WEBINAR

재택근무 보안 강화를 위한 지니언스와 포티넷의 협업 솔루션

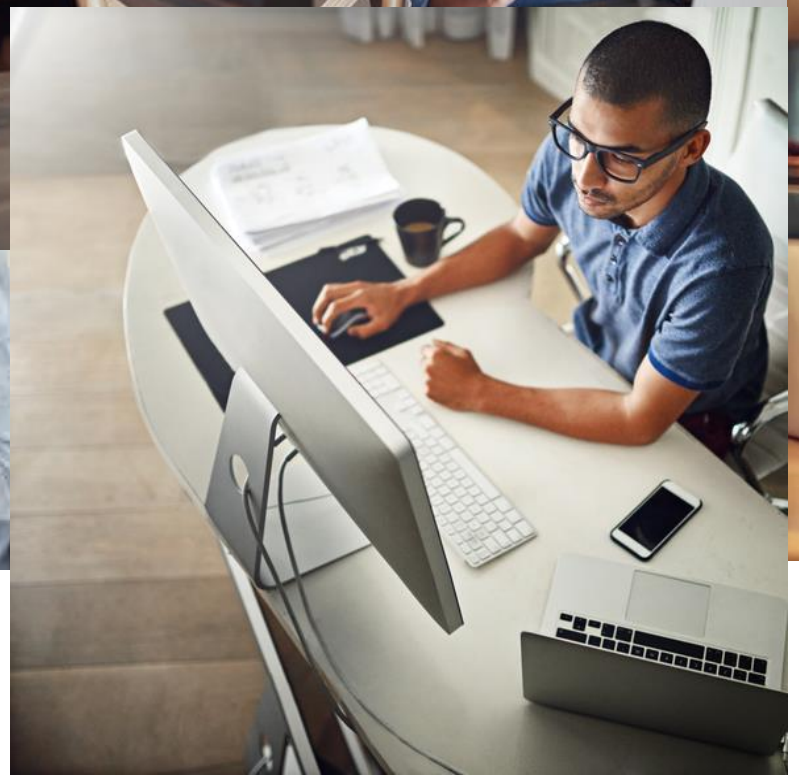
:재택근무 보안을 강화하고 보안 사고를 예방하기

지니언스 : 임무권 책임

포티넷코리아 : 이창운 이사

Genians | FORTINET

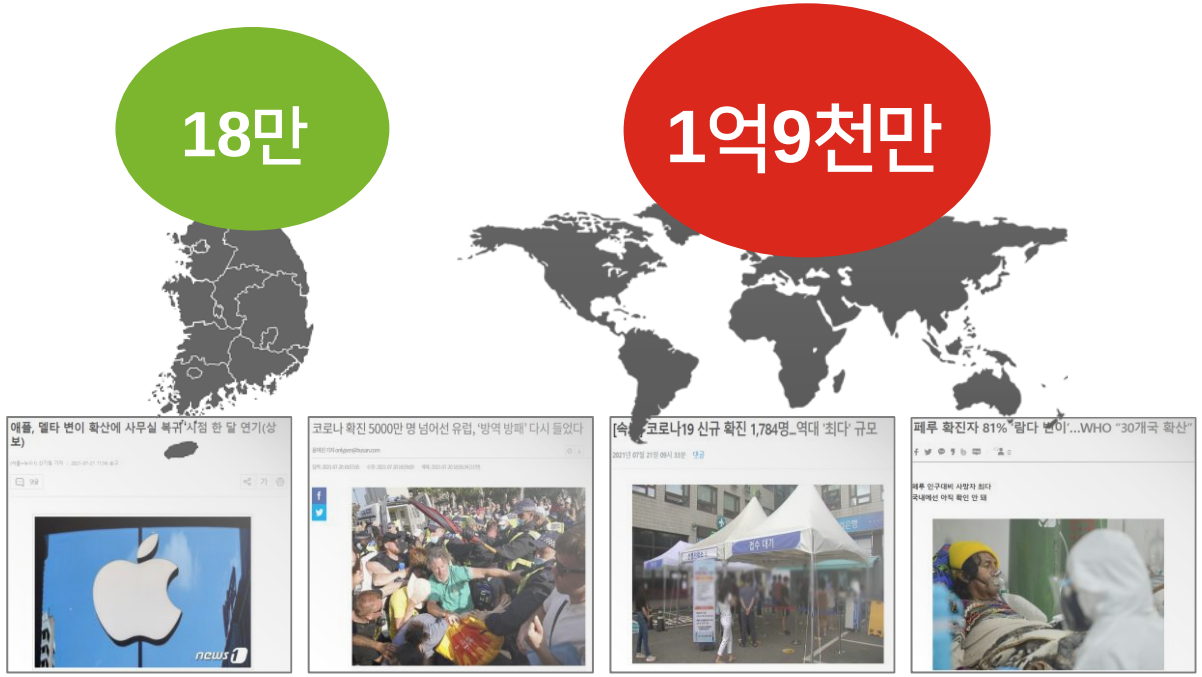
WEBINAR



Genians | FORTINET

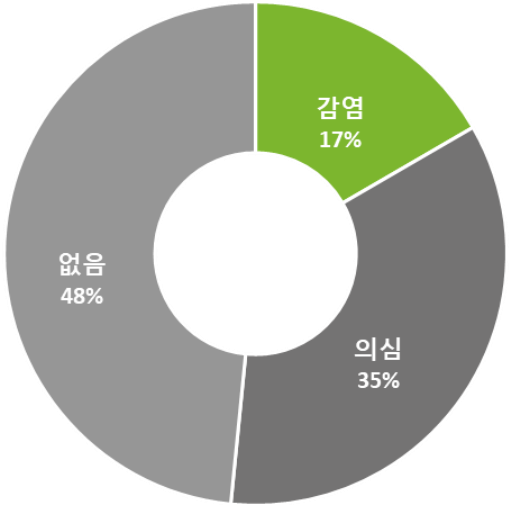
재택근무 배경과 위협 현황

재택근무 확산의 근본적 이유



Covid-19 Pandemic

[재택근무 위협 경험]

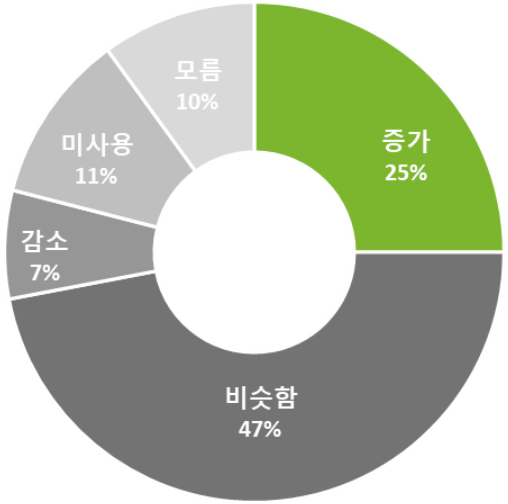


Source: 인터넷진흥원

50% ↑

악성 위협 경험

[코로나 이후 피싱/스팸 동향]



Source: Deloitte research

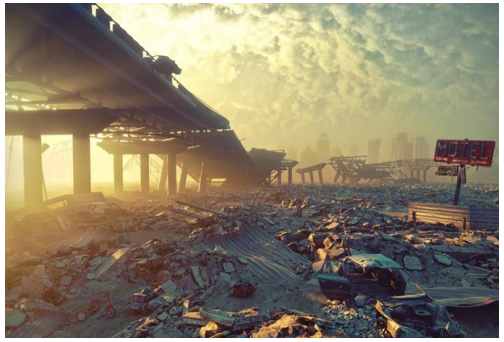
14% ↑

재택 보안 우려

업무 환경의 변화 : 재택근무

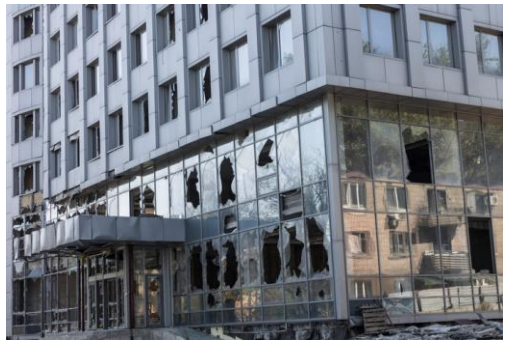
위기는 여러가지 형태로 다가옴 :

