정보 유출 사고와 포렌식 준비도

김 진 국

㈜ 플레인비트 대표

개요

PLAINBIT

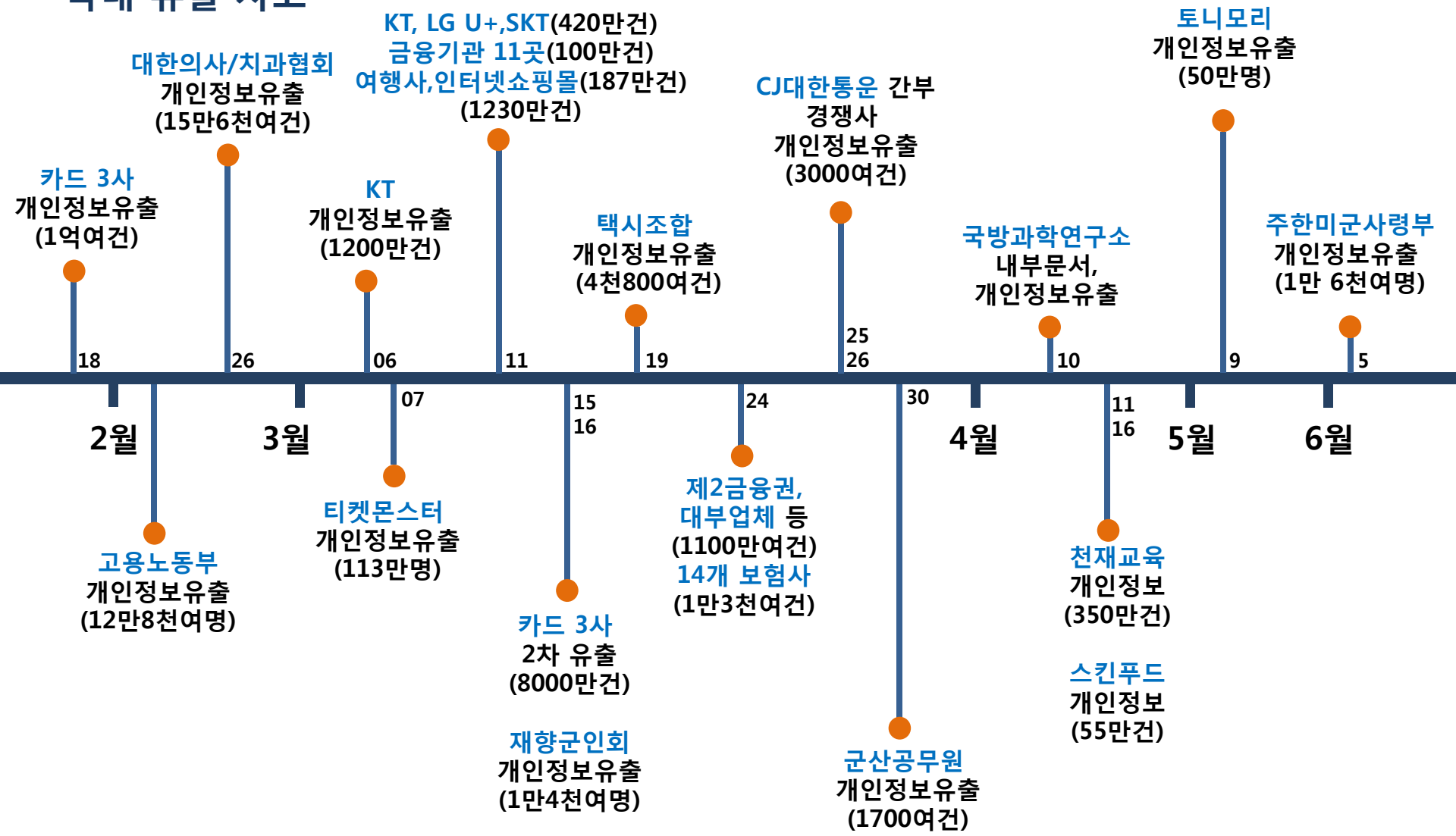
1. 최근 주요 정보유출 사고
2. 정보유출 사고의 일반적 문제
3. 정보유출 사고 사례
4. 정보유출 사고 준비 방안

