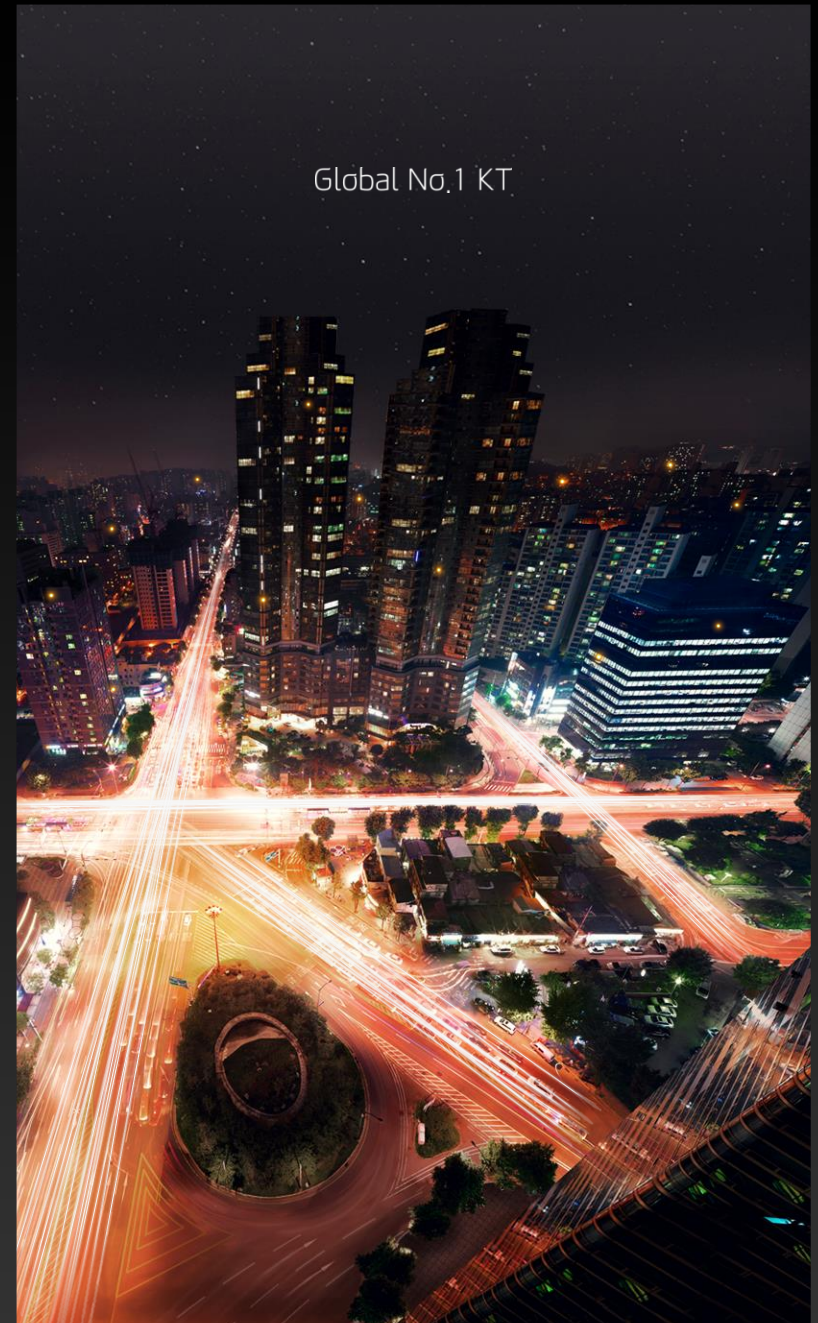


클라우드 환경의 보안 전략

KT 홍원규 상무 | 2016. 04. 05



Contents

1 클라우드 보안

2 클라우드 주요 특징 및 보안 위협 (CLOUDSEC Conference 2014 신영상 박사)

3 클라우드 정보보안전략

1 클라우드 보안

2 클라우드 주요 특징 및 보안 위협 (CLOUDSEC Conference 2014 신영상 박사)

