

<http://www.acrofan.com/ko-kr/consumer/content/?mode=view&cate=0303&wd=20111116&ucode=0003030202>

ACROFAN The Contents Agent Group

Consumer | Commerce | Life | Live

SEARCH SEARCH

Home > Live > Report

[취재] 2011 하반기 넷이벤츠 토론 I: IDC [종목] 컴퓨터 [분야] IT일반 [작성자] 류재용 [작성일] 2011.11.16. 23:35

2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아 태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

넷이벤츠는 통신 및 네트워크, 보안 기업의 C 레벨 임원들과 관련 시장조사기관이 한 자리에 모여 업계 동향 및 각 기업의 전략 등을 소개하는 정기행사다. 이번 행사에서는 엔터프라이즈 네트워킹, IT 보안, 무선 기술, 영상 회의, 클라우드 컴퓨팅, 차세대 통신망, 통신 인프라 등 업계 이슈에 관한 기업 및 시장 조사기관의 발표와 패널토론 등이 진행되었다.

16일 넷이벤츠 두 번째 세션은 IDC AP 엔드유저 및 모바일 리서치 AVP 팀 딜런(Tim Dillon)이 '데스크톱에서 스마트 디바이스로의 전환 추세에 따른 대처 - 인프라, 관리, 보안 관점에서 의미하는 바는 무엇인가?(원제: Defending the Enterprise from Latest Generation of Cyberattacks)'라는 주제로 진행했다. 엔터프라이즈 산업에서 가장 큰 당면과제로 떠오른 '보안'이 주인공인 세션이었다.



[취재] 2011 하반기 넷이벤츠 토론 I: IDC

[종목] 컴퓨터 [분야] IT일반 [작성자] 류재용 [작성일] 2011.11.16. 23:35

2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

넷이벤츠는 통신 및 네트워크, 보안 기업의 C 레벨 임원들과 관련 시장조사기관이 한 자리에 모여 업계 동향 및 각 기업의 전략 등을 소개하는 정기행사다. 이번 행사에서는 엔터프라이즈 네트워킹, IT 보안, 무선 기술, 영상 회의, 클라우드 컴퓨팅, 차세대 통신망, 통신 인프라 등 업계 이슈에 관한 기업 및 시장 조사기관의 발표와 패널토론 등이 진행되었다.

16일 넷이벤츠 두 번째 세션은 IDC AP 엔드유저 및 모바일 리서치 AVP 팀 딜런(Tim Dillon)이 '데스크톱에서 스마트 디바이스로의 전환 추세에 따른 대처 - 인프라, 관리, 보안 관점에서 의미하는 바는 무엇인가?(원제: Defending the Enterprise from Latest Generation of Cyberattacks'라는 주제로 진행했다. 엔터프라이즈 산업에서 가장 큰 당면과제로 떠오른 '보안'이 주인공인 세션이었다.



▲ IDC AP 엔드유저 및 모바일 리서치 AVP 팀 딜런(Tim Dillon)

팀 딜런 AVP는 신용카드 정보 하나 당 10센트인데 비해, 링크드인 같은 것에 들어간 신용정보는 2~3달러 정도로 거래되고 있다고 밝히고, 이제는 해킹이 금융정보에서 신상정보로 가치를 두는 타겟이 이동되었다고 설명했다. 이는 PC부터 모바일 디바이스까지 기기와 소셜 네트워크 서비스가 확산되는 환경적인 변화와도 맞물려 점점 더 큰 문제로 대두되고 있다.

소셜 네트워크는 침해상황 측면에서 보면 전례없던 경향을 보이고 있다. 일례로 60만 건의 침해가 하루 동안에 페이스북 상에서 발생한다고 한다. 소셜 네트워크는 쓰는 그 순간 내재적으로 보안이 취약해지는 측면도 있는데, 이로 인해 엔터프라이즈 등 산업 환경은 보안 관점에서 근본적으로 변화가 불피했다. 이제는 모바일부터 벤딩머신까지 보안 적용이 이슈가 되는 시대다.

