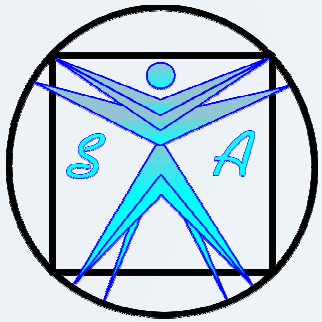


Adempimenti tecnici e misure di sicurezza informatiche”

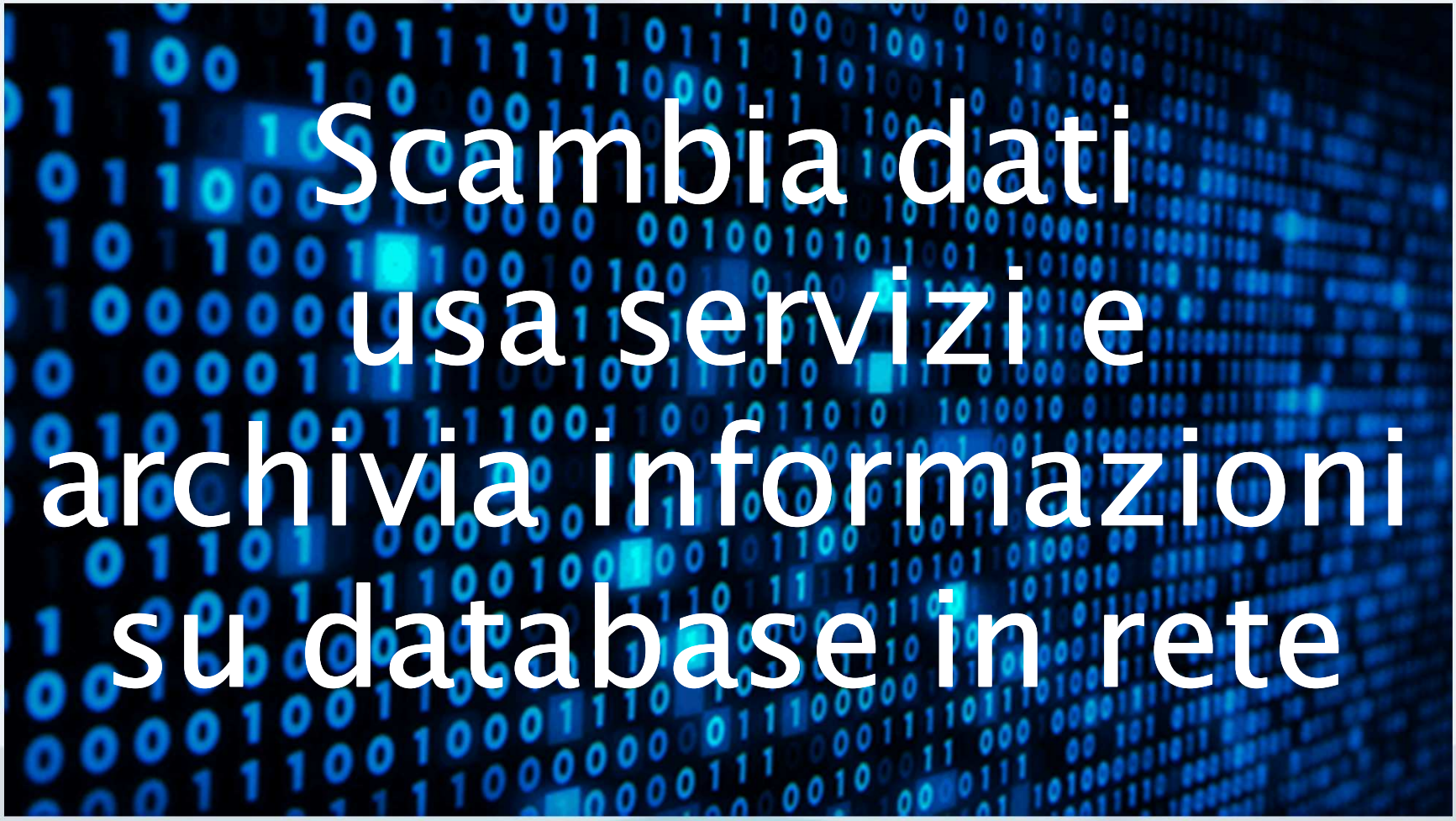
Dott. Paolo Aldeghi

Il mondo che viviamo

Il mondo che viviamo

Il mondo che viviamo

I nostri device



Device sempre più sofisticati

E il futuro?

Tutto connesso – pensando al servizio

- Connettere ogni tipo di dispositivo
- Senza alcun attenzione alla sicurezza e alla protezione dei dati

- Perché devono attaccare proprio me?
- … tanto non è mai successo …

Motivazione e spinta all'hacking dei sistemi

Perché devono attaccare proprio me?

Le informazioni sono l'Oro del terzo millennio

Motivazione e spinta all'hacking dei sistemi

… tanto non è mai successo …

Chi potrebbe giurare di non avere mai avuto un computer infetto da un malware nella rete della propria azienda?

