omat forum

Attacchi informatici e misure di difesa: i dati dell’Osservatorio Attacchi Digitali in Italia

Marco Bozzetti
Presidente, AIPSI Associazione Italiana Professionisti Sicurezza Italiana

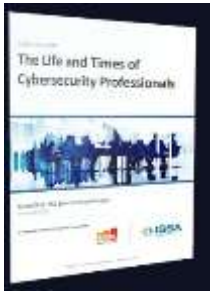
- **Marco R. A. Bozzetti, Ingegnere elettronico al Politecnico di Milano, è Presidente AIPSI e CEO di Malabo Srl**
- **Ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e Gea/Gealab, oltre ad essere stato il primo responsabile dei sistemi informativi (CIO) dell'intero Gruppo ENI (1995-2000).**
- **Nella seconda metà degli anni 70 è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, partecipando alla standardizzazione dei protocolli del modello OSI dell'ISO**
- **È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser"**
- **Commissario d'Esame per le certificazioni eCF (EN 16234 - UNI 11506).**
- **Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT**

- **Malabo Srl è stata creata da M. Bozzetti nel 2001**
- **una società di consulenza direzionale per l'ICT, che opera per Clienti lato domanda e lato offerta basandosi su una consolidata rete di esperti e di società ultra specializzate**
- **Obiettivo primario degli interventi di Malabo è di creare valore misurabile per il Cliente, bilanciando adeguatamente gli aspetti tecnici con quelli organizzativi nello specifico contesto del Cliente**
- **Dispone di un proprio laboratorio ICT con server e storage duali, virtualizzati, collegati con switch a 10 G e connessi ad internet con fibra ottica a 100 Mbps, oltre ad uno spazio in cloud (IaaS)**
- **Per garantire un effettivo trasferimento di know-how, fornisce come servizio ai Clienti le proprie metodologie e gli strumenti informatici usati nell'intervento consulenziale**

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- È una Associazione apolitica, aconfessionale e senza fini di lucro cui possono associarsi solo persone fisiche, non giuridiche
- È **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org) che conta circa 13.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo
- **Obiettivo principale AIPSI** : aiutare i propri Soci (**persone fisiche**) nella **crescita professionale** → competenze →carriera e crescita business
  - Offrendo ai propri Soci **servizi qualificati** per tale crescita, che includono
    - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
    - **ISSA Journal**
    - Indagini con relativi rapporti annuali e specifici, quali ad esempio
      - **ESG ISSA Survey** "The Life and Times of Cyber Security Professionals"
      - Rapporto annuale **OAD** nel nuovo sito **https://www.oadweb.it**
      - **Indagine in corso sulla professione femminile della cybersecurity in Italia (CSWI)**
    - Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016)
    - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
    - Gruppo Specialistico di Interesse **CSWI, Cyber Security Women Italy**, aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI)

ISSA



OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

- *Che cosa è*
  - Indagine via web sugli attacchi digitali intenzionali ai sistemi informatici in Italia
- *Obiettivi iniziativa*
  - Fornire informazioni sulla reale situazione degli attacchi digitali in Italia
  - Contribuire alla creazione di una cultura della sicurezza informatica in Italia, sensibilizzando in particolare i vertici delle aziende/enti ed i decisori sulla sicurezza informatica
- *Che cosa fa*
  - Indagini annuali e specifiche su argomenti caldi, condotte attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende
- *Come*
  - Rigore, trasparenza, correttezza, assoluta indipendenza (anche dagli Sponsor)
  - Rigoroso anonimato per i rispondenti ai questionari
  - Collaborazione con numerose Associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori

OAD 2018
10 anni di indagini via web sugli attacchi a informatici

Per scaricare il Rapporto 2018 OAD (gratuito):
- Registrarsi a https://www.oadweb.it
- Consenso esplicito privacy
- Scaricare il file in pdf

- 160 pagine A4
- 140 grafici
- 11 Capitoli → 131 pagine A4
  - Cap. 11: Dati dalla Polizia Postale e delle Telecomunicazioni, commentati dall'autore
- 9 Allegati → 29 pagine A4
- Prefazione dott. ssa Nunzia Ciardi, Direttore Polizia Postale e delle Telecomunicazioni
- Executive Summary in italiano e in inglese

