CAMERA DI COMMERCIO
TREVISO - BELLUNO | DOLOMITI
bellezza e impresa

Belluno, 9 maggio 2019
Treviso, 10 maggio 2019

SICUREZZA DIGITALE
tutto quello che le PMI dovrebbero sapere

Rapporto 2018 dell'Osservatorio Attacchi Digitali (OAD): i rischi digitali da cui difendersi

Marco R. A. Bozzetti

Presidente AIPSI, Capitolo Italiano ISSA
Ideatore e realizzatore OAD
CEO Malabo Srl

m.bozzetti@aipsi.org
www.aipsi.org
www.oadweb.it
www.malaboadvisoring.it

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

Indice

Osservatorio
Attacchi Digitali
in Italia

L'iniziativa OAD

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

2018
10 anni di indagini via web sugli attacchi ai sistemi informatici in Italia

Rapporto 2018 OAD

- 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

Per scaricare il Rapporto 2018 OAD (gratuito):

- Registrarsi a https://www.oadweb.it
- Consenso esplicito privacy
- Scaricare il file in pdf

OAD 2018

SPONSOR

PAT

Con la collaborazione della Polizia Postale e delle Comunicazioni
e con la Prefazione al Rapporto 2018 del Direttore dott.ssa Nunzia Ciardi

Osservatorio Attacchi Digitali in Italia

La separazione tra tipologie e tecniche di attacco da OAD 2018

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

Che cosa è attaccato	Come (tecniche attaccco)						
	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, pharming, hoax,scanning, indagini su Internet, ecc.)	Script e programmi maligni (ransomware, spyware, adware, ..)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	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

Gantt OAD 2019

Da https://www.oadweb.it/it/oad2018/oad-2019.html è **scaricabile la proposta di sponsorizzazione**.

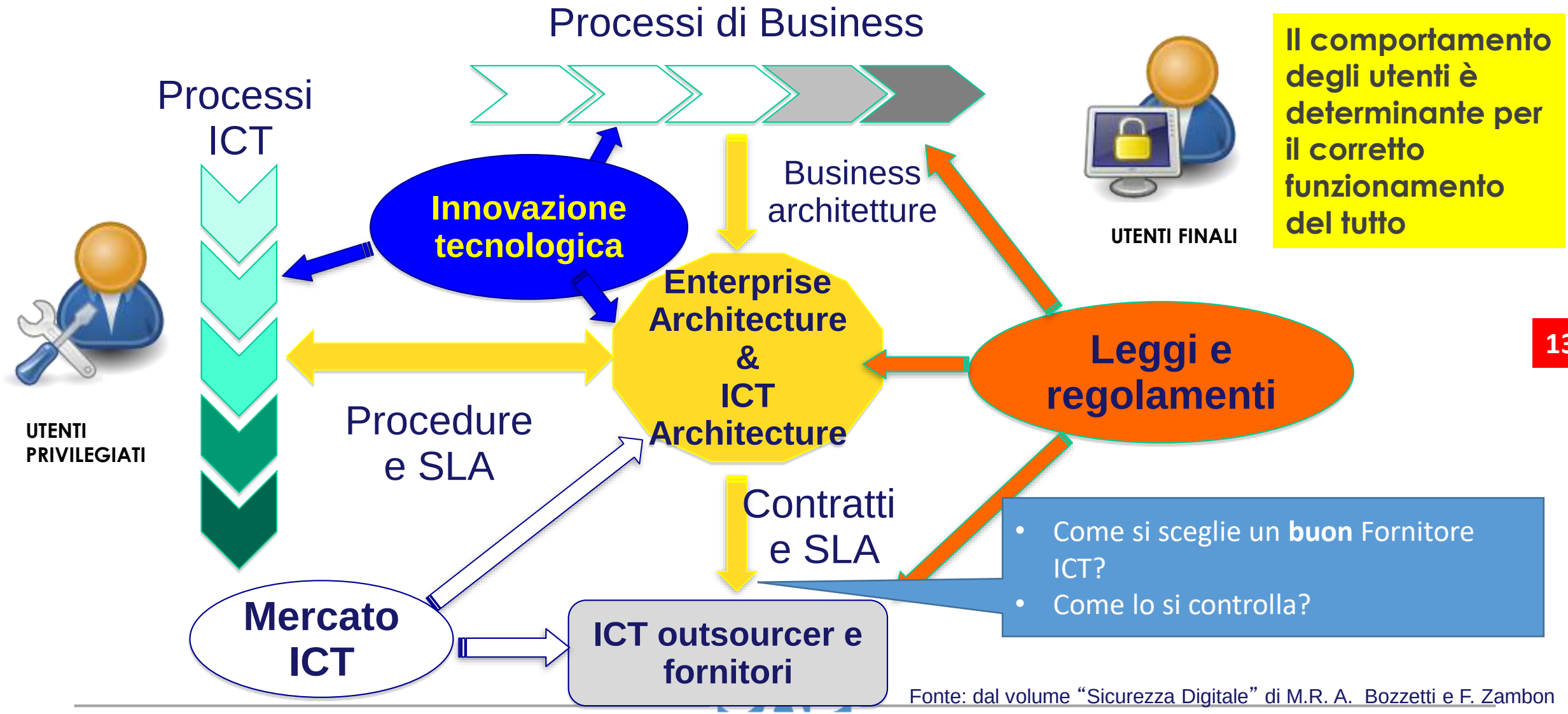
ATTIVITA'	apr-19	mag-19	giu-19	lug-19	ago-19	set-19	ott-19	nov-19	dic-19	1° trim. 2020
Lancio ed inizio OAD 2019										
Acquisizione Sponsor e Patrocinatori										
Creazione Questionario OAD 2019 via web										
Ampliamento e aggiornamento mailing list rispondenti										
Invio invito a compilare il Questionario 2019 OAD via web										
Raccolta risposte al Questionario 2019 OAD via web e loro elaborazione										
Stesura Rapporto 2019 OAD										
Pubblicazione Rapporto 2019 OADe comunicato stampa,										
Creazione pagina web per il download con raccolta dei nominativi di chi lo scarica										
Convegni e workshop per la presentazione generale o settoriale dei risultati raccolti										
Primo elenco di chi ha scaricato il Rapporto 2019 OAD										
Ulteriuori elenchi di chi ha scaricato il Rapporto 2019 OAD										
Iniziative ad hoc per Sponsor Gold e Platinum										

Vulnerabilità ed attacchi digitali per le PMI

Il ruolo del Sistema Informatico (SI) per il business

- Ogni attività si basa ormai su applicazioni del Sistema Informatico
- Il Sistema Informatico non può che operare su Internet, ed è quindi esposto ad attacchi dall'esterno, oltre che dall'interno
- Il corretto, continuo e sicuro funzionamento del Sistema Informatico garantisce:
  - la **continuità operativa** (business continuity)
  - l'integrità dei dati
  - il mantenimento del vantaggio competitivo rispetto ai competitori
  - la compliance alle varie normative: GDPR per la privacy, L. 231, etc.
- Le informazioni del Sistema Informatico sono un **bene (asset) aziendale**, e come tali vanno protette e gestite
- **La sicurezza digitale** non è solo un problema tecnico, ma **di business**, dato che deve garantire la continuità operativa → **deve vedere coinvolto il vertice aziendale**
- Una PMI non può disporre al proprio interno le competenze tecniche ed organizzative per la gestione della sicurezza digitale: **deve terziarizzarle, ma deve controllarle**

