SMART WORKING E CYBER SECURITY

Difendere i dati aziendali e i propri dati personali

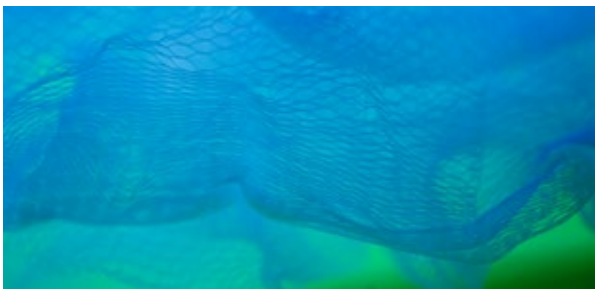
A cura di **Vincenzo Calabrò**

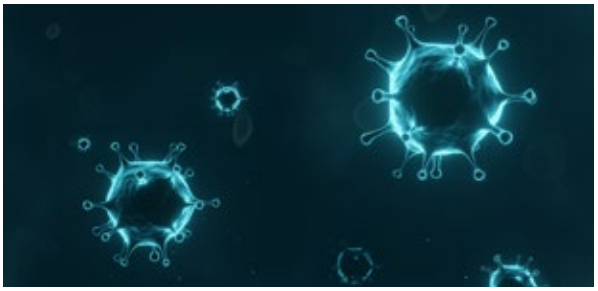
IL LAVORO AI TEMPI DELL'EMERGENZA

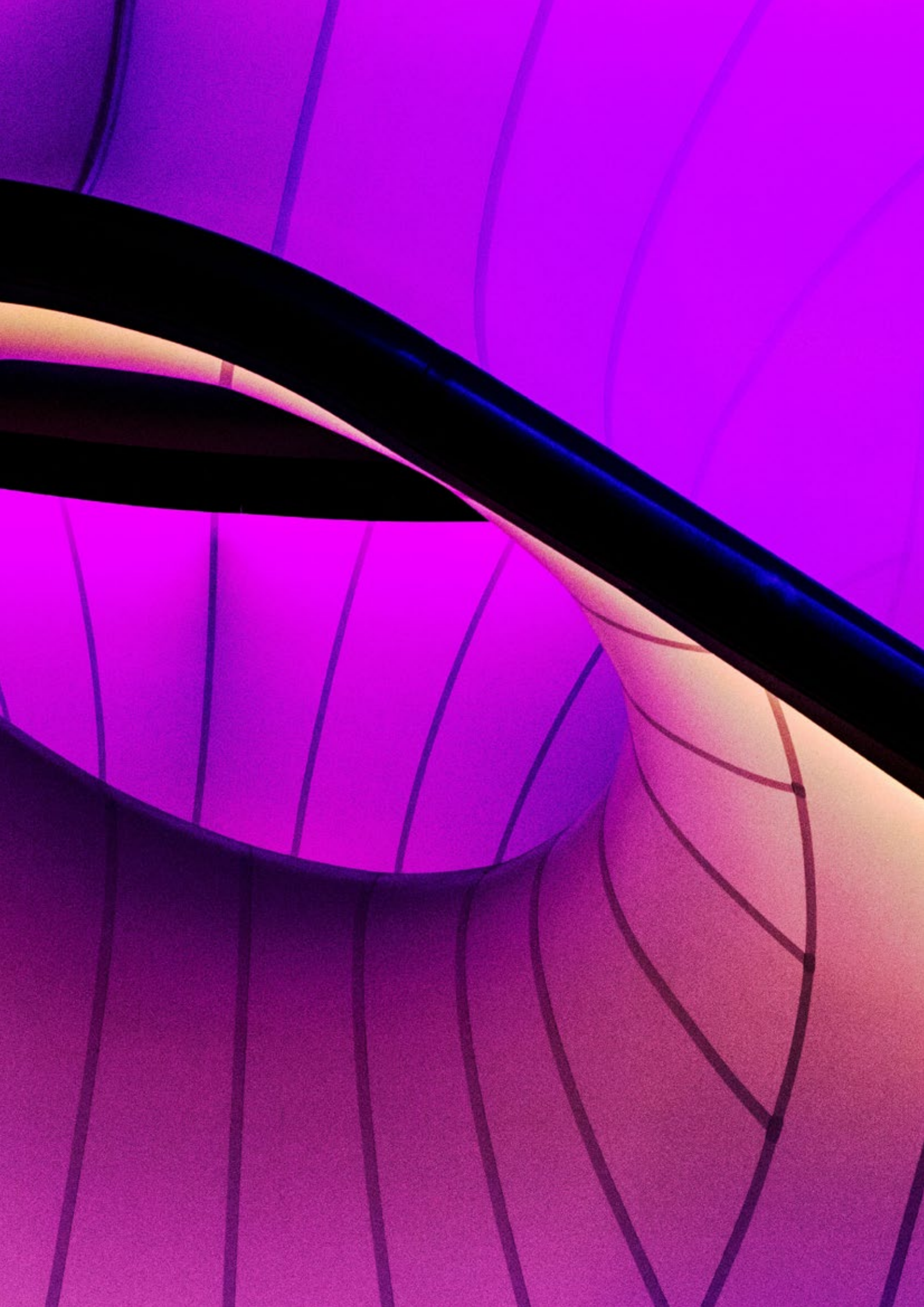
Rischi, minacce e raccomandazioni per fronteggiare il lavoro agile

A cura di **Andrea Boggio**

ICT Security MAGAZINE







Se dovessimo individuare la parola chiave di questo difficile primo trimestre 2020, smart working sarebbe sicuramente tra le favorite.

