경제혁신 3개년 계획 — 경제의 틀을 바꾸면 미래가 달라집니다.

미래창조과학부	**보 도 자 료**	http://www.msip.go.kr

2015. 3. 6.(금) 조간(온라인 3. 5. 12:00)부터 보도하여 주시기 바랍니다.

문의 : 사이버침해대응과 최병택 과장(02-2110-2890), 고창휴 사무관(02-2110-2924)

미래부, 공유기 보안 강화대책 발표

- 공유기 제조·유통, 통신망 접속·이용 등 단계별 보안 강화 -
- 취약점 발견시 보안업데이트 체계 구축 -

□ **미래창조과학부**(장관 최양희, 이하 미래부)는 최근 공유기의 보안 취약점을 악용한 침해사고가 발생하고, **공유기의 보안 취약점에 대한 위험성이 증가**함에 따라 **「공유기 보안 강화대책」을 마련**하여 3월부터 시행한다고 밝혔다.

□ 공유기*는 **일반 퍼스널컴퓨터(PC)와 달리**, 보안패치, 백신 프로그램 등 **별도의 보안 대책이 마련되어 있지 않아** 사이버 공격에 무방비 상태로 노출되었다는 지적이 많았다.

* 하나의 인터넷 회선을 여러대의 인터넷 단말기(PC, 인터넷전화, 스마트폰 등)가 함께 사용할 수 있도록 지원하는 네트워크 장비

○ 공유기는 **저가의 네트워크 장비**로 **별도의 보안인증이 없이** 제작·유통되고 있으며, **제조업체**는 그간 생산원가 상승을 이유로 **보안 조치에 소극적**이었다.

○ 특히, 대다수의 **공유기 이용자**는 **제품 생산시** 보안설정이 **취약한 상태인 아이디/패스워드(ID/PW)*를 그대로 사용**하고 있으며, 추가적인 보안설정 및 관리의 필요성도 인식하지 못하고 있는 실정이다.

* 공장 출고시 부여된 ID/PW : admin/admin, root/password 등

□ 구체적으로, 지난해 11월 발생한 에스케이(SK)브로드밴드 **침해사고 원인을 조사한 결과**(붙임 1), **악성코드에 감염된 사설공유기**가 디엔에스(이하, 'DNS') 대상 디도스(이하, **'DDoS') 공격에 악용**된 것으로 나타났으며, 지난해 4월부터 **공유기 DNS**를 **변조**하여 **파밍 사이트 접속 및 개인정보 탈취**를 유도하는 사례가 발생하는 등 공유기를 통한 사이버공격이 늘어나고 있다.

○ 금년 1월, **박근혜 대통령은 "사이버공격이 어떤 공격보다도 위협적이라는 인식하에 사이버공격에 대한 대비를 철저히 하라"**고 강조한 바 있다.

□ 이에 미래부는 공유기에 대한 보안을 강화하기 위하여 **미래부, 통신사, 공유기 제조업체 및 한국인터넷진흥원 협력***을 통해 다음과 같은 **「공유기 보안 강화대책」을 마련하여 3월부터 추진**하기로 하였다.

* 참여 사업자 : 통신사 3사(KT, SK브로드밴드, LGU+), 공유기 제조업체 (EFM네트웍스, NetTop C&C, 애니게이트이앤씨, 다보링크, 블레스정보통신, 네티스코리아, D-Link, 디지털존, TP-LINK 등)

첫째, 통신사와 제조업체간 협력을 통해 **통신망에 접속·이용중인 '사설 공유기의 실시간 모니터링 시스템'**을 **금년 6월중에 구축**하여 운영하기로 하였다.

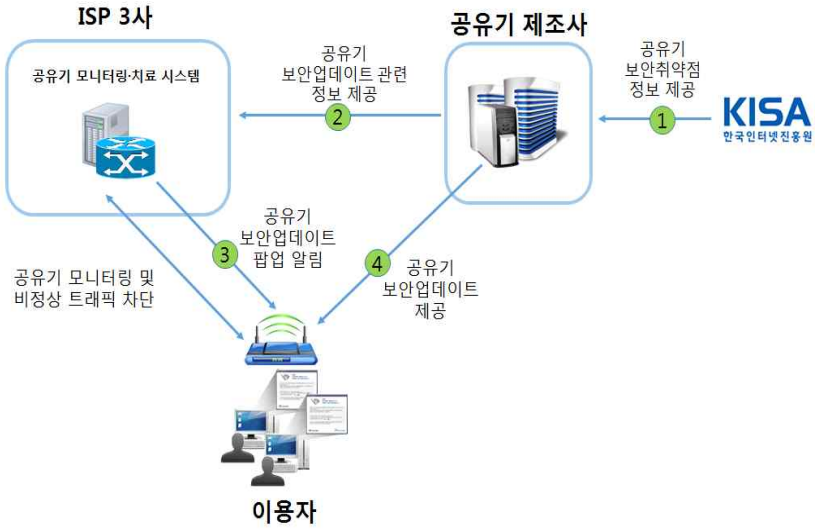
○ 이를 통해 통신사들은 사설 공유기에서 발생하는 **비정상적인 트래픽을 모니터링**하고, **DDoS 공격 등 사이버공격**이 의심되는 경우 **접속**을 **차단**하는 등 침해사고에 신속하게 대응한다는 방침이다.