Il Data Breach

*"A **data breach** is the intentional or unintentional release of secure or private/confidential information to an untrusted environment"*

Esempi Eclatanti

BREACH

21,5M record
4M persone

- Dati Personali
- N. prev. sociale
- Impronte digitali

BREACH

79M record
Pazienti

Sentenza:
Rifonderà $115M

Dati: semplici dati personali

BREACH

145M persone

- Dati personali
- N. prev. sociale
- Carte di credito

Manuale di come non ci si deve comportare

- 5 settimane per comunicare
- Comunicazione in chiaro (altro illecito)

BREACH

70M CC
4M persone
$200M danno
Riduzione vendite 4%

- Malware sui pc dei punti vendita
- Furto n. carte di credito in chiaro

Esempi di casa nostra

Esempi di casa nostra

Cliente

Fornitore

Ci viene da sorridere… ma?

TGCOM24 MEDIASET Martedì 15 Maggio

10 MAGGIO 2018 10:30

Web, hackerato il sito dell'azienda leader degli anti-virus: "Offline chi contribuisce al controllo delle masse"

Il collettivo AnonPlus ha "defacciato" la pagina di Symantec, casa del software Norton, inserendo il loro manifesto poltico

(209)

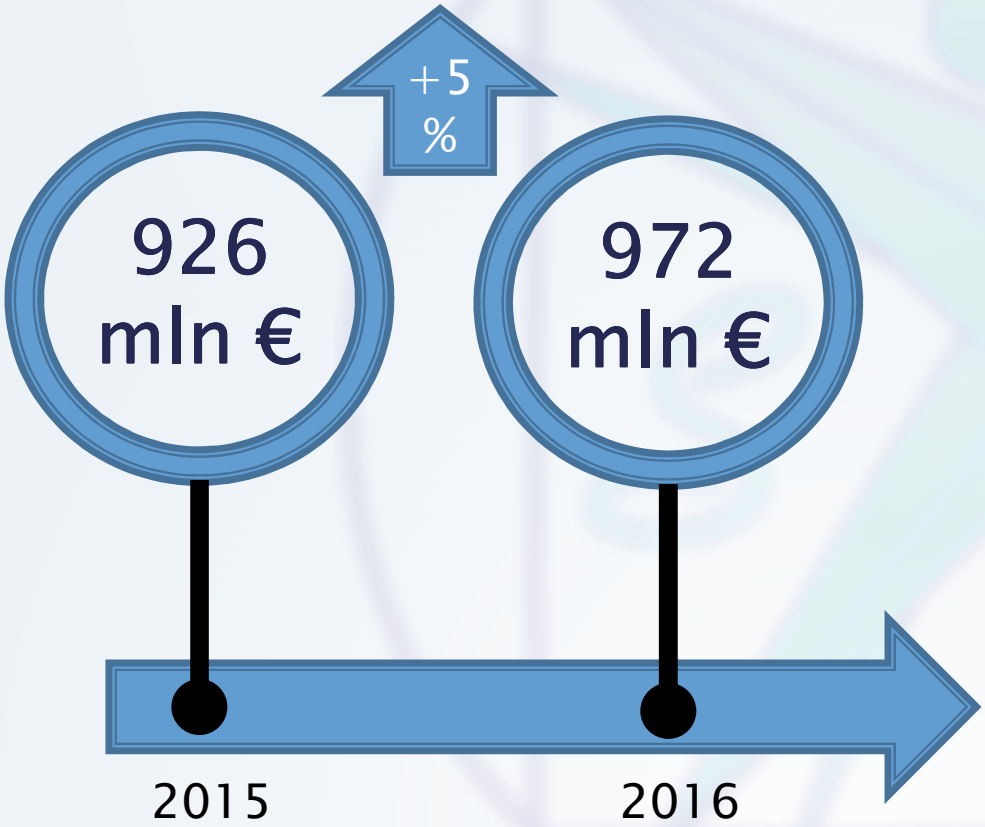
LEGGI DOPO COMMENTA

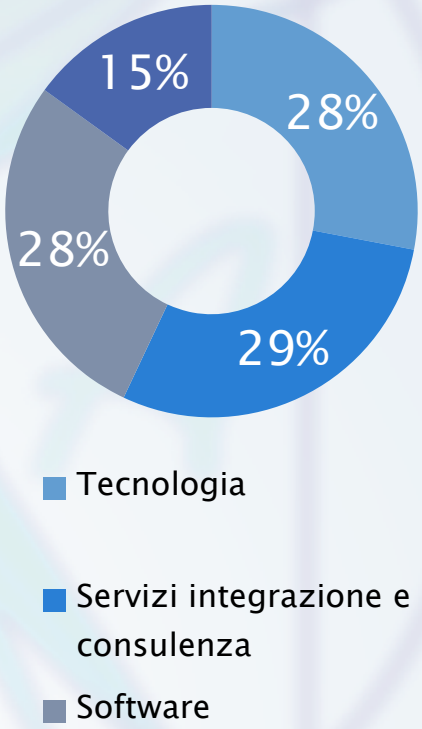
Anche gli esperti della sicurezza informatica hanno dei punti deboli. Nella notte tra il 4 e il 5 maggio, degli **hacker** hanno preso il controllo di un sito di **Symantec**, azienda leader nel settore degli antivirus e casa del software **Norton**. In seguito all'attacco, rivendicato dal collettivo **AnonPlus**, gli intrusi hanno "defacciato" la pagina web (dall'inglese defacing, sfigurare), inserendo il loro manifesto politico.

