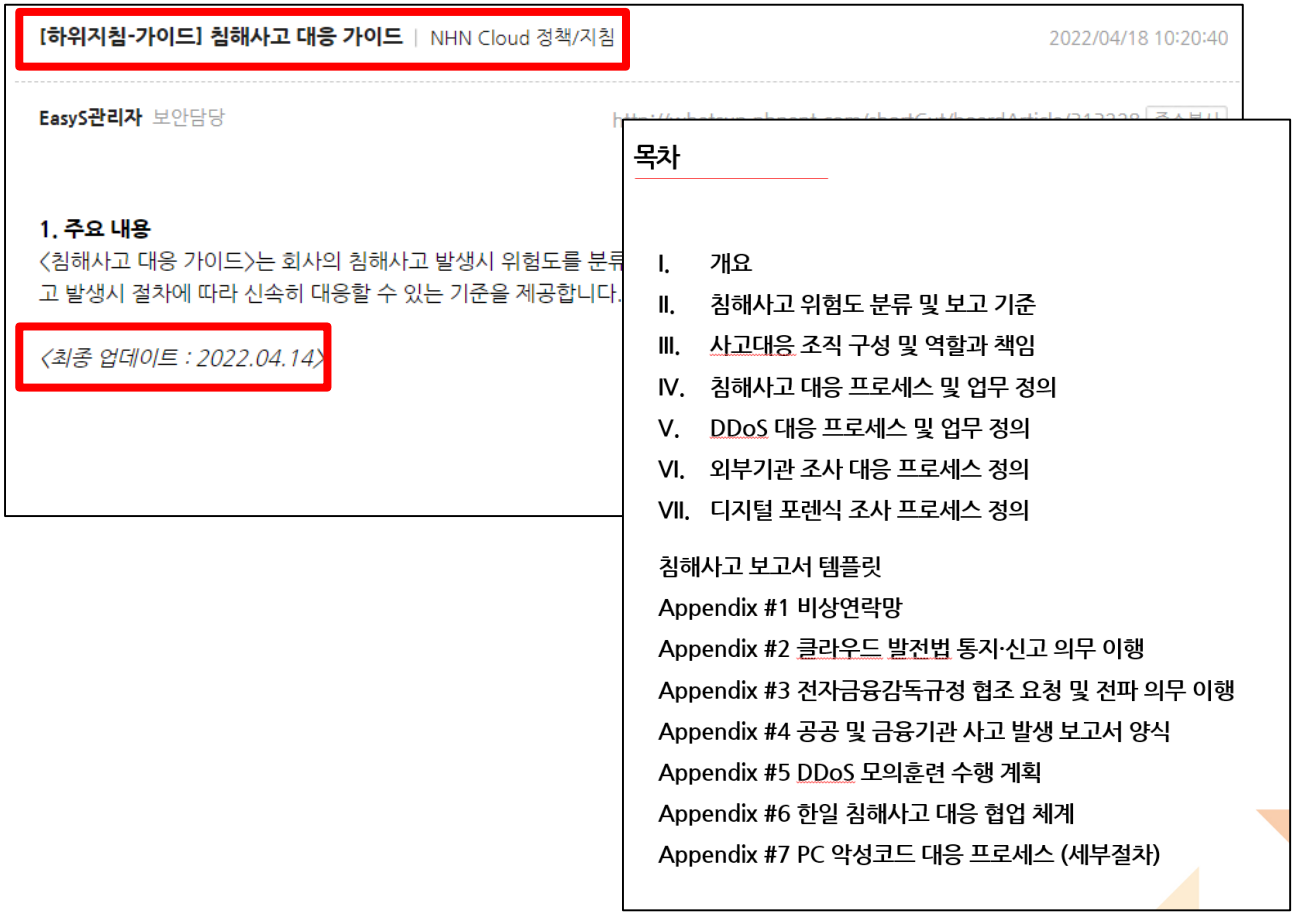
1-2. 침해사고 대응 절차 및 사후관리대책

증적

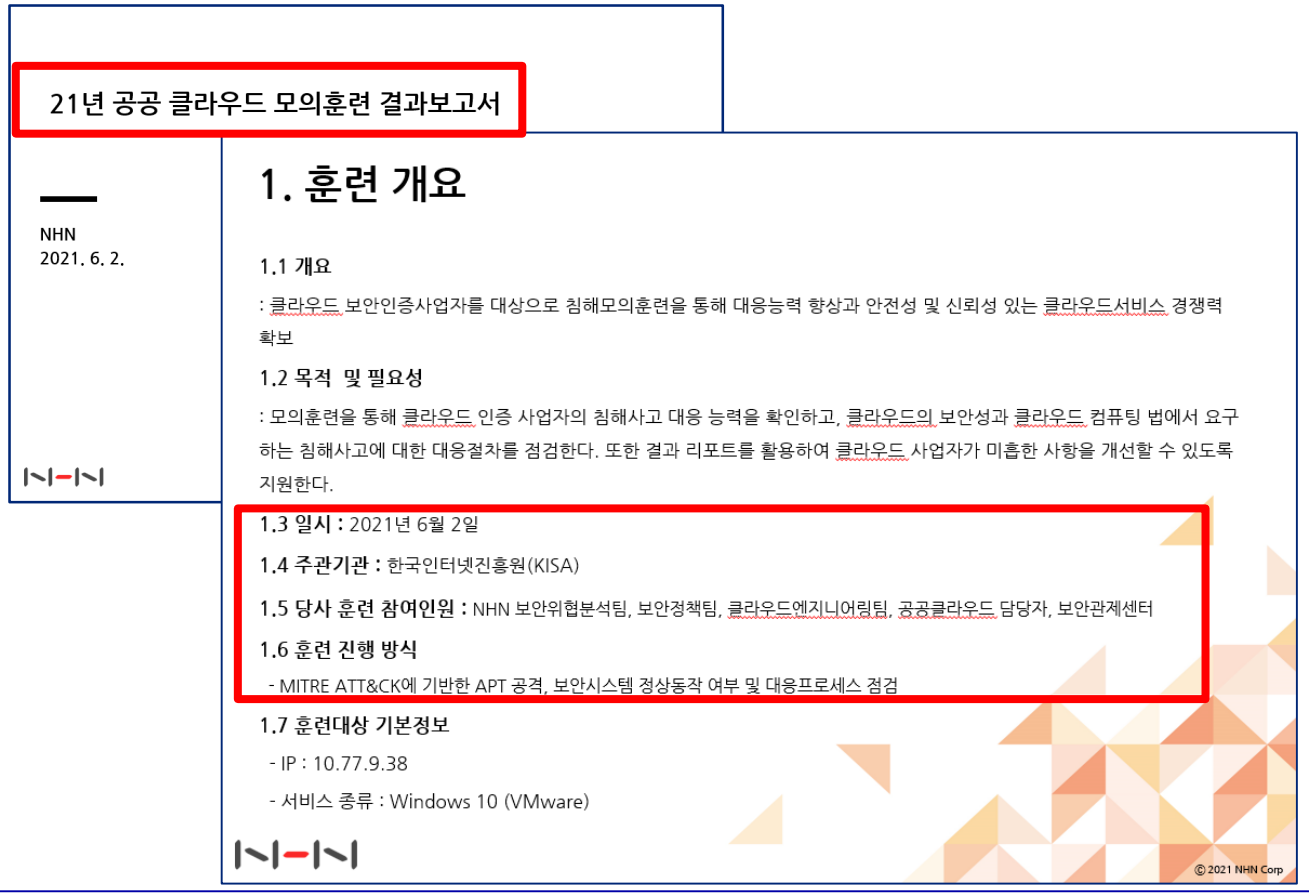


Description

- **NHN Cloud는 다음 사항이 반영된 침해사고 대응 절차를 수립하여 운영 중이며, 클라우드컴퓨팅법, 개인정보보호법, 정보통신망법 등 관련 법률에서 요구하는 사항을 반영하여 준수하고 있음**

1-2. 침해사고 대응 절차 및 사후관리대책

증적	Description
■ 공공 클라우드 침해사고 모의 훈련 증적 (1/5)	• 공공 클라우드 침해사고 모의훈련은 연 1회 KISA주관 하에 보안위협분석팀, 보안정책팀 및 유관부서와 진행하고 있으며, 2022년은 하반기 진행 예정임



21년 공공 클라우드 모의훈련 결과보고서

NHN
2021. 6. 2.

1. 훈련 개요

1.1 개요

: 클라우드 보안인증사업자를 대상으로 침해모의훈련을 통해 대응능력 향상과 안전성 및 신뢰성 있는 클라우드서비스 경쟁력 확보

1.2 목적 및 필요성

: 모의훈련을 통해 클라우드 인증 사업자의 침해사고 대응 능력을 확인하고, 클라우드의 보안성과 클라우드 컴퓨팅 법에서 요구하는 침해사고에 대한 대응절차를 점검한다. 또한 결과 리포트를 활용하여 클라우드 사업자가 미흡한 사항을 개선할 수 있도록 지원한다.

