Webinar AIPSI OAD 14/01/2021 ore 18

L'impatto della pandemia Covid-19 sulla cybersecurity di Aziende ed Enti in Italia – Considerazioni dal Rapporto 2020 OAD

I principali dati emersi da OAD 2020 ed il nuovo Progetto *OAD Extended* 2021-22 nel Piano Strategico *Repubblica Digitale*

A cura di: Marco R. A. Bozzetti
(m.bozzetti@aipsi.org)

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- Associazione apolitica e senza fini di lucro → https://www.aipsi.org/
- **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org) che conta >>12.000 Soci, la più grande associazione no-profit di professionisti della Sicurezza ICT nel mondo
- **Obiettivo principale**: aiutare i propri Soci 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
  - Rapporti annuali e specifici; esempi:
    - Rapporto annuale **OAD** nel sito **https://www.oadweb.it**
    - **Rapporto 2020 AIPSI CSWI, Cyber Security Women Italy**
    - ESG ISSA Survey "The Life and Times of Cyber Security Professionals"
    - Position Paper AIPSI **su** Bozza Linee Guida AgID sul document informatico
  - Servizio **AIPSIAlert**
  - Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e supporto alle certificazioni, in particolare **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale
    - **AIPSI Giovani**
  - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
  - Gruppo Specialistico di Interesse **CSWI,** aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI) → **nuova indagine 2021**

2

OAD 2020

12 anni consecutivi di indagini via web sugli attacchi digitali intenzionali ad aziende/enti in Italia

Rapporto OAD 2020

- **Costituito da 186 pagine A4, 148 immagini e grafici, 11 Capitoli (147 pagine A4) e 9 Allegati (39 pagine A4)**
- **Nel Capitolo 11 i dati dalla Polizia Postale e delle Telecomunicazioni, commentati dall'autore**
- **Executive Summary in italiano e in inglese**
- Gold Sponsor: **Cloudflare, Darktrace, Qintesi, Sophos**
- Silver Sponsor:Technology Estate
- Patrocinatori: AICA, AIPSI, AISIS, AITASIT, Anorc, Assi-BO, Assintel, Assolombarda, Aused, CDI Torino, CDTI Roma, Centro Ricerca sulla Scrittura, CIOClub, ClubTI Centro, ClubTI Emilia Romagna, ClubTILiguria, ClubTI Milano, FIDA Inform, Grafobiometristi Italiani Associati, IEEE-Italian Chapter, Inforav.

Scaricabile gratuitamente da:
https://www.oadweb.it/it/oad-2020/per-scaricare-il-rapporto-2020-oad.html