최근 주요 정보유출 사고

- 국내 주요 정보유출 사고
- 해외 주요 정보유출 사고

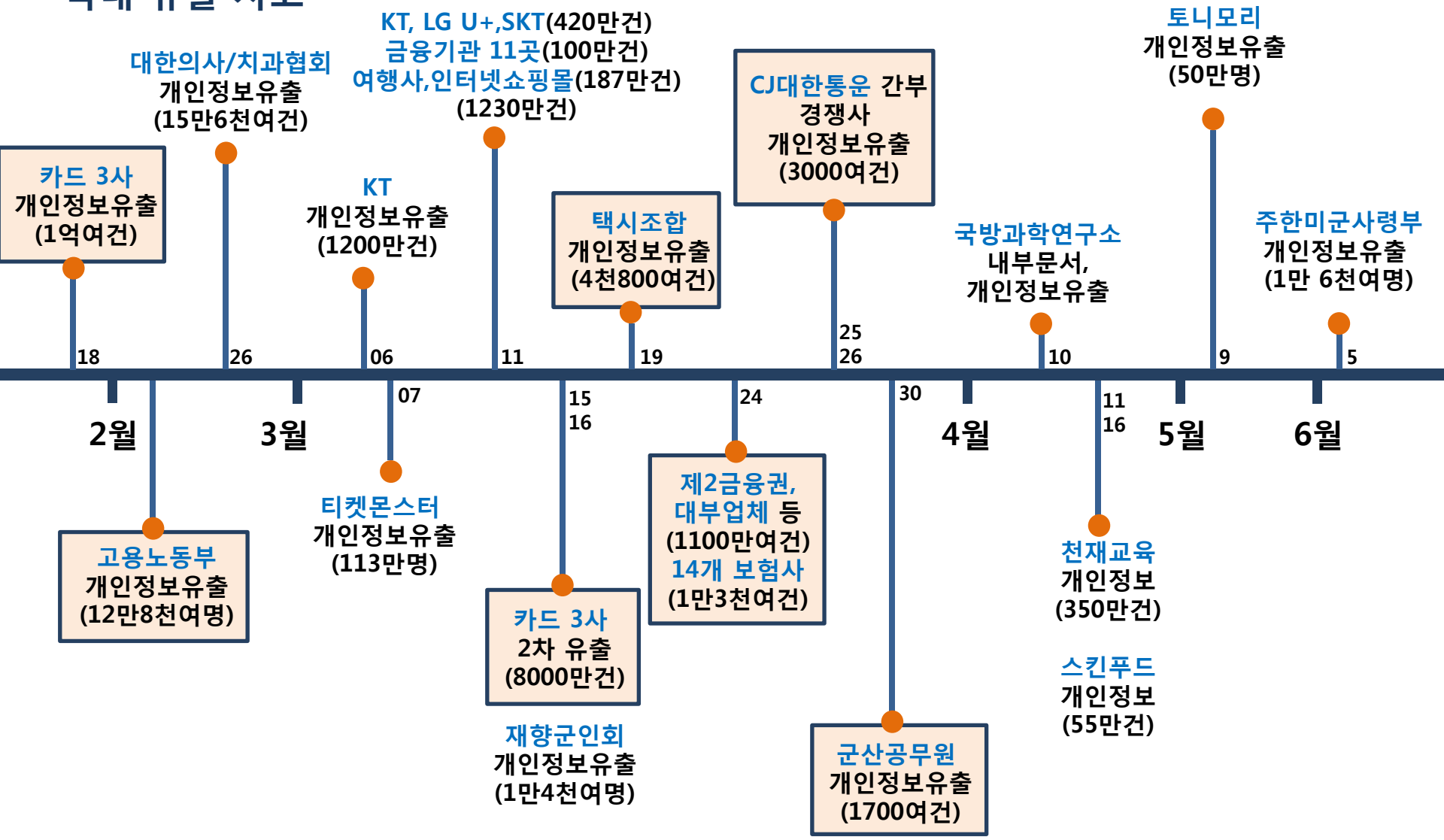
최근 주요 정보유출 사고

국내 유출 사고



최근 주요 정보유출 사고

국내 유출 사고



최근 주요 정보유출 사고

PLAINBIT

해외 유출 사고

국제경제

美 니만마커스, 110만 고객 카드정보 해킹

승인 2014.01.24

전직 MS 직원, 불

김우용 기자/ yong2@zdn

Like 3 Tweet

[Game Tech 컨퍼런

영업팀의 업무 수행

전직 마이크로소프트(MS) 직

적발됐다.

19일(현지시간) 미국 지디넷

재직 기간 중 윈도 관련 기밀

다.

워싱턴주 서부지구 연방법원

는 윈도8 RT와 ARM 기반 기

버 소프트웨어개발도구(SDK

개인의 스카이드라이브 계정

이후 프랑스의 익명 블로거

K-radio

60.247.128)

모가 당

됐던 소

번 피해

이메일

이베이, 1억4500만 회원 개인정보 유출…"비밀번호 바꿔야"

<<< 보험료가 오르지않는 비갱신형 암보험 문의폭주!

ebay tm

돋보기 女간호사 환자와 성행위? 영상유출!