Attacco informatico

Quando

Investimenti in sicurezza (comparto IT)





1,5% degli investimenti totali in ICT

Fonte: Rielaborazione da dati Assinform2017 e Osservatorio Information Security & Privacy 2016, Politecnico di Milano

Confronto sicurezza automotive

1€ : 66€

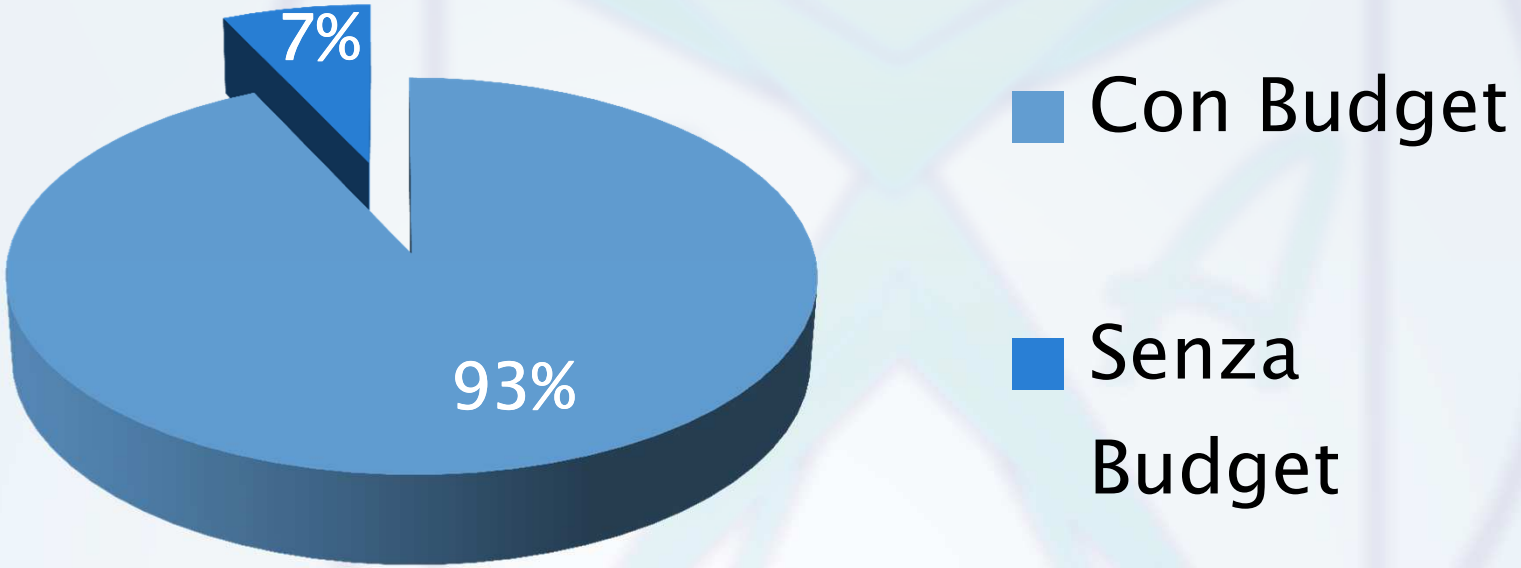
Rapporto spese sicurezza informatica rispetto a quanto speso in comparto ICT

