



consulenti
PRIVACY^{srl}

SMART WORKING

LINEE GUIDA

PRIVACY & IT

A CURA DI

Paolo Rosetti - DPO

Massimiliano Sarto - DPO & LEAD AUDITOR

Fabio Pari - AVVOCATO

IL BOOM DELLO SMART WORKING

Una delle conseguenze più evidenti della pandemia è stata l'accelerazione incredibile dello "smart working":

2019 - **570.000 smart-workers**

2020 - **1.827.792 smart-workers**

(Fonte: Ministero del Lavoro e delle Politiche Sociali)

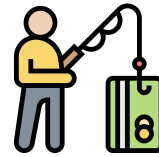
L'aumento ha inoltre generato un **+68%**
nell'utilizzo VPN (virtual private network)



...ED IL CONNESSO BOOM DEGLI ATTACCHI INFORMATICI



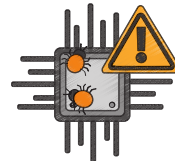
La digitalizzazione del lavoro, con una massiccia fuoriuscita dei dati dalle “porte” dell’azienda, ha inevitabilmente attratto i criminali informatici:



+ 600 % phishing



+ 715 % ransomware



+ 405 % exploit



+ 6.000 % spam

Fonte: Threat Landscape Report 2020

METTERE IN SICUREZZA IL NUOVO PERIMETRO AZIENDALE

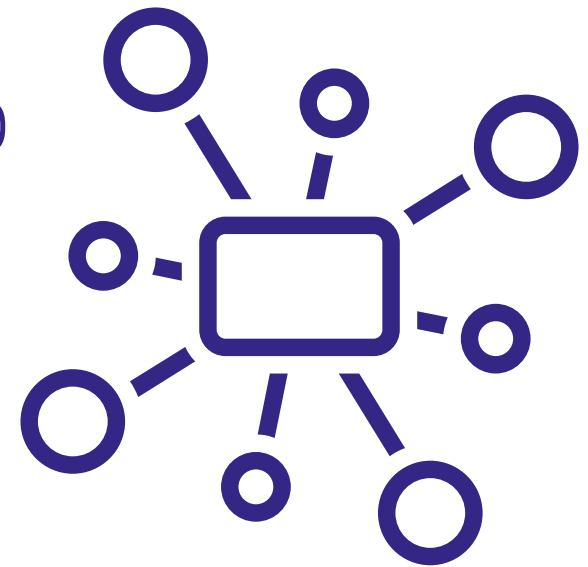
E' quindi di primaria importanza **l'individuazione del perimetro aziendale e la sua messa in sicurezza:**

- **Misure di data governance** (utilizzo sistemi di crittografia; adozione processi di cancellazione sicura del dato; mappatura dell'ubicazione del dato)
- **Misure per il controllo degli accessi** (gestione dei privilegi; procedure di autenticazione; Log Management)
- **Protezione end-point** (Antimalware; Intrusion Prevention; Patch Management)
- **Security Process** (Policy aziendali; Piano di risposta agli incidenti; Audits & VA/PT)

RESPONSABILIZZARE DIPENDENTI E COLLABORATORI

Spesso il rischio più grande arriva però da dipendenti non formati che, ignari dei rischi, adottano condotte non corrette spalancando i cancelli dell'azienda ai criminali informatici (es. apertura email sospette). Occorre prevenire mediante:

