제목 : 윈도우 2000 보안 서버 점검 분석 리포트

아래 자료는 최근 윈도우 2000 보안 점검을 실시 후 알게 된 문제점과 해결에 대한 일반적인 내용입니다.
NTFAQ 에서는 계속 해서 새로운 정보와 보안에 대해서 정보를 제공 할 예정이며, 여러분이 알고 있는 정보가 있다면 제공 바랍니다.

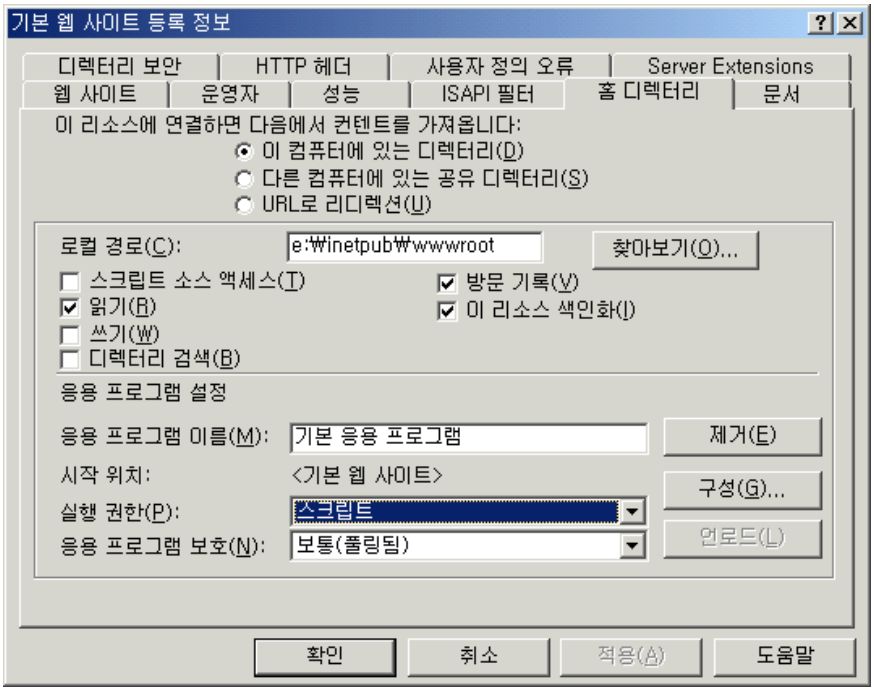
자료 출처 : NTFAQ (http://www.ntfaq.co.kr)

