https://doi.org/10.33778/kcsa.2023.23.5.209

방산업체 비대면(재택) 근무를 위한 보안 요구사항 연구

황 규 섭*, 류 연 승**

요 약

2019년 12월 코로나19 바이러스의 급격한 확산으로 인해 대면 중심의 근무환경이 비대면 중심의 근무환경으로 급격히 전환되었다. 그러나 방산업체의 경우 군과 관련된 기술을 다루는 조직으로 망분리 정책을 적용하고 있어 비대면 적용에 제한이 많은 상태이다. 비대면 근무는 전세계적인 변화이고 향후 급변하는 환경을 고려했을 때 방산업체도 적용해야 하는 시급한 과제이다. 때문에 현재 방산업체가 비대면 근무를 시행하기 위해서는 VPN, VDI, 망연동시스템 등은 필수 요소로 적용되어야 한다. 결국 필연적으로 일부 접점이 발생할 수 밖에 없는데 이로 인해 보안취약점이 증가할 것이며 적극적인 보안관리가 중요하다. 이에 본 논문에서는 미국의 MITER에서 사이버 공격을 체계적으로 탐지하고 대응하기 위해 주기적으로 발표하고 있는 MITRE ATT&CK Framework의 공격전술을 기반으로 공격유형을 선정, 위협을 분석하고 STRIDE 위협 모델링을 적용하여 보안위협을 분류, 구체적인 보안 요구사항을 제시하고자 한다.

A study on security requirements for Telecommuting in defense industry

Hwang Gue Sub*, Yeon Seung Ryu**

ABSTRACT

Due to the rapid spread of the COVID-19 virus in December 2019, the working environment was rapidly converted to telecommuting. However, since the defense industry is an organization that handles technology related to the military, the network separation policy is applied, so there are many restrictions on the application of telecommuting. Telecommuting is a global change and an urgent task considering the rapidly changing environment in the future. Currently, in order for defense companies to implement telecommuting, VPN, VDI, and network interlocking systems must be applied as essential elements. Eventually, some contact points will inevitably occur, which will increase security vulnerabilities, and strong security management is important. Therefore, in this paper, attack types are selected and threats are analyzed based on the attack tactics of the MITER ATT&CK Framework, which is periodically announced by MITER in the US to systematically detect and respond to cyber attacks. Then, by applying STRIDE threat modeling, security threats are classified and specific security requirements are presented.

Key words : (STRIDE Threat modeling, Network Connection, Telecommuting, MITRE ATT&CK Framework)

접수일(2023년 9월 25일), 수정일(2023년 10월 29일), 게재확일(2023년 11월 20일)

* 명지대학교/보안경영공학과(주저자)
** 명지대학교/보안경영공학과(공동저자)

1. 서 론

2019년 12월 코로나19 바이러스가 전세계적으로 급격히 확산되면서 대면 중심의 근무환경이 급격하게 비대면 중심으로 전환되었다[1]. 그러나 방산업체의 경우 군과 동일하게 망분리 정책을 적용받아 비대면 근무에 제한사항이 많이 발생하고 있다. 이는 군사기밀을 취급하는 조직 입장에서는 비대면 근무 시행 시 내・외부망의 접점이 발생하기 때문에 이에 대한 위험을 최소화하면서 시행해야 하는 어려움에 기인한다.

방산업체의 경우 재택근무를 위해서는 여러 가지 원격근무 솔루션을 사용해야 하는데 대표적인 기술로는 VPN(Virtual Private Network), 망연동(연계) 시스템, VDI(Virtual Desktop Infrastructure) 등이 있다[2]. 방산업체에서는 이러한 솔루션을 이용해 보안이 구비된 재택근무 시스템을 구축하는 것이 목표이나 현실적으로 많은 어려움이 있다. 우리나라에서 사이버 위협을 논할 때 대표적으로 거론되는 OWASP TOP 10[3], 국정원 사이버위협 전망[4], 한국인터넷진흥원 사이버위협 동향[5] 등을 살펴보면 사이버 공간에서의 다양한 위협을 절실히 느낄 수 있다.

본 논문에서는 이와 관련하여 미국 연방정부의 지원을 받으며 국가안보 업무를 수행하는 비영리 연구단체(MITRE)에서 공개 연구를 통해 작성된 사이버공격 절차 및 기술을 다룬 MITRE ATT&CK Framework[6]를 기반으로 STRIDE 모델을 적용하여 비대면(재택) 근무의 보안위협에 대해 분석하여 제시한다.

2. 비대면 재택근무의 핵심 기술과 재택근무를 위한 보안적용 방안

비대면 근무는 가상사설망을 이용한 사외업무 방식이다. 방산업체의 특수성을 고려시 망분리 정책으로 사외업무가 제한됨을 고려시 다양한 보안대책을 강구하여 비대면 근무를 시행해야 한다. 이러한 비대면 근무를 시행하기 위해 보안과 관련되 연구가 다수 있다[7-8, 10-11, 13]. 김다현은 가상 사설망 취약점을 SRTIDE 위협모델을 기반으로 가상 사설망을 사용할 때 발생하는 데이터 흐름에 따라 위협을 분석하고 보안 요구사항을 도출하였다[7]. 박상길은 비대면 근무를 위해 가상사설망, SDP, RDP, VDI 방식을 적용했을 때 각 기술의 장단점을 연구하였다[8]. 허기열은 ISMS-P를 기반으로 재택근무 환경에서 공공기관 보안 강화를 위한 개선요인을 찾고 계층적 의사결정방법론(AHP)을 사용, 전문가 의견수렴을 통해 공공기관 보안 강화 개선을 위한 요인의 우선순위를 분석하였다[10]. 박찬규는 ISMS-P를 기반으로 재택근무 환경의 보안실태를 분석하고 ISMS-P 인증제도 내 재택근무와 관련하여 통제항목을 도출하였다. 이후 이를 인증과 관련된 부분에 집중하여 연구하였다[11]. 명성식은 원격근무의 보안 인프라의 변화를 제시하며 MITRE ATT&CK Framework를 통해 위협분석이 가능함을 제시하였다. 본 연구에서는 앞에서 제시한 연구들과 마찬가지로 비대면 근무의 보안환경에 대해 분석하고 표준안을 제시하는 한편 MITRE ATT&CK Framework에서 다루고 있는 세부적인 공격기법을 분석 및 활용하여 Attack Library를 심도있게 작성하여 STRIDE 위협 모델에 적용하여 보안 취약점을 도출하고 각 위협별 보안 요구사항을 제시하였다.

