La resilienza del sistema informativo aziendale: quali misure di sicurezza digitali nell'attuale contesto di crescenti attacchi e terziarizzazioni?

Marco R. A. Bozzetti
Presidente AIPSI
Founder e CEO Malabo Srl

16 ottobre 2020

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
  - 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)

- *Che cosa è*
  - OAD è una indagine via web sugli attacchi digitali **intenzionali** ai sistemi informatici in Italia
    - rilevati da Enti Pubblici ed Aziende di ogni dimensione e settore merceologico (Codici Ateco)
    - totalmente anonima
    - Produzione annuale di un Rapporto che include e commenta **anche i dati dell'anno della Polizia Postale**

- *Obiettivi iniziativa*
  - Fornire informazioni sulla reale situazione degli attacchi digitali in Italia, anche verso le piccole e piccolissime organizzazioni
  - 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

Ultimi giorni !

Compilatelo/fatelo compilare!

2020: 12° edizione OAD in corso

- **Questionario on line: https://www.oadweb.it/limesurvey2020/index.php/574592?lang=it**
- Per maggiormente motivare la/il rispondente, alla fine della compilazione appare una **macro valutazione qualitativa del livello di sicurezza del sistema informatico oggetto delle risposte**. E' inoltre possibile scaricare, sempre gratuitamente:
  - il numero di maggio 2020 della rivista **ISSA Journal** sul**la crittografia quantistica**
  - la seconda edizione 2019 del libro "**Information Security e Data Protection**", edito da Reportec.

Inquadramento

Resilienza e sicurezza digitale

Resilienza

- In fisica: Capacità di un materiale di assorbire un urto senza rompersi
- In psicologia: capacità di un individuo di affrontare e superare un evento traumatico o un periodo di difficoltà
- In informatica: capacità di un sistema ICT di assorbire malfunzionamenti ed attacchi, volontari ed involontari (errori degli utenti), continuando ad erogare i suoi servizi

Per poter garantire una effettiva resilienza del Sistema Informatico occorre in particolare:

- Disporre e ben gestire risorse ICT ridondate
- Attuare un Piano di Business Continuity e di Disaster Recovery
- Garantire elevati livelli di sicurezza digitale, sia a livello tecnico che organizzativo
- Disporre di un assessment e monitoraggio continuo delle risorse del Sistema Informatico
- Sistematica Analisi dei Rischi ICT e dei relativi impatti
- Sensibilizzazione e formazione a tutti i livelli sulla cyber security

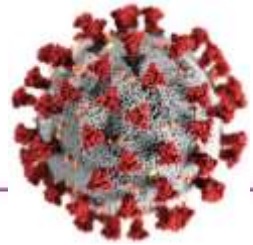
Sicurezza digitale

- La **protezione dai requisiti di integrità, disponibilità e confidenzialità delle informazioni trattate**, ossia acquisite, comunicate, archiviate, processate, dove:
  - ***integrità*** è la proprietà dell'informazione di non essere alterabile; o poter verificare se è stata alterata
  - ***disponibilità*** è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati;
  - ***confidenzialità*** è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto di accedervi
- Per le informazioni e i sistemi connessi **in rete** le esigenze di sicurezza includono anche:
  - ***autenticità***, ossia la certezza da parte del destinatario dell'identità del mittente
  - ***non ripudio***, ossia il mittente o il destinatario di un messaggio non ne possono negare l'invio o la ricezione

