# Smart Working ed emergenza: rischi, minacce e raccomandazioni

## Pandemia e rischio cyber

COVID-19 è una malattia respiratoria causata da un nuovo coronavirus, identificato per la prima volta alla fine del 2019[1]. L'attuale pandemia determina impatti dirompenti su ogni aspetto della nostra vita quotidiana, mettendo in discussione quelli che fino a ieri erano considerati pilastri fondamentali dal punto di vista economico, sociale, politico e di salute pubblica.

Uno dei capisaldi della strategia di contrasto e contenimento del contagio è il cosiddetto **distanziamento sociale**[2], ovvero un insieme di misure– peraltro adottate da un numero sempre crescente di nazioni in tutto il mondo – finalizzate a ridurre drasticamente la probabilità di contatto tra le persone. L'applicazione sempre più stringente di questa politica di controllo dell'infezione ha determinato, ormai da diverse settimane, una condizione di *lockdown* progressivo dei luoghi fisici tradizionalmente e naturalmente deputati alla socialità: scuole, luoghi di lavoro legati ad attività considerate non essenziali, negozi, centri commerciali, spazi adibiti a ospitare eventi di massa quali cinema, teatri e stadi. I voli sono quasi tutti cancellati e le città sono vuote. Altre misure adottate comprendono la quarantena, l'autoisolamento e il cordone sanitario. Ad oggi (fine marzo 2020) si stima che oltre 2 miliardi di persone in tutto il pianeta siano costrette a vivere in un regime di distanziamento sociale, isolate all'interno delle proprie abitazioni e private, quanto più possibile, di contatti fisici con altre persone.

Appare evidente che, nonostante la riduzione ai minimi termini del campo di azione individuale nel dominio fisico della realtà, i bisogni umani non possano essere similmente compressi: ne consegue che **la nostra dipendenza dalla tecnologia digitale aumenta** esponenzialmente. Le infrastrutture digitali e Internet (in senso lato) diventano l'elemento principale che abilita l'interazione umana nelle modalità in cui comunichiamo, ci aiutiamo, studiamo o lavoriamo. Il bisogno che i servizi essenziali continuino a funzionare senza interruzioni non è mai stato più urgente: la situazione globale è senza precedenti e, di fatto, ci si trova in una condizione di verifica sul campo dei limiti e delle capacità di comunicare, capire il contesto e reagire in modo appropriato. Proprio durante una crisi di queste dimensioni e portata è fondamentale garantire il corretto funzionamento dell'infrastruttura digitale nel suo complesso[3].

In un contesto come quello attuale, senza precedenti e caratterizzato dai tratti della totale emergenza, un attacco cyber in grado di privare le organizzazioni pubbliche e private e le famiglie dell'accesso ai propri dispositivi, ai propri dati o all'infrastruttura digitale sarebbe devastante. Nello **scenario peggiore**, attacchi cyber di grande portata potrebbero disconnettere intere comunità o città, interrompendo, per esempio, la normale operatività dei servizi erogati dal sistema sanitario o da altri operatori essenziali. Una dipendenza maggiore dall'infrastruttura digitale aumenta anche il costo complessivo di un suo eventuale malfunzionamento e la pandemia in corso ha già ottenuto l'effetto di veder aumentare gli attacchi cyber: le campagne di *phishing* sono in preoccupante aumento[4], applicazioni malevole promettono di tracciare le dinamiche di diffusione del virus (in realtà sono *trojan*[5]), i *social media* sono oggetto di attacchi differenziati (*fake news* e attività di *Social Engineering[6]* finalizzate a manipolare consensi, influenzare opinioni o destabilizzare le comunicazioni) e gli ospedali e le infrastrutture sanitare sono attaccate in vari

modi (*ransomware*, attacchi DDoS).

Nel presente articolo il focus è relativo agli aspetti di sicurezza logica delle infrastrutture e delle tecnologie digitali coinvolte nell'applicazione dei comuni scenari di Smart Working. Gli elementi attinenti al fattore umano e alla sfera comportamentale (*Security Awareness*[7], *Social Engineering*, le buone pratiche di *Cyber Hygiene*[8], etc) sono disseminati e distribuiti all'interno delle misure consigliate sotto forma di Raccomandazioni.

