· PUT, DELETE Method는 제한된 사용자만 가능하도록 하거나 아무도 사용하지 못하도록 아래와 같이 설정

```
...
<Directory "/home/*/public_html">
<Limit POST PUT DELETE>
Require valid-user
</Limit>
</Directory>
```

• 헤더 정보 노출 취약점에 대한 조치

설명 – 웹 서버에서는 응답 메시지의 헤더에 웹 서버 버전이나 응용 프로그램 버전 등을 전송하는데, 많은 정보들이 노출될 경우 알려진 취약점을 이용한 공격에 악용될 수 있는 취약점

· 아파치 웹 서버의 경우 httpd.conf 내용에 ServerTokens 지시자를 삽입하여 헤더에 의해 전송되는 정보를 최소화

• 오류 메시지 노출 취약점에 대한 조치

설명 – 오류 메시지가 공격자에게 무엇이 틀렸는지 알려주는 표시를 해주는 것으로 인해 공격자가 다양한 공격 방법을 시도할 수 있게 되는 취약점

· 별도의 오류 페이지를 제작하여 각각의 오류코드에 대해 제작된 하나의 오류 페이지로 Redirection 처리
· 아파치 웹 서버의 경우 httpd.conf 파일에서 아래와 같이 설정

```
ErrorDocument 404 /error_page.html
```

• 파일시스템 설정 오류 취약점에 대한 조치

설명 – 악성 프로그램을 /tmp, /dev/shm 등의 파일시스템 관련 디렉토리에 업로드하여 실행하는 형태로 공격에 악용될 수 있는 취약점

· /etc/fstab(파일시스템의 마운트 설정정보 파일) 내용을 아래와 같이 수정하여 해당 디렉토리의 실행권한을 제거(변경 후에는 mount 명령을 실행하여 적용해야 함)

```
none on /dev/shm type tmpfs (rw.noexec)
/dev/nda9 on /tmp type ext3 (rw.noexec.nosuid.nodev)
```

• 심볼릭 링크 취약점에 대한 조치

설명 – 웹 서버에서 심볼릭 링크를 이용해서 기존의 웹 문서 이외의 파일시스템에 접근하는 것이 가능한 취약점
· 아파치 웹서버 환경설정파일(httpd.conf)의 Options 지시자에서 심볼릭 링크를 가능하게 하는 옵션인 “FollowSymLinks”를 제거

• 최신 보안 패치 항상 유지

- 제로보드, 테크노트, 그누보드 등의 웹 어플리케이션에 대한 최신의 보안패치를 유지

부 록

부록 ▶인터넷 침해 관련 주요용어

ㄱ

악성코드 감염 단말 사이버치료체계

침해사고를 유발하는 악성코드 감염단말 이용자에게 악성코드 감염사실을 알리고, 자동 점검·치료 기능을 제공하는 서비스

ㄷ

디도스 공격(DDoS, Distributed Denial of Service)

공격자(해커)가 악성코드에 감염된 다수의 PC를 이용하여 대량의 유해 트래픽을 특정 시스템에 전송함으로써 네트워크 및 시스템의 과부하를 유발하여 정상적인 서비스를 방해하는 사이버 공격

디도스 사이버대피소

자체적으로 DDoS 대응이 어려운 중소기업을 대상으로 대피소에서 공격 트래픽을 방어하고 정상 이용자의 접속을 웹사이트로 전달해주는 DDoS 공격 방어 서비스

ㄹ

랜섬웨어(Ransomware)

몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로 사용자의 동의 없이 컴퓨터에 불법으로 설치되어서, 사용자 문서 등을 암호화하여 인질로 잡고 돈을 요구하는 악성프로그램