Il ruolo del Sistema Informatico (SI) e della sua sicurezza

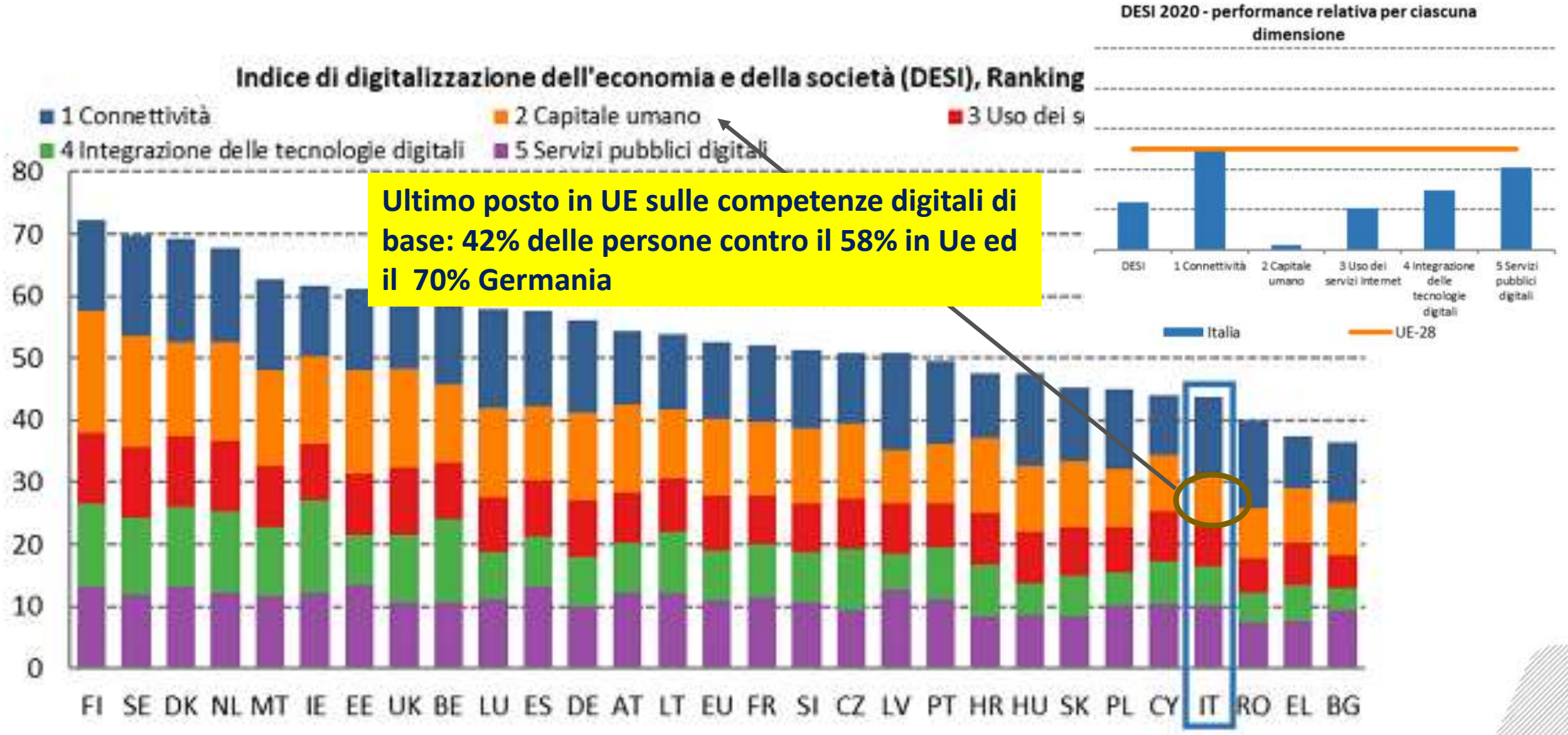
- Quasi ogni attività si basa ormai su applicazioni del Sistema Informatico
- Il Sistema Informatico non può che operare su Internet, ed è quindi esposto ad attacchi dall'esterno, oltre che dall'interno
- Il corretto, continuo e sicuro funzionamento del Sistema Informatico garantisce:
  - la **continuità 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**

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 ed 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 Continuty (BC)

Indice DESI 2020



Imprese e PA in Italia

ISTAT: Imprese private per numero dipendenti	ISTAT 2019 Numero dipendenti	% sul totale ISTAT 2019	% rispondenti OAD 2019	ISTAT 2020 Numero dipendenti	% sul totale ISTAT 2020	% rispondenti OAD 2020
< 10	4.179.818	**95,05%**	18,70%	4.180.761	**94,92%**	in co
11-49	191.004	**4,34%**	18,70%	196.076	**4,45%**	in corso
50-249	22.906	**0,52%**	25,20%	23.647	**0,54%**	in corso
>250	3.895	**0,09%**	37,40%	4.017	**0,09%**	in corso
Totale dipendenti ISTAT /rispondenti OAD 2019 e 2020	4.397.623		296	4.404.501		in corso
PMI 1-249	4.393.728	**99,91%**	62,60%	4.400.484	**99,91%**	in corso

L'Italia è una nazione di micro e nano imprese

PA: <u>non esistono dati di dettaglio per numero dipendenti di PAC e PAC</u>
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, **<u>la maggior parte sono di piccole e piccolissime dimensioni</u>**

Vulnerabilità ed attacchi

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 → decine di 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