Le misure globali di distanziamento sociale, in prima linea nel fronte della prevenzione dei contagi da COVID-19, hanno fornito un poderoso impulso alla diffusione di pratiche di lavoro (e didattica) da remoto: solo in Italia il ricorso a tale modalità lavorativa - pur già esistente da diversi decenni e oggetto di una crescente diffusione, con oltre mezzo milione di persone coinvolte (dati 2019) nei più svariati settori - ha visto nei due mesi appena trascorsi un'impennata del 20% (che scende, però, al 12% nelle PMI). Istituzioni e aziende di tutto il mondo stanno tentando, con la diffusione di regole e buone pratiche condivise, di supportare tale cambiamento senza precedenti. Ma una revisione generalizzata dei protocolli di sicurezza e la formazione capillare delle persone coinvolte appaiono urgenti per scongiurare il concreto rischio che il cybercrime faccia tesoro di questa occasione per attaccare, a scopo di profitto o destabilizzazione politica, reti e sistemi pubblici, aziendali o personali (distinzione spesso vanificata dall'uso promiscuo dei dispositivi) oggi più esposti e vulnerabili che mai.

Definire e implementare buone pratiche di sicurezza informatica e Cyber hygiene, d'altronde, è necessario anche per evitare che lo smart working resti relegato a pratica emergenziale: considerati gli innegabili vantaggi in termini di benessere delle persone coinvolte e sostenibilità ambientale, infatti, questa pratica ha oggi la sua occasione per inserirsi a pieno titolo nel panorama del lavoro contemporaneo per restare con noi, anche quando - si spera presto - la pandemia sarà sotto controllo, come possibile ricaduta positiva di questi tempi difficili.

SMART WORKING E CYBER SECURITY

Difendere i dati aziendali e i propri dati personali

A cura di **Vincenzo Calabrò**

Premessa

Le restrizioni imposte in questi giorni dal Governo hanno spinto molte aziende, e la stessa Pubblica Amministrazione, a sposare velocemente il paradigma dello Smart Working generalizzato ed esteso per evitare il blocco delle attività e le relative conseguenze. La maggior parte delle soluzioni emergenziali adottate prevedono lo sfruttamento dei dispositivi e della connessione alla rete degli stessi lavoratori. Alcune organizzazione sono già pronte, poiché utilizzano da tempo strumenti di Digital Collaboration oppure soluzioni di Virtual Desktop Infrastructure (VDI), altre si sono adeguate in corsa acquisendo prodotti per il re-

mote working, anche open source, dotati di un minimo di sicurezza (Software per lo Smart Working, VPN, Autenticazione a due fattori e Strumentazione aziendale preconfigurata,) e, infine, le imprudenti si sono limitate ad abilitare i protocolli di Remote Desktop (RDP) sulle postazioni aziendali, per consentire ai propri collaboratori di collegarsi da remoto alle postazioni in ufficio, oppure sfruttano i programmi utilizzati ordinariamente per l'assistenza remota, notoriamente pieni di bug, anche per il telelavoro (a riguardo, effettuando un raffronto tra i dati rilevati dal portale Shodan. io nel mese di gennaio e di marzo del 2020, si registra un incremento del 300% del numero di hosts connessi ad Internet con i "noti" protocolli di Remote Desktop abilitati). Cerchiamo di analizzare i rischi e le soluzioni.

DEFINIZIONE E AMBITI DI APPLICAZIONE

Cosa s’intenda per “Smart Working” e in quali settori possa essere implementato con successo

SMART WORKING

Modalità di lavoro che slega la prestazione professionale dai tradizionali vincoli di spazio, tempo e strumenti deputati allo svolgimento delle attività. Diverso dal cd. telelavoro (dove la persona resta vincolata a una postazione fissa e a limiti di orario prestabiliti), si basa su principi di flessibilità e responsabilità personale, implicando una revisione della cultura organizzativa

Fonte: Osservatorio Smart Working del Politecnico di Milano

DEFINIZIONE E AMBITI DI APPLICAZIONE

Ma che cos'è lo Smart Working?

Uno studio dell'Osservatorio del Politecnico di Milano lo definisce *"una nuova filosofia manageriale fondata sulla restituzione alle persone di flessibilità e autonomia nella scelta degli spazi, degli orari e degli strumenti da utilizzare a fronte di una maggiore responsabilizzazione sui risultati"*.