3 클라우드 정보보안전략

Apple vs FBI

'국가안보와 사생활보호'논쟁



테러범 수사를 위해 FBI가 Apple에 iPhone 잠금해제 요구

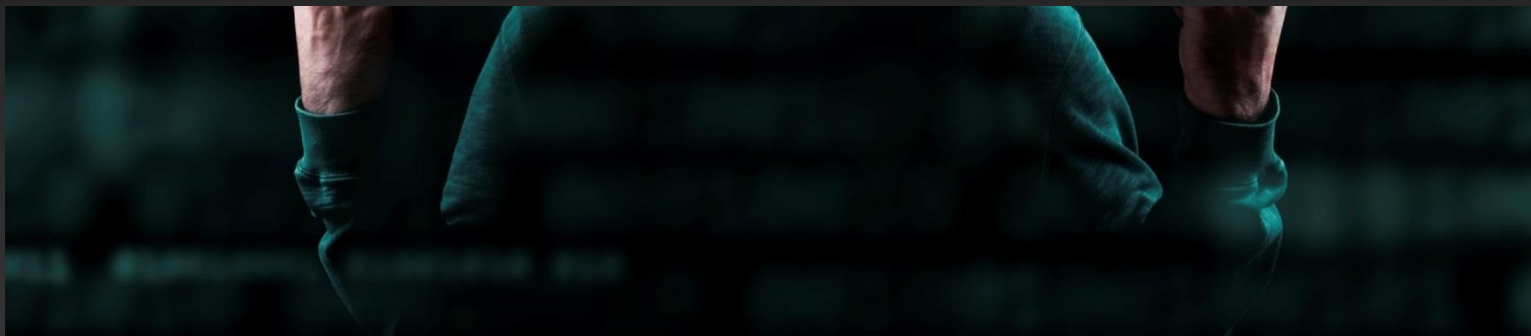


Apple은 거부



FBI의 iPhone Hacking으로 결말

난공불락(難攻不落)으로 여겨지던 iPhone 보안체계 무너져



Apple의 Cloud 정책



- 고객 개인정보가 담긴 iCloud 보안을 강화
- iCloud 데이터에 본인만 접근할 수 있도록
- Apple사에서도 읽기가 불가하도록

출처 : 3월16일, 포브스

방어中心에서 대응中心으로



- RSA2016에 제품을 선보인 553개 기업은 사이버위협을 100%막을 수 없다는 현실 인정
- 기존의 방어중심의 솔루션보다는 사고 후 신속한 원인분석, 피해를 최소화하는 대응에 집중

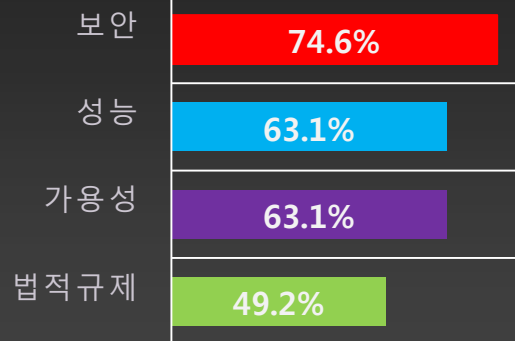
1 클라우드 보안

2 클라우드 주요 특징 및 보안 위협
(CLOUDSEC Conference 2014 신영상 박사)

3 클라우드 정보보안전략

TOP THREATS IN 2015

사용자 우려사항



<출처 : IDC Research, INC.>

10 Worst Cloud Security Threats Of 2015



1. Data Breaches



2. Data Loss



3. DDoS Attack



4. Account Hijacking



5. Insider Attacks



6. Insufficient Due Diligence



7. Malware



8. Viruses



9. Phishing Attacks



10. BYOD

<출처 : talkincloud.com>

Major Concerns

- 서비스의 악의적인 사용과 남용
- 악성 내부 사용자에 의한 정보유출
- 데이터 손실 및 누출
- 계정, 서비스와 트래픽 하이재킹
- 알려지지 않은 위험 프로파일

Reality

네트워크 보안

- Firewall
- IPS / IDS
- Application Firewall(L7)
- SSL / IPSec

관리적/ 물리적/ 기술적 보안

- 암호
- 보안관제
- 로그관리 / 보안규제관리
- 접근통제관리

자원공유로 인한 취약성-비인가자 접근

- 동일 호스트 상에 타인의 정보가 혼재되어 비 인가자(내/외부)의 정보 접근 가능성이 높아짐
 - 설정오류, 취약 PW 사용, 정보 접근제어 관리

비인가자의 정보접근 문제

- 인가되지 않는 타 고객에 의한 정보 접근/유출 위협
 - 사례 : M사 기업용 클라우드 솔루션의 권한설정 오류로 기업 정보가 타인에게 열람됨(2010)
- 내부자의 위협으로 인한 고객의 정보 훼손/오용 위협
 - 사례 : 일본 FirstServer 관리자 실수 5,698개 기업정보유실(12)