Indice dei contenuti del Rapporto 2020 OAD

Sintesi

Quadro di riferimento attacchi e vulnerabilità digitali

Tipologia attacchi rilevati nel 2019 e nel 1° quadrimestre 2020

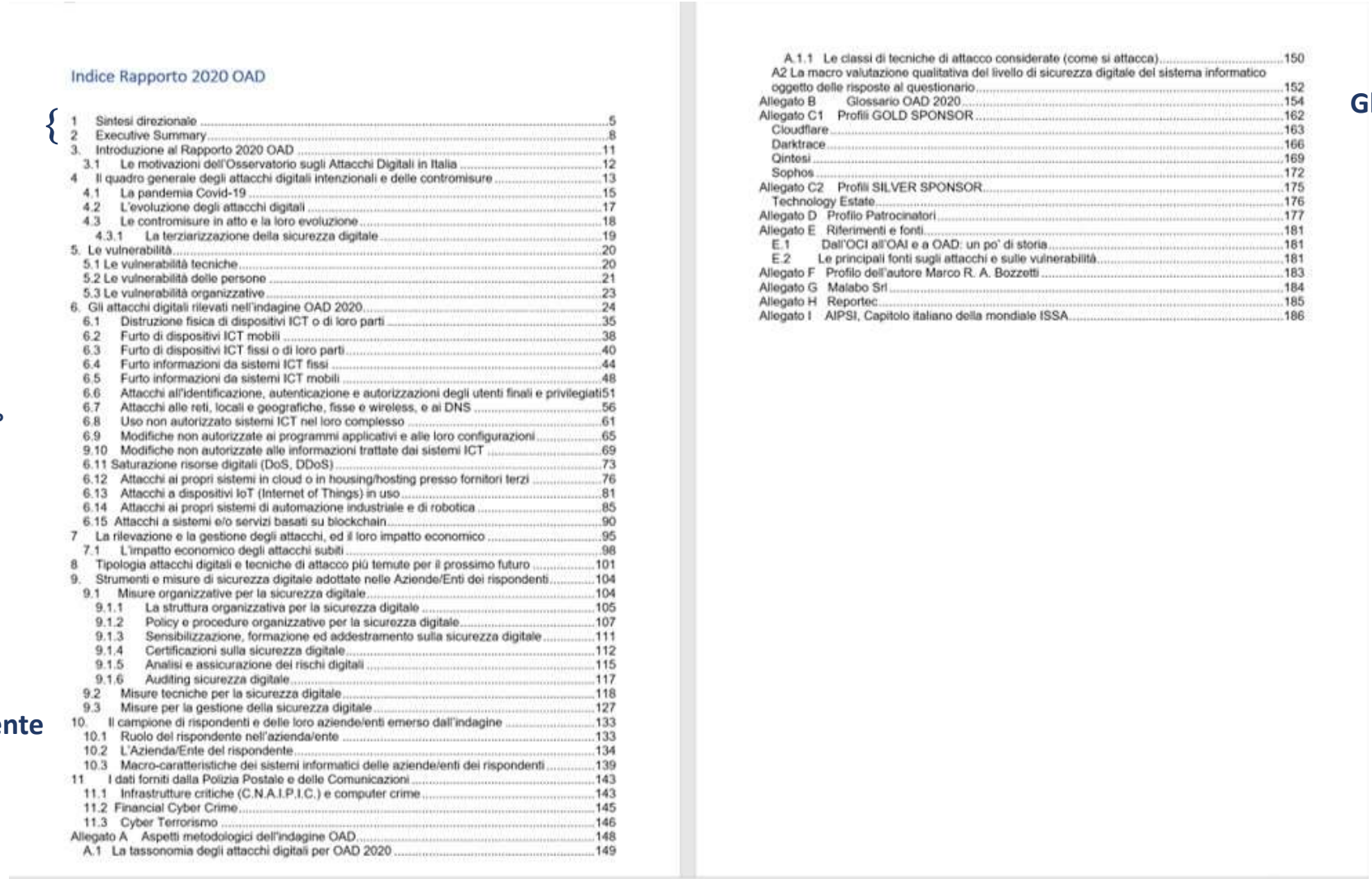