30€ : 100€

Rapporto spese sicurezza rispetto a quanto speso in Automotive

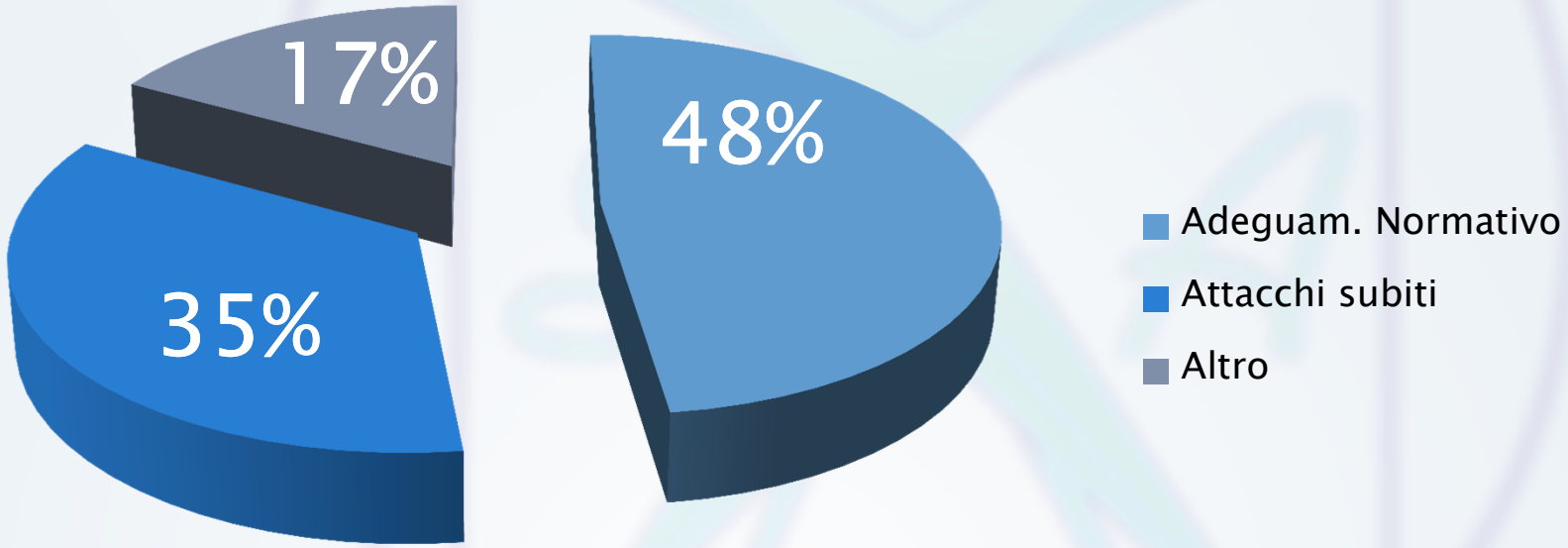
Fonte: Rapporto CLUSIT sulla Sicurezza ICT in italia - 2017

PMI – Pianificazione investimenti



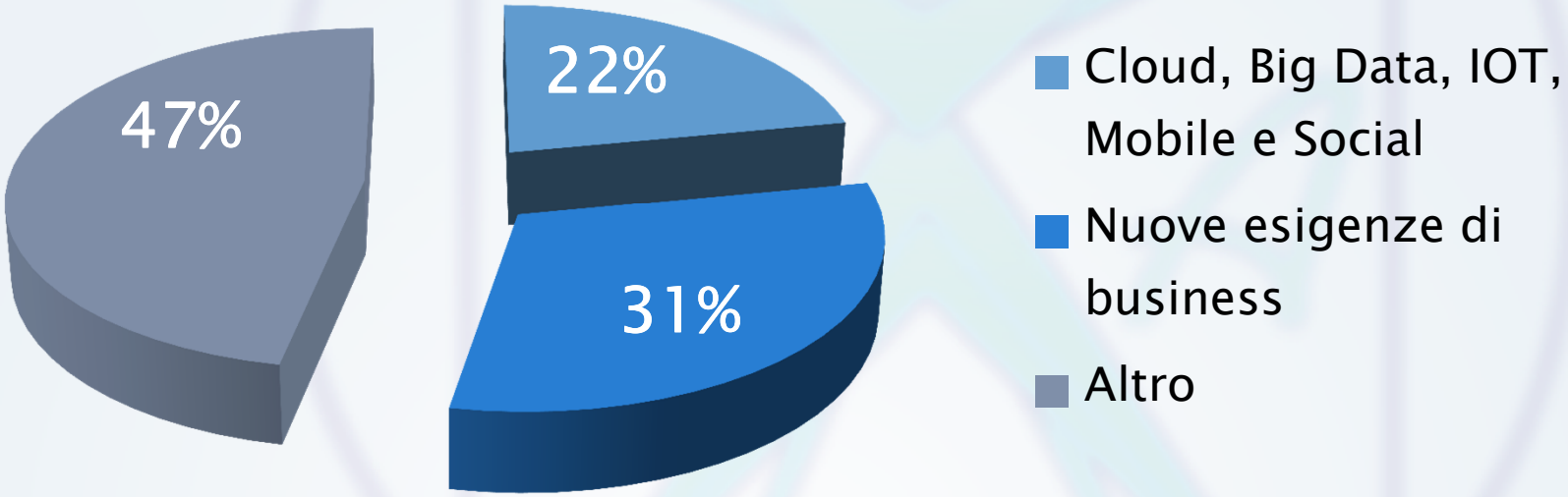
Fonte: Osservatorio Cloud & ICT as a Service

