IBM Security

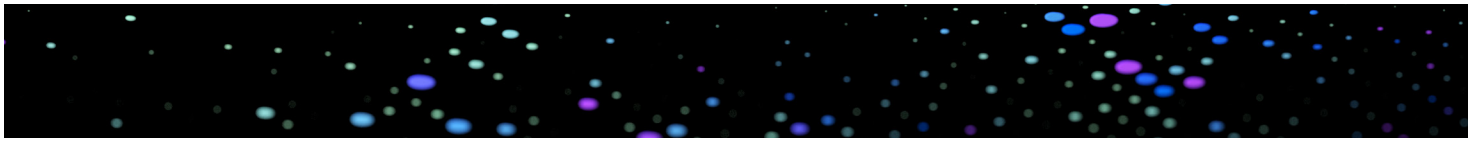
2021 IBM Security X-Force 내부자 위협 보고서

IBM Security X-Force Threat Intelligence

2021년 2분기 특별 인텔리전스 보고서

IBM

목차



소개

공격자와 방어자 모두 새로운 기술과 프로세스로 혁신을 꾀하고 있으므로 사이버 위협 환경은 끊임없이 변화하고 있습니다. 조직들은 자산을 보호하고 공격을 방지하고 이에 대응하기 위한 인력을 채용하기 위해 전체적으로 연간 약 600억 달러를 지출하고 있습니다. 보안 지출은 2021년에 10% 증가했습니다.[1]

조직의 주된 보안 노력과 이를 위한 지출의 많은 부분은 회사 밖에서 시작된 공격을 저지하기 위한 것이지만, 내부자 위협은 간과되는 경우가 많습니다. 내부자 위협은 조직 내에서 발생합니다. 많은 경우 악의적이지 않거나 우발적인 것으로 밝혀지는 내부자 위협은 데이터 도난, 재무 손실, 지적 재산 도난, 평판 훼손 등의 형태로 파괴적인 피해를 불러올 수 있습니다. 2020년 설문조사에서 Ponemon Institute는 조직들이 인시던트의 원인에 상관없이 내부자 위협으로 인한 인시던트에서 복구하는 데 평균 644,852달러를 지출한다고 추정했습니다.[2] 이러한 비용에는 의심스러운 내부자 이벤트를 모니터링하고 조사하는 데 드는 비용과 내부자 인시던트 대응, 통제, 제거, 해결 비용이 포함됩니다.

이 보고서에서 IBM Security X-Force는 내부자를 다음과 같이 정의합니다.

— 우발적 내부자: 부주의한 직원 또는 타사 벤더/계약자.[3]

— 악의적 내부자: 범죄 의도를 가졌거나 악의적인 직원 또는 타사 벤더/계약자.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. 부주의한 내부자는 조직 내에서 데이터 또는 시스템의 기밀성, 무결성 또는 가용성에 영향을 주는 인시던트를 우발적으로 유발하는 내부자로 정의됩니다. 여기에 피싱/사회 공학 인시던트는 포함되지 않습니다.

X-Force는 실제 인시던트 대응 조사에서 수집된 독점적 데이터를 사용하여 2018년부터 2020년까지 조직에 영향을 끼친 내부자 위협 인시던트 의심 사례(우발적 인시던트와 악의적 인시던트 모두 포함)를 분석했습니다. 이 보고서는 가장 두드러진 내부자 위협 공격에 대한 오픈소스 정보를 보고하는 동시에 이러한 데이터를 통해 얻은 중요한 정보를 살펴볼 것입니다. 주요 내용은 다음과 같습니다.

— 대부분의 내부자 공격이 발견되는 경로.

— 액세스 수준이 내부자 공격과 관련하여 수행하는 역할.