1.3 일시 : 2021년 6월 2일

1.4 주관기관 : 한국인터넷진흥원(KISA)

1.5 당사 훈련 참여인원 : NHN 보안위협분석팀, 보안정책팀, 클라우드엔지니어링팀, 공공클라우드 담당자, 보안관제센터

1.6 훈련 진행 방식

- MITRE ATT&CK에 기반한 APT 공격, 보안시스템 정상동작 여부 및 대응프로세스 점검

1.7 훈련대상 기본정보

- IP : 10.77.9.38
- 서비스 종류 : Windows 10 (VMware)

1-2. 침해사고 대응 절차 및 사후관리대책

증적

■ 공공 클라우드 침해사고 모의 훈련 증적 (2/5)

1. 대응 현황

■ 사고대응 타임라인

발생 일시	2021-6-2 13:31:00			
분석시스템	Windows 10			
발생 원인	스피어 피싱을 통한 악성코드 유입			
피해 현황	G 클라우드 담당자 PC(NHN-PC) 1대 감염			
심각도 등급	3 등급			
대응 시작 일시	2021-6-2 13:44:00			
대응, 보고, 복구 현황 Timetable	수행 시간	수행 내용	수행 부서	비고(특이사항, 보고자 등)
	13:31~13:44	최초 공격 인지 및 보안관제팀 이벤트 탐지 후 전파	보안관제팀	보고 : IDC 담당자, 보안위협분석팀 / 메일, 유선연락
	13:44~13:48	보안 이벤트 및 1차 분석	보안위협분석팀	침해사실 인지
	13:48~13:49	감염 PC 네트워크 절체 및 IP 차단	보안위협분석팀	선 차단 조치
	13:48~13:51	유관 부서 및 협력 업체 해당 내용 전파 및 영향도 확인	보안위협분석팀	메신저/메일
	13:53	악성코드 감염 최초 내부 보고	보안위협분석팀	보고 : CISO / 메일
	13:55	악성코드 감염 및 정보유출에 대한 이용자 공지	클라우드엔지니어링팀	홈페이지 공지 및 메일 안내
	13:56~13:59	감독기관 최초 신고	보안정책팀	보고 : 감독기관 / 메일
	13:59	감염 PC 포맷 진행	클라우드시스템팀	N/A
	14:00~14:06	보안 이벤트 및 2차 분석 수행, 유입경로 및 추가 확인	보안위협분석팀	N/A
	14:07~14:08	악성코드 감염 및 정보유출에 대한 이용자 정상화 완료 공지	클라우드엔지니어링팀	홈페이지 공지 및 메일 안내
	14:09	감독기관 최종 신고(정상화 완료)	보안정책팀	보고 : 감독기관 / 메일
	14:09	악성코드 감염 최종 내부 보고(재발방지를 위한 향후 대책)	보안위협분석팀	보고 : CISO / 메일

Description

- 공공 클라우드 침해사고 모의훈련 진행 시, 클라우드컴퓨팅법에서 요구하는 항목에 대해서 고객에게 통지 / 감독기관 신고 훈련 진행하고 있음
- 침해사고 대응 완료 후, 재발방지 대책을 포함한 최종 내부 보고 절차도 포함하여 훈련 진행하고 있음

1-2. 침해사고 대응 절차 및 사후관리대책

증적

■ 공공 클라우드 침해사고 모의 훈련 증적 (3/5)

Description

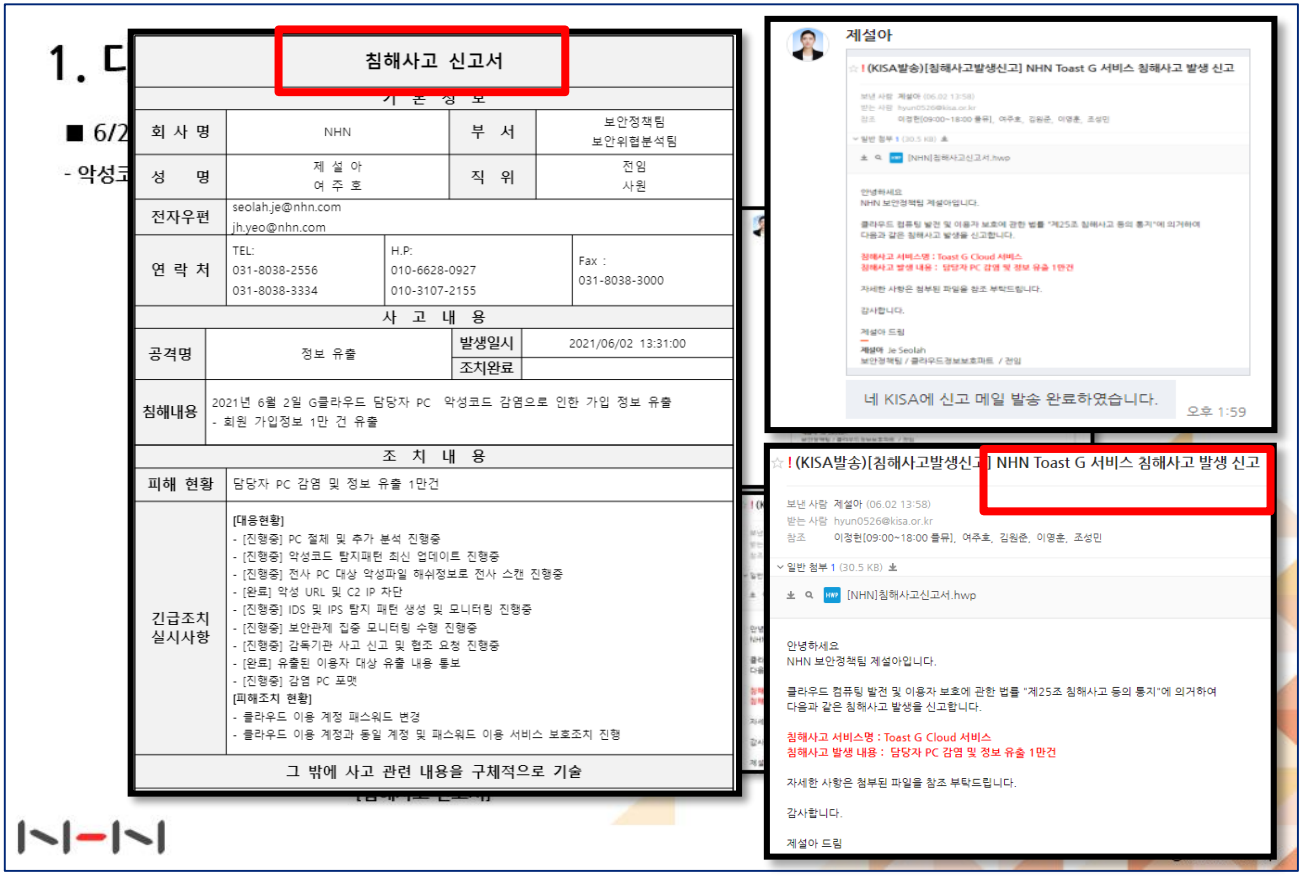
- 공공 클라우드 침해사고 모의훈련 진행 시, 클라우드컴퓨팅법에서 요구하는 항목에 대해서 고객에게 공지사항으로 통지하고 있음

