중소기업 데이터 유출사고 대응 및 복구전략

최동수*, 김경택**, 유도진**
*극동대학교 대학원 인공지능보안학과
**극동대학교 해킹보안학과
e-mail:dhy8906@naver.com

Response and Recovery Strategies for Small and Medium Enterprises in Data Breach Incidents

Dong-Su Choi*, Gyeong-Taek Kim**, Prof. Dr. Doh Jim Yoo**
*Dept. of Artificial Intelligence Security, FarEast University Graduate school
**Dept. of Department of Hacking Security, FarEast University

요 약

데이터 유출 사고는 현대 사회에서 조직 또는 개인의 중요 정보, 민감한 데이터, 그리고 개인정보가 무단으로 노출되거나 유출되는 상황을 의미한다. IT 기술의 발전과 함께 사이버 공격의 기회도 증가하며, 이는 데이터 유출 사고의 증가로 이어진다. 이러한 사고는 조직과 개인에게 중대한 위험을 초래하며, 이에 따라 개인 정보 보호 및 사이버 보안에 대한 엄격한 대응 및 예방 조치가 필요하다. 더욱이, 데이터 유출 사고는 내부에서의 부족한 보안 인식으로 인한 인적 실수나 부주의로 인한 사건도 급증하고 있다. 이러한 내부적 위험은 대부분 조직 내에서의 적절한 보안 인식과 교육의 부재에서 비롯된다. 이로 인해 데이터 유출 사고의 가능성이 증가하며, 특히 보안 인프라가 부족한 중소기업에서는 이러한 위험이 더욱 높아진다. 따라서 중소기업은 데이터 보호와 사이버 보안에 대한 주의를 강화하며, 데이터 유출 과정을 분석하여 대응 및 예방할 수 있는 방안을 모색하고 제시해야 한다.

1. 서론

최근 3년간 기업 규모별 사이버 위협 발생 현황을 분석하면, 대기업과 비영리 단체는 전체 사이버 위협 사례 중 약 10%를 차지하며, 그 반대로 중소기업은 전체의 90%로 큰 비중을 차지하고 있다[1]. 이는 중소기업이 대기업과 비영리 단체와 달리 보안 조치와 자원이 부족해 사이버 공격이나 데이터 유출 사고에 대해 굉장히 취약하다는 현실을 보여준다. 상기 관련 내용을 정리하면 아래 [표 1]과 같다.

[표 1] 최근 3년간 기업 규모별 사이버 위협 발생 현황

구분	2018	2019	2020	2021.7	합계	비율
대기업	4	10	23	9	42	3%
중소기업	467	386	522	338	1,246	90%
비영리	29	22	58	15	95	7%
합계	500	418	603	362	1,383	100%

또한, 최근 3년간 민간기업에 대한 사이버 위협 발생 현황을 살펴보면, 시스템해킹이 44%로 가장 빈도가 높았으며, DDoS(분산 서비스 거부) 공격이 34%, 악성코드 감염 및 유포는 22%로 나타났다[1]. 이러한 통계는 아래의 [표 2]와 같이 시스템 해킹과 DDoS 공격이 민간기업에 대한 주요한 사이버 위협 유형으로 부각되고 있다는 사실을 분명히 보여준다. 특히, 중소기업들은 이러한 시스템해킹과 DDoS 공격과 같은 유형의 사이버 위협에 대비할 필요성이 점점 더 커지고 있다.

