okta

체크리스트:

데이터 유출을 방지하는 12가지 핵심 단계

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

체크리스트: 데이터 유출을 방지하는 12가지 핵심 단계

오늘날 조직들은 클라우드, 모바일, 최신 플랫폼, 레거시 온프레미스 애플리케이션 등 다양한 환경에서 데이터를 보호해야 하는 문제를 겪고 있습니다. 빠르게 늘어나는 많은 양의 데이터를 보호하기란 쉽지 않습니다. 산업 분야와 조직의 규모를 막론하고 모든 기업이 데이터 유출 문제에 노출되어 있다는 사실이 이러한 문제를 더욱 복잡하게 만들고 있습니다. 실제로 Ponemon의 보고 에 따르면 데이터 유출에 따른 총 복구 비용이 평균 362만 달러에서 386만 달러로 6.4퍼센트 증가한 것으로 나타났습니다.

기업이 보안 시스템을 강화하고 있긴 하지만 이러한 데이터 유출 사고의 대부분이 아이덴티티 기반 공격이라는 사실을 깨달아야 합니다. 실제로 2017 Verizon 데이터 유출 조사 보고서에 따르면, 데이터 유출 사고의 81%가 탈취되었거나 취약한 자격증명에서 비롯되는 것으로 나타났습니다. 이제는 데이터 유출을 저지하기 위해 적극적인 조치를 취해야 할 때이며, 이때 주요 위협 벡터 중 하나를 차단하도록 조치를 취해야 합니다.

Okta에서는 데이터 유출의 주요 원인 중 하나인 아이덴티티 기반 공격을 차단하는 데 도움이 되는 전략 및 전술적 팁을 제공하기 위해 이 체크리스트를 작성했습니다.

아이덴티티 집중화

조직들은 저마다 계정과 비밀번호가 있는 수천 개의 애플리케이션을 보유하고 있습니다. 이렇게 많은 계정과 비밀번호를 관리하는 일이 점차 문제가 되고 있습니다. 게다가 여러 개의 계정에 동일한 비밀번호를 허술하게 사용하는 직원들이 많은 실정입니다. 가장 많이 사용되는 10가지 비밀번호 중에는 Password123와 Football이 있습니다. 이로 인해 공격자가 자격증명을 추측하거나 탈취하여 액세스를 확보(주로 여러 개의 계정)할 가능성이 높아지게 됩니다.

- ❑ SSO(single sign-on)를 이용해 계정과 액세스를 중앙에서 관리하세요.
  이는 사용자와 관리자 모두 간편하게 관리할 수 있는 방법입니다.
- ❑ 가능하면 비밀번호를 없애는 방안을 고려하십시오. 비밀번호를 없애면 비밀번호 취약성으로 인한 위험이 줄어들 수 있습니다.
- ❑ 모든 곳에서 고유하고 강력한 비밀번호를 사용하십시오.
  이렇게 하면 자격증명 스터핑이나 비밀번호 살포 공격과 같은 아이덴티티 기반 공격의 위험이 줄어들게 됩니다.

강력한 인증 구현

강력한 비밀번호를 사용하고 있다고 할지라도 피싱 공격을 받거나 탈취될 가능성이 있습니다. 강력한 인증 체계는 조직의 가장 중요한 자산인 데이터에 대한 액세스를 강화하는 데 도움이 됩니다.

- ❑ 가능한 한 모든 곳의 인증을 강화하십시오. 이렇게 하면 공격자가 탈취된 아이덴티티를 통해 액세스를 확보하거나 권한 에스컬레이션을 사용해 네트워크 내 다른 계정을 겨냥하는 것을 방지할 수 있습니다.

- ❑ 모든 애플리케이션 전반에 걸쳐 MFA(Multi Factor Authentication)를 구현하십시오. MFA를 사용하면 자격증명이 탈취되더라도 무단 액세스를 방지할 수 있습니다.

- ❑ 적응형 기능을 통해 MFA 솔루션을 실행하십시오. 이 테크놀로지는 사용자, 디바이스, 위치 등과 같은 각종 속성을 기반으로 상황에 맞는 액세스 결정을 지능적으로 내리는 데 도움이 됩니다. 이렇게 하면 엔드 유저의 부담을 줄이고 높은 보안 표준을 유지하여 사용자가 필요할 때에만 인증을 강화하도록 유도함으로써 전반적인 사용성이 개선됩니다.