PMI – Uso degli investimenti



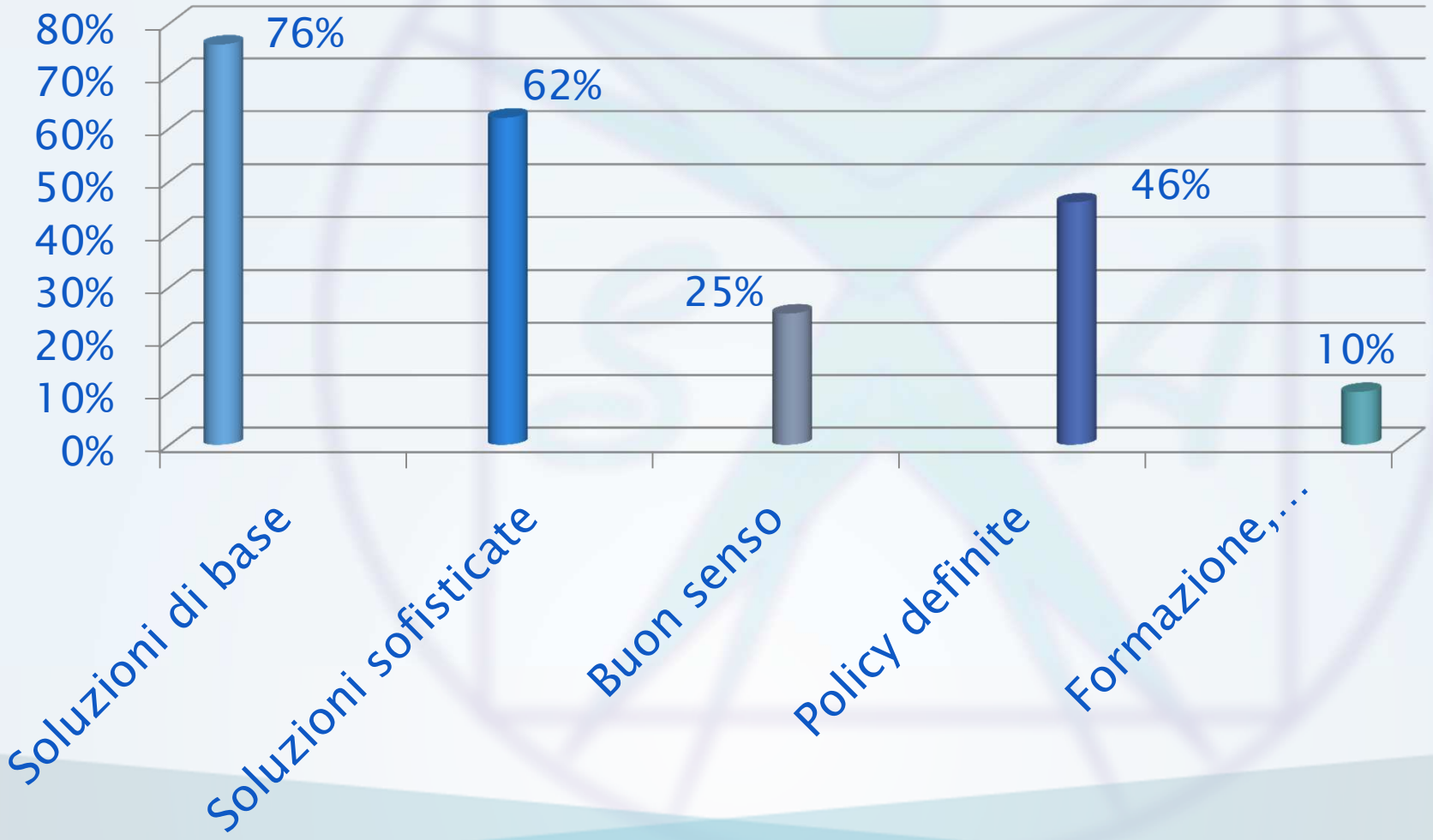
Fonte: Osservatorio Cloud & ICT as a Service