  1. 발생시간
  2. 발생내용
  3. 발생원인
  4. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 현황
  5. 클라우드컴퓨팅서비스 이용자의 피해 예방 또는 확산 방지 방법

1-2. 침해사고 대응 절차 및 사후관리대책

증적

■ 공공 클라우드 침해사고 모의 훈련 증적 (4/5)



침해사고 신고서

기 본 정 보			
회 사 명	NHN	부 서	보안정책팀 보안위협분석팀
성 명	제 설 아 여 주 호	직 위	전임 사원
전자우편	seolah.je@nhn.com jh.yeo@nhn.com		
연 락 처	TEL: 031-8038-2556 031-8038-3334	H.P: 010-6628-0927 010-3107-2155	Fax : 031-8038-3000

사 고 내 용			
공격명	정보 유출	발생일시	2021/06/02 13:31:00
		조치완료	
침해내용	2021년 6월 2일 G클라우드 담당자 PC 악성코드 감염으로 인한 가입 정보 유출 - 회원 가입정보 1만 건 유출		

조 치 내 용	
피해 현황	담당자 PC 감염 및 정보 유출 1만건
긴급조치 실시사항	[대응현황] - [진행중] PC 격제 및 추가 분석 진행중 - [진행중] 악성코드 탐지패턴 최신 업데이트 진행중 - [진행중] 전사 PC 대상 악성파일 해쉬정보로 전사 스캔 진행중 - [완료] 악성 URL 및 C2 IP 차단 - [진행중] IDS 및 IPS 탐지 패턴 생성 및 모니터링 진행중 - [진행중] 보안관제 집중 모니터링 수행 진행중 - [진행중] 감독기관 사고 신고 및 협조 요청 진행중 - [완료] 유출된 이용자 대상 유출 내용 통보 - [진행중] 감염 PC 포맷 [피해조치 현황] - 클라우드 이용 계정 패스워드 변경 - 클라우드 이용 계정과 동일 계정 및 패스워드 이용 서비스 보호조치 진행
그 밖에 사고 관련 내용을 구체적으로 기술	

제설아

☆ ! (KISA발송)[침해사고발생신고] NHN Toast G 서비스 침해사고 발생 신고

네 KISA에 신고 메일 발송 완료하였습니다. 오후 1:59

☆ ! (KISA발송)[침해사고발생신고] NHN Toast G 서비스 침해사고 발생 신고

보낸 사람 제설아 (06.02 13:58)
받는 사람 hyun0526@kisa.or.kr
참조 이정현(09:00~18:00 출퇴), 여주호, 김원준, 이영훈, 조성민

일반 첨부 1 (30.5 KB)

[NHN]침해사고신고서.hwp

안녕하세요
NHN 보안정책팀 제설아입니다.

클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 "제25조 침해사고 등의 통지"에 의거하여
다음과 같은 침해사고 발생을 신고합니다.

침해사고 서비스명 : Toast G Cloud 서비스
침해사고 발생 내용 : 담당자 PC 감염 및 정보 유출 1만건

자세한 사항은 첨부된 파일을 참조 부탁드립니다.

감사합니다.