둘째, 미래부는 공유기 **신규 취약점**을 **적극 발굴**하여 **보완프로그램을 개발**하는 한편, **취약점의 신속한 보완·조치**를 위해 **통신망을 통한 사설 공유기 보안 업데이트 체계**를 **금년 7월**부터 **구축·운영하고, '공유기 자가 점검도구' 개발·보급도 추진**하기로 하였다.

※ 통신사가 제공하는 공유기는 보안취약점 발생시 중앙에서 일괄 보안업데이트 가능

○ '공유기 **보안취약점 신고포상제**'와 **주기적인 공유기 보안준수 이행실태 조사**를 통하여 **신규 취약점을 신속하게 발굴**하는 한편, 취약점이 발견된 공유기에 대해서는 **해당 제조업체**로 하여금 **보완프로그램 개발**을 **요청**하여 **취약점을 개선**해 나갈 계획이다.

○ 또한, **통신사**는 보안패치가 필요한 **이용자에게 팝업 창으로 보안 업데이트를 안내**하고, 이용자 동의하에 **인터넷망을 통해 취약점 보완프로그램이 보다 쉽게 업데이트**가 이루어질 수 있도록 할 예정이다.



○ 아울러, **이용자가 공유기의 보안 취약점을 스스로 점검**하고, **보안 설정**을 쉽게 할 수 있는 '**공유기 자가 점검도구***'를 개발·보급토록 관련 제조업체에 지속적으로 독려해 나갈 계획이다.

* EFM네트웍스(ipTIME 제조사)는 '15. 6월까지 공유기 자가 점거도구를 개발 예정

셋째, 공유기의 **DNS 변조**를 통한 **파밍 피해를 최소화**하기 위해 **해외 파밍용DNS* 탐지 및 차단**을 강화하기로 하였다.

* DNS가 변조된 공유기 이용자를 해외 파밍사이트로 안내하는 DNS 서버

○ 이를 위해 **주요 통신사와 한국인터넷진흥원이 공동**으로 '**해외 파밍용DNS 탐지 시스템**'을 **금년 6월**까지 **구축**하고, 파밍용 악성코드에 감염된 공유기 **이용자가 해외 파밍사이트로 유도·접속되지 않도록 해외 파밍용DNS를 차단**할 계획이다.

넷째, **보다 안전한 공유기의 제조·유통**을 위하여 '**공유기 제품 생산시 적용할 보안가이드**(붙임 2)'**를 제정하여 3월중 제조업체에 권고**하고, 유통중인 공유기에 대해 **주기적인 실태조사를 통해 보안가이드의 이행 여부를 확인·점검**하는 등 공유기 보안 조치 이행에 관한 행정지도를 지속적으로 추진한다.

○ 보안가이드에는 ① 관리자 페이지의 비밀번호를 제품별 다르게 설정, ② 외부 접속포트(Telnet, FTP 등) 비활성화, ③ 무선구간 암호화(WPA2) 기본설정, ④ 펌웨어 업데이트 등 공유기 제품 생산시 주요 보안 고려사항을 포함하고 있다.

다섯째, **공유기 보안위협**에 대한 **이용자의 인식을 제고**하고, **안전한 공유기 이용문화를 조성**하기 위하여 7월 정보보호의 달 행사의 일환으로 '**취약한 공유기 클린 캠페인**'**을 전개**할 예정이다.

○ **공공장소, 카페 등 인구밀집 지역**에서 공유기 보안이용 실태 조사를 실시하여 **현장에서 맞춤형 취약점 점검 및 기술 지원**을 제공할 계획이다.

○ 또한, 전문가 및 이용자들이 **공유기 취약점 신고포상제에 참여토록 적극 홍보**하고, **보안업데이트 방법 및 이용수칙*** 등도 지속적인 홍보를 통해 **공유기 보안설정을 생활화**할 수 있도록 유도해 나갈 예정이다.

* 공유기 이용수칙 : ▲공유기 관리자 페이지 비밀번호 설정 ▲ 공유기의 무선랜(Wi-Fi) 비밀번호 설정 ▲공유기 원격관리 기능 사용안함 ▲공유기 펌웨어 최신 버전 유지 ▲제공자가 불분명한 무선랜 이용하지 않기

□ **미래부 정보화전략국장**은 "**금번 공유기 보안 강화대책** 마련으로 **공유기를 보다 안전하게 이용할 수 체계**를 갖추었지만, **공격자(해커)가 끊임없이 보안 취약점을 찾아 악용**할 수 있어 **신속한 취약점 발굴 및 개선 등을 통해 지속적으로 대처**할 계획이다"고 밝히면서, "침해사고로부터 피해를 최소화하기 위해서는 **이용자의 보안설정 이행이 무엇보다 중요**하므로, 아이디/패스워드 변경 등 **주기적으로 보안설정을 해야 한다**"고 당부했다. 끝.