PMI – Volontà di innovazione



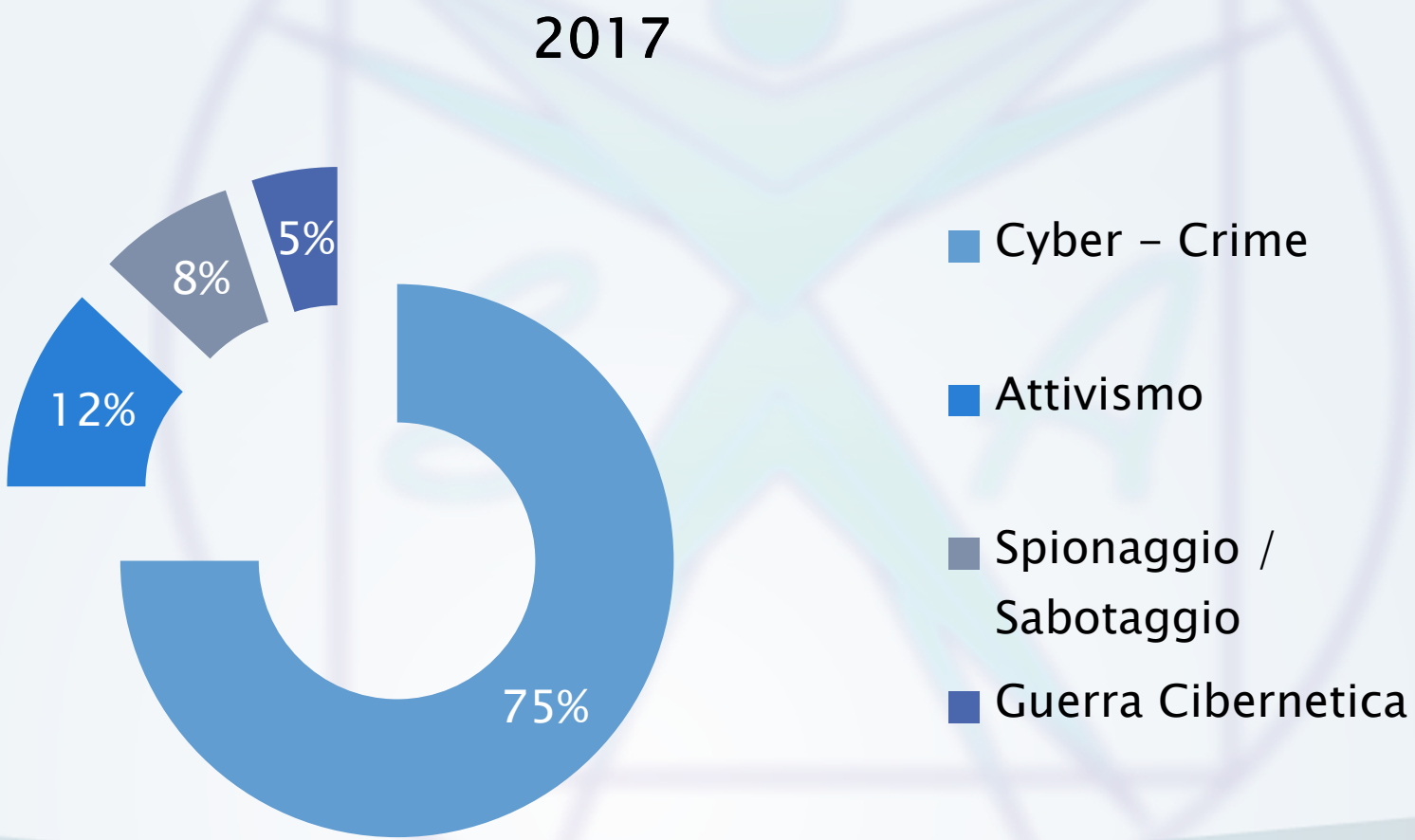
Fonte: Osservatorio Cloud & ICT as a Service

PMI – Come si proteggono



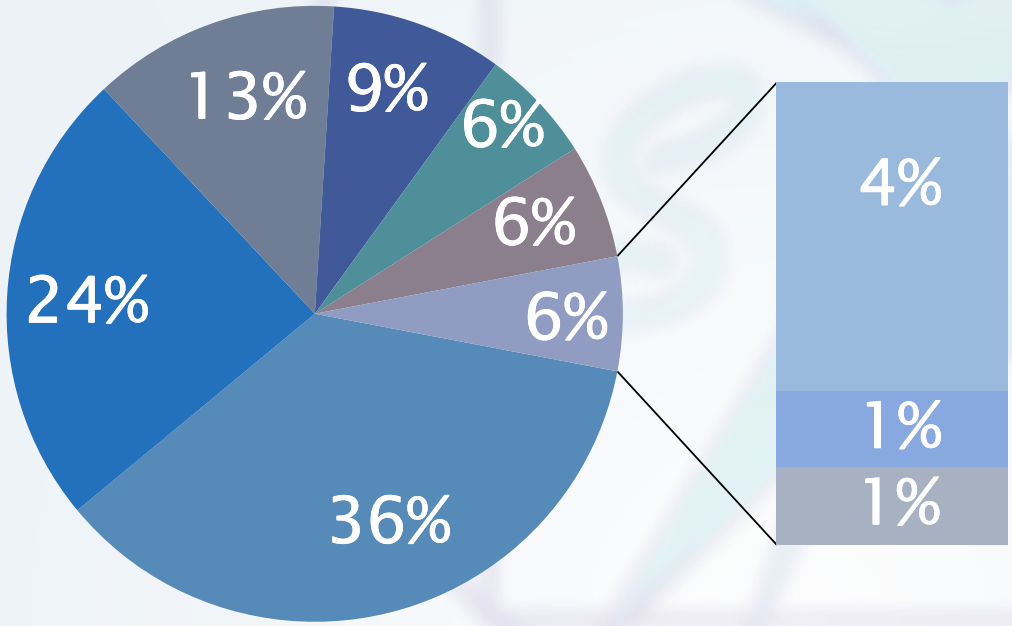
Fonte: Osservatorio Cloud & ICT as a Service

Motivazione degli Attacchi



Fonte: CLUSIT – Rapporto 2017 sicurezza ICT in Italia

Tipologia e distribuzione delle tecniche di attacco



- Malware
- Sconosciuta
- Vulnerabilità
- Phishing/Social Engineering
- Multiple Threats / APT
- Account Cracking
- DDoS
- 0-day

Fonte: CLUSIT – Rapporto 2017 sicurezza ICT in Italia

Cosa stiamo facendo?