돋보기 로또1등 당첨자만 타는 엘리베이터? 뭐길래!

온라인 경매 사이트 이베이의 회원 정보 데이터베이스가 해킹됐다. 암호화된 패스워드와 로그인 정보, 생년월일, 전화번호 등이 유출된 것으로 확인됐으나 신용카드 등 금융 정보는 빠져나간 흔적이 발견되지 않았다.

이베이는 21일(현지시간) 사이트 공지사항을 통해 이런 사실을 알리고 회원 1억4500만명 전원에게 암호를 바꾸도록 요청했다.

최근 주요 정보유출 사고

PLAINBIT

유출 사고 통계 ➔ SAFENET'S BREACH LEVEL INDEX

http://www.breachlevelindex.com/#!breach-database

2014.01

~

2014.06

RANK	ORGANIZATION BREACHED	DATE BREACHED	RECORDS BREACHED	LOCATION	INDUSTRY	SOURCE OF BREACH	TYPE OF BREACH	RISK SCORE
1	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	1/20/2014	104,000,000	South Korea	Financial	Malicious Insider	Identity Theft	10.0
2	Korean Medical Association, Association of Korean Medicine and Korean Dental Association	2/17/2014	17,000,000	South Korea	Healthcare	Malicious Outsider	Identity Theft	9.4
3	Northwestern city of Verden	4/3/2014	18,000,000	Germany	Government	Malicious Outsider	Financial Access	9.3
4	Naver	3/28/2014	25,000,000	South Korea	Technology	Malicious Outsider	Account Access	9.3
5	Korea Telecom	2/15/2014	12,000,000	South Korea	Technology	Malicious Outsider	Identity Theft	9.3
6	Internet country Germany	1/3/2014	16,000,000	Germany	Government	Malicious Outsider	Account Access	9.1
7	eBay	5/21/2014	145,000,000	United States	Retail	Malicious Outsider	Nuisance	8.8
8	Bulgaria Citizens	4/15/2014	2,832,312	Bulgaria	Other	Malicious Outsider	Identity Theft	8.7
9	FC Barcelona's official Twitter account	2/19/2014	11,119,878	Spain	Other	Malicious Outsider	Nuisance	8.6
10	Michael's Stores, Aaron Brothers	1/27/2014	3,000,000	United States	Retail	Malicious Outsider	Financial Access	8.6

최근 주요 정보유출 사고

PLAINBIT

유출 사고 통계 ➔ SAFENET'S BREACH LEVEL INDEX

http://www.breachlevelindex.com/#!breach-database

2013.01

~

2014.06

TOP 100

IN 8/100

OUT 85/100

ETC 7/100

RANK	ORGANIZATION BREACHED	DATE BREACHED	RECORDS BREACHED	LOCATION	INDUSTRY	SOURCE OF BREACH	TYPE OF BREACH	RISK SCORE
1	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	1/20/2014	104,000,000	South Korea	Financial	Malicious Insider	Identity Theft	10.0
2	Target	11/4/2013	110,000,000	United States	Retail	Malicious Outsider	Financial Access	10.0
3	Adobe Systems, Inc	9/18/2013	152,000,000	United States	Technology	Malicious Outsider	Financial Access	10.0
4	Country's Supreme Election Committee (YSK)	12/16/2013	54,000,000	Turkey	Governmen	Malicious Outsider	Identity Theft	9.9
5	Cupid Media	11/20/2013	42,000,000	Australia	Other	Malicious Outsider	Identity Theft	9.8
6	Korean Medical Association, Association of Korean Medicine and Korean Dental Association	2/17/2014	17,000,000	South Korea	Healthcare	Malicious Outsider	Identity Theft	9.4
7	Northwestern city of Verden	4/3/2014	18,000,000	Germany	Governmen	Malicious Outsider	Financial Access	9.3
8	Naver	3/28/2014	25,000,000	South Korea	Technology	Malicious Outsider	Account Access	9.3
9	Korea Telecom	2/15/2014	12,000,000	South Korea	Technology	Malicious Outsider	Identity Theft	9.3
10	LivingSocial	4/4/2013	50,000,000	United States	Retail	Malicious Outsider	Account Access	9.3

최근 주요 정보유출 사고

PLAINBIT

유출 사고 ➔ 문제점은?

- **정보보호에 대한 투자의 문제?**

  ➔ 장비/솔루션 도입? 인력 양성?