Pertanto, i vantaggi connessi all'applicazione dello Smart Working comprendono anche il **telelavoro** e la **formazione a distanza** che possono essere sfruttati nel caso in cui è impossibile o complicato raggiungere la sede lavorativa. Queste ultime finalità hanno, ormai da qualche anno, parallelamente incentivato la pratica di fare affidamento sui dispositivi personali dei dipendenti per lo svolgimento delle attività lavorative. Il fenomeno ribattezzato **BYOD**, "Bring Your Own Device" (in italiano: Porta il Tuo Dispositivo), sembra, a primo acchito, la soluzione migliore perché le prestazioni dei dispositivi mobili, strumenti da cui la maggior parte delle persone non si separa mai, sono equiparabili a quelle delle postazioni di lavoro fisse, l'utente li usa con molta facilità e, inoltre, si evita la duplicazione in termini di investimento tecnologico per acquisto e manutenzione di ulteriori dispositivi e i costi relativi alla connessione alla rete.

I benefici che derivano dallo Smart Working a distanza sono oramai un dato assodato per le aziende e per i lavoratori; mentre non è chiaro a tutti, ma si può comprendere, a quali **rischi legati alla cyber security** siano esposti entrambi i soggetti.

RISCHI E PROBLEMATICHE DI SICUREZZA

Oltre a innegabili vantaggi, il lavoro da remoto presenta numerose difficoltà, anche sul fronte della cybersecurity

RISCHI E PROBLEMATICHE DI SICUREZZA NEL LAVORO DA REMOTO

Il problema ha una duplice chiave di lettura: da un lato l'azienda vorrebbe mantenere lo stesso grado di confidenzialità, integrità e affidabilità raggiunto all'interno del perimetro lavorativo; dall'altro il lavoratore mal sopporterebbe un'invasione della propria privacy o una limitazione alla libertà di pensiero.

Solitamente l'azienda, per raggiungere i propri obiettivi di business, impone ai propri *smart worker* delle soluzioni tecnologiche che consentono di estendere le policy aziendali di sicurezza informatica ai dispositivi di loro proprietà, ad esempio l'installazione dello stesso *Endpoint* aziendale, l'utilizzo della VPN per la connessione sicura alla rete aziendale, l'aggiornamento del software, fino alla configurazione di sistemi di ***Mobile device management*** per gestire i dati e le app aziendali da remoto.

Le policy per lo Smart Working spesso richiedono caratteristiche tecniche – in termini di hardware e software – che non coincidono con le proprietà del dispositivo del lavoratore.

Tutto ciò, di converso, può apparire agli occhi del proprietario del *device* come **un'intrusione nel proprio domicilio digitale**. Infatti, il dispositivo potrebbe contenere informazioni e applicazioni che l'utente non vorrebbe che venissero conosciute dall'azienda (o, più in generale, da persone non autorizzate).

POSSIBILI SOLUZIONI

A seconda del settore di attività, servono protocolli differenziati per la gestione sicura di dati e informazioni

POSSIBILI SOLUZIONI

Le potenziali **soluzioni tecniche e organizzative** scelte dalle organizzazioni sono molteplici ed eterogenee perché si adattano ai diversi modelli organizzativi e devono tenere conto delle caratteristiche accennate (confidenzialità, integrità e affidabilità; privacy e libertà di pensiero).
In questo testo sono trattate le sole questioni tecniche.

L'organizzazione che adotta soluzioni tecnologiche molto rigide tutela i propri asset e, indirettamente, anche i dati del lavoratore. D'altro canto, come è noto, la maggior parte delle moderne ed efficaci misure di prevenzione e protezione cyber prevedono il *logging* dell'attività dell'utente e del dispositivo e, pertanto, violano potenzialmente il diritto alla privacy e alla libertà di pensiero del proprietario del device fuori dal contesto lavorativo.

Viceversa, l'azienda può limitarsi a indicare ai propri dipendenti delle linee guida o delle prescrizioni da seguire, sia durante l'utilizzo personale che lavorativo, per cui il lavoratore continua a mantenere la gestione del proprio dispositivo e dei propri dati. Questa soluzione, sicuramente, tutela i diritti del lavoratore, ma consente **una certa aleatorietà e incertezza sulla *compliance*** alle politiche di sicurezza aziendali.

A tutto ciò, occorre aggiungere l'obbligo di adottare le misure tecniche conseguenti all'applicazione di diverse normative che possono riguardare: il tema della riservatezza (documenti classificati), la tutela dei dati personali (GDPR), la business continuity e il *disaster recovery* (NIS), ecc.

A parere dello scrivente non è possibile implementare lo Smart Working attraverso l'applicazione generalizzata del modello BYOD in qualsiasi contesto lavorativo: occorre innanzitutto valutare una serie di fattori che aiutano a scegliere la soluzione adeguata.

Il primo elemento discriminante è rappresentato dalle **tipologie di informazioni** che devono essere elaborate durante lo Smart Working. Se le informazioni trattate sono classificate, o richiedono un elevato livello di tutela, è necessario che il dispositivo utilizzato dal lavoratore sia conforme alle stesse proprietà delle postazioni aziendali, al fine di garantire identiche misure di sicurezza. Di conseguenza, se lo *smart working* prevede la gestione di queste tipologie di dati, è fortemente sconsigliato sfruttare apparecchiature di cui non si ha il controllo diretto da parte dell'organizzazione.