- 자연 재해
- 세계적인 전염병
- 테러 행위

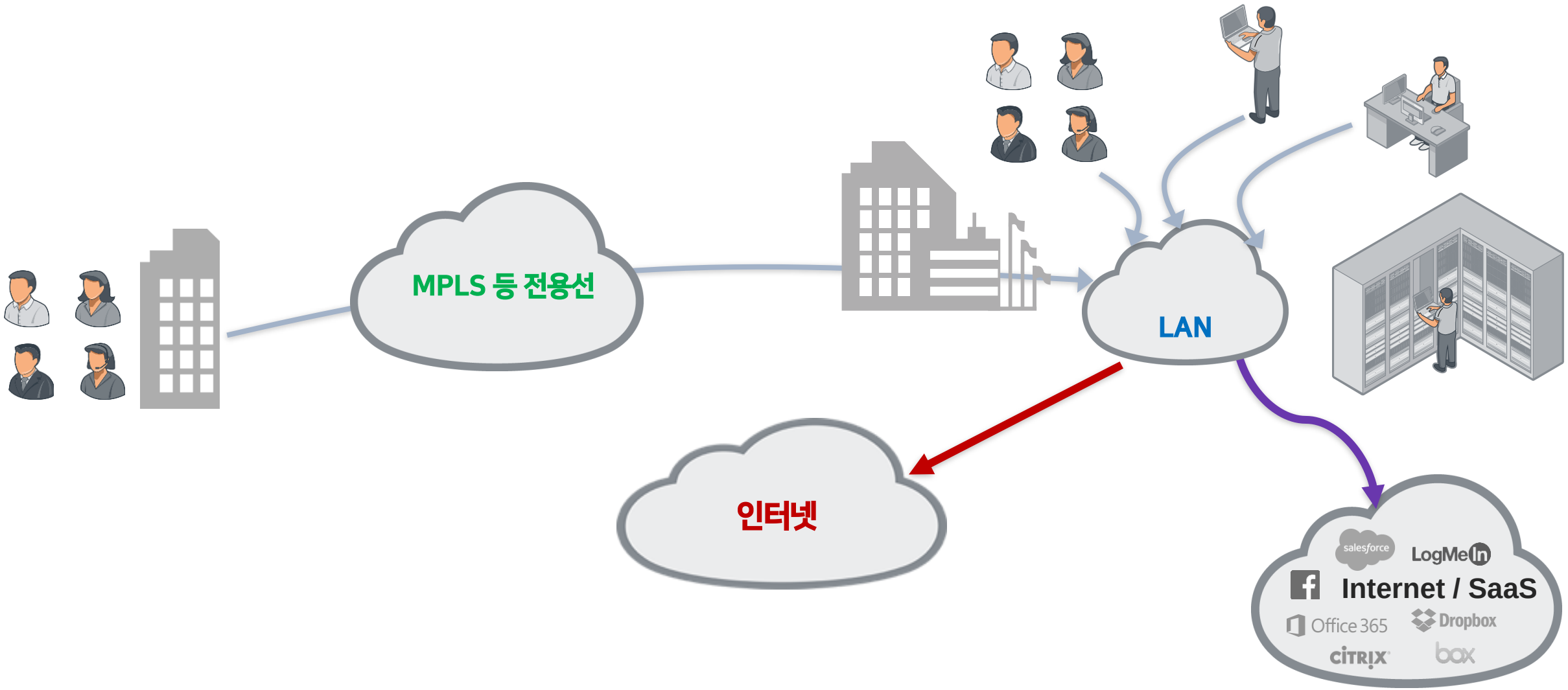


아무런 경고나 징조가 없이도 타격을 받을 수 있음 :

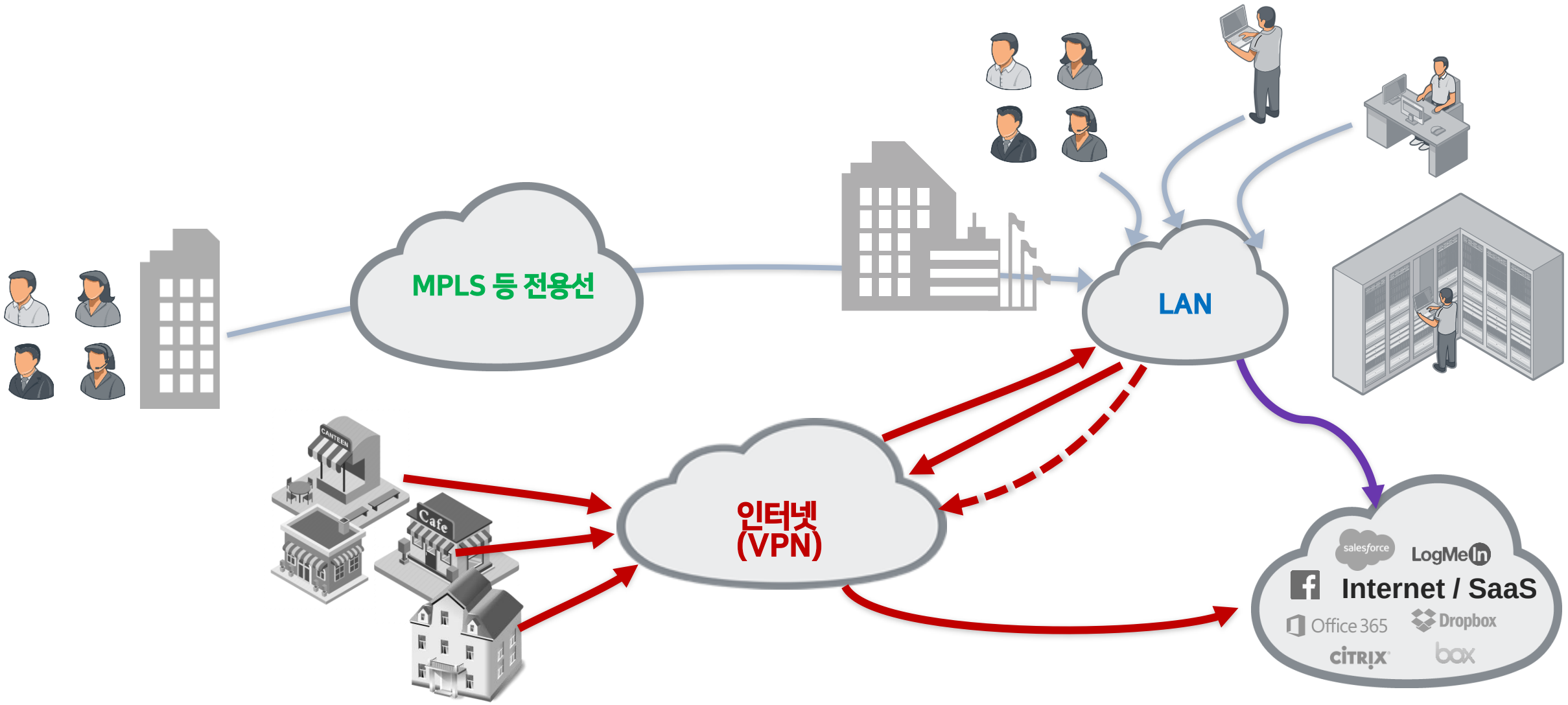
- 업무 연속성 계획 / 재해복구
- 외부에서 근무하는 직원
- 모든 규모의 업무가 영향



