금융결제원 금융ISAC

사람 中心의 정보보호

전 세계에서 우리나라처럼 전자금융거래 시스템이 발달한 나라는 없다고 해도 과언이 아니다. 물론 비대면 사이버 거래에 따른 위험은 항상 존재한다. 특히 최근처럼 각종 사이버 위협이 부각되고, 실제로 크고 작은 침해사고가 발생하는 상황에서 금융기관의 침해사고는 금전적 피해 이상으로 사회적 파장을 가져올 수 있다. 때문에 금융기관에서는 작은 위협 하나도 무시할 수 없는 상황이다. 그런 의미에서 이번 호에서는 금융기관이라는 특성 때문에 보다 더 전문적이고, 보다 더 책임감 있는 사람들을 만나봤다. 금융결제원 금융ISAC이 그들이다.

글·사진 정보보호뉴스 취재팀

금융결제원은 1986년 설립 당시 어음교환과 지로제도 운영이란 업무로 시작해, 현재는 은행 간 공동지급 결제 시스템을 공동으로 구축·관리하는 영역에까지 이르고 있다. 즉, 우리가 매일 사용하는 인터넷뱅킹과 같은 전자금융거래는 금융결제원의 서비스를 통해 제공되고 있는 것이다. 때문에 금융결제원의 서비스 신뢰도와 안전성은 국내 전자금융거래의 안전성과 직결돼 있다고 해도 과언이 아니다. 그래서 금융결제원 내에는 금융기관을 겨냥한 사이버 위협에 공동대응하기 위한 금융ISAC(Information Sharing & Analysis Center)이 설립돼 있다.

정보수집에서부터 사고대응까지

"금융ISAC의 업무는 위협 정보제공 서비스, 취약점 분석평가 서비스, 실시간 보안관제 및 예·경보 서비스, 그리고 교육에 이르기까지 크게 4가지로 구분해 볼 수 있어요."금융결제원 금융ISAC 침해사고대응팀 이만호 팀장의 말이다. ISAC의 주요 업무가 그러하듯, 이들 역시 정보보호와 관련된 최신 위협 정보를 탐지하고 회원기관에 제공하는 것에서 시작된다. "모든 일에 기본이 있듯, 정보보호 분야에서도 어떤 공격유형이 등장하고, 그에 상응하는 대응전략에는 무엇이 있는지 알아내는 것이 가장 기본적인 것이라고 봐요. 최근에는 공격기술이 교묘해지고 급변하고 있기 때문에 정보습득은 매우 중요한 업무 요소죠." 많은 시간을 할애하는 이들의 정보수집 활동은 자연스럽게 365일 24시간 진행되는 보안관제 업무와 연계된다. "일반적인 보안관제가 그러하듯, 금융ISAC의 보안관제 업무는 회원기관을 위한 공동관제 시스템과 인터넷뱅킹 서비스, 침해사고 분석 예·경보 발령으로 요약할 수 있어요"라는 이 팀장은 금융ISAC 보안관제가 가진 특별함은 없다고 겸손해 한다. 하지만, 금융ISAC의 보안관제는 그 어느 곳보다 뛰어나다고 평가받는 곳 중 하나다. 그리고 그 차이는 보안관제 요원들의 능력에서 비롯된다.

사실 해킹에 성공(?)한 횟수는 그리 많지 않지만, 적어도 기업의 네트워크와 시스템을 공격하기 위한 '염탐' 횟수는 상당히 많은 편이다. 특정기업의 IT 자산을 공격하기 위한 스캐닝은 하루에도 수십, 수백 건씩 일어나고 있고, 이 같은 공격시도를 어떻게 탐지하고 또 처리하느냐가 보안관제의 핵심 요소가 된다. 그런데 그 과정은 '솔루션'이 아닌 '사람'에 의해 이뤄진다.

"공격기법이 지능화되고 또 교묘해짐에 따라 공격에 대응해야 하는 정보보호 담당자들의 실력이 매우 중요해요. 요즘처럼 취약점을 악용한 공격이 빠르게 등장하는 경우에는 더욱 그러하죠." 금융결제원 금융ISAC 침해사고대응팀 이만호 팀장은 정보보호 활동에 있어 담당자의 능력이 가장 중요하다고 역설한다.

공격자의 기술, 따라잡아야 한다

이런 사실을 어느 누구보다 잘 알고 있는 이 팀장은 때문에 금융ISAC의 관제요원들은 일정 이상 '내공'을 가진 요원들로 구성돼 있다고 말한다. "현재의 상황에서 공격시도 자체를 막는 방법은 없다고 봐요. 사고발생 이전에 위협을 감지하고 빠르게 대처하는 것이 가장 중요하겠죠. 다양한 보안 솔루션이 등장하면서 정보보호 담당자들이 보안 솔루션에 의존하는 경우가 많아지고 있지만, 그 기기를 활용하는 사람의 기술이 더 중요하다고 봐요." 금융ISAC 침해사고대응팀 박상수 차장 역시 매번 새로운 이슈가 등장하는 사이버 위협에 대응하는 가장 효과적인 방법은 실력있는 사람을 양성하는 것이라고 강조한다. 여기에 금융이라는 산업구조를 누구보다 잘 알고 있는 이들이 수행하는 보안관제는 큰 강점을 가질 수밖에 없다. 그리고 금융권에 대한 특화된 이들의 정보보호 전략은 2003년부터 진행해 온 금융기관에 대한 취약점 점검 서비스에서도 빛을 발한다.

"금융기관들이 제공하는 서비스에 대한 특징을 이해한다는 것만으로도 금융ISAC의 취약점 점검 서비스는 차별화돼 있다고 봐요. 금융환경에 대한 전문가적 접근을 통해, 취약점 결과와 대응방안을 효과적으로 제시할 수 있기 때문이죠." 보안관제와 마찬가지로 취약점 점검 서비스 역시 금융 ISAC이 제공하는 차별화된 서비스라고 이 팀장은 강조한다.

금융기관 겨냥한 공격, 공동 대응으로 해결

최근 금융기관을 대상으로 다양한 공격 유형이 등장하고 있다. 그동안 발생하지 않았던 피싱공격을 비롯해 DDoS 공격, 개인정보 유출시도, 무선 랜 보안 등의 위협들이 고개를 들고 있고, 그래서 이런 공격을 차단해야 하는 금융ISAC은 더 바빠진다.

"모든 침해사고가 그렇지만, 한 기관에서 발생하는 사고는 다른 기관에서도 동일하게 발생할 수 있어요. 단순한 정보의 공유만이 아닙니다. 최근의 공격성향이 과거와 달리, 돈을 목적한 것이 많아졌기 때문에 특히, 금융기관의 정보보호는 한시라도 눈을 뗄 수 없는 상황이죠" 라는 이 팀장은 ISAC의 설립 취지를 최대한 살려 최신의 공격 위협으로부터 회원사를 보호하는 공동 대응 시스템을 구축해 나갈 것이라고 강조한다.

금융기관으로서 최고의 보안 서비스를 펼쳐야 하는 '숙명'을 지닌 금융ISAC. 그리고 그들 앞에 놓여진 위협들. 이들이 만들어내는 공동의 방패가 어떤 창들을 막아낼 것인지 지켜보는 것은 흥미로운 일이 아닐 수 없다. S