Il secondo fattore da prendere in considerazione è l'interfaccia attraverso cui il lavoratore interagisce con i sistemi informativi aziendali. Se l'utente, per l'assolvimento delle attività assegnate, utilizza servizi o applicativi interni, ciò che non sono esposti sulla rete Internet (intranet), è necessario che, prima di accedere a tali sistemi, instauri una **connessione sicura** tra il suo *device* e la rete aziendale. Ciò solitamente comporta l'installazione di software e certificati sulla postazione remota, oltre all'adozione di determinate restrizioni, per evitare il furto dei dati o la diffusione di malware. Quindi, anche in questo caso è svantaggioso utilizzare device eterogenei e senza limitazioni.

Un'altra peculiarità potrebbe essere rappresentata dalla **classificazione del *device***. Se, ad esempio, il dispositivo utilizzato dallo smart worker è condiviso - o, peggio ancora, pubblico - non si avrà contezza di chi sia l'utente dall'altra parte del terminale e, di conseguenza, l'organizzazione deve necessariamente impiegare tecnologie di autenticazione più forti rispetto a quelle utilizzate nel contesto interno.

Si potrebbero analizzare altre criticità, ma quello che si vuole evidenziare è un concetto semplice: se l'attività da svolgere in modalità Smart Working non prevede particolari restrizioni tecniche e implicazioni legali – ovvero sono state adottate soluzioni lato azienda che garantiscono il rispetto dei principi di confidenzialità, integrità e affidabilità – allora può essere adottato il modello BYOD; in caso contrario è conveniente adottare soluzioni alternative, come ad esempio **l'approccio CYOD**, *"Choose Your Own Device"* (in italiano: Scegli il Tuo Dispositivo) e il COPE, *"Corporate-Owned, Personally Enabled"* (in italiano: di Proprietà Aziendale, Abilitato all'Uso Personale).

Questi ultimi modelli risolvono molti dei problemi analizzati. In questi casi è l'azienda che si occupa dell'acquisto (COPE) o della selezione (CYOD) dei dispositivi utilizzati dai dipendenti e, soprattutto, della loro gestione; questi saranno abilitati anche all'uso personale e, di conseguenza, il lavoratore potrà decidere se utilizzarlo anche per finalità private.

CONCLUSIONI

In sintesi, lo Smart Working è sicuramente un **paradigma lavorativo positivo**, sia per l'azienda che per il lavoratore; ma, considerando che ad oggi la maggior parte delle attività si svolgono in modalità digitale, è necessario valutare le soluzioni tecniche, oltre a quelle organizzative, adottate per evitare di abbassare le misure di sicurezza oppure ampliare, in maniera indeterminata, il perimetro aziendale introducendo apparecchiature con requisiti di sicurezza sconosciuti.

Come brevemente illustrato, il modello BYOD non è compatibile con molte realtà aziendali perché l'organizzazione deve essere in grado di gestire una vastità di applicazioni, modelli e dispositivi molto differenti l'uno dall'altro, senza contare le questioni connesse alla sicurezza dei dati e alla privacy dei lavoratori.

Di conseguenza, tra le migliori soluzioni percorribili troviamo quelle in cui:

- l'Azienda amministra direttamente i dispositivi, siano essi di proprietà dell'Organizzazione o dello Smart Worker.
  Con questa opzione, oltretutto, gestisce dispositivi simili tra loro e i costi legati all'acquisto e alla personalizzazione sono recuperati in termini di gestione dell'ICT. Un ulteriore problema risolto riguarda la gestione da remoto: il dispositivo è in tutto e per tutto controllato dall'azienda quindi, in caso di furto, l'organizzazione avrà i permessi per cancellare da remoto tutti i dati contenuti sul dispositivo senza incorrere in sanzioni e senza violare la privacy dei propri dipendenti.

- L'Infrastruttura IT implementa una Zero Trusted Network (ZTN), una rete terza, sia per l'azienda che per il dipendete, che consente il collegamento dalla postazione del lavoratore alla Rete Lan aziendale solo ad un set predefinito di servizi e di dati e, inoltre, grazie all'attivazione di security policy è possibile monitorare in maniera efficace le attività eseguite da remoto attraverso questa interfaccia. Con questa soluzione si realizza una sottorete dedicata, in cui non si accede alle reti che contengono le risorse, ma si espongono le risorse in un network separato a cui gli utenti remoti possono accedere. Tutto ciò che non è dichiarato all'interno della ZTN è invisibile agli utenti.

IL LAVORO AI TEMPI DELL'EMERGENZA

Rischi, minacce e raccomandazioni per fronteggiare il lavoro agile

A cura di **Andrea Boggio**

“Garantire riservatezza, integrità e disponibilità dei dati coinvolti in pratiche di smart working impone un tempestivo aggiornamento delle prassi di cybersecurity”

