SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION

CYBER SECURITY TALKS

Cybersecurity e Smart Working

Nuove tipologie di “attacco”, protezione dei dati nel lavoro a distanza, cybersecurity check list per grandi imprese e pmi.

23 novembre 2020 | 11.00 - 12.30

FIERA MILANO

La Pubblica Amministrazione in numeri

Amministrazioni Centrali *

unità	**169**
personale	**1.348.428**
smart worker	**~ 2 %**

- Sistemi informativi strutturati, omogenei e integrati
- Parziale digitalizzazione dei processi amministrativi
- Servizi Informatici in house

Amministrazioni Locali

unità	**10.373**
personale	**1.547.927**
smart worker	**~ 1 %**

- Sistemi informativi diversificati, disomogenei, non integrati
- Scarsa digitalizzazione dei processi amministrativi
- Servizi Informatici in outsoursing

(*) Tra le Amministrazioni Centrali sono comprese quelle afferenti al Comparto Istruzione e Ricerca

FIERA MILANO

Fonte ISTAT: Censimento Permanente delle Istituzioni Pubbliche
Fonte Dip. Funzione Pubblica: Monitoraggio sul Lavoro Agile

La Cybersecurity nella PA pre lockdown

Attuazione delle Misure minime di sicurezza ICT (AgID)

- Amministrazioni centrali **~ 99 %**
- Amministrazioni locali **~ 50 %**

Sicurezza di tipo perimetrale

Metodi di autenticazione «*deboli*»

Modelli di accesso basati sulla «*fiducia*»

Data center principalmente on-premise e poco impiego del cloud computing

FIERA MILANO

Fonte ISTAT: Censimento Permanente delle Istituzioni Pubbliche

Le criticità Cybersecurity durante il lockdown

Dispositivi e connettività del lavoratore

- Dispositivi condivisi e/o obsoleti
- Assenza delle misure minime di sicurezza

Supporto tecnico scarso o assente

Configurazione di Remote Desktop

Utilizzo di VPN e piattaforme di Cloud Collaboration free e insicure

Incremento degli attacchi di

- Social engineering e Phishing
- Frodi informatiche o Furto d'identità
- Data breach (sia per l'Ente che per l'Utente)
- Denial of Service

Dipendenti in Smart Working

- Amministrazioni centrali **~ 75/80 %**
- Amministrazioni locali **~ 50 %**

FIERA MILANO

Fonte Dip. Funzione Pubblica: Monitoraggio sul Lavoro Agile

Lo Smart Working nella PA post lockdown

Fornitura di dispositivi sicuri e gestiti o Hardening di quelli dei dipendenti

Metodi di autenticazione Multi-Fattore o Sistemi di Identity Access Management

Adozione del modello Zero Trust Security

Incremento delle soluzioni di cloud computing gestite e monitorate quali:

- Virtual Desktop Infrastructure
- Soluzioni di Collaboration
- Storage Crittografati

Innovazione per la Resilienza

Cosa abbiamo appreso?

Per garantire la **Business Continuity** durante il lockdown
abbiamo sfruttato le peculiarità della **Cyber-Resilienza**:
la capacità di gestire un attacco informatico o una violazione dei dati
continuando a gestire la propria attività in modo efficace.

La resilienza come fattore di successo.

Per raggiungere questo obiettivo è necessario:

- Adottare un modello di gestione della cybersecurity ***«Risk based»***
- Attuare una reale ***«Digital Trasformation»*** dei processi lavorativi
- Aumentare la ***«Cybersecurity Awareness»*** dei dipendenti
- Elaborare un ***«Business Continuity Plan»***

FIERA MILANO

SICUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

Contattaci

vincenzocalabro.it
vincenzo.calabro@interno.it

www.sicurezza.it

FIERA MILANO