제설아 드림

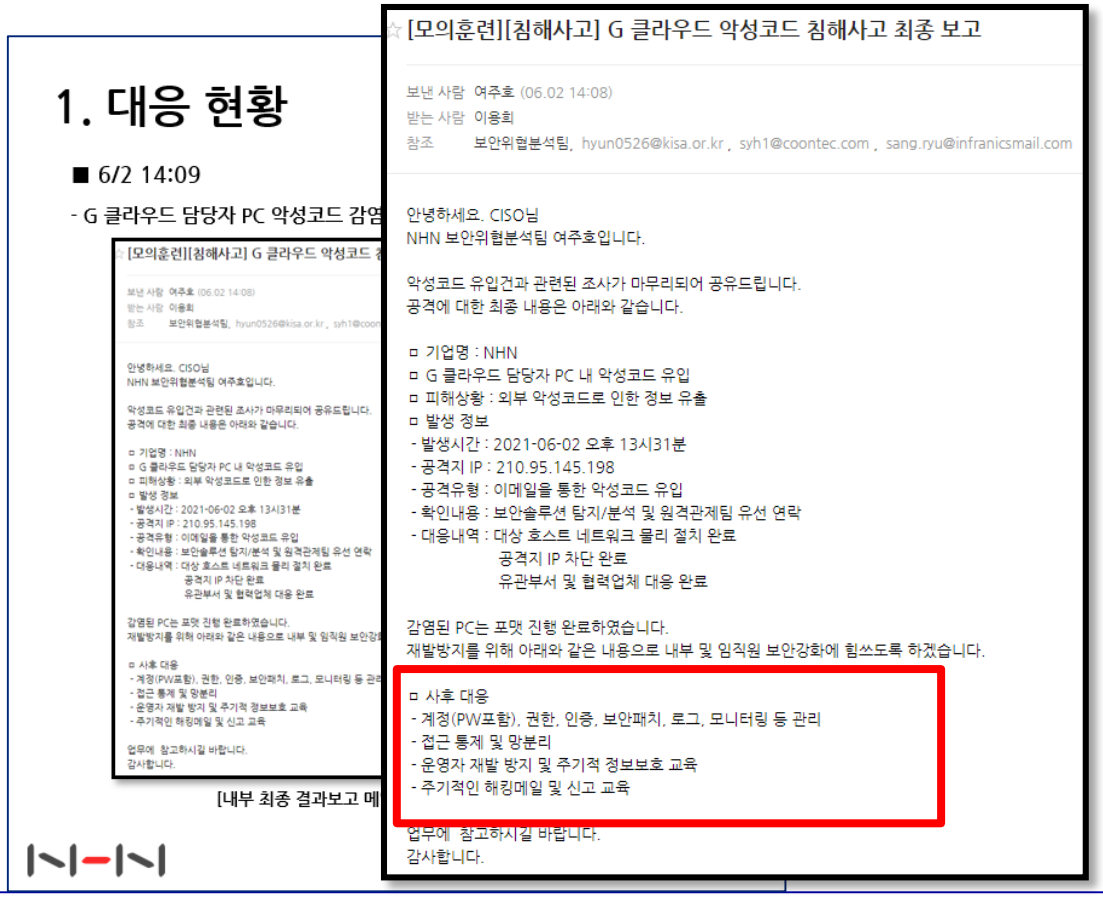
Description

- 공공 클라우드 침해사고 모의훈련 진행 시, 감독기관 신고 훈련 진행하고 있음

1-2. 침해사고 대응 절차 및 사후관리대책

증적

■ 공공 클라우드 침해사고 모의 훈련 증적 (5/5)



1. 대응 현황

■ 6/2 14:09

- G 클라우드 담당자 PC 악성코드 감염

[내부 최종 결과보고 메

[모의훈련][침해사고] G 클라우드 악성코드 침해사고 최종 보고

보낸 사람 여주호 (06.02 14:08)
받는 사람 이용희
참조 보안위협분석팀, hyun0526@kisa.or.kr , syh1@coontec.com , sang.ryu@infranicsmail.com

안녕하세요. CISO님
NHN 보안위협분석팀 여주호입니다.

악성코드 유입건과 관련된 조사가 마무리되어 공유드립니다.
공격에 대한 최종 내용은 아래와 같습니다.

▫ 기업명 : NHN
▫ G 클라우드 담당자 PC 내 악성코드 유입
▫ 피해상황 : 외부 악성코드로 인한 정보 유출
▫ 발생 정보
- 발생시간 : 2021-06-02 오후 13시31분
- 공격지 IP : 210.95.145.198
- 공격유형 : 이메일을 통한 악성코드 유입
- 확인내용 : 보안솔루션 탐지/분석 및 원격관제팀 유선 연락
- 대응내역 : 대상 호스트 네트워크 물리 절치 완료
공격지 IP 차단 완료
유관부서 및 협력업체 대응 완료

감염된 PC는 포맷 진행 완료하였습니다.
재발방지를 위해 아래와 같은 내용으로 내부 및 임직원 보안강화에 힘쓰도록 하겠습니다.