IT자원 공유에 대한 문제



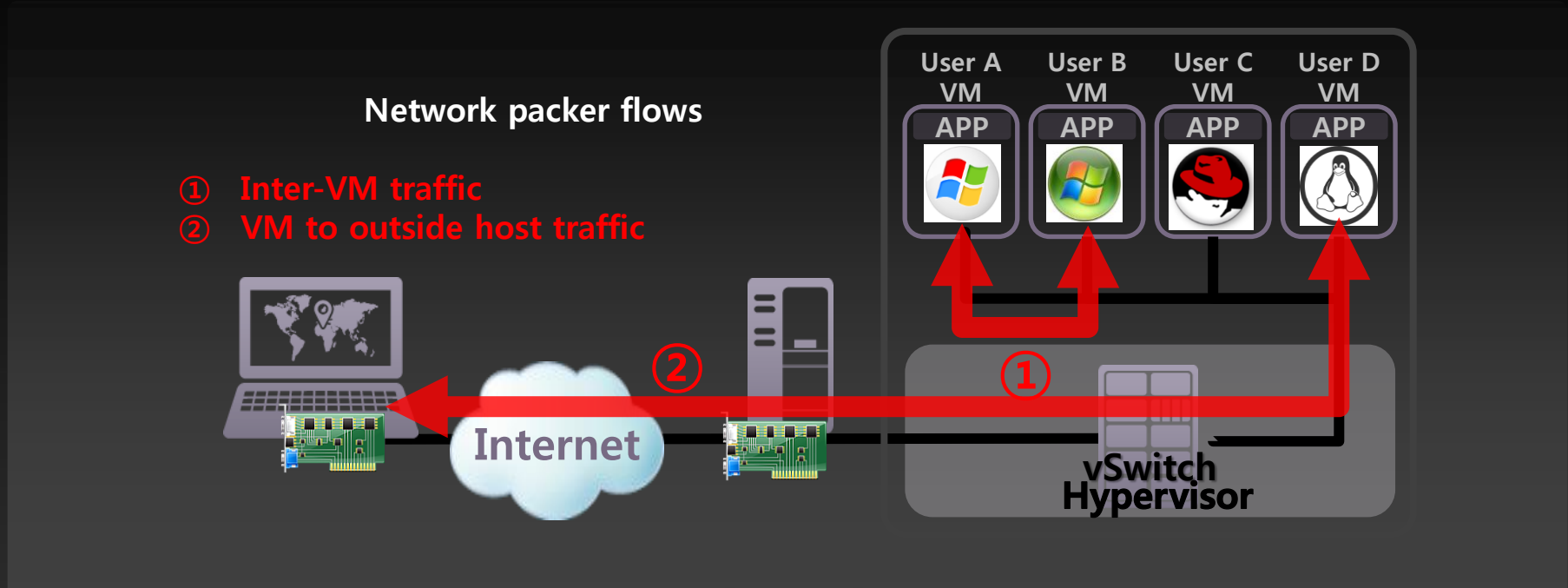
<출처 : CSA>

대응 현황

- 고객별 접근제어 (포탈 인증, API Key, SSH Password/ Key 방식 제공)
- 설정 오류 방지 (설정오류 점검, 패스워드 보안성 강화)
- 운영자 접근 권한 프로세스 및 운영 관리
- 이용자의 정보 저장위치 관리
- VR을 통한 VM접근 제어, WAF/DB접근제어 등 활용

가상화 기반 취약성 – 가상화 네트워크

- 가상화 네트워크를 통한 VM간의 통신



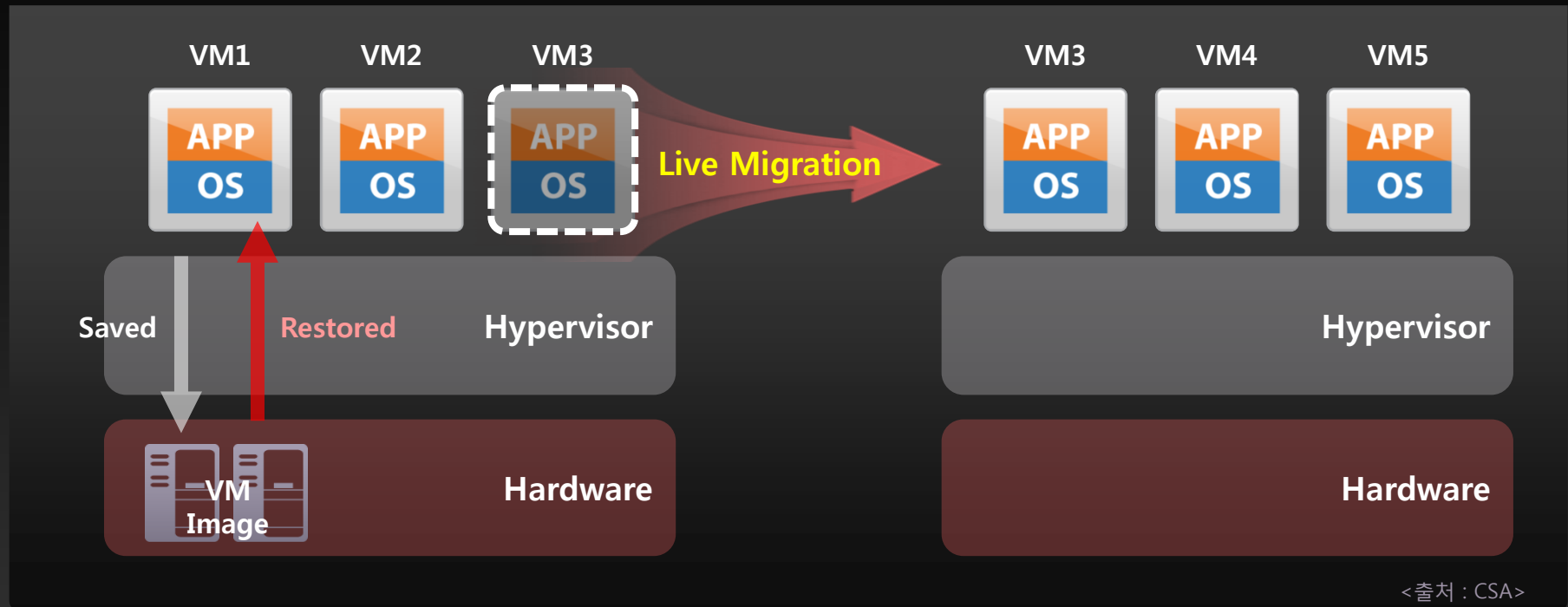
<출처 : CSA>

대응 현황

- 호스트 내부 : VIF를 통한 호스트 내부 VM간 접근제어
- 호스트 외부 - VM : VLAN을 통한 격리
- 호스트 외부 - 인터넷 : Virtual Router를 통해 네트워크 자원 공유 제어