## Smart Working

Il lavoro da casa – più in generale, da remoto – è una delle caratteristiche intrinseche all'infrastruttura digitale: finora è stato utilizzato da un numero ristretto di organizzazioni all'interno delle quali, tipicamente, tale opzione veniva offerta a una quota della popolazione aziendale. La realtà che stiamo vivendo ha accelerato drammaticamente questa dinamica, estendendo la platea del lavoro da remoto a una parte significativa della forza lavoro globale. Di fatto si tratta di un test di proporzioni giganti dettato dalle condizioni di emergenza e di incertezza, non da una pianificazione articolate secondo passaggi graduali.

Il **cambiamento** così repentino, *ex abrupto*, di una consuetudine plurisecolare (i luoghi di lavoro sono da sempre un contesto materiale di socialità e relazioni interpersonali) potrà essere valutato in futuro nella sua portata e nei relativi impatti (ad esempio di natura psicologica, economica o sociale), ma **nell'immediato pone concretamente determinati rischi cyber** che richiedono misure tecniche e organizzative adeguate unitamente a comportamenti corretti.

Nel contesto del quadro normativo di riferimento italiano il *"lavoro agile (o Smart Working) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi,*

*cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività. Come indicato nel DPCM dell'11 marzo 2020,* ***si raccomanda venga attuato il massimo utilizzo, da parte delle imprese, di modalità di lavoro agile per le attività che possono essere svolte al proprio domicilio o in modalità a distanza****[9]".*

## Problematiche comuni

Esistono diverse problematiche di sicurezza connesse allo Smart Working[10]:

- le persone operano da remoto – in questo caso da casa propria, sia tramite dotazioni aziendali sia tramite dispositivi di loro proprietà. Si tratta di sistemi che potrebbero essere datati, privi di *patch* di sicurezza e di protezione. Sono maggiormente esposti alle vulnerabilità semplicemente perché sono meno sicuri;
- i dati sensibili dell'organizzazione potrebbero muoversi al di fuori della rete. I dipendenti che lavorano da casa potranno salvare i dati sui propri dispositivi, dove non sono poste in essere le misure tecniche di protezione tipiche dell'organizzazione. Questa condizione espone i dati a essere oggetto di furto e *hacking*;
- le persone potrebbero accedere alle reti aziendali in maniera poco sicura. Alcune aziende predispongono accessi remoti VPN per i quali è opportuno l'utilizzo di un apposito software client di connessione. Anche se può essere faticoso far installare tale client su un dispositivo proprio da parte di una persona con poca competenza tecnico informatica, è molto peggio non prevedere l'utilizzo di una VPN;
- le persone potrebbero essere costrette a utilizzare strumenti di lavoro e videoconferenza relativamente

nuovi e poco familiare come Zoom[11] (per esempio) al fine di sostituire gli incontri faccia a faccia. A volte il *set up* frettoloso di questi sistemi può creare problematiche di sicurezza;
- il caos generale derivato dal dover agire improvvisamente in modo diverso è di per se una condizione di potenziale attacco. Azioni quali il *Business Email Compromise[12]*, quando cioè si riceve un'e-mail fasulla da una figura apicale della propria organizzazione che ci chiede di effettuare un trasferimento di denaro, tenderà ad avere maggior successo nel momento stesso in cui non abbiamo più la possibilità di verificare fisicamente la validità stessa del messaggio – magari andando a parlare di persona con il presunto mittente. Quando si agisce in uno stato di distrazione diffusa e generalizzata il livello di attenzione e di difesa tende ad abbassarsi e molte cose rischiano di essere fatte in maniera diversa da solito.

## Obiettivi di sicurezza

Gli obiettivi di sicurezza per lo Smart Working sono:

- **Riservatezza**: assicurare che le comunicazioni tramite accesso remoto e i dati degli utenti interessati non possano essere acceduti da entità non autorizzate;
- **Integrità**: rilevare qualsiasi cambiamento intenzionale o non intenzionale alle comunicazioni che avvengono durante il transito dei dati;
- **Disponibilità**: assicurare che gli utenti possano accedere alle risorse tramite accesso remoto ogni volta che ne hanno bisogno.

Al fine di raggiungere tali obiettivi è necessario che tutte le componenti tecnologiche coinvolte all'interno della filiera (dispositivi client, server di accesso remoto, server interni all'organizzazione acceduti tramite l'accesso remoto) siano opportunamente messe in sicurezza contro un insieme di minacce

cyber. Uno dei problemi principali è dovuto al fatto che le tecnologie di accesso remoto sono per propria natura maggiormente esposte a minacce esterne nei confronti delle tecnologie che vengono normalmente accedute e utilizzate dall'interno dell'organizzazione: è per questo che è necessario, già in fase di progettazione e design, modellizzare opportunamente le minacce cyber che sarà inevitabile affrontare.