PANDEMIA
E RISCHIO CYBER

Dati di contesto e misure governative per la gestione dell’emergenza

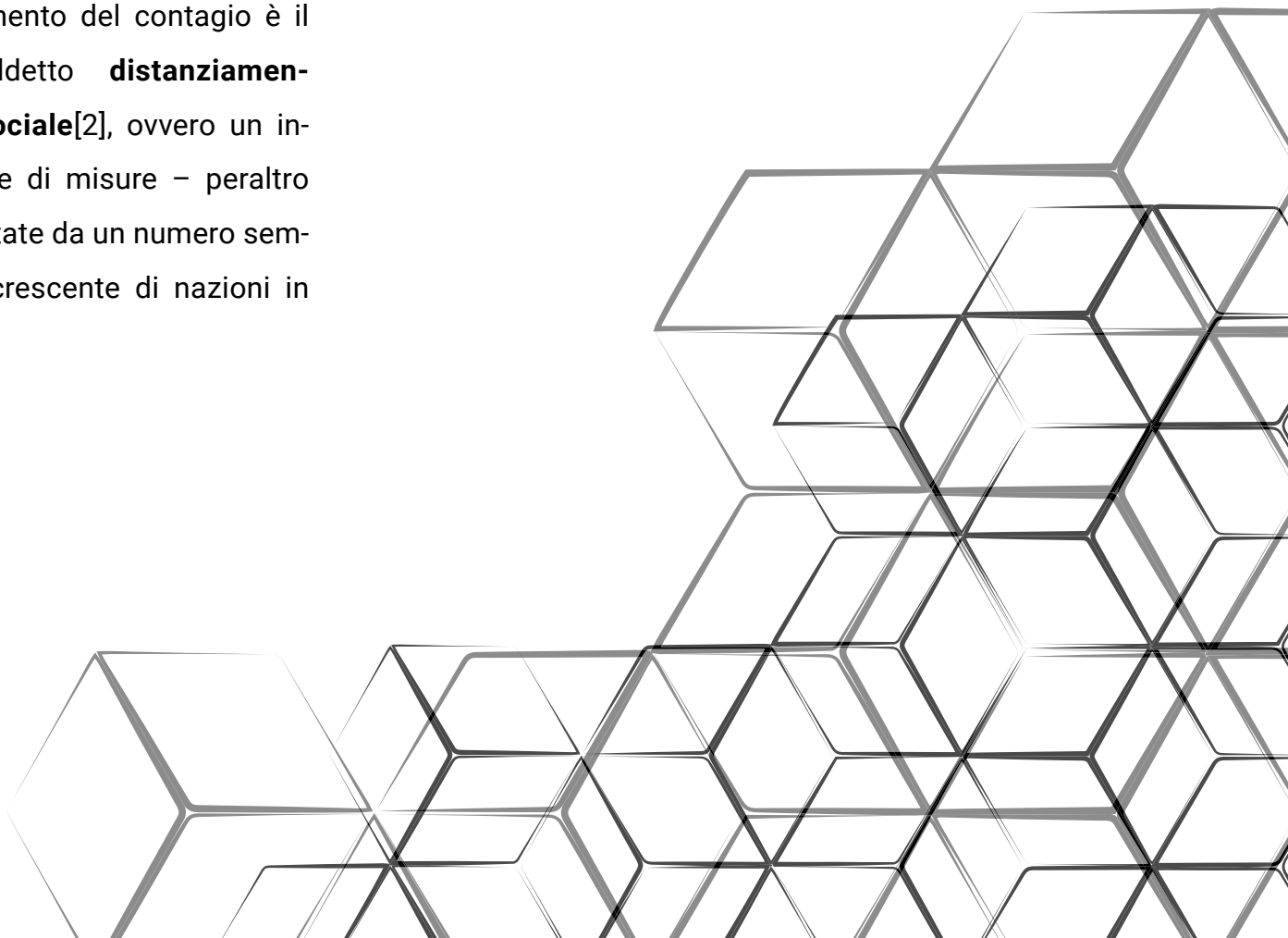
COVID-19

Un virus ad alta trasmissibilità, mai identificato prima negli esseri umani, che si diffonde principalmente tramite contatto con persone infette e causa una malattia respiratoria caratterizzata da sintomi quali tosse, febbre e - nei casi più gravi - polmonite. Nel primo trimestre del 2020 il virus è ritenuto responsabile di oltre 30 000 decessi in tutto il pianeta

Fonte: World Health Organization

La 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.

