1^ Edizione

6 Luglio 2022, Live web, 9.00 - 13.00

convegno sulla gestione del rischio e della sicurezza digitale

aipsa aipsi ANIPA ASSI BUSINESS Community intellera consulting

KappaeMme

1^ Edizione

6 Luglio 2022, Live web, 9.00 - 13.00

convegno sulla gestione del rischio e della sicurezza digitale

In collaborazione con

CONSERVE ITALIA

ENAV

POLIZIA DI STATO POSTALE E DELLE COMUNICAZIONI

STUDIO LEGALE MEAZZA

UNIVERSITA' DI MILANO

1^ Edizione

6 Luglio 2022, Live web, 9.00 - 13.00

convegno sulla gestione del rischio e della sicurezza digitale

Il Cyber Risk Management in tempi di Covid e di cyber warfare

Marco R. A. Bozzetti, Presidente AIPSI

Relatore

MARCO R. A. BOZZETTI

Organizzazione

AIPSI

PROFILO

- Presidente AIPSI
- Laureato in ingegneria elettronica al Politecnico di Milano, dal 2001 è Founder e CEO di Malabo Srl società di consulenza direzionale nell'ICT. 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 CIO dell'intero Gruppo ENI. Ideatore e curatore dell'indagine OAD. E' Presidente di AIPSI, capitolo italiano della mondiale ISSA.

ANALISI e GESTIONE DEL CYBER RISCHIO

Rischio = Impatto * Probabilità

- Con Probabilità (P) occorrenza attacco intenzionale

  P= F (V, M)

  - **V** = Vulnerabilità
  - **M** = Motivazioni dell'attaccante

L'asset da proteggere: il dato

Occorre garantire la sua :

- ***integrità, disponibilità, confidenzialità***
- ***autenticità, non ripudio*** (in rete)