Al fine di mitigare i rischi derivanti da tali minacce, sarà necessario identificare le risorse di interesse, le minacce più probabili, le vulnerabilità e i controlli di sicurezza applicabili a tali risorse, quindi quantificare la probabilità di buon esito di un attacco con i relativi impatti analizzando, infine, l'informazione per determinare dove i controlli di sicurezza devono essere migliorati o creati *ex novo*.

La modellizzazione delle minacce permette di definire i requisiti di sicurezza e progettare di conseguenza le soluzioni tecnologiche in grado di incorporare i controlli di sicurezza capaci di soddisfare tali requisiti.

# Modelli di minaccia

## Mancanza di controlli della sicurezza fisica

I dispositivi tramite cui il dipendente può connettersi alle risorse dell'organizzazione sono utilizzati in una estrema varietà di luoghi tutti al di fuori del perimetro di controllo dell'organizzazione: casa propria, hotel, etc. La natura mobile di questi dispositivi ne rende più semplice il furto e lo smarrimento, aumentando proporzionalmente il rischio di compromissione dei dati ospitati all'interno di tali dispositivi.

Il **modello di minaccia deve assumere che l'appropriazione indebita del dispositivo**, sia per cercare di estrarne dati

aziendali sia per cercare di usarlo come strumento di accesso alla rete aziendale, **si verificherà.**

## Reti insicure

Normalmente non è possibile effettuare alcun controllo sul livello di sicurezza della rete da cui il dipendente si connette quando opera in Smart Working. I sistemi di comunicazione utilizzabili comprendono reti a banda larga, ADSL e meccanismi wireless quali Wi-Fi e reti cellulari. Si tratta di sistemi di comunicazione suscettibili ad attacchi di tipo *eavesdropping*[13] che mettono a rischio di compromissione informazioni sensibili nel corso del loro transito. È anche possibile subire attacchi di tipo *Man In The Middle[14]* (MITM) finalizzati a intercettare e modificare i contenuti delle comunicazioni.

**È necessario assumere che le reti esistenti tra il dispositivo usato dal dipendente per operare in Smart Working e l'organizzazione non possono essere considerate affidabili (*trusted*).**

## Dispositivi infetti

I dispositivi – particolarmente BYOD[15] e portatili controllati da terze parti – sono spesso utilizzati all'interno di reti estranee all'organizzazione. Un attaccante che ha accesso fisico a uno di questi dispositivi può installarvi a bordo codice malevolo per raccogliere dati da esso e dalle reti e dai sistemi con cui interagisce. Se un dispositivo client è infetto da malware, tale malware potrebbe diffondersi all'interno dell'organizzazione non appena il dispositivo client si connetta alla rete dell'organizzazione.

**Le organizzazioni devono assumere che i dispositivi client prima o poi si infetteranno e devono pianificare conseguentemente i propri controlli di sicurezza.**

### Accessi esterni a risorse interne

L’accesso remoto fornisce a entità esterne un accesso diretto a risorse interne e protette, ad esempio server o applicativi aziendali. Rendere tali risorse disponibili ad accessi esterni le espone a nuove minacce cyber aumentando sensibilmente la probabilità di essere compromesse. Ogni forma di accesso remoto a risorse interne ne aumenta intrinsecamente il rischio di compromissione.

Le aziende dovrebbero bilanciare molto attentamente i benefici correlati all’accesso remoto con il potenziale impatto derivante dalla compromissione di tali risorse: ogni risorsa interna che potrà essere acceduta da remoto dovrà essere sottoposta ad attività di *hardening[16]* e di applicazione di configurazioni di sicurezza, limitandone l’accesso allo stretto necessario attraverso meccanismi di controllo degli accessi e filtraggio del traffico di rete (*Next Generation Firewall, Web Application Firewall*, etc).

## Raccomandazioni

Per tutelare la riservatezza, l’integrità e la disponibilità dei dati aziendali tutte le componenti di rete e delle soluzioni di accesso remoto (dispositivi client, server di accesso remoto e server acceduti da remoto) devono essere messe in sicurezza e al riparo da una varietà di minacce.

Prima di progettare e successivamente realizzare una soluzione di Smart Working ogni azienda deve sviluppare un sistema che modelli le minacce cyber che insistono sulle componenti infrastrutturali di accesso remoto e sulle risorse che sono accedute tramite l’accesso remoto.

