# 의료기관 원격접속 보안조치 가이드



▶ 외부 오픈된 원격접속(RDP)를 통해 침투 후 LI부 서버(원격허용) 추가 접속하여 랜섬웨어 감염

## 1. 원격접속 보안조치 미흡으로 인한 해킹 사고 사례

원격 접속(RDP) 서비스를 이용한 내부 정보시스템 침투

### 운영체제, 보안장비, 시스템 등 보안조치를 통한 안전한 서비스 이용 필요 2. 원격접속 보안 조치 사항



### 사용하지 않는 원격 데스크톱 프로토콜(RDP) 비활성화 2-1. (OS) RDP 서비스 비활성화

#### (방법1)

▶ 제어판 → 시스템 → 원격 설정 → 시스템 속성 → 원격 탭
 → 원격 연결 허용 안 함 선택

#### (방법2)

▶ 시작 → 설정 → 시스템 → 원격 데스크톱 → 원격 데스크톱 활성화 끔



### 원격 데스크톱이 필요한 시스템은 기본 포트 변경하여 사용 2-2. (OS) RDP 기본 포트 변경

### (순서1)

▶ 윈도우 귀() #R → 실행 창에서 "regedit" 입력 → "HKEY\_LOCAL\_MACHINE₩SYSTEM₩ CurrentCont rolSet₩Col7.ntrol₩TerminalServer₩Wds₩rdpw d₩Tds₩tcp" 경로 확인

#### 📑 레지스트리 편집기

퓨터₩HKEY_LOCAL	MACHINE#SYSTEM#CurrentCo	ntrol	Set₩Control₩Termina	l Server₩Wds₩rdpwd¥	₩Tds₩tcp
	ConnectionHandler DefaultUserConfiguration KeyboardType Mapping RCM SessionArbitrationHelper SysProcs TerminalTypes Utilities VIDEO Wds PIDEO Wds Pds Pds VinStations TimeZoneInformation	^	이름 (기본값) (기본값) 이utBufCount OutBufCount OutBufCount OutBufLength PdClass PdCLass PdCLass PdFlag PdFlag PdPame PdPame PdPame PdPame ServiceName	종류 REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_MULTI_SZ REG_SZ	데이터 (값 설정 안 됨) 0x0000000a (10) 0x00000006 (6) 0x0000006 (73) 0x000000212 (530) 0x0000002 (2) tdtcp 0x0000004e (78) tcp 0x000000d3d (3389) tssecsrv tcpip

### (순서2)

▶ [PortNumber] 수정 → (단위) 10진수 선택 → 기본 값 "3389" 에서 임의의 숫자로 변경 후 확인



Windows 방화벽 설정을 통해 인가된 IP만 원격 접속 허용

## 2-3. (OS) Windows 방화벽 RDP 접근 설정

### (순서1)

 ▶ 윈도우 귀(聲) + R → 실행 창에서 "wf.msc" 입력 → "인바 운드 규칙" 내 "원격 데스크톱 - 사용자 모드" 정책 확인
 ※ RDP 디폴트 포트 변경하여 사용 시 새 규칙을 통해 변경된 포트로 프로토콜 TCP, UDP 용 2개 규칙 생성 필요

