사이버 복원력 강화를 위한 준비 및 구성방안

최선오
전북대학교 소프트웨어공학과 교수
suno7@jbnu.ac.kr

Preparation and Configuration Method to Enhance Cyber Resilience

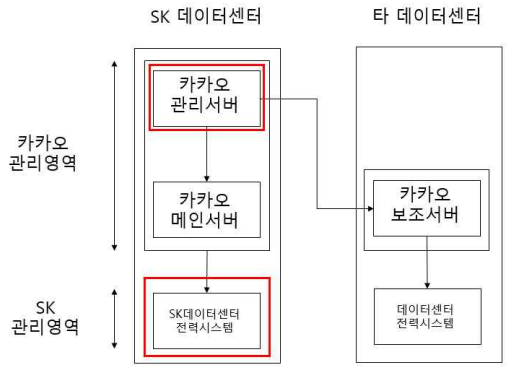
Sunoh Choi
Dept. of Software Engineering,

요 약

카카오 데이터 센터 화재 사건이나 콜로니얼 파이프라인 해킹 사건과 같이 시스템에 대한 다양한 공격이나 사고가 발생하고 이로 인하여 중요한 필수 서비스가 중단되는 문제가 발생하고 있다. 이러한 문제를 해결하기 위하여 사이버 복원력이 관심을 받고 있다. 사이버 복원력은 사이버 보안에 추가해서 예측, 내구, 회복, 적응의 목적을 가진다. 이 논문에서는 사이버 복원력이 무엇인지 소개하고 사이버 복원력을 기술적인 관점에서와 제도적인 관점에서 소개한다.

1. 서론

2022년 10월에 카카오 데이터 센터에서 화재가 발생되어서 카카오톡과 카카오모빌리티, 카카오 비즈 채널의 서비스가 중단되는 사고가 발생되었다. 사고의 원인은 2가지인데 첫째는 카카오가 이용하는 SK 데이터센터에 화재가 발생해서 아래의 그림과 같이 SK데이터센터에 있는 카카오 시스템이 동작하지 못했다는 것이다. 둘째는 카카오 시스템은 이중화되어 있어서 메인시스템이 동작하지 못할 경우 보조시스템이 동작하도록 관리시스템이 스위칭하도록 되어있었는데 관리시스템도 SK데이터센터에 있어서 화재시 동작하지 못했다는 것이다.



(그림 1) 카카오 데이터 센터 화재

이것이 시사하는 바는 IT시스템이 IT시스템의 문제 뿐만 아니라 전력시스템과 같은 다른 인프라시스템과도 밀접하게 연관되어있음을 보여주는 예가 된다.

다른 한편, 2021년 미국의 Colonial Pipeline은 미국의 동부지역에 석유를 공급하는 회사이다. 이 회사의 송유관시스템은 IT시스템에 의해 지원을 받고 있었는데 이 시스템이 랜섬웨어에 감염되어서 회사의 시스템이 6일 동안 동작하지 못해 미국 동부지역의 수백만명의 사람들이 석유를 공급받지 못하는 어려움을 겪었다[2]. 이것이 시사하는 바는 에너지 인프라와 같은 여러 인프라들이 점점 더 IT시스템에 의존하고 있고 IT시스템에서의 공격이나 사고로 인한 서비스 중단은 에너지, 교통, 상하수도, 금융 등 여러 다른 분야에서도 큰 문제를 일으킬 수 있음을 보여준다.

이러한 문제를 해결하기 위하여 사이버 복원력(Cyber Resilience)이 많은 관심을 받고 있다. 기존에 시스템을 보호하는 측면에서 사이버 보안 기술이 발달해 왔는데 사이버 보안 만으로는 현재의 고도화된 사이버 공격이나 점점 복잡해져가는 시스템의 사고에 대응하는 것이 충분하지 못하기 때문이다.

이 논문에서는 2.1절에서는 사이버 복원력이 무엇인지 소개하고 2.2절에서는 기술적인 관점과 제도적인 관점에서 사이버 복원력을 소개한다. 즉 사이버 복원력 기술이 무엇인지 그리고 사이버 복원력 제도가 어떻게 만들어지고 운영되고 있는지 소개한다.