Quando si pianificano le policy e i controlli di sicurezza relativi allo Smart Working, ogni azienda deve assumere che i dispositivi client remoti saranno compromessi da agenti ostili che cercheranno di appropriarsi dei dati in essi contenuti

oppure cercheranno di usare i dispositivi compromessi per ottenere accessi apparentemente legittimi alla rete aziendale.

Le organizzazioni devono:

- pianificare la sicurezza del proprio accesso remoto dando per assodato che le reti attraversate dal dispositivo client del dipendente in Smart Working e la rete dell'organizzazione stessa non possono essere fidate;
- dare per scontato che i dispositivi client dei dipendenti in Smart Working siano infettati da malware, predisponendo di conseguenza i relativi controlli di sicurezza;
- cercare di posizionare le infrastrutture di accesso remoto sul perimetro della propria rete, tenendo in considerazione fattori quali le prestazioni richieste, la capacità di analisi del traffico e la gestione del NAT;
- implementare meccanismi di autenticazione forte per validare l'identità del lavoratore remoto. Se possibile, sarebbe opportuno implementare meccanismi di mutua autenticazione;
- pianificare con attenzione le modalità di gestione e manutenzione dei client software per l'accesso remoto, ponendo attenzione che queste attività operative avvengano in maniera sicura, cifrando le comunicazioni di rete e applicando la mutua autenticazione tra gli *endpoint*;
- trarre vantaggio dalla capacità di gestione centralizzata ove applicabile. In ogni caso molti dispositivi potrebbero dover essere messi in sicurezza tramite configurazioni manuali ed è opportuno fornire guide tecniche agli amministratori dei dispositivi responsabili della sicurezza degli stessi;
- proteggere la riservatezza e l'integrità di qualsiasi informazione sensibile che possa attraversare reti non

*trusted* tramite l'utilizzo della crittografia;

- mettere in sicurezza i dispositivi client devono mantenendo nel tempo un adeguato livello di protezione. Se possibile, i dispositivi client dei lavoratori remoti dovrebbero avere lo stesso livello di sicurezza dei dispositivi client aziendali. Se l'utilizzo di particolari meccanismi di controllo non fosse applicabile, è opportuno predisporre tecnologie VDI o VMI per realizzare un ambiente sicuro oppure adottare soluzioni MDM per aumentare il livello di sicurezza dei dispositivi mobili;
- avere una policy per gestire informazioni sensibili, come certi tipi di proprietà intellettuale o dati classificati, e fare uso di tecnologie appropriate (crittografia, DLP, *Information Right Management*);
- definire una policy di sicurezza per lo Smart Working che individui quali sono le forme di accesso remoto consentite, quali tipologie di dispositivi sono permessie per usare le varie tipologie di accesso remoto, il tipo di accesso garantito a ogni lavoratore e come deve essere gestito il *provisioning* degli *account* e delle utenze sui sistemi;
- prendere le proprie decisioni basate sul rischio rispetto ai livelli di accesso remoto che intende concedere ai vari tipi di dispositivi client dei lavoratori remoti;
- periodicamente riesaminare le proprie policy considerando eventuali cambiamenti nei livelli di accesso e dei dispositivi remoti di connessione.

Si suggerisce l'adozione dell'insieme dei controlli applicabili contenuti all'interno del Cyber Security Framework del NIST[17] e della NIST Special Pubblication 800-53 "*Security and Privacy Controls for Federal Information Systems and Organizations*[18]" così come suggeriti all'interno della NIST Special Pubblication 800-46 "*Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD)*

*Security*[19]”:

| **Controllo NIST SP 800-53** | **NIST Cyber Security Framework Subcategory** | **Descrizione** |
|---|---|---|
| AC-2, Account Management IA-2, Identification and Authentication (Organizational Users) | PR.AC-1: Identities and credentials are managed for authorized devices and users | Il controllo riguarda la gestione di autenticazione a un fattore o multi fattore degli utenti che fanno accesso remoto, quali password, certificati digitali e/o token hardware e software di autenticazione. |
| AC-17, Remote Access | PR.AC-3: Remote access is managed | Il controllo è dedicato alla documentazione dei requisiti di accesso remoto. |
| AC-19, Access Control for Mobile Devices | PR.AC-3: Remote access is managed | Il controllo include requisiti di sicurezza e di controllo accessi dei dispositivi mobile con le relative autorizzazioni. |
| AC-20, Use of External Information Systems | ID.GV-1: Organizational information security policy is established | Il controllo coinvolge l’utilizzo di sistemi esterni quali dispositivi di proprietà personale (BYOD) e dispositivi controllati da terze parti che potrebbero processare, conservare o trasmettere i dati controllati dall’organizzazione per suo conto. |