2.1 가설사설망(VPN, Virtual Private Network)

사설망(Private Network)은 특정한 조직내에서만 사용되는 네트워크로 인증된 사용자만 사용이 가능하다는 점에서 보안성이 높지만 구축과 관리(유지) 비용이 매우 높다. 반면, 공중망(Public Network)은 인터넷과 같이 누구나에게 공개된 망을 의미하며 가용성은 높지만 보안이 취약하다는 특징이 있다.

가상사설망(VPN)은 인터넷과 같은 공중 네트워크를 통해 사설 네트워크를 사용할 수 있도록 가상의 네트워크를 구성한 것이다. 여러 지점에 분산되어 있는 사설망을 하나로 통합하기 어려운 한계를 극복하고 외부에 노출 없이 통신할 목적으

로 사용하는 사설 통신망이다[7].

2.2 망연계(연동) 시스템

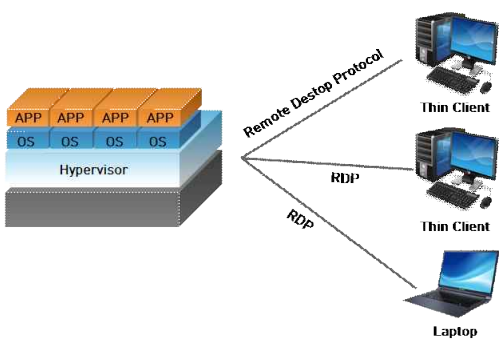
망연계, 일부에서는 망연동으로 부르는 시스템은 보안 수준이 서로 다른 영역의 서버나 PC를 보안 정책에 따라 안전하게 연결해 자료를 전송해 주는 시스템이다. 망연계 시스템은 두가지 방식으로 구분할 수 있다.

첫 째는 스트리밍 연계 방식(Streaming Service)이고 두 번째는 파일 연계 방식(File Transfer)이다. 스트리밍 연계 망구성도는 과 같다. 스트리밍, 파일 연계 방식은 업체 모두 동일하나 시스템을 구성하는 방식에서 각 업체별로 보안에 특화하여 악성코드 탐지, 자료보호(반입·출 통제 등)를 상이하게 운영한다[8].

2.3 가상 데스크톱 인프라(VDI)

가상 데스크톱 인프라는 가상 머신을 사용하여 사용자에게 가상 데스크톱을 제공하는 기술이다. 중앙 집중식 서버에서 데스크톱 환경을 호스팅하여 요청 시 사용자에게 제공하는 서버 컴퓨팅 모델이다. 엔드포인트 단말(노트북, 태블릿 등)을 사용하여 네트워크를 통해 액세스한다.

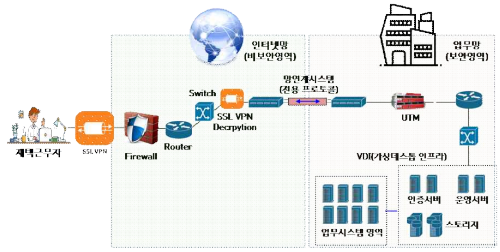
<그림 1>과 같이 모든 데이터는 중앙에서 관리하는 서버에 있고 사용자는 씬 클라이언트(VDI 이미지의 원격 액세스를 위한 네트워크 연결기기),PC, Laptop을 이용하여 접근한다.



(Figure 1) Virtual Desktop Infrastructure

2.4 방산업체 재택근무를 위한 보안적용 방안

보안이 중요하여 망분리를 구축한 방산업체에 재택근무를 적용하기 위해서는 아래의 <그림 2>와 같은 구성의 네트워크를 제안하고자 한다. 물론 방산업체의 자체 보안정책이나 업무의 성격에 따라 일부 구성은 변경될 수 있다[9][10][11].



(Figure 2) Telecommuting Network Configuration

위의 <그림 2>를 살펴보면 재택근무자는 SSL VPN을 통해서 암호화된 사설망화하여 업무망에 접속하게 된다. 물리적으로 분리되어 있는 인터넷망과 업무망을 연결해주는 시스템이 망연계시스템(스트리밍 방식)이다. 망연계시스템은 물리적으로 분리된 망을 연결하고 인터넷망에서 업무망으로 패킷이 넘어가는 구조로 보안이 취약해지므로 실시간 패킷을 탐지하기 위한 다양한 기능들이 포함된 솔루션들이 개발되고 있다. 망연계시스템은 망을 분리하여 운영하는 조직에서 재택근무를 하기 위해서는 필수불가결이라는 것을 알아야 한다.

재택근무자가 업무망에 접근하게 되면 차세대 방화벽으로 알려져 있는 UTM(Unified threat management)을 이용하여 바이러스 차단, 스팸 차단, 콘텐츠 필터링, 웹 필터링 등 다양한 보안활동을 수행한다. 마지막으로 재택근무자는 VDI를 이용하여 업무를 수행하게 된다.

방산업체에서 VDI를 사용하면 재택근무자가 업무행위를 했을 경우 모든 자료가 업무망 서버에 저장되고 재택근무자는 이미지만 외부에서 공유받는 시스템으로 침해시에도 업무망에 큰 영향을 줄 수 없다. 다만 취급 정보의 민감정도에 따라 캡쳐, 프린터 등 여러 가지 위협들이 존재하므로 단말 보안도 매우 중요하게 다뤄야 한다.