Misure di sicurezza digitale in atto

Dati campione rispondente

Dati Polizia Postale

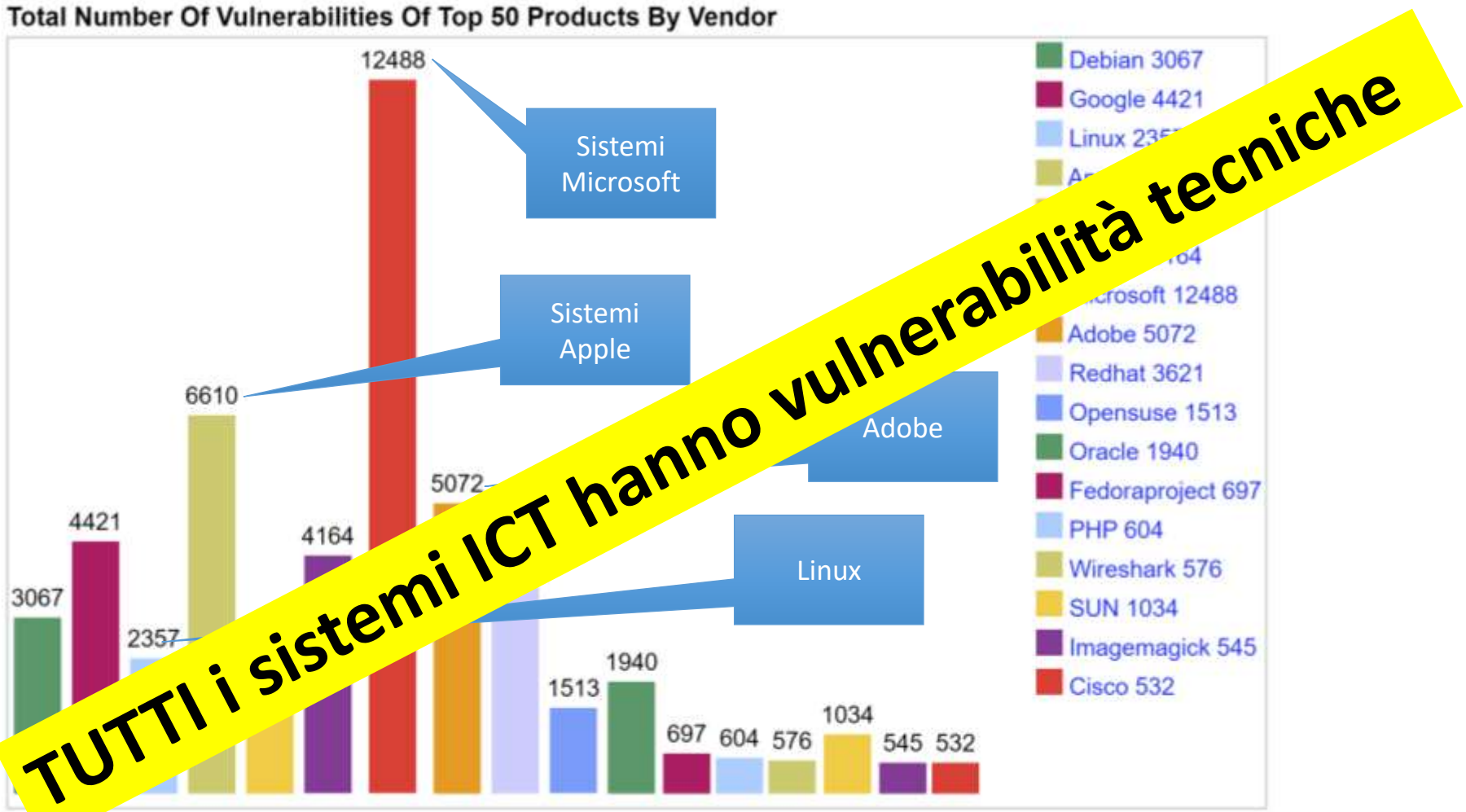
Metodologia OAD 2020

Glossario



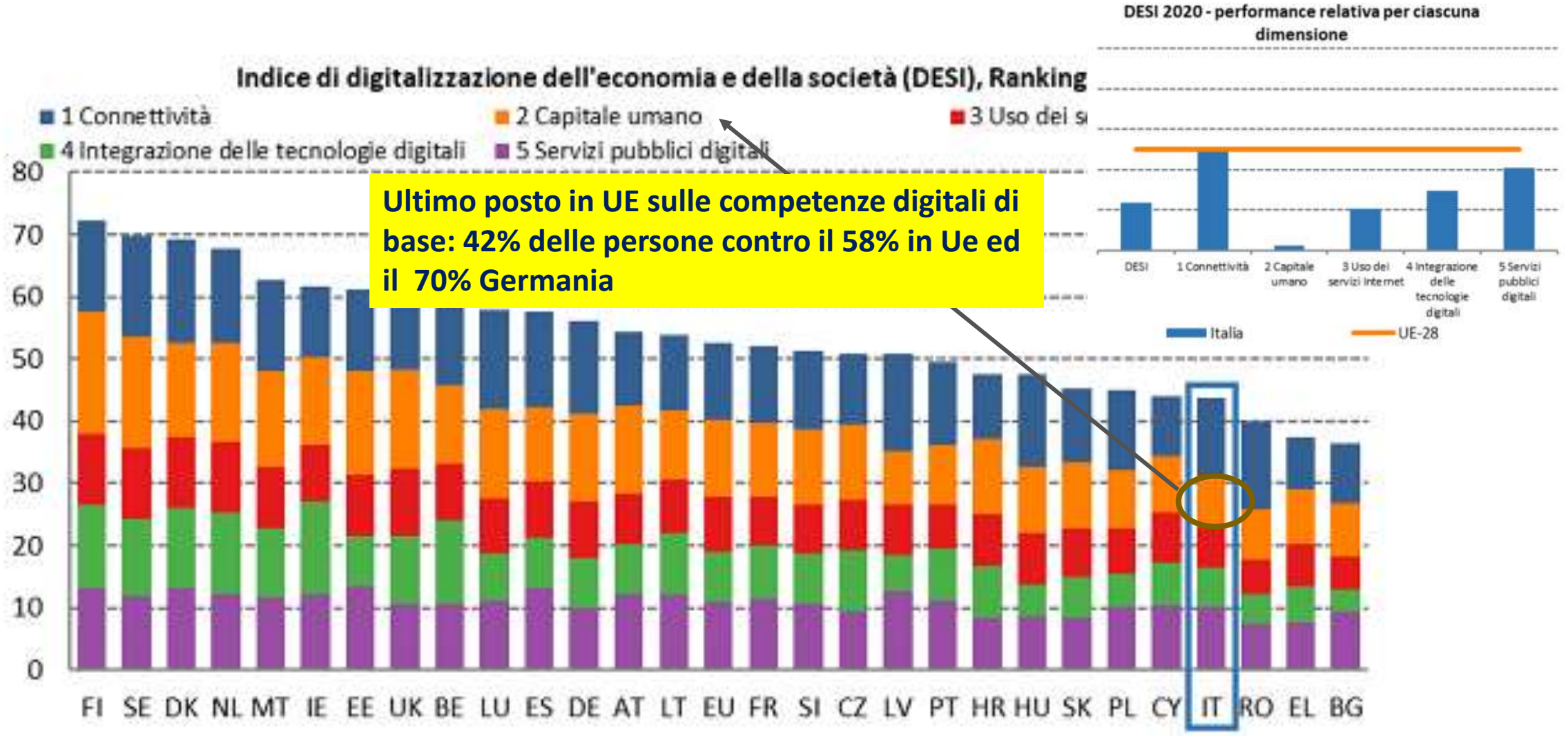
