Webinar CMMC 12/05/2023

Sicurezza come opportunità

La vulnerabilità agli attacchi digitali e le misure da adottare, organizzative e tecniche

Marco R. A. Bozzetti
Presidente AIPSI (m.bozzetti@aipsi.org)
Founder e CEO Malabo srl (www.malaboadvisoring.it)

AIPSI: chi siamo e cosa facciamo

- **Associazione apolitica e senza fini di lucro** di **sole persone fisiche** → https://www.aipsi.org/
- **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org), la più grande associazione no-profit di professionisti della Sicurezza ICT nel mondo
- **Obiettivi principali**
  - **Aiutare** i propri Soci nella **crescita professionale e delle loro competenze, tramite un insieme di servizi e di opportunità forniti da AIPSI a livello nazionale e da ISSA a livello internazionale**
  - **Sensibilizzare sulla sicurezza digitale gli utenti dei Sistemi Informativi e dei servizi digitali**

OAD Osservatorio Attacchi Digitali in Italia

https://www.oadweb.it/it/

REPUBBLICA DIGITALE

FIDA INFORM

https://fidainform.it/

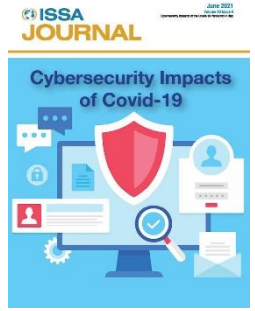
I principali servizi AIPSI-ISSA

Principali Servizi erogati da AIPSI

- **Aperti a tutti gli interessati anche non Soci**
  - Indagini: **OAD, Osservatorio Attacchi Digitali in Italia** e SIG **CSWI, Cyber Security Women Italy**
  - **Webinar ed eventi** anche in collaborazione con Associazioni, Enti ed Aziende
  - **Collaborazione con varie Associazioni ed Enti** per eventi ed iniziative congiunte
  - **AIPSI Giovani**
- **Riservati ai Soli Soci**
  - Supporto alle certificazioni, in particolare per **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale con AICA **con sconto**
  - **Mentorship professionale**
  - **SIG, Special Interest Group**, di approfondimento e discussione:
    - AI e Cybersec
    - Nuove architetture per Cybersec (SASE, SOAR, Zero Trust, etc.)
    - Crescita professionale Soci
  - **Network Soci** a livello nazionale

Principali Servizi erogati da ISSA

- **ISSA Journal**
- ESG ISSA Survey "The Life and Times of Cyber Security Professionals"
- Convegni, workshop, webinar (in inglese)
- Corsi online (in inglese)
- SIG, Special Interest Group
  - Privacy
  - Women in Security
- Accordi con sconti per certificazioni individuali
- Network Soci a livello mondiale



OAD, Osservatorio Attacchi Digitali in Italia

- OAD: indagine annuale AIPSI sugli attacchi digitali intenzionali ad aziende/enti e sulle misure di sicurezza in essere
- Aperta ad aziende/enti di qualsiasi dimensione e settore merceologico, Pubbliche Amministrazioni incluse
- Effettuata tramite un questionario online assolutamente anonimo
- Con l'edizione del 2023 **sedici anni consecutivi di indagini**
- 11 Rapporti finali pubblicati: https://www.oadweb.it/it/
- **In corso l'edizione 2023**: https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2023.html

Compilate e fate compilare il Questionario OAD 2023 anonimo

https://www.oadweb.it/ls2023/limesurvey/index.php/279362?lang=it

Vulnerabilità cause delle minacce → attacchi digitali

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 → **migliaia di 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