3. 최신 사이버위협 동향과 MITRE ATT&CK Framework

3.1 OWASP TOP 10

OWASP(The Open Web Application Security Project)는 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안취약점 등에 대해 3~4년 주기(2004년, 2007년, 2010년, 2013년, 2017년 2021년)로 10대 웹 애플리케이션 취약점을 발표한다[3].

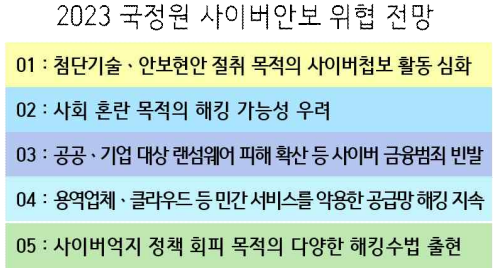
OWASP TOP 10은 아래의 <그림 3>과 같이 10가지 위협으로 구성되어 있다.

(Figure 3) OWASP TOP 10(2021)

지난 2017년에 발표된 위협과 비교하면 2021년에는 A04, A08, A10이 새롭게 추가되었다. A04(Insecure-Design)는 비효율적인 제어 설계로 다양한 취약점을 유발할 수 있다는 것을 의미한다. 구현 단계의 결함을 제시하는 것이다. A08(Software and Data Integrity Failures)은 무결성을 확인하지 않고 소프트웨어 업데이트의 위험을 제시한다. A10(Server-Side Regquest Forgery)은 웹 어플리케이션이 사용자가 제공한 URL의 유효성을 검사하지 않고 원격 리소스를 가져올 때마다 발생한다.

3.2 국가정보원, 2023년 사이버안보 위협 전망

2022년 국가정보원이 파악한 국내 해킹은 소폭 감소(5.6%)하였으며 해킹에 사용된 수법은 해킹 메일 유포와 IT솔루션 보안취약점 악용이었음. 해킹은 주로 국가가 배후에 있는 해킹조직이 외교·안보 현안 및 첨단기술을 절취하기 위해 시도했으며 이는 국가간 사이버분쟁 등으로 글로벌 안보 불안감이 고조되는 현상이 발생하였다.[4] 국가정보원은 2023년 사이버안보 위협으로 5가지를 제시하고 있으며 아래의 <그림 4>와 같다.



(Figure 4) 2023년 국정원 사이버안보 위협 전망

<그림 4>에서 제시된 5가지 위협을 살펴보면 방산기술은 첨단과 안보현안에 모두 해당되며 공급망 해킹에도 자유롭지 않다.

3.3 MITRE ATT&CK Framework

MITRE ATT&CK Framework는 사이버 공격을 체계적으로 탐지하고 대응하기 위해 MITRE 社에서 주기적으로 발표하고 있는 모델이다[6].

MITRE ATT&CK Framework는 전술, 기술 및 절차 등으로 구성되어 있으며 공격자들이 어떻게 행동할지를 주로 연구하고 있다.

3.3.1. 주요 공격전술(Tactics) 및 기술(Technique)

MITRE ATT&CK Framework는 14개의 공격전술과 224개의 기술로 구성되어 있다[6]. 이 중에서 재택(원격) 근무시 적용할 수 있는 주요 공격 기술을 구분하여 아래의 <표 1>과 같이 제시

한다. 14개의 공격전술 중 48개 기술을 구분하였는데 방산업체의 특수한 업무환경(독립망 구성)을 고려한 사회공학적 기법에 의한 침해에 중점을 두고 선정하였다[12].

<표 1> MITRE ATT&CK Critical Attack

Tactics	Technique
Reconnaissance	Active scannig
	Gather victim Host Information
	Gather victim Identiry Information
	Gather victim Network Information
	Gather victim ORG Information
Resource Development	Acquire Infrastructure
	Develop Capabilities
	Establish Accounts
persistence	Account Manipulation Create Account
	Traffic Signaling
Execution	Command and Scripting Interpreter
	Software Development Tools
Inital Access	External Remote Service
	Hardware Additions Supply Chain Compromise
	Trust Relationship
Privilege Escalation	Abuse Elevation Control Mechanism
	Event Triggered Execution
	Domain Policy Modification
	Process Injection
Defence Evasion	Exploitation for Defense Evasion
	Impair Defense
	Masquerading
	Rootkit
Credential Access	Brute Force
	Forge Web Credentials
	Two-Factor Authentication Interception
Discovery	Account Discovery
	Cloud Infrastructure Discovery
	Password Policy Discovery
	Peripheral Device Discovery
	System Network Connection Discovery
Lateral Movement	Remote Service
	Internal Spearphishing
Collection	Application Layer protocol
	Data from Network shared Drive
Command and Control	Application Layer protocol
	Data Encoding
	Data obfuscation
	Traffic Signaling - Port Knocking
Exfiltration	Exfiltration over alternative protocol
	Exfiltration over physical Medium
Impact	Account Access Removal
	Data Destruction
	Data Manipulation
	Endpoint Domain of Service
	Firmware Corruption
	Network Denial of Service
	Systerm shutdown / Reboot

STRIDE 위협 모델에 MITRE ATT&CK Framework에서 식별된 공격 유형을 적용하여 위협을 분석한다[13][14].

4. STRIDE 위협 모델을 적용한 재택 근무 보안취약점 분석

4.1 STRIDE 위협 모델

STRIDE 위협 모델은 공격자가 행할 수 있는 위협을 식별하고 분석하는 방법론이다. STRIDE 위협 모델은 기밀성, 무결성, 가용성의 보안 3요소와 인증, 부인방지, 권한부여 3요소가 더해져 총 6개 요소에 대해 위협을 분류하였다.

1. Spooling(위장)

Spooling은 보안속성 중 인증과 연관이 있으며 인증되지 않은(허가받지 않은) 사용자가 불법적으로 액세스를 시도하는 위협을 뜻한다.

