과학기술정보통신부 보도자료

보도시점 2025. 12. 29.(월) 14:00 (2025. 12. 30.(화) 조간) 배포 2025. 12. 29.(월) 10:00

KT, LGU+ 침해사고 최종 조사결과 발표

[KT 침해사고 조사 결과]

▷ (조사 방식) △KT의 펨토셀 관리 전반 보안 실태 조사, △경찰 압수물 정밀 분석 △KT 전체 서버(약 3.3만대) 대상 악성코드 감염여부 점검

▷ (피해 현황) △무단 소액결제 피해 규모 368명, 2.43억원, △감염서버 총 94대, 악성코드 총 103종, △22,227명 IMSI, IMEI, 전화번호 유출

▷ (사고 원인 및 문제점) 펨토셀 보안 관리 부실로 인한 불법 펨토셀의 접속 허용, 통신 암호화 해제, 정보보호 활동 미흡 등의 문제 확인

▷ (재발방지 대책) 펨토셀 보안관리 강화, 통신 암호화 설정 강화, 보안장비 도입 및 로그 보관기간 연장, CISO 중심 거버넌스 체계 확립 등

[KT 이용약관 상 위약금 면제 규정 적용 여부]

▷ 펨토셀 관리 부실로 불법 펨토셀이 언제, 어디서든 KT망에 접속할 수 있었으므로, KT는 이번 침해사고에 과실이 있는 것으로 판단

▷ KT는 펨토셀 보안 관리를 통해 전체 이용자에게 안전한 통신서비스를 제공해야 할 의무를 다하지 못한 것으로 판단

▷ 과기정통부는 KT 과실이 발견된 점, KT가 계약상 주된 의무를 다하지 못한 점 등을 고려 시, 위약금 면제 규정이 적용 가능하다고 판단

[LGU+ 침해사고 조사 결과]

▷ (조사 개요) 익명 제보자의 침해사고 정황 제보에 대한 사실관계 파악

▷ (조사 결과) 허위자료 제출 및 서버폐기 등으로 인해 확인 불가능

▷ (조치 사항) LGU+에 대해 위계에 의한 공무집행 방해로 수사 의뢰

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 “과기정통부”)는 KT, LGU+ 침해사고에 대한 민관합동조사단(이하 “조사단”)의 조사 결과 및 KT의 이용약관 상 위약금 면제 규정에 대한 검토 결과를 12월 29일(월)에 발표하였다.

Ⅰ. KT 침해사고 원인분석 및 재발방지 대책

지난 9.8일, KT는 소액결제 피해자의 통화기록을 분석한 결과 KT에 등록되지 않은 불법 기기가 내부망에 접속한 사실을 발견하고, 한국인터넷진흥원(원장 이상중, 이하 “KISA”)에 침해사고를 신고하였다.

과기정통부는 국민의 금전 피해 발생 등 사고의 중대성, 공격 방식에 대한 면밀한 분석이 필요하다고 판단하여 9.9일 조사단을 구성하여 피해현황 및 사고원인 등을 조사하였다.

조사단은 ▲불법 펨토셀에 의한 소액결제 및 개인정보 유출사고, ▲익명의 제보에 따른 KT 인증서 유출 정황(프랙보고서, 8.8), ▲KT가 외부업체를 통한 보안점검 과정에서 발견한 서버 침해사고 등 3건에 대한 조사를 통해 KT의 보안 문제점 등 사고원인 분석 및 재발방지 대책을 마련하였다.

1. 조사 방식

조사단은 KT가 보유·관리하고 있는 펨토셀 전반에 대한 보안 실태를 조사하고, 불법 펨토셀로 인한 침해사고가 발생한 경위와 사고 원인을 파악하기 위해 경찰청과 협력하여 피의자로부터 확보한 압수물을 정밀 분석하는 한편, KT 통신망 테스트베드를 활용하여 펨토셀 운영 및 통신 암호화 관련 문제점을 파악하였다. 아울러, 불법 펨토셀로 인한 개인정보 유출, 무단 소액결제 등 피해 규모도 검증하였다.

또한, KT 전체 서버(약 3.3만대)를 대상으로 6차례에 걸쳐 악성코드 감염 여부에 대해 강도 높은 조사를 시행하고, 감염서버에 대해서는 포렌식 등 정밀분석을 통해 정보유출 등 피해 발생 여부를 파악하였다.