- **Minaccia**
- **Vulnerabilità**
- **Rischio**
- **Attacco**

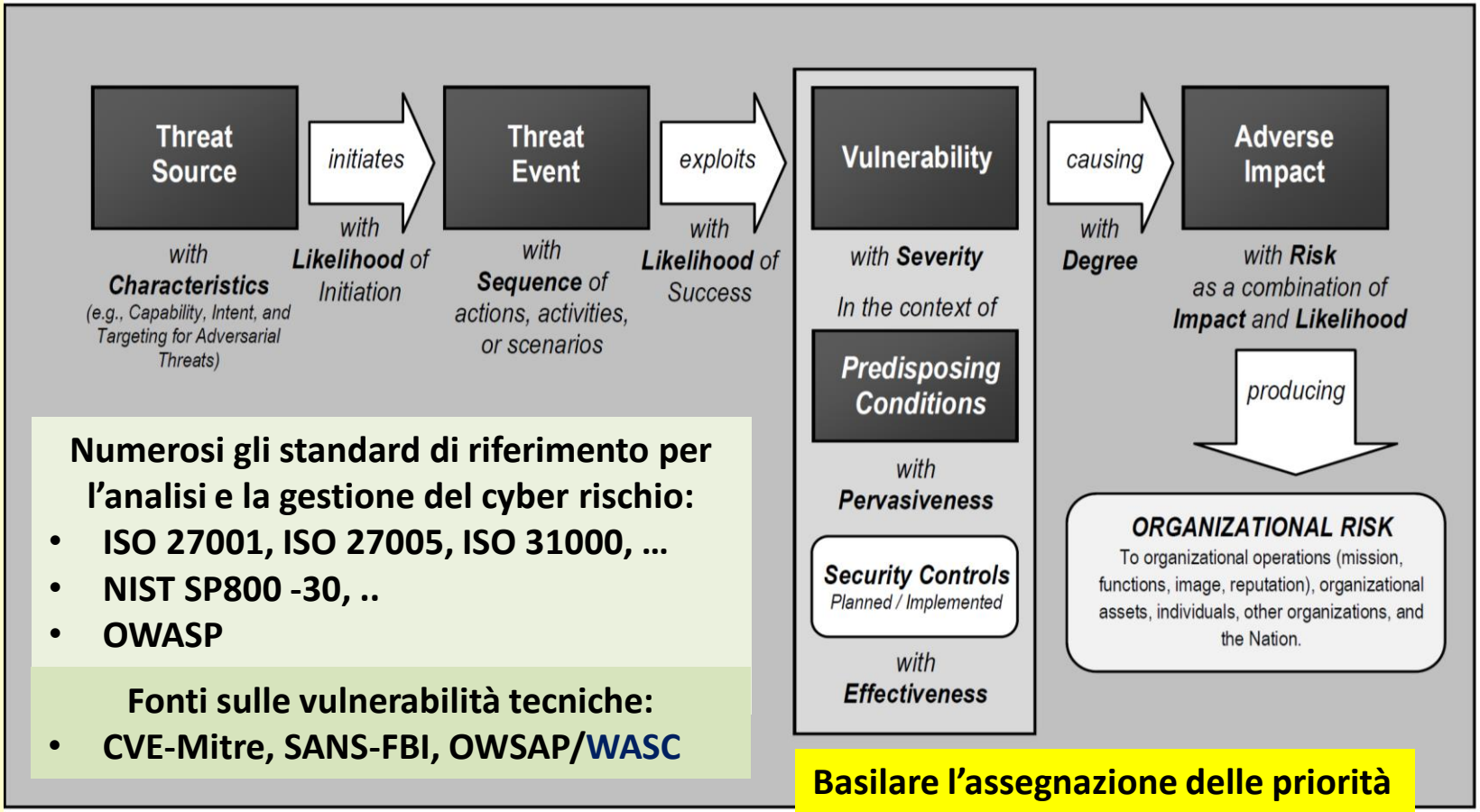
Vulnerabilità

- Tecniche
- Persone
- Organizzative

Occorre distinguere tra:

- **Analisi del rischio**
- **Gestione del rischio**
- **Analisi e gestione vulnerabilità**
- **Analisi e gestione degli impatti (BIA)**

Il modello dei rischi da NIS SP800-30



Numerosi gli standard di riferimento per l'analisi e la gestione del cyber rischio:

- **ISO 27001, ISO 27005, ISO 31000, …**
- **NIST SP800 -30, ..**
- **OWASP**

Fonti sulle vulnerabilità tecniche:

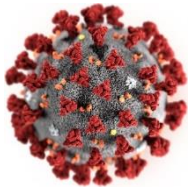
- **CVE-Mitre, SANS-FBI, OWSAP/WASC**

Basilare l'assegnazione delle priorità

La situazione in Italia

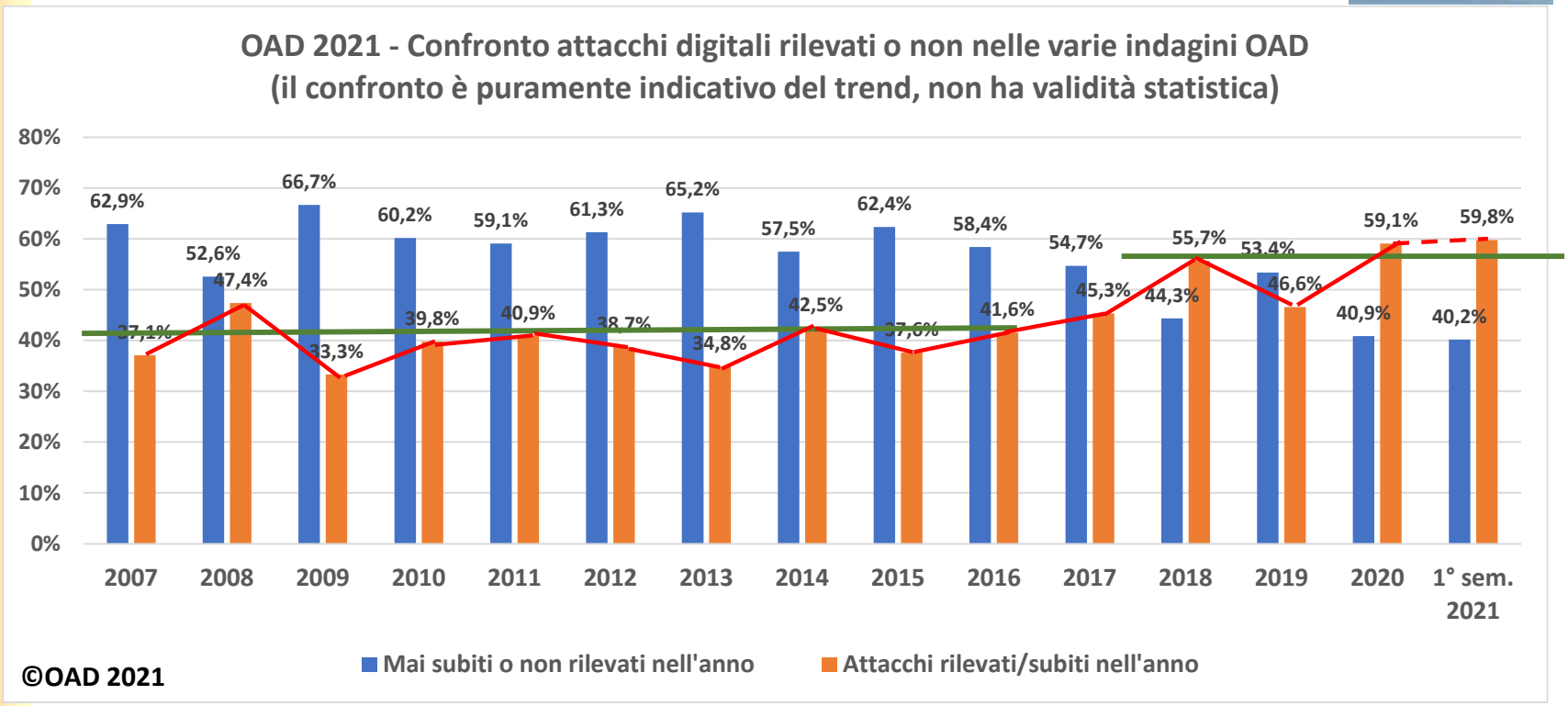
- **La miriade di piccole piccolissime aziende/enti in Italia**
  - Per le aziende private (dati ISTAT)
    - PMI 99,9 % del totale
    - Imprese fino a 10 dipendenti 95% del totale
  - per gli enti pubblici (PA) si stimano attorno ai 55,000, con prevalenza di piccole organizzazioni

