EXPERT COLUMN

POST-PANDEMIC

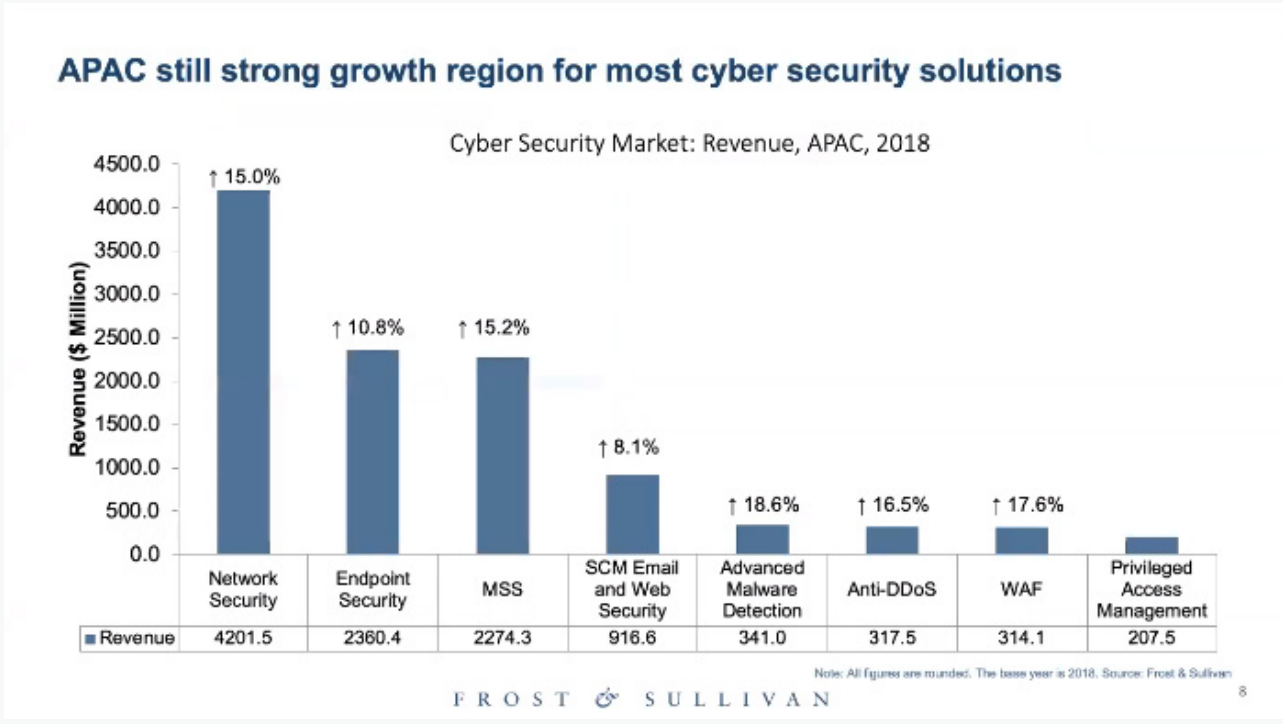
포스트 팬데믹 시대, 무엇을 준비해야 하나

포스트 팬데믹 시대 속 주목받는 '사이버 보안'

코로나19가 팬데믹(Pandemic, 세계적 대유행)으로 번지면서 글로벌 경제가 요동치고 있으며 거의 모든 산업이 영향을 받고 있다. 보안 산업도 예외는 아니다. 경제침체로 인해 보안 제품 및 서비스의 소비가 주춤해지는 등 영업이익에도 직접적인 영향을 받고 있다. 코로나19의 확산세가 한풀 꺾이며 한숨을 돌려도 된다고 생각했던 찰나에 '포스트 팬데믹(Post-Pandemic)' 또는 '뉴노멀(New normal)'이라고도 불리는 낯설고 새로운 시대가 찾아왔다. 포스트 팬데믹 시대에서 살아남기 위해서는 과거와는 다른 새로운 전략의 변화가 요구된다. 글로벌 시장조사기관 프로스트앤설리번(Frost & Sullivan)이 제시하는 포스트 팬데믹 시대가 보안 산업 및 관리자, 그리고 기업에 미치는 영향과 이에 대비하기 위해 반드시 알아야 할 연구 결과를 소개한다.

