목차

로그의 정기적 검토 및 보고 3
정책에 따른 시스템 로깅 설정 3

로그의 정기적 검토 및 보고

점검목적 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악하기 위함

보안위협 로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움

점검방법 정기적인 로그 분석을 위하여 아래와 같은 절차 수립

Step 1) 정기적인 로그 검토 및 분석 주기 수립 1. utmp, wtmp ,btmp 등의 로그를 확인하여 마지막 로그인 시간, 접속 IP, 실패한 이력 등을 확인하여 계정 탈취 공격 및 시스템 해킹 여부를 검토 2. sulog를 확인하여 허용된 계정 외에 su 명령어를 통해 권한상승을 시도하였는지 검토 3. xferlog를 확인하여 비인가자의 ftp 접근 여부를 검토

Step 2) 로그 분석에 대한 결과 보고서 작성

Step 3) 로그 분석 결과보고서 보고 체계 수립

정책에 따른 시스템 로깅 설정

점검목적 보안 사고 발생 시 원인 파악 및 각종 침해 사실에 대한 확인을 하기 위함

보안위협 로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없음

점검방법 Step 1) vi 편집기를 이용하여 `/etc/rsyslog.conf` 파일 열기

```
#vi /etc/rsyslog.conf
```

Step 2) 아래와 같이 수정 또는, 신규 삽입

```
*.info;mail.none;authpriv.none;cron.none     /var/log/messages
authpriv.*                                   /var/log/secure
mail.*                                       /var/log/maillog
cron.*                                       /var/log/cron
*.alert                                      /dev/console
*.emerg                                      *
```

Step 3) 위와 같이 설정 후 RSYSLOG 데몬 재시작

```
#ps –ef | grep rsyslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/rsyslogd
#kill –HUP [PID]
```

서비스 데몬 종류

메시지	설명
auth	로그인 등의 인증 프로그램 유형이 발생한 메시지
authpriv	개인 인증을 요구하는 프로그램 유형이 발생한 메시지
cron	cron, at 데몬에서 발생한 메시지
daemon	telnet, ftpd 등과 같은 데몬이 발생한 메시지
kern	커널이 발생한 메시지
lpr	프린터 유형의 프로그램이 발생한 메시지
mail	메일 시스템에서 발생한 메시지
news	유즈넷 뉴스 프로그램 유형이 발생한 메시지
syslog	syslog 프로그램 유형이 발생한 메시지
user	사용자 프로세스 관련 메시지
uucp	시스템이 발생한 메시지
local0	여분으로 남겨둔 유형

메시지 우선순위

등급	메시지	설명
4 (높음)	Emergency [emerg]	매우 위험한 상황
3	Alert [alert]	즉각적으로 조치를 취해야 할 상황
2	Critical [crit]	하드웨어 등의 심각한 오류가 발생화 상황
1	Error [err]	에러 발생 시
0	Warnnig [warning]	주의를 요하는 메시지
-1	Notice [notice]	에러가 아닌 알림에 관한 메시지
-2	Information [info]	단순한 프로그램에 대한 정보 메시지
-3 (낮음)	Debug [debug]	프로그램 실행 오류 발생 시

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/%EB%A1%9C%EA%B7%B8_%EA%B4%80%EB%A6%AC

Last update: **2022/01/18 01:12**