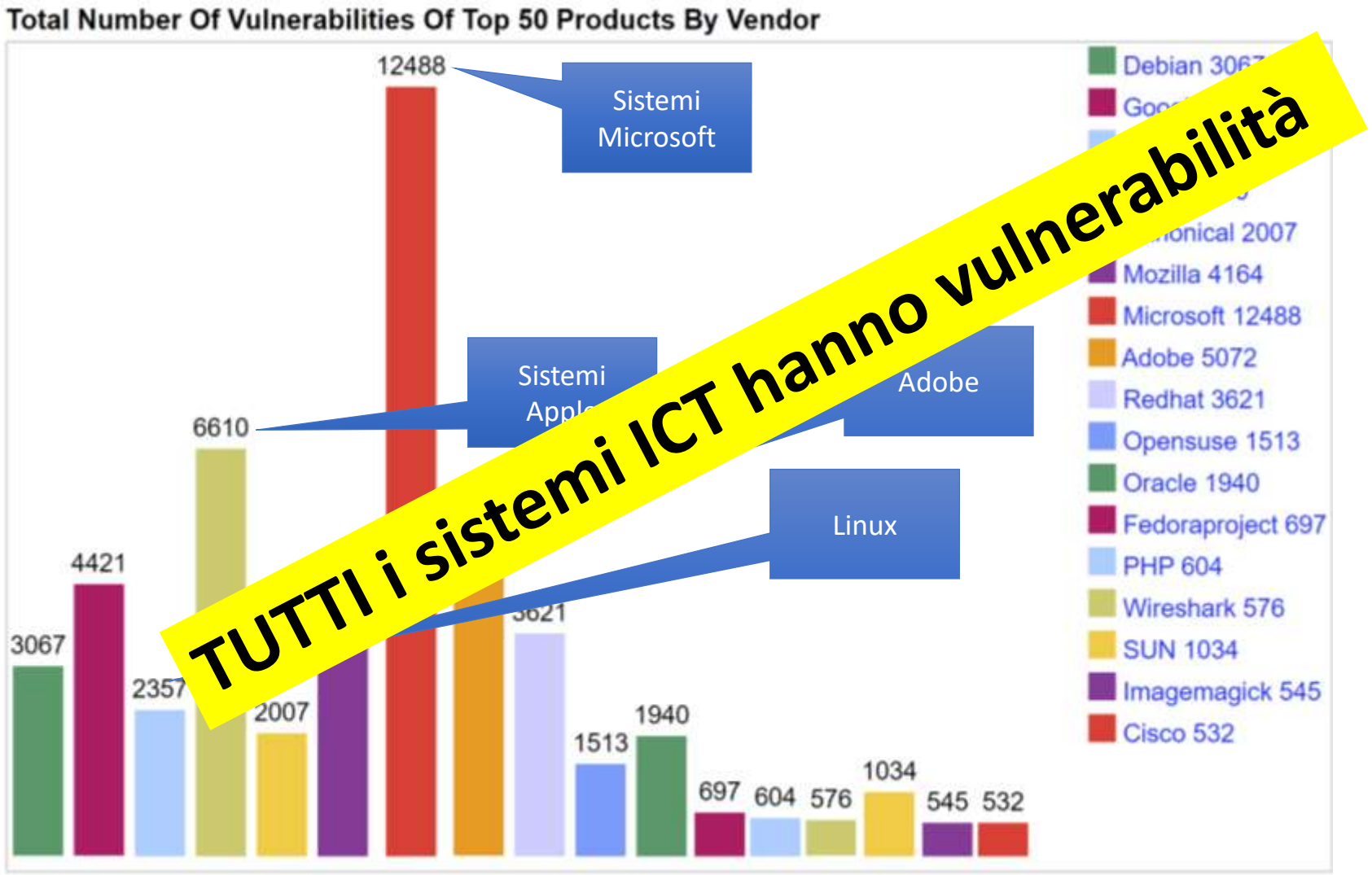
La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

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

Aggravata dalla non o inefficace organizzazione

Mancanza di consapevolezza sulla sicurezza digitale

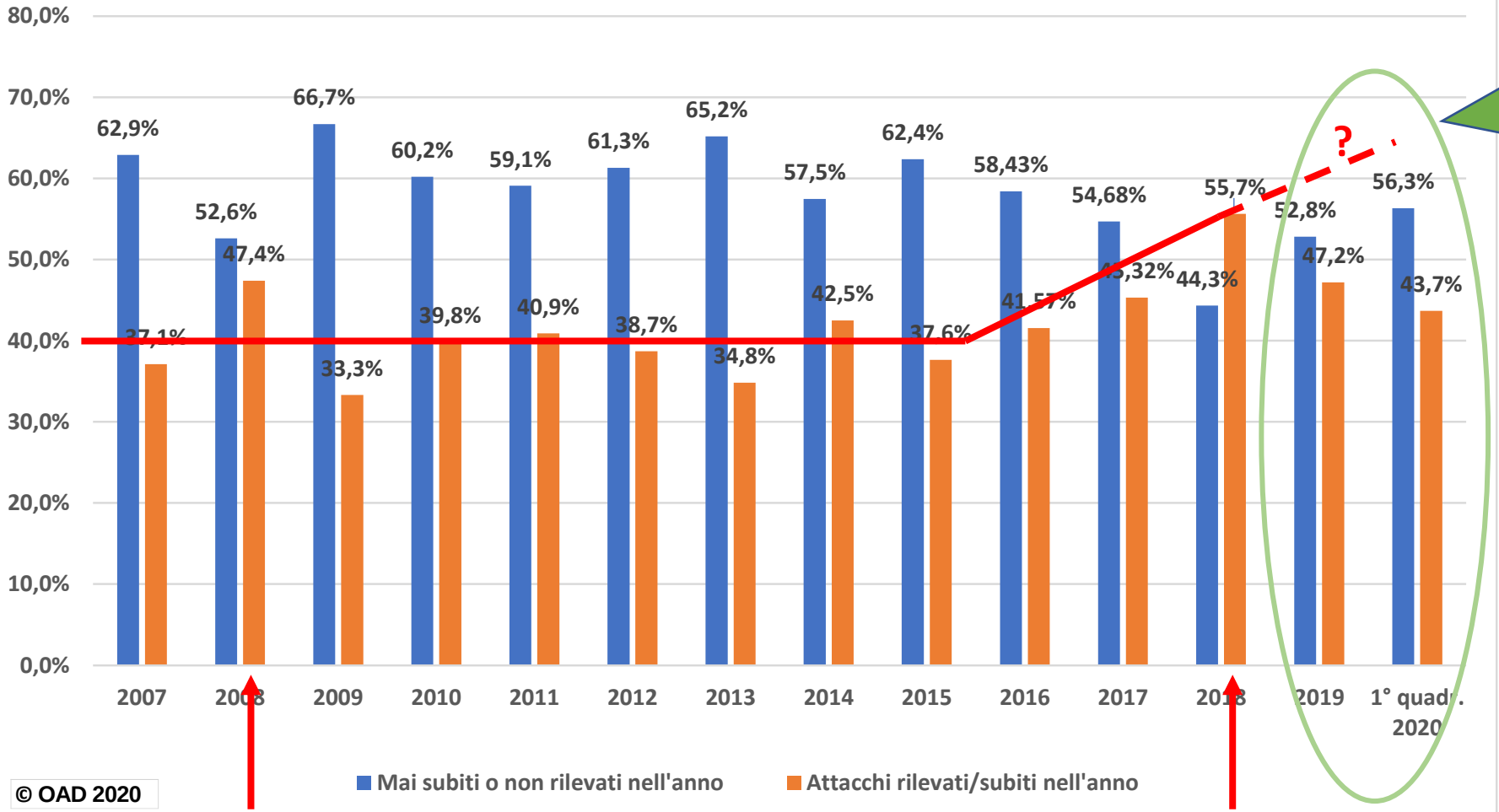
Le principali vulnerabilità per prodotti da CVE, Common Vulnerabilities and Exposures