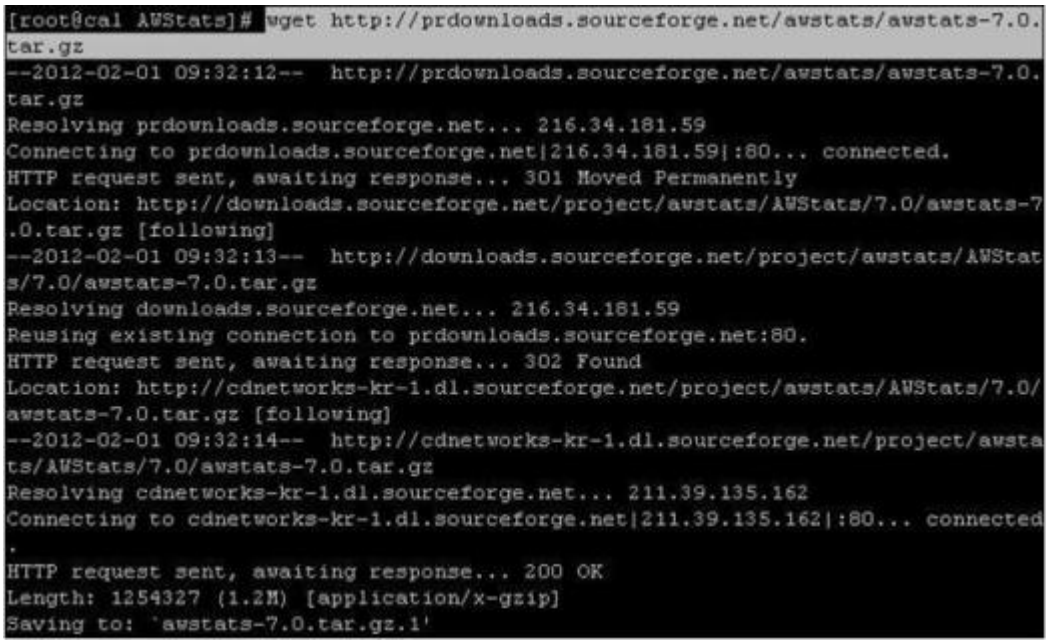
루트킷(Rootkit)

루트킷은 해커가 설치한 악성코드(트로이목마, 악성봇 등)가 백신이나 PC 사용자에게 발각되지 않도록 숨겨주는 역할을 함
대부분의 루트킷은 일반 프로그램이 동작하는 계층보다 더 하위계층, 즉 커널이라는 운영체제 핵심 부분에 숨어서 동작하여 탐지·분석이 어려움.
※ ‘커널 루트킷’, ‘커널 감염형 악성코드’라고 불리기도 함

로그분석

로그(log)는 시스템의 데이터 처리 내용이나 접속현황 등 다양한 운용 정보를 시간의 흐름에 따라 기록한 정보로써 로그분석을 통해 침해사고 발생 시점, 침입경로, 공격자 추적 등 침해사고 원인분석을 위한 단서를 확보할 수 있음

<웹서버에 기록된 로그 화면 사례>



명령·제어 서버 (C&C, Command and Control)

해커가 악성코드 등으로 감염시킨 좀비PC를 관리하고 DDoS 등의 공격명령을 내리기 위한 목적으로 구축한 서버

민관합동조사단

정보통신망에 중대한 침해사고 발생 시 원인조사, 기술지원 및 재발방지대책 마련을 목적으로 과학기술정보통신부에서 구성하는 합동조사단

※ 조사단은 민간분야 보안전문가들로 구성된 '사이버보안전문단' 구성원 중에서 20명 이내 선발

※ 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제48조의4(침해사고 원인분석 등)