2. Tempering(변조)

Tempering은 보안속성 중 무결성과 연관이 있으며 악의적인 사용자가 네트워크 전송값을 임의 변조하거나 프로세스, 파일 등에 대해 무결성을 훼손하는 위협을 뜻한다.

3. Repudiation(부인)

Repudiation은 보안속성 중 부인방지와 연관이 있으며 악의적인 사용자가 금지된 작업을 추적하는 기능을 거부하여 특정 서비스를 수행하지 않았다고 부인하거나 책임을 회피하는 위협을 뜻한다.

4. Information Disclosure(정보노출)

Information Disclosure은 보안속성 중 기밀성과 연관이 있으며 승인되지 않은 사용자에게 중요한 정보가 노출되는 위협을 뜻한다.

5. Denial of Service(서비스 거부)

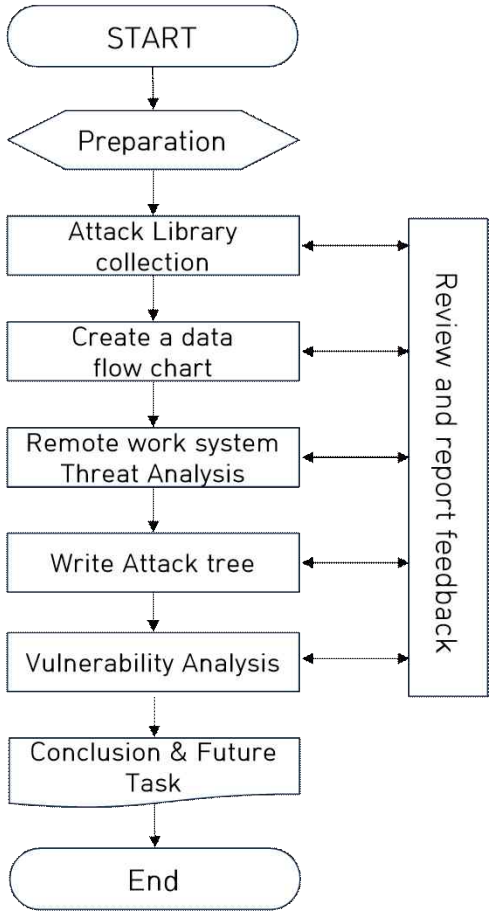
Denial of Service은 보안속성 중 가용성과 연관이 있으며 대량의 패킷을 일시적으로 전송해 웹 서버를 일시적으로 사용하지 못하도록 하는 등 서비스 또는 애플리케이션이 정상적으로 수행되지 않도록 공격하는 위협을 뜻한다.

6. Elevation of Privilege(권한 상승)

Elevation of Privilege는 악의적인 사용자가 관리자 권한을 임의 획득하여 시스템 및 데이터베이스를 침해하는 등의 위협을 뜻한다.

4.2 위협 모델링 방법론

재택(원격)근무에 적용하는 위협 모델링 절차는 <그림 5>와 같다.



(Figure 5) Threat Modeling Process

공격 라이브러리는 MITRE ATT&CK Framework에서 제시된 공격 절차와 기법을 위주로 분석하였고 추가로 신뢰할 수 있는 원격근무 보안위협에 대한 논문을 수집하였다. 이를 이용하여 데이터 흐름에서 발생할 수 있는 위협 요소들을 식별하며, 위협 식별과정에서 중복되는 부분을 제거하고 Attack Tree를 통해 공격방법을 구체화한다. 이후 분석을 통해 취약점 체크리스트를 작성하고 중요 보안 요구사항 및 대응 방안을 제시한다[15][16][17][18].

4.3 공격 라이브러리 수집

재택(원격)근무 공격 라이브러리는 MITRE ATT&CK Framework와 재택(원격)접속과 관련하

여 위협을 다룬 논문을 수집하였다. 총 10개의 논문을 수집하였고 아래의 <표 2>와 같다.

<표 2> Attack Library : Papers

Author	Title	Year	Ref
Park Chan Gyu	Security status and countermeasures in the increasing telecommuting environment after COVID-19 : Focusing on security certification system	2021	[11]
Myeong Seong Shik	Changes in security infrastructure due to remote work and A study on counterm easures against cyber threats	2021	[13]
Cho Sung young	An APT Attack Scoring Method Using MITRE ATT&CK	2022	[14]
Oh In Kyung	Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling	2020	[16]
Lee Seung wook	Kubernetes of cloud computing based on STRIDE threat modeling	2022	[17]
Cho Sa Rah	Cyber Security Requirement Analysis on Vehicle Remote Control Service via Threat Modeling	2022	[18]
Yu Dong Hyun	Consideration of New Convergence Security Threats and Countermeasures in the Zero-Contact Era	2021	[19]
Kim So Yeon	The Analysis for Cyber Security Threat in Remote Working Environment	2020	[20]
Ryu Hyo kyung	A Study on Attack Detection Technique Using SIEM in VPN Remote Working Environment	2021	[21]
Shin Seung Woo	Improvement Plan for Public Institution Remote Security Model in the New-Normal Era	2022	[22]

CVE(Common Vulnerbilities and Exposures)는 공개적으로 알려진 컴퓨터 보안 결함목록으로 VPN(Fortinet SSL VPN) 및 망연동(Microsoft Exchange Server) 취약점 8개의 CVE 공격 라이브러리를 수집하였다. 아래의 <표 3>과 같다.

