

정보보호 체크 가이드 - by 바다란 (p4ssion@naver.com)

보안의 강화는 기업을 위한 중요한 활동임과 동시에 개인 정보 유출을 막기 위한 최선의 방책이다. 2005년에 급속도로 증가한 개인정보 유출용 악성코드 및 정보유출을 위한 다양한 위험성들이 늘어나 특별히 보안에 관심을 두지 않는 한 일반직원의 입장에서는 문제가 그리 간단한 것만은 아니다.

매번 연말이나 특정한 이슈가 발생할 때면 보안 회사들에서 보안 강화를 위한 방침을 발표하고는 한다. 이런 방침에 항상 빠지지 않는 것이 “보안 패치의 활성화 “ , “백신의 업데이트 철저 “ 와 같은 항목이다.

왜 보안 패치가 중요하고 백신이 중요한 것인가? 개인은 물론 기업, 산업 기반에도 중요한 영향을 미치는 요소로 매번 강조되는 이유는 무엇일까?

완벽한 운영체제란 없으며 시일이 지나면서 필요가 변함에 따라 사용환경은 변화하고 진보하기 마련이다. 또한 이전에는 생각지 못했던 새로운 기술과 개념들을 낚거나 부족한 토대 위에 올려 놓으려다 보면 고려하기 힘든 부분들도 존재를 하게 되며 새로운 취약성이 발견이 되는 경우도 발생이 된다. 따라서 대부분의 운영체제를 만드는 곳에서는 발견된 문제의 중요성에 따라 보완하는 작업을 진행 한다. 2005년 연말에 발생하였던 wmf 취약성의 경우 Microsoft의 정식 패치 발표일이 아님에도 불구하고 일주일 가량 시간을 당겨서 보안상의 위험성을 보완하는 패치가 발표가 되었다. 문제의 심각성이 그만큼 심각한 사안이라는 경고가 세계 각국의 전문가들로부터 제기 되어 Microsoft도 무시하기는 어려웠으리라.

위험한 개인사용자

앞서 wmf 취약성을 예로 들었지만 wmf 취약성이 발표된 지 만 24시간도 되지 않아 취약성을 공격하는 코드가 발견이 되었다. 개념적인 코드차원에서 실제 공격을 하고 권한 획득을 할 수 있는 부분까지 발전이 되었으며 2~3일이 지난 후에는 메신저 (MSN , Yahoo ...)를 통해 감염이 되는 워 폼 형태로도 출현하였으며 앞으로도 계속될 문제로 발전이 될 것이다. 또한 지난 해를 뜨겁게 달구었던 중국발 해킹은 현재도 진행형 이다. 유명하거나 사용자의 방문이 많은 사이트는 집중적인 공격의 대상이 될 수 있을 것이다. 왜 이런 많은 문제들이 발생을 하고 있고 이런 문제들의 해결책은 대체 무엇이 있을까? 여러 가지 문제의 원인이 있을 수 있지만 특히 몇 가지만을 헤아리면 안전하지 못한 프로그래밍 기법의 일반화 (보안의 고려가 없었던 시절의 프로그래밍) , 악성코드를 통한 정보유출 및 감염에 민

감하지 못한 무관심과 같은 두 가지 유형을 대표적으로 들 수가 있다. 프로그래밍 기법의 일반화를 제외한 무관심의 경우는 개인 사용자의 위험 노출이 매우 높음에도 불구하고 인지를 못하고 있어서 향후에도 계속 발생될 수 있는 문제라 할 수 있다.

공격 기법도 계속 변화하고 있으며 2005년 12월에 발견된 wmf 취약성을 이용한 중국발 해킹도 연이어서 발생을 하고 있는 상황이다. 공격하는 자들은 계속 발전하고 있고 변화하고 있으나 사용자들의 인식은 그에 미치지 못하고 있다. 더욱이 기업의 인식도 그리 많이 나아지지 못하고 있는 상황이다.