- 1000 attacchi alle infrastrutture critiche
- 28500 allarmi nel 2017 su obiettivi di interesse nazionale
- 500% rispetto all'anno precedente

Fonte: Repubblica.it

Perché così pochi risultati

- Il fattore X (distrazione, mancanza di consapevolezza, scarsa preparazione)
- Software a matriosca
- Device senza certificazione di sicurezza (IOT: backdoor)
- Atteggiamento mentale (progettazione in sicurezza)
- Bassa propensione delle PMI a scegliere partner qualificati (budget)

Okkio alla Talpa

Come abbiamo risposto agli attacchi sino ad ora?

GDPR: By Design – By Default

- Privacy by Design: tutelare il dato sin dalla progettazione dei sistemi informatici che ne prevedono l'utilizzo

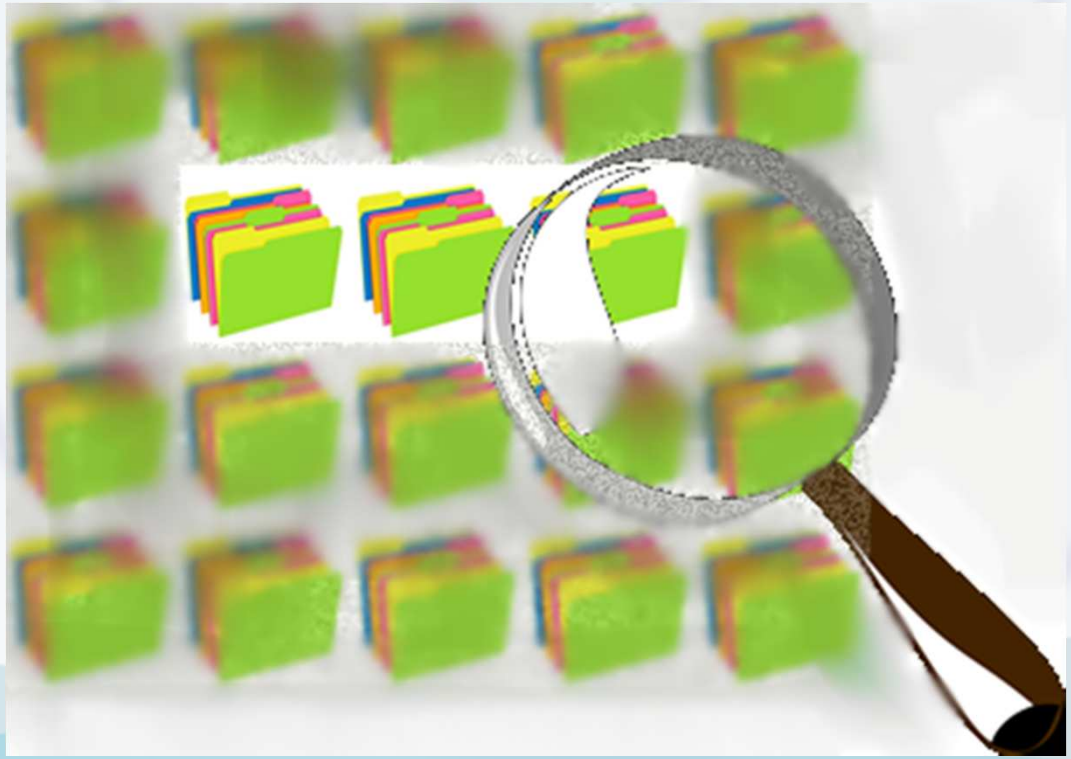
- Privacy by Default: tutela della vita privata per "impostazione predefinita", ovvero in modo automatico

GDPR: indicazioni sul trattamento elettronico dei dati

- Abbandonare il concetto errato di «massima funzionalità» che prevedeva di rimuovere tutte le barriere perché intralcio al lavoro quotidiano;
- Sicurezza durante tutto il **ciclo del prodotto o servizio ovvero durante tutto il trattamento**
- **Distruzione del dato** al termine del trattamento se non diversamente previsto da normative