TUTTI i sistemi ICT hanno vulnerabilità

Anteprima OAD 2020 sul trend degli attacchi digitali nelle indagini OAD-OAI

Anteprima parziale OAD 2020
Confronto risultati indagini OAD-OAI 2007-2020
(valido solo come indicatore del trend, non statisticamente)

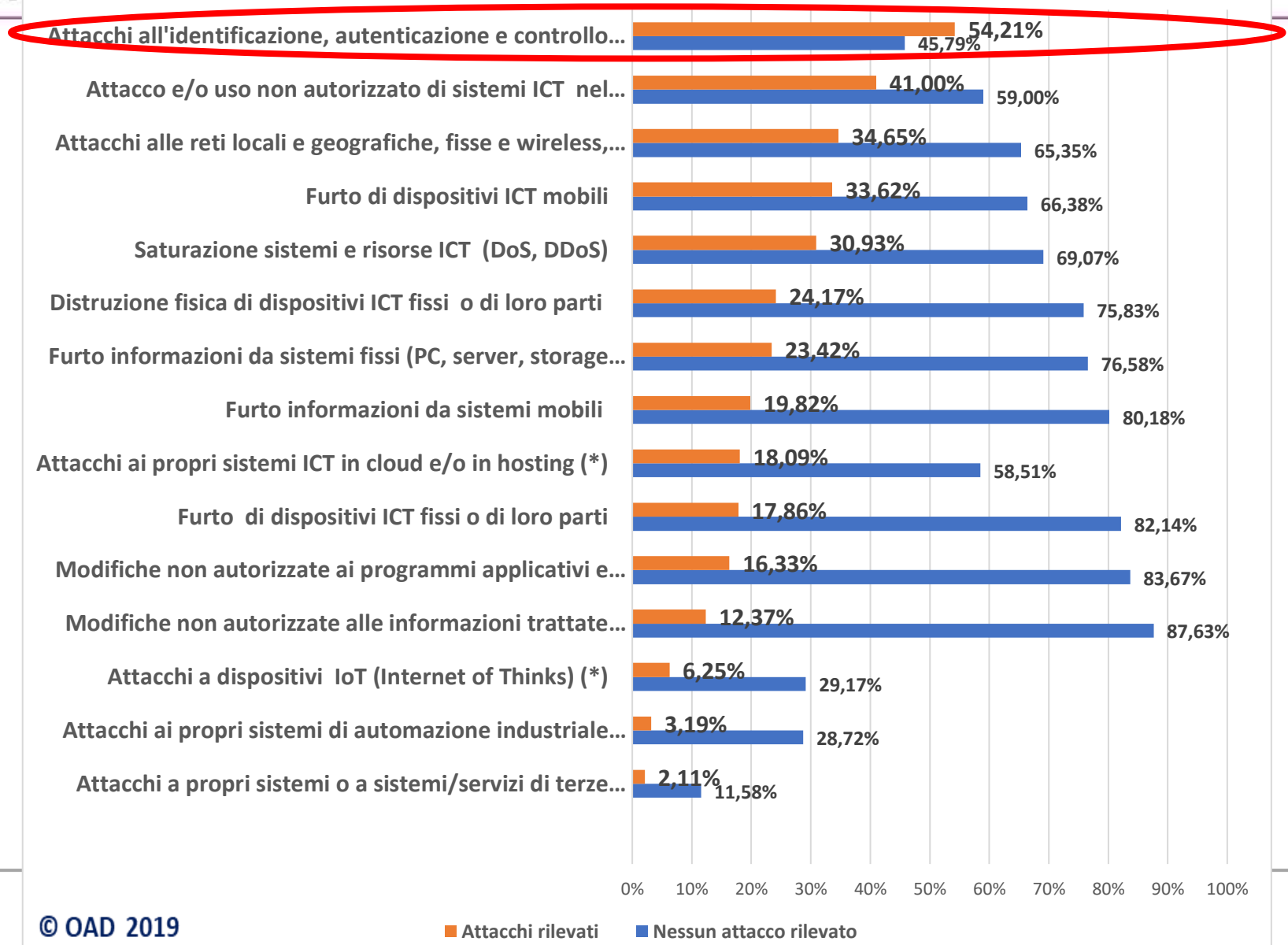


Dati parziali
Indagine 2020 ancora in corso

I valori 2019-2020 potrebbero cambiare nella versione finale di OAD 2020

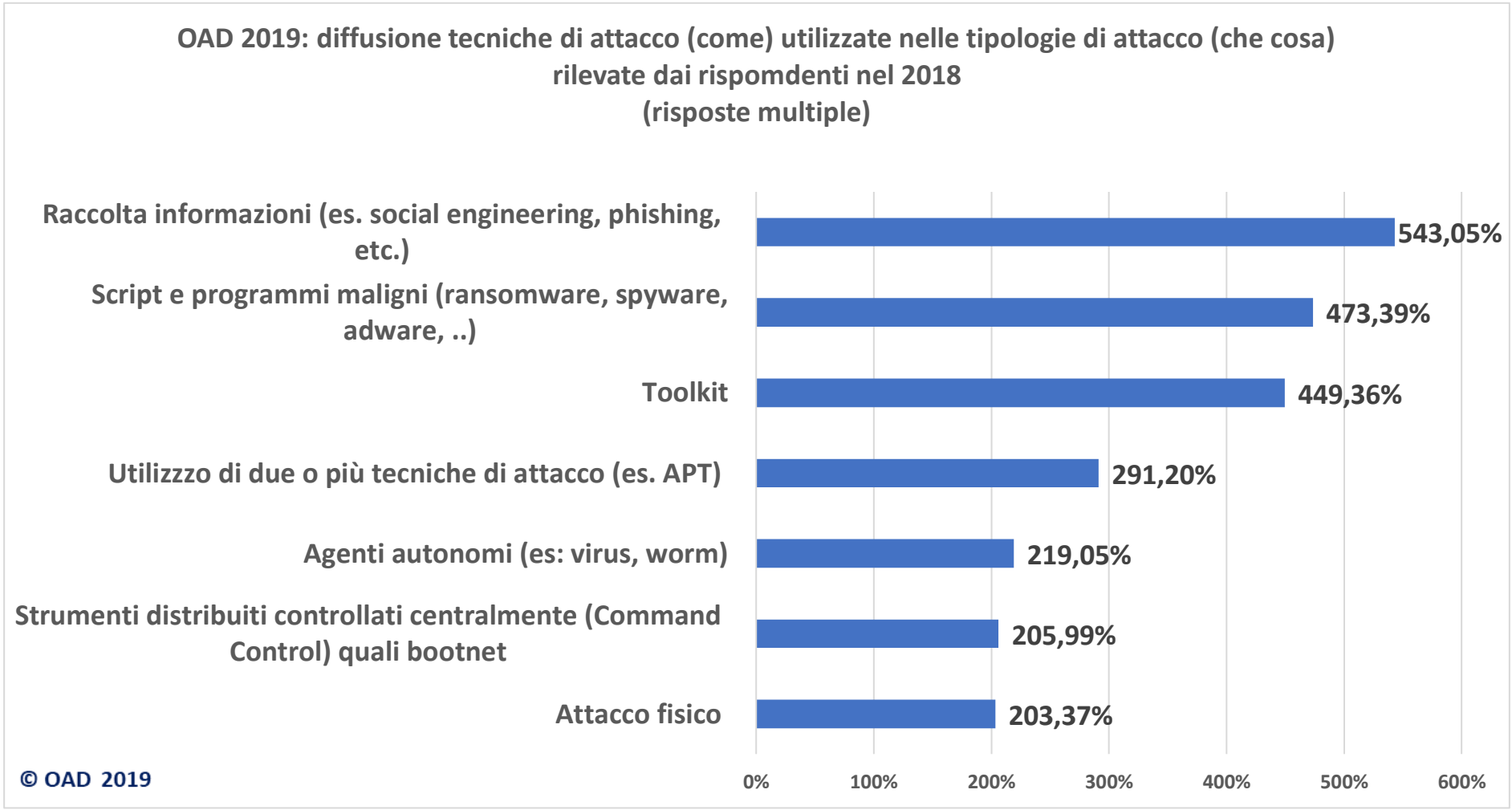
OAD Osservatorio Attacchi Digitali in Italia

Diffusione % tipologia attacchi digitali ai sistemi informatici dei rispondenti nel 2018 (risposte multiple)



14

OAD 2019: diffusione tecniche di attacco



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%

OAD Osservatorio Attacchi Digitali in Italia

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**

Anteprima OAD 2020: stato delle misure di sicurezza digitale

- **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!!)
  - **Consapevolezza (awarness) sicurezza digitale a tutti i livelli**
  - Auditing
- **Misure di gestione e di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

Misure di base da potenziare

Molto Carenti

Carenti

OAD Osservatorio Attacchi Digitali in Italia

Spunti sui criteri e sulle principali misure da adottare

Principali logiche e criteri da seguire per rafforzare la sicurezza del SI

- La sicurezza digitale si deve basare su **processo continuo**, che tenga ben conto sia delle misure tecniche che di quelle organizzative, oltre alla conformità alle varie leggi e normative
- La sicurezza digitale deve essere contestualizzata alla specifica realtà (di business, di cultura, tecnica, organizzativa) dell'azienda/ente
- **Non si deve considerare SE avverrà un attacco o un incidente, ma QUANDO e COME**
- Obiettivo: ridurre gli impatti in caso di incidente o di attacco, volontario o involontario
- Assicurare il rischio residuo ed il suo impatto sull'azienda/ente
- Security by design e by default
- Per la maggior parte delle aziende/enti è necessario terziarizzare la sicurezza digitale, ma con interlocutori realmente esperti e competenti → **right sourcing**
  - Occorre **controllare e governare i fornitori**
  - Non si possono delegare le decisioni strategiche