[표 2] 최근 3년간 민간기업에 대한 사이버 위협 발생 현황

구분	2019		2020		2021.7		합계	
	건수	비율	건수	비율	건수	비율	건수	비율
DDoS	155	37%	213	35%	97	27%	465	34%
악성코드	59	14%	140	23%	105	29%	304	22%
시스템 해킹	204	49%	250	41%	160	44%	614	44%
합계	418	100%	603	100%	362	100%	1,383	100%

본 논문은 최근 증가하는 사이버 위협의 동향을 분석하고 중소기업의 특성과 이러한 위협에 대한 취약성을 고려하여, 중소기업에 적합한 사이버 보안 전략과 대응 방안을 제시하는데 목적이 있다. 특히, 이 논문은 데이터 유출 사고의 주요 원인과 중소기업이 직면한 사이버 보안 위험을 깊이 이해하고, 이를 효과적으로 예방하고 대응하기 위한 실질적인 방안과 지침을 제공하려 한다. 이를 통해 중소기업이 사이버 위협으로부터 안전한 비즈니스 환경을 구축하고 유지할 수 있도록 돕고, 이에 따라 중소기업의 사이버 리스크 관리능력을 향상시키고 비즈니스 지속성을 보장하는데 기여하고자 한다.

2. 대응 방안

데이터 보호와 사이버 위험 관리는 중소기업의 지속 가능성과 성공에 필수적이다. 중소기업은 기술적 대응, 정책적 대응 및 리소스 제약과 기술적 제한에 대한 적절한 대응 전략을 수립하여 이러한 위험을 최소화하고 데이터 보호를 강화할 수 있다.

2.1 기술적 대응

중소기업은 데이터 유출 사고로부터의 위험을 최소화하고 데이터 보호를 강화하기 위해 강력한 암호 정책과 다중 인증 구현이 필요하다. 첫째, 모든 직원에게 복잡한 암호를 사용하도록 권장하며, 다중 인증을 도입하여 계정 보안을 강화해야 한다. 또한, 안티바이러스 및 방화벽 소프트웨어의 사용은 시스템의 보안을 높이는데 도움이 된다. 둘째, 안티바이러스 및 방화벽 소프트웨어를 설치하고 이를 정기적으로 업데이트하여 시스템을 보호하고 있다. 데이터 암호화는 중요한 데이터의 무단 접근을 방지하며, 셋째, 중요한 데이터를 암호화하며, 클라우드 기반 백업 솔루션을 사용하여 데이터를 정기적으로 백업해야 한다. 넷째, 데이터 백업 및 복구 계획은 비상 상황에 대비하는데 필수적이므로, 데이터 백업 및 복구 계획을 수립하여 비상 상황에 대비해야 한다. 또한 보안 업데이트 및 패치 관리는 시스템의 취약점을 최소화하는 것이 중요하며, 보안 업데이트 및 패치 관리 시스템을 도입하여 시스템의 취약점을 최소화 해야 한다. 마지막으로, 위기 대응 팀의 구성은 사이버 보안 사고에 신속하게 대응하는데 필수적이며, 사이이버 보안 사고에 신속하게 대응하기 위해 위기 대응 팀을 구성해야 한다. 이러한 조치를 통해 중소기업은 데이터 유출 사고로부터의 위험을 최소화하고 데이터 보호를 더욱 확고하게 할 수 있다.

2.2 정책적 대응

정책적 대응은 중소기업의 사이버 보안을 강화하는 데 중요하다. 보안 교육 및 인식 강화는 모든 직원에게 사이버 보안 원칙을 가르치고 인식을 높이는데 필요하다. 이를 살펴보면 첫째, 직원들에게 월별 사이버 보안 교육을 제공하며, 이를 통해 직원들의 보안 인식을 향상시켜야 한다. 둘째, 정기적인 보안 감사는 시스템 취약성을 확인하고 보안 문제를 해결하는데 도움이 된다. 따라서 보안 컨설턴트 등 외부 보안 전문가에게 정기적인 보안 감사를 의뢰하여 시스템 취약성을 확인하고 보안 문제를 해결해야 한다. 셋째, 조직 내부에서 데이터 보호와 사이버 보안을 위한 정책을 개발하고 모든 직원에게 이를 준수할 책임을 할당해야 한다. 데이터 보호와 사이버 보안을 위한 정책을 개발하고 모든 직원에게 이를 준수할 책임을 할당해야 한다. 마지막으로, 외부 공급업체와의 계약에서 데이터 보호 및 보안 요구사항을 명확하게 규정하고 계약 감사를 통해 확인하는 것이 중요하다. 즉, 외부 공급업체와의 계약에서 데이터 보호 및 보안 요구사항을 명확하게 규정하고 계약 감사를 통해 확인하고 있다.