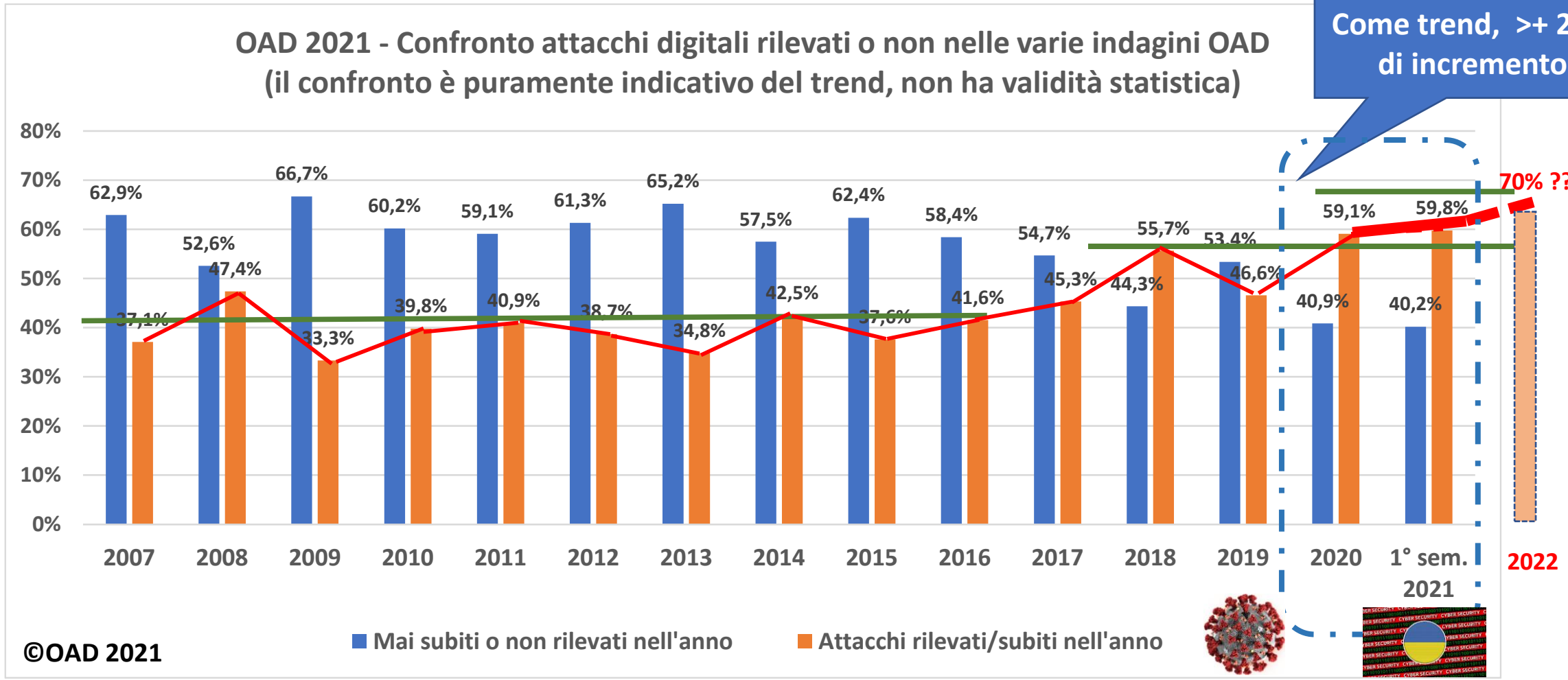
La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

