



인터파크 지마켓 보안팀 행복한 보안팀의 보안 이야기

정보보호 담당자가 해야 할 일들이 점차 많아지고 있다. 침해사고 대응을 비롯해, 내부 정보 유출방지, 개인정보보호, 보안 프로세스 확립, 보안활동에 대한 평가까지. 그럼에도 정보보호팀이나 관련 부서가 수행해야 하는 여러 업무 가운데 가장 기본적인 임무는 해커의 공격으로부터 기업의 IT 자산을 안전하게 보호하는 것일 수밖에 없다. 인터파크 지마켓 보안팀은 그 기본에 가장 충실한 곳으로 손꼽히는 곳이다.

글·사진 정보보호뉴스 취재팀

다양한 구매자와 소비자가 만나는 오픈마켓은 국내 전자상거래는 물론, 인터넷의 확산을 이끌어온 주역 중 하나로 평가받고 있다. 물론 오픈마켓을 포함해 온라인 상거래의 성장배경에는 공인인증서 사용, 휴대전화 인증 등 다양한 본인확인 수단과, 에스크로우 서비스와 같은 보안 인프라가 사이버 공간의 신뢰를 높였기에 가능한 것이다.

하지만 이 같은 굵직굵직한 대책들만이 전자상거래의 신뢰를 높이는 것은 아니다. 각 기업이 제공하는 서비스의 안전성을 확보하고, 고객 정보를 내·외부의 위협으로부터 보호하는 기업 스스로의 노력이 필요하다. 최근 발생하는 각종 개인정보 유출사고의 원인으로 정보보호에 대한 각 기업의 책임감 부족이 지목되는 것은 기업의 정보보호 활동이 왜 중요한지를 다시 한번 강조하는 것이다. 그런 면에서 국내 대표적인 오픈마켓인 인터파크 지마켓은 ‘사이버 공간의 신뢰성 확보’에 사운을 걸고 있다고 해도 과언이 아니다.

행복한 보안팀의 보안 이야기

정보보호를 이해하는 경영진 만나다

“지마켓의 비즈니스 영역은 온라인을 통해 소비자와 공급자가 만나는 지점에 있어요. 때문에 사이버 공간은 지마켓의 가장 필요한 수단이자, 한편으로는 비즈니스를 위협하는 최대 위험 요인입니다.” 인터파크 지마켓 보안팀 박의원 팀장은 오픈마켓과 정보보호는 서로 불가분의 관계라고 한다.

물론 국내에도 많은 정보보호 담당자와 부서가 존재하고, 이들 대부분은 박 팀장의 말처럼 정보보호의 중요성을 공감하고 있을 것이다. 하지만 정보보호 활동이 실제로 얼마나 잘 되고 있는지는 정보보호 관련 부서가 얼마나 추진력을 갖고 업무를 할 수 있는지에 달려있다. 하지만 국내에서 기업의 정보보호 수준을 결정하는 열쇠는 기업 경영진이 가지고 있다. 때문에 정보보호 담당자들 사이에서는 정보보호 활동에 관심을 가지고 있는 경영진의 유무에 따라, 보안 담당자의 행복과 불행을 구분한다고 한다.

경영진의 지원만을 놓고 분류해 본다면 지마켓 보안팀은 확실히 행복한 보안부서에 속한다. “정보보호에 대한 리스크를 경영진이 얼마나 인식하고 있는냐 하는 점이 가장 중요한 문제인 것 같아요. 또 단순히 리스크를 인지하는 것만으로는 부족해요. 리스크에 대한 인지가 곧 투자로 이어지는 의지가 필요하죠. 리스크를 아무리 계량화한다 해도, 경영진의 실천의지가 가장 중요해요” 라는 박 팀장은 지마켓 정보보호팀이 행복한 보안 담당자로 분류된다는 사실에 고개를 끄덕인다.





“기업 정보보호 활동에서 이슈가 되고 있는 관리적 보안의 필요성도 매우 중요한 것이라고 생각해요. 하지만, 기술과 관리적 보안 체계는 함께 움직여야 하는 것이죠. 그런데 최근에는 기술적 보안이 점차 관심밖으로 밀려나 있는 것 같아요. 공격자의 기술이 발전하는 만큼 담당자의 고민도 깊어져야죠.”
 인터파크 지마켓 보안팀 박이원 팀장은 정보보호 담당자의 기술적 수준향상이 필요하다고 덧붙인다.



정보보호는 하모니다

지마켓의 행복한 보안팀은 지마켓을 이용하는 이용자들에게 신뢰를 주는 것을 가장 큰 목표로 안전한 서비스 운영 보장을 위한 사고 예방 및 대응이 그 어떤 업무보다 우선 시 된다. 최근 적지 않은 기업 정보보호팀이 기술적 대응에 대한 관심을 줄이는 상황에서 엔지니어적인 보안활동에 대한 높은 관심은 오히려 낮설기까지 하다. “일반적으로 분류하는 기술적인 보안과 관리적인 보안의 간극이 멀어지는 것은 옳지 않다고 봐요. 그런데 최근에는 관리적 보안에 대한 이슈가 부각되면서 기술적 보안은 보안 솔루션에만 의지한 채, 보안 관리자의 관심에서 점차 멀어지고 있는 것 같아 아쉬워요.” 박 팀장은 최근의 공격 기법은 점차 전문화되고 있다는 점에서 대응기술의 발전을 위한 노력도 함께 병행되어야 한다고 강조한다. “정보보호는 조화를 이뤄야 한다고 생각해요. 경영진과 보안부서의 조화, 관리적 보안과 기술적 보안의 조화 그리고 보안장비와 인력의 조화가 필요하죠. 특히 장비를 운영하는 담당자의 기술적인 능력이 반드시 뒷받침되어야 해요”

보안 솔루션의 능력차를 극대화하라

보안 기술에 대해 많은 관심을 보이고 있는 지마켓 보안팀의 새로운 계획은 보안 솔루션 운영의 고도화라고 한다. “공격기술이 다양해짐에 따라 보안 솔루션의 운영을 고도화해야 하는 부분이 있어요. 전체 서비스의 안전성을 높이기 위해서는 기존의 보안 솔루션을 단순히 운영하고 또 새로운 솔루션을 구매하는 것만이 아니라 구축된 보안 솔루션의 운영 수준을 좀 더 깊게 가져가 보자는 의도죠”라는 박 팀장은 지금까지 많은 기업들이 보안 솔루션을 도입해 사용해 왔지만, 공격기법의 진화로 인해 보안 장비를 우회하는 기술이 등장하고 있다며 우려를 나타낸다. “지난 몇 년간 운영자의 관점에서 보안 솔루션이 구축 운영돼 왔다면, 앞으로는 공격자의 관점을 점검해 볼 필요가 있다고 봐요. 공격자는 계속 발전하는데, 관리자들도 발 빠르게 움직여야 되지 않겠어요?” 라고 반문하는 박 팀장의 말 속에서 향후 몇 년내 이들의 보안 솔루션 운영 노하우가 많은 기업들에게 또 한번 모범사례를 제시해 줄 수 있을 것이라고 조심스럽게 전망해 본다. S