지난 4월 프로스트앤설리번(Frost & Sullivan) 보안 전문 애널리스트인 케니 여(Kenny Yeo)가 '코로나19 팬데믹 속 비즈니스 우선순위로 주목받는 사이버 보안(Cybersecurity as a Business Priority Amidst the COVID-19 Pandemic)'이라는 주제로 온라인 세미나를 진행했다.

프로스트앤설리번은 한국, 중국, 아시아 태평양과 일본(Asia Pacific & Japan) 등의 지역을 포함한 13개국에 다양한 공급 업체, 규제 기관 등의 고객을 보유하고 있다. 더불어 사물 인터넷(IoT), 인공지능, 클라우드 컴퓨팅, 사이버 보안, 디지털 거래 등의 광범위한 분야에 걸쳐 시장 조사를 실시하고 있으며 시장 전망 정보를 제공하고 있다. 프로스트앤설리번이 13개국을 대상으로 실시한 연구 결과에 따르면 2018년 사이버 보안 매출액의 가장 큰 비중은 네트워크 보안이었으며, 엔드포인트 보안이 2위, 보안 관제 서비스(MSS)가 3위를 차지했다([그림 1] 참고). 그 외에도 공급망 관리 이메일 및 웹 보안, 지능형 위협 탐지, 안티-DDoS, 웹 방화벽, 권한 접근 관리 등이 있다.



[그림 1] 2018년 사이버 보안 영업이익과 전년대비 성장률

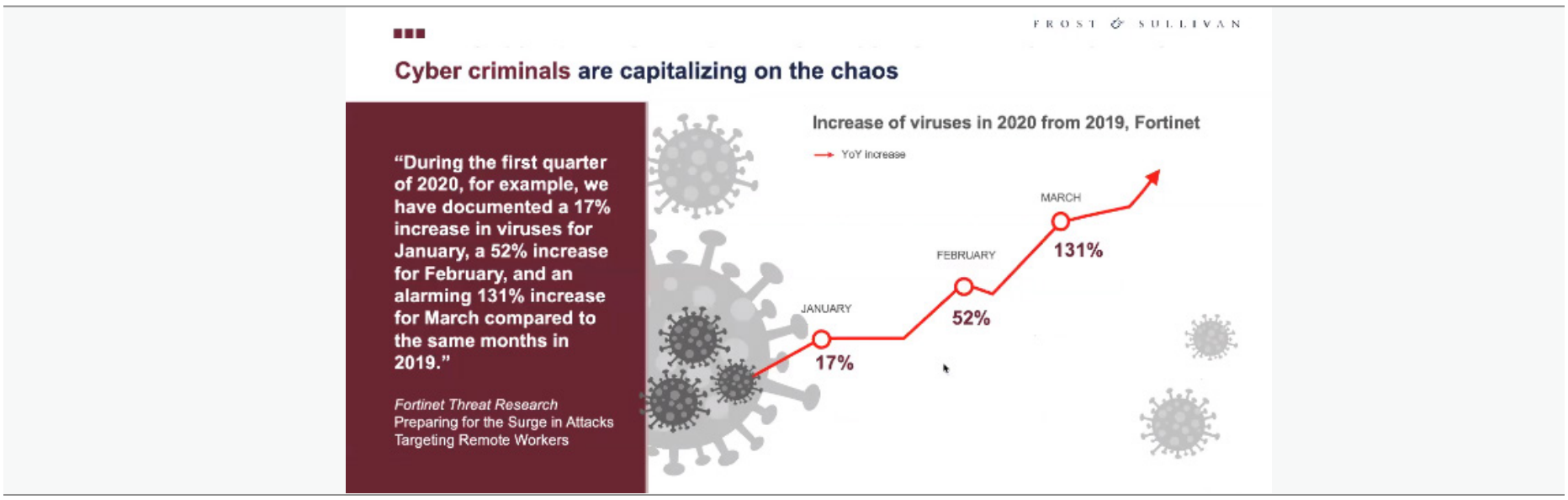
꾸준한 상승세를 이어가고 있던 사이버 보안 시장도 팬데믹이라는 큰 변화 앞에서는 주춤한 모습을 보이고 있다. 사이버 보안 시장은 팬데믹으로 인해 어떻게 변했으며 기업 성장에 영향을 미칠 가장 큰 도전 과제와 그 해결책은 무엇일까? 또한 어떻게 하면 고객과 원활하게 소통하고 잠재 고객을 확보할 수 있을까? 프로스트앤설리번은 실질적인 시장 조사 결과를 바탕으로 우리가 그토록 궁금했던 질문들에 대해 답한다.