#### 🔗 고급 보안이 포함된 Windows Defender 방화벽

파일(F) 동작(A) 보기(V) 도용	륨말(H)											
🗢 🄿 🙋 💼 🗟 🖬 🖬												
🌧 로컬 컴퓨터의 고급 보안이 포[	인바운드 규칙											
鐵 인바운드 규직	이름	그룹	프로필	사용	작업	다시 정의	프로그램	로컬 주소	원격 주소	프로토콜	로컬 포트	원격 포트
이경 보안 규칙	🔮 영화 및 TV	영화 및 TV	도메인,	q	허용	아니요	모두	모두	모두	모두	모두	모두
> 토 모니터링	🔮 영화 및 TV	영화 및 TV	도메인,	예	허용	아니요	모두	모두	모두	모두	모두	모두
	🔮 영화 및 TV	영화 및 TV	도메인,	예	허용	아니요	모두	모두	모두	모두	모두	모두
	원격 데스크톱 - (TCP-WS-In)	원격 데스크톱(WebSocket)	모두	아니요	허용	아니요	System	모두	모두	TCP	3387	모두
	월경 데스크토 (TCD WSS In)	의견 데스크토(MohSocket)	05	0110	치요	01110	System	05	05	TCD	2202	05
	원격 데스크톱 - 사용자 모드(TCP-In)	원격 데스크톱	모두	아니요	허용	아니요	%Syste	모두	모두	TCP	3389	모두
	원격 데스크톱 - 사용자 모드(UDP-in)	원격 데스크톱	모두	아니요	허용	아니요	%Syste	모두	모두	UDP	3389	모두
	원격 네으크훕 - 섀도(ICP-IN)	원석 네스크옵	모두	아니포	어중	아니포	%Syste	모두	모두	TCP	보누	모두
	원격 볼륨 관리 - 가상 디스크 서비스 로	원격 볼륨 관리	개인,	아니요	허용	아니요	%Syste	모두	로컬 서브넷	TCP	RPC 동적	모두
	원격 볼륨 관리 - 가상 디스크 서비스 로	원격 볼륨 관리	도메인	아니요	허용	아니요	%Syste	모두	모두	TCP	RPC 동적	모두
	원격 볼륨 관리 - 가상 디스크 서비스(RP	원격 볼륨 관리	개인,	아니요	허용	아니요	%Syste	모두	로컬 서브넷	TCP	RPC 동적	모두
	원격 볼륨 관리 - 가상 디스크 서비스(RP	원격 볼륨 관리	도메인	아니요	허용	아니요	%Syste	모두	모두	TCP	RPC 동적	모두
	원격 볼륨 관리(RPC-EPMAP)	원격 볼륨 관리	도메인	아니요	허용	아니요	%Syste	모두	모두	TCP	RPC 끝점	모두
	원격 볼륨 관리(RPC-EPMAP)	원격 볼륨 관리	개인,	아니요	허용	아니요	%Syste	모두	로컬 서브넷	TCP	RPC 끝점	모두
	원격 서비스 관리(NP-In)	원격 서비스 관리	개인,	아니요	허용	아니요	System	모두	로컬 서브넷	TCP	445	모두
	원격 서비스 관리(NP-In)	원격 서비스 관리	도메인	아니요	허용	아니요	System	모두	모두	TCP	445	모두
	원격 서비스 관리(RPC)	원격 서비스 관리	도메인	아니요	허용	아니요	%Syste	모두	모두	TCP	RPC 동적	모두
	원격 서비스 관리(RPC)	원격 서비스 관리	개인,	아니요	허용	아니요	%Syste	모두	로컬 서브넷	TCP	RPC 동적	모두
	원격 서비스 관리(RPC-EPMAP)	원격 서비스 관리	도메인	아니요	허용	아니요	%Syste	모두	모두	TCP	RPC 끝점	모두
	원격 서비스 관리(RPC-EPMAP)	원격 서비스 관리	개인,	아니요	허용	아니요	%Syste	모두	로컬 서브넷	TCP	RPC 끝점	모두
	원격 시스템 종료를 위한 인바운드 규칙(	원격 시스템 종료	모두	아니요	허용	아니요	%syste	모두	모두	TCP	RPC 끝점	모두

#### (순서2)

► [원격 데스크톱-사용자 모드] 확인 → 영역 탭 → 원격 IP 주 소 선택 → 허용된 원격접속 사용자 IP 추가 후 적용(TCPin, UDP-in 모두 적용)