▫ 사후 대응
- 계정(PW포함), 권한, 인증, 보안패치, 로그, 모니터링 등 관리
- 접근 통제 및 망분리
- 운영자 재발 방지 및 주기적 정보보호 교육
- 주기적인 해킹메일 및 신고 교육

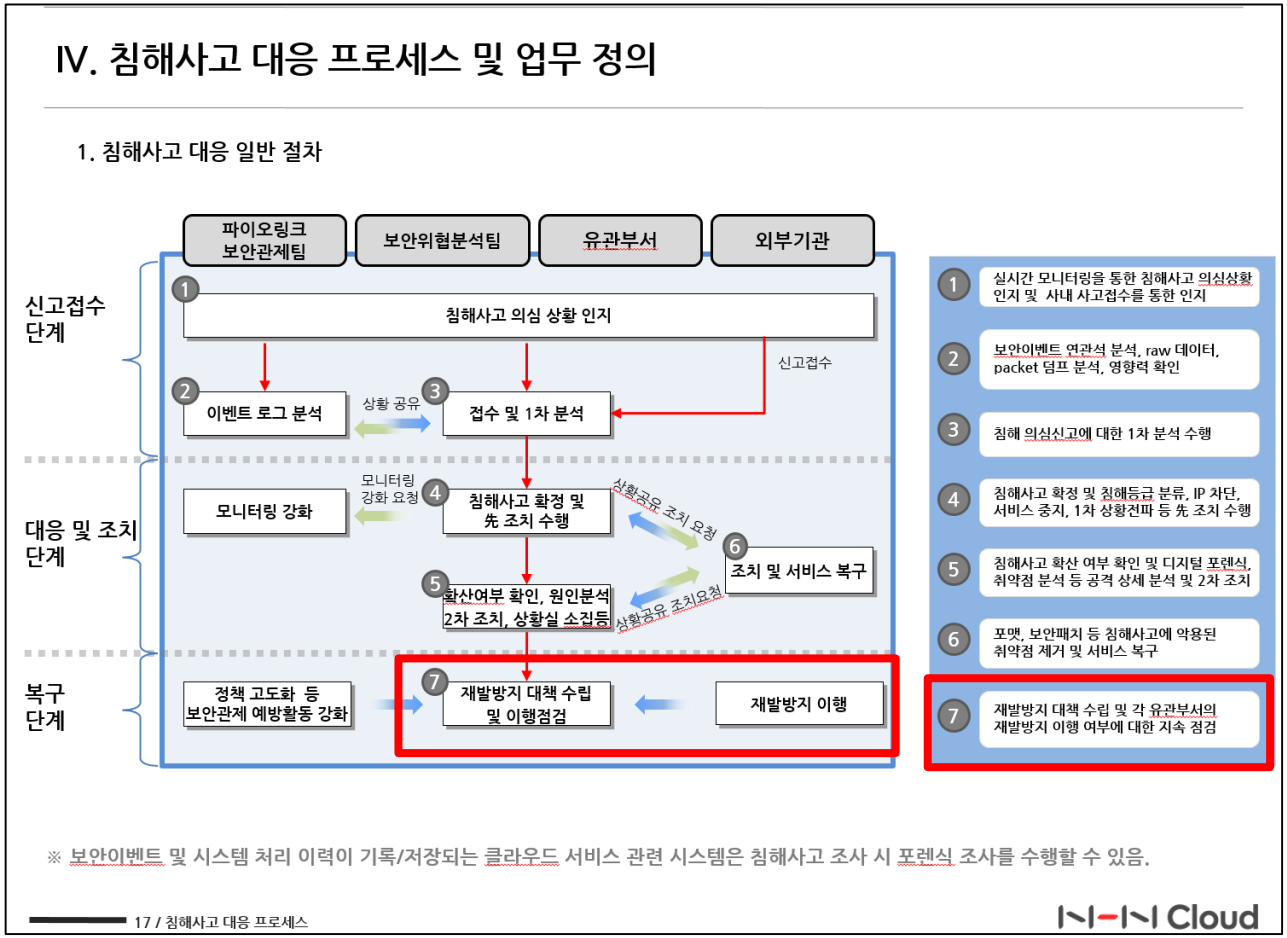
업무에 참고하시길 바랍니다.
감사합니다.