2. 침해사고 피해현황

< 불법 펨토셀에 의한 침해사고 >

조사단은 KT가 지난 10.17에 발표한 피해 규모에 대한 산출 방법*의 적절성 및 산출과정에서의 피해 누락 여부 등의 검증을 거쳐, 불법 펨토셀로 인한 침해사고로 22,227명의 가입자 식별번호(IMSI**), 단말기 식별번호(IMEI***), 전화번호가 유출되었고, 368명(777건)이 무단 소액결제로 2.43억원 규모의 피해가 발생하였음을 확인하였다.

* '24.8.1~'25.9.10 동안 KT 기지국 접속기록 4조 3백억건, 통신결제대행 기록 1억 5천만건, 음성·SMS 기록 978억건, 고객문의(VOC) 30만건 이상의 데이터 분석을 통해 산출

** **I**nternational **M**obile **S**ubscriber **I**dentity : 유심 내 저장되며, 사용자 식별 시 사용

*** **I**nternational **M**obile **E**quipment **I**dentity : 휴대전화 기기 식별 시 사용

이는 KT가 산출한 피해 규모와 일치하는 수치이다. 다만, 통신결제 관련 데이터가 남아있지 않은 기간('24.7.31 이전)에 대해서는 추가 피해 여부를 확인하는 것이 불가능하였다.

< 악성코드 감염에 의한 침해사고 >

조사단은 KT 전체 서버 점검 및 감염서버 포렌식을 통해 총 94대 서버에 BPFDoor*, 루트킷 등 악성코드 103종이 감염되었음을 확인하였다.

* **B**erkeley **P**acket **F**iltering + Back**Door** : 중국 국가 배후 해커그룹(Redmenshen)이 만들었다고 알려졌으며, '22.5월 대외공개 후 일반 해커들의 변종 공격 증가

KT가 '24.3월~7월 기간에 감염서버를 발견했음에도 정부에 신고 없이 자체 조치한 악성코드 감염서버는 총 41대*로, BPFDoor 4종, 웹셸 16종, 원격제어형 악성코드 6종 등 26종을 확인하였다. 조사단은 SK텔레콤 침해사고 조사 당시('25.4.20.~'25.7.4.) KT의 BPFDoor 감염 여부를 점검하였으나, KT가 '24년에 이미 악성코드 삭제 등 조치를 취하여 BPFDoor 등의 악성코드가 발견되지 않았다.

* 중간조사 발표('25.11.6) 당시 43대 감염으로 발표했으나 추가조사 결과 2대 서버는 SQL인젝션 및 스캐닝 공격시도만 발생하였으며, 악성코드는 미감염

또한, KT가 자체적으로 실시한 외부업체 보안점검('25.5.22.~9.15.)에서 침해흔적이 발견되었다고 확인된 서버 및 이와 연계된 서버에 대한 조사단의 포렌식 과정에서 53대 서버 감염 및 루트킷 39종, 백도어 36종, 디도스 공격형 2종 등 77종의 악성코드를 확인하였다. 이 중 루트킷은 BPFDoor와 같은 은닉형 악성코드*로, 화이트해커가 프랙에 제보한 보고서에 언급된 바 있다.

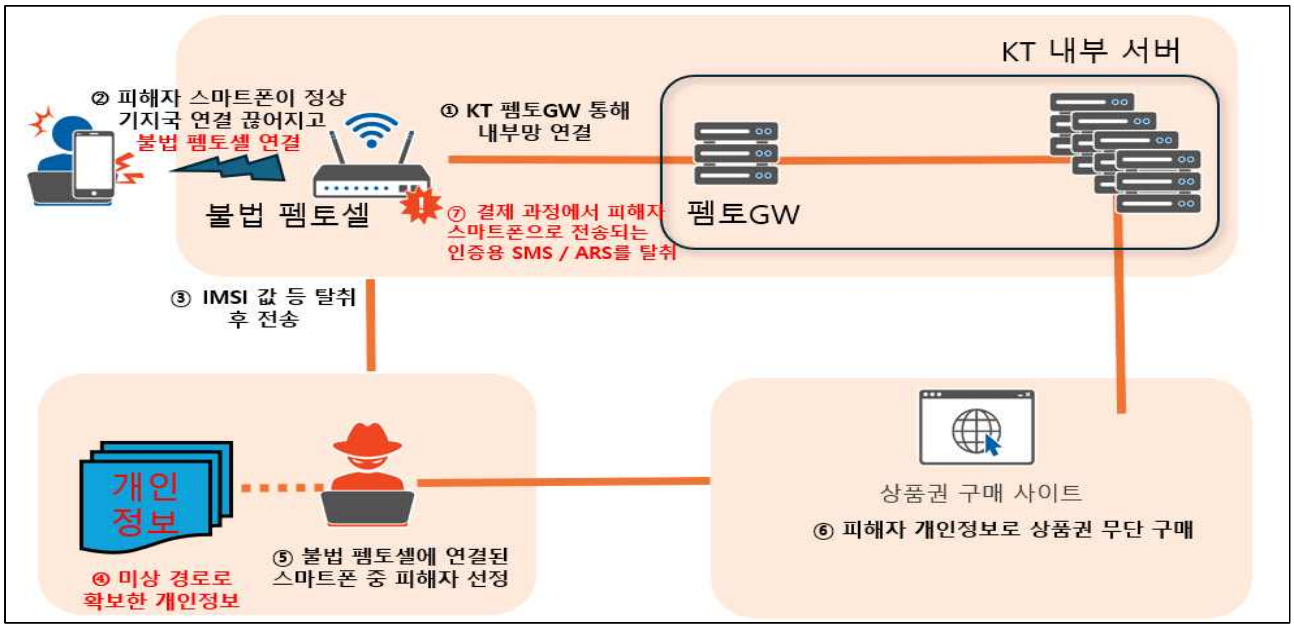
* (루트킷) 시스템 운영체제의 핵심(커널) 부분을 조작하여 악성코드 파일을 은닉
(BPFDoor) 공격자의 명령제어 신호를 전달받을 때만 악성코드 활성화