Le novità di OAD 2018

Chiara separazione tra **che cosa** e **come** attacco

Che cosa è attaccato	Come (tecniche attaccco)						
	Attacco fisi						utilizzzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)
Distruzione fisica di dispositivi ICT o di loro parti							
Furto fisico di dispositivi ICT o di loro parti							
Furto informazioni da sistemi fissi (PC, server, storage system, ...)							
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)							
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori							
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS							
Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)							
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.							
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT							
Saturazione risorse digitali (DoS, DDoS)							
Attacchi ai propri sistemi in cloud o in hosting presso Fornitori							
Attacchi a dispositivi IoT (Internet of Thinks) in uso							
Attacchi ai propri sistemi di automazione (DCS, PLC, ..) e di robotica							
Attacchi a sistemi e/o servizi basati su blockchain							

- per ogni tipo di attacco (che cosa), se l'attacco è stato rilevato appaiono delle sotto domande che includono:
  - la frequenza di attacchi
  - le "macro" tecniche di attacco (come)
  - i principali impatti subiti dall'attacco più grave
  - le possibili motivazioni dell'attacco più grave
  - il tempo massimo richiesto per il ripristino ex ante nel caso del più grave attacco di quel tipo subito nell'anno
- se no si salta al tipo di attacco successivo

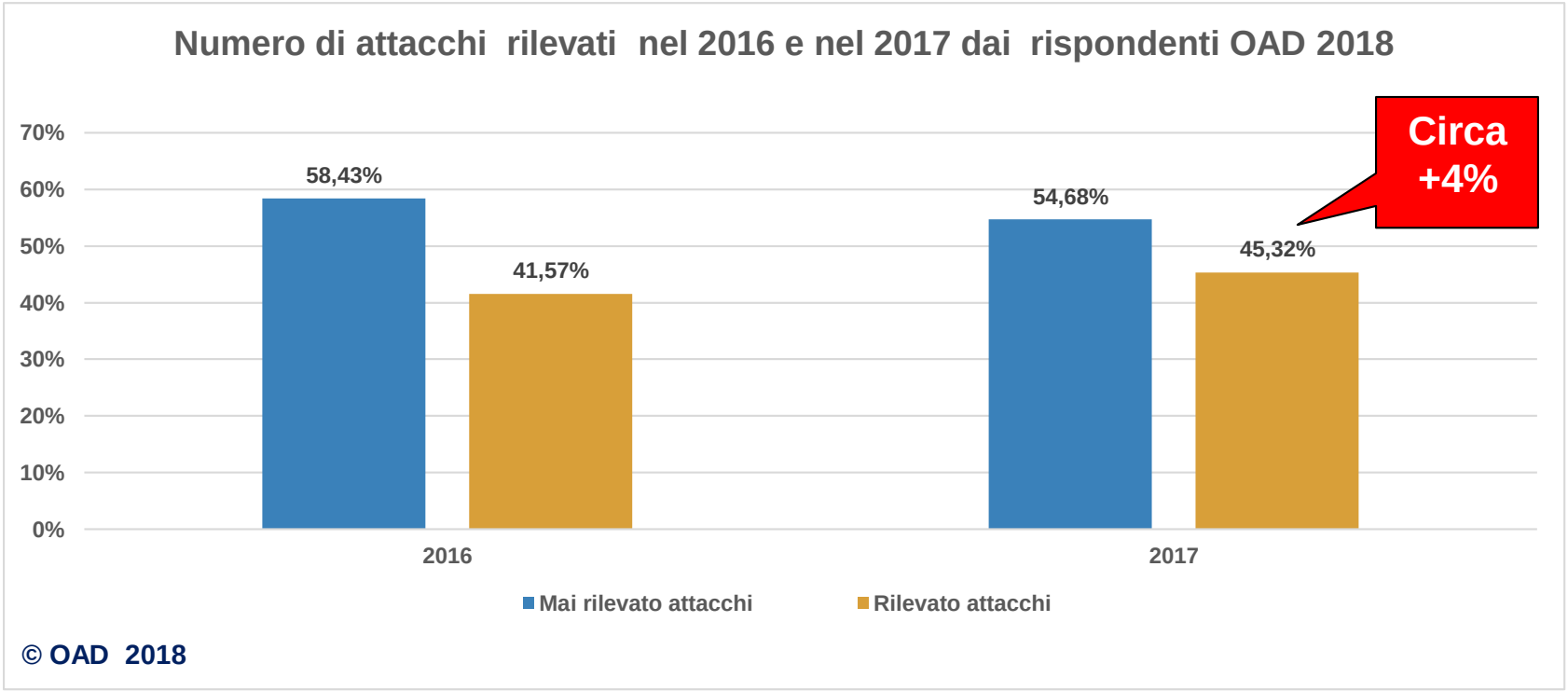
Attacchi ai servizi ICT terziarizzati

Attacchi a IoT

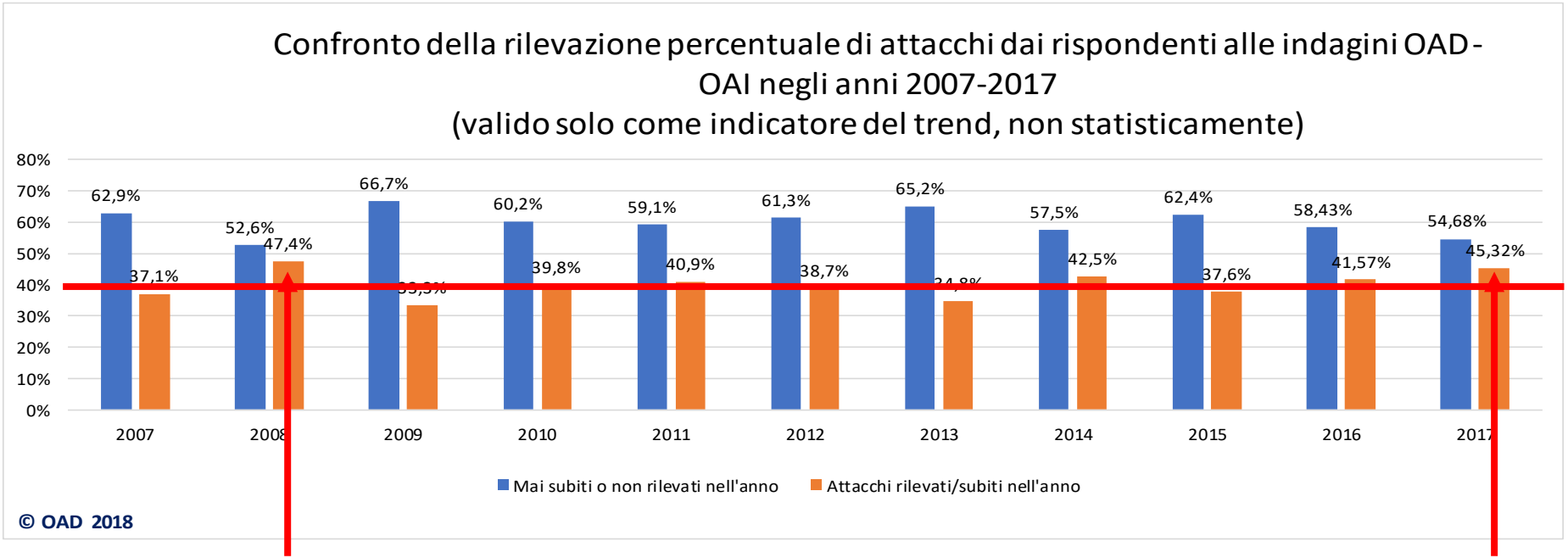
Attacchi sistemi aut. industriale e robotici