Processi, architetture, utenti, terziarizzazioni



Fonte: dal volume "Sicurezza Digitale" di M.R. A. Bozzetti e F. Zambon

Il possibile impatto di un comportamento errato dell'utente

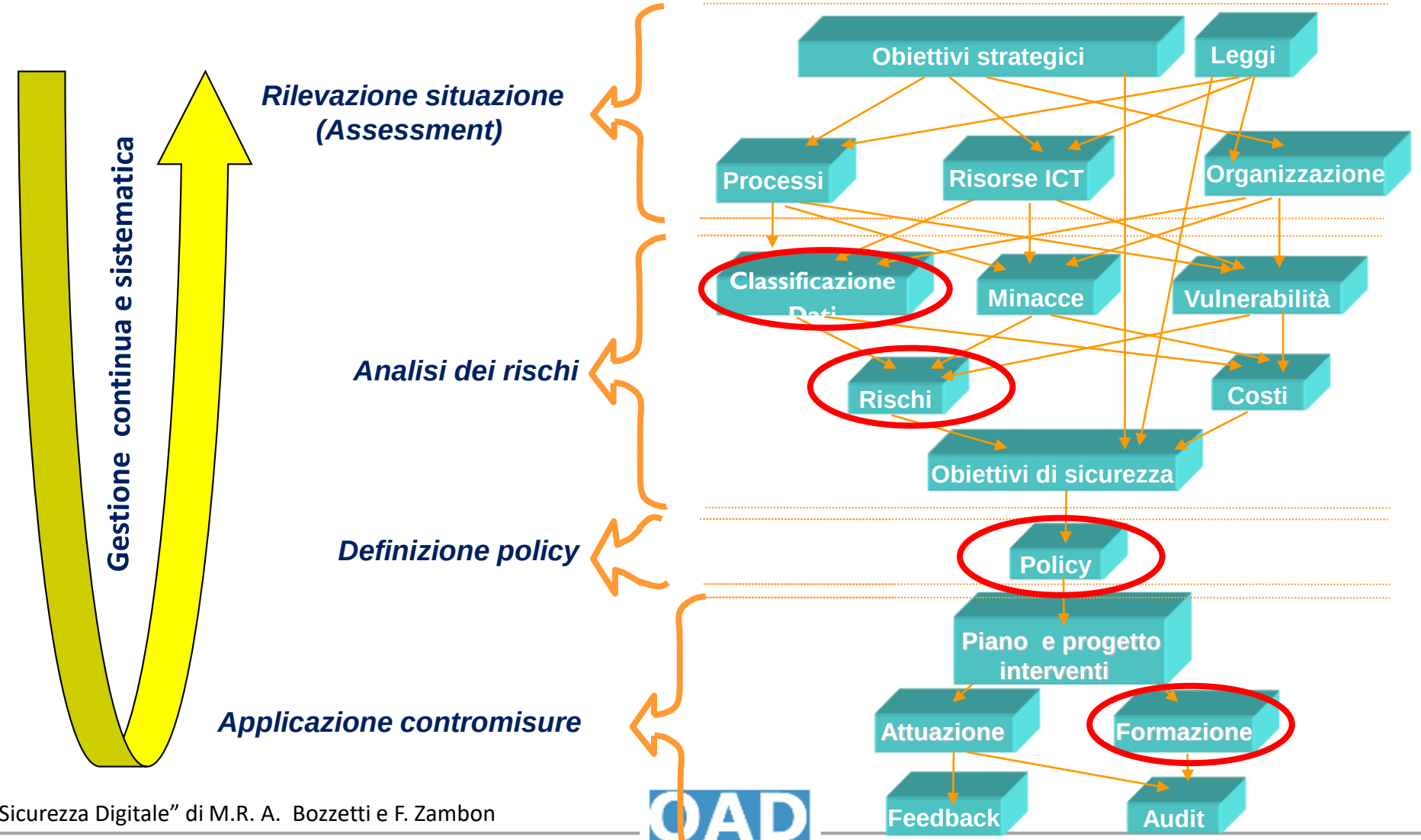
- Il comportamento sbagliato dell'utente può essere:
  - Involontario
  - Volontario
- Qualora un comportamento scorretto dell'utente facesse scattare delle sanzioni per l'azienda/ente, questa può poi **rivalersi sugli utenti che hanno causato la sanzione, o che vi hanno contribuito**.
- Questo vale in particolare per gli utenti privilegiati interni

Attenzione !
Comportamenti sbagliati possono causare sia problemi con l'Azienda sia a livello civile e penale

La sicurezza globale ICT

Fonte: dal volume “Sicurezza Digitale” ed. 2007 di Marco Bozzetti

Il “processo continuo” per la sicurezza ICT

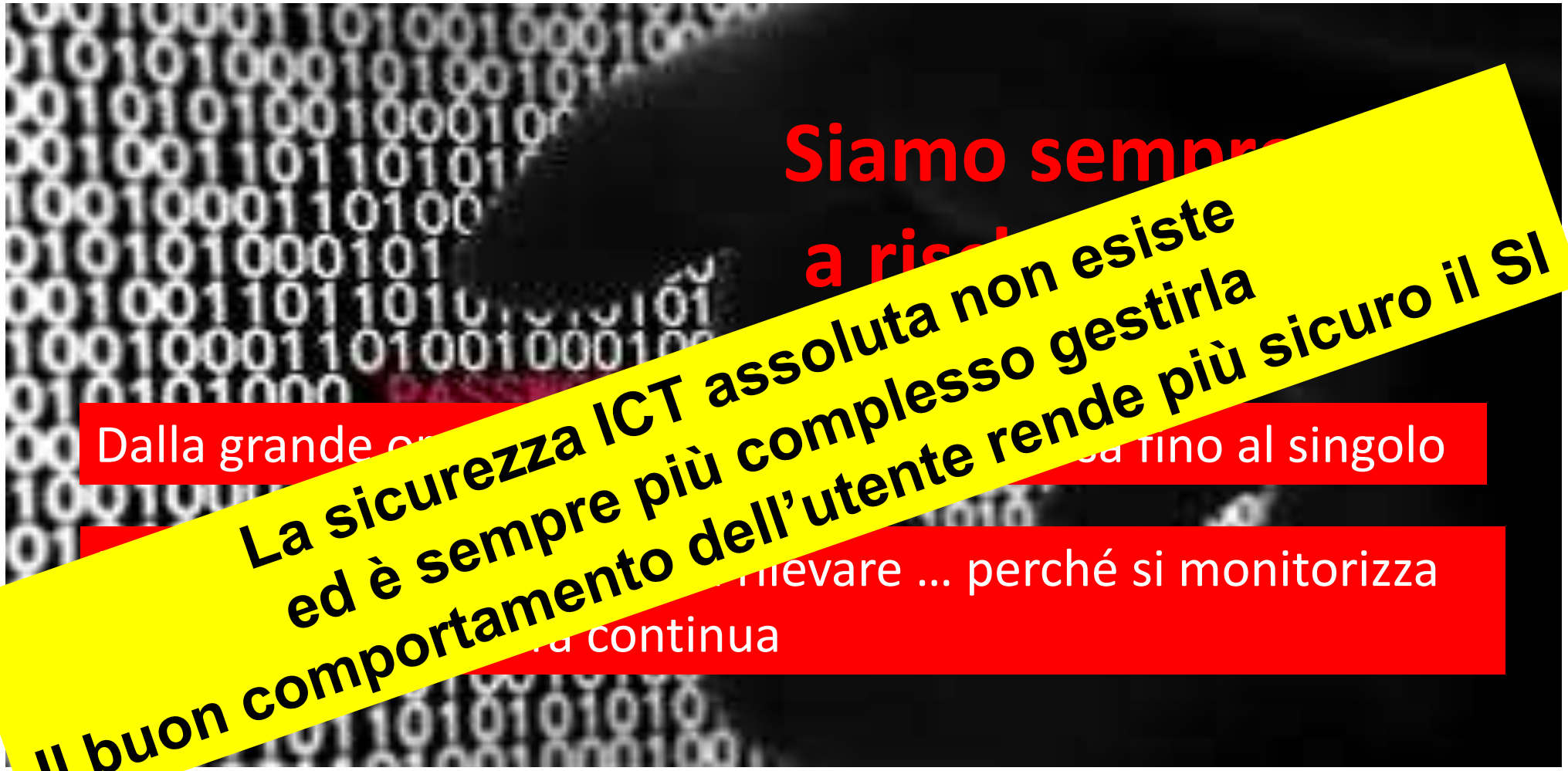


Fonte: dal volume “Sicurezza Digitale” di M.R. A. Bozzetti e F. Zambon

Sistema informatico sicuro …

- La **sicurezza assoluta** NON esiste: occorre essere in grado di gestire eventi e/o attacchi con il minimo del danno per l'azienda/ente
- Attivazione di adeguate e ben bilanciate **misure tecniche ed organizzative**
    - di **prevenzione**, di **protezione**, di **ripristino**
    - a seguito di una contestuale analisi dei rischi, formale o non,
    - e gestendo il tutto come un unico processo continuativo
- Le **vulnerabilità dei sistemi ICT e del personale** (utenti, sviluppatori software, operatori) esistono sempre ..
- Gli **attacchi volontari** possono sempre accadere

Gli attacchi digitali: sempre di più e sempre più critici



aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

CAMERA DI COMMERCIO
TREVISO - BELLUNO | DOLOMITI
bellezza e impresa

Vulnerabilità cause 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):

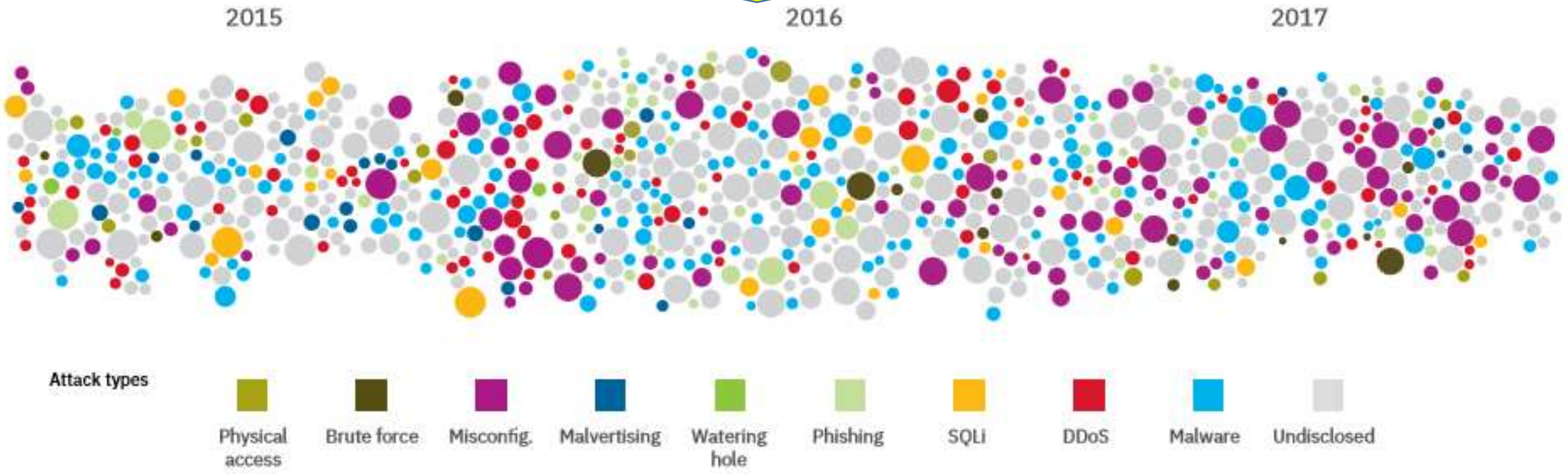
- **Inconsapevolezza**
- **Imperizia**
- **Ignoranza**
- **Imprudenza**
- **Dolo**