2억 3천만개의 모바일기기가 아태지역(일본제외)에서 판매가 전망되고 있다. 이러한 수적 증대는 보안관리 자체를 어렵게 만들고 있다. 특히 모바일 기기 기반에서의 관리라는 것은 동기화 경향까지 보여서 조직 입장에서 대대적인 문제가 발생한다. 그런데 역설적이게도 이러한 모바일 환경 변화를 지탱하는 클라우드 컴퓨팅 서비스는 앞으로 계속 쓰일 것이라는 점이다. 특히 비즈니스에서 보면 아주 합목적성 지니고 있는 개념이고, 전세계 엔터프라이즈 소프트웨어 중 80%가 클라우드를 겨냥해 개발 중일 정도로 대세로 정착했다.

개인용이든 기업용이든 보안이 안될 수 있다. 취약점 발생은 당연한 일로 마음의 준비를 하는 것이 나올 정도다. 이러한 환경 속에서 빅데이터도 엔터프라이즈에서 가장 현실적인 이슈로 대두되고 있다. 2011년 한 해 1.8 제타바이트 데이터 용량이 생성되었는데, 오는 2014년에는 7 제타바이트 용량으로 데이터 생성이 일어날 것으로 예상되고 있다.

앞으로 점점 더 복잡성이 늘어나고, 또 기하급수적으로 데이터가 늘어나서 문제로 더오르고 있다. 이 와중에 기업 데이터는 규정과 법규를 준수해야 된다. 개인정보 보호도 덩이다. 글로벌 기업이라면 데이터 주권 문제도 있어서, 데이터가 국경을 넘을지 말지도 문제가 된다. 이제 조직들은, 사고방식 자체를 보안위협을 당연시하는 쪽으로 바꾸는 것이 차라리 나은 상황이다.

End-points and Apps



- Perimeter is everywhere
- Attack platform is the individual
- Not just your device, all
 - Best protections no longer at the gate

230+ million

threat-capable Smartphone devices
In Asia Pacific in 2012

1.3 million

"un-assured" apps

ACROTEAN

▲ 모바일 기기 보급이 늘어나면서 서비스 사용자가 폭증하는 추세다.

Cloud Services



- Resiliency questions, new core infrastructure
- Risk sharing, new governance
- Legacy will co-exist, hybrid security
- Security premium