보안 시장, 무엇이 어떻게 달라졌나

프로스트앤설리번은 아시아태평양 지역(이하 APAC)에서 글로벌 보안 산업을 선도하는 국가인 싱가포르와 말레이시아를 중점적으로 연구 결과를 진행했다. 이번 연구에 참가한 기업 임직원 대다수가 IT 관리자 또는 의사결정자 이상이었으며, IT 기업, 물류 및 운송업, 금융 서비스, 소매업과 소비자 등 다양한 산업군의 담당자가 참여했다.

디지털 트랜스포메이션은 지난 몇 년간 많은 기업들이 가장 신경 쓰고 있던 도전 과제였다. 그러나 최근에는 팬

데믹으로 인해 많은 기업들이 원격 근무에 돌입하며 오히려 보안 운영에 대한 도전 과제에 직면하고 있다. 팬데믹에서 살아남기 위해 어떻게 적응 또는 변화할지 고민하는 모습을 확인할 수 있었다. 직원들은 자택에서 근무하며 기업 정보에 접근하기 위해 개인 단말을 사용하거나 파일 공유를 위해 클라우드 컴퓨팅 서비스 또는 불안정한 링크에 접속하는 등 다양한 사이버 위협에 상시 노출돼 있다.



[그림 2] 전년 대비 2020년 1분기 악성코드 증가 추이

사이버 범죄 조직은 이러한 업무 환경의 변화를 악용하고자 발빠르게 움직이고 있다. 사이버 보안 공급 업체인 포티넷(Fortinet)에 의하면 사이버 범죄는 지난 3월 전년대비 탐지된 악성코드는 131% 증가했다. 이같이 기하급수적으로 늘어나고 있는 사이버 범죄에도 불구하고 많은 보안 솔루션 공급 업체들은 적게는 1%에서 많게는 9%까지 보안 솔루션 및 제품에 대한 수요가 줄어들었다고 답했다. 그렇다면 뉴노멀 시대를 바라보고 있는 기업들은 어떻게 대응해야 할까?

프로스트앤설리번은 팬데믹으로 인한 타격이 지역과 산업을 불문하고 1년 이상 중대한 영향을 미칠 것이라고 예측했다. 따라서 뉴노멀 시대에 고객과 원활하게 소통하고 더 깊은 관계를 형성하기 위해서는 새로운 디지털 이니셔티브가 중요할 것이라고 강조했다.

새로운 디지털 이니셔티브: 클라우드 보안

싱가포르와 말레이시아 지역의 경우 클라우드 컴퓨팅 서비스 도입률이 62%를 넘어섰다. 많은 기업들이 클라우드의 장점을 활용하기 위해 재빠르게 클라우드로 마이그레이션한 것이다.

또한 싱가포르 기업의 71%, 말레이시아 기업의 84%가 1개 이상의 클라우드 서비스를 사용하고 있어 보안 운영에 대한 부담이 증가하고 있는 것으로 드러났다. 이렇게 많은 기업들이 클라우드 서비스를 도입해서 사용하거

나 도입을 고려하고 있는 상황에서도 클라우드 보안에 대한 고민은 크지 않았다. 싱가포르의 경우 41%의 기업이 클라우드 서비스 제공 업체에 의존하거나 클라우드 보안에 많은 고민을 하지 않는다고 답했다.

클라우드 도입과 복잡성은 늘고 있는 반면 클라우드 보안에 대한 대응은 제대로 이루어지지 않고 있는 모습을 확인할 수 있다. 이에 프로스트앤설리번은 클라우드 보안은 필수이며, 클라우드 서비스 제공 업체는 보안의 극히 일부만 제공하고 있기 때문에 기업도 클라우드 보안에 대한 공동 책임을 가져야 한다고 강조했다.

프로스트앤설리번 조사에 따르면 싱가포르 및 말레이시아 기업들은 클라우드 보안 외 예산 부족, 보안 인력 및 기술 부족, 그리고 신기술 도입에 대한 고민을 도전 과제로 꼽았다.