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

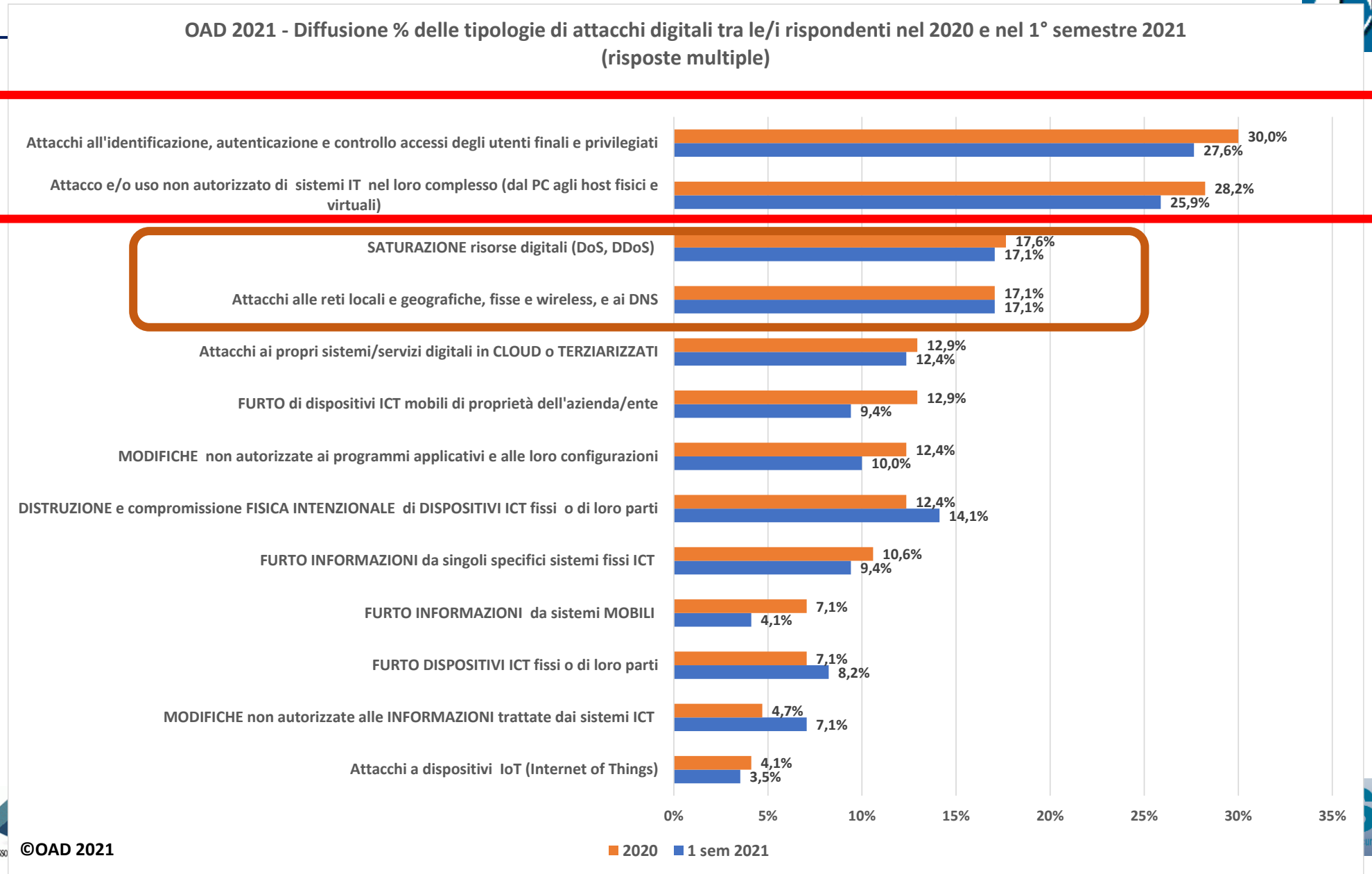
Aggravata dalla non o inefficace organizzazione