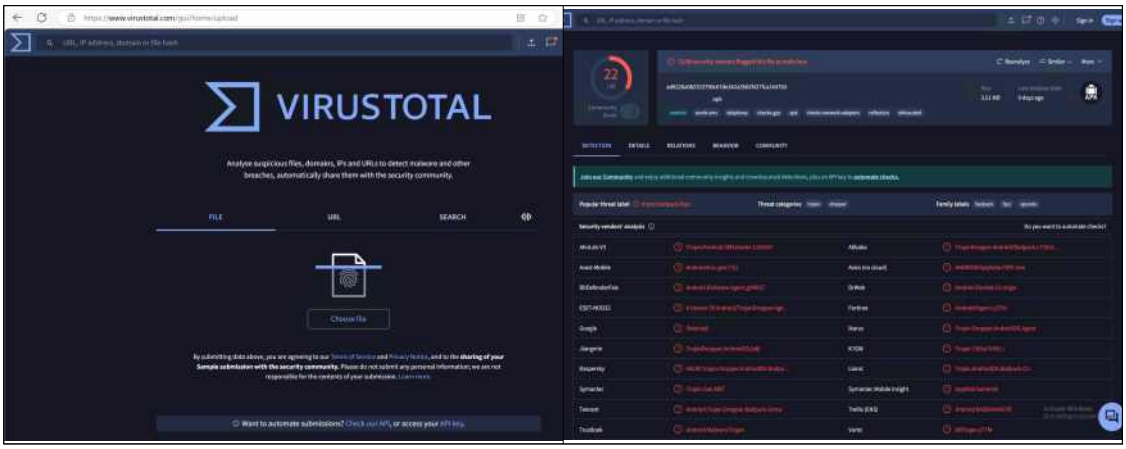
※ 『정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령』제59조(민·관합동조사단의 구성·운영)

바이러스 (Virus)

정상적인 실행파일에 달라붙어(기생) PC를 다운시키거나 파일을 파괴하는 등 컴퓨터의 운영을 방해하는 악성코드의 일종
감염대상이 되는 파일이 있어야 하며, 자신을 복제하는 기능은 없음.
※ 주로 '80~ '90년대에 많이 발생했으며, 플로피디스크 등을 통해 감염

바이러스 토탈(Virus Total)

구글이 운영하는 악성코드 점검 사이트
해당 사이트에 의심스러운 파일을 업로드하면, 국내외 40여개 백신프로그램으로 해당 파일에 대해 악성 여부를 검사하여 그 결과를 실시간으로 제공



< 바이러스 토탈 사이트 샘플파일 점검화면 사례 >

백도어(Backdoor)

일명 '개구멍'과 같이 허가되지 않은 비정상적인 출입통로를 의미
해커가 이용자 몰래 컴퓨터에 접속하여 악의적인 행위를 할 수 있도록 출입통로 역할을 해주는 악성코드

버퍼 오버플로우(Buffer Overflows)

컴퓨터상에서 특정 프로그램에 할당된 메모리 영역을 초과하는 크기의 데이터를 입력시킴으로써 발생하는 취약점을 이용한 해킹기법
버퍼의 크기보다 더 많은 데이터를 입력하면 버퍼가 넘쳐 메모리의 다른 영역으로 침범하게 되는데, 이때 프로그램이 오류를 일으켜 해커가 원하는 공격코드가 실행되도록 하는 방식
※ 버퍼 : 시스템이 연산 작업에 필요한 데이터들을 일시적으로 저장하는 메모리상의 저장 공간

보이스피싱(Voice Phishing)

음성(Voice)과 개인정보(Private Data), 낚시(Fishing)의 합성어. 전화로 수사기관·정부기관·금융기관 등을 사칭해 돈을 송금하게 하거나 개인정보·금융정보 등을 탈취하는 사기수법

ㅅ

사이버대피소

자체적으로 DDoS·웹 공격 대응이 어려운 중소기업을 대상으로 대피소에서 공격을 방어하는 서비스

사이버 위협정보 분석·공유(C-TAS)

여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위해 한국인터넷진흥원이 2014년부터 구축한 체계로 보안기업, 금융, 전자상거래, 호스팅 등 다양한 분야의 기업이 참여하여 위협정보를 공유

소프트웨어 보안약점

소프트웨어 결함, 오류 등으로 해킹 등 사이버공격을 유발할 가능성이 있는 잠재적인 보안취약점

소프트웨어 신규 취약점 신고 포상제

「소프트웨어산업 진흥법」에 따른 소프트웨어의 최신 버전에 대한 신규 보안취약점을 최초로 신고한 자에게 포상금을 지급하는 제도 (단, 대한민국 국적자에 한함)