확인된 악성코드 정보는 피해확산 방지를 위해 백신사, 경찰청, 국정원 등 주요 민간·공공기관에 즉시 공유하고, 악성코드 점검 가이드를 보호나라 누리집(www.boho.or.kr)을 통해 배포하였다.

정보유출과 관련하여, 조사단은 일부 감염서버에 개인정보(이름, 전화번호, 이메일 등)가 저장되어 있으나, 정밀 분석 결과 로그기록이 남아있는 기간에는 유출 정황이 없는 것을 확인하였다. 다만, KT는 서버 내부 파일접근 및 실행, 오류 등 동작을 기록하는 시스템로그 보관 기간이 1~2개월에 불과하고 주요 시스템에 대해 방화벽 등 보안장비 없이 운영하여 로그 분석에 한계가 있었으며, 로그기록이 남아있지 않은 기간에 대한 유출 여부를 확인하는 것이 불가능하였다.

3. 사고 원인 분석

< 불법 펨토셀에 의한 침해사고 >



조사단은 경찰이 피의자로부터 확보한 불법 펨토셀을 포렌식 분석한 결과, 해당 펨토셀에 KT망 접속에 필요한 KT 인증서 및 인증서버 IP 정보와 해당 셀을 거쳐가는 트래픽을 캡쳐하여 제3의 장소로 전송하는 기능이 있음을 확인하였으며, 이를 바탕으로 사고 원인을 파악하였다.

공격자는 먼저 불법 펨토셀에 KT의 펨토셀 인증서, KT 서버 IP 주소 정보를 복사하여 KT 내부망에 접속하였다. 그 후, 불법 펨토셀이 강한 전파를 방출하도록 하여 정상적인 기지국에 접속했던 단말기가 불법 펨토셀에 연결되도록 하고 해당 셀에 연결된 피해자의 전화번호, IMSI, IMEI 등의 정보를 탈취하였다.

공격자는 불법 펨토셀에서 탈취한 정보를 미상의 경로로 취득한 개인정보(성명, 생년월일, 휴대전화번호)와 결합하여 피해자를 선정하고, 피해자의 개인정보로 상품권 구매 사이트를 접속하여 상품권 구매 시도 및 피해자에게 전달되는 ARS, SMS 등 인증정보를 불법 펨토셀을 통해 탈취하여 무단 소액결제를 한 것으로 판단된다.

< 악성코드 감염에 의한 침해사고 >

웹셸 및 BPFDoor 악성코드의 경우 인터넷 연결 접점이 있는 서버의 파일 업로드 취약점을 악용하여 서버에 웹셸을 업로드하고 BPFDoor 등의 악성코드를 확산시킨 것으로 추정된다.(‘22.4.2.~’24.4.19.에 걸쳐 감염)

루트킷, 백도어 등의 악성코드에 대해서는 감염 시점 당시 방화벽, 시스템 로그 등 기록이 남아있지 않아 공격자의 침투 방법 등을 판단하는 것이 불가능하였다.(‘23.3.11.~’25.7.4.에 걸쳐 감염)

4. 문제점 및 재발방지 대책

조사단은 조사를 통해 KT의 정보보호 체계에 문제점을 발견하고 재발방지 대책을 마련하였다.