— 내부자 위협을 완화하기 위한 우수 사례

주요 연구 결과

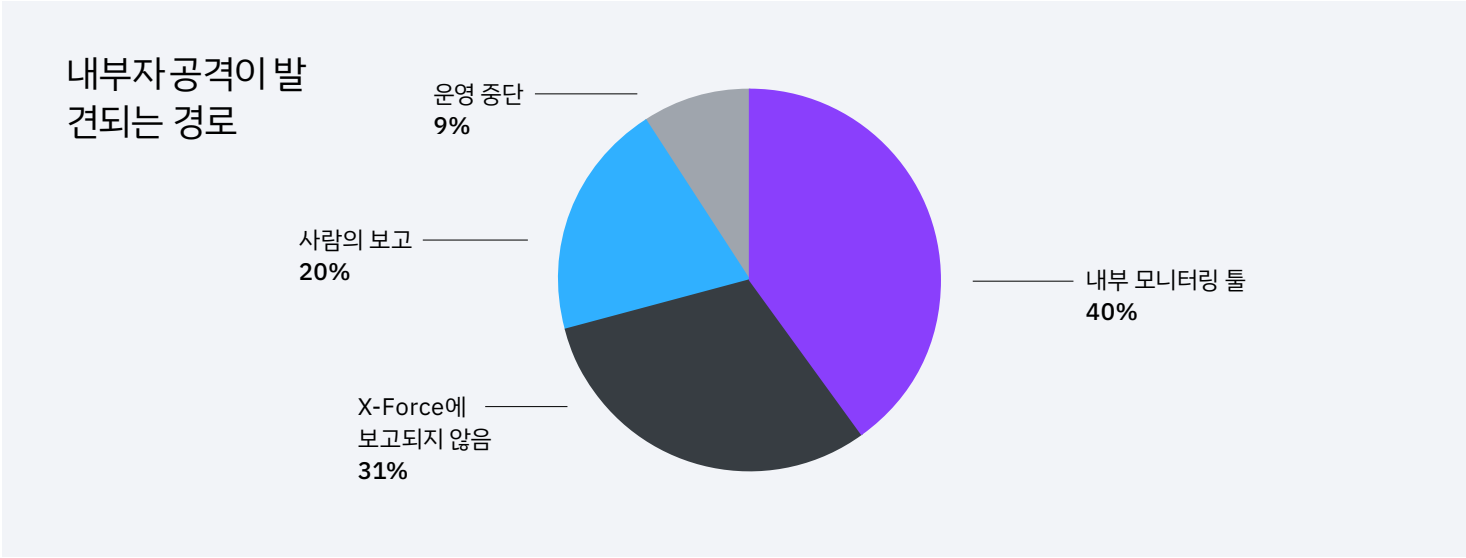
인시던트 중 40%는 내부 모니터링 툴에 의해 생성된 알림을 통해 탐지되었습니다.

인시던트 중 40%는 회사 자산에 대한 특별 액세스 권한을 가진 직원과 관련이 있었습니다.

인시던트의 100%는 내부자가 관리 액세스 권한을 가진 것으로 확인되었거나 이러한 권한을 가졌을 가능성이 높은 경우였으며, 이 경우 상승된 액세스 권한이 인시던트 자체에서 일정한 역할을 수행했습니다.

내부자 위협 공격이 발견되는 경로

내부자 위협은 일반적으로 기업 자산에 일정 수준의 액세스 권한을 가진 적법한 사용자가 이러한 권한을 악의적으로 또는 우발적으로 활용하여 궁극적으로 조직에 피해를 유발하는 공격으로 정의됩니다. 이러한 위협은 현재 또는 이전 직원, 또는 지정된 비즈니스 기능을 수행하기 위한 액세스 권한을 가진 타사 계약자 또는 벤더로 인해 발생할 수 있습니다.



2018년 이후 X-Force가 대응한 내부자 위협을 분석한 결과, 이러한 인시던트의 40%는 내부 모니터링 툴에 의해 생성된 알림을 통해 탐지되는 것으로 나타났습니다. 직원이 조직에게 이상 활동을 알려주는 경우와 같은 사람의 보고는 탐지 사례의 20%를 차지했고, 시스템 운영 중단으로 인해 보안 팀이 위협을 알게 된 경우는 전체 사례의 9%를 차지했습니다.

