Network Working Group
Request for Comments: 3227
BCP: 55
Category: Best Current Practice

D. Brezinski
In-Q-Tel
T. Killalea
neart.org

February 2002

증거 수집과 보관에 관한 지침
(Guidelines for Evidence Collection and Archiving)

요 약

Internet Security Glossary (RFC2828)에 정의된 것처럼 보안 사고(Security incident)란 시스템의 보안정책을 위반하거나 침해하는 보안 관련 시스템 이벤트를 말한다. 본 고는 시스템 관리자(administrator)에게 이러한 보안 사고와 관련된 증거의 수집과 보관에 관한 지침을 제공하고자 한다.

만약 증거 수집이 올바르게 이루어진다면, 공격자를 체포하는데 많은 도움을 줄 것이고, 증거로 인정받을 가능성이 클 것이다.

목 차

1. 소개(Introduction)

Internet Security Glossary (RFC2828)에 정의된 것처럼 보안 사고(Security incident)란 시스템의 보안정책을 위반하거나 침해하는 보안 관련 시스템 이벤트를 말한다. 본 고는 시스템 관리자(administrator)에게 이러한 보안 사고와 관련된 증거의 수집과 보관에 관한 지침을 제공하고자 한다. 보안 사고가 발생했을 때 매번 모든 시스템 관리자가 엄격하게 이 지침을 따라야 하는 것은 아니다. 그보다는 침입과 관련된 정보를 수집하고 보존하는 업무를 맡았을 때 수행해야 하는 것에 대한 지침을 제공하고자 하는 것이다.

시스템 관리자 입장에서 증거를 수집하는 일은 많은 노력을 필요한다. 최근에 운영체제의 재설치가 빨라지고 시스템을 원상태로 복구시키는 것이 용이해졌으며, 간단한 조작만으로 시스템 복구가 가능하다. 반면에 증거를 수집·보관하는 기술은 거의 진척되지 않았다. 더욱이 디스크와 메모리의 용량이 늘어나고 은닉기법과 추적 방지 기법이 발달하여 문제가 훨씬 어려워지고 있다.

만약 증거 수집이 올바르게 이루어진다면, 공격자를 체포하는데 많은 도움을 줄 것이고, 증거로 인정받을 가능성이 클 것이다.

이 지침은 증거 수집 절차를 제정하는 기초자료로 활용될 수 있으며, 사고 처리 절차를 만드는데 도움을 줄 수 있을 것이다. 증거 수집 절차를 만들었다면 적정한 지에 대해 법집행기관에 문의할 것을 권고한다.

1.1 용어 관례

본 고에서는 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119]에서 기술한 것처럼 '요구된다(REQUIRED), 반드시 해야 한다(MUST), 반드시 하지 않아야 한다(MUST NOT), 해야 한다(SHOULD), 하지 않아야 한다(SHOULD NOT), 할 수 있다(MAY)'라는 용어를 사용한다.

2. 증거 수집 처리 지침

- 해당 기관의 보안 정책을 준수하고 사고 처리와 법무를 담당하는 직원을 채용하라.

- 가능한 시스템이 정확하게 나타나도록 촬영하라.

- 상세히 기록하라. 여기에는 날짜와 시간이 포함되어야 한다. 가능하다면 자동으로 기록하라. (예를 들어 Unix에서 script 프로그램을 사용할 수 있다. 단 출력 파일이 증거가 들어 있는 매체에 생성되지 않아야 한다.) 기록이나 출력물에 대해서는 날짜를 기입하고 서명한다.

- 시스템 시간과 UTC 사이의 차이를 기록한다. Timestamp를 기록할 때마다 UTC를 사용했는지 로컬 타임을 사용했는지 표시한다.

- 조사시 취했던 모든 행위와 시간을 기록함으로써 (몇년 후에 있을) 증언에 대비하라. 상세하게 기록하는 것이 중요하다.

- 수집하는 데이터의 변형을 최소화 하라. 이것은 내용의 변경만을 의미하는 것은 아니며, 파일 또는 디렉토리의 접근 시간의 경신도 하지 않아야 한다.

- 변경될 외부 요인을 제거하라.

- 수집과 분석 둘 중 하나를 선택할 상황이면 먼저 수집하고 나중에 분석하라.

- 말할 필요조차 없지만 수행 절차는 실행 가능해야 한다. 사고 대응 정책처럼 절차 역시 특히 위기 상황에서 유용성이 있는지 검증되어야 한다. 가능하다면 절차는 속도와 정확성을 위해 자동화 되어야 한다. 체계적으로 되도록 하라.