< 펨토셀 관리 및 내부망 접속 인증 관련 문제점 >

조사단은 KT의 펨토셀 관리 체계가 전반적으로 부실하여 불법 펨토셀이 KT 내부망에 쉽게 접속할 수 있는 환경이었음을 확인하였다. 먼저, KT에 납품되는 모든 펨토셀 제품이 동일한 제조사 인증서를 사용하고 있어 해당 인증서를 복사하는 경우 정상 펨토셀이 아니더라도 내부망의 인증서버로부터 KT 인증서를 받아 KT망에 접속이 가능함을 확인하였다. 또한, KT 인증서의 유효기간이 10년으로 설정되어 한 번이라도 KT망에 접속한 이력이 있는 펨토셀은 지속적으로 KT망에 접속할 수 있는 문제점을 발견하였다.

또한 KT는 내부망에서의 펨토셀 접속 인증과정에서 타사 또는 해외 IP 등 비정상 IP를 차단하지 않고 있었고, 펨토셀 제품 고유번호, 설치 지역정보 등 형상정보가 KT망에 등록된 정보인지 여부에 대해서도 검증하지 않았다.

아울러, 조사단은 펨토셀 제조사가 펨토셀에 탑재되는 셀ID, 인증서, KT 서버 IP 등 중요정보를 보안관리 체계 없이 펨토셀 제작 외주사에 제공하였고, 펨토셀 저장 장치에서 해당 정보를 쉽게 확인 및 추출하는 것이 가능함을 확인하였다.

조사단은 불법 펨토셀 접속 차단을 위해 통신3사의 신규 펨토셀 접속을 전면 제한(9.10)하는 한편, KT에 ▲펨토셀이 발급받은 통신사 인증서 유효기간 단축(10년 → 1개월, 9.10), ▲펨토셀이 KT 망에 접속 요구 시 KT 유선 IP 외에는 차단(9.23), ▲펨토셀이 KT 망에 접속 시 형상정보를 확인 및 인증(10.3~), ▲펨토셀 제품별 별도 인증서 발급(11.5) 등을 조치토록 하였다.

⇒ **(재발방지 대책)** KT는 제조사가 펨토셀 생산 시 인증서, 통신사 인증서버 IP, 셀ID에 대한 보안정책을 마련하여야 한다. 또한 펨토셀의 시큐어부팅 기능 구현, KT 인증서버 IP 주기적 변경 및 대외비 관리, 불법 펨토셀 접속에 대한 이상징후 모니터링 및 탐지·차단 등 기술적 조치를 취하고, 펨토셀 보안 취약점 발굴·조치를 위한 화이트해커와의 협력 등 지속적 관리체계를 구축·운영해야 한다.

< 통신 암호화 관련 문제점 >

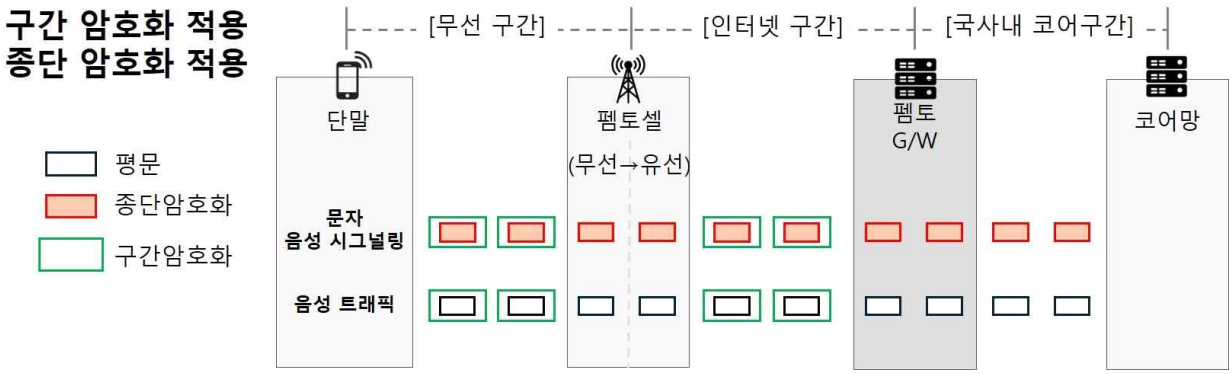
KT는 국제표준화기구(3GPP) 및 한국정보통신기술협회(TTA) 표준권고에 따라 단말과 펨토셀 간(무선망), 펨토셀과 통신사 국사 간(인터넷망)의 구간 암호화와 단말과 코어망 간 종단 암호화를 하고 있다.