업무 환경의 변화 : 재택근무



업무 환경의 변화 : 재택근무



WEBINAR

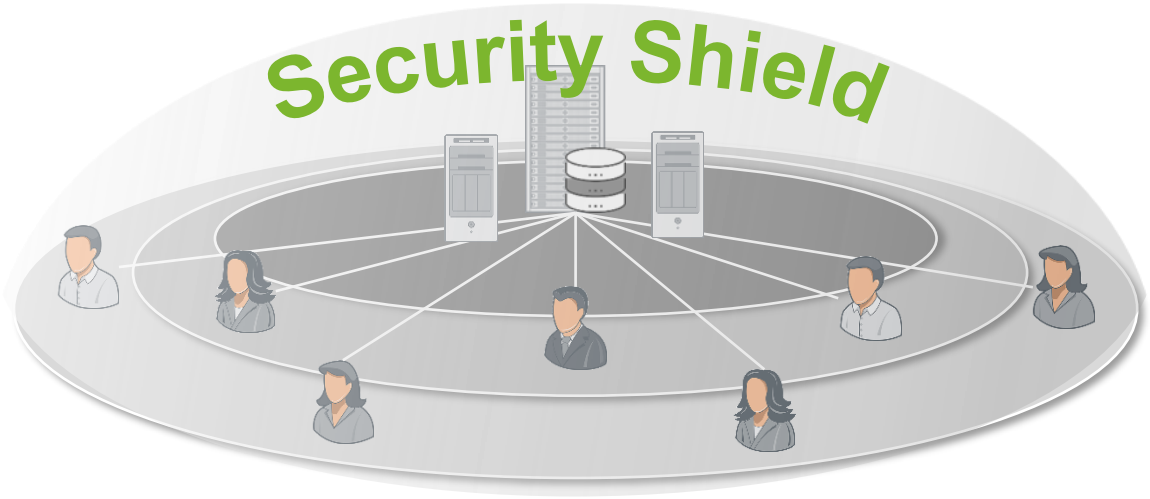
재택근무의 중요성

Genians | FORTINET

재택근무 보안의 중요성

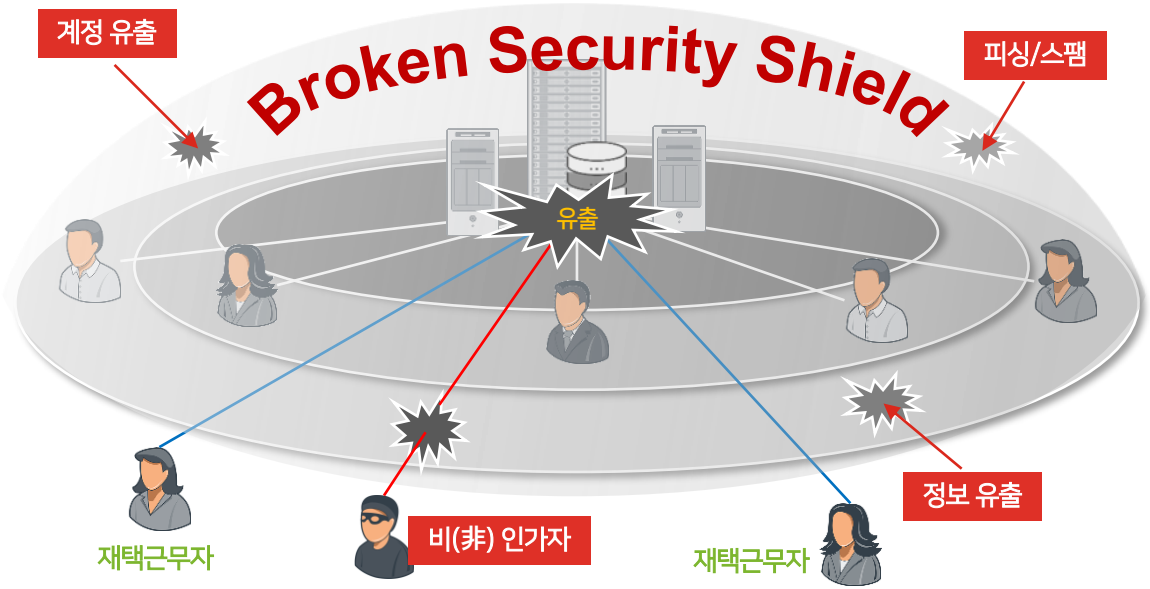
기존 내부 통제정책 만으로 재택 근무자 보호 및 보안 유지 불가

[재택근무 이전]



내부 통제 정책↑ 직원 관리 용이↑ 보안 솔루션 견고↑

[재택근무 시행]



위협 홀(Hole)↑ 피싱/스팸 메일↑ 비인가자 유입↑

국내 의료업계 사례

'병원 의료정보' 해킹에 유출...국내 첫 확인

발행일 : 2013.08.28

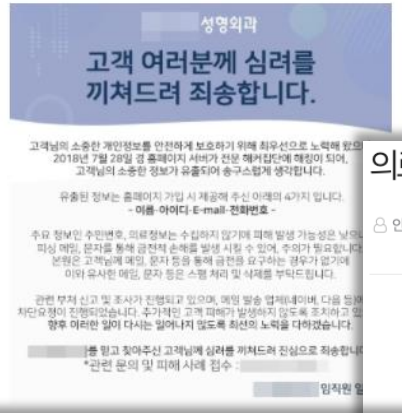
[AD] [DS&G] 슈퍼마이크로 JBOF 출시, 초고속 NVMe 기반 1PB 대용량 스토리지!

해커가 PC 원격제어 가능해 충격

병·의원 홈페이지 해킹 후 개인정보로 환자 '협박'

서울 대형 성형외과 지난달 피해…복지부, 하반기 보안 통합관제센터 운영

〔 2018년 08월 03일 06시 08분 〕



〔데일리메디 한해진 기자〕 최근 한 유명 성형외과 홈페이지 해킹에 따라 환자들의 개인정보가 유출되는 등 2차 피해가 발생하는 사태가 벌어져 의료기관들이 홈페이지 보안에 경각심을 가져야 할 것으로 보인다.

의료 사이트, 디페이스 공격 당해...해킹에 여전히 취

좋아요 66개 | 입력 : 2018-04-08 16:55

대형병원 웹사이트 및 모바일 페이지 디페이스 해킹

낮은 버전 OS와 윈도우 서버 사용 등 보안 취약

의료정보 보호 위한 정보보안 관리체계 도입 서둘러야

[보안뉴스 김경애 기자] 의료 사이트의 경우 내부 시스템에 연결될 수 있어 민감한 환자정보와 의료정보까지 탈취될 수 있다. 이에 따라 높은 보안성이 요구되는 곳이 바로 의료기관이

의료기기마저...'해킹 안전지대' 없다

안경진 기자 | 승인 2015.08.18 17:00 | 댓글 0

미국 이어 국내서도 환자정보 유출...원격의료 논란 예상

미국에서 보안 문제로 약물주입펌프가 대량 리콜되는 사태가 벌어졌다.

도 환자정보 유출에 이어 지난주에는 서울 한 대학 개월 동안이나 북한으로부터 전산망을 장악당한 사 지면서 의료기기 해킹이 뜨거운 감자로 떠오를 전

물주입펌프 사용 중지 조치

식품의약국(FDA)은 보안상 취약을 이유로 모든 보 관에 대해 호스피라(Hospira)의 심빅 약물주입펌 piq Infusion System) 사용을 금지시켰다.

은 물론 응급실, 수술실 등 다양한 의료영역에서 사용되는 약물주입펌프가 대부분 병원 네트워크 있기 때문에 해킹될 우려가 크다는 것. 무선통신 기술 덕택에 체내 장치로부터 환자정보를 컴퓨터 내려 받거나 장치조작만으로 치료가 가능해지는 등 혜택이 늘어난 대신, 의료사고나 공격에도 취약 다.

자에게 자동으로 약물을 투여해 주는 인슐림펌프나 심박조율기(pacemaker)같이 혈역학적 상태 게 관여하는 체내 이식형 기기에 누군가 악의적으로 접근한다면 환자 생명까지도 위협받을 수 있

HOME > 정책

IoT 의료기기 해킹 빈번...병원의료정보 보안 '구멍'

홍숙 | 승인 2018.08.13 05:10

[redacted] 의장은 "[redacted]에서 정보 보안 담당자는 1명이다. 따로 의료정보 보안은 담당자가 없는 곳도 부지기수다"며 "의료정보 보안 분야와 관련해 전문적인 면허가 없는 것이 대부분이며, 정보 보안문제는 고려하지도 않고 대부분 의료정보 '활용'에만 관심을 가지고 있다"고 지적했다.

이어 그는 "민감한 의료정보에 보안이 제대로 이뤄지지 않아 해킹을 당할 경우 심각한 위기가 올 것"이라며 "단지 개별의료기관에만 맡긴 것이 아니라 의료계, 정부, 산업계의 협력이 필요하다"고 덧붙였다.

이동근 KISA 침해사고 분석단장 역시 의료정보는 다른 어떤 정보보다 해킹의 위험성이 매우 높다고 지적했다. 이 단장은 "현재 의료정보의 가치가 올라가면서, 해커들이 랜섬웨어들을 통해 병원정보에 대한 해킹을 많이 시도하고 있다"고 언급했다.

이 단장이 경험상 지적한 보안문제는 크게 두 가지다. ▲병원 전산시스템 ▲여러 의료기기 등으로 인한 보안 문제다.

이 단장은 "병원 측에서 개발자와 유지 보수 담당자에 대한 통제 수준이 매우 약하다. 실제로 보안과 관련된 일을 하고 있는 사람들은 의료정보와 관련해 매우 큰 권한을 가지고 있다. 병원에 주요 시스템을 접근할 수 있을 뿐만 아니라 특정 시스템에 대한 환경 설정값을 변경할 수 있는 권한을 가지고 있다"며 "이렇게 큰 권한을 가진 인력을 병원 측에서 통제할 수 없다면, 큰 위험이 초래된다. 실제로 병원 외에 다른 기업도 해커들이 개발팀을 타겟으로 내부망을 장악하는 사례가 종종 있다"고 설명했다.

이어 그는 "IoT 기술이 발달하면서 이러한 기술이 접목된 의료기기를 통한 해킹 사고도 빈번히 발생하고 있다"며 "병원은 IoT 기기에 대한 보안 점검도 철저히 할 필요가 있다"고 덧붙였다.