2. 준비 및 구성방안

2.1 사이버 복원력 정의

사이버 복원력은 아래의 그림과 같이 사이버 보안보다 더 넓은 범위에 해당된다. 컴퓨터와 네트워크 기술이 발달함에 따라 많은 사이버 공격과 사고들이 발생하였고 이러한 문제를 해결하기 위하여 사이버 보안 기술이 발전해왔다.

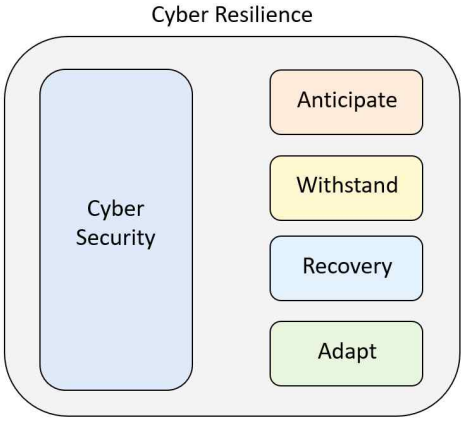
그러나 사이버 보안 기술의 발전 뿐만 아니라 사이버 공격 기술 또한 발전해 왔고 사회와 시스템이 점점 더 복잡해져감에 따라 우리가 예측하지 못한 사고들이 많이 발생하고 있다.

따라서, 사이버 복원력에서는 기존의 사이버 보안 뿐만 아니라 아래의 그림과 같이 4가지 목적을 가지고 있다 [3]. 첫째는 예측하는 것이다. 다양한 공격과 위협이 있을 수 있는데 이러한 것들을 예측하고 또한 다양한 시스템 간의 연관성 및 인과성을 고려하는 것이다.

둘째는 견디도록 하는 것이다. 시스템에 대한 다양한 공격과 다양한 사고에도 시스템이 지속적으로 서비스를 제공할 수 있도록 시스템 중복성 등을 사용하여 일부 시스템이 동작하지 못하는 상황에서도 필수 서비스를 제공할 수 있도록 하는 것이다.

셋째는 회복하는 것이다. 혹시 시스템이 공격이나 사고에 의해 동작하지 못하는 상황에서 백업시스템 등을 이용하여 가능한한 빠르게 회복하도록 하는 것이다.

넷째는 적응하는 것이다. 기술들이 빠르게 발전하고 환경과 조건도 바뀌는 상황에서 시스템이 적응할 수 있도록 하는 것이다.



(그림 2) 사이버 복원력

2013년 2월 오바마 대통령은 Presidential Policy Derective-21 (PPD-21)을 발표하였다 [4]. PPD-21에서는 복원력을 변화하는 조건에 대해 예측하고 견디고 회복하고 적응하는 것이라고 정의하였다.

또한, 미국의 필수 인프라는 통신, IT, 에너지, 교통, 상하수도 등 16개의 분야로 나누어서 정의하고 각 분야의 복원력을 1차적으로 해당부처에서 점검하고 2차적으로 국토안보부 장관이 점검하도록 명령하였다.

그리고 오바마 대통령은 세가지 전략적 명령을 내렸는데 첫째, 각 필수 인프라 간의 연관성을 파악하도록 하였다. 둘째는 각 분야 간 효율적으로 데이터를 교환할 수 있도록 필수 인프라를 식별하고 데이터 포맷을 통일시키도록 하였다. 셋째는 필수 인프라는 분석할 수 있는 방법을 구현하도록 하였다.

그리고 사이버 복원력은 기술적인 관점과 제도적인 관점에서 접근할 수 있다.

2.2 사이버 복원력 기술

NIST에서는 14가지의 사이버 복원력 기술을 제시하고 있다[3]. 첫째는 Adaptive Response이다. 이것은 다양한 공격에 대해 유연하게 대응하는 것이다. 둘째는 분석적 모니터링이다. 시스템에 대해서 모니터링을 하고 내용을 분석하는 것이다. 셋째는 상황인식이다. 어떠한 위협이 있을 수 있고 우리의 대응방법은 무엇인지 인식하는 것이다. 넷째는 조직화된 보호이다. 이것은 다양한 보호수단을 조직적으로 효과적으로 사용하는 것이다. 다섯 번째는 기만이다. 적을 혼동시키는 것이다. 여섯 번째는 다양성이다. 이것은 다양한 시스템을 사용하여 하나의 취약점이 전체 시스템에서는 유효하지 않도록 하는 것이다. 일곱 번째는 동적 포지셔닝이다. 시스템과 정보의 위치는 동적으로 변경하는 것이다.