가상화 기반 취약성 – 가상화 라이프사이클

- 가상머신의 동적인 라이프사이클 관리 및 Live Migration시 데이터 기밀성 우려



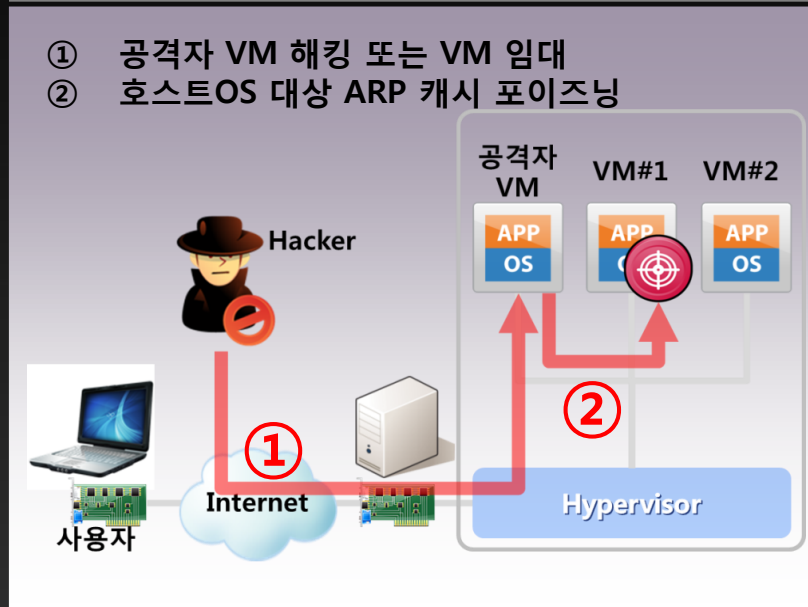
대응 현황

- 별도의 관리망을 통한 VM Live Migration 수행(기밀성 보장)
- Live Migration 시 공유 스토리지의 볼륨을 사용함으로써 무결성 및 기밀성 보장

가상화 기반 취약성 - 새로운 공격 경로

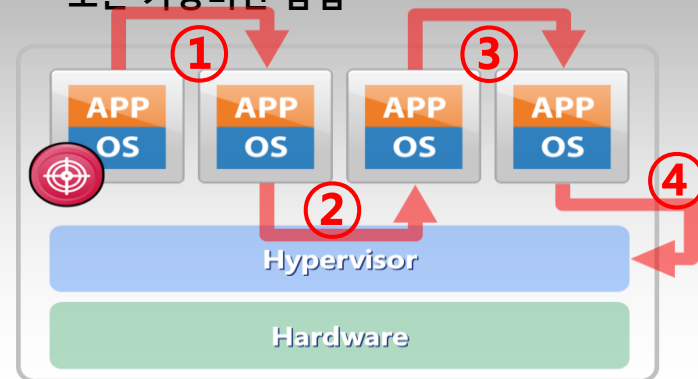
- 가상화 기술을 통해 이용자 VM들이 상호 연결되어 다양한 공격경로 신규 발생 우려
 - 해킹, DDoS, 악성코드 전파 등

가상 네트워크를 통한 패킷 스니핑



VM간의 해킹

- ① 악성코드 감염
② 1차 감염 : 호스트OS > 게스트OS
③ 2차 감염 : 게스트OS > 게스트OS
④ 3차 감염 : 하이퍼바이저 감염으로 모든 가상머신 감염