IT 환경 변화를 이용한 공격 사례

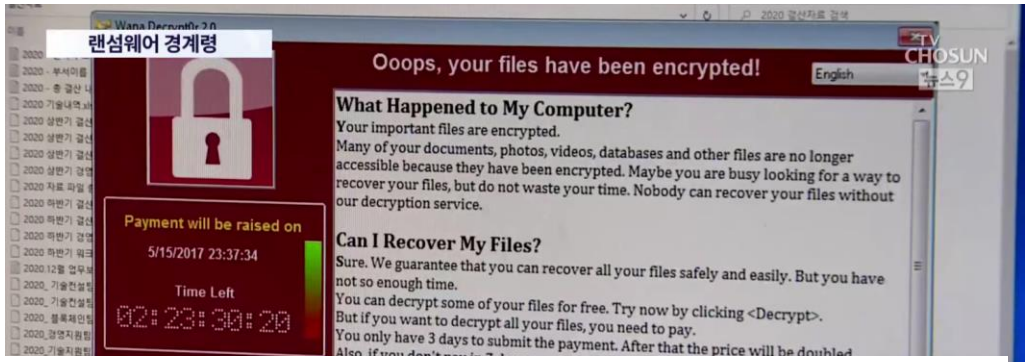
재택근무로 늘어난 '빈틈' 노린다…전세계 10초당 1건 랜섬웨어 피해

무차별 유포는 옛말, 마약 조직처럼 분업화·전문화

직원들 이메일·원격 업무망등
보안 취약한 침투경로 많아져
전세계서 10초당 한 번꼴 피해

작년 의료기관 공격 45% 쑥
환자 데이터 빼내 공개 협박
몸값 협상 전문가까지 등장

◆ 랜섬웨어 주의보 ◆



재택근무의 역습, 누군가 우리집 PC를 노린다

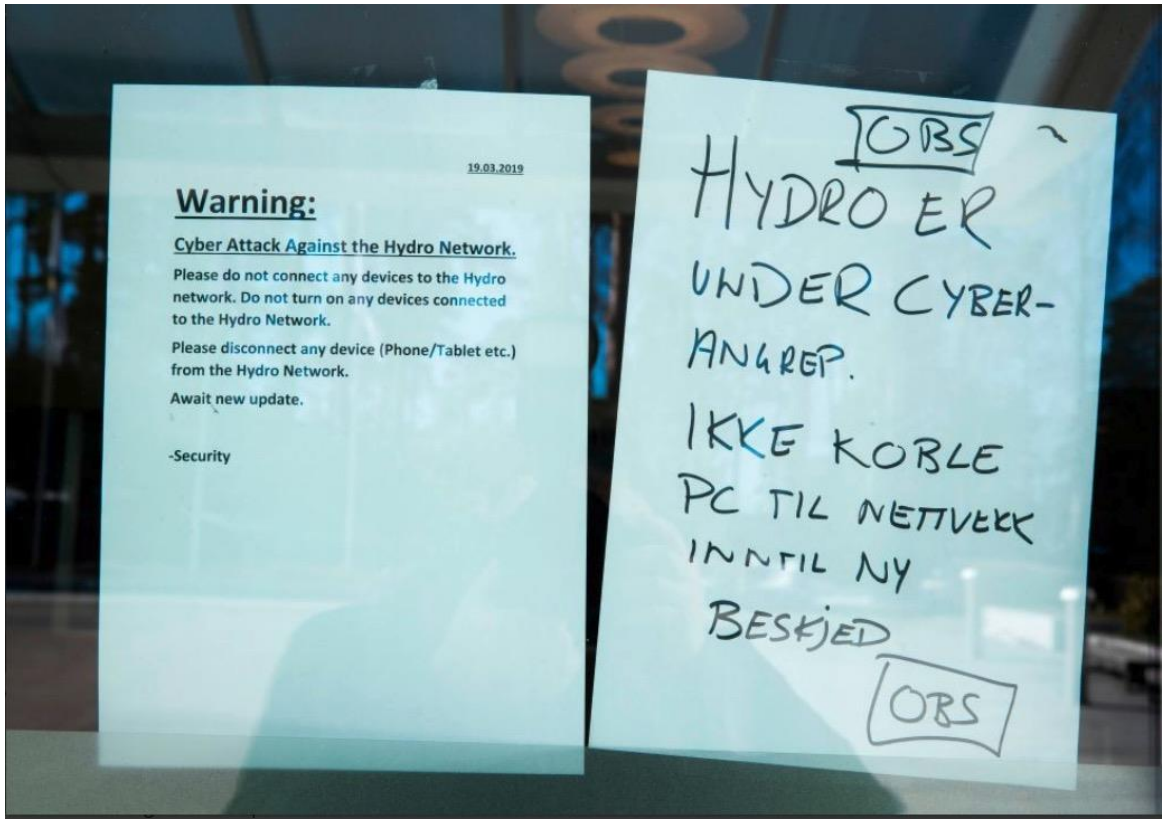
안경애 기자 | 입력: 2021-02-23 10:11

서울 송파구 삼성SDS 사옥 전경

삼성SDS(사장 황성우)는 지난해 국내외에서 발생한 보안 이슈와 현장 사례를 분석해 '2021년 사이버보안 7대 트렌드'를 선정해 발표했다.

7대 트렌드로는 △비대면 환경을 노린 위협 증가 △랜섬웨어 고도화 △AI를 활용한 해킹 지능화 △산업설비에 대한 위협 본격화 △개인정보 등 민감 데이터 보호 중요성 증대 △클라우드 대상 공격 증가 △의료분야 집중 공격이 꼽혔다.

전세계 사무실의 업무 및 공장 시스템 중단 사고(IT/OT망)



회사 사무실 문에 붙여진 안내문

Norsk Hydro(세계 최대 알루미늄 생산 제조사)

공격자로부터 온 메일 내용

“

당신 회사의 보안 시스템에는 심각한 결함이 있다. 이 결함은 몇몇 초보자들에 의해 발생된 것이 아닌 보안을 위반한 사람들에 의해 악용되었다는 것에 감사해야 한다. 이들이 실수 또는 재미 삼아 당신들의 데이터에 피해를 준 것이다.

파일들은 강력한 군사용 알고리즘인 RSA4096 및 AES256으로 암호화 되었고, 우리들의 특별한 복호화 키 없이 데이터를 복구하는 것은 불가능하다. 만약 Photorec, RannohDecryptor 등과 같은 소프트웨어를 통해 복구를 시도하면 데이터가 손상되어 돌이킬 수 없게 된다.

IT 환경 변화를 이용한 공격 사례

미국의 에너지 보급과 정유 산업에 핵심 역할을 하는 인프라(폐쇄망)

Issue

5 월 7 일 Colonial Pipeline은 이것이 사이버 보안 공격의 희생자임을 알게 되었고 그 이후이 사건이 랜섬웨어와 관련이 있음을 확인했습니다. FBI는 DarkSide, ransomware-as-a-service 그룹이 관련되어 있음을 확인했습니다.

Impact

이러한 사건으로 인해 Colonial Pipeline은 5,500 마일의 파이프 라인 운영을 모두 중단했습니다. Colonial은 위협을 억제하기 위해 사전에 특정 시스템을 오프라인으로 전환했습니다. 또한 손상된 시스템을 치료하고 복원하기 위해 작업하는 동안 일부 IT 인프라를 종료합니다. 파이프 라인의 장기적인 폐쇄는 여름철 운전 성수기를 앞두고 가솔린 펌프의 가격이 급등하게 하여 미국 소비자와 경제에 타격을 줄 수 있습니다.

Targets

공격 자체에 대한 많은 정보가 공개되지 않았습니다. DarkSide 그룹은 웹 사이트에서 공격 한 다른 조직을 나열했지만 이 공격이 더 큰 캠페인의 일부라는 증거는 없습니다. DarkSide는 동기가 정치적이지 본질적으로 금전적이라고 말했습니다.

Insights

Colonial Pipeline은 이벤트가 진행됨에 따라 정보를 추가하는 보도 자료를 발표했습니다. CISA (Cybersecurity and Infrastructure Security Agency)와 FBI (Federal Bureau of Investigation)는 랜섬웨어 공격으로 인한 비즈니스 중단을 방지하기위한 권장 사항을 나열하는 공동 자문을 발표했습니다.

Recommendation

우리는 고객이 위협 신호 및 블로그에 설명 된대로 Fortinet 제품을 보호 수준으로 업데이트 할 것을 강력히 촉구합니다. 고객은 또한 공동 자문을 검토하고 권장 사항에 대한 조치를 취해야합니다.

계속해서 업데이트를 확인하십시오

FortiGuard Labs는 '위협 신호 리포트' 와 초기 분석 및 포티넷 제품 보호 기능에 대해 블로그를 발표

5월 6일
2021

소식통은 블룸버그 뉴스에 해커들이 몸값을 요구하기 전에 목요일 콜로니얼 네트워크에서 거의 100GB의 데이터를 훔쳤다고 전했습니다.

5월 7일
2021

Colonial Pipeline은 랜섬웨어 사이버 공격으로 인해 전체 파이프 라인 네트워크를 차단했습니다. 그 당시 배후는 알려지지 않았지만 "DarkSide"라는 위협 행위자의 정보가 등장하기 시작했습니다.

5월 10일
2021

May 11
2021

ICS 시스템이 아닌 정보 시스템 만 영향을 받은 것으로 보입니다 Colonial은 몸값을 지불했을 수 있다는 보고 이후 시스템을 온라인 상태로 만들기 시작했습니다.

WEBINAR

재택근무 가이드라인

Genians | FORTINET

재택근무 보안을 위해 무엇을 해야 하는가?