80%

of *new* enterprise apps will be developed for cloud in 2011

30%+

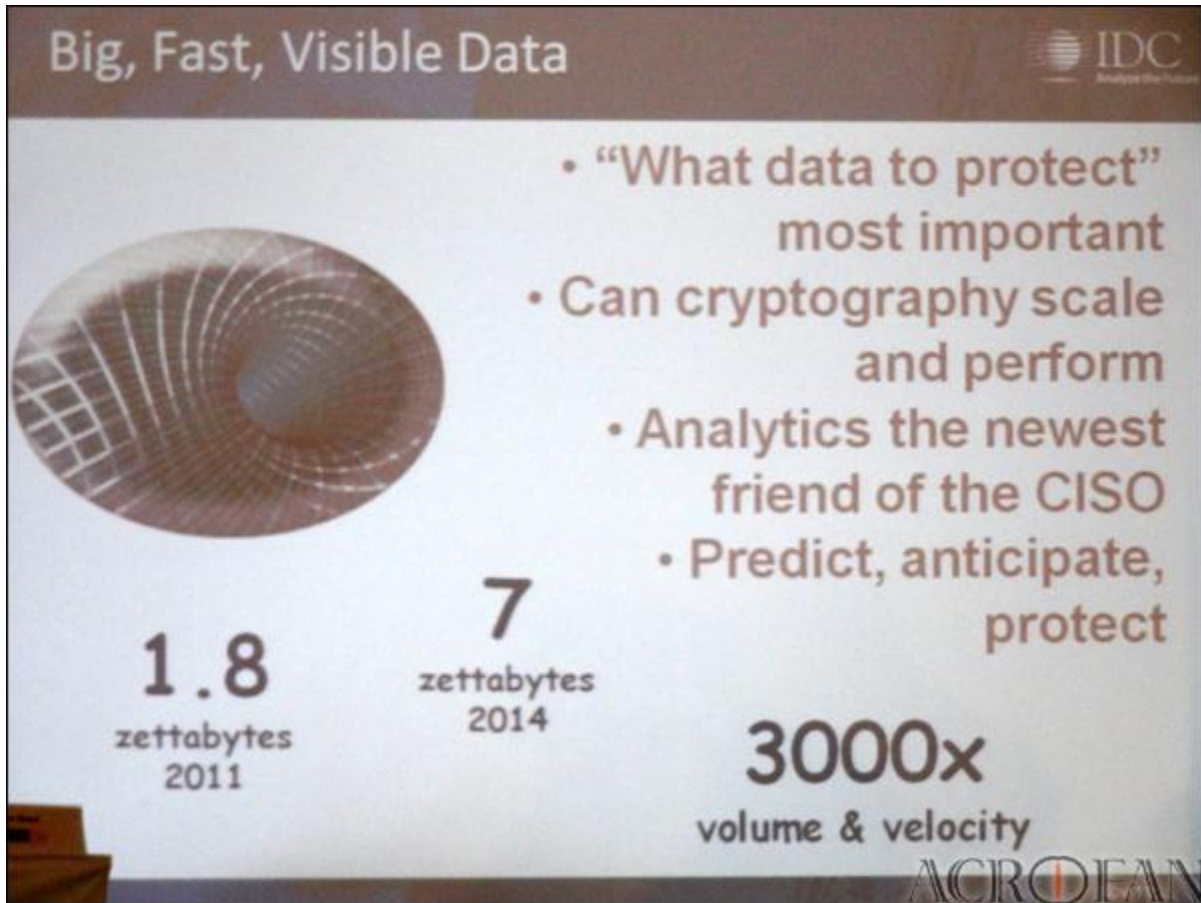
of 2014 spending on enterprise apps will be via the cloud model

>80%

of Global 2000 will still have lots of IT onsite in 2020

ACROJEAN

▲ 클라우드는 이제 도입기를 지나 한창 성장기에 진입하는 추세다.



▲ 사용자와 서비스가 늘어나니, '빅데이터'는 필연적인 과제가 되었다.

팀 딜런은 업계 현황을 살펴보는 프레젠테이션을 끝낸 뒤, 세 명의 패널과 함께 주제를 주고 받았다. 이번 패널토론에는 포티넷 에릭 찬 웡 킵(Eric Chan Weng Keong) SEA & 홍콩 리전 테크니컬 매니저, 팔로알토 네트웍스 마이크 하로(Mike Haro) 코퍼레이트 커뮤니케이션즈 디렉터, 소스파이어 레온 와드(Leon Ward) 필드 프로덕트 매니저 등이 나섰다.

Q1. 아이폰, 아이패드 등 새로운 기기가 조직으로 들어온다. 이들이 어떤 영향을 미칠까?

(소스파이어) 많은 기기를 업무에 갖고 와 썩 있다. 여기에서 발생하는 도전과제는 엔터프라이즈 네트워크를 잘 이해 못하고 있다는 점이다. 새로운 디바이스가 들어오고 계속 바뀐다. 보안 측면에서 보면 어느 정도 노출되는지 아는게 중요하다. 악의적인 공격자들이 여러분들보다 잘 알면 문제가 된다. 어떤 디바이스가 네트워크에 올라가는지 우선적으로 이해하는 게 중요하다.

(팔로알토) 팔로알토는 지난 주에 애플 iOS, OS X 지원을 발표했다. 이걸 가지고는 컨택슈얼하게 네트워크 트래픽에 대한 가시성 이해가 가능하다. 동일한 수준의 가시성을 모바일까지 확장했다. 랩탑은 이미 강구되고 있다.

(포티넷) 포티넷은 엔드포인트 솔루션을 안드로이드, iOS에서 지원하고 있다. 매니지먼트로 들어가는 중이다. 모바일 디바이스를 볼 때, 어떠한 전송수단을 택하는지 보면 무선이다. 무선까지 보안을 강구하는 것이 중요하다. 유선은 당연한 일이겠다. 요즘 나오는 솔루션들을 보면 유무선을 한 솔루션으로 통합하는 추세다.