Attacchi alla blockchain

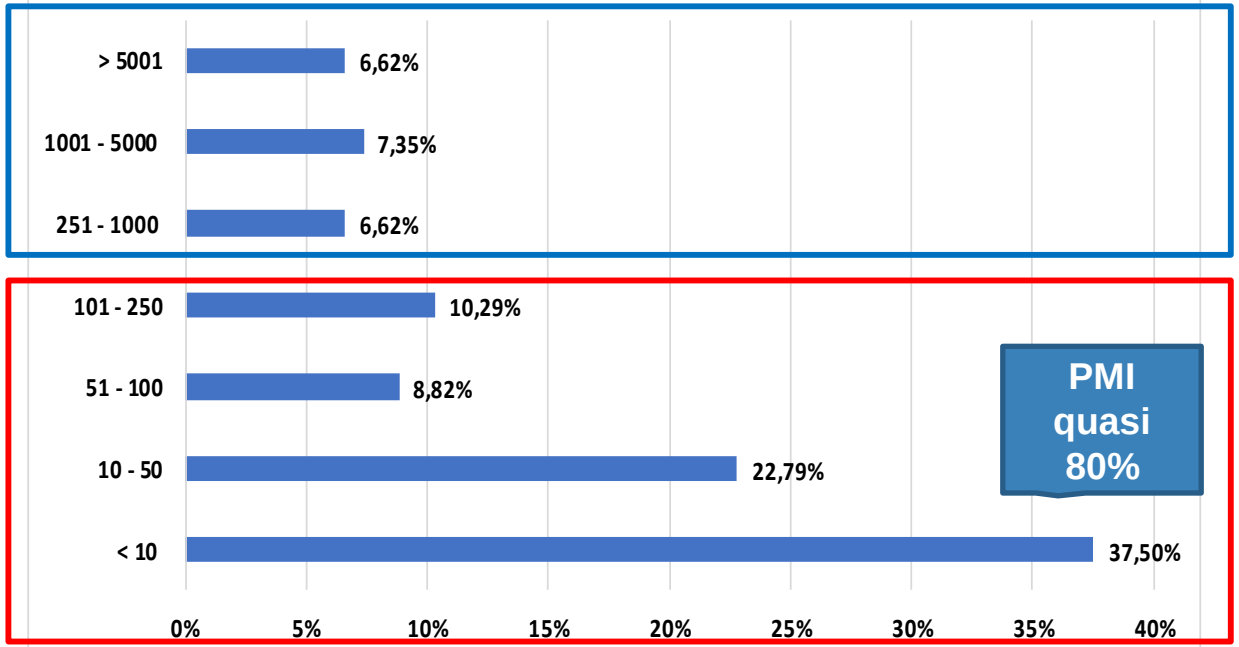
OAD 2018: attacchi rilevati 2016-17



Un confronto indicatore 2007-2017



Distribuzione dei rispondenti per dimensione della loro Azienda/Ente per numero di dipendenti



I più recenti dati ISTAT per le aziende:

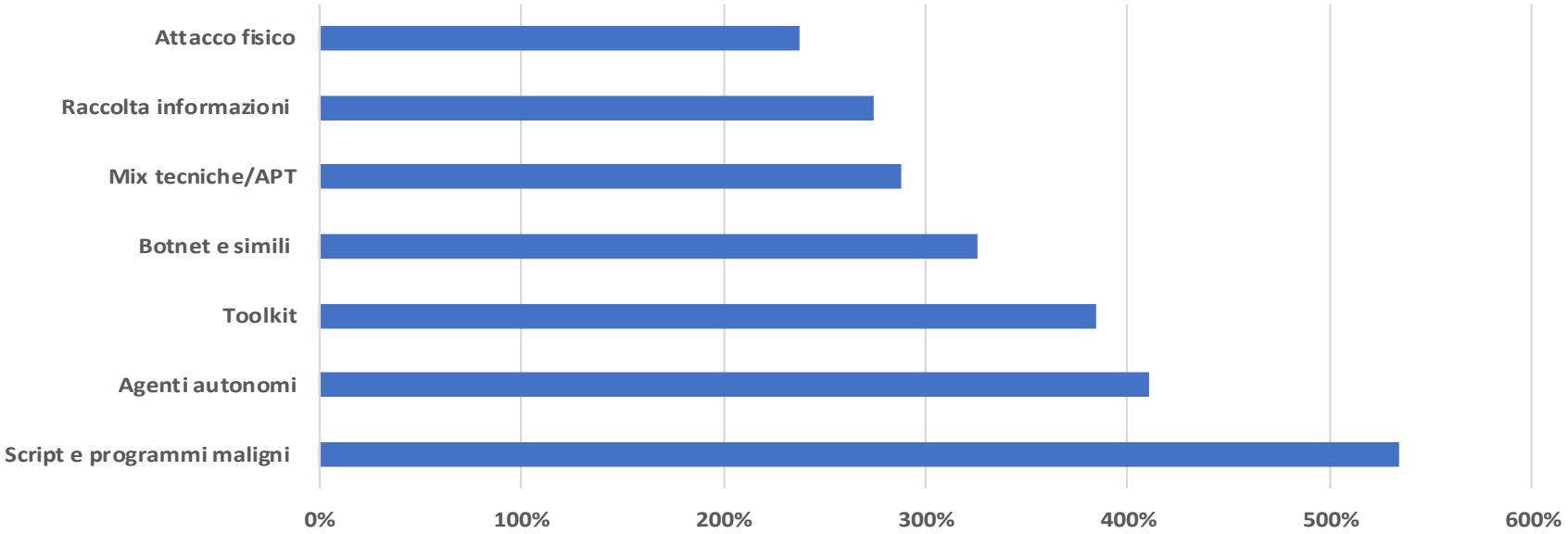
- Fino a 9 dipendenti: **4.180.870**
- Da 10 a 49: 184.098
- Da 50 a 249: 22.156
- 250 e più: 3.787.