취약성이란 무엇인가? 그렇다면 앞으로도 취약성은 증가하고 Zeroday 위협은 증가할 것인가?. 대답은 증가할 수 밖에 없다 이다.

일반 사용자들에게는 익숙하지 않으나 전문가들에게는 날마다 쌓이는 보안 관련 취약성 및 위험성 정보가 존재한다. 전 세계에서 개발되고 이용되는 Application의 수치는 얼마나 될 것인가? 또 오늘 당장 개발 되거나 내일 새롭게 발표되는 제품의 수는 얼마나 될까?. 매우 많은 수치의 제품이 현재 사용 중이며 또 개발 중일 것이다. 앞으로의 세상에서는 더욱 더 많은 제품들을 사용하게 될 것이 명확한 사실이다.

한 가지 더욱 명확한 사실은 이 모든 제품들이 완벽하지는 않다는 점이다. 서로간의 정보 교류를 하는 이상 그 어떤 제품도 100% 안전한 제품은 존재하지 않을 것이다. 보다 더 안전한 구성을 통해 안전성을 높다는 것은 보장할 수 있어도 100%를 보장할 수는 없을 것이다.

아래와 같은 사이트 (정말로 많은 취약성 관련 사이트 들이 존재한다.) 에는 날마다 취약성에 관련된 신규 정보들이 올려져 온다. 공격코드들이 작성 되어 올려지기도 한다.

```
?2006-01-24 : Eterm LibAST Configuration Engine --X Option Local Buffer Overflow Exploit
?2006-01-16 : VERITAS NetBackup Volume Manager Daemon Remote Buffer Overflow Exploit
?2006-01-15 : Microsoft Windows Metafile (WMF) "SetAbortProc" Remote File Download Exploit
?2006-01-12 : eStara SoftPhone 3.0.x SIP Packets Handling Remote Buffer Overflow Exploit
?2006-01-07 : BlueCoat WinProxy "Host:" Header Handling Remote Command Execution Exploit
?2006-01-05 : PHP 4.x "mysql_connect" Function Named Pipe Handling Buffer Overflow Exploit
?2006-01-05 : Microsoft Windows 2000 Kernel APC Local Privilege Escalation Exploit (MS05-055)
?2006-01-01 : Mozilla Firefox "InstallVersion.compareTo()" Remote Command Execution Exploit
?2005-12-31 : Microsoft Windows Metafile (WMF) "SetAbortProc" Remote Code Execution Exploit
?2005-12-28 : Microsoft Windows / Internet Explorer WMF Remote Code Execution Exploit
?2005-12-24 : phpBB <= 2.0.17 "signature_bbcode_uid" Remote Command Execution Exploit
?2005-12-23 : PHP-Fusion 6.00.x "rating" Parameter Handling Remote SQL Injection Exploit
?2005-12-20 : Eudora Qualcomm WorldMail "LIST" Command Remote Buffer Overflow Exploit
?2005-12-19 : Mailenable Enterprise "EXAMINE" Command Remote Buffer Overflow Exploit
?2005-12-19 : Microsoft IIS Malformed HTTP Request Handling Remote Denial of Service Exploit
?2005-12-15 : Watchfire AppScan QA HTTP Response Handling Remote Buffer Overflow Exploit
?2005-12-12 : Mozilla Firefox "InstallVersion.compareTo" Remote Buffer Overflow Exploit
?2005-12-09 : Lyris ListManager "/read/attachment" Script Remote SQL Injection Exploit
?2005-12-08 : HP OpenView Network Node Manager Remote Command Execution Exploit
?2005-12-08 : Oracle 9i Database XDB HTTP Authentication Remote Stack Overflow Exploit
?2005-12-01 : Microsoft Windows MSDTC Service Remote Code Execution Exploit (MS05-051)
?2005-11-30 : Microsoft Windows Metafile (WMF) "mntNoObjects" Remote Exploit (MS05-053)
?2005-11-30 : QNX Realtime Operating System (RTOS) "phgrafx" Local Buffer Overflow Exploit
english/services
```

< 취약성 정보가 게시되는 해외 웹 사이트 >

보안 관련된 논의 및 메일링을 통해 전 세계의 전문가들과 의견 교환을 할 수 있는 bugtraq 은 취약성의 흐름 및 빠른 정보 수집을 위해 필수적인 사이트 이다.

