Cybersecurity e Digital Trasformation

26 Maggio 2018

Polizia di Stato

Il Questore della Provincia di Udine

Dr. Claudio CRACOVIA

Polizia di Stato

RISVOLTI DEL DIGITALE

Polizia di Stato

CONSEGUENZE DEL DIGITALE

- SPOSTAMENTO DELLE ATTIVITA' CRIMINALI IN AMBITO TRANSNAZIONALE
- NECESSITA' DI NUOVE SINERGIE DI COLLABORAZIONE CON
- NUOVE PREVISIONI NORMATIVE
- NECESSITA' DI NUOVI STRUMENTI INVESTIGATIVI PER IL CONTRASTO

Polizia di Stato

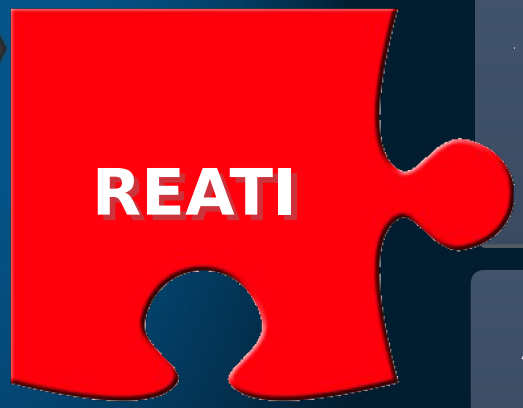
CONSEGUENZE DEL DIGITALE

STRATEGIE

- SVILUPPO DI NUOVI RAPPORTI ISTITUZIONALI PER GARANTIRE UNA SICUREZZA PARTECIPATA
- IMPLEMENTAZIONE DELLE COMPETENZE DEL PERSONALE DELLA P.S. SUI REATI COMMESSI CON IL
- INFORMAZIONE E DIVULGAZIONE SUI PERICOLI CONNESSI ALL'USO DEI
- ADOZIONE DI PROTOCOLLI CON LE INFRASTRUTTURE CRITICHE, PMI E PA

Polizia di Stato

CONSEGUENZE DEL DIGITALE



- TERRORISMO E TRAFFICO DI SOSTANZE STUPEFACENTI ATTRAVERSO CHAT
- MOLESTIE, CYBERBULLISMO, PEDOPORNOGRAFIA ALL'INTERNO DI CHAT CHE
- AGGRESSIONE ALL'INTEGRITA' DEI DATI E ALLA RISERVATEZZA DELLE
- FRODE, FURTO D'IDENTITA', CONTRAFFAZIONE, VIOLAZIONE DELLA PROPRIETA' INTELLETTUALE

Polizia di Stato

LINEE D'INTERVENTO

Riorganizzazione Uffici Territoriali

Nuova direttiva Ministro competenze Hacking, I.C., Pedo, Terrorismo, Financial CyberCrime

Razionalizzazione territoriale e nuova organizzazione degli

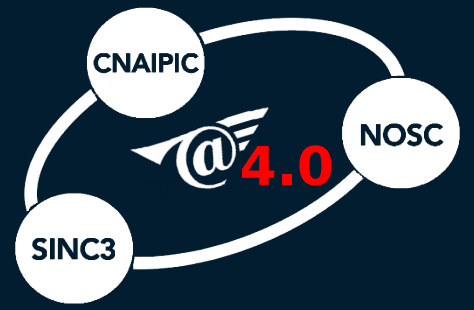
Nuova denominazione degli Uffici

Riorganizzazione degli Uffici territoriali

Polizia di Stato

Sistema Nazionale Anticrimine Informatico

dal **C.N.A.I.P.I.C.** al **Sistema Nazionale Anticrimine Informatico**



PROGETTO SINC 3

Polizia di Stato

L'INIZIATIVA SINC3
SISTEMA INFORMATIVO NAZIONALE CONTRASTO CYBER CRIME

In linea con la normativa europea introdotta dalla Network and Information Security Directive (NIS) che richiede di incrementare le capacità di infosharing e di risposta agli attacchi cyber l'iniziativa si pone i seguenti obiettivi:

- **Realizzare un Sistema Nazionale Anticrimine Informatico (valorizzazione dell'esperienza CNAIPIC)**
- **Partenariato pubblico-privato**
- **Costruire un modello di diagnosi e prevenzione delle minacce cyber esteso alle PMI (Piccole e Medie Imprese) ed alle PAL (Pubbliche Amministrazioni Locali)**
- **Veicolare in tempo reale preziose informazioni di sicurezza (prevenzione)**
- **Formare squadre per il pronto intervento presso le realtà colpite da attacchi cyber (contrasto – attività di PG)**

Polizia di Stato

Direttiva NIS (Network and Information Security)

Obiettivo: raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri dell'UE.

Punti chiave:

- Migliorare le capacità di cyber security;
- Aumentare il livello di cooperazione.
- Obbligo di gestione dei rischi e di denunciare gli incidenti di una certa entità da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Servizi essenziali:

Aziende pubbliche o private che hanno un ruolo importante per la società e l'economia tra cui :

- PMI (Piccole e Medie Imprese)
- PAL (Pubbliche Amministrazioni Locali)

Polizia di Stato

I Principali Centri Operativi

Servizio Polizia Postale e delle Comunicazioni

C.N.A.I.P.I.C

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

C.N.C.P.O

Centro Nazionale per il Contrasto alla Pedopornografia On-line

COMMISSARIATO DI P.S ON LINE

www.commissariatops.it