스미싱(Smishing)

문자메시지(SMS)와 피싱(Phishing)의 합성어. 스마트폰 문자메시지를 통해 악성앱을 설치하도록 유도하여 개인정보, 금융정보 등을 탈취하는 사기 수법

신규 취약점(Zero-Day Vulnerability)

최신 버전의 소프트웨어에서 동작하는 취약점으로 해당 취약점을 제거하는 보안패치가 발표되지 않은 상태의 취약점

악성 앱(Malicious App)

스마트폰에 설치되어 과금유발, 정보유출, 파일을 조작하여 이용자에게 정신적·금전적 피해를 유발시키는 프로그램

악성봇(Bot)

해커가 원격에서 조종할 수 있도록 좀비PC를 만드는 악성코드이며, PC가 악성봇에 감염되면, 해커의 조종에 따라 PC 사용자도 모르는 사이에 스팸발송, 악성코드 유포, 분산 서비스 거부 공격(DDoS) 등에 악용될 수 있음

악성코드 은닉사이트

악성코드 자체 또는 악성코드를 유포하는 주소(URL)를 숨기고 있는 홈페이지로, 보안에 취약한 이용자 PC 가 해당 홈페이지에 접속 시 악성코드에 감염될 우려가 있음

역공학(Reverse Engineering)

정보보호 분야에서는 주로 악성코드의 기능이나 동작을 분석할 때 사용되며, 소스코드가 제공되지 않는 프로그램을 역으로 분석하여 기능을 추적하는 행위를 의미함
시스템이나 프로그램 등을 개발하기 위하여 설계-구현-테스트 등 단계적으로 절차를 진행하는 것에 반대되는 개념

웜(Worm)

다른 파일에 기생하지 않고 독립적으로 자신을 복제하여 확산함으로써 전파속도가 매우 빠른 특징을 가지는 악성코드 유형, 주로 메일이나 네트워크 공유폴더 등을 통해 전파되고 시스템과 네트워크에 부하를 높이는 증상을 보임

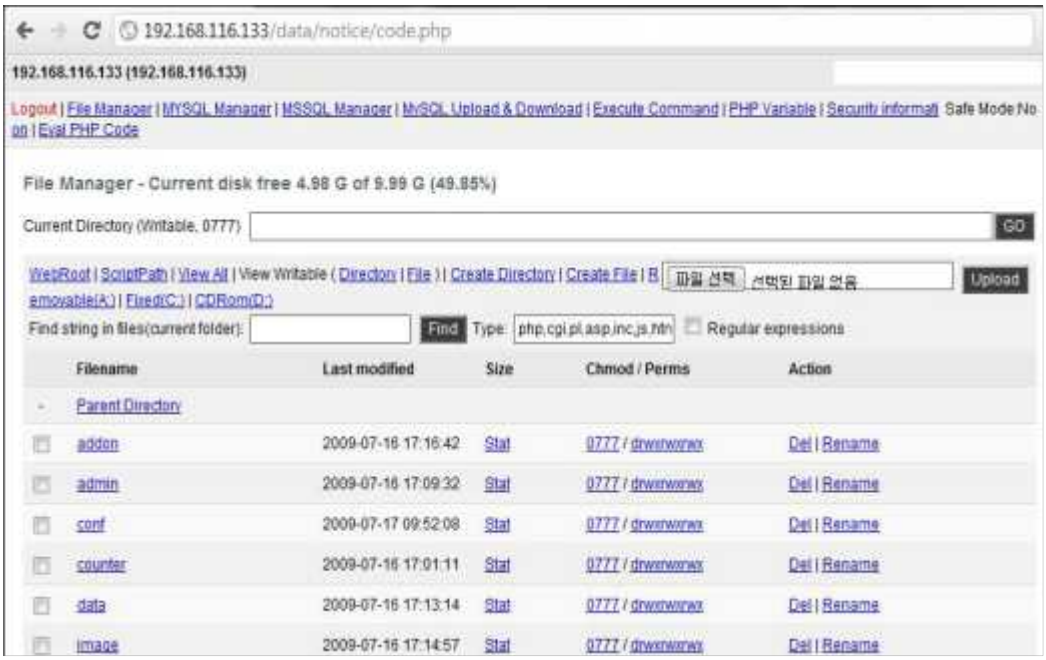
웹 해킹(Web Hacking)