Aggravata dalla non o inefficace organizzazione

Mancanza di formazione e addestramento

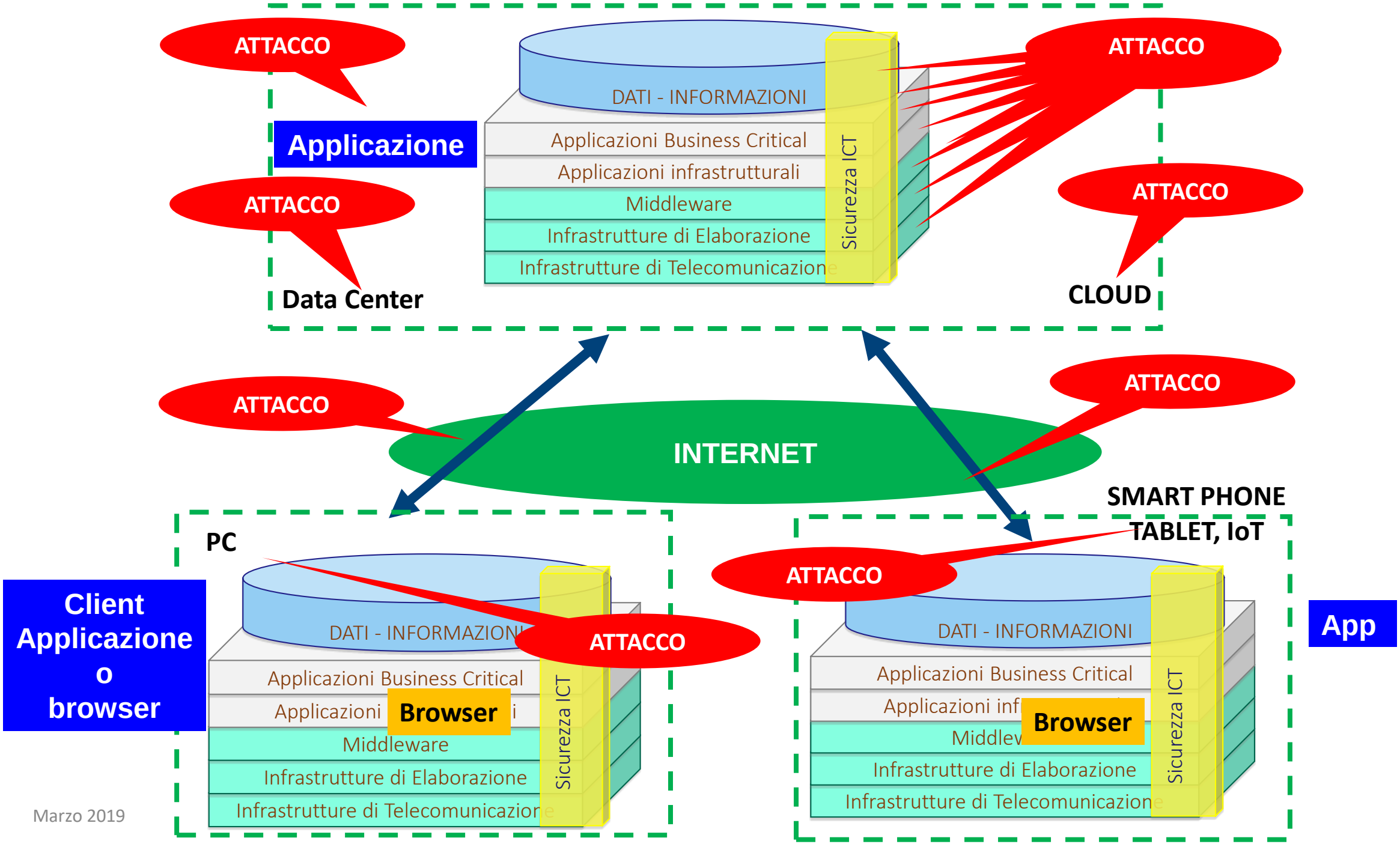
Attacchi 2015-17 per vulnerabilità tecnica a livello mondiale per tipo e durata

Il grigio è il colore più diffuso
→ attacco sconosciuto



Cover Image: Sampling of security incidents by attack type, time and impact, 2015 through 2017.

Fonte: IBM Xforce, aprile 2018


ATTACCO
Applicazione
DATI - INFORMAZIONI
Applicazioni Business Critical
Applicazioni infrastrutturali
Middleware
Infrastrutture di Elaborazione
Infrastrutture di Telecomunicazione
Sicurezza ICT
ATTACCO
ATTACCO
Data Center
ATTACCO
CLOUD
ATTACCO
INTERNET
ATTACCO
SMART PHONE
TABLET, IoT
PC
Client
Applicazione
o
browser
ATTACCO
ATTACCO
Browser
Browser
App