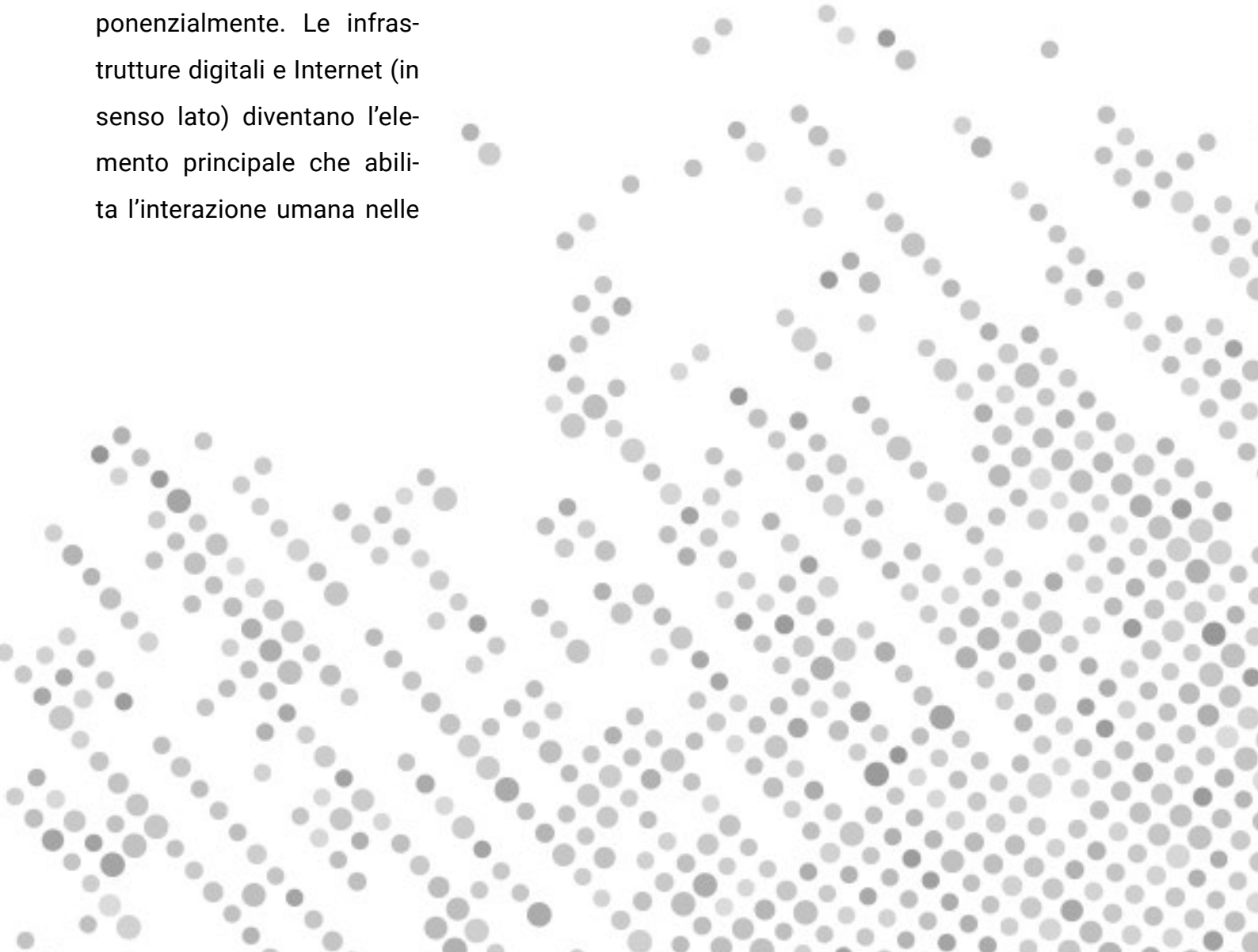
Uno dei capisaldi della strategia di contrasto e contenimento del contagio è il cosiddetto **distanziamento sociale**[2], ovvero un insieme di misure – peraltro adottate da un numero sempre crescente di nazioni in tutto il mondo – finalizzate a ridurre drasticamente la probabilità di contatto tra le 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 e spazi adibiti a ospitare eventi di massa, quali cinema, teatri e impianti sportivi. I voli sono quasi tutti cancellati e le città sono deserte. 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, dei 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 organizzazioni e persone 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 (in realtà *trojan*[5]) promettono di tracciare le dinamiche di diffusione del virus, 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 vengono attaccati 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:
UN NUOVO PARADIGMA

Definizione e impatto dei modelli di lavoro da remoto nel contesto attuale

SMART WORKING

La definizione di smart working, contenuta nella Legge n. 81/2017, pone l'accento sulla flessibilità organizzativa, sulla volontarietà delle parti che sottoscrivono l'accordo individuale e sull'utilizzo di strumentazioni che consentano di lavorare da remoto (come ad esempio: pc portatili, tablet e smartphone).

Fonte: Ministero del Lavoro e delle Politiche Sociali

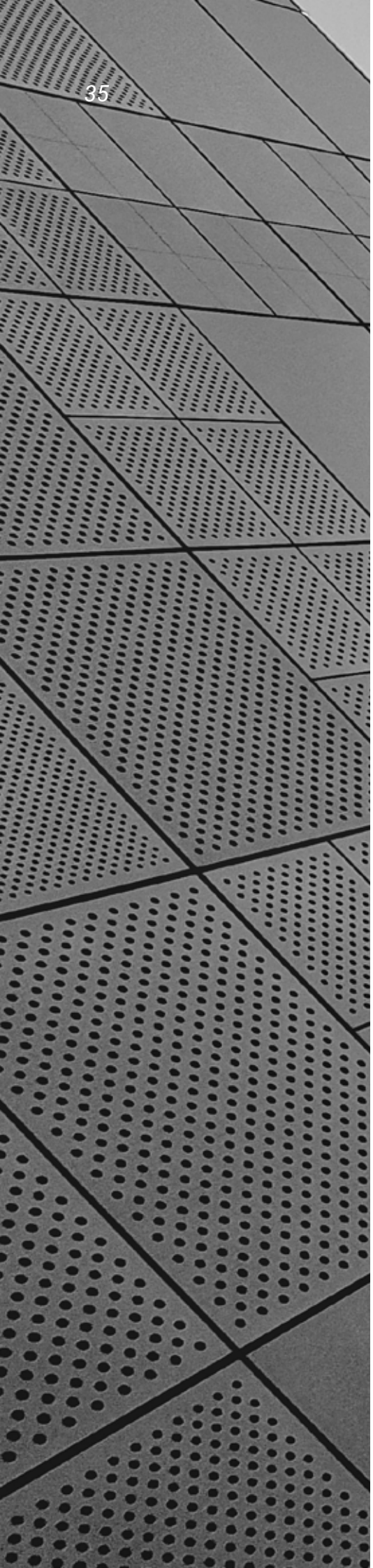
Il lavoro da casa – più in generale, da remoto – è una delle possibilità intrinseche all'infrastruttura digitale: finora è stato utilizzato da un numero ristretto di organizzazioni all'interno delle quali, tipicamente, tale opzione veniva offerta a una quota della popolazione aziendale. La realtà che 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 gigantesche proporzioni** dettato da condizioni di emergenza e di incertezza, non da una pianificazione articolata 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