웹 서비스와 관련된 구성 요소들을 공격하여 이용자 권한이나 관리자 권한을 획득하는 행위를 의미
웹은 누구나 쉽게 접속할 수 있도록 구성되고 웹 게시판이나 DB 등 다양한 어플리케이션들이 연동되기 때문에 취약점 발생 가능성이 높고 해킹 위험도 큼

웹셸(Web Shell)

공격자가 원격으로 웹서버에 악의적인 명령을 실행할 수 있도록 작성한 웹스크립트 파일로, 웹서버 내 취약점을 악용하여 업로드 됨

< 웹셸을 실행한 화면 예시 >



이미지 분석

시스템의 하드디스크와 완벽히 같은 사본 파일을 만드는 과정을 이미징(Imaging) 이라고 하며, 해당 사본 파일을 분석하는 것을 의미
숨김파일, 임시파일, 손상/삭제 파일의 잔여정보가 그대로 존재하고, 원본 증거를 보호할 수 있는 장점 제공

<일반 복사와 디스크 이미징 차이>

구분	디스크복사	디스크이미징
저장방식	디스크 내부의 파일들을 읽어서 순차적으로 복사를 실시	디스크의 첫 번째 위치에서부터 끝 위치까지 복사를 실시
저장대상	파일과 디렉터리 단위의 정보	디스크의 모든 물리적 섹터
정보손실	시스템 파일, 사용 중인 파일은 내용을 읽을 수 없으므로 복사가 실패	하드웨어의 물리적 오류를 제외하고 디스크의 모든 정보를 복사
파일복구	삭제 파일의 정보를 수집하지 않음	디스크 섹터에 삭제파일 정보가 남아있는 경우 복구 가능

익스플로잇(Exploit)

해커가 컴퓨터 소프트웨어(또는 하드웨어)의 취약점을 이용해 악성(개인정보 탈취, 악성코드 유포 등)행위를 하기위해 제작한 악성 프로그램

인터넷 연동구간(IX, Internet eXchange)

ISP(인터넷 서비스 제공자)간의 인터넷 트래픽을 원활하게 소통시키기 위한 인터넷 연동 서비스로, ISP간의 상호접속을 목적으로 국내 ISP간 트래픽을 교환하는 국내 연동구간과 해외 ISP와 연결되는 국제 연동구간이 있음

ㅈ 정보공유·분석센터 (ISAC : Information Sharing & Analysis Center)

통신, 금융, 행정 등 분야별 주요정보통신기반시설에 대한 해킹 및 사이버테러 등 전자적 침해행위에 관한 정보를 분석하고, 침해사고 발생시 대응요령 및 지침을 신속하게 전파하는 등 사이버 공격에 효과적으로 예방, 탐지, 대응하도록 지원할 수 있는 시스템 및 조직

정보보호 관리체계 (Information Security Management System)

기업 또는 조직이 각종 위협으로부터 주요 정보자산을 보호하기 위해 정보보호관리 절차를 체계적으로 수립하여 지속적으로 관리·운영하는 종합적인 체계(’13년부터 ISMS 인증제도가 의무화되었으며, ’18년부터 개인정보 보호 인증기준이 통합된 ISMS-P 제도로 운영 중)

※ 인증심사 기준 : 총 101개 인증기준으로 구성(관리체계 수립 및 운영 16개, 보호대책 요구사항 12개 분야 64개 통제사항, 개인정보 처리 단계별 요구사항 21개)

정보보호의 날(매년 7월 둘째 주 수요일)

범부처 합동으로 사이버 공격을 예방하고 국민들의 정보보호 생활화를 위해 지정된 정부 주관 기념일('12. 10. 22, 대통령령)로써 정보보호의 날(매년 7월 둘째 주 수요일)에는 정보보호의 날 기념식을 개최