- 수집 절차에 규정된 지침에 입각하여 각각의 기기에 대한 체계적인 접근이 채택되어야 한다. 종종 조사에 필요한 기기가 많아 속도가 아주 중요할 수 있고, 여러 명이 동시다발적으로 증거를 수집하는 것이 적합할 수 있다. 하지만 한 시스템에서는 단계적으로 수행해야 한다.

- 휘발성이 높은 것에서 낮은 순서로 진행하라. (아래의 휘발성 순서 참조)

- 시스템의 저장 매체에 대해서는 bit 레벨의 복제를 해야 한다. 포렌식 분석을 하려 한다면, 분석으로 인해 대부분 파일의 접근 시간이 변경되기 때문에 증거 복제본(evidence copy)의 bit 레벨 복제를 해야 한다. 증거 복제본으로 포렌식 분석을 하지마라.

2.1 휘발성 순서 (Order of Volatility)

증거를 수집할 때는 휘발성이 높은 것에서 낮은 순서로 진행해야 한다. 다음은 전형적인 시스템에서 휘발성 순서의 예이다.

- 레지스터, 캐쉬
- 라우팅 테이블, arp 캐쉬, 프로세스 테이블, kernel statistics, 메모리
- 임시 파일 시스템 (temporary file systems)
- 디스크
- 의심되는 시스템과 관련된 원결 로깅과 모니터링 데이터
- 물리적 설정, 네트워크 토폴로지
- 기록 보관 매체 (archival media)

2.2 주의 사항 (Things to avoid)

부주의한 행동으로 인해 증거가 너무 쉽게 파괴된다.

- 증거 수집이 종료되기 전까지는 시스템을 종료하지 않아야 한다. 많은 증거가 손실될 수 있고 공격자가 증거를 파괴하기 위해 시작/종료 스크립트 또는 서비스를 변경했을 수도 있다.
- 시스템 상에 있는 프로그램을 신뢰하지마라. 적절하게 위해 보호된 매체(아래 참조)에서 증거 수집 프로그램을 구동하라.
- 시스템 내에 있는 각종 파일의 접근 시간을 변경시키는 프로그램을 사용하지마라(예, tar 또는 xcopy)
- 단순히 네트워크를 필터링하거나 차단하기 위해 외부 연결을 제거할 때, 망이 차단되면 증거를 영구 삭제하는 자폭장치(deadman switches)가 구동될 수 있다.

2.3 프라이버시 고려 사항

- 소속 기관과 사법 체계의 프라이버시 관련 규정이나 지침을 고려하라. 특히 수색하는 증거과 함께 수집된 어떠한 정보도 그 정보에 정상적으로 접근할 수 없는 자에게 이용되지 않게 하라. 여기에는 사적 데이터 파일 뿐만 아니라 (사용자의 행동 패턴이 노

출될 수 있는) 로그 파일에 대한 접근도 포함된다.

- 강력한 사법 권한 없이 사람들의 프라이버시를 침범하지 마라. 특히 실제 사건과 관련된 충분한 징후가 없는 한, (개인의 파일 저장소와 같이) 정상적으로는 접근할 이유가 없는 영역으로부터 정보를 수집하자 마라.

- 사건 관련 증거 수집 단계에서 취한 행위가 소속 기관에서 수립한 절차에 부합하는지 확인하라.

2.4 법적 고려 사항

컴퓨터 증거는 다음을 만족할 필요가 있다.

- 허용(admissible): 법정에 제출되기 전에 해당 법률에 반드시 부합해야 한다.

- 인증(authentic): 증거물이 사건과 반드시 연관되어야 한다.

- 완벽(complete): 반드시 특정 한 측면이 아닌 전체에 대해 말할 수 있어야 한다.

- 신뢰(reliable): 증거의 수집과 후속 처리 과정에서 증거의 확실성(authenticity)과 진실성(veracity)이 의심될 수 있는 어떠한 여지도 반드시 없어야 한다.

- 이해(believable): 반드시 법정에서 쉽게 이해되고 수긍할 만 해야 한다.

3. 수집 절차

수집 절차는 가능한 상세해야 한다. 사고 처리 전체 과정과 마찬가지로 모호하지 않아야 하고, 수집 과정 동안 별도의 의사 결정할 상황이 최소화 되야 한다.

3.1 투명성

증거 수집을 위해 사용한 방법은 투명하고 재현할(reproducible) 수 있어야 한다. 사용한 방법은 정확하게 재현할 준비를 해야 하고, 외부 전문가에 의해 검증되어야 한다.

3.2 수집 방법

- 증거는 어디에 있는가? 사건에 연루된 시스템과 수집할 증거를 목록화 하라.