Anche nel mutato scenario, restano invariate le esigenze di tutela delle informazioni e comunicazioni aziendali



ESISTONO DIVERSE PROBLEMATICHE DI SICUREZZA CONNESSE ALLO SMART WORKING[10]:

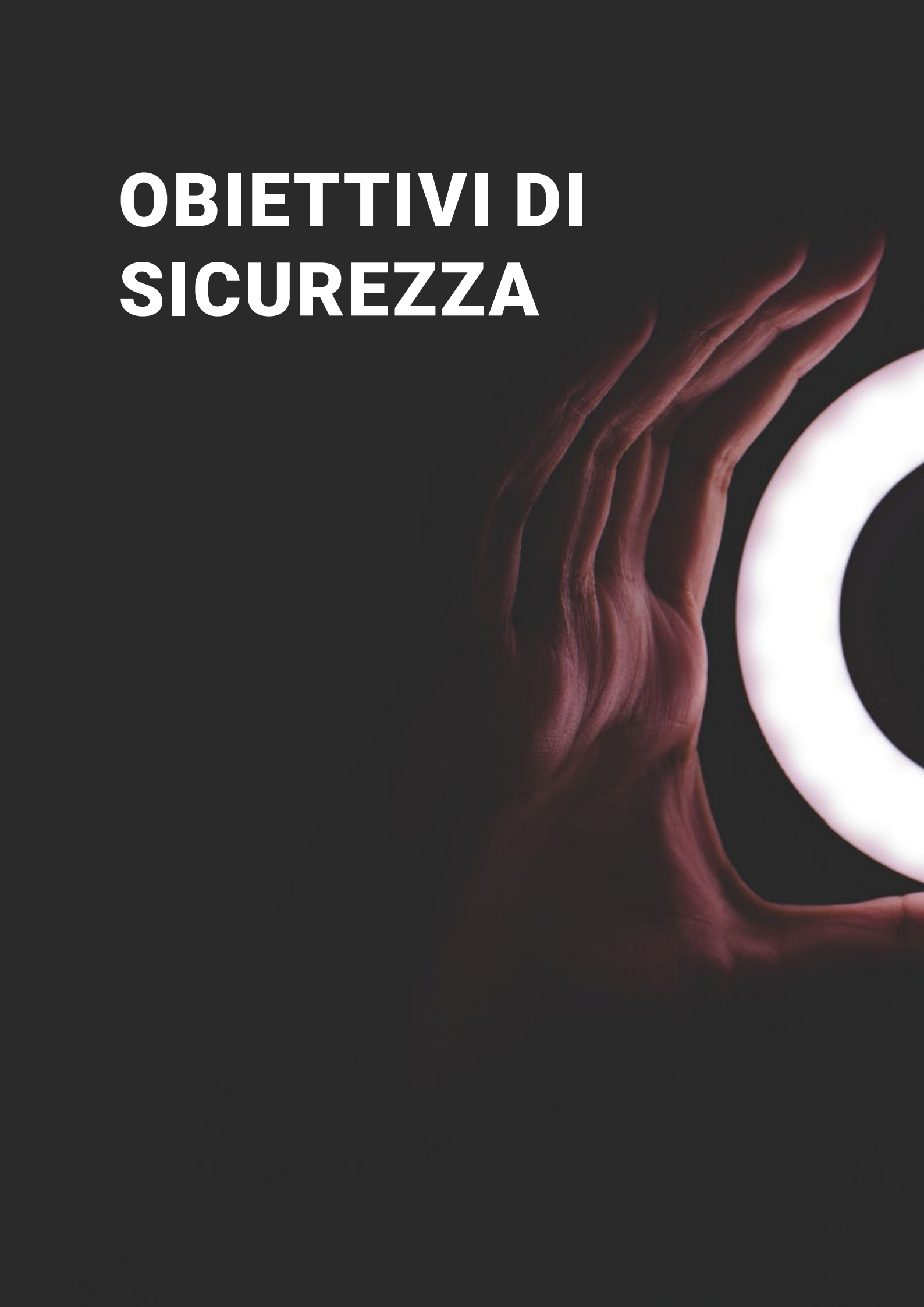
Innanzitutto, poiché le persone operano da remoto – in questo caso da casa propria - possono utilizzare sia dotazioni aziendali sia, in molti casi, dispositivi di loro proprietà: spesso si tratta di sistemi datati, privi di *patch* di sicurezza e di protezione e, quindi, maggiormente esposti alle vulnerabilità. Inoltre, i dati sensibili dell'organizzazione potrebbero muoversi al di fuori della rete aziendale (i dipendenti che lavorano da casa potranno salvare i dati sui propri dispositivi, non soggetti alle misure tecniche di protezione tipiche dell'organizzazione, così esponendoli al rischio di furti e *hacking*). Le persone potrebbero, poi, accedere alle reti aziendali in maniera poco sicura. Alcune aziende predispongono accessi remoti VPN per i quali è opportuno l'utilizzo di appositi software client di connessione: una pratica utile in termini di sicurezza, anche se può risultare complesso per i dipendenti dotati di scarse competenze informatiche.