규제 준수 시행 및 보안 인식 훈련 마련 필요

- 국가정보보안 기본 지침
- 전자금융감독 시행 세칙
- 재택근무 보안 가이드 라인
- 재택근무 보안 안내서

Trust

- 인증
- 비인가단말
- 암호채널
- 인터넷차단

Compliance

- 외부저장매체
- 바이러스 백신
- 필수 소프트웨어
- 최신업데이트

Visibility

VM | VM | VM
Virtual Desktop Infra

간접 접속 - 1

- 사용시 인터넷 차단
- 파일 송수신 차단
- 업무용 단말 가시성 확보

간접 접속 - 2

- 소프트웨어 취약점 관리
- 기본 접속 포트 변경
- 미인가 차단
- 업무용 단말 가시성 확보

서비스 직접 접속

- 상시 인터넷 차단
- 필수 소프트웨어 실시간 감시
- 위반시 즉시 차단

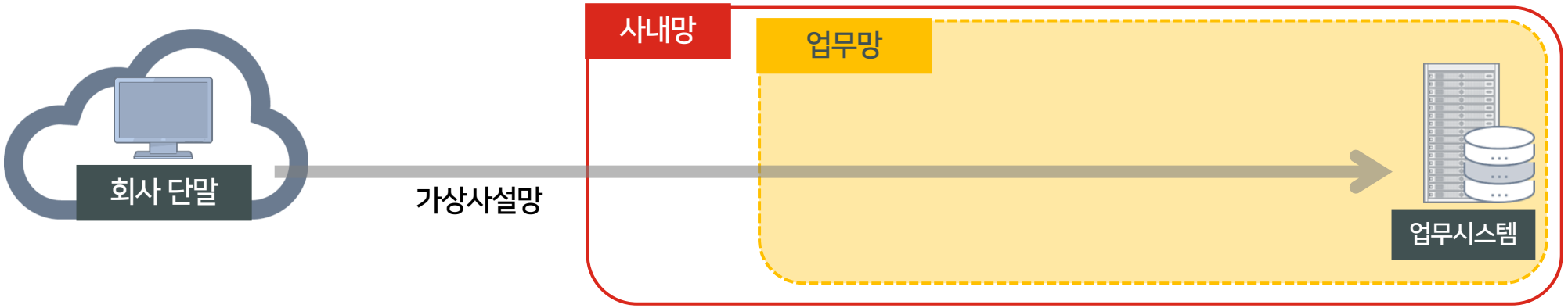
전자 금융 감독 규정 시행세칙 개정(2020.10)

보안 정책	직접 연결	간접 연결 방식
허용되는 단말기의 종류	회사 지급 단말기만 가능	개인 단말기도 가능
인터넷 차단	항상 차단	업무망 연결시 차단
백신 설치, 최신 운영체제 유지, 비밀번호 설정	사내 근무시와 동일	사내 근무시와 동일
파일 송수신	허용	차단*
단말기 설정 변경, 외부저장장치 사용	차단	허용
내부 전산자료 출력, 화면 캡쳐	차단	차단*
내부 전산자료 저장	암호화 저장	차단*

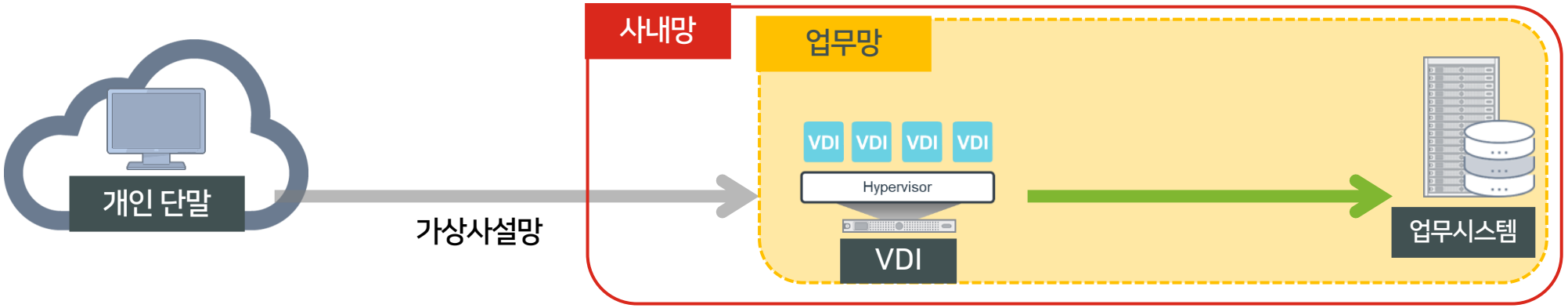
*원격 접속용 단말기가 아닌 내부 시스템에서 차단

전자 금융 감독 규정 시행 세칙 개정(2020.10)

[직접 연결 방식 예시]



[간접 연결 방식 예시]



WEBINAR

재택근무 협업 솔루션

Genians | FORTINET

어떻게 재택근무 보안을 강화할 수 있나?

누구도, 무엇도 믿을 수 없습니다.

[Pre-Connection]

Tier - 1

Home Cafe Business Trip

- 업무 접속 전 인터넷 차단
- 단말 무결성 1차 검사

Tier - 2

- VPN 외 접속 불가
- VPN 인증 시작
- 단말 인가 여부 1차 확인
- ID/PASS + OTP

USERNAME
*****
+
384629

Tier - 3

- 접속 단말 인가 여부 2차 확인
- 단말 무결성 2차 정밀 검사
- 소프트웨어 업데이트 실행

접속 성공

[Post-Connection]

업무망 접속 성공

VM VM VM
Virtual Desktop Infra

간접접속-1 간접접속-2 직접접속

- VDI, 원격 데스크톱 가시성 제공
- 접속 사용자 및 단말 가시성 제공
- 실시간 규제 준수 여부 모니터링
- 규제 위반 시 즉시 차단 수행
- 모든 감사기록

단말 무결성 검사 기준

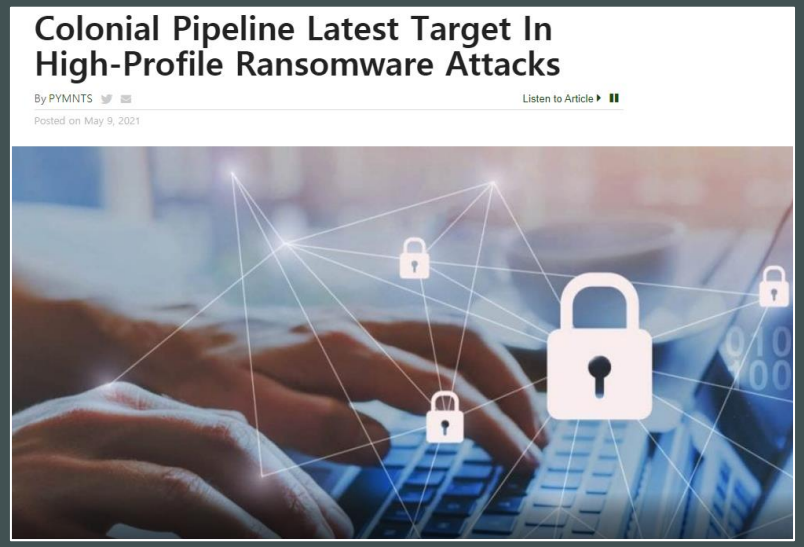
정부 규제 정책 의무 / 권고 / 가이드 라인 준수

자동 차단 **위반 교정**

강력한 인증과 정교한 검증으로 보안 강화 유지

어떻게 재택근무 보안을 강화할 수 있나?