Le principali misure tecniche di difesa

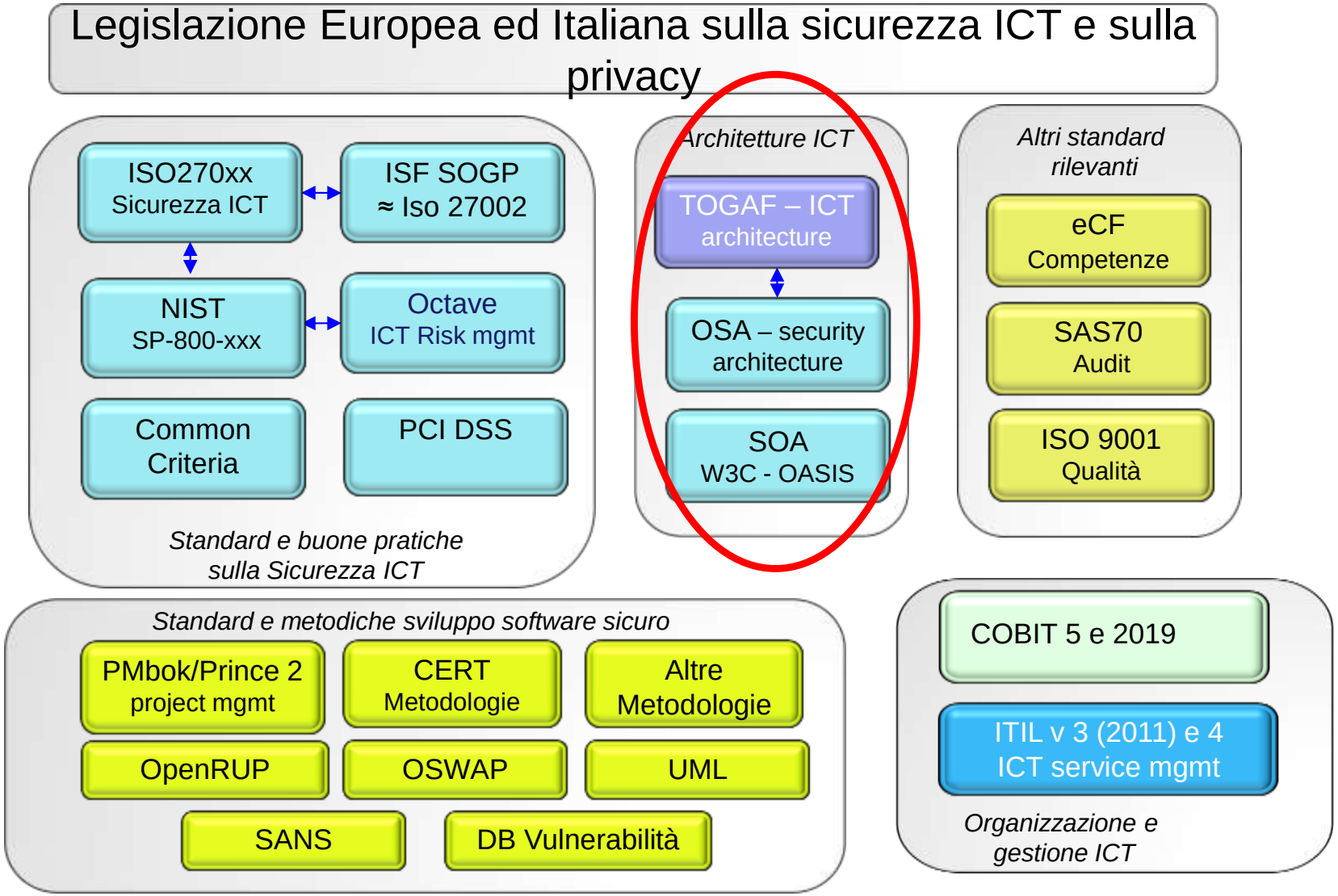
- ***di prevenzione***
  - Crittografia, Stenografia
  - Periodiche analisi del rischio vs processi ed organizzazione
  - Sicurezza fisica: controlli perimetrali, controlli acc… …ione, UPS, anti-incendio, fumo, gas …
  - Sicurezza delle reti: Firewall, IPS/…
  - Identificazione: user i…
  - autenticazi… Active Directory, ..), SSO, …
  - Sicurezza…
  - Architettu…
- ***di ripristino***
  - Back-up
  - Disaster Reco…
- ***di gestione e di gove…***
  - Tecnica: monito… …ne delle patch e delle release del software (→ licenze)
  - Organizzativa: for… …destramento, operation (ITIL v3), help-desk/contact center, ERT, ..