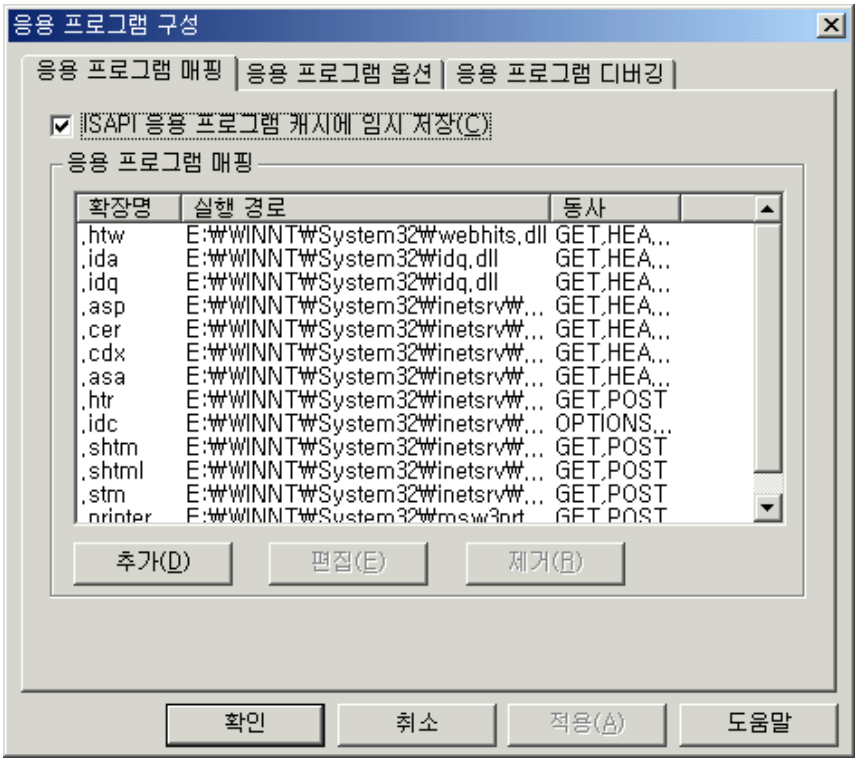
1. 웹 서비스

최근 가장 문제가 많이 제시되고 있는 것으로 많은 웹 서버 관리자에게 관심 1호로 자리 잡고 있다. 문제는 바로 관리자에게 있을 수도 있지만 또한 MS 에서 기본적으로 IIS 에는 많은 기본 기능을 내장 하고 있어 불필요한 응용프로그램에 대한 자료를 가지고 있다.
그에 대한 아무런 대책 없이는 관리 소홀로 문제를 접할 수 밖에 없다는 것이다.

문제점 들

- 기본 웹사이트 및 관리 웹사이트를 제거해라 - 이 이야기는 정말 무수히 많이 했던 사항이다. 그렇지만 쉽게 적용 되지 않는 것이 많다.
  참고 자료 : http://www.ntfaq.co.kr/security/view.asp?pid=44
- 불필요한 응용 프로그램 매핑을 제거 해라





위 그림에서 보시면 .idc , .htw, .htr , .idq 등에 대해서는 많은 논란이 있었던 것이며, 사실 대부분의 웹사이트에서 사용하지 않고 있다.

- 최근의 보안 패치를 적용 해라
  MS, IIS 통합 보안 패치 발표 : http://www.ntfaq.co.kr/news/view.asp?pid=68
- 코드레드 바이러스 패치
  http://www.ntfaq.co.kr/security/view.asp?pid=55

2. SMTP 서비스

SMTP 서비스에 문제는 릴레이 허용에 대한 외부 사용자가 쉽게 메일을 보낼 수 있다는 것입니다. 그러면서 서버에 부하 및 네트워크에 부하가 발생하여 내부 사용자가 원할하게 사용 할 수 없도록 하는 문제가 발생 할 수 있습니다.

상용 제품일 경우에는 SMTP 에 대한 릴레이 방지 기능이 제공이 되고 있지만 모든 것은 아니기 때문에 다소 문제의 소지를 갖고 있다.

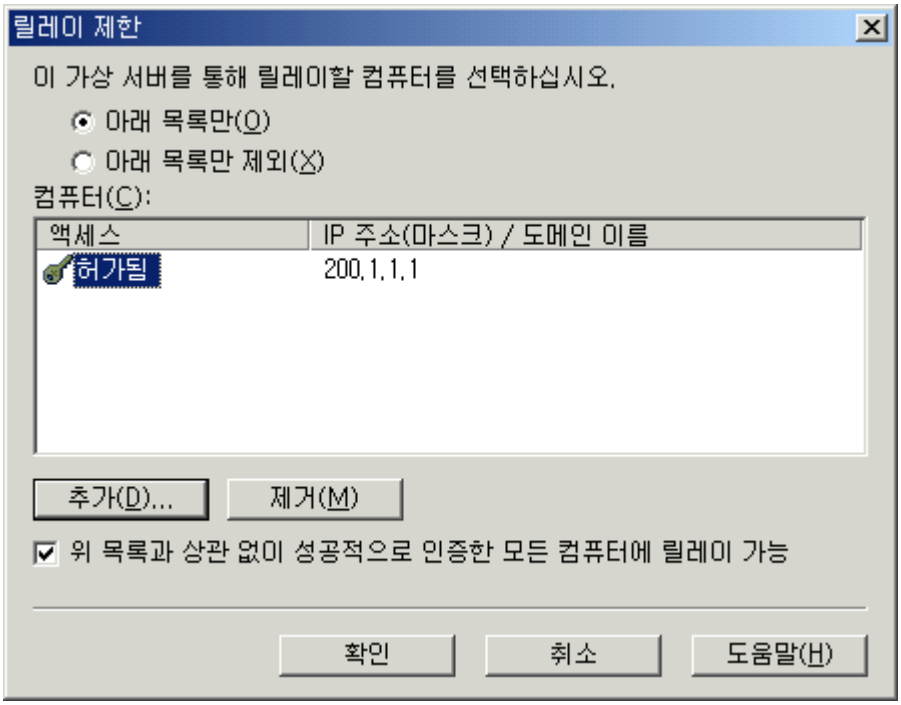
윈도우 NT/2000 사용자의 대부분은 EMWAC 을 사용하여 메일 서비스를 하고 있으며, 또한 IIS 에 있는 SMTP 서비스가 동작을 하고 있다.