- **정보보호 체계의 미흡?**

  - ISMS 인증을 받은 KT도 유출…

- **과도한 정보 요구?**

  - 목적에 필요한 최소한의 정보만 요구하도록 법 신설 ➔ 동의 하에 그대로 수집

- **인터넷 인프라의 발달로 빠르게 전산화된 정보?**

  - 과연 그것만이 문제일까??

- **솜방망이 처벌이 문제?**

  - 징벌적 손해배상제 도입?

누가 인지하였는가?

정보유출 사고의 일반적 문제

영업비밀의 성립 요건

I. 비공지성

II. 비밀관리성

III. 경제적 유용성

정보유출 사고의 일반적 문제

I. 문제가 발생한 이후에 문제점 인식

II. 보안팀 V(IT)S 감사팀

III. 임원의 예외 설정

IV. 솔루션/장비의 지나친 의지

V. 제어가 힘든 모바일 환경

VI. 제어가 힘든 저장장치

VII. 개인정보보호법과의 충돌

VII. 노조와의 이해 관계

정보유출 사고 사례

내부자 유출 사고 사례 – I, 설계 도면 유출

- 특수 배관 제조업체 'A사'
- 사원수 68명, 매출액 180억원
- 4개월에 걸쳐 연구관리직 직원 3명 퇴사
- 퇴사 직원 3명은 다양한 지원 사업 자금을 이용해 인근에 제조 공장 설립
- 1년 반 이후 시장에서 제품이 맞붙자 'A사'는 정보유출 가능성을 인지
- 퇴사 직원 3명이 사용했던 시스템 분석 의뢰

내부자 유출 사고 사례 – I, 설계 도면 유출

- **증거물** : 퇴사 직원이 사용했던 데스크탑 3대
- **보존상태** : 다른 직원이 인계 받아 계속 사용
- **비밀관리상태** : 비밀관리조치, 접근제한조치가 존재하지 않음
- **분석 과정**
  1. 저장장치 이미징
  2. 시간 임의 변경 유무 조사
  3. 정보유출 아티팩트 추출 및 복구
  4. 퇴사 직원 근무 기간을 기준으로 정보유출 흔적 분석

내부자 유출 사고 사례 – I, 설계 도면 유출

- 분석 결과
  - E:₩찌빠귀₩XXX₩문서₩규격 관련
  - E:₩XXXX₩WIN₩mn₩도면
  - E:₩XXXX₩WIN₩mn₩도면₩최종도면₩Valve₩
  - E:₩KKKK₩특허
  - C:₩Documents and Settings₩Users₩Local Settings₩Temporary Internet Files₩Content.IE5₩EK8TSB₩최종도면[1].zip₩
  - C:₩Documents and Settings₩Users₩Local Settings₩Temporary Internet Files₩Content.IE5₩EK8TSB₩valve_2012[2].zip₩

- 비밀관리상태 부족, 시간적 연관성 부족

내부자 유출 사고 사례 – II, 동종 업계로 단체 이직

- 국내 탄탄한 기반을 가진 제조업체 'A사'
- 외국계 기업 'B사'의 국내 진출
- A 회사의 영업직 직원 영입 시도
- 임원급 영입 후 팀 구성 요구 ➔ 이전 회사 직원의 지속적인 퇴사
- 국내 영업라인 중 일부가 B사로 넘어가자 A사 조사 착수
- B 회사로 퇴사한 직원 6명이 모두 넘어가 영업을 하고 있는 사실 인지
- 퇴사자 6명이 사용했던 시스템 분석 의뢰

내부자 유출 사고 사례 – II, 동종 업계로 단체 이직

- **증거물 :** 노트북 6대
- **보존상태** : 퇴사 후 다른 직원이 인계 받아 포맷 후 재사용
- **비밀관리상태** : 비밀관리조치, 접근제한조치가 존재하지 않음
- **분석 과정**
  - 노트북 저장장치 이미징
  - 정보유출 흔적 복구
  - 복구된 흔적 중 전 직원의 근무 기간에 남겨진 정보유출 흔적 분석

내부자 유출 사고 사례 – II, 동종 업계로 단체 이직

- **분석 결과**
  - 평상 시 다수의 회사 내부 자료 외장저장장치로 복사 흔적 (영업사의 정보는 아님)
  - 퇴사 즈음 개인자료 백업 흔적

- 비밀관리상태 부족, 파일 형태의 영업정보 부족
- 추후 유사 문제 발생에 대한 직원의 환기 목적
- 사고 이후, 대대적인 비밀관리성 방안 마련