• Adaptive Response	• Non-Persistence
• Analytic Monitoring	• Privilege Restriction
• Contextual Awareness	• Realignment
• Coordinated Protection	• Redundancy
• Deception	• Segmentation
• Diversity	• Substantiated Integrity
• Dynamic Positioning	• Unpredictability

(그림 3) 사이버 복원력 기술

여덟 번째는 자원이 제한된 시간동안만 유효하도록 하는 것이다. 아홉 번째는 사용자의 권한을 제한하는 것이고 열 번째는 시스템과 자원을 재구조화하는 것이다. 열한번째는 중복성을 제공하는 것이고

열두번째는 중요한 시스템을 분리하는 것이고 열세번째는 시스템의 무결성을 보장하는 것이고 마지막 열네번째는 예측하지 못하도록 하는 것이다.

사이버 복원력을 위한 14가지 기술은 현재 기술 수준에서 어느 정도 구현 가능하지만 다만 이러한 기술을 구현하고 사용하기 위해서는 리더십과 조직과 예산이 필요한 측면이 있다.

2.3 사이버 복원력 제도

사이버 복원력은 2개의 기관에서 주료 관심을 두고 있다. 첫째는 IOSCO라는 국제증권감독기구이고 둘WO는 CISA라는 미국 국토안보부 산하의 사이버 보안 및 인프라보안청이다.

2.3.1 IOSCO

금융시장인프라에서는 사이버 복원력이 다른 분야보다더 더 빨리 중요하게 고려되었다. IOSCO (International Orginization of Securities Commissions)는 아래의 그림과 같이 사이버 복원력 구성요소를 제시하고 있다 [5]. 첫째는 거버넌스이고 둘째는 식별, 셋째는 보호, 넷째는 탐지, 다섯째는 회복, 여섯째는 시험, 일곱 번째는 상황인식, 여덟번째는 학습 및 진화이다.

(그림 4) IOSCO의 사이버 복원력 구성요소

2.3.2 CISA

CISA (Cybersecurity and Infrastructure Security Agency) 는 미국 국토안보부 산하의 사이버보안과 인프라보안을 담당하는 부서이다. PPD-21에 따라 CISA는 Resilience Service Branch (RSB)라는 복원력 담당부서를 만들고 RSB를 통해 IRPF (Infrastructure Resilience Planning Framework)를 만들고 IRPF를 이용하여 미국내 100여곳의 필수인프라의 복원력을 점검하고 있다 [6].

IRPF는 아래의 그림과 다섯단계로 구성되는데, 첫째는 협력적 계획그룹을 만드는 것이고 둘째는 시스템 간 의존성을 식별하는 것이다. 셋째는 위험을 평가하는 것이고 넷째는 위험 해결 및 복원력 향상을 위한 행동계획을 개발하는 것이고 다섯째는 복원력 솔루션을 구현하는 것이다.

(그림 5) IRPF 5단계

3. 결론

우리는 이 논문을 통하여 사이버 복원력이 무엇인지 그리고 사이버 복원력을 달성하기 위해 필요한 기술이 무엇인지 그리고 사이버 복원력을 달성하기 위하여 어떠한 제도들이 도입되어 운영되고 있는지 소개하였다.

한국에서도 시스템에 대한 다양한 공격과 사고가 일어나고 있는 상황에서 필수 서비스에 대한 사이버 복원력을 강화하기 위하여 사이버 복원력 기술 도입과 사이버 복원력 제도 수립이 필요하다고 할 것이다.

이 논문은 정보통신기획평가원의 디지털 서비스의 사이버 복원력 확보 방안 연구(과제번호: 1711197773)의 지원을 받아 작성되었음

참고문헌

[1] 카카오 데이터 센터 화재, https://www.kakaocorp.com/page/detail/9902

[2] Colonial Pipeline Ransomware Attack, https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

[3] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie Mcquaid, Developing Cyber-Resilient Systems, NIST Special Publication 800-160, Volume 2, Dec 2021

[2] Presidential Policy Directive-21, “Critical Infrastructure Security and Resilience”, White House, Feb 2013

[3] IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures, June 2016

[4] CISA, Infrastructure Resilience Planning Framwork, June 2023