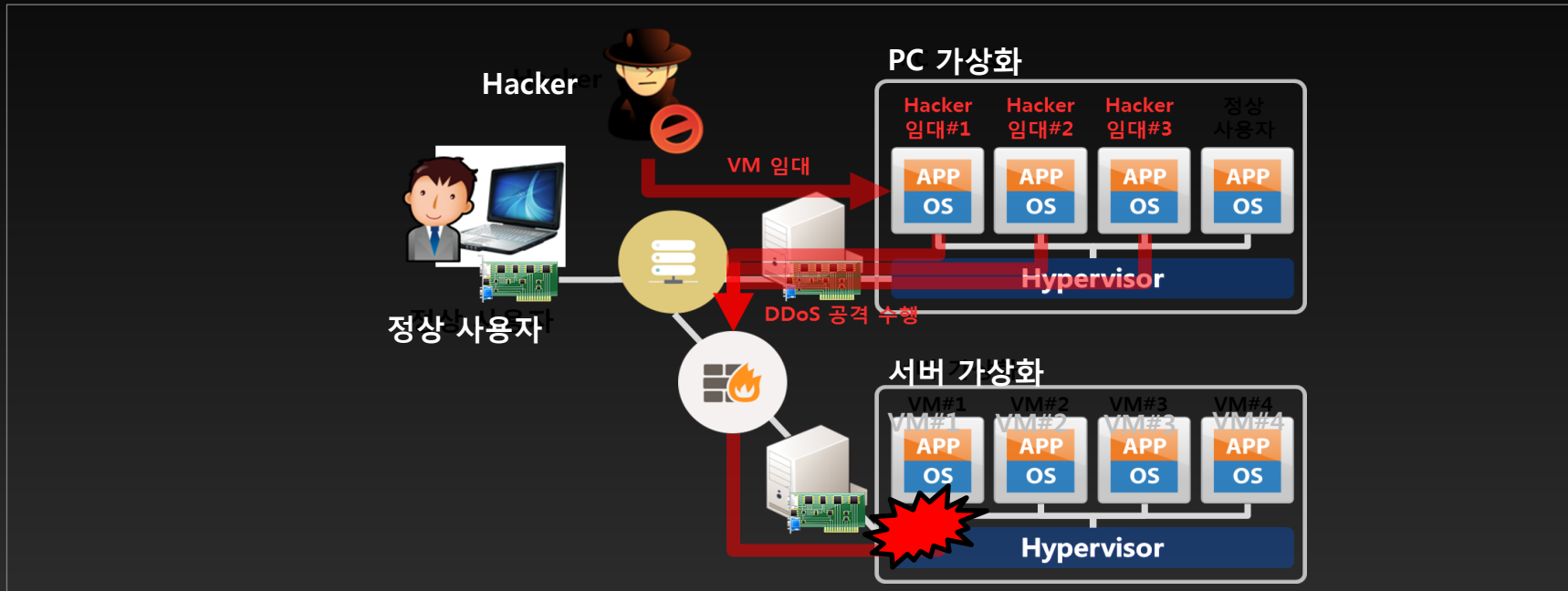
<출처 : CSA>

대응 현황

- ARP 캐시 포이즈닝은 고객 VM 및 네트워크 별 독립 구성으로 타 고객 영향 없음
- Hypervisor에 대한 취약점(CVE)에 대해 지속적인 패치 및 업데이트 수행

가상화 기반 취약성 - 대규모 피해

- 클라우드 서버에 고객 정보 및 자원이 集積되어 해킹, DDoS 공격의 표적이 되거나 공격 경유지로 악용 우려



<출처 : CSA>

대응 현황

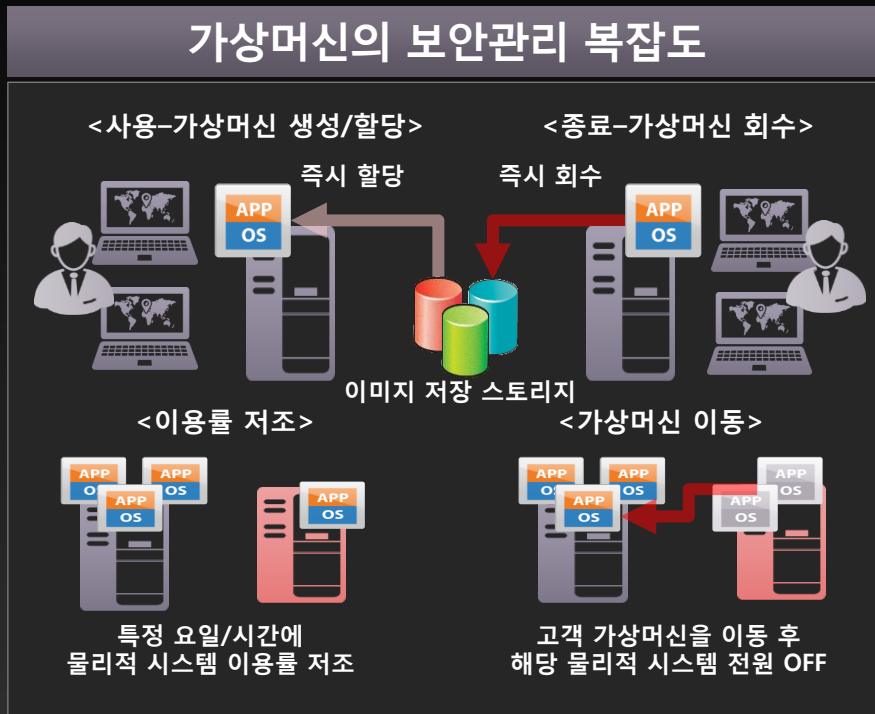
- 실명인증, OTP를 통한 사용자 인증 수행
- 개별 기업이 구매하기 힘든 보안 장비를 갖추어 DDoS 방어, 침입탐지 수행
- 물리적으로 독립된 여러 DC(Multi Availability Zone)에 서비스를 분산 운영

보안 책임소재 불분명 및 보안 정책 복잡화

- E2E 보안 관리 및 정책 적용 복잡



<출처:Microsoft>



<출처 : CSA>

대응 현황

- 중소기업의 Legacy 환경 등 적절한 보안 대책을 자체적으로 구비하기 어려운 경우 Cloud 사용이 더 우위

법규 및 규제 문제

- 기존 법규와 규제 적용의 한계 → 정보의 소유/관리 분리, 서버의 분산 배치 등
 - 국외 데이터센터 이용 시, 서버의 위치에 따라 국내 법규 및 규제 적용이 어려움
- 클라우드 활성을 위한 범 정부차원의 네거티브 규제방식으로 전환중(공공, 금융, 교육, 의료 등)

국가간 서비스 이용 변경

Korea Cloud




- 정보통신망법
- 개인정보보호법
- 저작권법
- ...




USA Cloud



- FISMA, HIPAA, GLBA
- COBIT, PICDSS, SOX
- ...



클라우드 | 보안
클라우드 도입 기업의 절반, “컴플라이언스에 자신없다”
2010.10.28



클라우드 서비스 업체를 이용하고 감사 때문에 어려움을 겪을 수 있기에 잠재적인 위험요소가 있다는 것 고 답했다.

“클라우드 보안, 해킹·데이터 침해 보다 법규제가 더 큰 이슈”

2010년 10월 19일 10:19:02 / 0:00:00 기자 yjlee@ddaily.co.kr

- 장 리베스 CSA글로벌 대표, “소프트웨어와 SaaS 혁신이 클라우드 광국 패를 열 것”

[디지털데일리 인터뷰기] “현재 나타나는 거창 큰 클라우드 보안 이슈는 해커에 자사 클라우드 기반 애플리케이션(이하 공격 등 데이터 침해나 유출 보다는 컴플라이언스(규제준수)이다.”