내부자 유출 사고 사례 – III, 임원에 의한 회사 기밀 유출

- 정보보호체계가 잘 되어 있는 IT업체 'A사'
- 중요 프로젝트 진행 중 퇴사를 하게 된 임원 'K씨'
- 'K씨'는 회사의 모든 보안정책 예외처리
- 회사 정보 회수를 위해 'K씨'의 개인 노트북 임의 제출 받음
- 'K씨' 노트북 분석 의뢰

내부자 유출 사고 사례 – III, 임원에 의한 회사 기밀 유출

- **증거물 :** 노트북 1대
- **보존상태** : 구입한 이후 제출 시까지 사용 (2년 간)
- **비밀관리상태** : 임원에 대한 예외처리
- **분석 과정**
  - 노트북 저장장치 이미징
  - 제출 이전의 사용 흔적 분석
  - 임원의 근무 기간 중 정보 유출 및 관리 흔적 분석

내부자 유출 사고 사례 – III, 임원에 의한 회사 기밀 유출

- **분석 결과**
  - 제출 전 증거 은폐 흔적
  - 다수의 회사 프로젝트 자료의 사용 흔적
  - 프로젝트 자료의 백업 흔적 (USB, 외장하드로 복사)

- 퇴사 보류, 추가 분석을 통해 프로젝트 자료 회수

내부자 유출 사고 사례 – IV, 프로그램 소스 코드 유출

- 관리용 프로그램에 특화된 업체
- 초기 국내 시장을 장악하여 캐시카우가 확실한 상태
- 관리용 프로그램 개발을 초기부터 설계한 핵심 개발자 'K'씨
- 퇴사 후 동종 업종을 창업
- 'K'씨가 사용했던 노트북 분석 의뢰

내부자 유출 사고 사례 – IV, 프로그램 소스 코드 유출

- **증거물 :** 노트북 1대
- **보존상태** : 퇴사 후 다른 직원이 사용
- **비밀관리상태** : 거의 되어있지 않음
- **분석 과정**
  - 노트북 저장장치 이미징
  - 직원의 근무 기간 중 정보 유출 흔적 분석

내부자 유출 사고 사례 – IV, 프로그램 소스 코드 유출

- **분석 결과 (1/2)**
  - 퇴사 1달 전 노트북 포맷
  - 포맷 후 USB로 복사한 폴더 목록
    - ✓ G:₩Borland₩Delphi6₩Lib₩build₩
    - ✓ G:₩Borland₩Delphi6₩Lib₩Code₩
    - ✓ G:₩Borland₩Delphi6₩Ocx₩
    - ✓ G:₩Borland₩Delphi6₩Projects₩
    - ✓ G:₩Borland₩Delphi6₩Source₩
    - ✓ G:₩Borland₩Delphi6₩src₩

내부자 유출 사고 사례 – IV, 프로그램 소스 코드 유출

- **분석 결과 (2/2)**
  - 아티팩트 복구를 통해 분석한 결과,

    노트북을 포맷하기 전에 연결된 USB에 다음 파일들이 존재

    - ✓ F:/XXX/동업계약서.hwp
    - ✓ F:/XXX/동업계약서.hwp
    - ✓ I:/오라클/201XXX13/data/테이블주석.txt
    - ✓ I:/오라클/201XXX13/data/테이블주석.txt
    - ✓ I:/오라클/201XXX13/data/ORA_SCRIPT_table_주석.sql
    - ✓ I:/오라클/201XXX13/data/ORA_SCRIPT_table_주석.sql

- 비밀 관리 상태 부족

정보유출 준비 방안

무엇이 문제인가?

정보보호 사고에 대한 인식의 문제

"사고를 막아보자"

"사고를 조기에 식별하여

피해를 최소화하자 "