Indice Rapporto 2020 OAD

Vulnerabilità top 50 Vendor da CVE

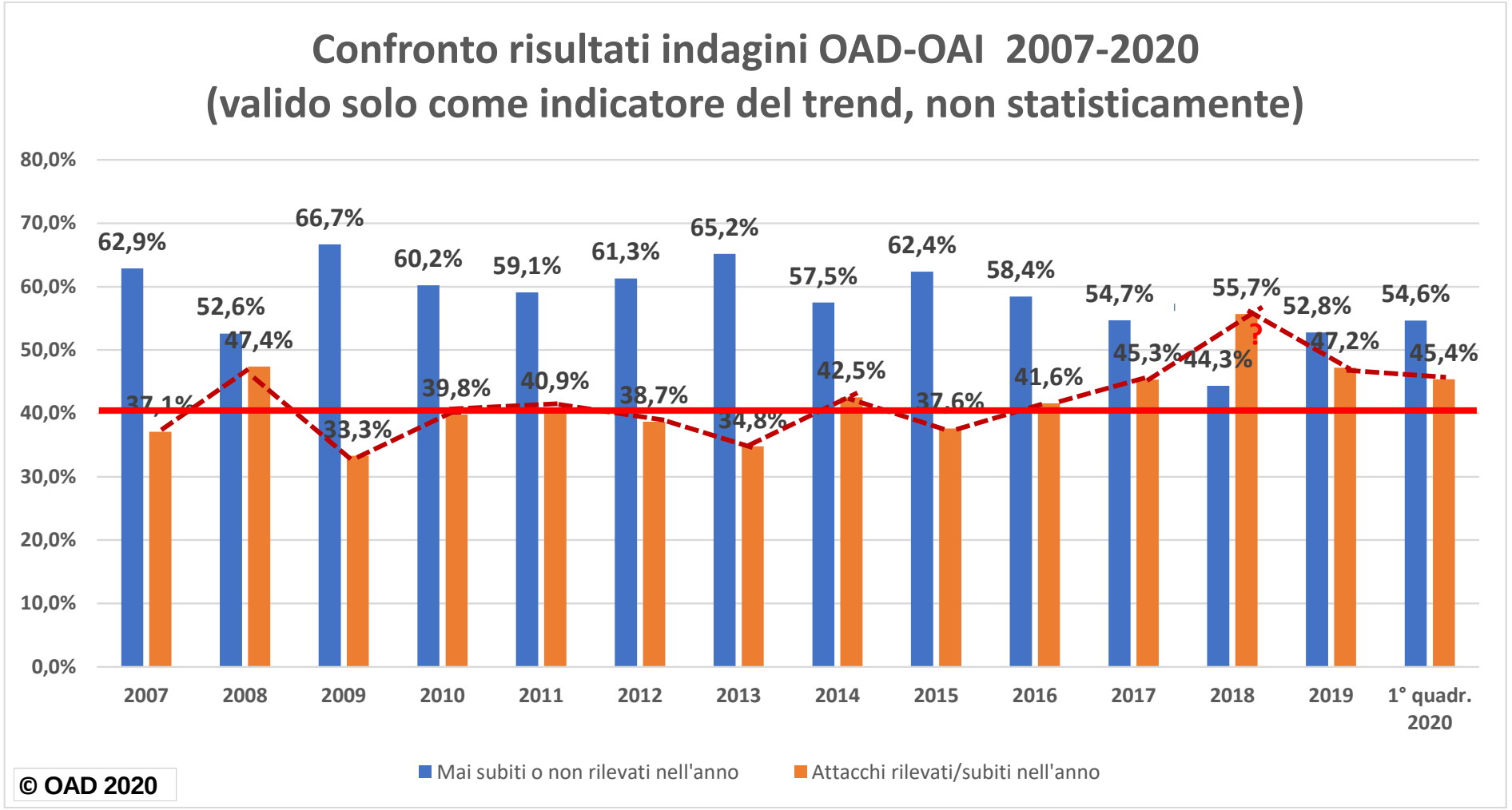


Fonte: CVE Mitre

Indice DESI 2020



Macro Trend attacchi digitali indagini OAD (non statistico)