ObserveIT 및 IBM이 후원하고 Ponemon Institute가 작성한 2020 내부자 위협 비용: 글로벌 보고서에 따르면, UBA(User Behavior Analytics), PAM(Privilieged Access Management), SIEM(Security Information and Event Management)과 같은 툴, 그리고 위협 인텔리전스 공유, 사용자 교육 및 인식 향상과 같은 프로그램을 활용하면 조직은 내부자 위험을 줄이거나 제거하는 과정에서 평균 300만 달러를 절약할 수 있는 것으로 추정되었습니다.[4]

300만 달러의 비용 절감

UBA, PAM, SIEM과 같은 툴, 그리고 위협 인텔리전스 공유, 사용자 교육 및 인식 향상과 같은 프로그램을 활용하면 조직은 내부자 위험을 줄이거나 제거하는 과정에서 평균 300만 달러를 절약할 수 있는 것으로 추정되었습니다.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

X-Force 연구에서의 증거 부족 위협 및 알 수 없는 위협

발견 방법이 “X-Force에 보고되지 않음” 또는 “증거 부족”인 내부자 인시던트의 경우 X-Force 인시던트 대응 팀은 발견한 사항에 대해 판단을 내리기에 충분한 정보를 제공받지 못했습니다. 이는 많은 조직이 기본 환경과 그 운영 방식에 대한 가시성을 확보하지 못했기 때문에 발생하는 경우가 많습니다. 시스템 내부의 이상 활동을 탐지하려면 반드시 정상적인 활동의 특징을 이해해야 합니다. 그래야 이상값을 신뢰할 수 있는 방식으로 더욱 쉽게 찾아낼 수 있습니다. 2019년에 IBM은 조직에 고급 위협을 제기하는 환경을 살펴보는 SANS 보고서[5]를 후원했습니다. 연구 결과는 다음과 같았습니다.

- 조직의 48%는 인프라에 대한 가시성 결여를 가장 큰 보안 문제로 여겼습니다.
- 35%는 회사 내부자의 오용 사례를 탐지할 능력이 없다고 느꼈습니다.
- 조직의 47%는 네트워크 내에서 정상적인 기본 활동의 특징이 무엇인지 이해할 능력이 없다고 시인했습니다.

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

특별 액세스와 관리 액세스

X-Force는 내부자 위협 인시던트를 분석할 때 사용자를 두 가지 유형으로 분류했습니다.

특별 **사용자**는 중요한 데이터에 대한 액세스 권한을 가진 조직 내 구성원으로 정의됩니다. 중요한 데이터로는 지적 재산, 고객 데이터 또는 HR 정보 등이 있을 수 있습니다. 특별 사용자는 인수 합병 데이터 또는 기타 법무 정보와 같은 중요한 비즈니스 정보에 액세스할 수 있는 구성원일 수도 있습니다.

관리 액세스 권한을 가진 사용자는 관리자라고도 부르며, 네트워크 안에서 IT 시스템에 대한 상승된 액세스 권한을 가진 사람으로 정의됩니다. 이론적으로 이러한 유형의 액세스 권한은 중복되어서는 안 됩니다. 그러나 X-Force는 최종 사용자가 IT 환경에서 과다 프로비저닝되는 경우가 많다는 점을 알 수 있었습니다.

관리 액세스 권한을 가진 내부자는 기업 환경에 대한 중요한 액세스 권한을 가진 내부자와 다릅니다. 이들은 조직의 IT 환경에 대한 액세스 권한을 가진 직원, 계약자/벤더 등이며, 상승된 네트워크 권한을 기반으로 조직에 고유한 위험을 제기합니다.