정보통신기반시설

국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망

좀비PC(Zombie PC)

악성코드에 감염됐지만 스스로 인지하지 못한 채 스팸 발송, DDoS 공격 등 해커에 의해 원격조종당하는 PC

주요정보통신기반시설

중앙행정기관의 장이 소관분야의 정보통신기반시설 중 전자적 침해행위로부터 보호가 필요하다고 인정하여 지정한 시설

※ 지정 기준(정보통신기반보호법 제8조 관련) : ① 업무의 국가사회적 중요성, ② 정보통신기반시설에 대한 의존도, ③ 다른 정보 통신기반시설과의 상호 연계성, ④ 침해사고 발생시의 피해규모 및 범위, ⑤ 침해 사고 발생가능성 또는 복구의 용이성

지능형 지속 공격 (APT, Advanced Persistent Threat)

특정 대상을 겨냥해 명확한 목표를 두고 지능적, 지속적으로 은밀히 공격을 가하여 정보를 수집하고 유출하는 해킹기법

<APT 공격 절차>

※ 주요 대상 : 정부기관, 사회기반 산업시설, 금융, 정보통신 기업 등

※ 대표적 사례 : 스턱스넷(‘10년), 3·4 DDoS 공격(’ 11.3월), 농협전산망 마비사고(‘11.4월), 3·20 사이버공격(’ 13.3월), 6·한수원 내부정보 유출(’ 14.12월) 등

침해사고대응팀(CERT)

인터넷상에서 침해사고 발생 시 대응 및 예방 업무를 담당하는 조직으로 독립된 기관, 회사 내 소속된 부서 등 그 형태는 다양함. 특히, 국가 전체에 대한 침해사고 대응 업무를 하는 조직을 국가침해사고대응팀 이라고 부름

ㅋ 키로거(Keylogger)

사용자의 키보드 입력값을 로그파일로 저장하여 해커측으로 전송하는 악성 프로그램

※ 사례 : 키로거를 실행시켜 놓고 네이버에 로그인하면 아이디, 비밀 번호가 노출됨

<키로거 실행 및 로그인 정보 입력 사례>

ㅌ

트로이목마(Trojan)

그리스 신화에서 유래된 명칭으로, 컴퓨터에 숨어 있다가 사용자의 정보를 몰래 유출하는 악성코드의 일종이며, 정상적인 파일(게임, 응용S/W 등)에 포함되어 함께 설치되는 경우가 많음

ㅍ

파밍(Pharming)

이용자 PC에 악성코드를 감염시키거나, 해킹 등으로 도메인 네임 시스템(DNS) 등을 변조함으로써 사용자가 정상사이트 주소를 입력해도 가짜(피싱) 사이트로 접속하게 하여 개인정보, 금융정보 등을 탈취하는 수법

피싱(Phishing)

개인정보(private data)와 낚시(fishing)를 합성한 용어로, 불특정 다수에게 이벤트 당첨이나 개인정보 확인 요청 등의 내용을 담은 거짓 e메일을 보내거나 국가기관이나 금융기관 등을 사칭하는 가짜 사이트를 만들고 로그인이나 카드결제를 하는 것처럼 속여 정보를 빼가는 온라인 사기수법

ㅎ

해킹(Hacking)

컴퓨터 또는 시스템의 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신시스템에 침입하는 행위(정보통신망 이용촉진 및 정보보호 등에 관한 법률)제48조 1항, 3항에 의한 정의

해킹방어대회(Hacking Defence & Contest: HDCon)

국내 정보보호 인력의 해킹 방어수준 측정, 윤리적 해커 양성 등을 위해 KISA가 개최해 온 국내에서 가장 전통 있는 해킹방어대회
※ 공격보다 사고분석 및 방어에 중점을 두고 문제를 해결하는 국내 유일한 대회

허니넷

다수의 IP를 이용하여 보안에 취약한 PC 환경을 구축 후, 인터넷에 노출시켜 악성코드를 채증하는 시스템

홈페이지 변조(Homepage Defacement)

