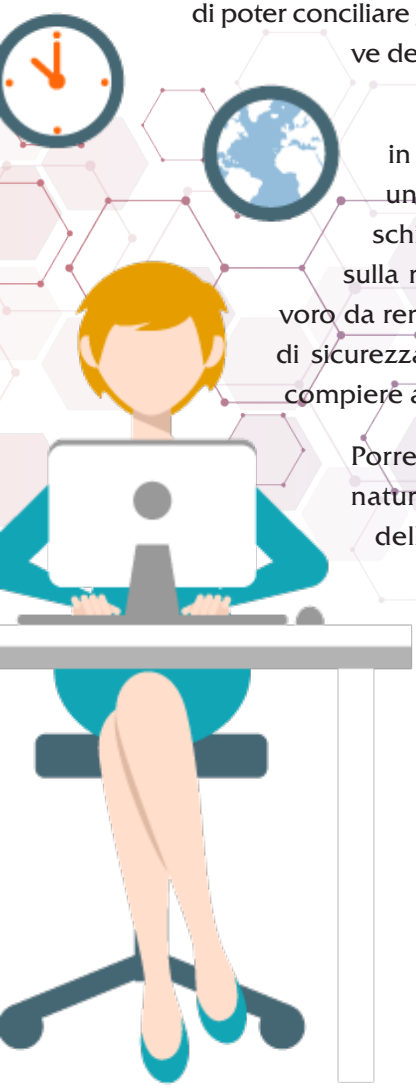
PRESIDENZA DEL CONSIGLIO DEI MINISTRI

SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA

LAVORO DA REMOTO

VADEMECUM DELLE POLICY DI SICUREZZA PER LE ORGANIZZAZIONI

Gli ultimi anni hanno visto un incremento del lavoro da remoto - con un' accelerazione dovuta all'emergenza epidemiologica da COVID-19 - quale strumento che consente ai dipendenti delle organizzazioni pubbliche e private la possibilità di lavorare a distanza utilizzando le tecnologie digitali, il che ha consentito di poter conciliare gli impegni personali con le esigenze lavorative delle organizzazioni di appartenenza.



Questa modalità lavorativa, tuttavia - in particolar modo laddove avviene senza un'adeguata formazione - aumenta anche i rischi cyber, in quanto un attaccante può fare leva sulla maggiore superficie di attacco creata dal lavoro da remoto, anche sfruttando possibili vulnerabilità di sicurezza delle soluzioni tecnologiche utilizzate per compiere attacchi informatici.

Porre in essere buone prassi in ambito ICT è il naturale prerequisito per una corretta gestione della sicurezza informatica. Risulta fondamentale, pertanto, che per contrastare il rischio cyber (ad esempio data breach, ransomware e defacement) le organizzazioni adottino precauzioni e misure di sicurezza per gli accessi da remoto a tutti gli asset lavorativi.

L'obiettivo di questo vademecum, pensato per i soggetti pubblici e privati che adottano modalità di lavoro agile, è quello di proporsi quale strumento di supporto fornendo utili raccomandazioni su come mantenere un elevato livello di allerta e implementare misure di cyber security adeguate.

6 RACCOMANDAZIONI PER IL LAVORO DA REMOTO

Uso consapevole e sicuro dei dispositivi e degli strumenti da parte dei dipendenti

Accesso sicuro alla rete dell'organizzazione

Adeguata sicurezza dei dispositivi

LE RACCOMANDAZIONI SONO RIVOLTE IN PARTICOLARE AI RESPONSABILI DELLE FUNZIONI DI SICUREZZA AZIENDALE E AGLI AMMINISTRATORI IT DELLE ORGANIZZAZIONI PUBBLICHE E PRIVATE CHE ADOTTANO MODALITÀ DI LAVORO DA REMOTO, PER SUPPORTARLI NELLE LORO ATTIVITÀ VOLTE A MITIGARE IL RISCHIO CYBER

Adeguata sicurezza della rete

Adeguata sicurezza del Cloud

Continuità operativa e risposta agli incidenti

1 USO CONSAPEVOLE E SICURO DEI DISPOSITIVI E DEGLI STRUMENTI DA PARTE DEI DIPENDENTI

- Promuovere la consapevolezza del personale sull'uso "sicuro" dei dispositivi e degli strumenti impiegati per il lavoro da remoto, anche attraverso la diffusione di linee guida che tengano conto di:
  - **indicazioni pubblicate da AgID**[1] "per aiutare i dipendenti pubblici quando lavorano da casa", che costituiscono comunque buone prassi utilizzabili da qualsiasi lavoratore;
  - **elementi relativi all'uso dei servizi informatici di supporto al lavoro agile**, con particolare riguardo a quelli erogati da fornitori di servizi in cloud, disciplinando, ad esempio, l'uso sicuro di webcam e microfoni, nonché la tipologia di attività che possono essere svolte.

