컴퓨터개론

13주차 보안기술

컴퓨터 바이러스

최근의 해킹동향

컴퓨터 보안전략 논문 요약

2024052015

컴퓨터학부

김동건

**신규 취약점 공격에 대한 효율적인 방어 메커니즘**

**저자 및 소속**

* 곽영옥, 조인준
* 배재대학교 대학원 사이버보안과

**논문 개요**

본 논문은 최근 급증하는 사이버 공격과 그에 따른 보안 취약점에 효과적으로 대응하기 위한 방어 메커니즘을 제안합니다. 특히 2015년부터 2020년까지 약 90,000건의 새로운 보안 취약점 코드(CVE)가 보고된 상황에서, 신속하고 효율적인 대응 방안의 필요성이 강조됩니다.

**문제점**

1. **보안 대응의 어려움**:
   * 기업과 공공 기관은 제한된 보안 예산과 인력 부족으로 인해 새로운 보안 취약점에 신속하게 대응하기 어려움.
   * 취약점 발견과 대응책 마련에 시간이 많이 소요됨.
   * 공공 기관은 국가 사이버 안전 센터의 일괄적인 보안 정책 배포로 인해 각 제조사의 특성에 맞는 보안 규칙 적용에 어려움을 겪음.
2. **기존 시스템의 한계**:
   * 수동 분석을 통한 대응으로 인한 시간적 비효율성.
   * 보안 규칙 등록 시 발생하는 오류와 그로 인한 시스템 부하 문제.

**제안된 방안**

1. **Snort 활용**:
   * 보안 규칙 정보 공유 사이트인 "snort.org"를 통해 보안 규칙을 신속하게 공유 및 적용.
   * Snort는 오픈 소스 침입 탐지 시스템(IDS)으로, 네트워크 패킷을 분석하고 사전에 정의된 규칙에 따라 위협을 탐지.
2. **보안 규칙 최적화**:
   * 중복되거나 유사한 보안 규칙을 최적화하여 시스템의 효율성을 증대.
   * 신규 보안 규칙 등록 시 발생하는 문제를 분석하고 개선 방안을 마련.
3. **검증 시스템 구축**:
   * 새로운 보안 규칙을 등록하기 전에 검증할 수 있는 시스템을 구축하여 장비 부하 및 서비스 장애를 예방.
   * 기존 서비스 환경에서 신규 정책 검증 시스템을 통해 보안 규칙의 정확성과 효율성을 높임.

**결론**

본 논문은 새로운 보안 취약점 공격에 대한 신속하고 효율적인 대응 방안을 제시합니다. 특히 보안 규칙 정보 공유 사이트와 검증 시스템을 활용하여 보안 규칙의 정확성과 효율성을 높이는 방법을 논의합니다. 이를 통해 보안 장비의 성능을 최적화하고, 새로운 보안 위협에 대한 대응 능력을 강화할 수 있습니다.

요약

해커들의 사이버 공격기법은 전에 볼 수 없었던 형태의 공격으로 점점 더 정교해지고 다양화되고 있다. 정보 보안 취약점 표준 코드(CVE)측면에서 살펴보면 2015년에서 2020년에 약 9만 건의 신규 코드가 등록되었다. 이는 보안 위협이 빠르게 증가하고 있음을 나타내고 있다. 신규 보안 취약점이 발생하면 이에 대한 대응 방안 마련을 통해 피해를 최소화해야 하지만, 기업의 경우 한정된 보안 IT예산으로 보안관리 수준과 대응 체계를 감당하기에는 역 부족인 경우가 많다. 그 이유는 수동 분석을 통해 분석가가 취약점을 발견하고 보안장비를 통한 대응 방안 마련 및 보안 취약점 패치까지 약 한 달의 시간이 소요되기 때문이다. 공공분야의 경우에 는 국가사이버안전센터에서는 보안운영정책을 일괄적으로 배포하고 관리하고 있다. 하지만, 제조사의 특성에 따라 보안규칙을 수용하는 것이 쉽지 않으며, 구간 별 트래픽 검증작업까지 약 3주 이상의 시간이 소요된다. 그 외 비 정상적인 트래픽 유입이 발생하면 취약점 분석을 통한 침해행위 공격 검출 및 탐지와 같은 대응방안을 마련해야 하나, 전문적인 보안전문가 부재로 인하여 대응의 한계가 존재한다. 본 논문에서는 신규 보안 취약점 공격에 효과적인 대응 방안 마련을 위해 보안규칙정보 공유사이트 “snort.org”를 활용하는 방안을 제안하였다.

■ 중심어:∣사이버 공격∣CVE∣취약점 분석∣보안규칙∣

나의 생각

시대에 발맞춰 해킹 기술도 늘어나고 있는 상황에서 사용자들의 정보들을 보호하기 위해서 많은 전문가들이 여러가지 방법들을 사용해서 대비를 하려고 노력하는 모습이 인상 깊다. 그리고 본 논문에서 여러가지 어려운 용어들이 사용되었는데 내가 기존에 있던 지식들로는 이해하기 어려워서 정확히 이해를 하며 읽고 요약하였는지 모르겠다.