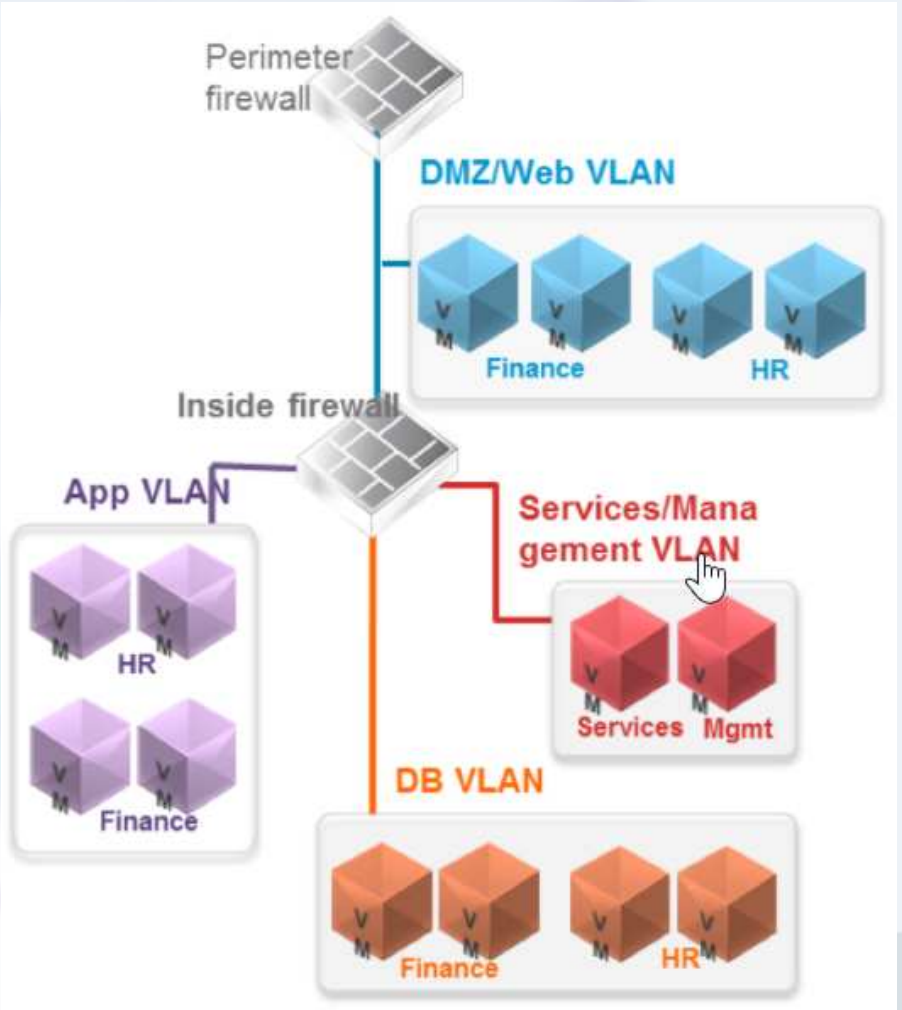
GDPR: Privilegio Minimo

- Concedere agli addetti di accedere al solo minimo dato che essi hanno necessità di vedere



GDPR: Micro-Segmentazione

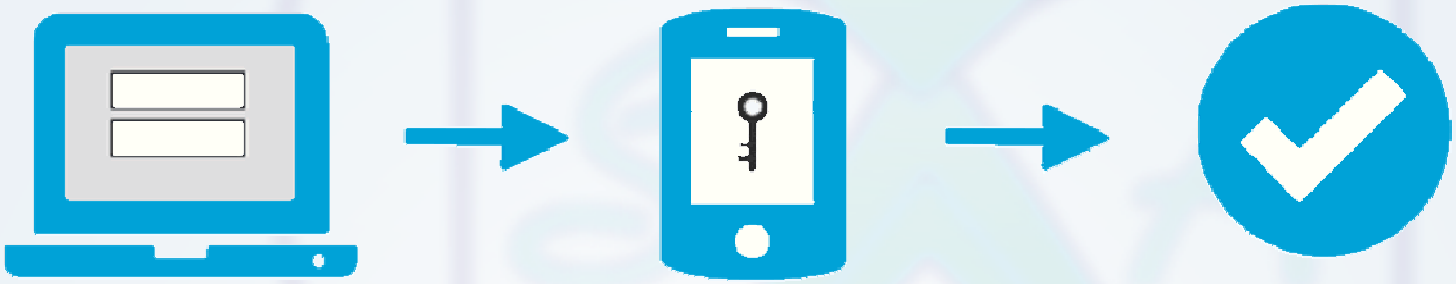
- Suddivisione della rete in sotto-reti separate
- Suddivisione dei servizi su sistemi differenti
- Suddivisione delle App in differenti aree accessibili in base a diritti differenti
- Suddivisione dei sistemi su macchine virtuali differenti



Virtualizzazione

GDPR: Criptaggio

GDPR: Verifica a fattori multipli



Password + Verification = Access

Regola del 3-2-1

- Possedere almeno tre copie
- In due luoghi differenti
- Una copia offline

GDPR: Backup

- Verificare periodicamente (registro delle prove di ripristino)
- Non affidarsi alla memoria (backup automatici)
- Utilizzare sistemi e software certificati
- Reportistica degli eventi

GDPR: Buone pratiche di gestione dei sistemi

- Patch di sistema:
  «Non lo aggiorno…. perché funziona»
- No alle soluzioni «Fai Da Te»
- E' nello stanzino…. allora è sicuro

L'amministratore di sistema

*"**l'amministratore di sistema** o, tecnico sistemista di rete, è una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione"*

GDPR... riassumendo

Impone:

- Metodo di lavoro
- Consapevolezza
- Responsabilità
- Protezione dei dati
- Continua sorveglianza

Occasione:

- Verifica
- Rettifica
- Ristrutturazione
- Messa in sicurezza
- Protezione del proprio patrimonio

Dott. Paolo Aldeghi
Studio Aldeghi

paolo.aldeghi@studioaldeghi.it