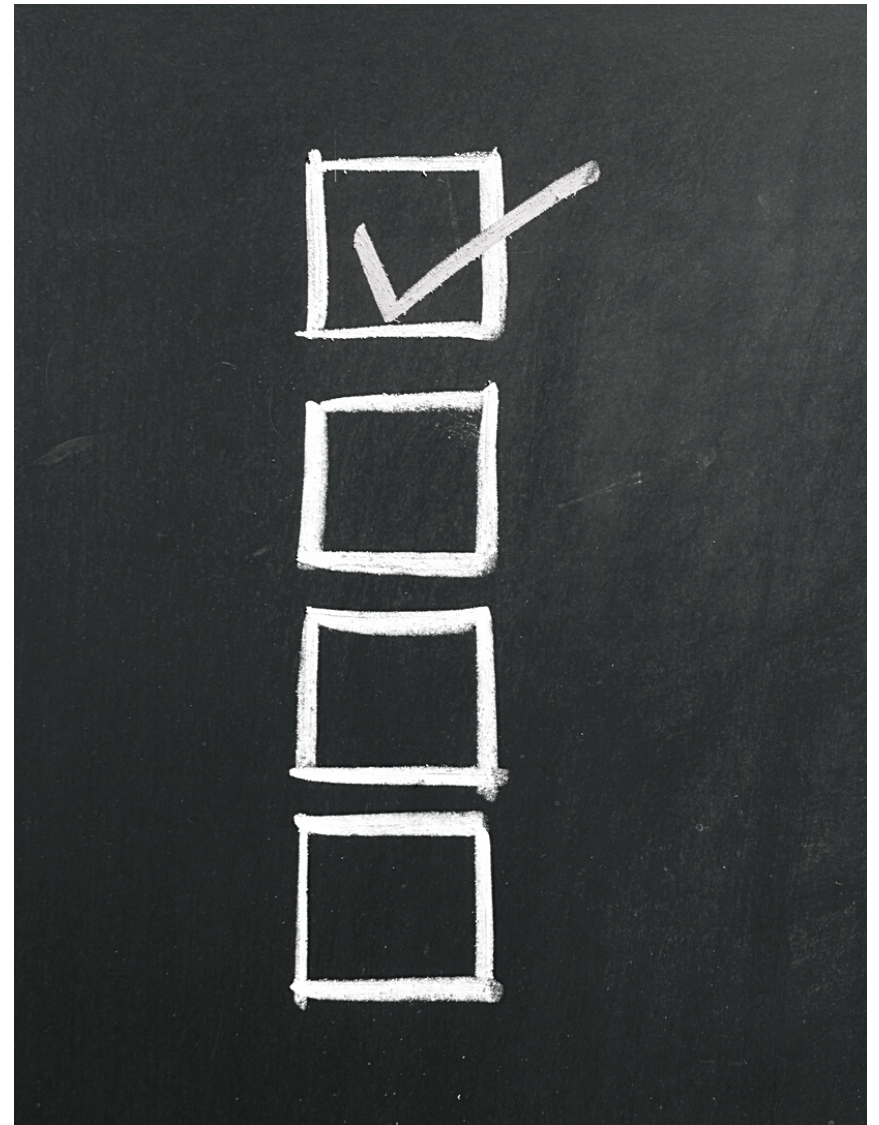
- **Formazione mirata del personale** sulle tematiche (es. con linee guida)
- **Formalizzare regolamenti per l'utilizzo delle tecnologie, responsabilizzando il dipendente:**
 - sul corretto uso dei **device aziendali** e dei BYOD
 - sulla sicurezza del proprio **end point**
 - sull'uso di **reti VPN sicure**
 - sul controllo delle **reti domestiche**
 - sull'utilizzo della **email** aziendale



GLI ADEMPIMENTI IMPOSTI DAL GDPR

Attenzione anche all'aggiornamento della **documentazione privacy aziendale:**

- Integrazione e aggiornamento del **registro dei trattamenti**
- Integrazione e aggiornamento **analisi dei rischi**
- **Formazione** e sensibilizzazione del personale
- Adozione di **regolamenti aziendali** (uso device e sistema IT, procedure per la gestione dei data breach, ecc.)