< 통신사의 통신 암호화 체계 >

□ 통신 3사는 3GPP 표준 및 TTA 표준에 따라 암호체계 적용

- o (구간 암호화) 통신패킷이 흐르는 경로의 암호화로, 무선, 인터넷 구간에 암호화(통신사 국사 내 신뢰구간에는 암호화 미적용)
- o (종단 암호화) 단말에서 코어망까지 통신데이터 자체를 암호화하는 것으로, 문자 및 음성 시그널링*에 대해 국사 내 코어망까지 암호화

* 통화 시 상대방 식별, 세션 연결·해제 등을 관리하는 정보



그러나 통신 과정에서 종단 암호화가 해제되지 않아야 함에도 불구하고, 불법 펨토셀에 의해 암호화가 해제되어 결제 인증정보(ARS, SMS)가 전송되었다.

이에, 공격자가 불법 펨토셀에 접속한 피해자 통신의 종단 암호화를 해제하여 평문의 정보가 단말과 코어망 간 통신이 가능하게 되었으며, 통신 트래픽 캡쳐가 가능한 불법 펨토셀에 평문의 문자, 통화 탈취*도 가능한 것을 확인하였다.

* 불법 펨토셀에서 트래픽 저장 및 전송할 수 있는 기능을 확인(실제 탈취 흔적은 미발견)

특히, 일부 단말(아이폰 16 이하)의 경우, KT가 암호화 설정 자체를 지원하지 않아 문자 메시지(SMS)가 평문으로 전송되는 문제를 확인하여, KT 해당 단말에 대한 통신 연결 시 종단 암호화 지원을 조치토록 하였다(10.16~).

⇒ **(재발방지 대책)** KT는 이용자 단말기부터 코어망까지 종단 암호화(IPSec)가 해제되지 않도록 설정하고, 종단 암호화 해제 여부 및 비정상 신호 트래픽 인입에 대한 모니터링을 강화하여야 한다.

< 정보보호 활동 및 거버넌스 체계 관련 >

조사단은 이번 침해사고 조사 과정에서 KT가 보안점검 미흡, 보안장비 미비 및 로그 단기보관 등 기본적인 정보보호 활동이 미흡했던 점과, 거버넌스, 자산관리 등 전반적인 정보보호 활동이 체계적으로 이루어지지 않는 사실을 확인하였다.

① 보안점검 미흡

KT는 자체 규정*에 따라 시스템 로그 및 이벤트를 분석하여 보안점검을 실시하여야 하나, 보안점검 미흡으로 인해 악성코드 뿐만 아니라 쉽게 탐지가 가능한 웹셸도 발견하지 못하였다.

* KT 정보보호업무처리지침 제55조(예방활동)

⇒ **(재발방지 대책)** KT는 EDR*, 백신 등 보안 솔루션 도입 확대, 제로트러스트 도입, 분기별 1회 이상 모든 자산에 대해 보안 취약점 정기점검 및 제거 등 보안관리 강화를 하여야 한다.

* **E**ndpoint **D**etection and **R**esponse : 서버 등 네트워크가 연결되는 장치에서 발생하는 모든 활동을 감지·분석하는 도구

② 보안장비 미비 및 로그 단기보관

KT는 펨토셀 인증 및 제품등록을 관리하는 시스템을 방화벽 등 보안장비 없이 운용하고 있어 외부 공격에 취약한 상태임을 확인하였다. 또한, 운영 중인 시스템의 로그기록 보관기간이 1~2개월에 불과하여, 침해사고 최초 침투시점, 악성코드 감염방법 등 상세한 사고원인 파악을 조사하는데 한계가 있었다.

⇒ **(재발방지 대책)** KT는 펨토셀 인증 및 제품등록을 관리하는 시스템에 방화벽 등 보안장비를 도입하고, 운영 시스템에 대한 로그기록을 최소 1년 이상 보관하는 한편, 중앙 로그 관리 시스템을 구축하여 모니터링하여야 한다.

③ 거버넌스 체계 미흡

KT는 정보통신망법 등에 따라 정보보호최고책임자(CISO)가 정보보호 관련 업무를 총괄하여야 함에도, 보안 업무를 정보기술 부문, 네트워크 부문, 정보보안실로 구분하여 조직별로 수행하고 있다.