The screenshot shows the BugTraq mailing list interface. The main content area displays a list of posts, including:

- [SECURITY] [DSA 951-1] New trac packages fix SQL injection and cross-site scripting 2006-01-23
- CAID 33778 - CA iGateway Content-Length Buffer Overflow Vulnerability 2006-01-23
- BlackWorm technical information 2006-01-24
- [FLSA-2006:152845] Updated perl packages fix security issues 2006-01-24
- [eVuln] Pixelpost Photoblog XSS Vulnerability 2006-01-23
- BlackWorm naming confusing [CME entry now available] 2006-01-24
- [USN-246-1] imagemagick vulnerabilities 2006-01-24
- LibAST 0.7 Release Fixes Security Vulnerability 2006-01-23
- Ege Internet Web Desing Remote Command Exucetion 2006-01-28
- Multiple vulnerabilities in CommuniGate Pro Server 2006-01-28
- [CORRECTIONS AND ADDITIONS] Jazbb v1.1.00 Cross-Site Scripting 2006-01-28
- The WorldsEnd.NET - Free Ping Script, written in PHP (2 vulns) 2006-01-23
- Azbb v1.1.00 Cross-Site Scripting 2006-01-23

On the right side, there are several advertisements:

- FREE Webinar on Penetration Testing**
- VeriSign SSL Certificates secure e-commerce transactions.
- Website Security: Tokens, Smart Cards & USB Dongles Try it or buy 5-user All-in-one Kit
- Security Audit Info: Summaries from 100s of top sources, Updated daily by our research staff
- security vulnerabilities: Deploy patches in Microsoft Windows and Linux OS. Web-based software
- IT Security: Firewall and...

< 취약성 관련된 메일링이 교환되는 Bugtraq >

발견되는 취약성은 일반직원들이 아는 것 보다 매우 많으며 그 복잡성도 높을 수 밖에 없다. 따라서 개개인이 직접적으로 대처를 하고 대응을 한다는 것은 어려울 수 밖에 없으며 기업 단위의 대처에도 영향을 미칠 수 밖에 없다. 한 기업에 있어서 공식적으로 사용하는 Application 외에 직원들이 사용하는 모든 Application을 알 수 있을까?. 또 취약성이 발견 되는 Application의 문제에 대한 해결책을 제때에 적용 할 수 있을까?

아마 해결책을 찾는 것도 전체의 Application (공식적인 것과 비공식적인 것 모두 포함) 목록을 체계화 하는 것은 일정 규모 이상의 기업에게는 매우 어려울 것이다. 현 상황에서의 조직 차원에서의 완벽한 해결책은 없으며 보다 더 안전할 수 있도록 꾸준히 노력하는 것 외에는 해결책이 존재하지 않는다.

기업의 보안 및 보다 큰 공동체의 안정성을 위한 보안 노력도 모두가 개인 및 구성원의 적극적인 노력으로부터 비롯된다. 구성원의 노력 없이는 전체적인 보안태세 및 보안에 대한 노력들도 독을 무너뜨리는 틈새와 같이 의미 없어 지는 것이 현재의 환경이다.