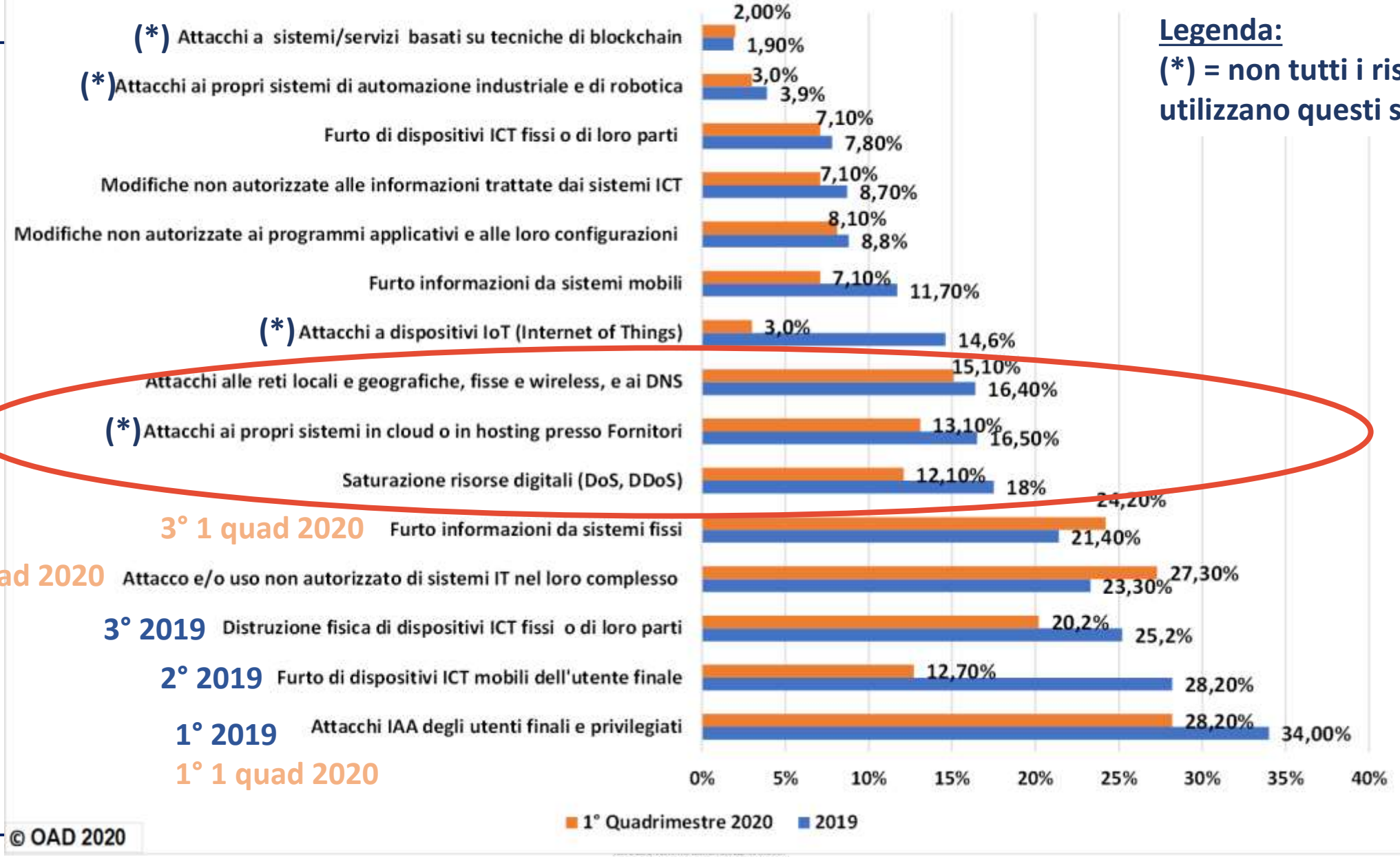


Imprese e PA in Italia vs rispondenti OAD 2020

ISTAT: Imprese private per numero dipendenti	ISTAT 2020 Numero imprese	% sul totale ISTAT 2020	% rispondenti OAD 2020
< 10	4.180.761	94,92%	22,10%
11-49	196.076	4,45%	14,40%
50-249	23.647	0,54%	21,20%
>250	4.017	0,09%	42,30%
Totale imprese censite ISTAT /rispondenti OAD 2020	4.404.501		310
Totale PMI 1-249	4.400.484	99,91%	57,70%

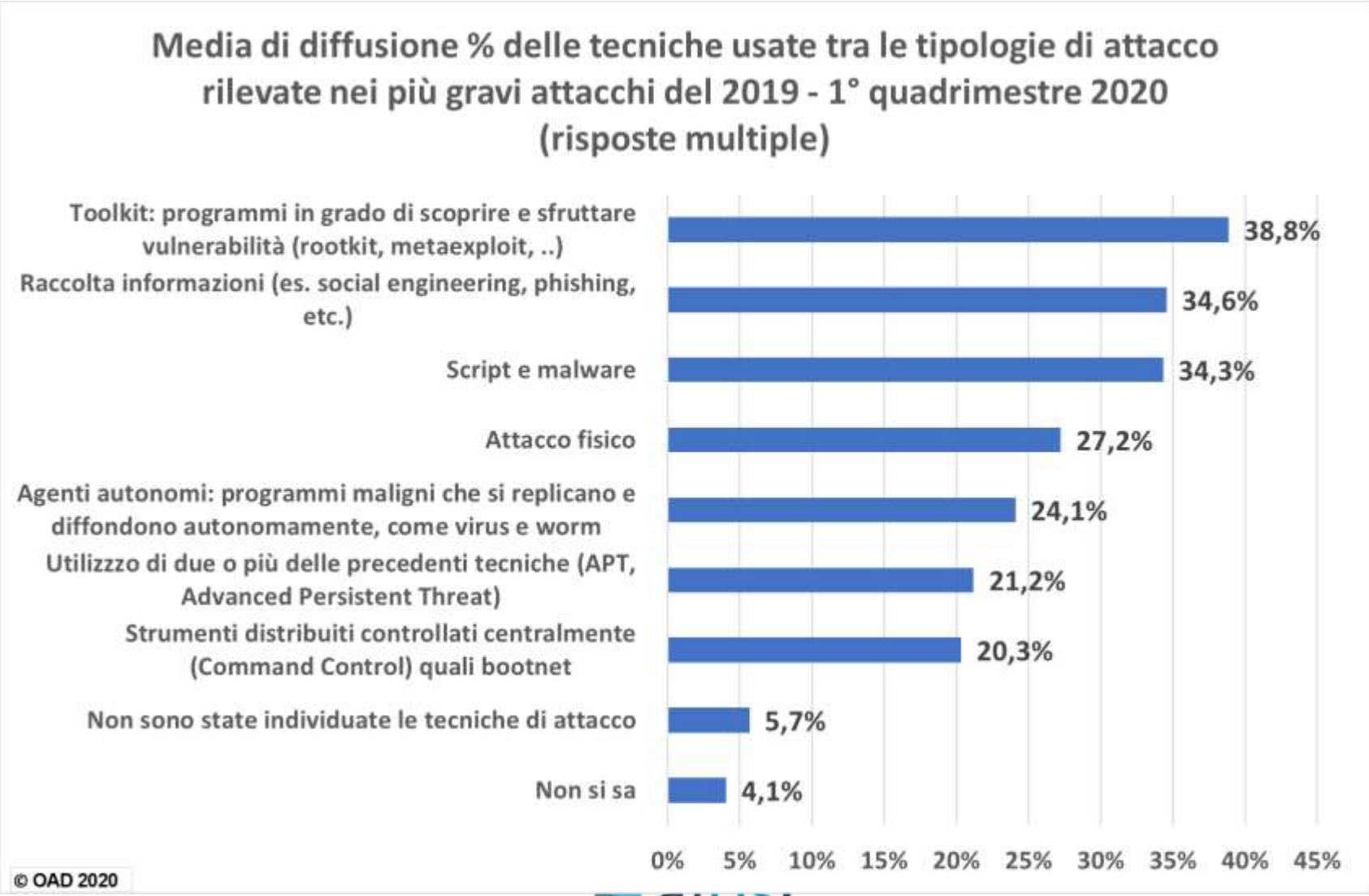
PA: non esistono dati di dettaglio per numero dipendenti di PAC e PAL
La stima più recente del 2015 fa riferimento a circa **55.000 enti pubblici**, sia locali che centrali, con autonome capacità amministrative e finanziarie.
Anche per le PA, e soprattutto per le PAL, **la maggior parte sono di piccole e piccolissime dimensioni**