⇒ **(재발방지 대책)** 현재 CISO의 정보보호 인력·예산 편성권, 이사회에 정보보호 현황 보고 등 권한을 강화하는 정보통신망법 개정이 진행 중인 상황을 고려하여('25.12.3 법사위 통과), KT는 정보보호최고책임자(CISO)가 전사 정보보호 정책을 총괄 관리할 수 있도록 개편하고, 전사 차원의 중장기 보안 업무 계획을 수립하여야 한다.

④ 자산관리 미흡

조사단은 KT 전체 서버 대상 악성코드 감염 여부를 조사하는 과정에서, 전체 자산 종류, 규모, 운용/유휴/폐기 여부 등 자산 이력이 체계적으로 관리되지 않고 있으며, 시스템 내 등록된 자산과 실물 간 정보도 불일치함을 확인하였다.

⇒ **(재발방지 대책)** KT는 전사 자산을 담당하는 정보기술 최고책임자(CIO)를 지정하고, 정보기술 자산관리 솔루션을 도입하여야 한다.

⑤ 공급망 보안 미흡

조사단은 KT가 협력업체로부터 공급받는 펨토셀 장비에 대한 표준 보안 규격서 및 소프트웨어 패키지에 대한 SBOM* 관리체계가 부재하고, 고객에게 유통된 펨토셀에 대한 실시간 자산 현황관리가 제대로 이루어지지 않음을 확인하였다.

* **S**oftware **B**ill **o**f **M**aterials : 소프트웨어의 구성 컴포넌트에 관한 메타정보

⇒ **(재발방지 대책)** 펨토셀 도입 단계부터 납품, 구축·운영단계 全 과정에서의 하드웨어, 소프트웨어 공급망 보안 관리체계를 수립하고 관리해야 한다.

< 과거 침해사고 미신고 관련 >

KT는 자체적으로 수행한 보안점검 과정에서 웹셸 및 BPFDoor 등 악성코드를 발견('24.3월)하였으나, 정보통신망법에 따른 침해사고 신고를 하지 않고 자체적으로 조치하였다.

⇒ **(재발방지 대책)** 침해사고 발생 시 신속한 보고체계를 확립하고 정보통신망법에 따른 신고 의무를 준수하여야 한다.

< 법 위반에 따른 제재 >

① 침해사고 신고 지연 및 미신고

정보통신망법에 따라 침해사고가 발생하면 이를 인지한 후 24시간 이내 신고하여야 하나 KT는 발생 사고에 대해 지연신고를 하거나, 신고 자체를 하지 않았다.

※ 무단 소액결제 이상 통신패턴 9.5에 조치 → 9.8에 침해사고 신고
외부 보안업체 점검결과 침해흔적 9.15에 확인 → 9.18에 침해사고 신고
'24년 BPFDoor 등 악성코드 발견하고도 미신고

⇒ **(조치 사항)** 정보통신망법에 따라 과태료를 부과할 예정이다.

※ 정보통신망법 제76조에 따라 3천만원 이하 과태료 부과 대상

② 조사 방해

KT는 프랙 보고서에 제보된 침해 정황 서버와 관련하여, 8.1일에 서버를 폐기하였다고 답변하였으나, 조사단에 폐기 시점을 허위 제출(실제 : 8.1^{2대}, 8.6^{4대}, 8.13^{2대})하고, 폐기 서버 백업 로그가 있음에도 불구하고 9.18일까지 조사단에 이를 보고하지 않았다.

⇒ **(조치 사항)** 정부 조사를 방해하기 위한 고의성이 있다고 판단되어, 형법 제137조(위계에 의한 공무집행방해)에 따라 수사기관에 수사를 의뢰('25.10.2.)하였다.

5. 향후 계획

과기정통부는 이번 조사단의 조사결과를 토대로, KT에 재발방지 대책에 따른 이행계획을 제출('26.1월)토록 하고, KT의 이행(~'26.4월) 여부를 점검(~'26.6월)할 계획이다. 이행점검 결과, 보완이 필요한 사항에 대해서는 정보통신망법 제48조의4에 따라 시정조치를 명령할 계획이다. 또한, 고의적인 침해사고 미신고*로 인한 피해 확산을 방지하기 위해 정보통신망법 개정을 통한 제재 강화 등 제도 개선을 추진할 계획이다.

* '22년 SKT 악성코드 발견 사실 미신고, '24년 KT BPFDoor 발견 사실 미신고 등

Ⅱ. KT 이용약관 상 위약금 면제 규정 적용 여부

1. 위약금 면제 규정 개요

KT 이용약관은 '기타 회사의 귀책 사유'로 이용자가 서비스를 해지할 경우, 위약금을 면제하도록 규정하고 있다.