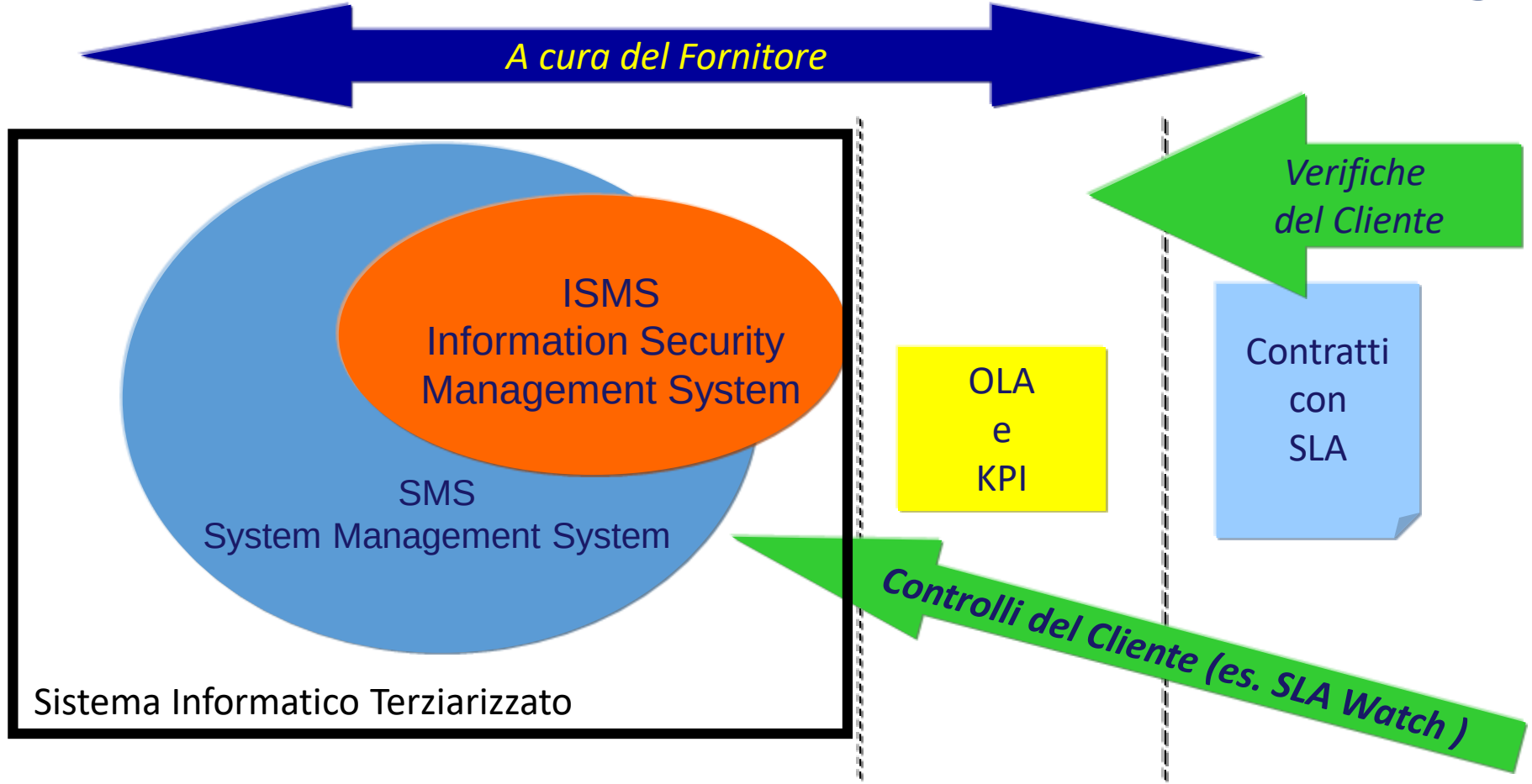
Marzo 2019

Due grandi categorie di attacchi

- **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

Il problema della terziazizzazione ICT e della sua gestione



Monitoraggio e controllo

Rilevazione
ed analisi

Confronto
con
Valori Soglia

Le effettive competenze sulla privacy e sulla sicurezza digitale

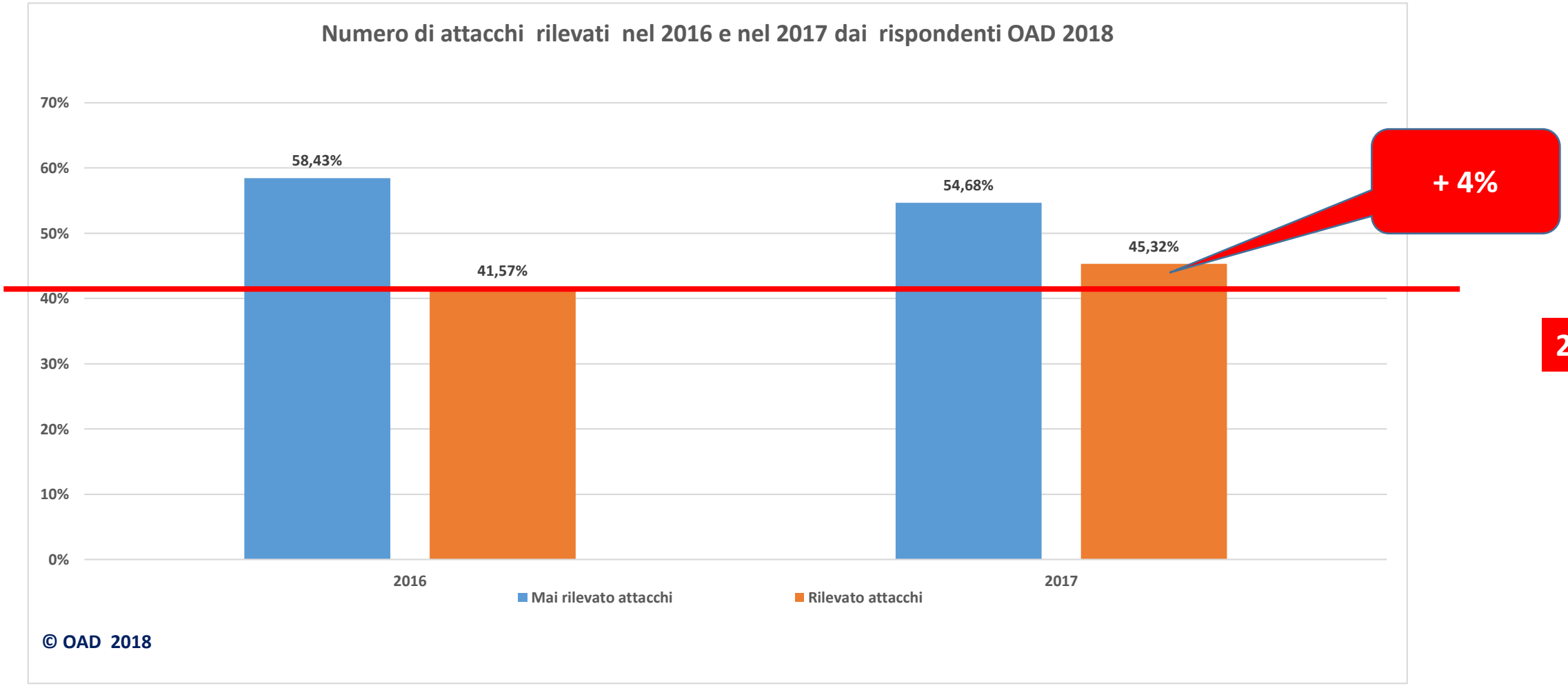
Condizione necessaria, ma non sempre sufficiente, è fare riferimento a:

- professionisti **certificati (es. eCF)**
- **Iscritti** ad **Associazioni** professionali **qualificate**
- Farli controllare periodicamente da terzi che siano totalmente indipendenti dai primi

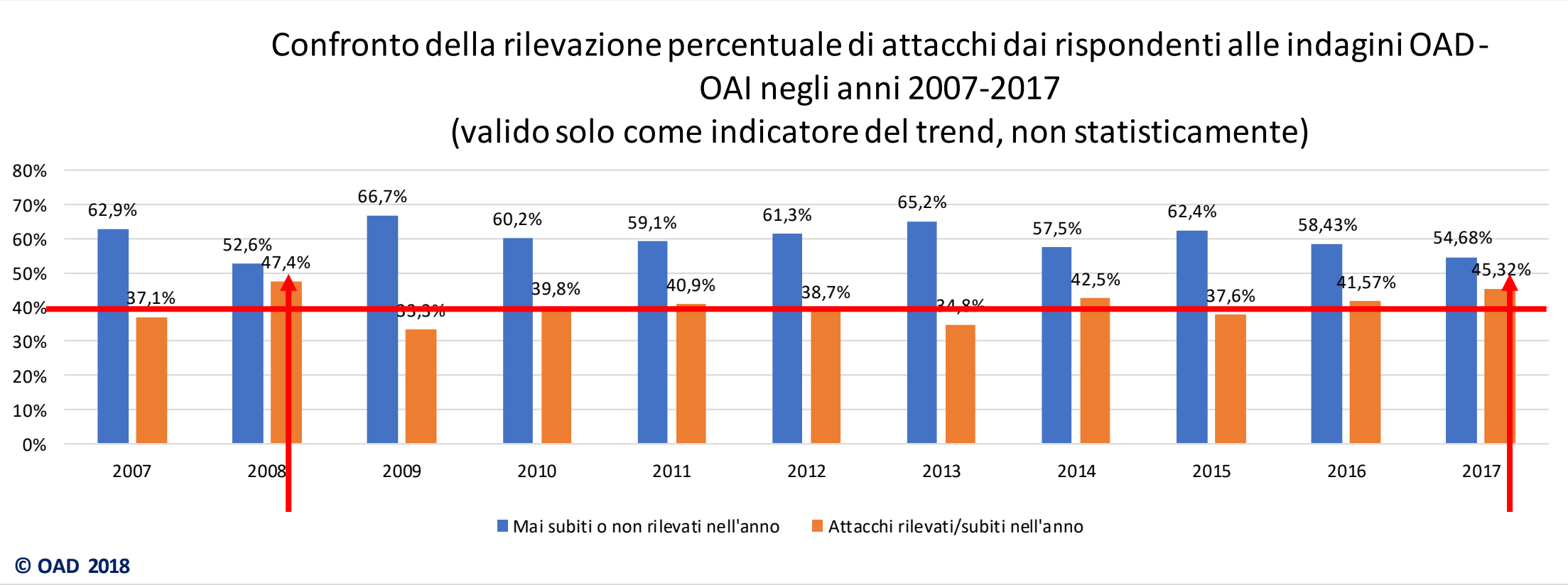
- Privacy e sicurezza digitale sono **multi-disciplinari** e richiedono una vasta ed effettiva gamma di competenze e di esperienza sul campo
- Difficilmente un'Azienda/Ente può avere al proprio interno specifiche e aggiornate competenze di privacy e sicurezza digitale
- Deve pertanto terziarizzare gran 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 l'azienda si può fidare? Come può garantirsi sulle reali competenze dei Fornitori e dei Consulenti?