Diffusione tipologia attacchi digitali ai sistemi informatici dei rispondenti nel 2019 e nel 1° quadrimestre 2020 (risposte multiple)

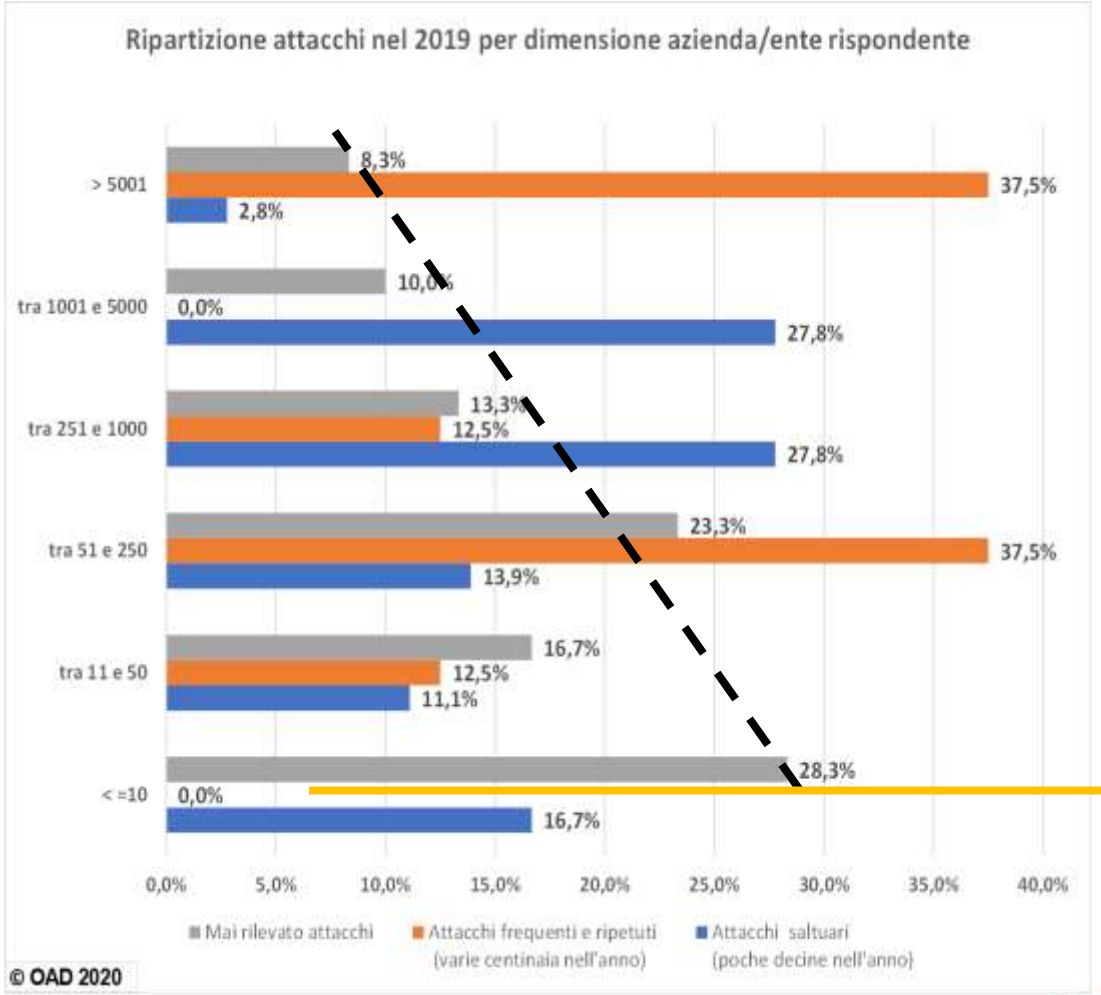


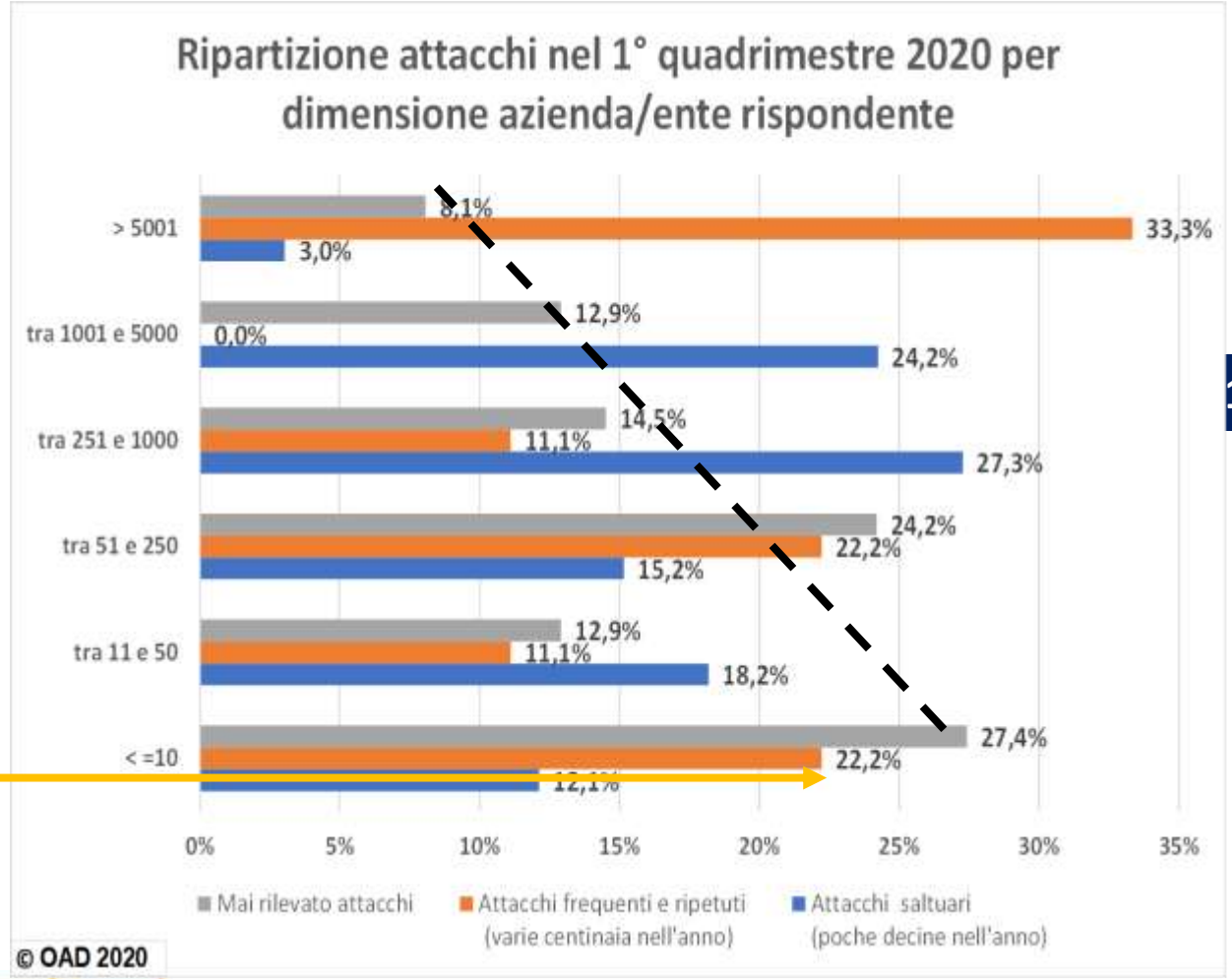
Legenda:
(*) = non tutti i rispondenti utilizzano questi sistemi ICT

OAD 2020: Tecniche di attacco più diffuse



Attacchi digitali per dimensione di Azienda/Ente





Anteprima OAD 2020
sui dati della Polizia Postale (definitivi)

Protezione strutture critiche	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati	282	1181	459	1.032	844
Alert diramati	24.824,00	82.484,00	80.777	31.524	6.721
Indagini avviate	34	155	74	72	70
Persone arrestate	0	3	1	3	3
Persone denunciate	0	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	17	79	108	83	85
Indagini avviate su attacchi rilevati	12,05%	13,12%	16,12%	6,98%	8,29%
Persone arrestate su persone denunciate	0%	2,50%	7,14%	0,23%	0,24%

Financial Cyber Crime	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	€ 20.200.000,00	€ 21.333.990,00	€ 38.400.000,00	€ 20.839.576,00	€ 16.050.812,50
Somme Recuperate	€ 8.700.000,00	€ 18.000.000,00	€ 9.000.000,00	€ 862.000,00	nd
Arrestati	nd	nd	nd	25	25
Denunciati	nd	nd	nd	2.851	3.772
Recupero/frode	43,06%	84,37%	23,44%	4,14%	

Cyber Terrorismo	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	11.962	36.377	36.000
Contenuti rimossi			250

OAD 2020: misure di sicurezza digitale dei rispondenti

Nel complesso nettamente migliorate rispetto alle precedenti indagini OAD

- **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

Migliorate, ma misure di base da potenziare per le PMI

- **Misure organizzative**
  - Struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative
  - Contratti e clausole sicurezza digitale con le Terze Parti (GDPR dovrebbe aiutare!!)
  - **Consapevolezza (awarness) sicurezza digitale a tutti i livelli**
  - Auditing

