금융정보를 노리는 사이버공격의 진화

120241001 박현승

금융정보를 탈취하여 금전적 이득을 취하려는 사이버공격이 진화를 거듭하고 있다. 대표적인 공격루트는 신용카드이다. 신용카드는 사용의 편리함과 다양한 이용으로 인하여 현금을 대체하는 일반적인 지급수단으로 자리잡았으나, 편리함의 이면에는 보안 위협이 항상 존재한다. 2008년부터 시작된 POS 악성코드 공격은 지속적으로 증가하고 있으며, 피해 규모는 수천만건에 달하는 것으로 추정된다. 해커는 복제카드를 제작하여 사용하거나 카드 정보를 암시장에 거래하여 금전적 이득을 얻는다. 공격자들은 다크웹을 통하여 공격 툴을 손쉽게 획득하고 이를 활용하여 카드 정보를 탈취한 후, 탈취한 카드 정보를 다시 다크웹 유통망을 통하여 거래하는 것으로 알려졌다. 기업의 입장에서 직접적인 금전적 손실은 발생하지 않으나, 결제 수단을 변경하여야 하는 등의 간접적인 피해가 따른다. 국내에서는 신용카드 정보 유출 피해를 막기 위하여 IC 카드 도입, IC 방식의 POS 단말기 리더기 교체, 이상금융거래를 탐지 및 차단하는 FDS(이상금융거래탐지시스템) 운영 등의 조치를 취하고 있다. 또한 국외 부정 사용을 차단하기 위하여 국외 거래 발생 시 실제 출입국 유무를 출입국관리소에 확인한 후 거래를 승인하는 등의 부가 서비스를 운영하고 있다. 디지털 경제의 발전으로 인하여 금융정보를 타깃으로 한 사이버공격은 지속적으로 진화할 것이다. 다단계 인증, 비밀번호 시스템 개선 등 관리자와 사용자는 각자의 영역에서 금융정보 유출을 막기 위한 적극적인 노력을 기울여야 한다.