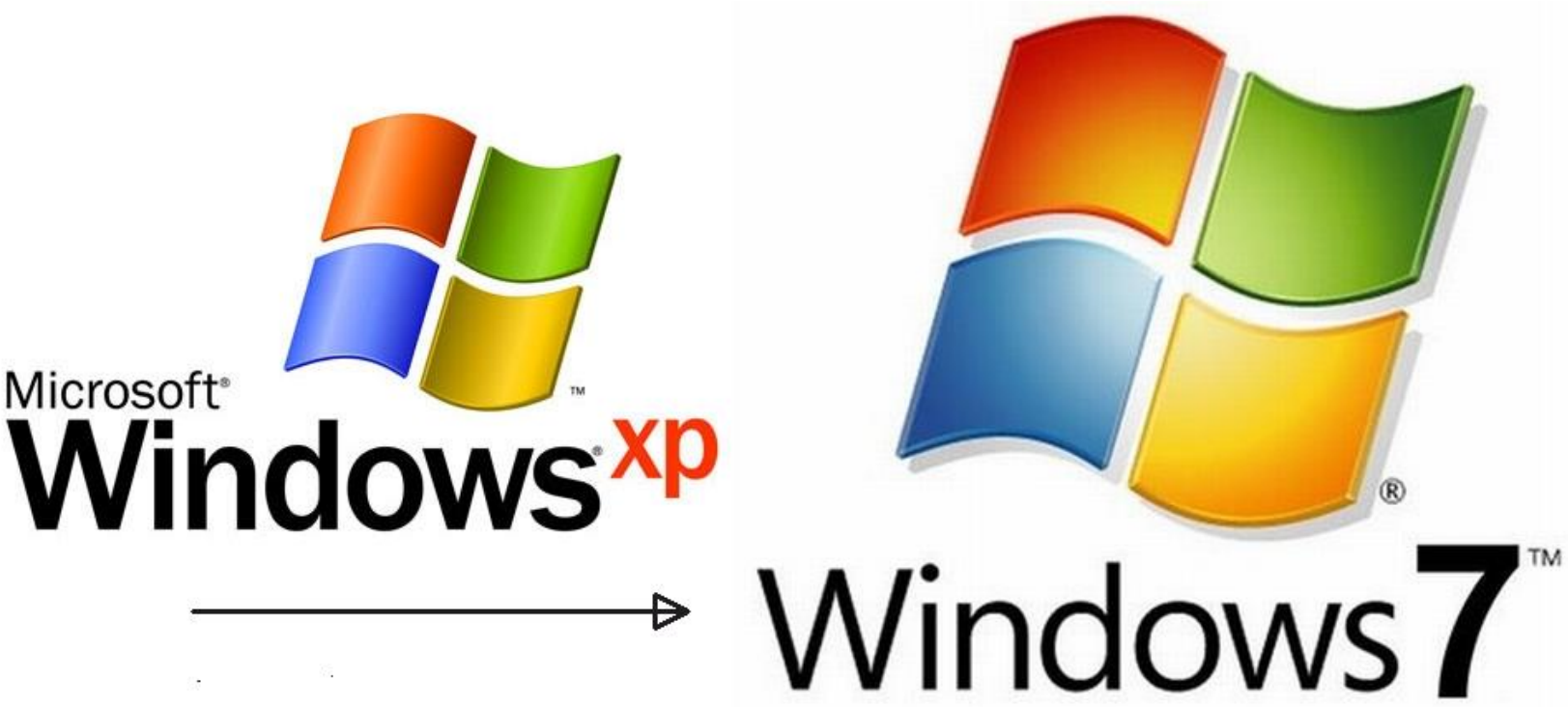
포렌식 준비도

조사 비용은 최소로, 디지털 증거의 활용 가능성은 최대로 하기 위한 조직의 준비 능력

- 사고 가능성을 낮추기 위한 것이 아닌 사후 대응을 위한 사전적 투자
- 기술적 준비 + 인적, 정책적, 조직적인 노력 포함
- 준비 능력
  - ✓ 사후, 사고를 조기에 식별하기 위한 준비
  - ✓ 사후, 빠르고 효과적인 대응으로 피해를 최소화하기 위한 준비
  - ✓ 사후, 사고의 원인과 과정을 밝혀내기 위한 준비
- 어려움
  - ✓ 사고 발생 가능성에 대한 공감이 되는가?
  - ✓ 많은 인적, 시간적, 경제적 비용이 필요한 것 아닌가?

1. 클라이언트 설정을 강화하자!!

① 운영체제 업그레이드



1. 클라이언트 설정을 강화하자!!

② 프리패치 서비스 활성화

- 프리패치 설정을 강화하여 프로그램의 실행 흔적을 추적
- 수정된 운영체제, 서버 제품군, SSD 사용 시스템 ➔ 강제 활성화
- **점검 항목**
  - ✓ KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩Memory Management₩PrefetchParameters₩**EnablePrefetcher**
- **설정 강화**
  - ✓ 0x00 : 비활성화
  - ✓ 0x01 : 응용프로그램 프리패칭 활성화
  - ✓ 0x02 : 부트 프리패칭 활성화
  - ✓ **0x03 : 응용프로그램 + 부트 프리패칭 활성화 (권장)**

1. 클라이언트 설정을 강화하자!!

③ NTFS 트랜잭션 로그 크기

- 트랜잭션 로그 크기를 증가시켜 장기간의 트랜잭션 정보 추적
- 기본 64MB로 설정 ➔ 2~3시간의 흔적 기록
- **점검 항목**

  $> chkdsk /L (트랜잭션 로그 크기 확인)

- **설정 강화**

  $> chkdsk /F /L:524288 (KB 값 지정, 512MB 이상 권장)

1. 클라이언트 설정을 강화하자!!