- **Covid 19**
  - Ampio uso servizi Internet
  - Smart working
  - Molte aziende/enti con insufficienti misure di sicurezza

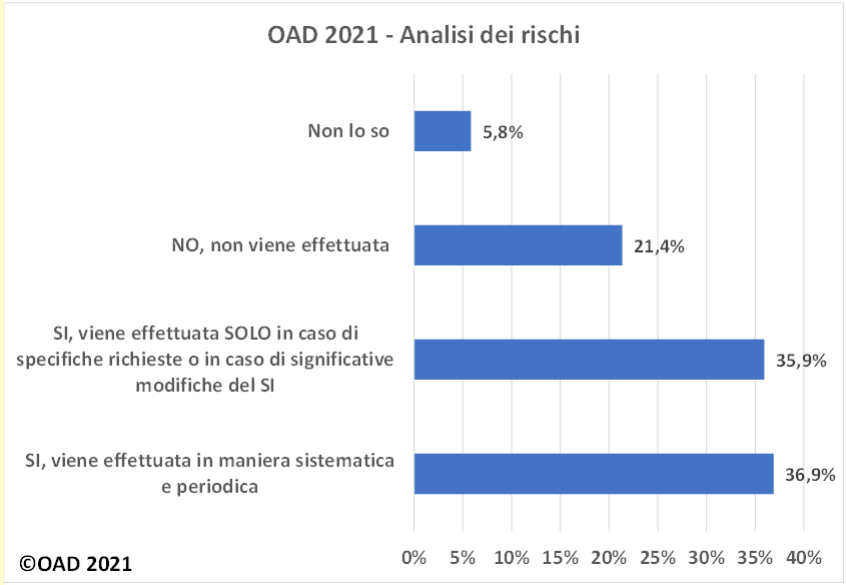


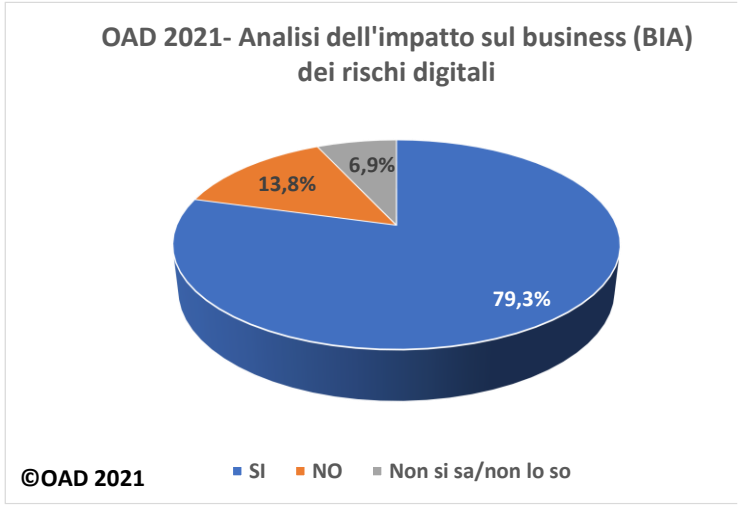
- **Invasione Ucraina**
  - Cyber warfare
    - Attacchi digitali soprattutto, ma non solo, a PA
      - DDoS, Wiper, etc.
      - Proliferazione di fake news

Trend attacchi digitali da OAD (www.oadweb.it)



OAD 2021 – Analisi dei rischi





Analisi e gestione dei cyber rischi: perché? E come?