Pubbliche Amministrazioni:

- Circa **55.000**

Diffusione % tipologia attacchi (che cosa attacco) rilevati dai rispondenti nel 2016 e nel 2017 (risposte multiple)

Diffusione tecniche di attacco (come) nelle varie tipologie (che cosa) di attacco rilevate dai rispondenti nel 2017



Queste perecentuali sono solo un indicatare e non hanno alcun senso statistico pur se indicati come %

Due grandi categorie di attacchi digitali

Attacchi a specifici obiettivi (target), con precisi obiettivi e larga disponibilità di risorse e competenze → Grandi Aziende/Enti

Attacchi di massa, anche non sofisticati, con l'obiettivo di colpire almeno qualcuno nella massa (es: ransomware, phishing) →
- PMI
- Studi
- Esercizi commerciali
- Singole persone

Vulnerabilità causa delle minacce

Tutte si basano sulle **vulnerabilità tecniche e/o umane-organizzative**

- ***Vulnerabilità tecniche*** (software di base e applicativo, architetture e configurazioni)
- siti web e piattaforme collaborative
- Smartphone e tablette → mobilità → **>>14.000 malware**
- Posta elettronica → spamming e phishing
- Piattaforme e sistemi virtualizzati
- Terziarizzazione e Cloud (XaaS)
- Circa il 40% o più delle vulnerabilità non ha patch di correzione
- ***Vulnerabilità delle persone***
- Social Engineering e phishing
- Utilizzo dei **social network,** anche a livello aziendale
- ***Vulnerabilità organizzative***
- Mancanza o non utilizzo procedure organizzative
- Insufficiente o non utilizzo degli standard e delle best practices
- Mancanza di formazione e sensibilizzazione
- Mancanza di controlli e monitoraggi sistematici
- Analisi dei rischi mancante o difettosa
- Non efficace controllo dei fornitori
- Limitata o mancante SoD, Separation of Duties

La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

- **Inconsapevolezza**
- **Imperizia**
- **Ignoranza**
- **Imprudenza**
- **Dolo**