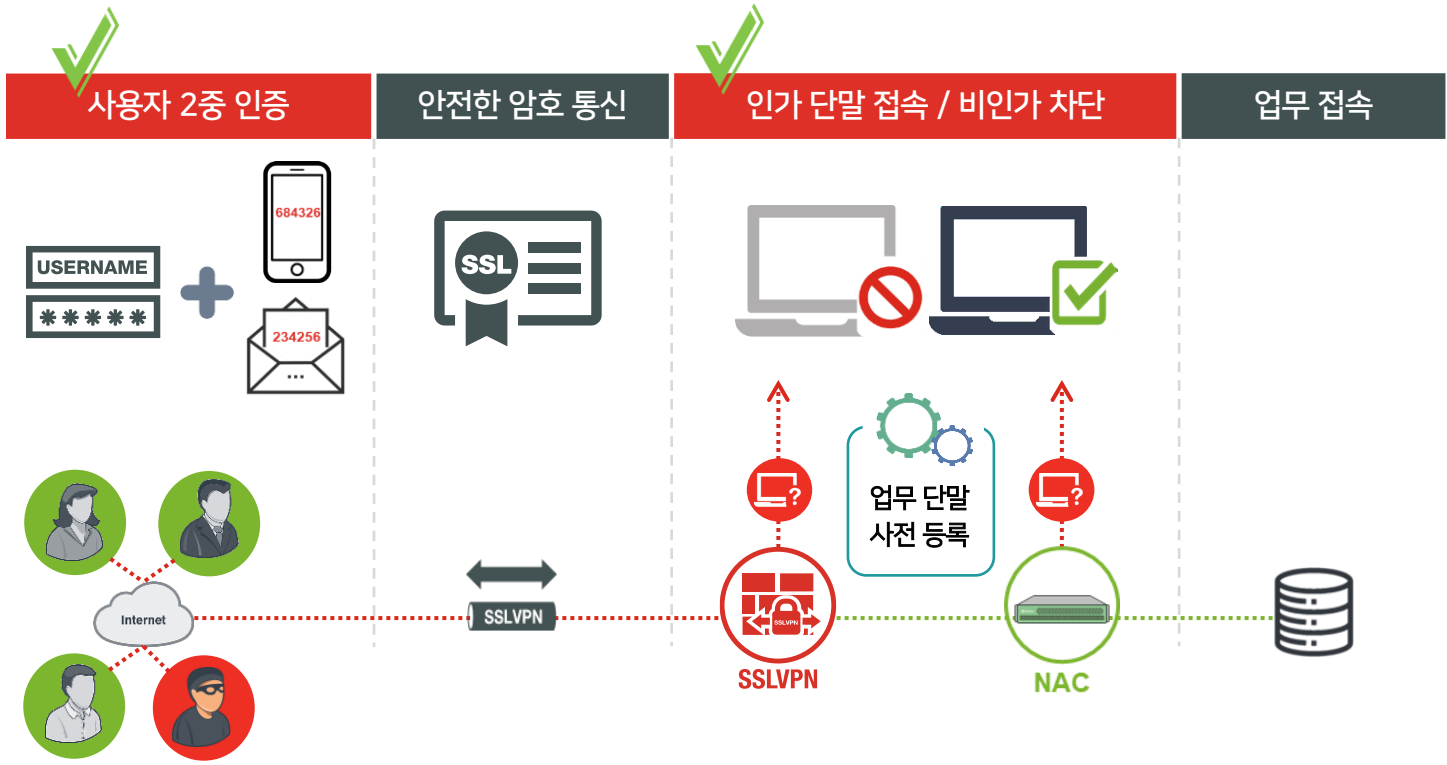
공격 사례와 원인에 따른 대응 방안



Source: www.pymnts.com/

지난 5월 미국 'Colonial Pipeline' 랜섬 공격 피해 발생

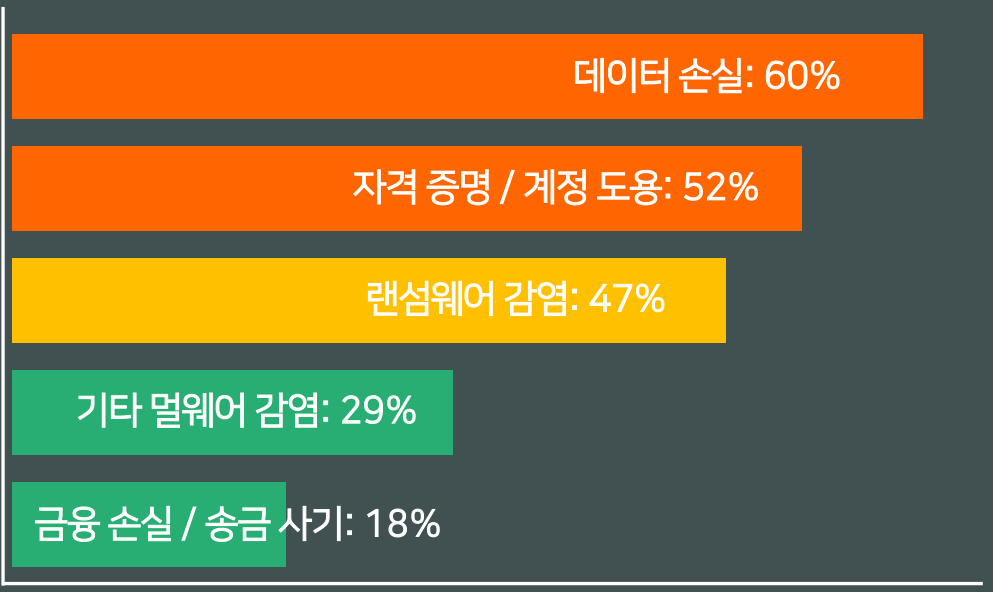
- Dark Side에 의한 공격
- 비밀번호만 사용, 다중 인증 미사용
- VPN 계정 탈취 후 외부를 통해 접속



'다중 인증' 및 철저한 '단말 검증'이 중요

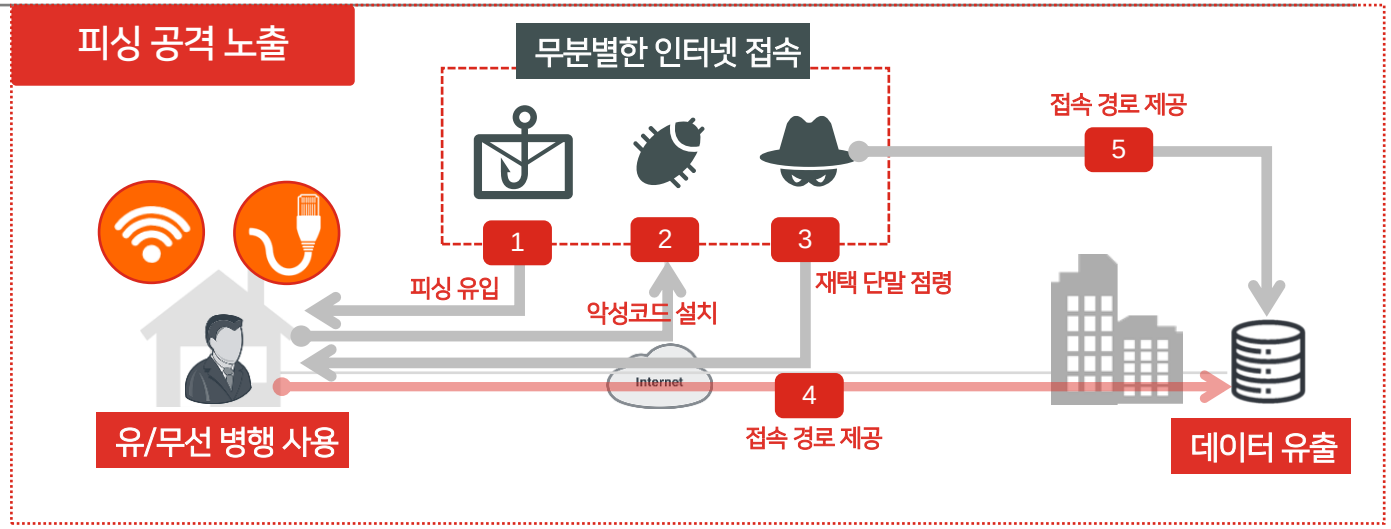
어떻게 재택근무 보안을 강화할 수 있나?