<표 3> Attack Library : CVE

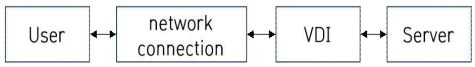
CVE Number	Title	Ref
CVE-2022-42475	heap-based buffer overflow vulnerability	[23]
CVE-2020-12812	An improper authentication vulnerability	[24]
CVE-2018-13379	An Improper Limitation of a Pathname to a Restricted Directory	[25]
CVE-2021-34473 CVE-2021-28482 CVE-2021-28481 CVE-2021-28480	Microsoft Exchange Server Remote Code Execution Vulnerability	[26]
CVE-2020-16875	improper validation of cmdlet arguments	[27]

4.4 데이터 흐름 도출

STRIDE 위협 모델링을 위해 <그림 2>에서 제시한 재택(원격)근무 시스템 표준 구조를 기반으로 데이터 흐름 다이어그램을 도출한다.

4.4.1 Level 1(High-Level). Diagram

최상위 레벨 데이터 흐름 다이어그램에서는 Very High-Level을 뜻하며 전체 시스템의 데이터 흐름을 제시한다. 방산업체 근무환경에서 재택(원격) 근무를 시행시 Level 1 수준의 DFD는 아래의 <그림 6>과 같다. 결국 User는 이종망을 사용하는 업무환경에 따라 망연동(연계) 시스템을 통해 내부 서버에 접속하게 되는데 이때 침해를 예방하기 위해 가상화 환경인 VDI를 통해 외부 침해행위를 보호한다.



(Figure 6) Level 1. Data flow diagram

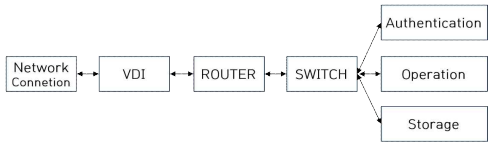
4.4.2 USER~망연동 사이의 상세 DFD

아래의 <그림 7>은 USER와 Network Connection 사이에서 DFD를 보여준다. 여기서 특이점은 방산업체의 데이터 흐름은 독립망을 사용하는 조직으로 VPN과 Level 1.에서 언급된 망연동(연계) 시스템을 거친다는 것이다.

(Figure 7) User~Network Detail DFD

4.4.3 망연동~Server 사이의 상세 DFD

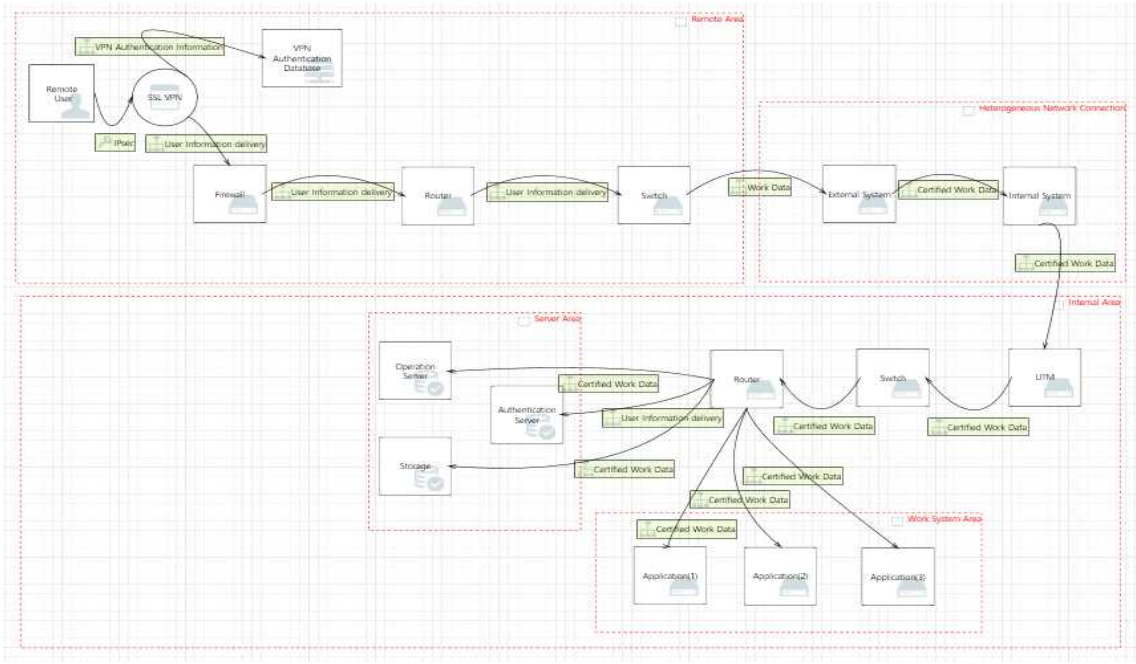
아래의 <그림 8>은 Network Connection와 Server사이의 DFD를 보여준다.



(Figure 8) Network Connection~Server DFD

4.4.4 Level 2.(Low-Level). Diagram

<그림 9>의 DFD Level 2는 비대면(재택)근무 네트워크 망도(동작원리/데이터 흐름)를 기반으로 Microsoft Threat Modeling Tool을 활용하여 위험을 식별한다.



(Figure 9) Level 2. Data flow diagram

<그림 5>와 같이 비대면(재택)근무 위협 모델을 구성하고 MITRE ATT&CK Framework 등을 통해 각 위협 요소별로 분류한 결과를 <표 5>와 같이 총 19개의 위험을 도출하였다.

4.5 공격 유형 분석

데이터 흐름을 기반로 분석한 위협 항목은 총53개이다. 본 논문에서 분석하는 재택근무 시스템은 기본구성, 네트워킹, 인프라를 포함한 환경을 뜻한다. 위협 시나리오 분석은 재택근무 시스템을 MITRE ATT&CK Framework에서 선별한 48개 위협과 논문에서 식별한 5개에 대해 아래의 <표 4>와 같이 기본구성, 네트워킹, 인프라로 매핑하여 분석하였다.

<표 4> 재택근무 시스템 구분

구 분	Details
기본구성	재택근무 시스템을 구축하는데 사용되는 기본 구성 요소
네트워킹	재택근무를 위해 망연동시스템 및 VDI를 사용하기 위해 상호작용하는 방법
인프라	재택근무 시스템을 사용하기 위한 네트워크를 포함한 제반 환경

4.5.1 공격 유형 세부 분석

STRIDE 위협 모델링을 통해 분석한 53개의 위협 항목 중 핵심적인 내용들만 정리하여 분류한 공격 항목은 19개로 <표 5>와 같다.