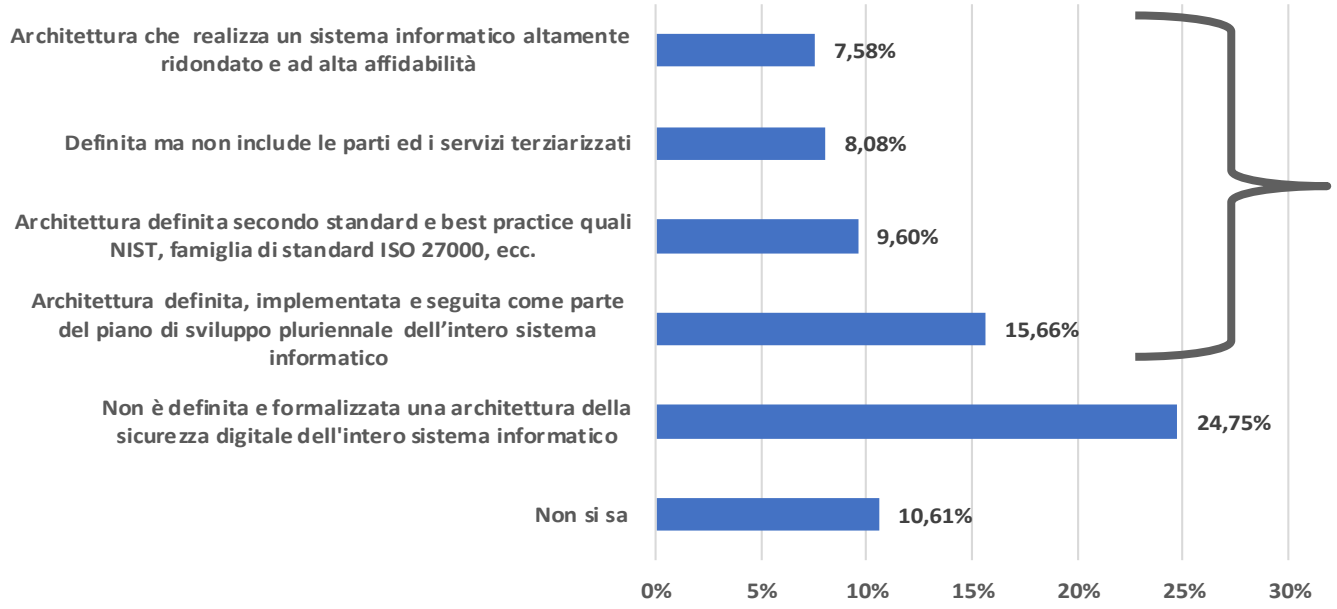
Aggravata dalla non o inefficace organizzazione

Mancanz di formazione e addestramento

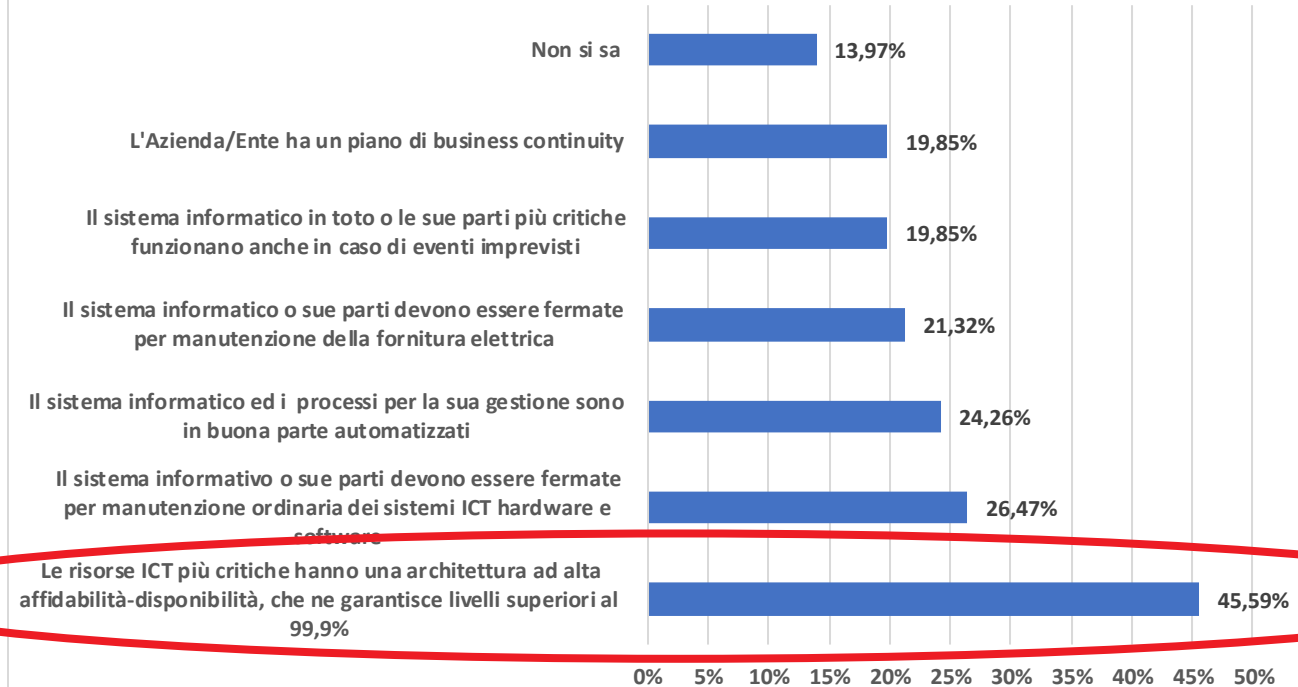
OAD 2018: le misure di sicurezza digitale delle aziende/enti dei rispondenti