1 https://www.cert-pa.it/notizie/smart-working-il-vademecum-per-lavorare-online-in-sicurezza/

ACCESSO SICURO ALLA RETE DELL'ORGANIZZAZIONE

- **Censire il personale interno ed esterno** (ad esempio consulenti) a cui è concesso lavorare da remoto, in particolare individuando gli utenti che possono accedere alle infrastrutture (amministratori) e/o ai dati (incaricati al trattamento), adottando misure di sicurezza incrementali in funzione dei livelli di accesso consentiti.
- Consentire l'accesso alla rete dell'organizzazione unicamente tramite:
  - **VPN** (Virtual Private Network) o tecnologie simili;
  - **meccanismi di autenticazione forte**, quali autenticazione a più fattori e/o one time password (OTP);
  - **dispositivi, fisici o virtuali**, messi a disposizione dall'organizzazione ovvero attraverso dispositivi personali censiti e dotati di MDM (Mobile Device Management) in modalità BYOD (Bring Your Own Device);
  - **vAPP** (virtual Application), **VDI** (Virtual Desktop Interface) personale, **RDP** (Remote Desktop Protocol) per accedere al desktop assegnato in sede.
- Attagliare le modalità di accesso alla tipologia di utenza, ad esempio:
  - **tramite vAPP con browser** per il personale non tecnico che impiega webconsole o altri servizi usufruibili via browser;
  - **tramite vAPP con RDP** alla postazione normalmente usata o alla VDI dedicata per il personale tecnico che impiega

frequentemente più sistemi per la gestione di configurazioni, incidenti, etc.;

- qualora inevitabile ed in via eccezionale, **tramite vAPP specifica** per il personale che deve poter accedere direttamente a singoli sistemi (non via browser).

- **Proteggere i servizi** raggiungibili nella rete dell'organizzazione, ad esempio tramite credenziali di accesso personali gestite con appositi sistemi sicuri.

3 ADEGUATA SICUREZZA DEI DISPOSITIVI

- Mantenere **aggiornati i dispositivi e software**, con particolare riguardo alle funzioni di sicurezza (anti-malware, etc.), nonché applicare tecniche di cd. hardening (insieme di operazioni di configurazione dei dispositivi e del software per minimizzare le vulnerabilità e i possibili impatti di un attacco).
- **Configurare le vAPP** per evitare qualsiasi accesso alle periferiche locali del dispositivo utilizzato per collegarsi (penna USB, etc.).
- **Tracciare gli accessi e le attività**, ad esempio tramite gli strumenti di virtualizzazione e di sistema, con particolare riguardo ai server e a basi dati[2] (tracciamento accesso diretto).
- Dotarsi, ove possibile e in relazione ad un'analisi del rischio, **di strumenti per la cd. Endpoint Detection and Response** (EDR).

2 L'accesso diretto alle basi dati non dovrebbe essere consentito se non in via eccezionale e con esplicita autorizzazione.

4 ADEGUATA SICUREZZA DELLA RETE

- Verificare **la corretta configurazione e l'aggiornamento** dei dispositivi fisici e virtuali perimetrali (firewall, proxy, etc.), nonché di rete (router, etc.).
- Dotarsi, ove possibile e in relazione ad un'analisi del rischio, **di sistemi di prevenzione dei DDOS** (con particolare attenzione alla protezione dei terminali delle connessioni VPN), nonché **di sistemi per l'identificazione di accessi impropri** (IDS - Intrusion Detection Systems).

5 ADEGUATA SICUREZZA DEL CLOUD

- Verificare che il fornitore di servizi cloud adotti:
  - gli adempimenti necessari in relazione agli obblighi in materia di sicurezza cibernetica e di **trattamento dei dati personali** (GDPR);
  - un **livello elevato di sicurezza informatica** in relazione agli standard nazionali ed internazionali;
  - politiche adeguate per la **tutela dei dati dell'organizzazione** (diritto all'oblio, crittografia dei dati memorizzati, etc.);
  - **protocolli cifrati e meccanismi di autenticazione forte** nell'ambito dei servizi erogati.

6 CONTINUITÀ OPERATIVA E RISPOSTA AGLI INCIDENTI

- Valutare la **congruità della banda passante** disponibile, tenendo conto dell'incremento di traffico derivante dall'accesso remoto alla rete dell'organizzazione.
- Aggiornare i piani per garantire la **continuità operativa e di servizio**, nonché i piani di **risposta agli incidenti** tenendo conto della forza lavoro in presenza.
- Valutare con particolare attenzione ogni **anomalia rilevata** in quanto potrebbe costituire un'evidenza di compromissione.
- Segnalare al **CSIRT italiano** eventuali incidenti.

www.sicurezzanazionale.gov.it

#SICUREZZANAZIONALE