2.3 중소기업의 리소스 제약과 대응

중소기업은 리소스와 기술적 제한으로 인해 보안에 대한 투자가 어려울 수 있다. 이러한 제한을 극복하기 위해, 중소기업은 다음과 같은 방안을 고려할 수 있다. 첫째, 자동화 및 적응 솔루션 활용이다. 중소기업은 자동화된 보안 솔루션과 기술을 적용하여 리소스를 효율적으로 활용할 수 있다. 이러한 솔루션은 기존 리소스와 기술적 제한을 최대한 활용하면서도 효과적인 사이버 보안을 제공할 수 있다. 둘째, 정부 및 비영리 조직의 지원 활용이다. 미국에서는 중소기업이 National Institute of Standards and Technology (NIST)의 Small Business Cybersecurity Corner, Cybersecurity and Infrastructure Security Agency의 Cyber Essentials for SME resources, 그리고 U.S. Small Business Administration의 Cybersecurity Resources를 통해 지원을 받을 수 있다. 또한, NIST는 중소기업을 위한 공개적으로 사용 가능한 프레임워크 자원을 제공한다[2].한국도 이러한 방향을 참고

하여 중소기업들이 적극 지원받을 수 있도록 정책을 연구해야 한다. 셋째, 오픈 소스 보안 솔루션 활용이다. 중소기업은 비용 효율적인 오픈 소스 보안 솔루션을 활용하여 기술적 제한을 극복할 수 있다. 넷째, 사이버 보안 위험 평가이다. 중소기업은 사이버 보안 위험 평가를 통해 기존의 리소스와 기술을 어떻게 최적화할 수 있는지 판단할 수 있다. 마지막은 커뮤니티 및 산업협회와의 협력이다. 지역 커뮤니티나 산업협회와 협력하여 기술적 지원을 받거나, 보안 전문가와 협력하여 기술적 제한을 해결할 수 있다. 이러한 방안들은 중소기업이 리소스와 기술적 제한을 극복하고, 사이버 보안 투자를 증대시키는 데 도움이 될 수 있다.

상기 기술적, 정책적 대응방안과 중소기업의 특화된 대응 방안을 정리하면 아래 표 3과 같다.

[표 3] 중소기업의 사이버 보안 대응 방안 정리

구분	대응방안	세부 사항 및 예시
기술적 대책	강력한 암호 정책과 다중 인증 구현	모든 직원에게 복잡한 암호를 사용하도록 권장, 다중 인증 도입으로 계정 보안 강화
	안티바이러스 및 방화벽 소프트웨어 사용	안티바이러스 및 방화벽 소프트웨어 설치 및 정기 업데이트
	데이터 암호화	중요 데이터 암호화 및 클라우드 기반 백업 솔루션 사용
	데이터 백업 및 복구 계획	데이터 백업 및 복구 계획 수립으로 비상 상황 대비
	보안 업데이트 및 패치 관리	보안 업데이트 및 패치 관리 시스템 도입으로 시스템 취약점 최소화
	위기 대응 팀 구성	사이버 보안 사고에 신속하게 대응하기 위해 위기 대응 팀 구성
정책적 대응	보안 교육 및 인식 강화	직원들에게 월별 사이버 보안 교육 제공, 정기적인 보안 감사 실시
	정기적인 보안 감사	외부 보안 전문가에게 정기적인 보안 감사 의뢰로 시스템 취약성 확인 및 보안 문제 해결
	조직 내 정책 개발	데이터 보호와 사이버 보안을 위한 정책 개발 및 모든 직원에게 준수 책임 할당
	외부 공급업체와의 계약 관리	데이터 보호 및 보안 요구사항 명확화 및 계약 감사
리소스 제약과 대응	자동화 및 적응 솔루션 활용	자동화된 보안 솔루션과 기술 적용으로 리소스 효율적 활용
	정부 및 비영리 조직의 지원 활용	미국의 NIST 등을 참고한 지원프로그램을 한국에서도 유사한 적용방안으로 연구 및 활용
	오픈 소스 보안 솔루션 활용	비용 효율적인 오픈 소스 보안 솔루션 활용으로 기술적 제한 극복
	사이버 보안 위험 평가	사이버 보안 위험 평가를 통한 기존 리소스와 기술 최적화
	커뮤니티 및 산업협회와의 협력	지역 커뮤니티나 산업협회와 협력으로 기술적 지원 받기, 보안 전문가와 협력으로 기술적 제한 해결