| **Controllo NIST SP 800-53** | **NIST Cyber Security Framework Subcategory** | **Descrizione** |
|---|---|---|
| CA-9, Internal System Connections | ID.GV-1: Organizational information security policy is established | Il controllo riguarda le connessioni tra un sistema e le sue componenti, inclusi dispositivi mobili e laptop. |
| CP-9, Information System Backup | PR.IP-4: Backups of information are conducted, maintained, and tested periodically | I dispositivi dei lavoratori remoti devono avere i propri dati protetti da backup locali o remoti. |
| IA-3, Device Identification and Authentication | PR.AC-1: Identities and credentials are managed for authorized devices and users | La mutua autenticazione è raccomandata ove fattibile per verificare la legittimità di un server di accesso remoto prima di fornirgli le credenziali di autenticazione. |
| IA-11, Re-Authentication | PR.AC-1: Identities and credentials are managed for authorized devices and users | Il controllo richiede ai lavoratori remoti di autenticarsi periodicamente durante le sessioni di connessioni, ad esempio dopo 30 minuti di inattività. |
| RA-3, Risk Assessment | ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Il controllo richiede l'effettuazione di un *risk assessment* per poter selezionare il miglior metodo di accesso remoto. |

| Controllo NIST SP 800-53 | NIST Cyber Security Framework Subcategory | Descrizione |
|---|---|---|
| SC-7, Boundary Protection | PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | Il controllo riguarda la segmentazione di una rete per mantenere i componenti pubblicamente accessibili separati dalle reti interne, monitorando e controllando le comunicazioni nei punti chiave e di confine. |
| SC-8, Transmission Confidentiality and Integrity | PR.DS-2: Data-in-transit is protected | I vari metodi di accesso remoto proteggono la riservatezza e l'integrità delle trasmissioni tramite l'utilizzo della crittografia. |

## Note

[1] http://www.salute.gov.it/nuovocoronavirus

[2] https://en.wikipedia.org/wiki/Social_distancing

[3] https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

[4] https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

[5] https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

[6]

https://en.wikipedia.org/wiki/Social_engineering_(security)

[7] https://en.wikipedia.org/wiki/Security_awareness

[8] https://www.ictsecuritymagazine.com/articoli/cyber-hygiene-gli-ingredienti-di-base-per-un-programma-di-cyber-protection/

[9] https://www.lavoro.gov.it/strumenti-e-servizi/smart-working/Pagine/default.aspx

[10] https://www.schneier.com/blog/archives/2020/03/work-from-home_.html

[11] https://en.wikipedia.org/wiki/Zoom_Video_Communications

[12] https://en.wikipedia.org/wiki/Business_email_compromise

[13] https://en.wikipedia.org/wiki/Eavesdropping

[14] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[15] https://en.wikipedia.org/wiki/Bring_your_own_device

[16] https://en.wikipedia.org/wiki/Hardening_(computing)

[17] https://www.nist.gov/cyberframework

[18] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[19] https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

Articolo a cura di **Andrea Boggio**

Andrea Boggio è Security Solutions Sales Manager in Vodafone

Business, la divisione Vodafone dedicata ai servizi per le imprese, e si occupa di attività di vendita, prevendita e progettazione di soluzioni e servizi di Cyber e ICT Security. In precedenza ha lavorato presso aziende focalizzate sulla sicurezza informatica (HP, NTT Data) e di telecomunicazione (Fastweb).
Andrea lavora da oltre 15 anni nell'Information Security Arena e si occupa di diverse aree tematiche quali: Governance, Risk & Compliance, SIEM e SOC, Mobile Protection, Threat e Vulnerability Management, Network Security e Cyber Security.
Andrea detiene le certificazioni professionali ISO/IEC 27001:2013 Lead Auditor, CISA, CISM, CGEIT, CRISC, ITIL e diverse altre legate a specifici vendor di sicurezza, è membro del capitolo italiano di ISACA e ha partecipato al Cloud Security and Resilience Expert Group di ENISA.

https://www.ictsecuritymagazine.com/articoli/smart-working-ed-emergenza-rischi-minacce-e-raccomandazioni/