특별 액세스 권한을 가진 직책의 예

- HR 직책
- 고위 경영진
- 재무 직책
- 법무 직책
- 연구직
- 조직의 지적 재산 또는 "가장 가치 있는 자산" 또는 고객 데이터에 대한 액세스 권한을 가진 기타 직책

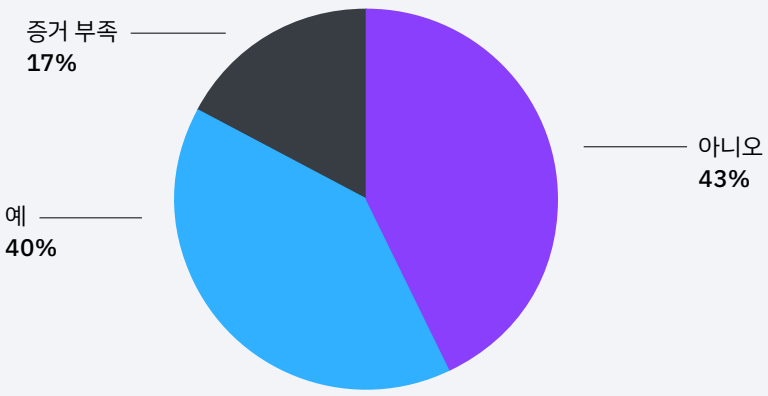
관리 액세스 권한을 가진 직책의 예

- 서버 관리자
- IT 관리자
- 헬프데스크
- 타사 IT 벤더
- IT 시스템의 구성/설정을 변경할 수 있는 기타 직책

누가 감시자를 감시하는가?

인시던트를 유발한 내부자는 일반적으로 특별 액세스 권한을 갖고 있습니까? 간단히 답하면 그렇습니다.

내부자가 데이터에 대한 특별 액세스 권한을 갖고 있었습니까?



X-Force 데이터를 분석한 결과 내부자가 유발한 인시던트의 40%는 중요한 회사 자산에 대한 특별 액세스 권한이 있는 직원과 관련이 있는 것으로 나타났습니다. 이 연구에서 X-Force는 IT 부서, 인사 부서, 재무 부서, 보안 부서에서 일하거나 임원직에 있는 사람을 특별 액세스 권한을 가진 자로 분류했습니다.

데이터 중 또 다른 17%에서는 내부자가 중요한 데이터에 대한 특별 액세스 권한을 가졌는지 여부가 불분명했습니다. 따라서 특별 액세스 권한을 가진 사용자가 유발한 인시던트 수는 상당히 더 높을 수도 있습니다.

네트워크 공유, 보안 어플라이언스, 이메일 시스템, 직원 또는 고객의 개인 식별 정보(PII), 지적 재산 또는 재무 데이터 등 중요한 자산에 상승된 액세스 권한을 가진 사람은 제한된 권한을 가진 사람보다 상당히 더 높은 위험을 제기할 수 있습니다.

그렇다면 특별 액세스 권한을 가진 우발적 내부자로 인한 인시던트가 더 낮은 액세스 권한을 가진 우발적 내부자로 인한 인시던트보다 더 많은 비용을 초래한다고 말할 수 있습니다. 높은 수준의 특별 액세스 권한을 가진 악의적 내부자로 인한 인시던트는 훨씬 더 많은 비용을 초래하고, 이러한 사용자로 인한 공격은 전면적인 데이터 유출로 발전할 수 있습니다. 예를 들면, 유명한 현지 중개업체에서 일하던 한 호주 부동산 중개인은 2018년에 이 중개업체에서 퇴사하기 전에 기밀 데이터베이스에 액세스하여 유죄 판결을 받았습니다. 이 중개인은 잠재 고객의 관심 등급을 낮춰 시스템에서 잠재적인 매출 현황을 조작했습니다. 또한, 이 중개인은 새 중개업체에서 비즈니스를 유치하기 위해 200개의 고객 레코드를 가로챘다고 시인했습니다. 이 내부자 공격 때문에 영향을 받은 중개업체는 잠재적인 부동산 매출 측면에서 3,000만 달러의 비용이 발생한 것으로 추정되었습니다.[6]