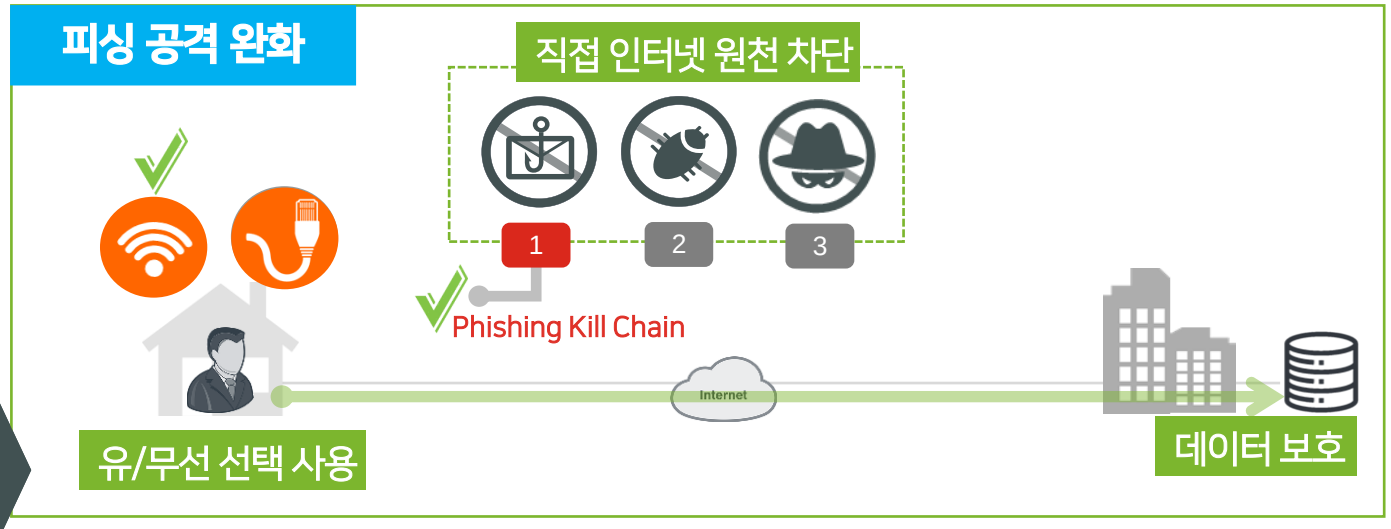
성공적인 피싱(Phishing) 공격의 영향



Source: proofpoint "2021 STATE OF PHISH" Report

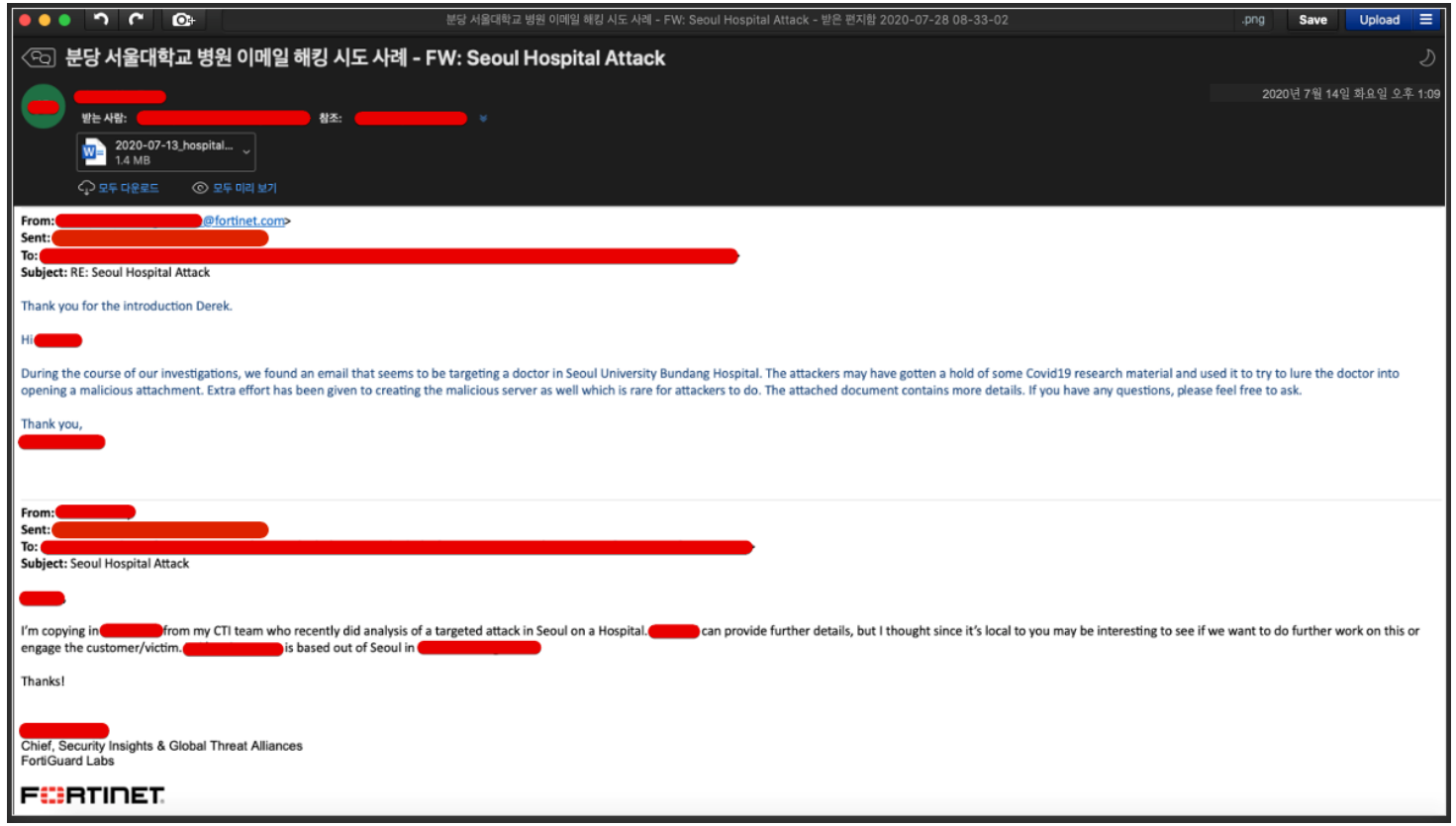
- 피싱 메일 발송 시 10명 중 1명 이상이 클릭
- 10명 중 1명 이상은 피싱 메일 클릭 열람
- 5명 중 1명은 첨부 파일 클릭





보안을 위협하는 취약점 중 사람이 가장 큰 취약점

피싱 메일 공격 사례



분당 서울대학교 병원 이메일 해킹 시도 사례 - FW: Seoul Hospital Attack

2020년 7월 14일 화요일 오후 1:09

2020-07-13_hospital...
1.4 MB

From: [redacted]@fortinet.com>
Sent: [redacted]
To: [redacted]
Subject: RE: Seoul Hospital Attack

Thank you for the introduction Derek.

Hi [redacted]

During the course of our investigations, we found an email that seems to be targeting a doctor in Seoul University Bundang Hospital. The attackers may have gotten a hold of some Covid19 research material and used it to try to lure the doctor into opening a malicious attachment. Extra effort has been given to creating the malicious server as well which is rare for attackers to do. The attached document contains more details. If you have any questions, please feel free to ask.

Thank you,
[redacted]

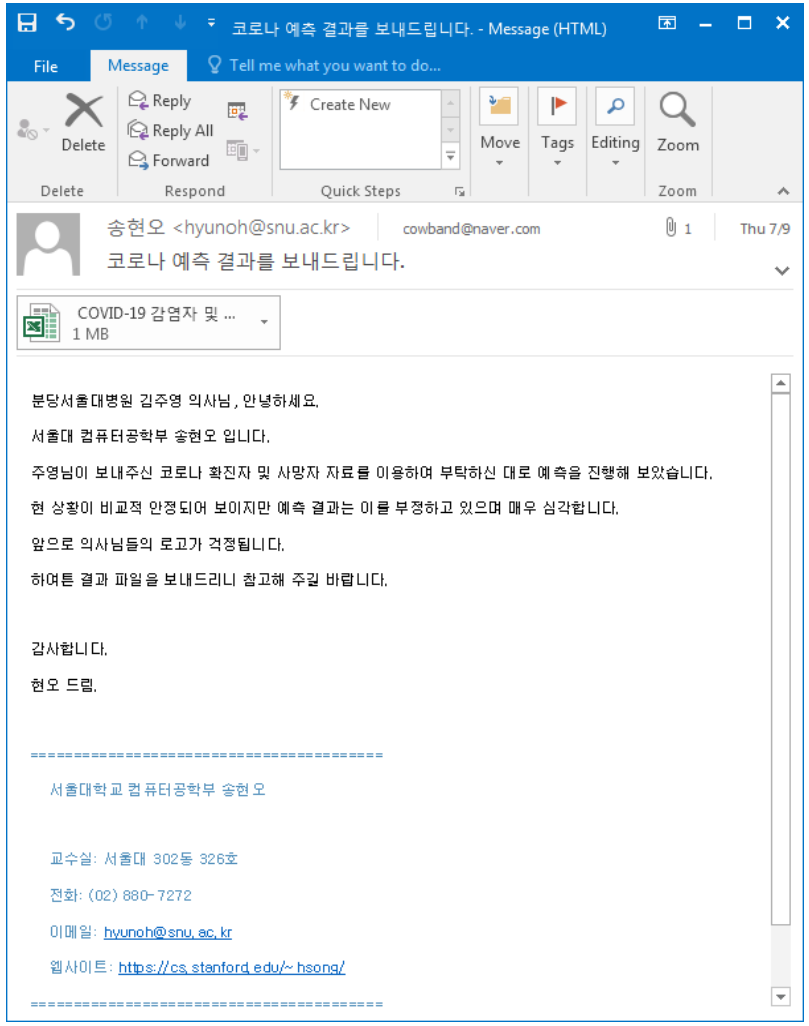
From: [redacted]
Sent: [redacted]
To: [redacted]
Subject: Seoul Hospital Attack

[redacted]

I'm copying in [redacted] from my CTI team who recently did analysis of a targeted attack in Seoul on a Hospital. [redacted] can provide further details, but I thought since it's local to you may be interesting to see if we want to do further work on this or engage the customer/victim. [redacted] is based out of Seoul in [redacted]

Thanks!

[redacted]
Chief, Security Insights & Global Threat Alliances
FortiGuard Labs



코로나 예측 결과를 보내드립니다. - Message (HTML)

File | Message | Tell me what you want to do...

Delete | Reply | Reply All | Forward | Create New | Move | Tags | Editing | Zoom

송현오 <hyunoh@snu.ac.kr> cowband@naver.com 1 Thu 7/9

코로나 예측 결과를 보내드립니다.

COVID-19 감염자 및 ...
1 MB

분당서울대병원 김주영 의사님, 안녕하세요.

서울대 컴퓨터공학부 송현오 입니다.

주영님이 보내주신 코로나 확진자 및 사망자 자료를 이용하여 부탁하신 대로 예측을 진행해 보았습니다.

현 상황이 비교적 안정되어 보이지만 예측 결과는 이를 부정하고 있으며 매우 심각합니다.

앞으로 의사님들의 로고가 걱정됩니다.

하여튼 결과 파일을 보내드리니 참고해 주길 바랍니다.

감사합니다.

현오 드림.

==========

서울대학교 컴퓨터공학부 송현오

교수실: 서울대 302동 326호

전화: (02) 880-7272

이메일: hyunoh@snu.ac.kr

웹사이트: https://cs.stanford.edu/~hsong/

==========

- COVID-19 상황을 이용한 사례

어떻게 재택근무 보안을 강화할 수 있나?