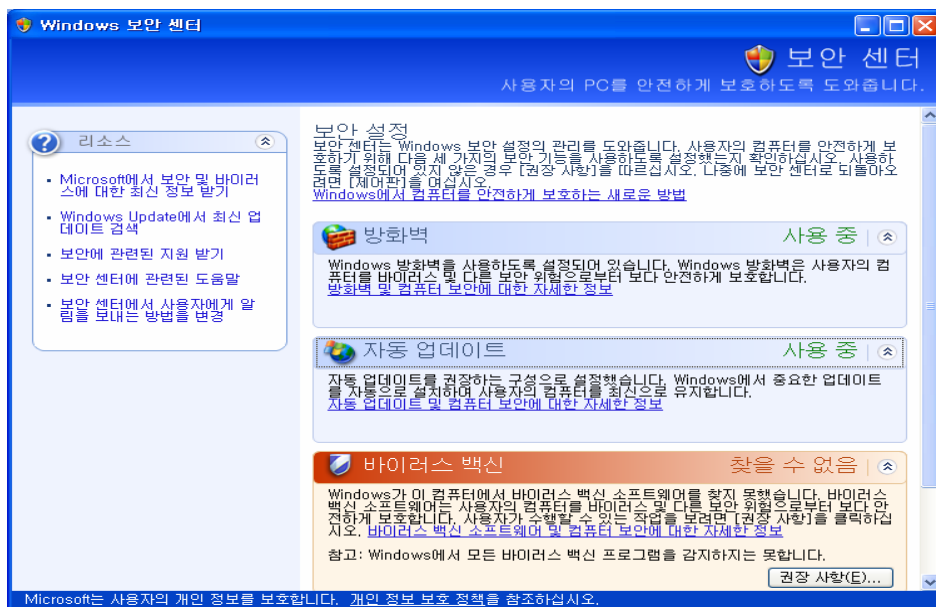
자 복잡하다. 명확한 것은 문제가 있고 이 문제를 풀기 위해서는 개개인도 노력을 해야 한다는 점이다. 현재 발생되고 있는 웜이나 악성코드가 얼마나 지독한가?. 웜에 감염되면 주변의 다른 사용자들에게도 동일한 웜이 감염을 시키고 종래에는 IT 회사라면 운영 하는 시스템에 피해를 주거나 업무에 지장을 받을 정도로 영향을 미칠 수 있다. 또 외부에서 자신

의 PC를 컨트롤 하여 중요 문서를 가져 간다면 어떻게 될 까?. 이제는 단 하나의 문제점만으로도 충분히 피해를 입을 수 있는 시대이므로 많은 주의가 필요하고 관심이 필요하다. 그러나 모두가 전문가가 될 필요는 없을 것이다. 각자 전문분야는 따로 있을 것이므로..

정보보호 실천을 위한 가이드에는 어떠한 것들이 있을 지 알아 보자.

먼저 가장 근본적인 원칙이며 한 달에 한번 정도의 간격으로 체크가 되어야 하는 부분은 다음과 같다. (일반 유저를 대상으로 하며 대부분 Windows 환경에서 문제가 발생하므로 Windows를 기준으로 하였다.)

1. XP의 경우 Service Pack 2를 설치한다. - 보안 기능을 활성화 시키고 여기에서 Windows Firewall 의 기능도 적절히 이용하도록 하자.



2. Windows Update의 정기적인 설정 - 경험상 점심시간 무렵이 적당한 것 같았다. 새벽시간으로 설정할 경우 PC를 계속 켜두어야 된다.
3. 바이러스 백신의 사용 - 일단 맹신 하지는 말자. 다만 알려진 위협 및 바이러스를 제거해 줄 수 있는 수단이라는 점에서 이용은 필수
4. 비정상적인 계정이 있거나 프로그램이 실행 되고 있는지 검수를 한다. - 계정의 경우는 사용자 관리 메뉴에서 프로그램은 Regedit 혹은 레지스트리 관련 프로그램에서 시작 프로그램 항목을 체크해 보면 된다. - 주위 사람에게 상의 하면 충분히 이행 가능하다.

5. 운영체제의 보안 - 불필요한 서비스 제거 (TCP/IP Netbios Helper 및 Messenger 서비스등 ...) 를 통한 위협요인 제거 - 불필요한 서비스 항목은 전산 담당자에게 문의 혹은 인터넷 상에서 충분한 가이드를 얻을 수 있다.
6. 계정의 보안 강화 및 공유 설정의 강화 - 공유 디렉토리의 경우 읽기 권한 만 주고 접근 권한 및 사용자를 최소화 한다. 로그인 계정의 경우 6자 이상의 ID 및 6~7 자리를 지니는 Password를 사용하도록 한다. 주기적인 변경도 고려 하여야 한다.