Mancanza di formazione e addestramento

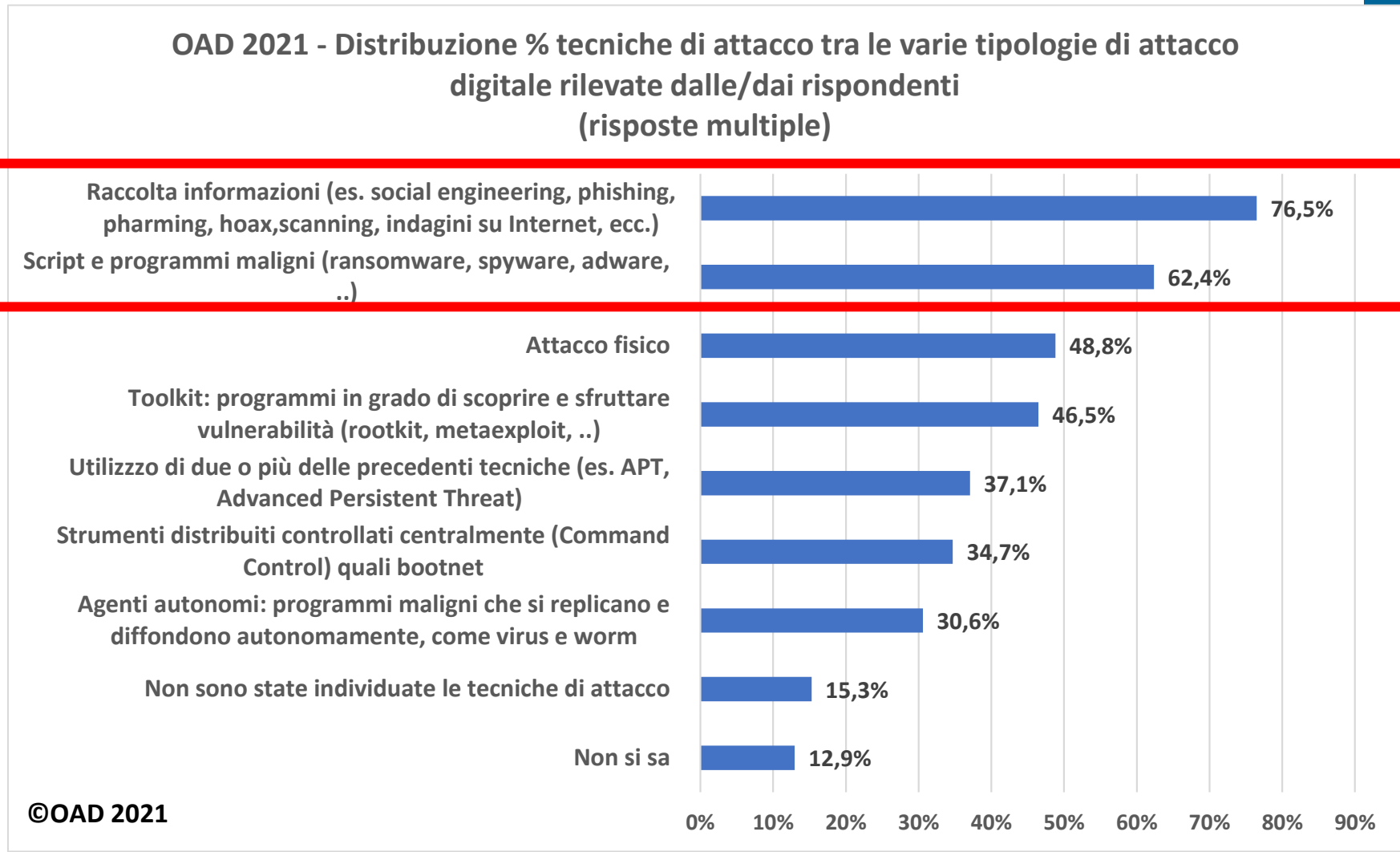
Forte incremento attacchi digitali intenzionali come trend da OAD 2007-2021 e per 2022