<표 5> STRIDE 위협모델링에 기반한 공격 유형 세부 분석

System No.	category	STRIDE Classification	Threat Details	Threat No.
P1	기본구성 (계정관리)	E	사용자 접속 단말 취약점 이용, 도메인, 웹 서비스 등 적대적 서비스와 결합, 계정 획득(자격 증명)한다.	T6
P2		S	사회공학적 기법을 사용, 허용된 접근자외 비인가 접근자 계정을 생성한다.	T8
P3		T	신뢰할 수 있는 제3자(유지보수, 서비스 계약자 등)에 의한 액서스 권한을 획득한다.	T15
P4		T	권한이 없는 사용자(계정)에게 특정 권한이 부여되어 내부 시스템 공격이 가능하다.	T16
P5		E	공격자는 시스템, 서비스 및 네트워크 리소스에 액세스하는데 사용할 수 있는 자격증명에 액세스하기 위해 2FA이하 인증 매커니즘을 공격한다.	T26
P6		I	물리적 통제가 불가한 장소에서 접근하는 계정 통제가 불가능할시 침해가 가능하다.	T50
P7	기본구성 (내부정보 관리)	I	공격 대상 조직을 스캔, 네트워크 트래픽을 통해 공격대상 인프라를 조사한다.	T1
P8		I	공격전 호스트에 대한 관리데이터를 수집 (이름, 할당된 IP, 기능 등)한다.	T2
P9		I	사용자에 대한 자격증명(ID/PW, 이름, 주소, 경력 등) 관련 정보를 수집한다.	T3
P10		I	사용자의 조직 정보 (부서 이름, 적용대상 부서, 주요직원들의 역할 등)를 수집한다.	T5
P11	네트워킹	D	공격자는 트래픽 신호를 이용하여 열린 포트에 악의적인 기능을 숨길 수 있다.	T10
P12		E	특정 이벤트를 기반으로 트리거되는 시스템 매커니즘을 이용하여 권한상승 공격을 수행한다.	T17

P13	인프라	D	공격자는 이동식 드라이브와 같은 물리적 매체를 통해 데이터를 유출할 수 있다.	T41
P14		T	공격자는 외부 결과를 조작하거나 숨기기 위해 데이터를 삽입, 삭제 또는 조작할 수 있다.	T44
P15		D	공격자는 사용자에 대한 대상 리소스의 가용성을 저하시키거나 차단하기 위해 네트워크 서비스 거부(Dos) 공격을 수행한다.	T47
P16		S	공격자가 시스템 접근을 위해 하드웨어 제품을 몰래 조작(백도어 등)한다.	T49
P17		E	사용자는 물리적으로 내부 업무영역과 이격(원격접속), 단말기 화면을 통해 데이터 유출이 가능하다.	T51
P18		I	내부 자료를 메일, 클라우드, P2P 등을 통해 유출가능하다.	T52
P19		R	사용자 단말기(PC) 침해에 의한 단말기 통제 권한을 상실, 자격증명, 자료유출이 가능하다.	T53

5. 재택근무 보안 요구사항 도출

인터넷에서 내부망에 접근하여 업무를 수행하는 재택근무 환경을 기반으로 19개 유형의 주요 보안 취약점을 분석하였다. <표 5>를 보면 19개 위협에 대해 기술하였으며 이에 대해 보안성을 확보를 위한 보안 요구사항을 도출하면 아래의 <표 6>과 같다. <표 5>에서 계정관리, 내부정보 관리, 네트워킹, 인프라를 구분하여 위협을 분석하였는데 이를 비슷한 위협별로 구분하여 같은 보안 요구사항을 도출할 수 있는 것으로 분류하여서 보안 요구사항을 제시했다. 동일한 대책으로 묶기 어려운 항목들은 각각 보안 요구사항을 제시하였으며 예로 T5는 사용자의 조직정보 위협으로 분석하였는데 공격자가 대상 조직정보(조직도, 부서별 역할 등) 수집을 시도할 수 있다는 것이다. 이에 보안 요구사항으로 제시한 것은 조직 정보에 대해 내·외부 공개 정보를 구분해야 하는 정책이 필요하다는 것과 외부에 노출시에는 중요부서는 마스킹 처리를 하는 등 최소한의 노출이 필요하다는 것이다. 만약 조직 내 중요 인원이 조직에서의 위치와 역할이 노출되고 개인정보(메일, 전화번호 등)까지 탈취된다면 공격받을 확률이 매우 높기 때문이다. 이와 같이 19개의 위협을 분석하여 아래의 <표 6>을 제시하였다. 이와 같은 <표 6>을 세부적으로 제시하면 개인과 조직의 역할을 구분할 수 있다. 개인은 T5 위협에 대해 개인의 조직에서의 위치와 신상정보가 노출되지 않도록 관리해야한다.

T6·T47 위협에 대해서는 회사에서 지급받거나 개인이 사용하고 있는 단말은 회사 보안정책 준수를 위해 수시로 바이러스 백신 및 필수 보안SW를 업데이트하여야 하며, 단말보호를 위해 비밀번호 등도 관리해야 한다. T16·T17·T26·T50 위협에 대해서는 개인이 수행하는 인증절차(패스워드, OTP 등/2FA 이상)를 시행해야 하며 주기적으로 패스워드를 변경 및 고도화하는 등 보안 대책을 강구해야 한다. T41 위협은 개인의 단말기에 사내에서 제공된 DLP 시스템을 설치하여 인증된 저장매체외에는 사용하지 않아야 한다. T44 위협은 사내에서 제공된 DRM 정책을 준수해야하며 DRM을 임의 해제하거나 시스템을 우회하지 않아야 한다.