- 관련성 있는 것과 증거로 인정될 수 있는 것을 확정하라. 확실하지 않을 때는 부족한 것 보다는 많이 수집하라.

- 각각의 시스템에 대해서, 휘발성 순위에 관한 정보를 획득하라.

- 변경될 수 있는 외부 접근 수단을 제거하라.

- 휘발성 순서를 따라 수집하라. 5절에 기술되어 있는 도구를 이용하여 수집하라.

- 시스템 클럭(clock)의 편차(drift)를 기록하라.

- 수집 단계 동안 증거가 될 수 있는 것이 무엇인지 질의하라.

- 모든 단계를 기록하라.

- 참여한 사람을 잊지마라. 누가 있었고 무엇을 하고 있었는지, 무엇을 관찰했고 어떻게 반응했는지 기록하라.

할 수 있다면 수집 증거에 대해 checksum과 암호학적 서명을 생성해야 한다. 이것은 강력한 증거의 절차 연속성을 유지하기 쉽게 해 줄 것이다. 그렇게 함으로써 증거는 절대로 변경되지 않아야 한다.

4. 보관 절차

증거는 반드시 엄격하게 보호해야 한다. 또한 명확하게 기록함으로써 절차연속성이 유지되야 한다.

4.1 절차 연속성 (Chain of Custody)

증거의 발견 방법, 처리 방법을 비롯하여 증거에 관련된 모든 사항이 명확하게 기술할 수 있어야 한다.

아래의 내용들이 기록될 필요가 있다.

- 증거를 발견하고 수집한 자, 장소, 시간

- 증거를 취급하고 조사한 자, 장소, 시간

- 증거를 보관한 자, 보관 기간, 보방 방식

- 증거 관리가 변경되었을 때, 이송 방법과 날짜 (선적 번호 포함)

4.2 보관 방법과 장소

가능하다면 (어떤 어려움이 있는 저장 매체 보다는) 일반적으로 사용되는 매체를 기록 보관에 사용해야 한다.

증거에 대한 접근은 엄격히 통제되어야 하고, 명확하게 기록되어야 한다. 인가되지 않은 접근을 탐지할 수 있어야 한다.

5 필요한 도구

읽기만 허용되는 매체(예., CD)에서 포렌식 활동과 증거 수집을 할 수 있는 프로그램을 보유해야 한다. 취급할 운영체제 각각에 해당하는 도구를 사전에 준비해야 한다.

도구에는 다음과 같은 것들이 포함되어야 한다.

- 프로세스를 조사하기 위한 프로그램 (예, ps)
- 시스템 상태를 조사하기 위한 프로그램 (예, showrev, ifconfig, netstat, arp)
- bit-to-bit 복제를 할 수 있는 프로그램 (예, dd, SafeBack)
- checksum이나 서명을 생성할 수 있는 프로그램 (예, sha1sum, checksum-enabled dd, SafeBack, pgp)
- core image를 생성하고 조사할 수 있는 프로그램 (예, gcore, gdb)
- 자동적으로 증거를 수집할 수 있는 스크립트 (예, Ther Coroner's Toolkit[FAR1999])

모든 프로그램은 정적으로 링크(statically linked)되어야 하고, 읽기만 허용된 매체에 저장된 라이브러리 이외의 것을 요구하지 않아야 한다. 최근의 rootkit들은 Loadable Kernel Module을 통해 설치될 수 있기 때문에 사용한 도구가 시스템의 모든 면을 출력하지 않을 수도 있음을 염두에 두어야 한다.

사용한 도구의 확실성(authenticity)과 신뢰성(reliability)을 증언할 준비를 해야 한다.

6. 참고 문헌

[FAR1999] Farmer, D., and W Venema, "Computer Forensics Analysis Class Handouts", http://www.fish.com/forensics/

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", FYI 8, RFC 2350, June 1998.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

7. 감사의 글

We gratefully acknowledge the constructive comments received from Harald Alvestrand, Byron Collie, Barbara Y. Fraser, Gordon Lennox, Andrew Rees, Steve Romig and Floyd Short.

8. 보안 고려 사항 Security Considerations

이 문서는 보안 관련 문제를 다루었다.

9. 저자 연락처

Dominique Brezinski
In-Q-Tel
1000 Wilson Blvd., Ste. 2900
Arlington, VA 22209
USA

EMail: dbrezinski@In-Q-Tel.org

Tom Killalea
Lisi/n na Bro/n
Be/al A/tha na Muice
Co. Mhaigh Eo
IRELAND

Phone: +1 206 266-2196

EMail: tomk@neart.org

10. 저작권

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.