Migliorate ma ancora carenti nelle PMI

- **Misure di gestione e di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

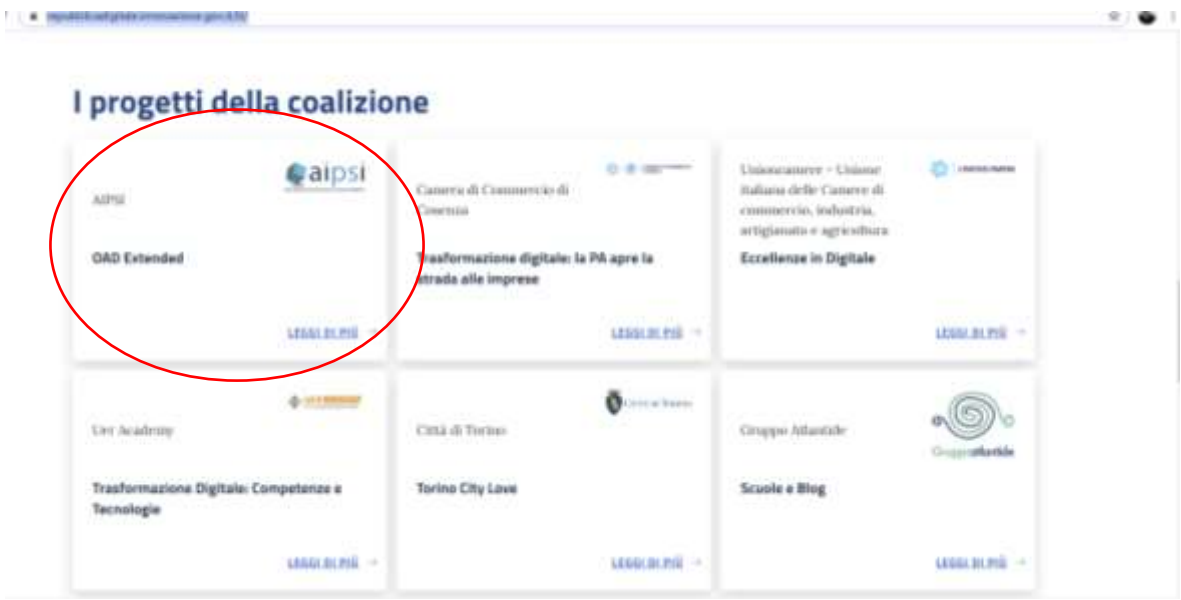
Migliorate ma:
- **Carenti per PMI**
- **Embrionali per le soluzioni più avanzate (AI, ML, etc.)**
- **DR più formale che sostanziale**

AIPSI aderisce a Repubblica Digitale del MID col Progetto OAD Extended (2021-22)

https://repubblicadigitale.innovazione.gov.it/it/

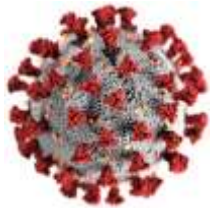
#RepubblicaDigitale
@innovazionegov

@innovazionegov



- **OAD *Extended-PO*** : estendere il bacino di rispondenti/interessati ai vari settori merceologici + PA
- **OAD *Extended-SO*** : nuovo sistema automatizzato e personalizzato, non più anonimo ma a richiesta della singola azienda/ente, in grado di fornire specifiche informazioni di ausilio nell'assessment del livello di sicurezza del sistema informatico considerato e degli interventi opportuni per migliorarlo

2020: l'impatto di Covid-19 e la *nuova normalità*



- **Gravissimi impatti economici** soprattutto per PMI ed i piccoli enti
  - Si sacrifica ancor più la sicurezza (e la trasformazione) digitale a medio-lungo termine alla flessibilità ed agilità a breve termine
- **Nuovi rischi derivati dal fenomeno pandemia:**
  - **Esplosione agile work**
    - Occorre modificare i diritti d'accesso ai sistemi e alle applicazioni aziendali, non più da locale ma da remoto, il più delle volte con uso di VPN
    - Picco d'uso delle reti fisse e mobili
    - Picco d'uso dei dispositivi personali anche per la professione (BYOD) → forte aumento rischi (GG: BYOD al 75% del totale nel 2022 rispetto al 35% del 2018)
  - Spear phishing e malware «ad hoc» e più critici
- **Necessità di aumentare il supporto allo smart worker** che, operando da solo, non ha più il supporto dei colleghi in caso di dubbi sulla sicurezza digitale (es: phishing, fake news, etc.)
  - **Lack of social control** → human protection shield
- **Necessità di potenziare** le esistenti **misure di sicurezza digitale**, tecniche **e soprattutto organizzative**
- **Necessità di Garantire la continuità operativa** almeno dei processi e delle attività più critiche per l'azienda/ente
  - Ridondanza risorse, Piano di Disaster Recovery (DR), Piano di Business Continuity (BC)

GRAZIE DELL' ATTENZIONE e …

- Le slide di questa presentazione saranno scaricabili dal sito AIPSI
- Il videostreaming di questo webinar sarà disponibile su YouTube
- Seguite i prossimi webinar AIPSI
  - 26/1/2019 ore 18 su SOAR
  - In prossime date in corso di definizione, Webinar di approfondimento con Cloudflare, Darktrace, Qintesi, Sophos
- Iscrivetevi alla newsletter AIPSI
- Se interessati alla cybersecurity iscrivetevi ad AIPSI
  - AIPSI GIOVANI, per i giovani (da 16 a 26 anni compiuti) iscrizione gratuita ad AIPSI per un anno e:
    - Corso gratuito di inquadramento cybersecurity
    - Supporto tesi/tesine su cybersecurity
    - Possibilità di stage in aziende della domanda e dell'offerta cybersecurity/ICT

OAD Osservatorio Attacchi Digitali in Italia

… passiamo alla Tavola Rotonda

Partecipano:

- **Dott. Angelo Amaglio, Presidente Qintesi**
- **Ing. Corrado Broli, Country Manager Italy Darktrace**
- **Dott.a Sara Maiolino, Account Executive Southern Europe Cloudflare**
- **Ing. Walter Narisoni, Sales Engineer Manager di Sophos Italia**
- **Dott. Mario Pitassi, CEO Technology Estate**

Il tema della TR: impatto del Covid-19 sugli attacchi e sulla sicurezza digitale dei Sistemi Informatici delle Aziende e degli Enti in Italia.

aipsi