- **da approccio reattivo a proattivo**
- **approccio architetturale ben bilanciato**
- **riferimento ai principali standard e alle best practices ben consolidate: OSA, ITIL , Cobit, ISO 27000, NIST SP xxx, …**

Misure organizzative per la sicurezza digitale

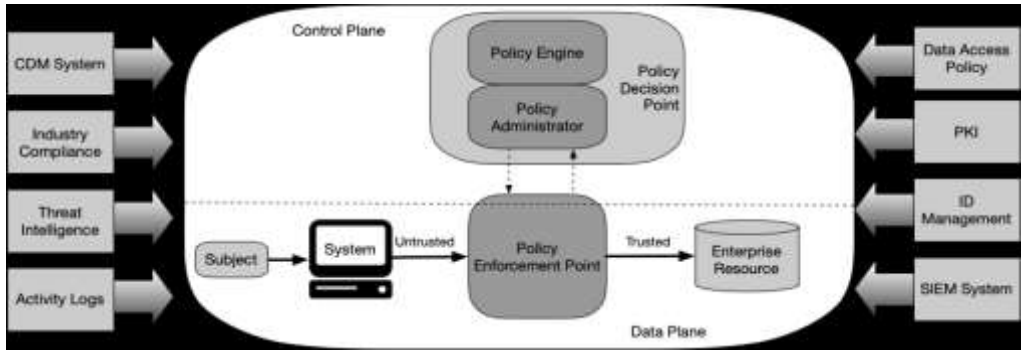
- Riferimento sicurezza ICT a livello di top management
  - Comitati “cross divisionali”
- ERT, Emergency Response Team, inter divisionale
- UOSI, Unità Organizzativa Sistemi informativi → ristrutturazione per orientamento ai servizi
  - Terziarizzazione dei servizi ICT
  - Terziarizzazione della gestione operativa della sicurezza
  - Consumerizzazione e BYOD
- Policy e line guida
- Conformità (compliance) alle varie leggi e normative, tra queste GDPR privacy
- Procedure organizzative
  - La gestione di incidenti ed attacchi
- Audit
- Piano di Disaster Recovery (DR), sovente nell’ambito del Piano di Business Continuity (BC)
- Sensibilizzazione, formazione addestramento dell’ utenza, sia finale sia privilegiata (amministratori di sistema, sistemisti, operatori Data Center, etc.)

Far riferimento ai principali standard e ad un approccio «architetturale»



Approccio Zero Trust (ZT): non mi fido di nulla

- Tutti gli ambienti ed i relativi collegamenti , prevalentemente via Internet, devono essere considerati intrinsecamente insicuri
- la logica zero trust richiede il controllo dell'identità e dell'integrità dei dispositivi indipendentemente dalla loro posizione e dal loro ambito operativo
- L'accesso ad applicazioni e servizi deve basarsi **sull'identità ed integrità dei dispositivi** e **dell'autenticazione forte dell'utente**, oltre che sulla riduzione al **minimo necessario del diritto di accesso** alle risorse considerate
- Gli attuali sistemi informatici sono sempre più eterogenei, distribuiti ed interconnessi via Internet, utilizzano servizi in cloud, sistemi e dispositivi mobili, sistemi OT che includono anche sistemi IoT
- L'approccio ZT si basa su 7 principi di base



- **Basilari le policy, il monitoraggio continuo, la gestione dei log, l'analisi dei rischi**
- CDM=Continuous Diagnostics and Mitigations
- SIEM= Security information and Event Management

- Si veda: NIST (SP) 800-207, "Zero Trust Architecture", agosto 2020

La terziarizzazione della sicurezza digitale

Per il right sourcing

- **Motivazioni**:
  - Finanziarie: Da Capex a Opex
  - Competenze: Società specializzate consentono di accumulare competenze
- **Ulteriori motivazioni di successo (non sempre vere)**:
  - Riduzioni del personale
  - Flessibilità dei contratti di lavoro
- **Come gestire il/i Fornitore/i per assicurarsi l'effettiva sicurezza digitale necessaria (suggerimenti di base)**
  - Selezionare i fornitori sulla base:
    - della loro reputazione (check il loro sito web, in rete e sui social) in particolare con clienti simili alla nostra realtà
    - della loro organizzazione
    - della loro competenza professionale: certificazioni a livello aziendale e personali dei loro dipendenti/collaboratori
    - del tipo di contratto proposto, delle relative clausole (SLA e KPI), della possibilità di personalizzarlo
  - Definire processi standardizzati (confrontabili nel tempo e sul mercato)
  - Misurare i processi
    - raffinare SLA, Service Level Agreement, e KPI, Key Performance Indicator
    - Verificarli eventualmente tramite altre Terze Parte specializzate

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

Disaster Recovery
e Business Continuity

Business Continuity

- **Business Continuity**: strategia dell'organizzazione per assicurare il funzionamento almeno parziale dei processi anche in caso di eventi disastrosi
- **IT Disaster Recovery**: piano degli interventi e della strumentazione IT necessari per il ripristino dei servizi nei diversi scenari prevedibili
- **Minaccie** da considerare ma da contestualizzare:
  - Naturali: alluvioni , incendi, pandemie, ..
  - Umani: errori , attacchi intenzionali che includono sabotaggi, terrorismo cybernetico, etc.
  - Ambientali: guasti di appartati di eleborazione, rete, supporto

Best practice: NIST SP 800-34 – *Contingency Planning Guide for Information Technology (IT) Systems*