액세스 수준 관련 내부자 인시던트를 예방하는 가장 좋은 방법 중 하나는 최소 권한 원칙을 준수하고 사용자에게 조직의 업무를 수행하는 데 필요한 최소한의 액세스 수준만을 허용하는 것입니다. 이를 위해 PAM(Privileged Access Management) 솔루션을 활용할 수 있습니다. 이러한 솔루션은 제로 트러스트 모델을 기반으로 구축될 수 있습니다.[7,8] 이 모델의 목표는 사용자 계정이 있는 모든 사람에게 가능한 한 최소한의 권한을 부여하여 내부자가 의도하지 않게 데이터 또는 자산에 액세스할 가능성을 낮추는 것입니다. 이러한 개념은 클라우드에서 더욱 중요합니다. 클라우드의 경우 데이터가 더 많이 보관되고 인간뿐만 아니라 인간이 아닌 요청자도 운영을 위해 액세스할 수 있어야 합니다.

2020 내부자 위협 비용: 글로벌 보고서에 따르면 조직 중 39%만이 조직 내에서 일정한 유형의 PAM을 채택한 것으로 나타났습니다.[9] 또한 PAM을 채택하여 310만 달러의 비용을 절감한 것으로 나타났습니다. 이 사실은 이러한 조치가 효과적임을 보여줍니다.

39%

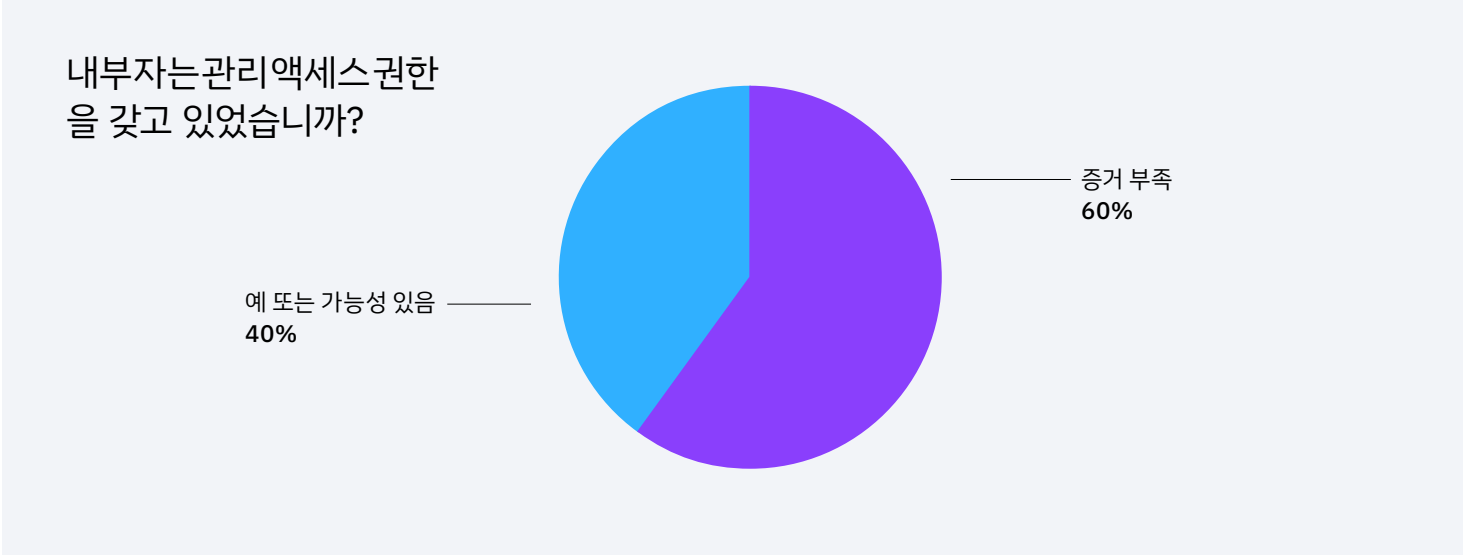
조직 중 39%는 조직 내에서 일정한 유형의 PAM을 채택했습니다.[9] PAM을 채택한 결과 310만 달러의 비용을 절감할 수 있었습니다.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/kr-ko/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