많은 기업들이 수많은 보안 관련 도전 과제를 직면하고 있다고 답변했는데, 그럼 얼마나 많은 기업들이 보안에 힘쓰고 있을까? 놀랍게도 50% 이상의 기업들이 보안 침해 사고를 경험했거나 이를 예방하기 위한 적절한 조치를 취하지 않고 있는 것으로 드러났다.

프로스트앤설리번은 사이버 범죄 조직을 글로벌 시장과 수익 창출에 대한 전술을 공유하는 체계적이며 성숙한 일종의 비즈니스라고 정의했다. 점점 더 정교해지는 범죄로부터 기업을 안전하게 보호하기 위해 우선순위를 보안에 두어 복잡한 위협 환경에 대응해야 한다.

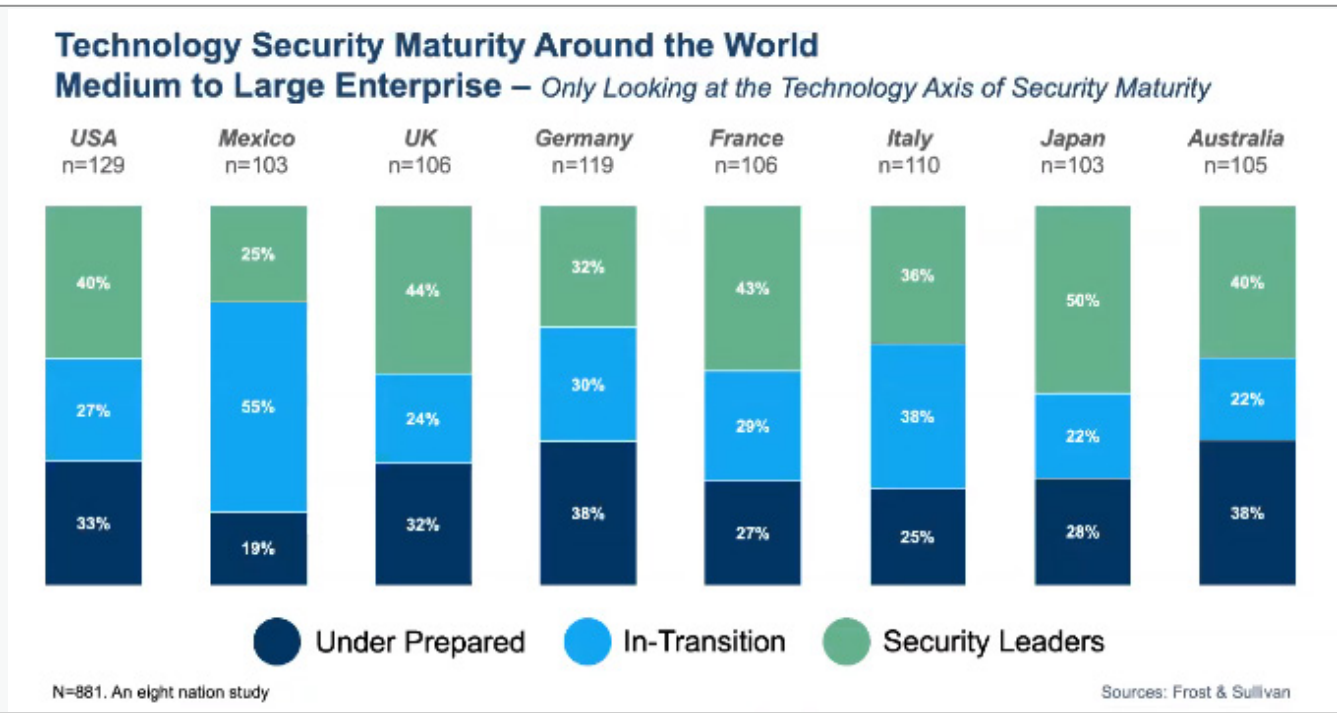
우리 기업의 보안 성숙도는 어느 정도?

그렇다면 마지막으로 사이버 범죄 조직으로부터 우리의 조직을 안전하게 보호하기 위해 IT팀을 어떻게 강화할 수 있을까? 프로스트앤설리번은 보안을 다방면으로 분석하고 대응하는 포괄적인(holistic) 보안 프레임워크를 추구해야 한다고 강조했다.

