1. 디지털 흔적 분석하기

 사용자가 온라인 공간에 남긴 ‘디지털 흔적’은 매우 방대하기 때문에 이를 전부 삭제하는 것은 불가능한 일이다. 사전에 사용자의 게시물을 삭제하는 예약 기능이 소셜 미디어에 새로 추가된다 하더라도, 사용자의 디지털 흔적을 지우기 위한 삭제 버튼은 없다. 언제 한번은 한 사이트에서 예약 삭제 기능을 탑재했는데 생각보다 대단히 어려운 작업이었으며, 상당한 시간이 소요됐고, 아주 일부분의 게스트만 삭제됐다.

온라인 전역에 사용자 정보가 퍼지기 때문에, 가치 있는 정보가 어떤 사이트에 저장돼 있는지 파악하는 것이 무엇보다 중요하다. 예를 들어, 얼마나 많은 웹사이트가 사용자의 신용 카드 정보를 보유하고 있는지, 얼마나 많은 사이트가 최신 카드 번호와 유효 기간 정보를 알고 있는지, 어떤 웹사이트에 중요한 문서와 파일, 비디오를 저장해 뒀는지를 알아야 한다는 것이다. 스프레드시트에 리스트를 작성하는 것에서부터 작업을 시작할 수 있으며, 각각의 사이트에 저장된 민감한 정보의 종류를 기입한다. 더 이상 이용하지 않는 사이트가 있다면, 해당 사이트의 사용자 계정을 삭제한다.

2. 가장 민감한 계정의 우선순위 정하기

 자신의 디지털 흔적을 분석하는 작업을 끝냈다면, 가장 민감한 계정의 우선순위를 정할 수 있으며, 주요 계정은 가능한 높은 보안 수준을 지정하면 된다. 사용자는 개인 자산 정보와 개인 건강 정보와 같은 민감한 데이터를 보유하고 있는 계정에 우선순위를 둘 수 있다. 좀 더 쉽게 하기 위해서는 각각의 사이트와 관련된 데이터 민감도에 따라 보안 수준을 낮음/중간/높음으로 분류하면 된다.

보안 수준에 따라 계정을 분류하기 위해서는 자산 및 건강 정보와 같은 민감한 데이터뿐만 아니라, 얼마나 많은 문제가 발생할 수 있는지도 고려해야 한다. 이를 테면 누군가가 사용자의 계정을 해킹해서 얻은 정보로 데이터 수정이나 부당 요금 청구, 신원 도용과 같은 문제를 일으킬 수 있다.

3. 우선순위가 높은 계정에는 가능한 강한 접근 제어와 인증 방식 설정하기

 우선순위가 높은 계정들은 하나씩 검토한 뒤, 보안 및 개인정보 보호 설정을 높인다. 즉, 좀 더 강력한 비밀번호를 설정하거나 보안 질문을 변경하고, 가능한 높은 수준의 인증과 개인정보 보호 설정을 하라는 뜻이다. 혹은, 이 계정의 비밀번호를 자주 바꾸는 것도 한 방법이다.

보안 질문에 대해 블로거 조니 에반스는 “답변은 정확한 것이 아니라, 사용자만 기억할 수 있는 것이어야 한다”고 강조했다. 최근 아이클라우드 누드 사진 유출 사건의 경우, 전반적인 공격 방식 중 하나로 보안 질문에 대한 답변을 쉽게 추측해냈는데, 에반스의 말을 따른다면 이와 같은 보안 사고를 막는 데 도움이 될 것이다.

가능하다면 사용자는 온라인 뱅킹, 아이클라우드와 같은 모바일 앱에 2단계 인증(2FA)를 설정하는 것이 좋다. 2단계 인증은 “사용자가 알고 있는 것(1단계)”과 “사용자가 소유하고 있는 것(2단계)”를 포함한다. “사용자가 소유하고 있는 것”은 스마트폰의 SMS로 발송되는 인증 코드를 의미한다. 최근 출시된 스마트폰의 경우, 지문과 같이 고유한 생체 인식 인증 방식을 탑재하기도 했다.

4. 보안 패치를 최신 상태로 유지하기, 온라인에 정보를 제출 할 때 주의하기, 데이터를 주기적으로 백업하기

 바이러스, 악성 코드의 위협을 최소화하기 위해서는 운영체제, 브라우저와 같은 소프트웨어에 대한 최신의 보안 패치를 받아야 하며, 게시물을 작성할 때는 최소한의 개인 정보만 담아야 한다. 온라인 쇼핑 사이트에서는 작은 글씨로 쓰인 ‘월 정액제’라는 말을 주의 깊게 살펴서, 할인가보다 더 많은 금액에 계약하지 않도록 주의한다.

DHS의 ‘멈춰라.생각하라.연결하라(Stop.Think.Connect)’ 캠페인은 좀 더 안전한 온라인 습관을 기를 수 있는 몇 가지 좋은 방법을 제시한다. 또한, 온라인 서비스 또는 외장 디바이스에 자신의 데이터를 백업해야 한다. 자동 백업 스케줄은 규칙적인 데이터 백업의 한 방법이 될 수 있다.

5. 자신만의 BC/DR 계획 미리 갖추기

 의심스러운 행위를 탐지하기 위해서는 사용자 계정을 늘 예의 주시해야 한다. 단순히 은행 계좌뿐만 아니라, 사용하지 않은 국제전화 비용이 직불 카드에서 자동 이체로 빠져나가는 해킹이 일어날 수 있는 다른 온라인 서비스도 살펴봐야 한다. 만약 해커가 사용자의 PIN번호를 알아냈다면, 사용자가 이 사실을 인지하기 전까지는 계속 국제 전화 비용을 자동 청구할 것이다 자신의 계정에 문제가 발생한 것을 인지했다면, 다른 계정에도 문제가 없는지 잘 살펴봐야 한다.

기업의 시스템과 마찬가지로, 사용자는 자신만을 위한 비즈니스 연속성(BC)/재해 복구(DR) 계획을 세운다면 데이터가 물리적 손상을 입는 경우나 사용자 계정이 사이버 공격으로 침해 당한 경우에 대비하는 데 도움이 된다. 이 계획은 사용자 접근에 대한 ‘평소와 다름없는’ 운용 및 복구를 도와준다. 신분 도용을 신고할 수 있는 전화 번호 목록과 도난을 대비해 신용 카드 번호 목록은 따로 보관해준다. 이 정보를 스마트폰에 저장하거나 종이로 인쇄해둔다면, 신용 카드 도난 즉시 이를 신고할 수 있다. 물론, 카드의 PIN 번호는 따로 보관해두지 말아야 하며, 쉽게 추측할 수 있는 정보를 활용해서 PIN 또는 비밀번호를 생성하지 않는다.