접속 전(前), 후(後), 업무 중(中) – 무결성 검사 지속

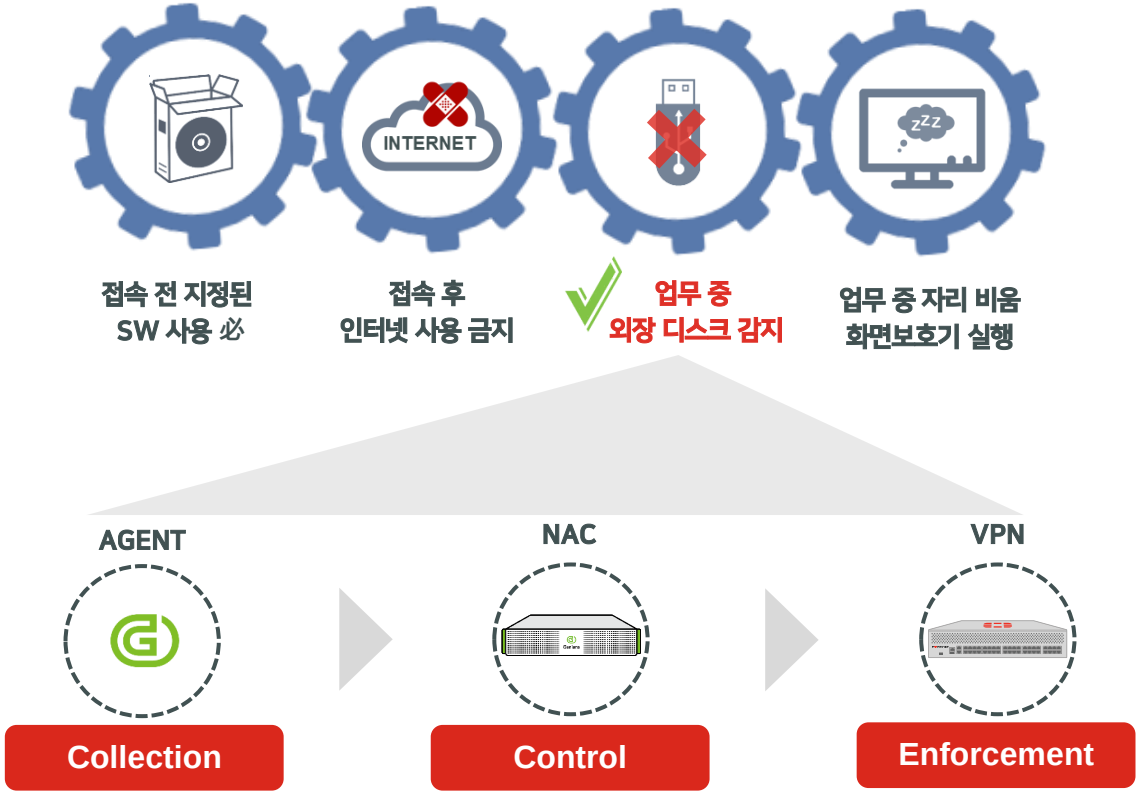
Heathrow probe after 'security files found on USB stick'

29 October 2017

Source: www.bbc.com/news/uk-41792995

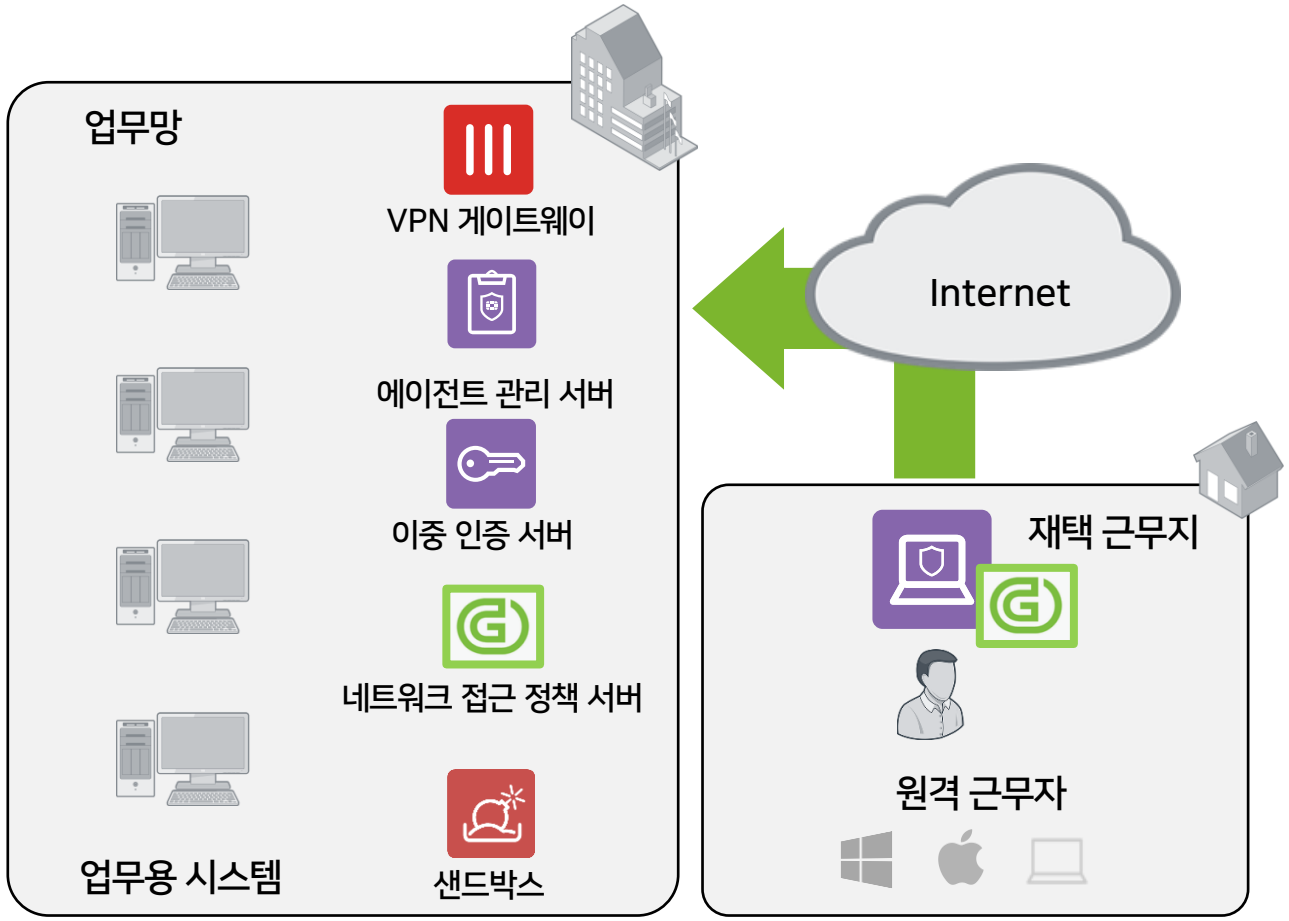
- 영국 '히드로 공항' USB 유출 사례
- 보안정보 저장된 USB 발견
- 외부 저장매체를 통해 정보 유출 사전 방지 중요

업무 도중 무결성 위반 발생시 즉시 통제 조치 시행



재택근무 시작부터 끝까지 실시간 수집, 분석, 통제

안전한 재택근무를 위한 협업 솔루션



VPN

- IPsec, SSL VPN 게이트웨이
- 재택 근무자 접근 제어
- 추가 제안 : 외부 위협으로부터 IPS / AV 보안 기능 수행

단말기 에이전트

- VPN 및 NAC 에이전트
- 관리 서버 및 네트워크 접근 정책 배포
- IPS / AV등 보안 기능 제공(옵션)

이중인증

- 등록 단말기 접속 검증
- VPN 접근 요청에 대한 사용자 인증
- OTP 토큰에 의한 **이중 인증** 수행

샌드박스

- 외부 유입 파일 멀웨어 감염 여부 검사
- ATP 공격 등 제로데이 공격 탐지/방어

WEBINAR

요약

위협 요소별 협업 솔루션 지원범위

주요 고려 사항

- 재택과 기업간 안전한 연결
- 원격접속 사용자에 대한 인증
- 인터넷 접근 제어
- 외부 위협에 대한 대비
- 단말기 검증 미약

협업 솔루션

- VPN
- 이중인증
- 단말기 에이전트
- 네트워크 접근제어
- 샌드박스(옵션, 악성코드 멀웨어 검출)

마무리

피할 수 없는 재택 근무

- 보안 정책의 사각지대
- 무분별한 웹서핑
- 불필요한 소프트웨어 설치

막아야할 외부 위협

- 지능적인 피싱 메일 공격 증가
- 랜섬웨어 공격 증가
- 계정 유출 사고 증가

지켜야할 내부 자산

- 기업의 생산성 저하 방지
- 기업 평판 저하 발생 방지
- 내부 기밀 유출 방지

안전한 재택근무로 가는 길...!

강력한 인증

- ID / PASSWORD + OTP 인증
- 인가 단말 식별

정확한 검사

- 100가지 이상의 점검 정책 설정
- 하드웨어/소프트웨어 식별 및 가시성

확실한 통제

- VPN 접속 통제
- 사용자 단말 인터페이스 통제

WEBINAR

Thank you!

Genians | FORTINET