현재 클라우드 보안 대표 단체인 CSA(클라우드보안협회)글로벌의 장 리베스 대표는 19일 CSA코리아가 개최한 “클라우드 보안: 고려와 행사에서 가져올까” 만나 이렇게 말했다. “현재 각 국가·지역의 법적 요건에 맞춰 클라우드 컴퓨팅을 운영하고 보안 투명성을 제공하는 것이 중요하다”고 강조했다.

클라우드 컴퓨팅 사용이나 확산 결정으로 작용하는 데이터 침해나 해킹 공격 등 보안 우려와 관련해서는 “클라우드 컴퓨팅은 위험성이 존재하고 있고, 완벽한 보안을 구현하기는 어렵지만 투명성을 유지함으로써 합리적 수준의 보안 대책을 확보할 수 있다”고 단언했다.

<출처 : IDG, 디지털데일리>

대응 현황

- ISO27001, ISAE 3402 SOC 인증, ISMS 등 인증확보
- 공공분야 G-Cloud 보안시험인증을 완료(관련 부처 공식인증 준비중)

1 클라우드 보안

2 클라우드 주요 특징 및 보안 위협
(CLOUDSEC Conference 2014 신영상 박사)

3 클라우드 정보보안전략

클라우드 정보 보안

침입

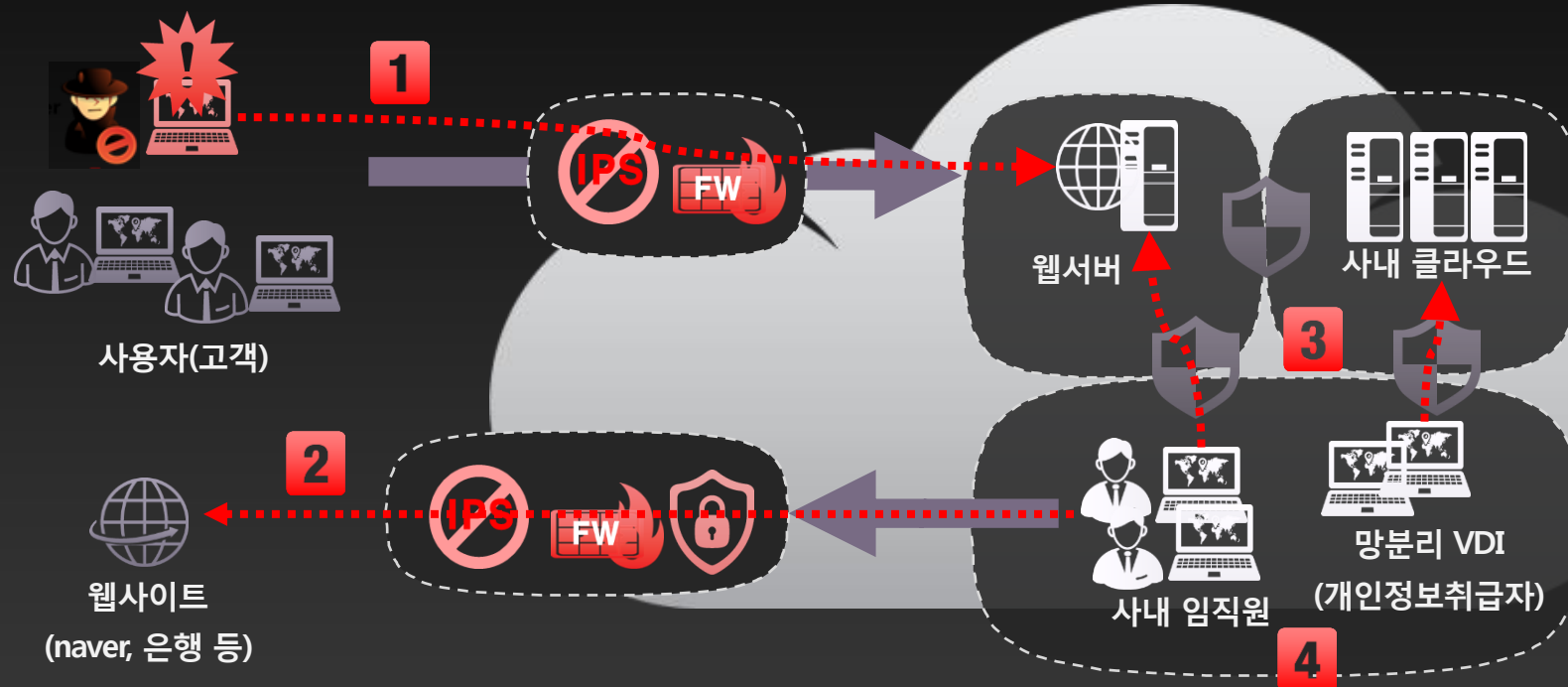
- 클라우드 서버, 임직원 단말에 악성코드 감염 시도

전파(확산)