많은 비용을 초래하는 관리 액세스 권한 남용

복수, 금전적 이득 또는 기타 악의적인 의도 등 비도덕적인 목적으로 내부자가 조직에서 관리자로서의 권한을 남용한 사례는 매우 많이 알려져 있습니다. 2020년 2월, 전에 Microsoft의 엔지니어였던 Volodymyr Kvashuk는 회사로부터 1,000만 달러의 디지털 자산을 훔치기 위해 특별 액세스 권한을 사용하여 유죄 판결을 받았습니다.[10] Kvashuk가 자신이 관리하던 소매 매출 플랫폼에서 관리 액세스 권한을 악용했기 때문에 이러한 도난 행위가 가능했습니다.[11] 구체적으로 말하자면, Kvashuk는 디지털 기프트 카드를 빼돌리는 등의 활동을 난독 처리하기 위해 시스템에서 동료의 이메일 주소와 유효한 테스트 계정을 사용했습니다. 이렇게 훔친 자산과 다른 자산은 개인적 수익을 위해 인터넷에서 다시 판매되었으며, Kvashuk는 나중에 이 수익을 사용하여 160만 달러의 주택을 구입하고 16만 달러의 Tesla 자동차를 구입했습니다.[12]

수치로 살펴보는 관리 액세스 권한 남용 사례

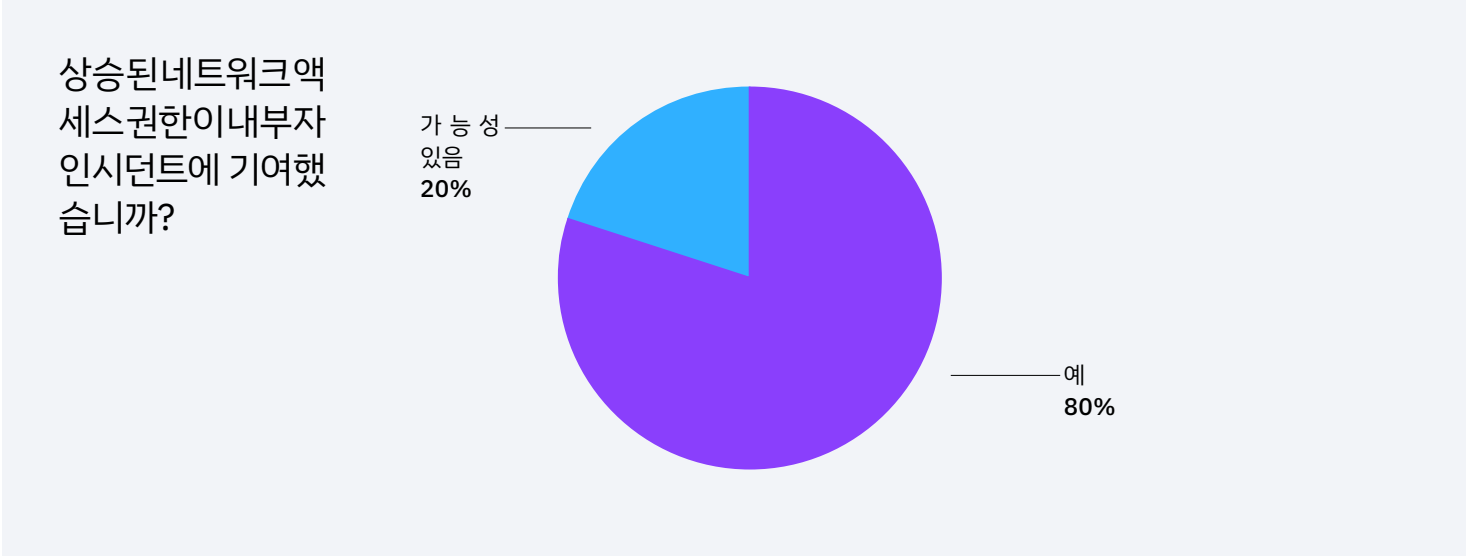


2018년부터 2020년까지 X-Force가 대응한 인시던트 중 40%에서 내부자는 네트워크에 대한 관리 액세스 권한이 있는 것으로 확인되었거나 이러한 권한을 얻었을 가능성이 있는 것으로 나타났습니다. X-Force 분석가는 고객이 사용자의 직책을 구체적으로 알려주지 않은 경우 인시던트에 관한 세부 정보를 기반으로 내부자의 액세스 권한 유형을 결정했습니다.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