< KT 5G 이용약관 제39조 (위약금 면제) >

① 다음 각 호의 경우에는 제38조에 의한 위약금 납부 의무가 면제됩니다.

5. 기타 회사의 귀책 사유인 경우

2. 법률 자문 결과

과기정통부는 이번 침해사고가 KT 이용약관상 위약금 면제 규정에 해당하는지 여부 검토를 위해 법률 자문을 진행하였다.

과기정통부는 조사단의 조사결과를 바탕으로 법률 자문(5개 기관)을 진행하였으며, 대부분 법률 자문 기관(4개 기관)에서는 이번 침해사고를 KT의 과실로 판단했고 펨토셀 관리부실은 전체 이용자에 대해 안전한 통신서비스 제공이라는 계약의 주요 의무 위반이므로, 위약금 면제 규정 적용이 가능하다는 의견을 제시하였다. 법률 자문기관 한 곳은 정보 유출이 확인되지 않은 이용자에게는 위약금 면제 규정 적용이 어렵다는 의견을 제시하였다.

3. 주요 검토 내용 및 결과

과기정통부는 이번 침해사고로 이용자가 계약 해지 시, KT의 이용약관상 위약금이 면제되는 '기타 회사의 귀책 사유'에 해당하는지에 대해 ① 침해사고에서 KT 과실 여부, ② 전체 이용자에게 통신서비스를 제공(계약상)하는데 있어 주된 의무를 위반하였는지 여부를 중점적으로 판단하였다.

① 침해사고에서 KT의 과실

조사단의 조사결과에 따르면, 이번 침해사고와 관련하여 KT에 펨토셀 인증서 관리, 펨토셀 제작 외주사 보안관리, 비정상 IP 접속 관리, 펨토셀 제품 형상정보 검증 등 기본적인 펨토셀 보안조치 과정에서 명백한 문제점이 있었으며, 이 과정에서 KT가 정보통신망법을 위반한 사실도 확인되었다.

따라서, KT는 안전한 통신서비스 제공을 위한 펨토셀 관리와 관련하여 일반적으로 기대되는 사업자의 주의의무를 다하지 못했을 뿐만 아니라 관련 법령을 위반하였으므로, 과기정통부는 이번 침해사고에서 KT의 과실이 있는 것으로 판단하였다.

② 통신서비스 제공(계약상)에 있어 주된 의무 위반 여부

과기정통부는 조사단의 조사결과, KT의 입장, 법률자문 결과 등을 종합적으로 검토하여 KT가 이용자에게 통신서비스를 제공함에 있어 계약상 주된 의무를 위반했는지 여부를 판단하였다.

정보통신망법상 통신사업자에게는 안전한 통신서비스를 제공할 의무가 있으며, 국민 일상생활 전반이 통신서비스를 기반으로 이뤄지고 있는 점을 고려할 때 이용자는 사업자가 안전한 통신서비스 제공을 위한 적절한 보호조치를 할 것으로 기대할 수 있다. 따라서 안전한 통신서비스 제공은 통신사업자와 이용자 간 계약에서 중요한 요소로 볼 수 있다.

이번 침해사고에서 KT가 부실하게 관리한 것으로 확인된 펨토셀은 이용자 단말기와 KT 내부망을 연결하는 장치로, 안전하고 신뢰할 수 있는 통신서비스 제공을 위한 필수적인 요소이다.

조사결과에 따르면 KT는 펨토셀 관리 전반이 부실하여, 불법 펨토셀이 언제, 어디서든 KT 내부망에 접속할 수 있었고 통신 트래픽 캡쳐가 가능한 불법 펨토셀과 연결된 이용자 단말기에서 송·수신되는 문자, 음성통화 정보 탈취가 가능했던 사실이 확인이 되었다.

또한, 통신과정에서 이용자 단말기와 KT 내부망 사이 구간의 송·수신되는 정보는 종단 암호화가 이뤄졌어야 하나, 불법 펨토셀에 의해 종단 암호화 해제가 가능했던 사실이 확인되었다. 이는 통신 트래픽 캡쳐가 가능한 불법 펨토셀에서 이용자가 송·수신하는 평문의 문자, 음성통화 정보를 탈취할 수 있는 위험한 상황에 이용자가 노출된 것이며, 실제 일부 지역에서 피해도 발생하였다.