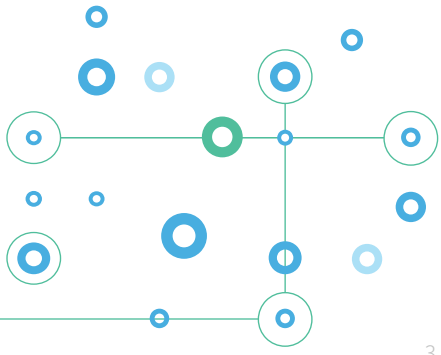
공격 대상 축소

퇴사하는 사용자로 인해 "좀비" 계정(디프로비저닝이 되지 않은 미사용 계정)이 생길 수 있는데 이로 인해 공격 대상이 노출될 수 있습니다. 귀사 역시 직무를 변경하는 사용자나 직원이 많을 수 있는데, 이로 인해 과도한 권한이 예기치 않게 생성될 수 있습니다. 가령, 경리과에서 인사부로 자리를 옮기는 직원의 경우 중요한 근로 계약 정보에 계속 액세스할 수 있게 되는데, 이로 인해 해당 직원의 계정이 공격자에게 노출될 수 있습니다.

- ❑ 가능하면 프로비저닝과 디프로비저닝을 자동화하십시오. 입사자/퇴사자 계정관리 프로세스를 자동화하면 직무나 권한의 업데이트 또는 계정 비활성화 작업을 기억할 필요가 없습니다.

- ❑ 각 애플리케이션에 액세스 권한을 가진 사용자와 그룹을 확인할 수 있도록 보고 기능을 구현하십시오. 이는 가시성 확보에 유용하며 감사 절차에도 도움이 됩니다.

- ❑ 애플리케이션에 대한 사용자 그룹 액세스를 주기적으로 검토하십시오. 적합한 사람이 자신의 역할에 대해 적정 수준의 권한을 갖게 하는 것이 중요합니다.



가시성 및 민첩한 대응 실현

모든 보안 격차를 해소할 수는 없을지라도 사전 대응적으로 보안 시스템을 최대한 강화할 수는 있습니다. 가시성과 통제력을 높이면 조직 내의 보안 현황을 총체적으로 시각화하여 보안에 신속이 대응할 수 있습니다.

- ❑ 아이덴티티 데이터를 사용해 가시성을 향상시키십시오. 이로써 데이터 유출로 피해를 입은 대상을 비롯해 액세스된 애플리케이션이나 계정을 파악하고 기존의 보안 투자 자산을 효과적으로 활용할 수 있습니다. 예를 들어, 특정 IP 주소에서 인증에 여러 차례 실패한 경우 이를 조사 대상으로 플래그처리할 수 있습니다.

- ❑ 전체적인 상황을 파악할 수 있도록 다른 보안 기록과 데이터를 아이덴티티 데이터와 연관시킵니다. 가령, 네트워크 기록과의 상관관계를 파악하면 네트워크 내에서 공격자가 어디서 어떻게 이동했는지 알 수 있습니다.

- ❑ 아이덴티티를 통해 대응 속도를 높입니다. IAM(Identity and Access Management) 솔루션의 경우 인증을 강화하도록 유도하거나, 혹은 의심스러운 이벤트나 사건이 발생할 경우 애플리케이션에 대한 사용자의 액세스를 제거할 수도 있습니다.

요구사항에 대한 충족 여부 확인

데이터 유출과 자격증명 기반 공격이 확산하면서 새로운 보안 시대가 빠르게 열리고 있지만 대부분의 조직들이 이러한 시대적 흐름을 따라가지 못하고 있는 상황입니다. 보안 솔루션은 본래 해커가 쉽게 침투하지 못하도록 복잡하게 설계되기 때문에 사용자와 관리자가 사용하기에 복잡한데, 바로 이 부분에서 많은 조직이 문제에 봉착하게 됩니다. 하지만 이제는 사용자와 관리자가 편리하게 사용할 수 있는 지능적인 보안 솔루션을 구현할 수 있게 되었습니다. Okta는 적응형 MFA와 SSO(Single Sign-On), 그리고 수명주기 관리 기능을 탑재한 간편하고 지능적인 보안 솔루션을 제공합니다. 이들 솔루션은 온프레미스와 클라우드 환경의 애플리케이션에 대한 액세스를 보호합니다. Okta는 가장 중요한 작업을 수행하는 데 필요한 테크놀로지를 안전하면서도 쉽게 사용할 수 있도록 만들어 조직이 자사의 임무를 달성할 수 있도록 지원합니다.

Okta가 조직의 안전을 보호하는 방법에 관한 자세한 내용은 데이터 유출 방지 페이지를 참조하시기 바랍니다.