이러한 인시던트의 예로는 데이터 유출, 중요한 데이터의 노출 및 삭제, 승인되지 않은 소프트웨어 설치 등이 있습니다. 구체적으로 말하자면, 서버에서 여러 페타바이트 규모의 로그가 삭제되었거나 의도적인 소스 코드 유출을 겪었거나 관리 액세스 권한이 있는 내부자 때문에 비용이 많이 드는 운영 중단을 감내한 조직도 있었습니다.

흥미롭게도, 인시던트의 100%는 내부자가 관리 액세스 권한을 가진 것으로 확인되었거나 이러한 권한을 가졌을 가능성이 높은 경우였으며, 이 경우 상승된 액세스 권한이 인시던트 자체에서 일정한 역할을 수행했습니다. (아래 차트 참조)



이 정보를 다르게 설명하면, 내부자에게 관리 액세스 권한이 없었다면 인시던트가 조직에 끼치는 영향이 훨씬 더 적었거나 많은 경우 아예 발생하지 않았을 것이라고 말할 수 있습니다. X-Force가 대응한 몇몇 내부자 인시던트에서는 중요한 데이터베이스와 로그가 서버에서 삭제되었습니다. 내부자에게 이러한 시스템에 대한 관리 액세스 권한이 없었다면 이러한 이벤트는 발생하지 않았을 것입니다.

조언

X-Force는 내부자 인시던트의 횟수가 타사 데이터에서 과소평가되었다고 생각합니다. 조직 내부에서 처리되고 법적 책임이나 조직의 평판 훼손에 대한 두려움 때문에 공개되지 않았을 가능성이 큰, 이러한 속성의 인시던트가 더 많이 있을 수 있습니다.[13]

X-Force 연구와 데이터에 따르면 이러한 인시던트가 조직에 줄 수 있는 영향을 바탕으로 잠재적 내부자 위협을 정보 보안 프로그램의 중대한 구성 요소로 포함해야 할 필요가 있는 것으로 나타났습니다. 특히, IBM Security는 내부자 위협과 관련하여 다음과 같은 사항을 권장합니다.

심층 방어 전략은 내부자 위협을 탐지하는 데 효과적입니다.

전통적으로 조직이 실행하는 기술과 프로세스에 다계층 접근법을 취하는 것은외부적 위협에 대응하기 위한 것으로 여겨졌습니다. 그러나 X-Force 연구에 따르면 SIEM(Security Information and Event Management) 솔루션을 포함하여 이러한 툴 중 다수가 내부자 위협 활동을 탐지하는 데 필수적인 것으로 나타났습니다.

환경에서 정상적인 활동의 특징을 이해해야 합니다.

어떤 유형의 공격자가 저지른 활동이건 의심스러운 활동을 탐지하는 가장 좋은 방법은 네트워크 내부에서 정상으로 간주되는 활동의 유형을 이해하는 것입니다. 기저 활동을 면밀하게 이해하면 이상 행동을 신속하고 효과적으로 탐지하고 이에 대응할 수 있습니다. 강력한 UBA(User Behavior Analytics) 솔루션은 이러한 기능을 수행하고 시간이 흐름에 따라 환경의 변화에 맞게 대응할 수 있습니다

정기적으로 관리 액세스 권한을 검토해야 합니다.

X-Force는 관리자와 관련된 여러 내부자 인시던트가 과다한 권한을 부여받은 사용자 때문에 발생한 것일 수 있다는 것을알게 되었습니다. 관리 액세스 권한에 대해 엄격한 변경 및 프로세스 제어 조치를 적용해야 합니다. 특히, 미션 크리티컬 서버에 대한 제어 조치는 더욱 엄격해야 합니다. 중요한 시스템과 기능에 대한 임시적 관리 액세스 권한을 로깅하고 부여하는 기술 솔루션을 고려하십시오.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

정보 보안 팀과 IT 관리 팀을 분리해야 합니다.