과기정통부는 KT의 펨토셀 부실 관리로 인해 야기된 평문의 문자, 음성통화 탈취 위험성은 소액결제 피해가 발생한 일부 이용자에 국한된 것이 아닌 KT 전체 이용자가 위험성에 노출되었던 것으로 판단했고, KT는 침해사고를 대비하여 적절한 보호조치를 통해 이용자에게 안전한 통신서비스를 제공해야 할 계약상 주된 의무를 다하지 못한 것으로 판단하였다.

결론적으로, 과기정통부는 ①이번 침해사고에서 KT의 과실이 발견된 점, ②KT가 계약상 주된 의무인 안전한 통신서비스 제공 의무를 다하지 못한 점 등을 고려할 때, 이번 침해사고는 KT 전체 이용자를 대상으로 KT 이용약관상 위약금을 면제해야 하는 회사의 귀책사유에 해당한다고 판단하였다.

Ⅲ. LGU+ 침해사고 조사결과

1. 조사 경과

KISA는 익명의 제보자로부터 LGU⁺의 자료 유출 관련 정보를 입수하고(7.18), LGU⁺에 관련사항을 공유하고 침해사고 신고를 안내(7.19)하였다. 과

기정통부(KISA)는 자체 조사단을 구성하여 8월25일부터 LGU+의 현장 조사를 실시하였고, 이후 LGU⁺가 10월23일 KISA에 침해사고를 신고한 후 조사단(10.24~)을 구성·운영하였다.

2. 조사 결과

익명의 제보자가 유출되었다고 주장한 LGU⁺의 통합 서버 접근제어 솔루션(APPM*)과 연결된 정보(서버목록, 서버 계정정보 및 임직원 성명)는 조사결과 실제 LGU⁺에서 유출된 것으로 확인되었다.

* APPM(Automated Process Policy Management): 시스템 계정의 패스워드를 주기적 일괄변경 및 관리하고 사용자에게 패스워드를 자동 생성/발급하는 통합 패스워드 관리 솔루션

조사단은 LGU⁺에서 제출받은 APPM 서버에 대해서 정밀 포렌식 분석을 진행한 결과, 익명의 제보자가 공개한 LGU⁺의 자료와 상이함을 확인하였다. 자료가 유출되었을 것으로 추정되는 또 다른 APPM 서버는 운영체제 업그레이드(8.12) 등의 작업이 이루어져 침해사고 흔적을 확인할 수 없는 상황임을 확인하였다.

또한, 익명의 제보자는 공격자가 LGU⁺에 APPM 솔루션을 제공하는 협력사를 해킹한 후 LGU⁺에 침투하였음을 주장하였다. 조사단은 이 주장에 대해서도 확인을 시도하였으나, 협력사 직원의 노트북에서부터 LGU⁺의 APPM 서버로 이어지는 네트워크 경로상의 주요 서버 등이 모두 OS 재설치 또는 폐기(8.12~9.15)되어 조사가 불가능한 상황임을 확인하였다.

조사단은 LGU⁺의 관련 서버의 OS 재설치 또는 폐기 행위가 KISA가 침해사고 정황 등에 대해 안내한(7.19) 후에 이루어진 점을 고려할 때, 이를 부적절한 조치로 판단하고 위계에 의한 공무집행 방해로 경찰청에 수사의뢰(12.9)하였다.

배경훈 부총리는 “이번 KT, LGU+ 침해사고는 SK텔레콤 침해사고에 이어, 국가 핵심 기간통신망에 보안 허점이 드러난 엄중한 사안”이라면서, “기업들은 국민이 신뢰할 수 있는 안전한 서비스 환경을 만드는 것이 생존의 필수 조건임을 인식하고 정보보호를 경영의 핵심가치로 삼아야 한다” 고 강조하였다.

아울러, “정부도 대한민국이 AI 3대 강국으로 도약하기 위해 정보보호가 반드시 뒷받침되어야 한다는 점을 인식하고 정보보호 역량을 고도화하는데 최선을 다하겠다.” 고 언급하며, “국민들이 혁신적인 AI 서비스를 안심하고 누릴 수 있는 환경을 만들도록 노력하겠다.”고 밝혔다.

담당 부서 <조사결과>	과학기술정보통신부 사이버침해대응과	책임자	과장	최광기 (044-202-6460)
		담당자	사무관	김성환 (044-202-6461)
담당 부서 <위약금>	과학기술정보통신부 통신이용제도과	책임자	과장	김준모 (044-202-6650)
		담당자	사무관	구희선 (044-202-6626)
관련 기관	한국인터넷진흥원 위협분석단	책임자	단장	박용규 (02-405-6620)
		담당자	팀장	김홍석 (02-405-4830)