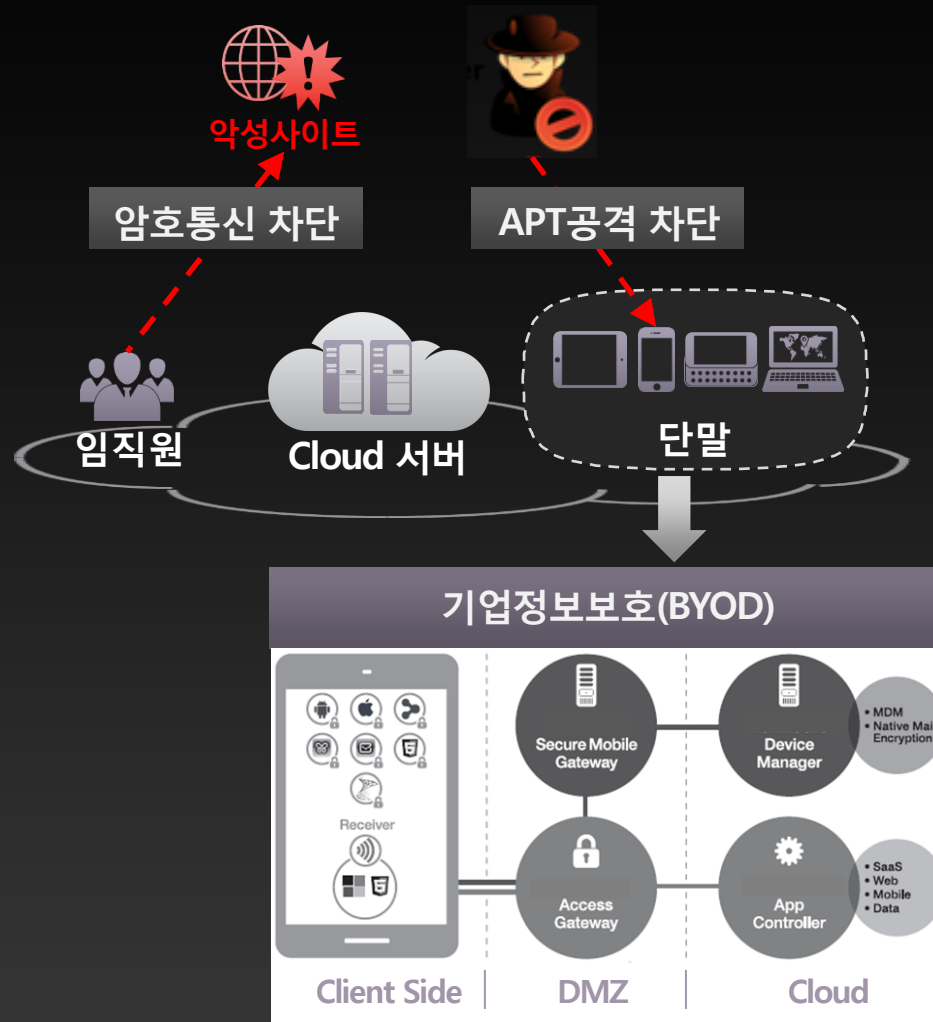
- 침입에 의해 확보된 서버, 단말을 이용한 내부정보 수집

정보유출

- 수집된 정보 중 주요정보 (개인, 기업) 외부유출 시도



기업 개인정보 유출 예방 분야



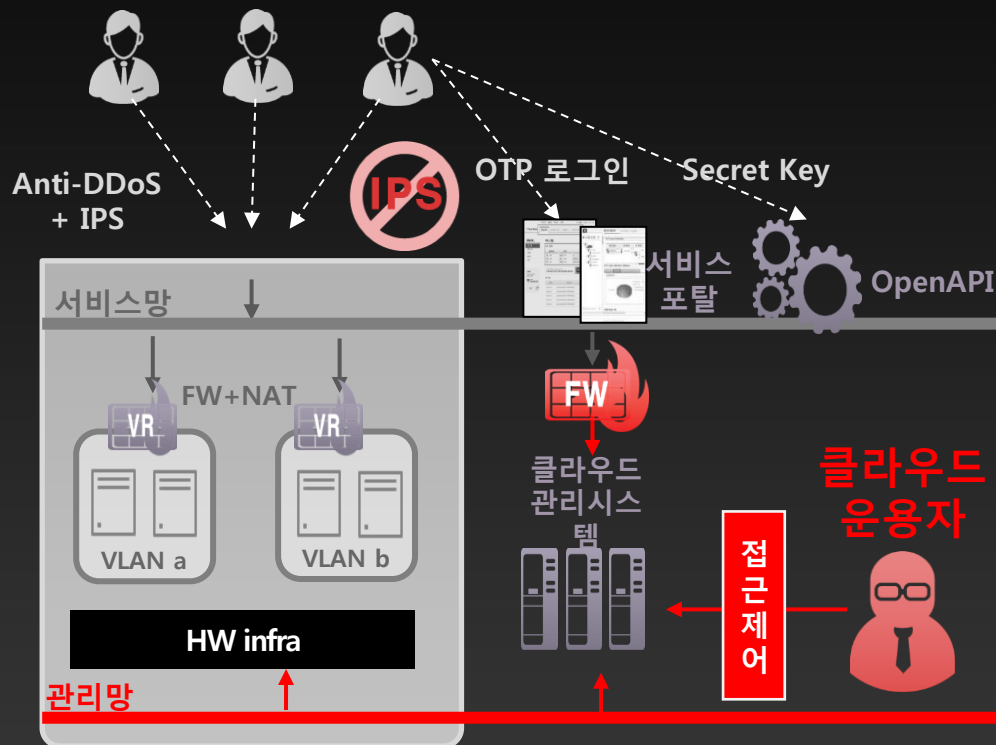
- PC 개인정보 격리/유통

- PC 수준진단 솔루션

- 서버 개인정보 검출

- 모바일 단말 통제

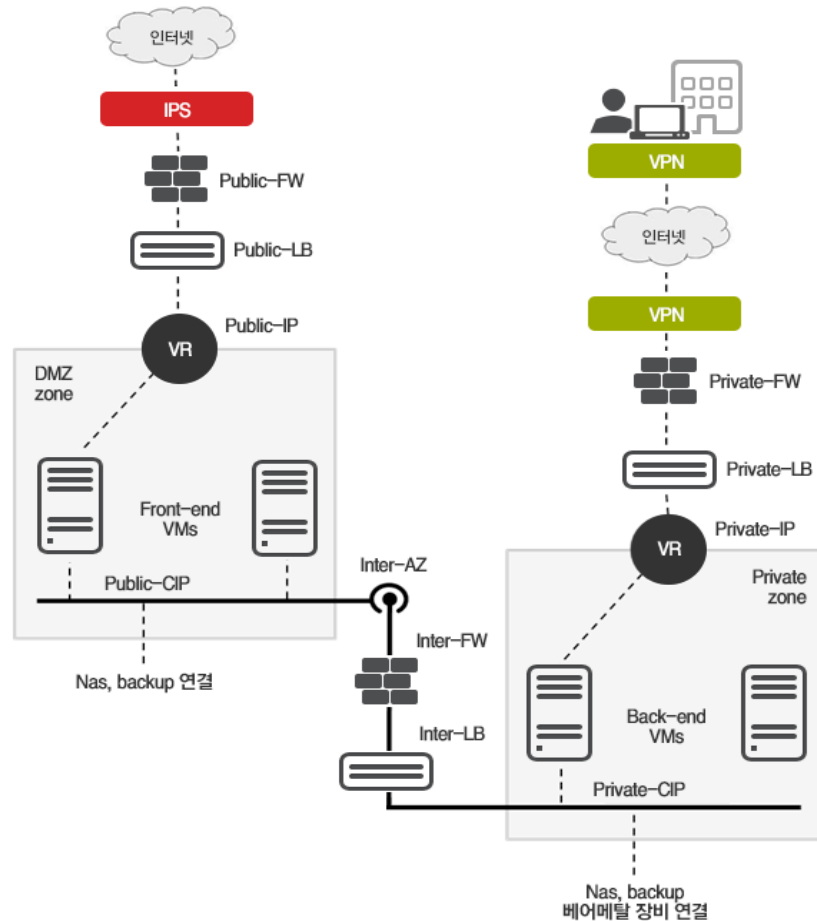
클라우드 시스템 접근통제 분야



접근통제 강화 (인증/권한관리)

- 1 개인정보 취급자 망분리 통제
- 2 서버 계정통제
- 3 인프라 VPN
- 4 OS 통제(STG)
- 5 DB 통제(DB-i)

침해사고 예방/대응 분야



1 정책 관리

2 Clean Zone(Ddos)

3 로그 상관 관계 분석

4 통합 보안 관제

SDP (SOFTWARE DEFINED PERIMETER)

- Invisible Cloud 구축 : 애플리케이션에 있는 DNS 정보나 IP주소를 제거



No visible IP address
(including DNS entries)

No response to pinging them



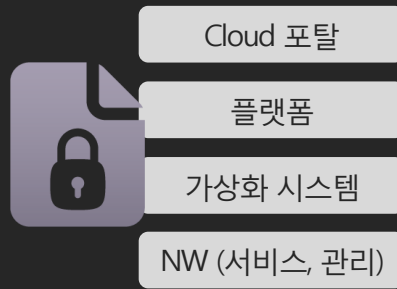

No SYN/ACK

No open ports at all