Description

- 침해사고 대응 완료 후, 재발방지 대책을 포함한 최종 내부 보고 절차도 포함하여 훈련 진행하고 있음

1-2. 침해사고 대응 절차 및 사후관리대책

증적



Description

- 재발방지를 위한 사고원인 분석하여 재발방지 대책을 수립하고 이행점검 절차를 갖추고 있음
- 각 유관부서에 재발방지 이행 여부에 대한 지속적인 점검 진행 절차를 갖추고 있음

NHN Cloud

1-2. 침해사고 대응 절차 및 사후관리대책

증적

IV. 침해사고 대응 프로세스 및 업무 정의

5. 침해사고 대응 프로세스 업무 정의

프로세스 명	침해사고 대응 및 사후조치 프로세스			
설명	심화 분석 -> 2차 대응 -> 2차 전파 -> 취약점 제거/복구 -> 재발방지수립 -> 결과보고			
시작 조건	피해 시스템 심화 분석 및 사고 대응			
종료 조건	결과보고 및 감독기관 신고			
업무 분류	입력물	설명	출력물	역할
심화분석	• N/A	• 침해사고 확산 여부 확인, 디지털포렌식 • 취약점 분석 등 공격 상세 분석	• 침해사고 보고서	• 보안위협분석팀
2차 대응	• N/A	• 심화분석을 통해 확인된 내용을 기반으로 추가 대응 - C&C IP 차단, 악성 바이너리 전수 조사, 백신 패턴 업데이트 등	• 침해사고 보고서	• 보안위협분석팀
복구 가이드	• 보고서	• 취약점 제거 및 서비스 복구를 위한 가이드	• 보고서, 메일	• 보안위협분석팀
취약점 제거	• 보고서, 메일	• 복구 가이드 기반 취약점 제거	• 메일	• 운영 및 개발 부서
서비스 복구	• 보고서, 메일	• 신규 서버 투입 및 서비스 구성 • 보안취약점 제거	• 메일	• 운영 및 개발 부서
재발방지 대책 수립	• N/A	• 재발 방지를 위한 후속 대응 방안 수립	• 보고서, 메일	• 보안위협분석팀
재발방지 대책 이행	• 보고서, 메일	• 각 운영 및 개발 부서는 수립된 재발 방지 대책 이행	• 메일	• 운영 및 개발 부서
이행 점검	• 조치 결과	• 취약점 제거 및 재발방지 대책 이행 내역 점검	• 보고서	• 보안위협분석팀
감독기관신고	• 보고서	• 감독기관에서 요구하는 항목 기준으로 사고보고서 작성 • 감독기관에 사고보고서 신고	• 감독기관 사고보고서	• 정보보호팀
이용자신고	• 보고서	• 법률에서 요하는 이용자 통지 게시 및 사고 발생 보고서 제공	• 공지, 메일	• 클라우드엔지니어링실
결과 보고	• N/A	• 최종 결과보고(재발방지 대책안 포함)	• 보고서, 메일	• 보안위협분석팀