※ 원격 접속 비활성화 시스템 추가 방화벽 설정 - 일반 탭 → 작업 → "연결 차단" 선택 후 적용

~ 급		로컬 보안 주체	원격	사용자	
일반	프로그램 및 서비스	원격 컴퓨터	프로토콜 및 포트	영역	
노주 위 털토	2				
	) 모든 IP 주소(N)				
📲 (	) 다음 IP 주소(T):				
		추가([	))		
		편집(E	)		
			D		
		AL 21 V			
원격 IP 주소	2				
	) 모든 IP 주소(Y)				
•	) 다음 IP 주소(H):				
	192, 168, 0, 10	추가			
		편집(	D		
		ער ונד	5.43		
		701210	1417		

#### 〈방화벽 기본 정책 예시〉

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	홈페이지서버	TCP_80(HTTP)	Allow
외부	Any	홈페이지서버	TCP_443(HTTPS)	Allow
Any	Any	Any	Any	Deny

▶ 방화벽 정책은 우선순위가 존재, 'Top-Down' 방식으로 정책 리스트에서 위쪽에 있을수록 정책의 우선순위 적용

<u>2-4. (보안장비) 방화벽(FW) 보안 정책 설정</u>

(설명)

책 적용 필요

'방화벽(FW) 보안 정책 적용을 통해 인가된 IP만 원격 접속 허용

※ 방화벽 마지막 정책에는 모든 접근을 차단하는(Any → Any, Deny) 정

### (윈격접속 정책 적용)

▶ 외부에서 내부 시스템 원격 접속 차단 권고

▶ 외부에서 원격 접속이 필요한 경우, "방화벽 원격접속 정책 적용 예시"와 같이 허용된 IP만 원격 접속 가능하도록 설정

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	홈페이지서버	TCP_80(HTTP)	Allow
외부	Any	홈페이지서버	TCP_443(HTTPS)	Allow
허용 IP	Any	원격 허용 시스템 IP	TCP_33899	Allow
Any	Any	Any	Any	Deny

〈방화벽 원격접속 정책 적용 예시〉

〈구성도〉



구성요소	기능			
가상화 서버(VDI)	원격근무를 위한 가상데스크톱 생성			
인증서버	원격 근무를 위한 접속 사용자 인증 수행			
관리서버	원격근무PC 와 가상 데스크톱 매치 및 관련 보안정책 적용			
원격근무 PC (VDI 단말)	가상데스크톱 접속			

# 2-5. (시스템) 원격근무시스템 구성

원격근무시스템을 구성하여 원격 근무자 보안관리 방안 마련

〈원격근무 절차〉

③ 가상화 서버는 인가된 근무자인지 인증 요청(인증 서버)
④ 근무자는 가상화 서버에서 관리 서버 가상데스크톱 요청
⑤ 관리 서버는 인증된 근무자에게 가상데스크톱 할당
⑥ 할당 받은 가상데스크톱 이용하여 원격근무 수행

② VPN 서비에서 원격 근무를 위한 VPN 사용자 인증

VPN 서비에 접속

① 원격근무자는 원격근무PC에 설치된 VPN Client이용,

► 원격근무 PC 보안관리(백신,화면캡처방지등)

- ▶ 업무 자료 유출 방지를 위한 자료 암호화 대책 적용
- ▶ 원격근무자이중인증(OTP등)을 활용하여 적절한 접근권한 통제
- ▶ 원격근무자변경시, 시스템에접근권한즉시반영절차마련·운영

〈보안대책〉

영웅·립수'침지기5딴안보

- ▶ 원격근무보안준수사항이포함된업무수칙등 '원격근무
- ▶ 원격근무시스템 구축 전, 원격근무 가능 업무 범위 선별

## 2-5. (시스템) 원격근무시스템 구성





### 외장디스크, TAPE, NAS, 클라우드, 자체 백업 시스템 등 이용하기



네트워크 분리하여 소산 백업하기



정기적인 백업 주기 정하기



랜섬웨어 대비 백업도 잊지 마세요!

랜섬웨어 피해 신고 병원 대다수가 데이터 백업 체계가 없어 어려움을 겪었습니다.

## HISC 의료정보보호센터 감사합니다.

문의사항: 의료정보보호센터 보안관제실

Tel.02-6360-6280 Fax.02-6360-6284 https://www.hisc.or.kr)