< 붙임 1 >

SK브로드밴드 침해사고 민관합동조사단 조사결과

□ 사고 개요

o 사고 일시 : '14.11.29(토), 10:45 ~ 12:09(84분)

o 사고 내용 : SK브로드밴드 **DNS(서초IDC, 동작IDC) 대상 DDoS 공격(3차례)**

- 1차 10분(10:45~10:55), 2차 14분(11:17~11:31), 3차 8분(12:01~12:09) 등 **총 32분**
- 서초IDC는 1차 공격 이후 1시간(11:00~12:07) 가량 라우터 장애(CPU 과부하) 발생

o 피해 내용 : 인터넷 **접속 중단(1·3차 공격, 18분) 및 지연(68분)**

- 2차 공격(14분)은 보안장비 IPS에서 차단되었으며, 라우터 장애시에도 해당 트래픽이 타 국사로 우회되어 서비스 중단은 없었으나, 복구과정에서 일부 접속 지연 발생

□ 사고원인 분석결과

o **DDoS 공격 기법** : flooding 공격기법 중 **'Random Subdomain*' 공격**

* 존재하지 않는 도메인 주소를 공격 목표 DNS에 다량으로 질의

- **다량의 패킷을 전송**하여 **과부하**를 일으키는 방식으로 DDoS 공격
- DNS(서초, 동작)로 **약 1,500만pps 규모의 패킷이 유입**되어, **SKB의 처리용량**(580만pps(IPS 2대 기준))을 **약 2.5배 상회**하여 장애 발생

o **보안 취약점 및 악성코드 감염·전파**

- **(취약점)** 원격에서 공유기 운영체제에 접속할 수 있는 **23번 포트(Telnet)가 열려져 있고, 쉬운 ID/PW**가 설정된 공유기에 악성코드를 감염
  ※ 감염된 공유기는 ID/비밀번호가 admin/admin, root/password 등으로 설정
- **(감염전파)** 악성코드는 **주변 다른 취약한 공유기**를 **스캔**하여 **전파**
  ※ 공격사용 IP(좀비 공유기) : 총 1,633대
- (조치) 악성코드 명령조종지(13개)·유포지(2개) 등 15개 IP 접속 차단(12. 1)

□ 재발방지 대책 : SK브로드밴드의 'DDoS 대응체계 강화'(~'15.6월)

o DNS 서버 및 DNS전용 IPS 증설, DNS 존(Zone) 확대, 클린존 용량 확대 등

< 붙임 2 >

공유기 제품 생산시 적용할 보안가이드

1. 고객이 공유기 보안설정을 쉽게 할 수 있도록 직관적인 사용자 인터페이스와 매뉴얼을 제공하여야 한다.
2. 공유기 관리자 페이지에 대한 원격 접속을 기본으로 허용하지 않아야 한다.
3. 공유기의 관리자 페이지 접속 시에는 ID와 비밀번호(PW) 없이 접속할 수 없도록 하여야 한다.
4. 무선(Wi-Fi) 인증시에도 비밀번호 없이 접속할 수 없도록 비밀번호 사용을 기본 설정하여야 한다.
5. 무선 암호화 방식은 보안강도가 높은 WPA2가 기본 설정되도록 하여야 한다.
6. 공유기의 관리자 페이지 및 무선 인증 시 최초 ID와 PW의 경우 제품마다 다르게 하거나 비밀번호를 설정하여야 공유기를 사용가능하도록 하여야 한다.
7. 모든 비밀번호(최초, 변경 모두 해당)는 영문, 숫자, 특수문자를 포함하여 8자 이상으로 하여야 하며, 비밀번호 설정 창에도 복잡도가 높은 문구로 설정하도록 사용자에게 안내하여야 한다.
8. 불필요한 외부 접속 포트나 Telnet, FTP 등의 서비스는 비활성화한다.
   반드시 필요할 경우에는 비밀번호를 설정하여야 사용 가능하도록 한다.
9. 고객 지원 목적의 접속 포트를 제거하고 필요하다면 접근 IP 제한 등 추가적인 보안 조치 방안을 마련한다. 유지 보수 등을 위해 공유기에 백도어 기능을 포함하지 않도록 한다.
10. 모든 관리자 페이지는 인증 후에 접근할 수 있도록 세션 인증 등을 구현한다. 세션 인증 구현 시 예측 가능한 세션 ID 값을 사용하지 않도록 한다.
11. 관리자 페이지에서 시스템 명령어 실행 기능을 제공하지 않도록 한다. 다만, 반드시 필요할 경우 지정한 특정 명령어만 실행하도록 제한한다.
12. 공유기 펌웨어 업데이트가 발생하는 경우 사용자가 인지할 수 있는 방안을 강구하여야 한다.
13. 공유기 펌웨어 업데이트 시 파일 고유 해시값을 비교하여 변조 여부에 대한 무결성 검증을 실시할 수 있도록 한다. 무결성 인증 시 SHA-256 이상의 암호화 알고리즘을 사용하도록 한다.