Q2. 네트워크 패러미터에서의 방어가 타당한 방법론일까?

(소스파이어) 패러미터가 바뀌고, 움직여 나갔다. 2003~2004년도에 포럼에서 디패러미터라이선 개념을 이야기한 적이 있었다. 고객들은 다른 패러미터를 만들어 낸다. 전체 조직이 아니라 여러 네트워크 존으로 나눠서 한다. 이 대 패러미터가 더 많아지고 그런다. 물론, 안에 있다고 해서 달라지는 것은 아니다.

Q2-1. 더 나빠진 것은 아닌가?

(소스파이어) 더 복잡해지고 많아졌으니까 그렇다. 그런데 쉬워졌다고 할 수도 있다. 큰 문제를 작게 쪼개서 방어할 수 있게 되면서 문제 피해를 줄일 수 있어졌다.

(팔로알토) 네트워크 안에서 벌어지는 문제를 더 잘 파악할 수 있게 되었다.

(포티넷) 패러미터 보안은 해야 된다. 이는 외부 공격 보안을 위해서다. 지금은 페러미터 자체가 진화했다. 방화벽, IPS, URL 필터링 등을 제공하고 있다. 그런데 이게 통합되는 추세다. 새로운 솔루션들이 나오면서 새 패러미터를 보고한다. 패러미터 보호가 1단계다. 이 다음에 애플리케이션 방어를 생각해야 된다. 소니 사태를 보면, 해커가 공격해서 신용카드 정보를 탈취했다. 이 공격은 그 웹사이트가 표적공격된 경우다. 그래서 애플리케이션 보안을 봐야 된다. 웹서버를 어떻게 공격하는지 잘 신경 써서 방어해야 된다. 웹 애플리케이션 방화벽이 이거 보호역할을 맡는다. 데이터베이스 방화벽도 데이터베이스 보호를 맡는다. 앱 애플리케이션 파이어월은 차세대 방화벽에 통합될 것이다. 몇 년 전을 생각해 보면 데티케이트로 보안요소들이 개별 구성되었다. 그런데 이게 통합되는 추세다. 현재는 단일한 솔루션으로 모든 보안 처리를 하는 게 아니지만,

점점 더 통합되는 추세다. 보안 솔루션에 이것저것 개별 솔루션을 넣는 추세다. 이는 점점 빨라질 것으로 본다.

(팔로알토) 통합은 이루어져야 된다. 스테이트풀 방화벽보다 차세대 방화벽이 중요하다. 훨씬 더 많은 걸 이해해야 된다. 트래픽을 보고 이해하고 방침이 무엇이고 누가 보냈는지 다 알아야 된다.

Q3. 과거에는 트래픽 흐름이 99.9%는 예측가능했다. 그런데 요즘은 30%는 예측가능하고, 70%는 실시간이고 그런다. 여기에 동기/비동기, 모바일까지 문제가 된다. 애플리케이션 환경 자체가 변화되었는데, 성능 보장이 힘들지 않을까?

(소스파이어) 애플리케이션 트래픽은 당연히 변화다. 두 가지 종류의 애플리케이션 프로파일이라고, 앞으로 늘 다를 것이다. 그래서 가시성이 중요하다는 이야기가 연결된다. '맥락(컨텍스트)'도 마찬가지다. 조직이 다양한 경로의 트래픽을 알고 있어야 된다. 2003년에 '맥락 인지'에 포커스를 둔 기술을 개발했다. 이를 통해 소스파이어는 애플리케이션이 무엇이고 어떤 트래픽을 내고 고객에게 어떤 의미인지 파악했다. 이를 바탕으로, 맥락 기반 결정을 조직이 내릴 수 있도록 했다.

Q4. 소스파이어와 포티넷에게 묻겠다. IPS 위협대응에 얼마나 빨리 대응할 수 있는가?

(포티넷) 추적 서비스가 있다. 컨셉은 팔로알토와 유사하다. 샘플을 체크해 분석해 결과를 적용시킨다. 기존 방식은 공격자를 쫓아가는 방식이라서 느리긴 하다. 제로데이 프로텍션을 원한다면 최신 시그니처를 2시간 내에 프리미엄서비스로 제공한다. 보장하는 엑셀레이가 2시간이다.