④ NTFS 변경 로그 크기

- 변경 로그 크기를 증가시켜 장기간의 NTFS 파일 변경 상태 추적
- 기본 32MB로 설정 ➔ 4~5일의 흔적 기록
- **점검 항목**

  $> fsutil usn queryjournal <volume> (변경 로그 크기 확인)

- **설정 강화**

  $> fsutil usn createjournal m=<maxsize> a=<allocationdelta> <volume>

  (Byte 값 지정, 4GB 이상 권장)

1. 클라이언트 설정을 강화하자!!

⑤ NTFS 접근 시간 갱신

- 접근시간을 갱신하여 시스템 및 사용자 흔적을 좀 더 정확히 추적
- **점검 항목**
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩FileSystem₩

    NtfsDisableLastAccessUpdate
- **설정 강화**
  - ✓ 0x00 : 갱신함 (권장)
  - ✓ 0x01 : 갱신 안함

1. 클라이언트 설정을 강화하자!!

⑥ 로컬 방화벽 로깅 활성화

- 로컬 방화벽을 활용하여 내부망에서 일어나는 비정상 접속 추적
- **점검 항목**
  - ✓ [제어판] → [Windows 방화벽] → [고급설정] → [동작] → [속성] → 각 탭 [로깅]
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩SharedAccess₩Parameters₩FirewallPolicy₩<Profile>₩Logging₩**LogDroppedPackets (손실된 패킷 로깅)**
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩SharedAccess₩Parameters₩FirewallPolicy₩<Profile>₩Logging₩**LogSuccessfulConnections (성공한 연결 로깅)**
- **설정 강화**
  - ✓ 0x00 : 로깅 안함
  - ✓ 0x01 : 로깅함

1. 클라이언트 설정을 강화하자!!

⑦ 로컬 방화벽 로그 크기

- 로컬 방화벽 로그 크기를 증가시켜 장기간의 흔적 추적
- **점검 항목**
  - ✓ [제어판] → [Windows 방화벽] → [고급설정] → [동작] → [속성] → 각 탭 [로깅]
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩SharedAccess₩Parameters₩FirewallPolicy₩<Profile>₩Logging₩**LogFileSize**
- **설정 강화**
  - ✓ 0x5000 (KB 값 지정, 20MB 이상 권장)

1. 클라이언트 설정을 강화하자!!

⑧ 볼륨 섀도 복사본 크기

- 볼륨 섀도 복사본 크기를 늘려 백업된 이전 상태 추적
- **점검 항목**

  ✓ [제어판] → [시스템] → [고급 시스템 설정] → [시스템 보호] 탭 → 볼륨 선택, [구성]

  $> vssadmin list shadowstorage /for=<volume>

- **설정 강화**

  $> vssadmin resize shadowstorage /for=<volume> /on=<storevolume> /maxsize=<size>

  (볼륨의 15% 이상 설정 권장)

1. 클라이언트 설정을 강화하자!!

⑨ 이벤트 로그 활성화

- 이벤트 로그 활성화를 통해 시스템 및 사용자 이벤트 추적
- **점검 항목**
  - ✓ [제어판] → [관리 도구] → [서비스] → Windows Event Log 서비스 상태
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog₩**Start**
- **설정 강화**
  - ✓ 0x02 : 자동 (권장)
  - ✓ 0x03 : 수동
  - ✓ 0x04 : 사용 안함

1. 클라이언트 설정을 강화하자!!

⑩ 이벤트 로깅 항목 설정

- 이벤트 로깅 항목을 설정하여 보다 상세한 시스템 및 사용자 이벤트 추적
- **점검 항목**
  - ✓ [제어판] → [관리 도구] → [로컬 보안 정책] → [로컬 정책] → [감사 정책]
  - ✓ HKEY_LOCAL_MACHINE₩SECURITY₩Policy₩PolAdtEv₩**(기본값)**
- **설정 강화**
  - ✓ 계정 관리 감사 – 성공, 실패
  - ✓ 계정 로그온 이벤트 감사 – 성공, 실패
  - ✓ 권한 사용 감사 – 성공, 실패
  - ✓ 로그온 이벤트 감사 – 성공, 실패
  - ✓ 시스템 이벤트 감사 – 성공, 실패

1. 클라이언트 설정을 강화하자!!

11 이벤트 로그 크기

- 이벤트 로그 크기를 증가시켜 효율적인 시스템 및 사용자 이벤트 추적
- **점검 항목**
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog₩<Log>₩**MaxSize**
  - ✓ HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩<Log>₩**MaxSize**
- **설정 강화**
  - ✓ 주요 이벤트 로그 4G 이상 설정
    - Application
    - Security
    - System

1. 클라이언트 설정을 강화하자!!