- L'analisi e la gestione dei rischi è richiesta/imposta da varie normative, certificazioni e leggi, in primis dal **GDPR per la privacy** (che prevede multe assai elevate ..)
- E' parte centrale del processo continuo della sicurezza digitale, ed indispensabile per il progetto delle misure tecniche ed organizzative della sicurezza digitale
- Fa anche parte della più generale analisi e gestione **dei rischi complessivi dell'intera organizzazione**

- Ma la sua effettuazione è complessa, logicamente continua, e richiede specifiche competenze anche interdisciplinari: in conclusione è costosa..
- Le piccole organizzazioni, private e pubbliche, **non hanno**, nella maggior parte dei casi, **competenze e risorse** per poterle fare ..
- Potrebbero/dovrebbero **terziarizzarle**, come tutta la gestione della sicurezza digitale, ma come possono scegliere il **right sourcing**?
- Quali i **possibili ausili dalle Associazioni e dalle Istituzioni**?

AIPSI capitolo italiano mondiale ISSA

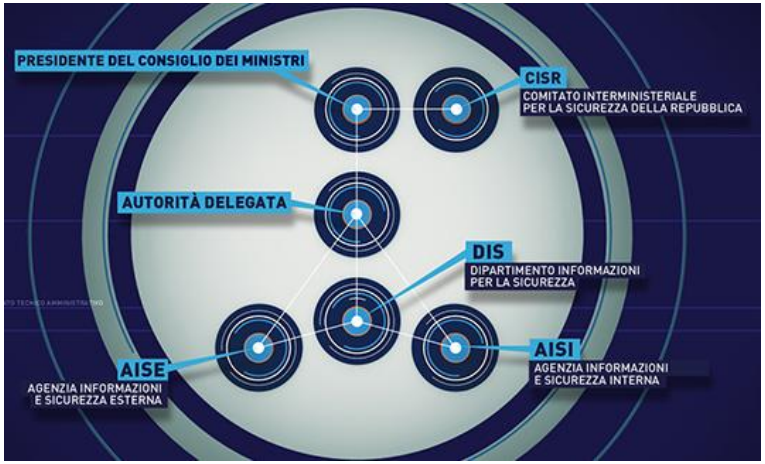
Per le infrastrutture critiche ed i servizi essenziali dal NIS al NIS2

- La direttiva europea **NIS, EU 2016/1148**, definisce le misure di sicurezza digitale necessarie a livello di ogni paese membro, così da uniformare, pur con una certa flessibilità, la risposta europea ai possibili attacchi digitali, soprattutto per le infrastrutture ICT critiche, chiamate anche "servizi essenziali". Recepita in Italia con il D. Lgs. n. 65 del 18/5/2018.
- **NIS 2**: obiettivo di rafforzare i requisiti di sicurezza e di introdurre misure di supervisione più rigorose e requisiti di applicazione più severi
  - Nuova classificazione servizi tra "essenziali" (es. cloud) ed "importanti" (es. social net) con diversi regimi di controllo
  - Ampliamento servizi: ad esempio produzione di prodotti farmaceutici, dispositivi medici e prodotti chimici, il settore alimentare, la gestione delle acque reflue e dei rifiuti, i servizi postali, la pubblica amministrazione. → un ordine di grandezza in più rispetto al NIS

Le istituzioni italiane per la sicurezza cibernetica e la cyber intelligence

- **ACN**, Agenzia Cybersicurezza Nazionale
  - **NCS**, Nucleo per la cybersicurezza
  - **CSIRT**, Computer Security Incident Response Team Italia
- **COR**, Comando Operazioni in Rete (Ministero Difesa)
- **Polizia Postale e delle Comunicazioni**: preposta al contrasto delle frodi postali e del crimine informatico
  - **CNAIPIC**, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
- **NSTPFT,** Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza contrastare le frodi digitali, nonché tutelare la privacy

Cyber intelligence italiana (dalla Legge 124/2007)



COPASIR

Comitato parlamentare per la sicurezza della Repubblica è l'Organo di controllo parlamentare

1^ Edizione

6 Luglio 2022, Live web, 9.00 - 13.00

convegno sulla gestione del rischio e della sicurezza digitale

GRAZIE PER L'ATTENZIONE !

Per informazioni:

JEKPOT SRL, Via Folperti 44/d, 27100 Pavia PV, Italy

www.jekpot.com | +39 0382 572287 | jekpot@jekpot.com