X-Force가 경험한 바에 따르면 보안 팀과 관리 팀의 독립성과 거버넌스를 균형 잡힌 방식으로 관리하면 보안을 향상하는 데 도움이 되는 것으로 나타났습니다. 또한, 그럴 경우 관리 팀은 위협을 탐색하고 발견하는 활동을 최적으로 수행하는 데 필요한 유연성과 창의성을 발휘하는 동시에 팀 내에서 위험을 최소화하기 위해 엔터프라이즈를 충분히 감독할 수 있습니다.

조직의 중요한 직책에 대한 위험 프로파일을 작성해야 합니다.

X-Force가 대응한 내부자 인시던트 중 다수에서 상승된 액세스 권한이 일정한 역할을 수행했으므로 시스템 또는 데이터에 중요한 액세스 권한 또는 관리 액세스 권한을 갖게 되는 조직 내 직책에 대해 위험 프로파일을 작성할 것을 권장합니다. 제로 트러스트 모델을 따르는 PAM (Privileged Access Management) 솔루션을 실행하면 사용자에게 최소한의 특별 액세스 권한을 부여하고 내부자 인시던트의 영향을 최소화할 수 있습니다.

인시던트 대응 플레이북을 업데이트하여 내부자 위협을 포함해야 합니다.

이러한 인시던트에 대응하는 데 일반적인 교육으로는 충분하지 않습니다. 대부분의 인시던트 대응 플레이북은 외부의 적이 가하는 공격을 위한 것이지만 우발적 또는 악의적 내부자 위협 시나리오를 추가하는 것을 고려해야 합니다. 사이버 공격에 더 효과적으로 대비하고 대응하기 위해 인시던트 대응 계획과 공격별 플레이북을 개발하는 활동을 지원할 수 있는 파트너를 활용하는 것을 고려하십시오.

지속적으로 직원을 교육해야 합니다.

윤리적 비즈니스 관행은 사회 공학 교육과 함께 수많은 조직이 연례 교육 프로그램에 포함시키고 있습니다. X-Force가 대응한 내부자 인시던트 중 다수는 기술이 아니라 다른 직원이 발견했습니다. 조직은 연례 비즈니스 윤리 교육 또는 사회 공학 교육에 내부자 인시던트 의심 사례를 보고하는 방법을 포함해야 합니다. 또한, 특별 액세스 권한을 가진 직원에게 직책 기반 교육을 제공하면 이러한 직원들은 주위에서 뭔가 잘못되어 가고 있음을 보여주는 명백한 조짐에 주의를 기울일 수 있습니다.

평판이 좋은 위협 인텔리전스 서비스를 활용해야 합니다.

고객은 위협 인텔리전스를 확보하고 관리하고 활용하는 데어려움을 겪는 경우가 많습니다. 규모에 맞게 위협 인텔리전스를 활용하는 데 필요한 집계 기능, 자동화 및 통합 기능을 제공하는 솔루션을 찾으십시오.

MDR(Manged Detection and Response) 서비스는 24시간 보호를 제공합니다.

MDR(Managed Detection and Response) 보안 서비스는 내부자 위협을 예방하고 탐지하고 신속하게 대응하는 데 필수적입니다. 행동 기반 차단, 조사 및 지속적인 정책 관리를 제공하는 차세대 AV를 활용하여 기존의 예방 조치를 뛰어넘는 솔루션을 활용하는 것이 중요합니다.

IBM Security가 어떻게 외부 위협과 내부 위협으로부터 가장 복잡하고 중요한 환경을 보호하도록 고객을 지원하는지 알아보십시오.

IBM Security에 대해 자세히 알아보기

IBM Security

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)
Tel. 02-3781-5114

Produced in the United States of America
2021년 5월

IBM