(소스파이어) VRT 경우를 보면, 다양한 정보가 들어온다. 지금 현재 200만명 유저들이 멤버십으로 멀웨어 탐지정보를 제공해 활용할 수 있다. 매일 2만여개의 멀웨어 정보가 리서치를 통해 알게 된다. 리서치 팀에서 좋은 연구 중이다. 고객들도 탐지능력도 모호하고 있다. 개방형 체제로 돌아가는 회사여서, 보안에서 지식품을 유저들에게 사용할 수 있도록 해서 자신 문제를 스스로 해결할 수 있도록, 탐지능력을 고객들이 갖추도록 하고 있다.

Q5. 시장에 나온 프로젝트 중에서 자동화된 멀웨어 분석 툴이 많다. 그런데 어떤 기술을 채용하고 있는지는 잘 모른다. 어떤 기술이 많이 쓰이는가?

(포티넷) 리서처들이 물론 있어야 된다. 사람들이 멀웨어를 살펴 본다. 그 다음에 자동화된 엔진시스템. IPS, AV 벤더들이 사람을 쓰면서 자동화툴도 같이 쓰는 중이다. 이는 샌드박스 접근법을 채택해 돌려보고 무슨 문제가 있는지 확인해야 되어서다. 사람+샌드박스 접근법을 자동화 구조로 가는데, 모든 IPS, AV 벤더들이 같은 방법론을 쓸 것이다.

(소스파이어) 자동화 분석은 쉽지 않다. 그럼에도 해야 되는 이유는 멀웨어가 너무 많아서다. 이를 다 직접 사람들이 하기에는 부담이다. 그런데 자동화도 난해하다. 버찰머신 탐지가 어렵다. 멀웨어가 실행을 거부하는 환경에서 들어간다. 자동화가 된 방식으로 버찰머신에서 탐지한다는 게 어렵다. 샌드박스에서 실행하면 얼마나 오래 보고 결정하는지도 문제가 된다. 극복해야 될 도전과제가 자동화 그 자체에도 있다. 모든 기업과 개인이 자동화를 쓴다고 하면, 이에 대한 극복역량도 가져야 된다.

Q6. 장기적으로 보면 필요한 것이 무엇이 있을까?

(소스파이어) 회의론적으로 생각해 본다. 내일의 보안침해를, 미래 예측은 어려움이 많다. 미래는 점점 더 어려워질 것이다. 이 질문을 5년 전에 들었다면 SSL 작동이랑 트러스트 유지를 중요하다고, 글로벌 커뮤니티로 해결하기 위해서 어려움을 겪었다고 했을 것이다. 타겟팅 멀웨어나 이메일 서티피케이션 등의 도전에 직면하고 있는 고객들이 있겠지만 이에 대처하기 위해서는 민첩한 적응과 접근법이 있어야 된다. 어떤 일이 있어도 대응이 가능해야 된다. 새로운 접근법이 있어야 된다고 보고, 포인트 솔루션만으로는 안된다고 본다. 민첩한 접근법 필요하다.

(팔로알토) 보안팀이 비즈니스 이네이블드에 더 포커스를 맞춰야 된다. 기업이 더이상 애플리케이션을 리스크 때문에 차단하는 것을 허용하지 않을 것이다. 새로운 정책, 뉘앙스적인 정책으로 애플리케이션에 내장되도록 하면서 잠재적인 위협을 막는 쪽으로 갈 것이다.

(포티넷) 700명의 CIO를 대상으로 최근에 조사를 했는데, 보안 위협에 관해 주요한 지출로 무엇을 2012년에 하고 싶은지를 물었다. 여기에서는 무선 네트워크가 가장 취약한 요소라고 답변이 나왔다. 1~2년내 어떤 기술을 도입하려는지 물으니, 애플리케이션 방화벽과 통합보안을 이야기했다. 포인트 솔루션을 줄이면서 통합보안도 원했다. 포티넷은 이런 추세를 보고 있다.