민간 클라우드 활성화를 위한 전략 (KT G-Cloud)

- 공공 기관이 신뢰하고 민간 클라우드를 사용할 수 있도록 정보보호 기준을 고시하고, 이를 기반으로 보안 인증제 추진

클라우드 컴퓨팅 서비스 정보보호 기준 ('16.4월 고시)

관리적 보호조치	물리적 보호조치	기술적 보호조치	공공기관 추가조치
 <ul style="list-style-type: none"> · 정보보호 정책 및 프로세스 · ISMS, ISO27001 등 인증 	 <ul style="list-style-type: none"> · 천안 클라우드 전용 데이터 센터의 엄격한 출입 통제 	 <ul style="list-style-type: none"> · 가상화 환경 보호 · 네트워크 및 시스템 접근 통제 	 <ul style="list-style-type: none"> · 공공 전용 물리적 분리 · 도입전산 장비의 CC인증 안정성

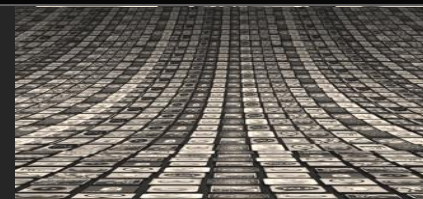
KT G-Cloud는 정보보호 기준 시범 점검을 양호하게 완료 (~'16.2)

공공 부문 클라우드 보안인증 제도

Remarks



RSA2016의 키워드 :
Connect to Protect (보호를 위한 연결)



정부 학계 기업간의 연결



위협정보 공유 및 보안전문인력 양성



IaaS, SaaS, PaaS 를 아우르는
통합적 관점의 보안 관리/정책 적용 필요



Thank you