[그림 3] 보안 성숙도 모델

프로스트앤설리번은 기업의 보안 성숙도를 측정하기 위해 [그림 3]과 같은 5가지를 사용한다고 설명했다. 기업은 보안의 성숙도를 향상시키기 위해 가장 먼저 힘쓰는 부분이 조직 문화(Organization Culture), 기술 도구와 제어(Technology Tools & Controls), 보안 운영(Security Operations), 사람(People), 그리고 클라우드 도입(Cloud Adoption)이다.

많은 기업들은 이 중에서도 가장 먼저 신기술 도입에 힘쓴다. 그러나 프로스트앤설리번은 가장 먼저 보안 인력과 이에 대한 기술 교육에 힘써야 한다고 조언한다.



[그림 4] 전 세계 주요 지역별 보안 성숙도

미국, 영국, 프랑스, 이탈리아, 일본, 그리고 호주 지역을 중심으로 보안 성숙도를 조사한 결과, 일본이 가장 높은 수준의 성숙도를 띄고 있는 것을 확인할 수 있다([그림 4] 참조). 즉, 보안 침해 사고를 예방하고 대응하기 위한 실천 계획과 최고의 보안 성능을 유지하기 위한 주기적인 점검 및 보안 아키텍처를 갖추고 있는 것을 의미한다.

'아직 준비가 덜 된(under-prepared)' 기업이나 '과도기(In-transition)'에 있는 기업은 예산 부족으로 인해 보안 성숙도의 성장이 더딘 것을 아닐까? 프로스트앤설리번이 보안 예산이 100달러 미만, 100에서 499달러 사이, 500달러 이상인 기업으로 재 분류해 보았다. 그 결과, 100달러 이상인 기업들이 상당수가 여전히 과도기에 있거나 준비가 덜 된 것으로 드러났다. 따라서 예산 부족으로 인해 보안 성숙도의 성장이 더디다고 볼 수만은 없는 것이다.

[그림 5] 피싱 이메일을 악용한 사이버 범죄

전 세계 기업들의 보안 성숙도가 날로 성장하는 동안 보안 범죄는 얼마나 고도화 되었는지 살펴보자. 놀랍게도 90%의 사이버 공격은 여전히 피싱(phishing) 메일을 통해 이뤄지고 있다. 피싱 메일은 개인정보(Private data)와 낚시(fishing)의 합성어로 인터넷 사용자들을 속여 개인정보를 탈취하는 가장 오래된 공격 기법 중 하나다. 최근에는 사회공학적 기법을 활용해 사용자들의 호기심을 자극하고 불안감을 조성하는 등 다양한 방법으로 공격하고 있어 사용자의 각별한 주의가 요구된다.

따라서 기업은 사용자를 포함한 다각도로 보안을 점검해 인적 요소(human factor)로 발생하는 보안 침해 사고도 예방해야 한다. 보안 침해 사고를 예방하기 위해 보안 관리자들은 '3P 접근 방식(3P Approach)'을 고려해야 한다. 3P 접근 방식(3P Approach)은 예방(Prevent), 대비(Prepare) 그리고 예측(Predict)을 의미한다. 이 3P를 고려해 기업이 우선순위로 두어야 할 것이 무엇인지 파악하고, 이에 대비하기 위한 충분한 인력 및 기술을 갖추고 있는지 점검해 지속 가능한 사업 계획을 세워야 한다.

코로나19 팬데믹으로 인해 많은 기업들이 성장과 보안에 대한 수요가 주춤하다. 이럴 때 어떻게 고객들과 언택트(untact) 또는 디지털 방식으로 소통하여 보안을 우선순위로 만들지 고민해야 한다. 화재를 대비해 화재경보기와 소화기를 빌딩 곳곳에 배치해 두듯이 보안도 지금 당장 필요한 요소가 아니기 때문에 투자하지 않는 선택사항이 아니라 보안 침해 사고를 대비해 필수로 고려하는 우선순위가 되어야 한다. 이러한 면에서 우리 조직은 보안을 포괄적인(holistic) 관점에서 접근하고 있는지, 이에 맞춰 지속 가능한 목표를 설정해 두고 있는지 가장 먼저 점검해보기를 바란다.