Ancora, va gestita la diffusione di strumenti di lavoro e videoconferenza relativamente nuovi e poco familiari, come ad esempio Zoom[11], al fine di sostituire gli incontri faccia a faccia: a volte, anche il *set up* frettoloso di questi sistemi può generare problematiche di sicurezza.

In generale, il caos derivante dal dover agire improvvisamente in modo diverso integra, di per sé, una condizione di potenziale attacco. Attacchi come il *Business Email Compromise[*12], nel quale si riceve un'e-mail fasulla da qualcuno che, fingendosi una figura apicale della propria organizzazione, ci chiede di effettuare un trasferimento di denaro, tenderanno ad avere maggior successo nel momento in cui non esiste la possibilità di verificare fisicamente (magari andando a parlare di persona con il supposto mittente) la validità del messaggio.

Quando si agisce in uno stato di distrazione diffusa e generalizzata, i **livelli di attenzione e difesa** tendono ad abbassarsi e molte cose rischiano di essere fatte in modo meno accurato del solito.

OBIETTIVI DI SICUREZZA



Garantire riservatezza, integrità e disponibilità dei dati coinvolti in pratiche di smart working impone un tempestivo aggiornamento delle prassi di cybersecurity

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: per questo è necessario, sin dalle fasi di progettazione e design, prevedere un'opportuna modellizzazione delle minacce cyber che sarà inevitabile affrontare.

Al fine di mitigare i rischi sarà quindi 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 debbano essere migliorati ovvero creati ex novo.

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

MODELLI DI MINACCIA

Le principali fonti di rischio includono aspetti di sicurezza fisica, delle reti e dei devices utilizzati dai lavoratori, oltre a inevitabili problematiche di accesso

MANCANZA DI CONTROLLI DELLA SICUREZZA FISICA

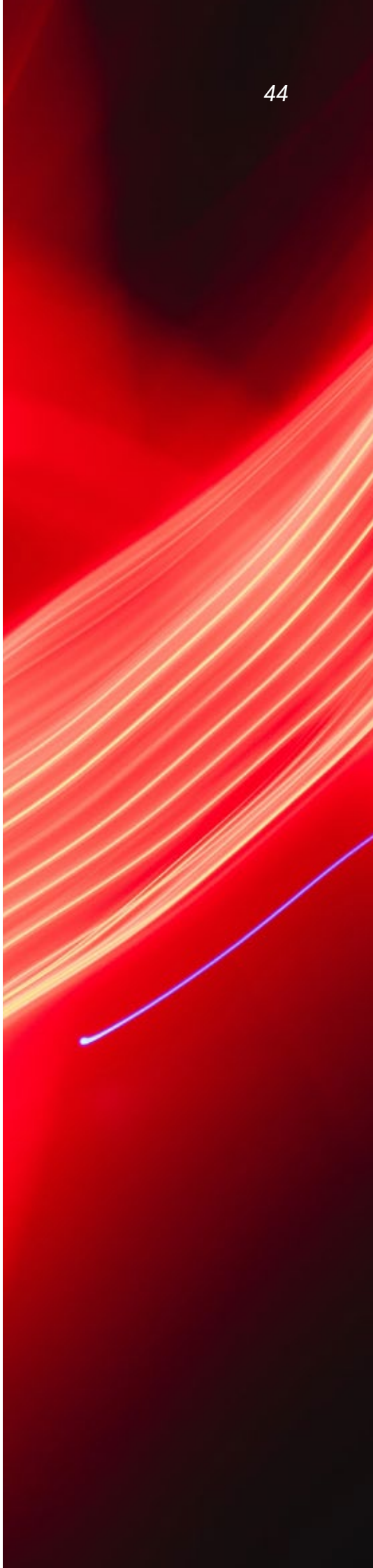
I dispositivi tramite cui il dipendente può connettersi alle risorse dell'organizzazione sono utilizzati in una estrema varietà di luoghi tutti al di fuori del perimetro di controllo dell'organizzazione: casa propria, hotel, etc. La natura mobile di questi dispositivi ne rende più semplice il furto e 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.il livello di attenzione e di difesa tende ad abbassarsi e molte cose rischiano di essere fatte in maniera diversa da solito.

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.
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.

Controllo NIST SP 800-53	NIST Cyber Security Framework Subcategory	Descrizione
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.
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