21 / 침해사고 대응 프로세스

NHN Cloud

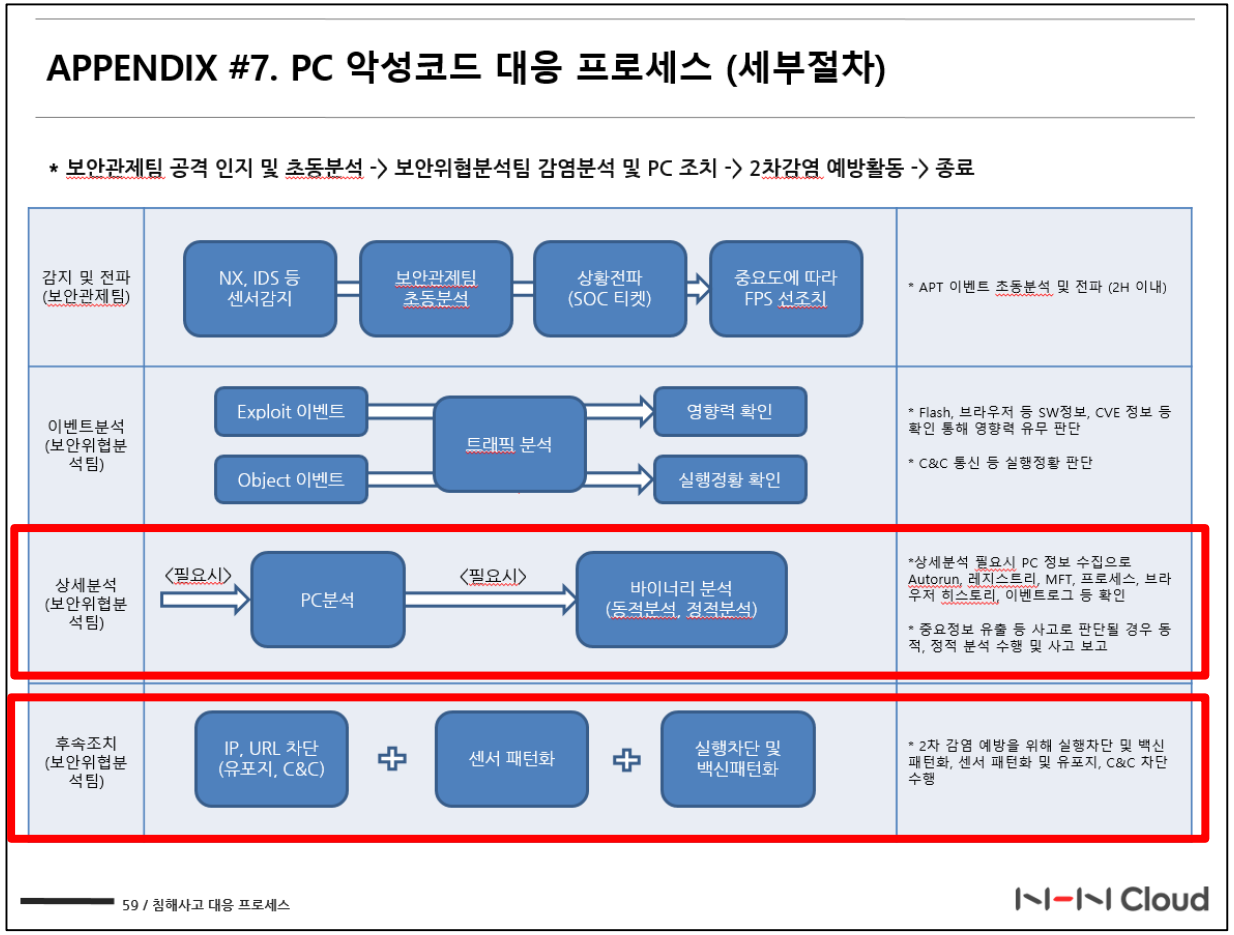
Description

- 재발방지를 위한 사고원인 분석하여 재발방지 대책을 수립하고 이행점검 절차를 갖추고 있음
- 각 유관부서에 재발방지 이행 여부에 대한 지속적인 점검 진행 절차를 갖추고 있음
- 재발방지 대책안을 포함하여 최종 결과보고
- 법률에서 요하는 방식으로 이용자 통지 게시

NHN Cloud

1-2. 침해사고 대응 절차 및 사후관리대책

증적



Description

- **2차 감염 예방을 위해 실행차단 및 백신 패턴화, 센서 패턴화 및 유포지, C&C 차단 수행**

1-2. 침해사고 대응 절차 및 사후관리대책

증적

■ DDoS 모의훈련 결과보고서

'21년도 KISA
상반기 모의훈련 (DDoS)

NHN
2021. 06. 04.

1. 훈련 개요

1.1 목적
: '21년도 KISA 상반기 DDoS 모의훈련을 통해 복구 단계별 ①보안시스템 정상동작 여부 ②프로세스 준수 여부 ③대응능력 ④위기관리 능력 4가지 항목에 대한 객관적인 점검을 수행하여 침해사고 대응체계에 대한 재점검 목적이 있음

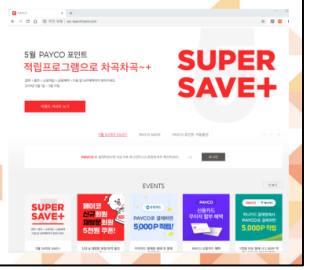
1.2 일시 : 2021년 05월 17일 ~ 2021년 06월 04일

1.3 주관기관 : 한국인터넷진흥원(KISA)

1.4 당사 훈련 참여인원 : NHN 인프라보안팀, 보안관제센터

1.5 DDoS 모의훈련 진행
1) 사전 모의훈련 기간인 24일 랜덤 시간에 KISA 에서 DDoS 트래픽 발생
2) 훈련 참가업체는 DDoS 트래픽 유입이 인지되면 KISA에 先 신고
3) 본 훈련(06월 07일) 사전 훈련에 대한 상세분석보고서 KISA 전달

1.6 훈련대상 기본정보
- Domain/IP : http://sec-test.nhnent.com (133.186.170.200)
- 서비스 종류 : web



3. 대응 현황

■ 본 훈련 타임라인 (05.24)
- 21/05/24 11:00 : DDoS 공격 발생 및 보안솔루션(자동방어전환)으로 차단
- 21/05/24 11:06 : 보안관제 DDoS 공격 탐지 유선연락수신
- 21/05/24 11:06 : 시스템운영조직 및 유관부서에 상황전파
- 21/05/24 11:07 : 시스템,네트워크 리소스 모니터링시 특이사항없음
- 21/05/24 11:19 : KISA에 공격상황 신고
- 21/05/24 11:21 : 보안솔루션 자동방어 종료
- 21/05/24 11:50 : DDoS 공격 추가 정보 및 대응 내용 전달 (DDoS 솔루션 자동 방어로 자체 방어)
- 21/05/24 11:55 : 상황 종료

Description

- DDoS 모의훈련은 KISA를 주관으로 인프라보안팀에서 상반기 또는 하반기에 진행하고 있음
- 2021년은 상반기(5~6월)에 DDoS 모의훈련진행 하였음
- 2022년은 하반기에 KISA DDoS 모의훈련 진행 예정