L'IMPORTANZA DI "LIMITARE I DANNI"

Numero medio documenti coinvolti in data breach ad aziende adeguate al GDPR: **75.000**



Numero medio documenti coinvolti in data breach ad aziende **non** adeguate al GDPR: **215.000**



Durata down del sistema per aziende adeguate al GDPR: **6 ore**



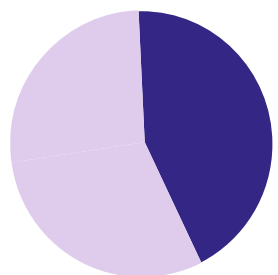
Durata down del sistema per aziende **non** adeguate al GDPR: **10 ore**



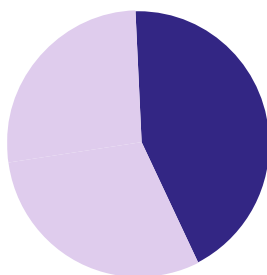
Fonte: rapporto "Data Privacy Benchmark 2019" (Cisco)

UN INVESTIMENTO "RIPAGATO"

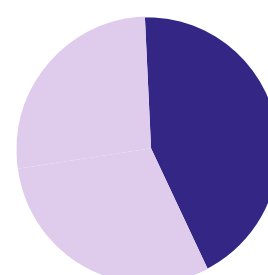
il 97% delle aziende che si è adeguata al GDPR ed ha adottato misure cyber security ha riscontrato almeno uno di questi benefici:



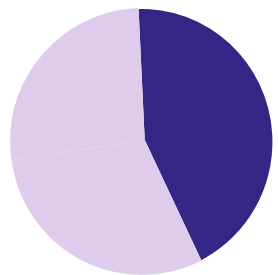
42% velocità e innovazione



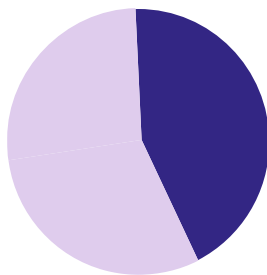
41% vantaggi sulla concorrenza



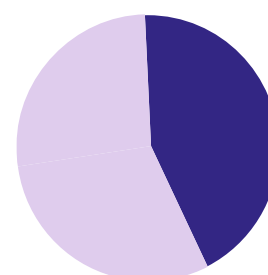
41% efficienza operativa



39% minori perdite da data breach



37% minori ritardi di vendita



36% appeal per investitori

Fonte: rapporto "Data Privacy Benchmark 2019" (Cisco)

PER SAPERNE DI PIÙ



Guarda su YouTube la registrazione del nostro webinar "Smart Working: cosa deve fare l'azienda?"

LA PRIVACY OLTRE L'UFFICIO

DECENTRALIZZAZIONE DEL LAVORO
le conseguenze...

CONSAPEVOLEZZA DEI TRATTAMENTI
la sensibilizzazione...

ESTENSIONE DELL'ACCOUNTABILITY
il risultato...

31:25 / 1:18:32

MISURE DI SICUREZZA

Data Governance
Crittografia
Ubicazione dei dati
Cancellazione sicura dei dati

Controllo Accessi
Gestione privilegi
Autenticazione
Log Management

Protezione end-point
Antimalware
Intrusion Prevention
Patch Management

Security Process
Policy aziendali
Piano di risposta agli incidenti
Audits & VA/PT

meccanismi di difesa

1:00:05 / 1:18:32

VUOI VERIFICARE IL LIVELLO DI COMPLIANCE DELLA TUA AZIENDA?

**consulenti
PRIVACY_{srl}**

PRIVACY STRESS TEST

La tua azienda è ancora aggiornata?

SCOPRILO CON NOI!

The advertisement features a man in a yellow sweater sitting on a stool, looking at a laptop. The background is a mix of yellow and blue with various icons like a padlock, a document, and a speech bubble.



IL TUO REPORT PERSONALIZZATO SU LIVELLO DELL'ADEGUAMENTO E PRINCIPALI CRITICITÀ

RICHIEDILO SUBITO:

CLICK HERE



I NOSTRI CONTATTI

RIMINI – Via Valentini 11

TEL. 0541 1798723

MILANO – P.zza Città di Lombardia 1

TEL. 02 45071182

BOLOGNA – Via Vittorio Lugli 4/A-D

TEL. 051 19907603

FERRARA – Viale Krasnodar 25

TEL. 051 19907603

info@iconsulentiprivacy.it

www.iconsulentiprivacy.it