* 계정 보안 관련: 외부 인터넷 사이트에 사용자 계정을 만들 때에도 자신만의 규칙을 지니고 생성하는 것이 좋다. 동일한 ID/ 동일한 PW로 거의 대부분의 웹 사이트에 가입을 한다는 것은 자신의 모든 정보를 내 주는 것과 동일한 행위이다. 가입 하는 모든 사이트의 보안성을 장담 할 수 있을까? 하루에도 수백 개의 사이트가 웹사이트 변조를 당하는 상황에서 과연 내 정보는 지켜 질 수 있을까? 사용자 개인의 특성에 맞는 규칙이나 자신만의 방식으로 몇 개의 부류로 나누어서 사용을 한다면 보다 안전한 서핑이 될 것이다.

한달 단위의 이행 대책의 경우 주위의 조언이나 전문가에게 도움을 요청해야 하는 사안들이 많이 있으나 주간 및 일간 단위의 체크는 좀 더 다른 방향으로 접근을 수행하면 된다.

주간 단위의 검사 항목으로는 다음과 같은 점을 유념하면 될 것이다.

1. 바이러스 감염 기록의 확인 및 바이러스 백신의 업데이트 일자 확인 - 감염 기록의 확인은 매우 중요하다. 자신이 인지하지도 못하는 상황에서 감염이 되었다면 추가적인 위험이 있을 수 있으므로 좀 더 주의를 기울여야만 한다.
2. Windows Update 서비스의 정상적인 동작 확인 - 정상적으로 설정이 되었는지 여부를 확인 하는 것이 좋다. 주일의 시작인 월요일이나 금요일에 한번쯤 Update에 시간을 두고 여유를 지니는 것도 좋은 방식이며 자동 설정을 통해 다운로드 발생시마다 처리하는 것이 가장 좋다.
3. 비정상적인 PC의 움직임 - 외부에서 조정을(Mouse 혹은 키보드) 하고 있거나 내부의 데이터에 인위적인 손상 등이 있을 때에는 전산담당자와 상의를 해보는 것이 좋다. 그 문제가 사소한 것이든 오해이든 이런 문제에 대해서는 확실히 하는 것이 좋다.

일반 보안 회사 및 신문지상에서 가장 많이 언급되는 일간 단위의 검사 항목은 다음과 같다.

1. 바이러스 프로그램의 가동 및 업데이트 설정- 모니터링 가능상태 유지
2. 윈도우 보안 패치의 설정 및 설치
3. E-mail 프로그램 사용시의 수/발신인의 확인 및 첨부 파일에 대한 백신의 검사 및 주의
4. P2P 프로그램 사용시의 백신을 이용한 검사 준수
5. 메신저 프로그램을 통한 링크 및 URL에 대한 확인 (최근 WMF 공격이 URL Link 를 이용한 공격이 많이 발생하고 있다.)
6. 공유 권한의 제한
7. 웹사이트 서핑시의 Active X 설치 유형과 같은 악성코드에 대한 주의 - 최근 유형이 매우 많으므로 주의를 기울여야 함.

간략하게 살펴 보면 위와 같은 검사 항목을 준수 한다면 전체적인 안정성을 높이는데 도움이 될 수 있을 것이다. 큰 방향성 아래에서 하위 항목을 준수하는 것이 강조 되어야 하며 왜 이런 노력들이 필요한 지에 대한 이해가 선행이 되어야 만 한다.

향후에도 많은 위험들이 있을 것이고 DMB 혹은 WiBro 등 수많은 변화 속에서 또 얼마나 많은 발전이 있을 것인가? 그 발전이 기술의 진보이든 위험의 진보이든 간에...

p4ssionable security explorer!

나를 숨쉬게 하는 것은 열정이 9할. 바다란?