- **Misure tecniche**
  - Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico
  - Contromisure fisiche
  - Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
  - Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
  - Contromisure tecniche per la protezione logica dei singoli sistemi ICT
  - Contromisure tecniche per la protezione degli applicativi
  - Contromisure per la protezione dei dati
- **Misure organizzative**
  - struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative
  - Contratti e clausole sicurezza digitale con le Terze Parti (GDPR dovrebbe aiutare!!)
  - Awarness sicurezza digitale
  - auditing
- **Misure di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

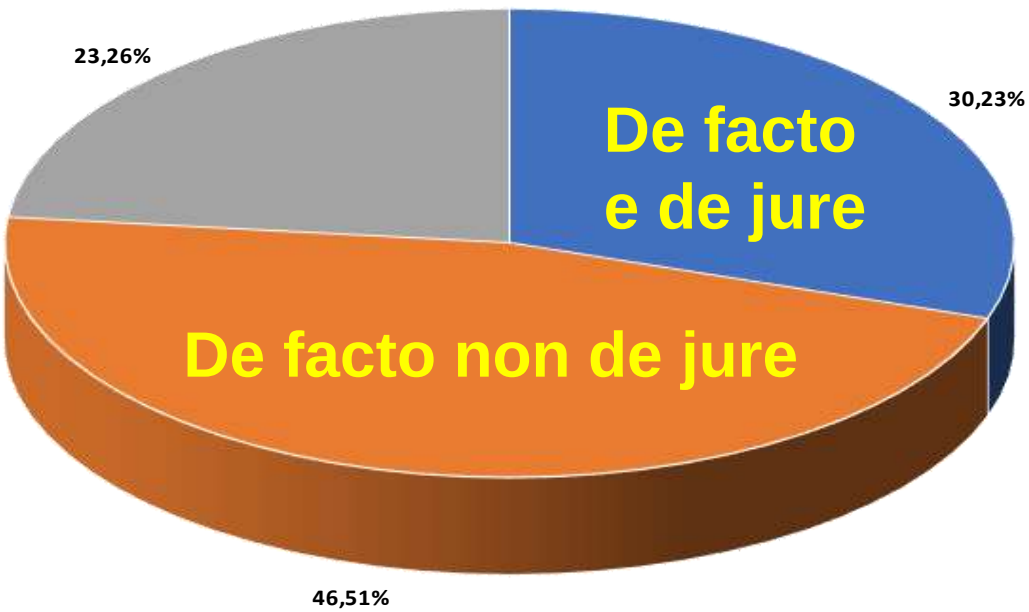
Architettura della sicurezza digitale nei sistemi informatici dei rispondenti (risposte multiple)



Affidabilità, disponibilità e gestibilità del sistema informatico del rispondente (risposte multiple)



Il ruolo del Responsabile della sicurezza digitale, CISO, nella organizzazione dell'azienda/ente dei rispondenti