홈페이지 메인 화면이 비정상적인 다른 이미지로 보이도록 해커가 변조한 것으로 특정 기업이나 조직의 이미지, 신뢰성 등을 실추시키려는 목적으로 많이 발생

A

APCERT(Asia Pacific Computer Emergency Response Team)

아태침해사고대응팀협의회. 아태지역 내 침해사고대응팀 연합

ActiveX

ActiveX는 MS사의 인터넷브라우저(IE)에서만 동작되는 기술로 이용자가 웹서비스를 이용하는데 필요한 응용프로그램을 PC에 자동 설치할 수 있도록 지원하는 비표준 기술

C

CC(Common Criteria)

IT제품의 보안성을 평가하기 위한 국제표준(ISO/IEC 15408)

CCRA(Common Criteria Recognition Arrangement)

한, 미, 일 등 25개 회원국이 CC에 따른 평가·인증 받은 제품을 상호인정 하는 국제 협정

CERT(Computer Emergency Response Team)

침해사고대응팀을 일컫는 말로, CERT/CC에서 로열티를 갖고 있음

CONCERT(CONsortium of CERTs, 한국침해사고대응팀협의회)

국내 정보통신망 침해사고대응팀(CERT) 간의 정보교류, 기술공유, 업무협조 등의 협력체계를 마련하기 위해 결성된 국내 CERT 협의체
※ 1996년 결성, 2005년 사단법인으로 재출범

CSIRT(Computer Security Incident Response Team)

침해사고대응팀을 일컫는 말로, CERT/CC에서 로열티를 갖고 있는 CERT(Computer Emergency Response Team)을 대체하기 위한 용어로 널리 사용 중

C-TAS(Cyber Threat Analysis & Sharing System)

3.20, 6.25 등 대규모 사이버 공격에 대한 후속조치로, 위협정보 수집·분석·공유 절차를 체계화하여 신속히 대응하기 위해 구축하였으며 악성코드, 취약점, 침해사고 등 위협정보를 체계적으로 수집·저장하고 정보를 종합적으로 분석하여 유관기관과 신속하게 공유하는 시스템

D

DNS(Domain Name System)

숫자로 이루어진 인터넷주소(IP)를 사용자가 알기 쉽게 문자로 표현된 도메인네임으로, 문자로 표현된 도메인네임을 다시 컴퓨터가 인식할 수 있도록 숫자로 표기된 IP 주소로 변환해 주는 시스템

DNS싱크홀

좀비PC가 C&C와 연결을 시도할 때 해당 트래픽을 우회시켜 해커가 C&C를 통해 좀비PC를 조종하지 못하도록 차단하는 시스템

F

FIRST(Forum for Incident Response and Security Teams)

국제침해사고대응팀협의회. 전 세계 최대 규모의 침해사고대응팀 연합

G

GCCD(Global Cybersecurity Center for Development, 글로벌정보보호센터)

WB(세계은행) 회원국의 정보보호 역량 강화를 목적으로 한국정부와 WB가 협력하여 인천(송도)에 설립

H HTML5(Hyper Text Markup Language 5)

차세대 웹문서 표준(’15년 확정)으로서, 텍스트와 하이퍼링크만 표시하던 HTML이 멀티미디어 등 다양한 애플리케이션까지 표현·제공하도록 진화한 “웹 프로그래밍 언어”

R Rooting(루팅)

안드로이드 운영체제를 탑재한 모바일 기기에서 root 계정을 획득하는 것
※ root 계정 : 모든 파일과 프로그램에 접근 가능한 권한을 가진 슈퍼유저(superuser)가 사용하는 계정

S SQL 인젝션(SQL Injection)

SQL을 사용하는 응용프로그램에서 S/W개발자가 생각하지 못한 입력 및 조작으로 인해 발생하는 오류
※ SQL(Structured Query Language) : 사용자가 데이터베이스(DB)에 질의, 삽입, 삭제 등의 작업을 수행할 수 있도록 해주는 표준 데이터베이스 질의 언어