그러면서 현재의 자신의 SMTP 서버가 어떻게 동작을 하고 있는지를 잊을 수도 있다는 것이다.

문제점과 해결 방법

- SMTP 서버가 릴레이 허용을 하고 있는지를 쉽게 테스트 할 수 있는 사이트가 제공이 되고 있다. 바로 적용 하길 바란다.
  http://www.ntfaq.co.kr/ntfaq_view.asp?faq_no=1900
- IIS 에 있는 SMTP 을 사용 시 인증된 사용자와 릴레이 방지 기능을 추가 하고자 해야 한다.
  인증된 사용자만 메일을 보낼 수 있도록 제공
  => http://www.ntfaq.co.kr/ntfaq_view.asp?faq_no=1691

  그외 릴레이 방지 기능을 제공 한다.



- EMWAC 을 사용 할 경우 필터링 및 플로그인을 설치 하여 적용 할 수 있다.
  http://www.ntfaq.co.kr/emwac/default.asp

그외 SMTP에 대한 문제점으로 일반적으로 SMTP 는 메일을 보낼 시 텍스트 형태를 그대로 보내어 전송을 하게 된다. 그렇게 될 경우는 쉽게 네트워크 캡쳐 프로그램으로 메일을 중간에 가로 챌 수 있는 사항이 발생하여 정보가 쉽게 노출 될 수 있다. 그러한 것을 현시점에서 해결 할 수 없다며 그에 대한 대책을 강구 할 수 있는 방법을 제시 해야만 한다.
예을 들어 SSL 적용을 할 수 있다. 그외 디지털 서명으로 작업을 할 수 있다.
이메일에 대해서는 S/MIME(Secure/Multipurpose Internet Mail Extensions)와 PGP(pretty Good Privacy) 의 방법은 전송과정에서의 수정을 막기 위해 디지털 서명 기능을 제공할 수 있으며 각각의 기능에 대해서는 부가 설명 하겠다.

- Secure Multipurpose Internet Mail Extensions (S/MIME) – S/MIME 확장은 공개/개인 키 쌍을 사용하여 메일 메시지를 암호화하고 디지털 서명하는 기능을 제공한다. S/MIME 를 구현할 때의 가장 큰 장점은 S/MIME 가 IETF 의 표준으로 보안적인 메일 기능을 제공하기 위하여 MIME 표준의 확장으로 디자인되었다는 점이다. S/MIME 는 S/MIME 를 지원하는 이메일 애플리케이션만을 필요로 한다. S/MIME 를 지원하기 위해 메일 서버에 필요한 요구사항은 없다..
- Pretty Good Privacy (PGP) – PGP는 메일 메시지를 암호화하고 디지털 서명하는 기능을 제공한다. S/MIME와 마찬가지로, PGP도 개인/공개 키 쌍을 사용하여 이 기능을 제공한다. S/MIME와 다른점은, PGP는 중앙의 표준 기구에 의해 통제되지 않는다는 것이다.

3. POP3

아직 이에 대한 정보는 많이 얻지 못했으며, 국내 POP3 에 대한 SSL 또는 전자 서명이 지원하는 프로그램은 상용 제품만 있을 것을 알고 있습니다.
좀 더 좋은 정보를 제공 하기 위해 차후 준비 하겠습니다.

4. MS SQL

SQL 에 있어서는 보안에 대한 중요성을 크게 가져야만 한다. 회사내의 모든 데이터가 보존하고 있기 때문이며, 그 만큼 주의를 요하지 않으면 쉽게 노출 될 경우가 많이 발생하기 때문이다.
보안에 가장 쉽게 노출 되는 점은 사용자 아이디와 패스워드가 거의 같게 구성 하고 있다는 점이다. 우습게 생각 하시리라 판단 되지만 거의 20% 정도가 그렇게 되어 있는 것을 볼 수 있다. 그외 패스워드의 복잡성이 거의 없기 때문에 쉽게 찾을 수 있다는 점도 유의 하시길 바란다.
SQL 에 대한 좀 더 유익한 정보와 자료를 곧 제공 하겠다.

