㈜ 세계로시스템

08506 서울 금천구 가산디지털1로 137, 1501호(가산동 it캐슬2차) / TEL. 1599-0056 / FAX. 02) 2627-8272 / 업무담당 : 김기춘

문서번호 : 제 2019 - 0602호 2019. 06. 18

수 신 : ACA2000 사용 고객 대표님

참 조 :

제 목 : **랜섬웨어 침해사태 대처와 보상 및 향후 예정 사항 안내**

---

1. 인재양성을 위해 애쓰시는 귀원/귀기관의 노고에 감사드립니다.

2. 지난 5월 11일 새벽 당사 ACA2000의 FROGO 랜섬웨어 침해사태로 피해와 어려움을 겪으신 모든 고객님들께 다시 한번 사과 말씀 드립니다. 랜섬웨어 침해사태 발생 1개월이 지난 현재 ACA2000 서비스는 거의 정상적으로 운영되고 있습니다. 그러나 아직도 부분적으로 서버 안정화 작업이나 보안 업데이트 작업이 진행 중에 있음을 안내드립니다.

3. 이번 랜섬웨어 침해사태 관련 고객 여러분께 랜섬웨어 사태 대처 일지, 재발방지 조치사항, 피해 고객 보상 등에 대해 공식적으로 아래와 같이 보고 드립니다.

(1) 랜섬웨어 침해피해 대처 일지

- 2019.05.11(토) 오전 01:30분경 랜섬웨어 공격 시작
- 2019.05.11(토) 오전 05시경 랜섬웨어 피해 확인
- 2019.05.11(토) 오전 09시경 한국인터넷진흥원, 금천경찰서 피해 신고 접수
- 2019.05.11(토) 오전 랜섬웨어 복구전문업체 지정, 해커와 협상 시작
- 2019.05.11(토) 오후 1:10분경 랜섬웨어 非피해 고객(전체중 30%) 서비스 정상화
- 2019.05.11(토) 오후 ~ 12(일) 투트랙으로 피해복구 준비
  TRACK 1 : 암호화 해제코드 복호화 성공시
  TRACK 2 : 복호화 실패시 백업DB 활용안
- 2019.05.12(일) 오전 해커와 1차 협상통해 암호해제코드 확보
  총 9개 피해서버중 1개 서버 복호화 성공
- 2019.05.12(일) 오후 6시경 2차 협상 후 해커로부터 피해서버 8개 암호코드 수령
- 2019.05.12(일) 오후 12시경 피해서버 8개 복호화 실패 확인
- 2019.05.13(월) 오전 05시경 복호화성공 1개서버(전체고객중 10%) 서비스 정상화
- 2019.05.13(월) 오전 09시경 복호화실패 8개서버 고객(전체고객중 60%)
  3차 백업DB로 조회용 서비스 재개
- 2019.05.13(월) 오전~ 해커와 3차 접촉 계속 시도하였으나, 무응답
- 2019.05.13(월) 오전~오후 랜섬웨어 피해 복구 전문업체 컨설팅 복수 미팅 진행
- 2019.05.13(월) 오후 8시경 컨설팅업체 추천 복구 솔루션 구매, 복구 재시작
- 2019.05.15(수) 오후 1시경 복구솔루션으로 랜섬웨어 피해 서버 완전복구는 실패
  백업DB 제공 고객에 공백자료 입력 요청

- 2019.05.18(토) 오후 1시경 복구솔루션 활용 부분 복구 데이터 조회 기능 적용
- 2019.05.20(월) 오전 결제관련 부가서비스를 제외한 프로그램 기능 정상화
- 2019.05.20(월) 한국인터넷진흥원(KISA)에 침해사태 분석 요청
- 2019.05.21(화) KISA로부터 피해 원인분석결과와 대응방안 통보 받음
  IDC센터내 웹서버 감염파일을 통해 타 서버 악성 코드 유포로 확인

(2) 랜섬웨어 침해 재발방지 및 서비스 업그레이드 조치 사항

- 최신 서버로 전면 교체 / 장비 업그레이드
- 최신 방화벽 장비교체 + 지능형 침입방지 시스템 구축
- 실시간 이중화 시스템 구축
  메인서버 장애시 자동으로 예비서버로 전환
- 백업시스템 추가
  1~3차 백업 외 별도 4차 백업 진행
- 기가급 이중회선 적용
  대역폭 크게 향상
- 전문 서버 관리 유지보수 업체 위탁 계약

(3) 피해고객 보상 계획

5월1일 백업DB 적용고객	4월1일 백업DB 적용고객	3월1일 백업DB 적용 고객
1개월 사용료 면제 (5월 ACA2000사용료 면제)	2개월 사용료 면제 (5,6월 ACA2000사용료면제)	3개월 사용료 면제 (5~7월 ACA2000 사용료 면제)

* **통신문자비용(SMS/LMS/MMS), 부가서비스 연동비용은 청구**됩니다.

* 매월 익월 1일 청구분에 면제금으로 반영됩니다.

4. 이번 랜섬웨어 사태를 계기로 저희 ACA2000은 위에서 보고드린 바와 같은 보안 강화와 장애대처 서비스 업그레이드를 진행할 예정에 있습니다. 이에 저희 ACA2000 전 고객에 영향을 미칠 사항들을 아래와 같이 안내드리오니 꼭 인지하여 주시길 부탁드립니다.

(1) IDC 센터 통합 이전 안내

- 기존 신세계아이앤씨IDC(구로)와 LGU+ IDC(금천구 가산동)로 분산하여 운영되던 IDC센터를 LGU+ IDC가산센터로 서버통합 예정
- **일시 : 2019년 6월 22일(토) 저녁 11시 ~ 6월 23일(일) 오전 8시**
- 장애사항: ACA2000 프로그램 사용 불가

※ 별도 작업 공지 예정 합니다.

(2) 랜섬웨어 피해고객 5월 통신문자 비용 청구 안내

- 청구대상 : **2019년 5월 1일 ~ 5월 10일 사이 통신문자 이용분**
- 사유: 통신문자 내역 복구 지연으로 6/1일 사용료에 청구 미반영
- 청구방법 : 6/30일자로 청구내역에 반영 예정

※ 청구내역에 대한 확인 방법은 별도 안내 예정 입니다.

5. 이번 랜섬웨어 사태로 고충을 겪으신 고객님들께 다시 한번 사죄의 말씀을 드립니다. 저희는 이번 랜섬웨어 침해 사태로 고객님들의 신뢰를 저버리게 된 것에 대해 무한히 죄송하고 책임을 통감하고 있습니다. 이번 사태에 대한 저희의 보상안에 부족함을 느끼시더라도 잘 포용해주시고, 저희에게 한 번만 더 기회를 주시길 부탁드립니다. 이번 사태를 계기로 더욱더 서비스의 보안을 강화하고 서비스의 업그레이드를 위해 최선을 다하겠습니다. 감사합니다.
(문의 ☎ 1599-0056)

주식회사 세계로시스템

대표이사 진 병 식