Gli attacchi digitali intenzionali rilevati nel Rapporto 2018 OAD

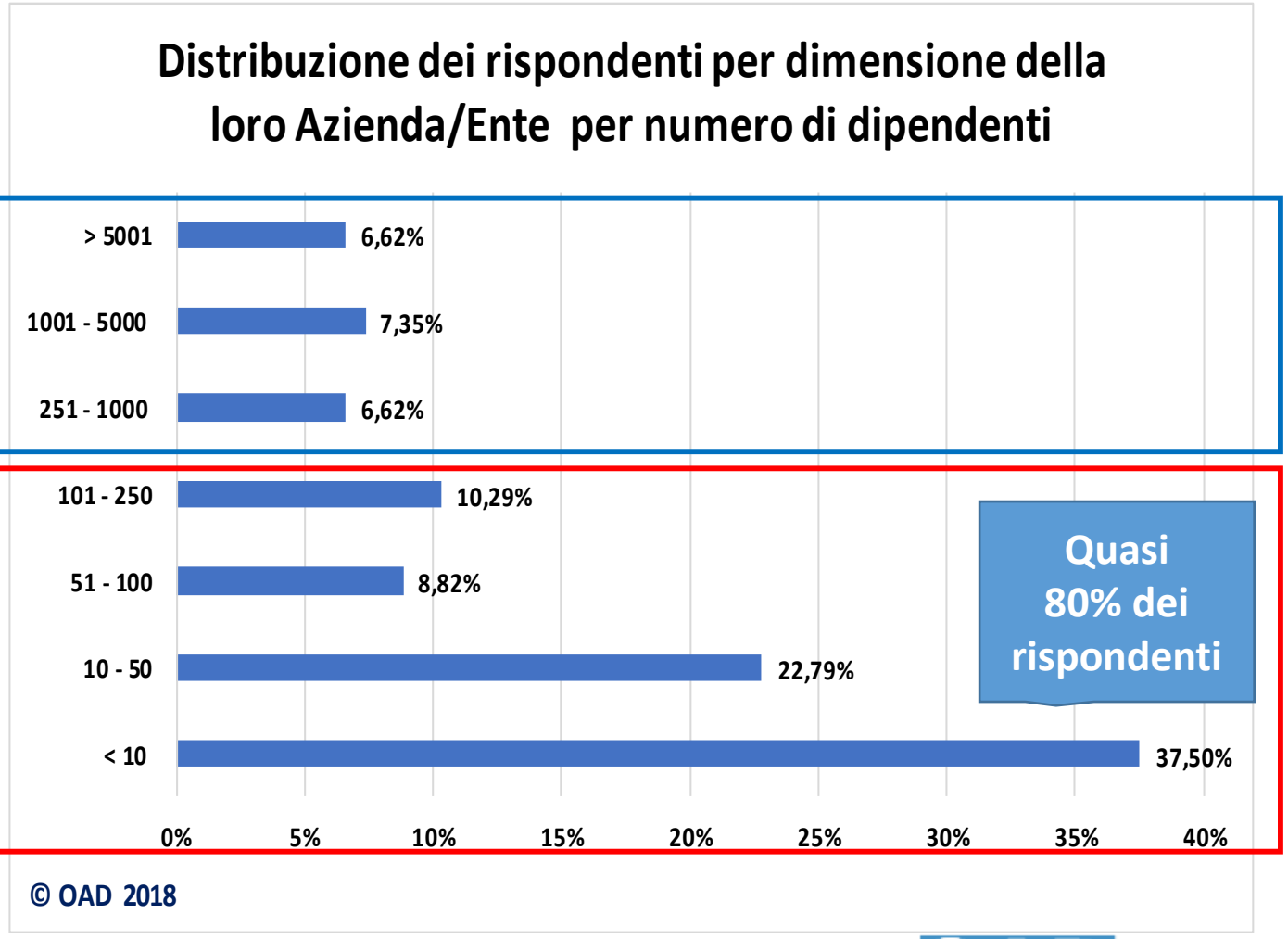
OAD 2018: attacchi rilevati 2016-17



Un indicatore di confronto 2007-2017



OAD 2018: rispondenti per dimensioni azienda/ente



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.

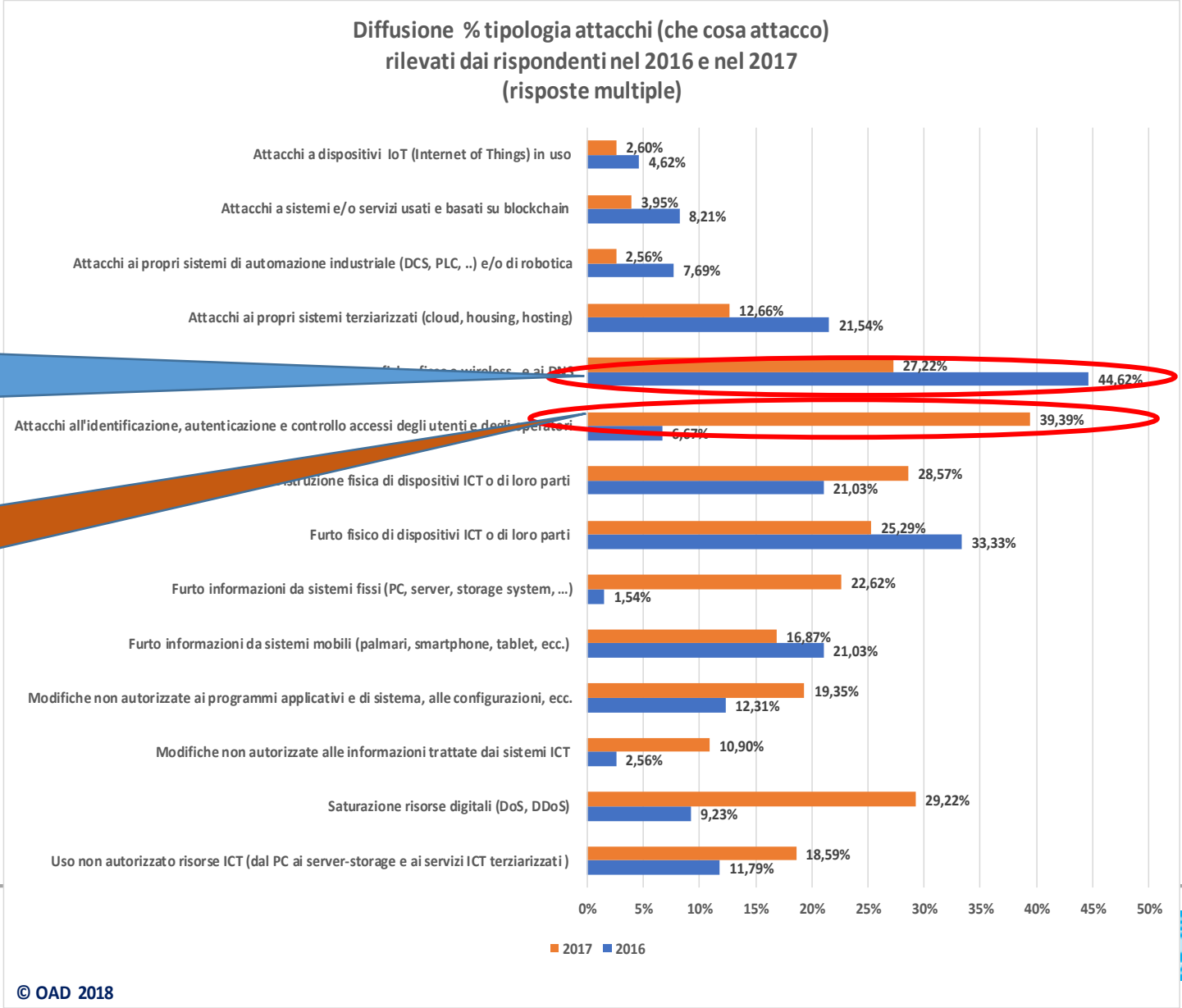
Pubbliche Amministrazioni:

- Circa **55.000**

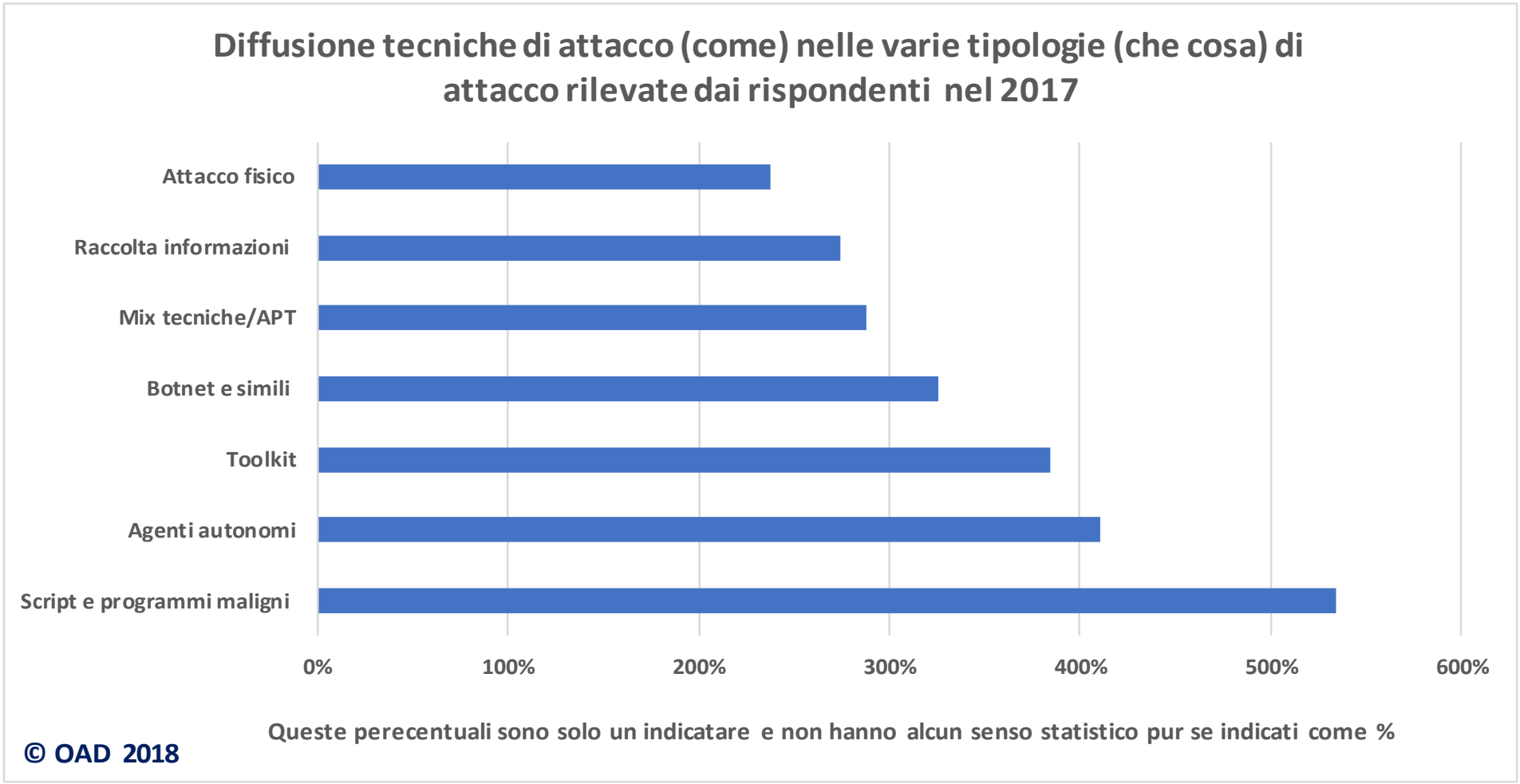
OAD 2018: diffusione tipologia attacchi rilevati 2016-17