조직에서는 T1·T2·T20 위협에 대해 24시간 상주 인력에 의한 네트워크 관제·방화벽 관리가 필요하다. 이를 수행하기 어려운 영세한 업체의 경우 필요시 보안 업체에 위탁을 통해 관제가 이루어져야 한다. T3·T15 위협에 대해서는 방산업체의 경우 무기체계 기술 등은 국가 전략자산에 대한 기술로 외부에 노출되서는 안되는 자료들에 대한 접근이 철저히 통제되어야 한다. 이에 따라 조직에서는 외부에서 접근을 허용할 어플리케이션과 데이터를 분류하여야 하며, 주기적인 위협분석을 통해 필요시 상황에 맞는 허용범위를 설정해야 한다. T5 위협은 IP기반으로 내부에서 접근 가능한 조직 및 구성원에 대한 정보의 공개범위와 외부에서 접근 가능한 조직 및 구성원에 대한 정보

공개의 범위를 구분해야 한다. 외부에서 접근시에는 업무에 필요한 최소한의 정보만 제공해야 한다. T6・T47 위협은 방산 업체 특성을 고려, 보안 강화를 위해 전용 단말을 지급하고 필수 보안SW를 설치해야 하며 업무 자료는 단말에 남지 않고 서버에 남도록 클라우드 서비스를 이용하는 것을 권장한다. T8 위협은 용역업체 등 외부자의 자료 접근에 대해 물리적인 통제(인원에 의한 보안조치)와 기술적인 통제(자료 접근권한 설정 등)가 동시에 이루어져야 한다. T16・T17・T50 위협은 비대면 재택근무 사용자에 대한 자격인증 절차에 대해 지속적인 고도화가 요구되며 특히, 파견・퇴직・휴직 등 자격인증이 불필요한 인원에 대한 수시관리가 적절히 이루어져야 한다. T26 위협은 조직차원에서 2FA 이상의 정책에 대한 검토가 필요하며, 주기적인 평가를 통해 인증방법을 변경하거나 유지하는 등 정책적인 평가가 필요하다. T41・T44・T51・T52・T53 위협은 사용자 단말에 대한 보안정책으로 조직에서는 사용자의 우회 행위에 대해 지속적으로 관제하며 일탈행위를 차단해야 한다. T49 위협은 사내에서 운영하는 정보보안 시스템에 대해 공급망 보안을 고려해 CC인증을 필한 제품으로 도입해야 하며 주기적인 시스템 업데이트를 통해 최적의 보안 수준이 유지되도록 해야 한다.

<표 6> 재택근무 시스템 보안 요구사항

Threat No.	Details
T1	시스템 관리자(네트워크, 서버 등)에 의한 NMS 관제, 방화벽 등 관리를 통해 외부에서 내부 시스템 스캔 시도 등 침해행위를 방지해야 한다.
T2	
T10	
T3	내부 보안정책을 고도화하여 내부망에 대한 자격증명과 일반 시스템 사용시 사용하는 자격증명과 분리가 필요하다.
T15	
T5	조직 정보에 대해 내부 공개용과 외부 공개용을 구분하는 정책이 필요하며 외부 공개시 공격에 노출되지 않도록 최소한 범위에서 공개가 필요하다.
T6	보안 필수S/W가 설치된 업무 전용 단말을 지급하여 재택근무를 시행해야 하며, 재택근무용 단말기는 업무용으로 사용시 상시 관제가 가능해야 한다.
T47	
T8	외주용역 직원, 내부자에 의한 공격 등을 방지하기 위해 사내 보안정책을 강화해야 한다.
T16	주기적으로 사용자에 대한 자격인증 적절성 관리가 이루어져야 한다.
T17	
T50	
T26	자격증명 시스템 고도화가 필요하며 최소한 2FA(ID/PW, 출입카드, 생채정보 등)이상의 정책이 적용되어야 한다.
T41	사용자의 단말기(PC)에 저장매체 통제(DLP) 시스템을 적용해야 한다.
T44	사용자의 단말기(PC)에 파일암호화 (DRM) 시스템을 적용해야 한다.
T49	공급망 보안 / 도입하는 제품은 CC인증 등 보안적합성 검증을 필한 제품을 사용해야 한다.
T51	사용자의 단말기(PC)에 워터마크 삽입, 화면 캡쳐방지 등 화면보안 시스템(DLP)을 적용해야 한다.
T52	사용자의 단말기(PC)에 비인가 사이트 접속 차단 기능을 적용해야 한다.
T53	사용자의 단말기(PC) 분실시 원격으로 삭제할 수 있는 기능을 적용해야 한다.

6. 결 론

방산업체가 무기체계를 다루는 높은 보안이 요구되는 특수한 조직임을 고려하여도 비대면 재택근무는 앞으로도 지속될 수 밖에 없는 중용한 기술이자 정책이다. 이에, 본 논문에서는 STRIDE 위협 모델링을 기반으로 방산업체의 비대면(재택) 근무 시 참고할 수 있는 19개 주요 위협에 대한 보안 가이드를 제시하였다. 방산업체의 비대면(재택) 근무시 발생할 수 있는 보안 위협을 실질적인 기술에 기반하여 작성하였고 MITRE ATT&CK Framework에서 다루는 공격자의 전술, 절차에 대해 세부적으로 분석하여 공격자가 시행할 수 있는 위협을 세부적으로 분석하였다. 여기에 재택근무시 인터넷에서 내부망으로 접속하는 데이터 흐

름을 고려하여 주요 위협에 대해 보안 요구사항 제시하였으며 특히, 방산업체가 무기체계 기술 등 국가 전략자산과 관련된 자료를 다루는 조직임을 고려하여 비대면 근무시 접근 가능한 어플리케이션 및 데이트 분류, 내외부자 접근통제 강화, 조직 정보노출 최소화 등 보다 높은 보안 요구사항을 충족하도록 제시하였다. 이를 충족하여 보다 안정적인 비대면(재택)근무가 가능하기를 기대한다.