11 이벤트 로그 크기

- **설정 강화**
  - ✓ 추가 이벤트 로그 100MB 이상 설정
    - Microsoft-Windows-Application-Experience
    - Microsoft-Windows-DriverFrameworks-UserMode
    - Microsoft-Windows-NetworkProfile
    - Microsoft-Windows-OfflineFiles
    - Microsoft-Windows-TerminalServices-LocalSessionManager
    - Microsoft-Windows-TerminalServices-RemoteConnectionManager
    - Microsoft-Windows-WER-Diagnostics
    - Microsoft-Windows-Windows Defender
    - Microsoft-Windows-WLAN-AutoConfig

1. 클라이언트 설정을 강화하자!!

12 이벤트 로그 백업

- 이벤트 로그 백업을 통해 장기간의 시스템 및 사용자 이벤트 추적
- **점검 항목**
  - ✓ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog₩<Log>₩**AutoBackupLogFiles**
  - ✓ HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩<Log>₩**AutoBackupLogFiles**
- **설정 강화**
  - ✓ 0x00 : 백업 안함
  - ✓ 0x01 : 자동 백업 (권장)

2. 모니터링을 강화하자!!

- 차단보다는 모니터링이 필요!
- 공격자의 목적은 흔적 최소화가 아닌 정보 유출!
- 고위험군 분류 (연구직, 영업직, 임원 등 고위험군) 모니터링
- 사전에 관리된 정보유출 지표 모니터링

3. 대응 절차를 마련하자!!

- 신속한 대응 절차 마련!!!!!!!!!!!!!!!!!!!!!!!!
- 사고 식별 시 주요 데이터 백업 (3~5분) 방안 마련
- 사고 대상 별 현장 및 데이터 수집 절차 마련
- 사고 위험도 별 대응 절차 마련

4. 인력을 활용하자!!

- 장비/솔루션은 인력적인 부분을 보완하는 역할 ➔ 판단은 사람이!
- 식별된 징후에 대해 분석할 수 있는 새로운 역할의 '분석팀' 필요
- 자체적인 인력을 구성하기 어렵다면 ➔ 외부의 전문 감사 서비스 활용
- 대응보다는 원인 파악에 초점을 맞춘 분석!

- **평시** ➔ 정기 감사, 위협 요인에 대한 다양한 정보 수집 및 샘플 테스트
- **전시** ➔ 징후의 원인과 과정을 분석하여 보안성 강화

5. 형상 관리를 하자!!

- 포맷은 답이 아니다!
- 정상적인 퇴사 직원도 회사의 위협이 될 수 있음
- 목적/위험도에 따라 보존 절차 마련 ➔ 추후 원인 파악, 법률적 대응에 활용
- 저장장치 보관이 가능하다면 최소 3개월 이상 보관
- 용량이 부담된다면 압축하여 용량 최소화
- 사건 유형에 따라 조사에 필요한 데이터만 보관

6. 정보유출 지표를 관리하자!!

- 정보유출을 식별할 수 있는 포렌식 아티팩트
- 내부자 행동 패턴 (출/퇴근, 시스템 로그인/아웃, 프로그램 사용, 저장장치 사용 등)
- 특이 이력 점검
- 분석 인력을 통해 지속적인 지표 업데이트

7. 입/퇴사자 프로세스를 갖추자!!

- 위험군에 따라 입사자 프로세스!
- 어렵게 영입한 실력 좋은 경력자가 회사에 해가 될 수도...
- 입사하면서 가지고 나온 전 회사의 자료로 인해 개인 혹은 기업간 소송

- 위험군에 따라 퇴사자 프로세스!
- 퇴사자 발생 시 조직의 위험 요인에 대한 분석
- 조직의 정보 회수 목적

8. 비밀관리방안을 마련하자!!

- 비밀관리성 ➔ 상당한 노력에 의해 비밀로 유지되고 있는가?
- 비밀관리의사 및 조치

  ➔ 대외비/비밀/외부유출금지표시, 비밀등급지정 및 고지, 비밀유지서약서, 보안 교육
- 접근제한조치

  ➔ 잠금장치, 암호화, 등급별 접근 제한, 출입보호장치, CCTV 등
- 상당한 노력

  ➔ 조직의 규모와 상황에 맞는 노력을 취했느냐?

"준비해야 할 것이 너무 많다?"

"시간과 비용이 많이 든다?"

"완벽하게 막을 수 있는가?"

"직원의 불만을 줄이자!! "

질문과 답변