2016
Attacchi alle reti
44,62% risp.

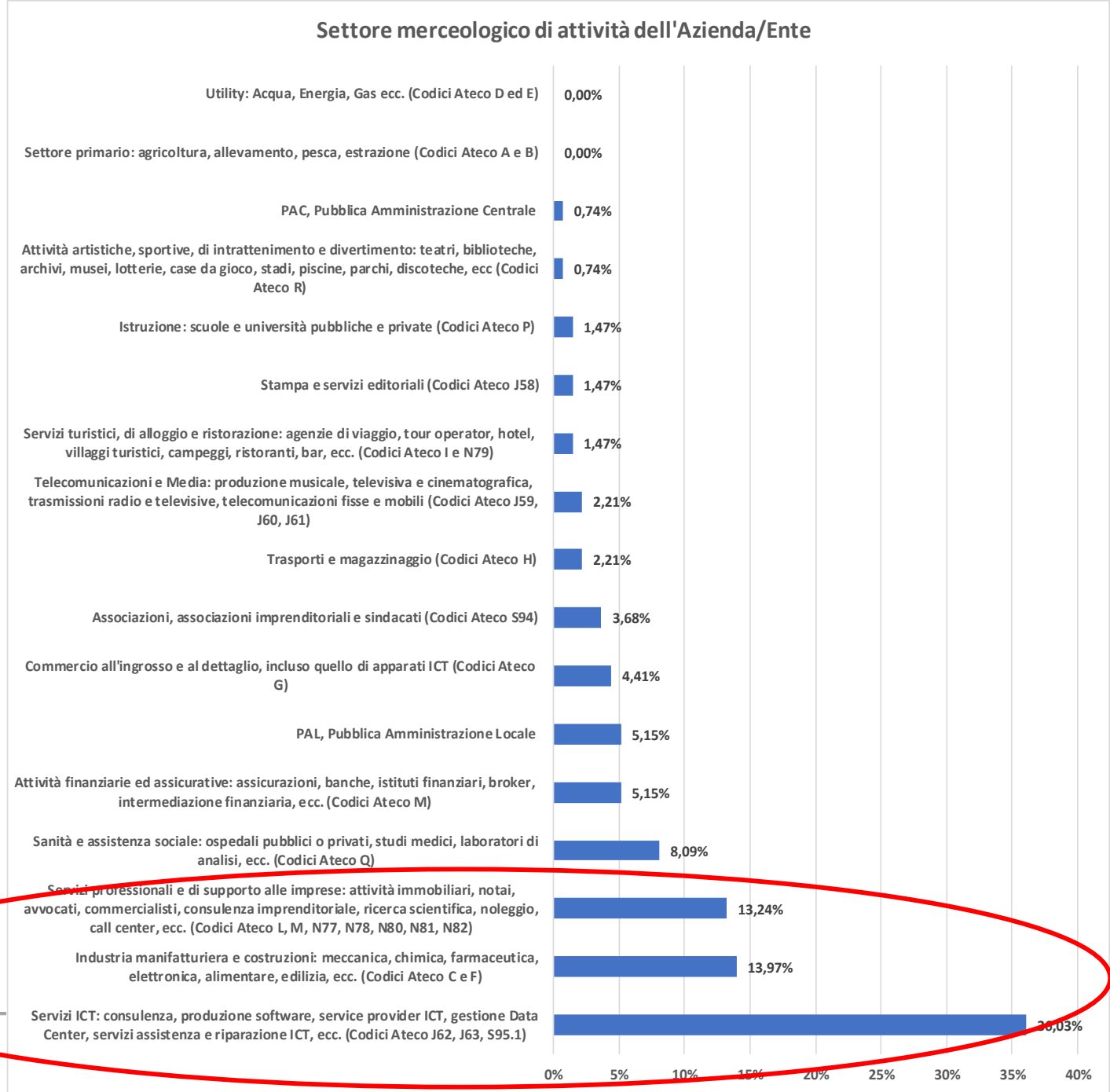
2017
Attacchi IAA
33,39% risp.



OAD 2018: diffusione tecniche di attacco 2017



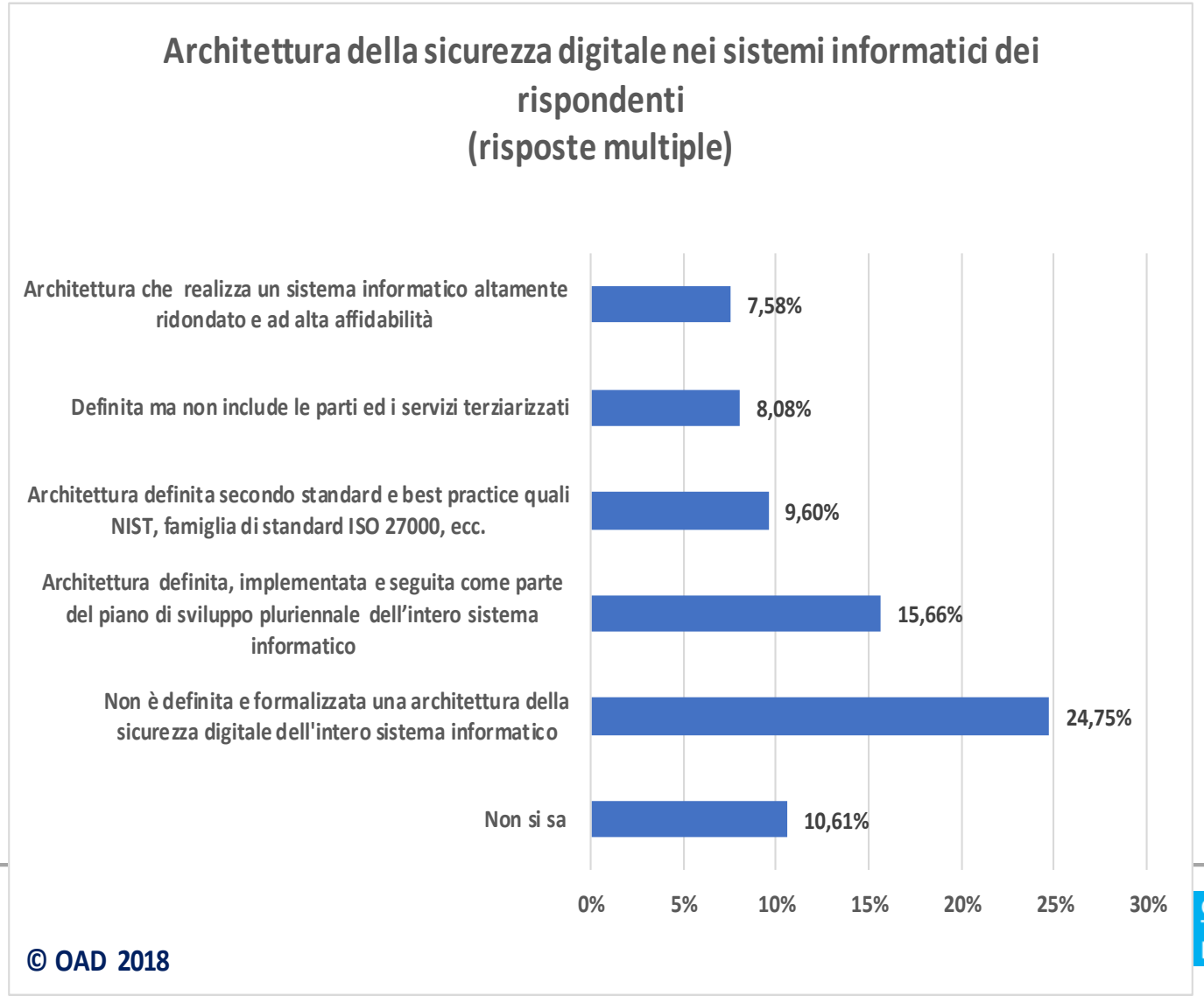
OAD 2018: settore merceologico aziende/enti dei rispondenti