참고문헌

[1] 권영환, 박태형, 서영희, 송지환, 이종엽, 전희승, 원격근무 솔루션 기술・시장 동향 및 시사점, SPRI(소프트웨어정책연구소) 연구보고서, 2020. 4.29. IS-093.

[2] 강동윤, 이상웅, 이재우, 이용준, 최근 사이버 위협 동향과 가상사설망을 활용한 재택 근무자 보안 강화 기술 연구, 정보보호학회지 제31권 제3호, 2021. 6.

[3] https://owasp.org/www-project-top-ten/, OWASP Top Ten 2021.

[4] 국가정보원, 2023년 사이버안보 위협 전망

[5] KISA(한국인터넷진흥원), 2023 사이버보안 위협 전망.

[6] https://attack.mitre.org/, Miter Att&ck Framework

[7] 김다현, 민지영, 안준호, STRIDE 위협 모델링 기반 가상 사설망 취약점 분석 및 보안 요구사항 도출, 한국인터넷정보학회, Dec 30. 2022. 23(6):27.

[8] 박상길, 김기봉, 손경자, 이원석, 박재표, 공공기관 물리적 망분리 환경에서의 비대면 스마트워크 근무 환경구축을 위한 보안 모델 연구, 한국융합학회논문지, 10/31/2020, Vol. 11, Issue 10, p. 37-44.

[9] 정여진, 스마트워크 환경에서의 윈도우즈 퍼스널 컴퓨터 모니터링 및 보안 감사 방안, 2021, 성균관대학교 정보통신대학원 석사 논문.

[10] 허기열, 공공기관 보안 강화를 위한 개선안의 중요 요인에 관한 연구 : 재택근무를 중심으로, 2020, 숭실대학교 대학원 석사 논문.

[11] 박찬규, COVID-19 이후 증가하는 재택근무 환경의 보안실태와 대책 : 보안 인증제도를 중심으로, 2021, 숭실대학교 정보과학대학원 석사 논문.

[12] 황찬웅, 배성호, 이태진, MITRE ATT&CK 및 Anomaly Detection 기반 이상 공격징후 탐지기술 연구, 2021, 융합보안논문지, 21:3, 13-23.

[13] 명성식, 원격 근무에 따른 보안 인프라 변화와 사이버 위협 대응 방안에 관한 연구, 고려대학교 컴퓨터정보통신대학원 석사 논문.

[14] 조영성, 박용우, 이건호, 최창희, 신찬호, 이경식, MITRE ATT&CK을 이용한 APT 공격 스코어링 방법 연구, Journal of The Korea Institute of Information Security & Cryptology, VOL.32, NO.4, Aug. 2022.

[15] 윤영수, STRIDE 위협 모델링에 기반한 블록체인 서비스 보안성 확보 방안, 2022, 고려대학교 컴퓨터정보통신대학원 석사 논문.

[16] 오인경, 서재완, 이민규, 이태훈, 한유나, 박의성, 지한별, 이종호, 조규형, 김경곤, STRIDE 위협 모델링에 기반한 스마트 TV 보안 요구사항 도출, Journal of The Korea Institute of Information Security & Cryptology, VOL.30, NO.2, Apr. 2020.

[17] 이승욱, 이재우, STRIDE 위협 모델링에 기반한 클라우드 컴퓨팅의 쿠버네티스의 보안 요구사항에 관한 연구, 한국정보통신학회논문지 Vol. 26, No. 7: 1047~1059, Jul. 2022.

[18] 조세라, 위협 모델링을 통한 차량 원격제어 서비스 보안 요구사항 도출, 2022. 고려대학교 컴퓨터정보통신대학원 석사 논문.

[19] 유동현, 김용욱, 하영재, 류연승, 비대면 시대의 신 융합보안 위협과 대응 방안에 대한 고찰, Journal of the Korea Convergence Society, Vol. 12. No. 1, pp. 1-9, 2021.

[20] 김소연, 하영민, 김성율, 최상용, 이종락, 원격근무 환경에서의 사이버 보안 위협 분석, 한국컴퓨터정보학회 하계학술대회 논문집 제28권 제2호 (2020. 7).

[21] 류효경, VPN 원격 근무 환경의 SIEM을 활용한 공격 탐지 기법 연구, 2021, 고려대학교 컴퓨터정보통신대학원 석사 논문.
[22] 신승우, 조인준, 뉴노멀 시대의 공공기관 원격보안 모델 개선방안, 한국콘텐츠학회 논문지, 22(9), pp.104-112 Sep, 2022.
[23] Common Vulnerabilities and Exposure, “CVE-2022-42475”[Internet], https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2022-42475.
[24] Common Vulnerabilities and Exposure, “CVE-2020-12812”[Internet], https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-12812.
[25] Common Vulnerabilities and Exposure, “CVE-2018-13379”[Internet], https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2018-13379.
[26] Common Vulnerabilities and Exposure, “CVE-2021-34473”, “CVE-2021-28482”, “CVE-2021-28481”, “CVE-2021-28480”[Internet], https://cve.mitre.org/cgi-bin/ cvekey.cgi?keyword=CVE-2021-34473. CVE-2021-28482, CVE-2021-28481, CVE-2021-28480
[27] Common Vulnerabilities and Exposure, “CVE-2020-16875”[Internet], https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-16875.

〔저자소개〕

황 규 섭 (Gue-Sub Hwang)
2009년 2월 전북대학교 학사
2021년 1월 국방대학교 석사
2021～현재 명지대학교 박사과정
email : Playnamo1@naver.com

류 연 승 (Yeon-Seung Ryu)
1990년 2월 서울대학교 학사
1992년 2월 서울대학교 석사
1996년 8월 서울대학교 박사
2003～현재 명지대학교 교수
email : ysryu@mju.ac.kr