패치 정보 : **SQL Server 7.0 (서비스 팩 1, 2, 3 적용 시스템) 패스워드 취약성에 대한 패치**

⇨ http://www.ntfaq.co.kr/security/view.asp?pid=23

5. DNS

일반적으로 DNS 에 대해서는 크게 문제시 될 것이 없다고 판단을 하고 있다. 가장 문제시 되고 있는 것은 영역에 대한 외부에서 쉽게 접근 할 수 있는 문제이다. 그것이 무엇이 문제냐고 생각 할수 있지만 내부에 있는 컴퓨터 정보를 외부에 공개 한다는 것은 앞으로 해킹하고자 하는 사용자에게 아주 쉽게 정보를 유출 하는 데 있다.
또는 최근 윈도우 2000 에서는 동적 업데이트가 가능 하며, 그러면서 발생 하는 것이 중간에 세션을 가로 채기 하여 직접 사용 하도록 하여 현재의 서비스가 다른 곳으로 이동 할 수

있게 구성 할 수 있다는 것이다. 그렇기 때문에 윈도우 2000 액티브 디렉터리을 사용 하여 DNS 보안을 좀 더 강구 하도록 유도 하고 있다.

DNS 에 대한 정보는 추후 좀 더 자세히 제공 하겠다.
참고 자료 : http://www.ntfaq.co.kr/security/view.asp?pid=10

6.사용자 계정 유출 문제

일반적으로 윈도우 NT/2000 에서는 사용자에 대한 정보를 외부와 통신을 하면서 공유 하고자 한다. 그래서 외부에서 관리 작업을 진행 할 수도 있기 때문이다. 하지만 그와 같은 작업을 진행 하면서 쉽게 사용자 계정 유출이 되고 있다는 것이다.
사실 얼마나 유출이 될까 생각 하지만 아마 그 내용을 보시면 심각한 우려가 아닐 수 없다. 이번 5개 업체에 대한 분석을 한 후 저 또한 이렇게 무방비 상태에서 사이트를 운영 할 수 있다는 것에 흥분 되면서 분석을 했던 적이 생각난다.

일반적으로 여러분의 컴퓨터에는 공유 된 폴더가 있다. 그 공유 된 폴더는 외부와 PRC 통신을 하면서 관리를 할 수 있는데 그런 공유 된 디렉터리르 아래와 같다.

- C$, D$
- IPC$
- ADMIN$

그외 추가된 공유 폴더 들이 있지만 일반적으로 위와 같은 경우는 기본적으로 관리폴더라고 해서 공유가 되어 있다. 제거도 가능 하지만 윈도우 2000 도움말을 보면 제거 하지는 말라고 한다. 서로간의 통신을 하기 위해서다.
그외 정확하게 무엇을 위해서 사용하는지는 판별이 나지 않았지만 꼭 필요하지 않는 경우는 제거 하는 것을 권한다.
혹시 아시는 분이 있고, 그에 대한 꼭 필요시 작업이 무엇인지를 알고 있다면 공개 해 주시길 바란다.
그외 여러 서비스에서 그에 대한 것을 추가로 제공 하는데 SNMP 와 같은 경우에는 자신의 컴퓨터 정보를 외부에 제공하는 역할을 한다. SMS 서버와 같이 작업을 진행 할 수 있는 것이지만 없을 경우는 꼭 필요 하지는 않다.

7. 맺은 말

여기까지가 1차 점검을 하면서 여러분에게 제공했던 내용입니다.
그 외 몇가지 기능들이 추가 되었지만 아직 정확한 원인에 대한 해결을 하지 못하고 있는 것이 많이 있다는 것이다.
그에 대한 NTFAQ 에서는 계속해서 공부를 해서 여러분에게 제공을 약속 드리겠습니다.
곧 2차 점검 업체를 선발을 진행 할 예정입니다.
많은 참여 바랍니다.

NTFAQ 에 보안 채널을 참고 하시면 최신 패치 및 정보를 제공 하고 있습니다.
=> http://www.ntfaq.co.kr/security/default.asp

홍순성