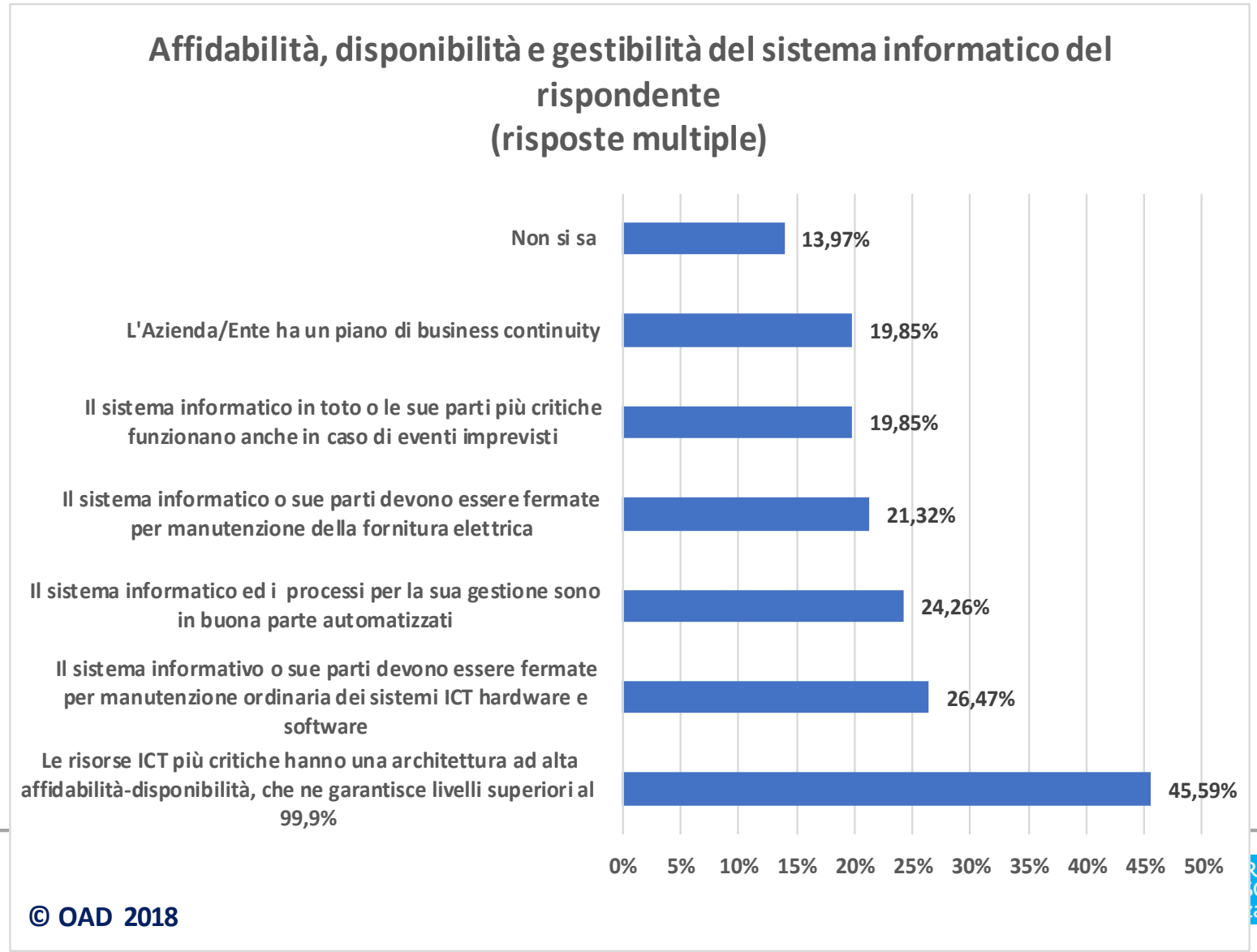
OAD 2018: le misure di sicurezza digitale delle aziende/enti dei rispondenti

- **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, stretta separazione di ruoli anche con Terze Parti
  - 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)

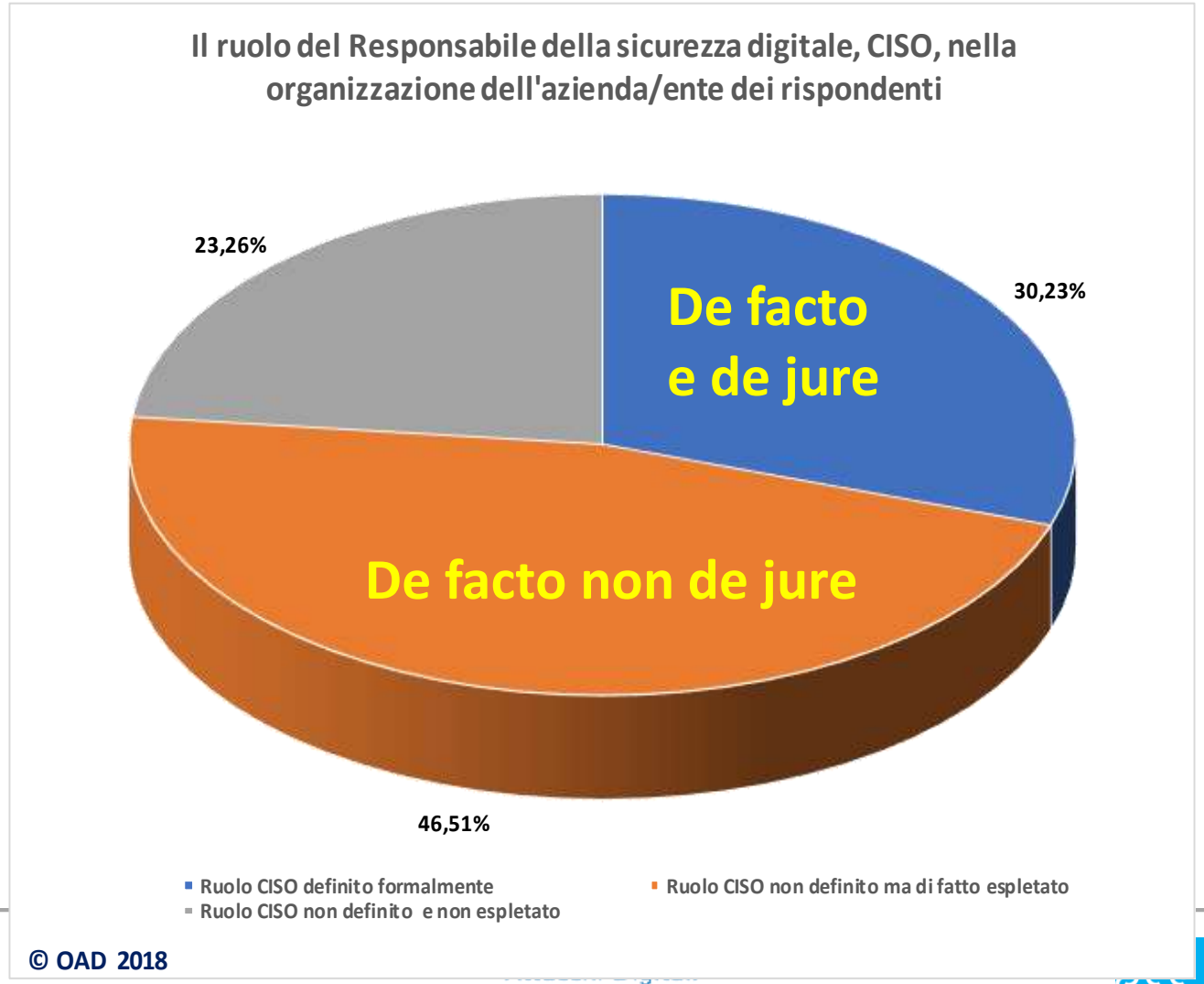
OAD 2018: architettura sicurezza digitale nei SI delle aziende/enti dei rispondenti