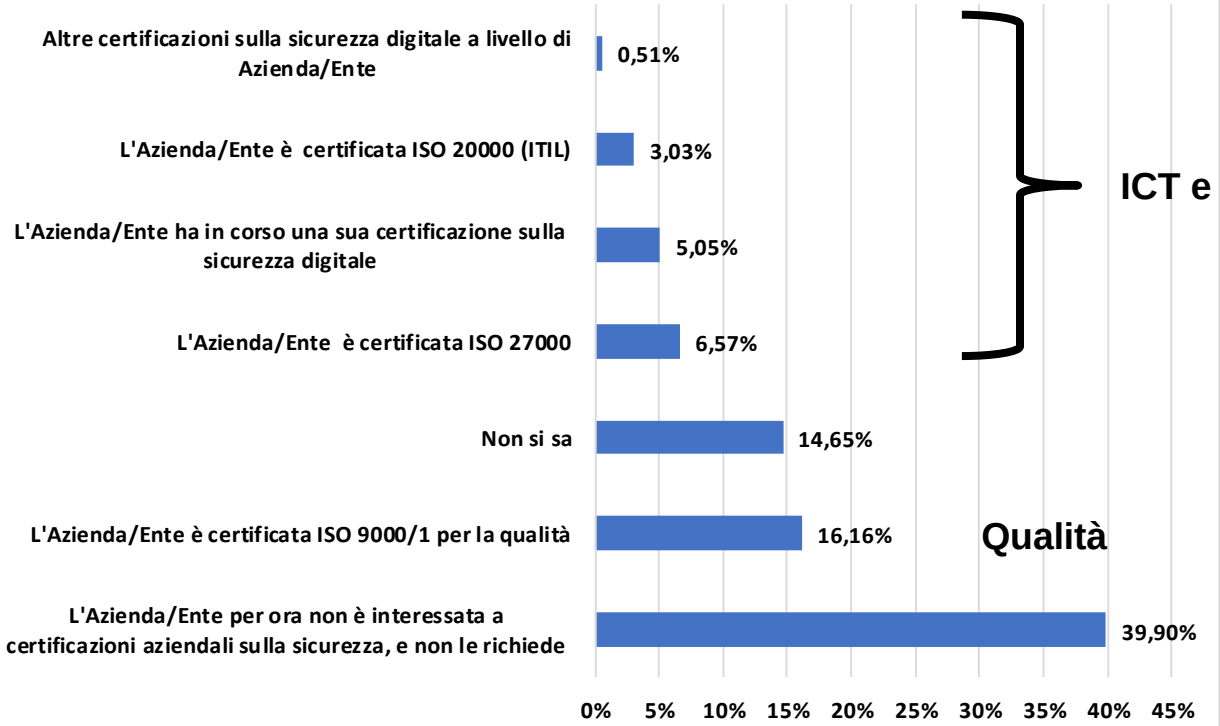
Il problema delle effettive competenze sulla sicurezza digitale

Condizione necessaria, ma non sempre sufficiente, è fare riferimento a:

- professionisti **certificati**
- **Iscritti** ad **Associazioni** professionali **qualificate**

- La sicurezza digitale è **multi-disciplinare** e richiede una vasta gamma di competenze e di esperienza sul campo
- Difficilmente un'Azienda/Ente può avere al proprio interno specifiche e aggiornate competenze di sicurezza digitale
- Deve pertanto terziarizzare gran parte (o la totalità) delle decisioni e dell'operatività, e l'unico criterio di scelta è spesso il passa parola ed il costo
- Ma di chi si può fidare? Come può garantirsi sulle reali competenze dei Fornitori e dei Consulenti?

Certificazioni sulla sicurezza digitale (risposte multiple)



Le certificazioni eCF (EN 16234 1:2016)

- **Sono le uniche ad avere valore giuridico** in Italia e in Europa (se erogate da un Ente accreditato Accredia)
    - AIPSI collabora con AICA, Ente Certificatore accreditato
- possono valorizzare alcune altre **certificazioni indipendenti**
- si basano sulla **provata esperienza** maturata sul campo dal professionista
- qualificano il professionista considerando **l'intera sua biografia professionale** e le competenze ed esperienze maturate nella sua vita professionale (e non solo per aver seguito un corso e superato un esame)
- Per la sicurezza digitale eCF prevede due profili:
    - Security Specialist
    - Security Manager

Grazie dell'attenzione

m.bozzetti@aipsi.org

www.aipsi.org

www.oadweb.it

www.malaboadvisoring.it