3. 결론

데이터 유출 사고는 현대 비즈니스 환경에서 심각한 위협으로 작용하며, 특히 중소기업은 이러한 위험에 노출되기 쉽다. 이 논문에서는 중소기업을 대상으로 데이터 유출 사고에 대한 대응 및 예방 전략을 탐구했다. 중소기업은 데이터 보호와 사이버 보안에 더 많은 주의를 기울여야 하며, 이를 위해 보안 교육, 강력한 보안 정책, 그리고 기술적인 조치를 적극적으로 채택해야 한다. 데이터 보호와 사이버 보안은 모든 기업에게 중요한 과제이며, 중소기업은 리소스 부족과 기술적 제한으로 인해 이러한 과제에 대한 투자가 어려울 수 있다. 그러나 보안에 투자하는 비용은 데이터 유출로 인한 손실과 평판 상실을 방지하는데 중요한 요소이다. 중소기업은 보안 전문가와의 협력, 정기적인 보안 감사, 데이터 암호화, 다중인증 구현, 그리고 위기 대응 계획을 통해 데이터 유출 사고로부터 보호할 수 있다. 이러한 조치는 중소기업이 안전한 온라인 환경에서 비즈니스를 성공적으로 운영하고 민감한 데이터를 보호하는 데 도움을 줄 것이다. 데이터 유출 사고로부터의 보호는 비즈니스의 장기적인 지속성을 보장하며, 신뢰를 유지하는 핵심적인 역할을 할 수있다. 중소기업은 이러한 보안 원칙을 적용하여 미래의 사이버 위협으로부터 안전하게 보호될 수 있을 것이다. 또한, 이 논문에서 제시된 표를 참조하면 중소기업이 기술적, 정책적, 그리고 리소스 및 기술적 제한에 대해 어떻게 대응할 수 있는지 구체적인 방안을 확인할 수 있다. 중소기업은 이러한 방안을 참고하여 사이버 보안 전략을 개발하고 실행함으로써, 데이터 유출 사

고의 위험을 줄이고 사이버 보안을 강화할 수 있다. 더 나아가, 중소기업은 정부 및 비영리 조직의 지원, 오픈 소스 보안 솔루션, 그리고 커뮤니티 및 산업협회와의 협력을 통해 리소스와 기술적 제한을 극복하고, 사이버 보안 투자를 증대시킬 수 있다. 이러한 방안들은 중소기업이 비즈니스의 안정성과 성공을 보장하며, 미래의 사이버 위협으로부터 안전하게 보호될 수 있도록 도울 것으로 기대된다.

참고문헌

[1] KISA, “2021년 하반기 사이버 위협 동향 보고서” pp. 49-52, 2월, 2023년

[2] Timothy Zimmerman (NIST), CheeYee Tang (NIST), Michael Pease (NIST), Keith Stouffer (NIST), “Cybersecurity Standards and Guidelines to Assist Small and Medium-Sized Manufacturers” USNC Current vol. 16, no. 1, pp. 6-7, 2001