OAD 2018: livello sicurezza digitale dei SI delle aziende/enti dei rispondenti

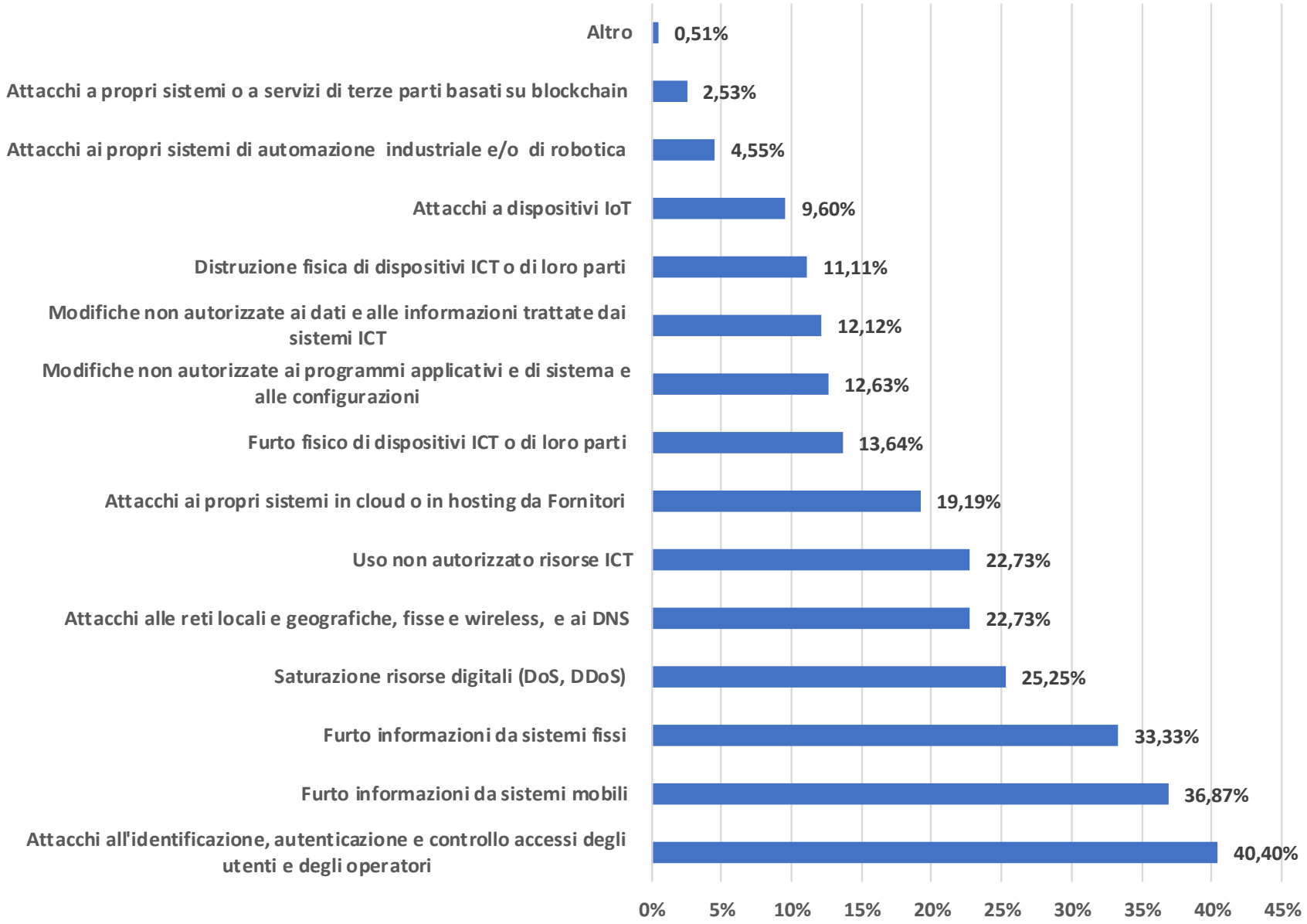


OAD 2018: CISO nella organizzazione per la sicurezza digitale delle aziende/enti dei rispondenti

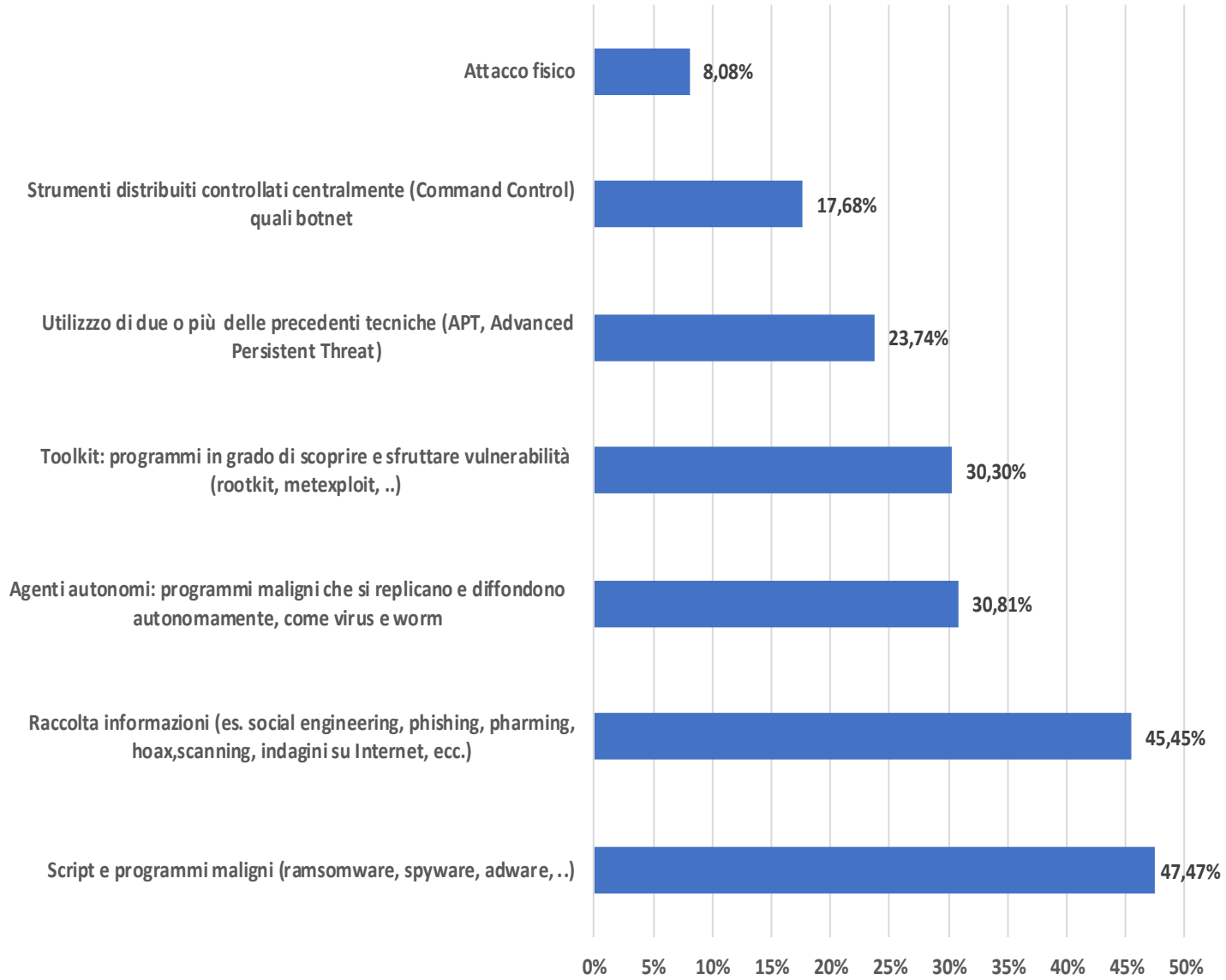


© OAD 2018

Tipologia attacchi (che cosa) più temuti nel prossimo futuro (risposte multiple)



Tecniche di attacco (come) più temute nel prossimo futuro (risposte multiple)



OAD 2018: dati Polizia Postale - 1

C.N.A.I.P.I.C. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Protezione strutture critic	gen – 31 dic 201	gen – 31 dic 2016	Differenza %
Attacchi rilevati	1032	844	**22,27%**
Alert diramati	31524	6721	**369,04%**
Indagini avviate	72	70	**2,86%**
Persone arrestate	3	3	**0,00%**
Persone denunciate	1316	1226	**7,34%**
Perquisizioni	73	58	**25,86%**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	83	85	**-2,35%**

Indagini/ attacchi 6,89%

Indagini/ attacchi 8,29%

Arresti/ denunce 0,23%

Arresti/ denunce 0,24%

OAD 2018: dati Polizia Postale - 2

Financial Cyber Crime

Financial Cyber Crime	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Transazioni Fraudolente Bloccate in €	€ 20.839.576,00	€ 16.050.812,50	**29,84%**
Somme Recuperate	€ 862.000,00	=	
Arrestati	25	25	**0,00%**
Denunciati	2851	3772	**-24,42%**

Arresti/ denunce 0,88%

Arresti/ denunce 0,66%

Cyber Terrorismo

Cyber Terrorismo	1 gen – 31 dic 2017	gen – 31 dic 2016	Differenza %
Arrestati	4	2	**100,00%**
Denunciati	18	9	**100,00%**

Arresti/ denunce 22%

Arresti/ denunce 22%

GRAZIE DELL' ATTENZIONE
e …

- Seguite le iniziative AIPSI e, se interessati, diventati Soci
- Scaricate il Rapporto 2018 OAD
- Rispondete al prossimo Questionario 2019 OAD (check annunci sul sito OAD e sul sito AIPSI)

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

CAMERA DI COMMERCIO
TREVISO - BELLUNO | DOLOMITI
bellezza e impresa