OAD 2021 – Distribuzione % tipologia attacchi digitali



OAD 2021 – Distribuzione % macro-tecniche di attacco digitale



Quali misure di sicurezza? Tecniche ed organizzative

Le classiche misure tecniche

- **architettura complessiva delle misure di sicurezza digitale, integrata con l'intera architettura del sistema informativo**
- **contromisure fisiche**
- **misure di Identificazione, Autenticazione, Autorizzazione (IAA)**
- **contromisure tecniche sicurezza digitale a livello di reti locali e geografiche**
- **contromisure tecniche per la protezione (non fisica) dei singoli sistemi ICT anche terziarizzati/in cloud**
- **contromisure tecniche per la protezione del software e degli applicativi dei sistemi ICT anche terziarizzati/in cloud**
- **contromisure per la protezione dei dati, in primis backup e crittografia dati critici/sensibili**
- **sistemi di controllo, monitoraggio e gestione della sicurezza digitale**
- **Piano di Disaster Recovery (DR) con l'allocazione, o non, dei relativi ambiti alternativi.**

- **Corsi** di sensibilizzazione e formazione sulla **sicurezza per tutti gli utente**
- Ufficializzazione **Data Owner**
- **Classificazione** dei dati/informazioni
- Nuove **Architetture Sicurezza Digitale** (Zero Trust, SASE, etc.)
- **Autenticazione forte** utenti, in particolare di quelli privilegiati
- Orientamento al **passwordless** → riconoscimento biometrico
- Attenta assegnazione **profili di accesso** e loro aggiornamenti
- Sistematico e tempestivo **aggiornamento software**
- Sistematica ed effettiva **verifica delle SLA e KPI dei contratti di outsourcing/cloud**
- **Minime/no info personali sui social net** dell'azienda/ente e del personale
- Verifica per **attendibilità siti web, fake news** e **deepfake → DISINFORMAZIONE**

ENISA & Unione Europea: verso un approccio unificante e migliorativo per la sicurezza digitale in Europa

- **NIS2,** normative misure di sicurezza digitale per infrastrutture critiche e servizi essenziali in ogni paese UE
- **Regolamento DORA** per incrementare le misure di sicurezza a favore della resilienza e della sicurezza informatica del settore finanziario
- **Direttiva CER** relativa alla resilienza dei soggetti critici
- **Regolamento DSA, Digital Services Act**: nuove regole per contrastare la diffusione di contenuti illegali e disinformazione sulle piattaforme ed I motori di ricerca
- **DMA, Digital Market Act**
- **Coordinated Vulnerability Disclosure**: **Towards a Common EU Approach**
- **EU CyCLONe, EU Cyber Crisis Liaison Organisation Network →collaborazione con le Agenzie dei vari paesi UE (per l'Italia ACN)**
- **EU Cyber Resilience Act**
- **Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies**

https://www.enisa.europa.eu/

Le principali necessità e opportunità in Italia

- Forte sensibilizzazione e incremento consapevolezza dei **decisori di aziende/enti** sull'importanza dell'informatica e della sua sicurezza
- Forti incentivi per **creare competenze** sulla sicurezza digitale e per **gestirle** all'interno di aziende/enti (**ruolo, compenso**, etc.)
- **Migliorare le misure di sicurezza** tecniche ed organizzative grazie a progetti di trasformazione digitale
- L'opportunità di **terziarizzare**, soprattutto per le piccole realtà, la gestione della sicurezza digitale:
  - **MSS,** Managed Security Services
  - **CSaaS,** CyberSecurity as a Service
- Maggior accentramento decisionale e di controllo con **ACN, Agenzia Cybersicurezza Nazionale**
- Compliance alle nuove direttive-regolamenti europei (**NIS2, CORE,** etc.)
- Progetti in ambito **PNRR**

Grazie per l'attenzione, e …

Questa presentazione sarà scaricabile in pdf dai siti CMMC e AIPSI

Se la **sicurezza digitale vi interessa**:

- Iscrivetevi alla newsletter AIPSI
- Seguite i webinar AIPSI e le altre nostre iniziative

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

https://www.aipsi.org/

Se volete essere sistematicamente aggiornati e **crescere professionalmente** nel campo della sicurezza digitale:

- **Diventate Soci di AIPSI – ISSA**

ISSA
Information Systems Security Association

https://www.issa.org/

Per informazioni: segreteria@aipsi.org, aipsi@aipsi.org