29

Disaster Recovery Plan

- *"DRP si riferisce ad **un piano focalizzato sull'ICT** per ripristinare l'operatività di un sistema, di un'applicazione o di un centro elaborativo **in un sito alternativo** dopo un emergenza. In particolare non si riferisce quindi a interruzioni minori che non richiedono rilocazione di sito."* (da Comitato-CNSI)
- l termine "Disaster Recovery" indica una attività specifica, all' interno di un piano "enterprise" di "Business Continuity".
- Il Disaster Recovery è quella parte che si occupa di rendere disponibili le risorse informatiche necessarie allo svolgimento dei **processi vitali dell' azienda/ente** a fronte di eventi disastrosi
- **Evento Disastroso**: rende inagibile l'utilizzo di infrastrutture e sistemi ICT per un tempo tale da compromettere in modo irreversibile affari, produttività ed immagine aziendale.
- Standard e best practice di riferimento: **ISO 27031**, **NIST 800-34 Rev. 1**

Siti alternativi per il DR

Sito	Costo	HW	Rete	Restart	Località
Stand by Freddo	basso	nessuno	nessuna	lento	fissa
Stand by Caldo	medio	parziale	Parziale /tutta	medio	fissa fissa
Pronto - Hot	Medio-alto	tutto	tutta	breve	fissa
Duale - Mirrored	alto	duplicato	tutta	istantaneo	fissa

- Il sito alternativo può essere di una terza parte
- Il contratto può includere anche l'affitto dell'HW.
- Il tempo di restart e il costo dipendono dalle SLA del contratto
- In caso di disastri molto gravi si possono presentare situazioni di overbooking

Prossime (o già in corso) evoluzioni nella cybersecurity

Con vulnerabilità ad alta densità, le attuali misure sono ancora valide?

- Le tipiche **misure tecniche ed organizzative di sicurezza digitale**, **dal costo crescente**, ***sono ancora sufficienti ed efficaci?***
  - Sono **necessarie** **ma non sufficienti**, con una continua e costosa rincorsa per far fronte alle nuove vulnerabilità e ai nuovi attacchi, che in molti casi sono comunque a favore degli attaccanti
- Molti esperti, a livello mondiale, ritengono che non si debba più spendere prevalentemente per tali misure (ma sono ancora necessarie), ma investire di più in **misure per bloccare e reprimere l'hackeraggio/cyber crime**, riducendo fortemente i loro alti guadagni con pochissimi rischi
  - *… If they [vulnerabilities] are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it." (da Dan Geer)*
  - *But if you care about systemic security […] don't chase and fix vulnerabilities, […] design a system around fundamentally stopping routes of impact. (da Bas Alberts)*
- **Si dovrebbe entrare nella logica di security by design e by default, ossia di sicurezza digitale intrinseca nei dispositivi e nelle applicazioni ICT, indipendentemente dal buono o cattivo uso da parte dell'utente finale. Ma allo stato attuale è realmente fattibile? Alcuni passi in tale direzione sono già stati compiuti o si stanno compiendo**

Esempi di novità per la sicurezza digitale a livello tecnico (elenco non esaustivo)

- Nuove logiche e tecniche di autenticazione: out of band, passwordless, FIDO2, etc.
- Nuove logiche e tecniche di autorizzazione: Diameter, NGAC, NISTIR 8112, etc.
- intelligenza artificiale (AI), sistemi esperti, machine learning
- Analisi comportamentale sistemi e utenti : AI, logiche bayseniane, etc.
- Crescente integrazione tra security e safety nell'ambito dei *cyber physical system*
- Crescente integrazione ed innovazione nei sistemi di monitoraggio e controllo
- Nuove logiche ed ambienti di sviluppo sw: **DevOps**, leaning/agile programming, etc., ritenuti (ma è vero?) intrinsecamente sicuri
- Blockchain: utilizzi al di fuori delle cripto valute, prevalenza soluzioni private (chiuse)
- ……

Novità a livello organizzativo e normativo

- **A livello organizzativo**
  - ITIL 4, profonda evoluzione di ITIL 3/2011
  - COBIT 2019
  - Mancanza competenze e sensibilizzazione (soprattutto ai vertici) sulla sicurezza digitale
  - Crescita terziarizzazione servizi di sicurezza digitale
  - Impatto della gestione e della terziarizzazione della sicurezza digitale sulla struttura organizzativa

- **A livello normativo europeo ed italiano**
  - Direttiva EU 2019/881 chiamata **CyberSecurity Act,** formalmente in vigore dal 27/6/2019**,** a completamento della Direttiva EU 2016/1148 chiamata **NIS**, Network and Information Security (D.Lgs. 65/2018, formalmente in vigore dal 27/6/2019), che fa riferimento a carrier TLC e a infrastrutture critiche
  - Dal 2019 impatto crescente delle azioni del Garante sulla compliance al GDPR

Per finire …

Qualche considerazione finale …

- La sicurezza digitale assoluta non esiste e non può esistere
- Occorre una **soluzione ben bilanciata** tra le varie misure tecniche ed organizzative, tenendo anche conto delle misure già in essere
- Occorre sensibilizzare e formare il personale a tutti i livelli sulla sicurezza digitale
- La sicurezza digitale è multidisciplinare e costosa: **ma quanto costa la non sicurezza**?
- Occorre sostanzialmente far leva sul ruolo della cybersecurity:
  - **per la continuità operativa del business** (non entrare in dettagli tecnici con i decisori)
  - per evitare **sanzioni civili e penali**
  - per salvaguardare **l'immagine aziendale** (brand reputation)
- Nella maggior parte dei casi **occorre terziarizzare la sicurezza digitale**, dal progetto alla gestione operativa (es. SOC): ma questo non vuol dire rinunciare alle competenze in merito, altrimenti si diverrà preda dei fornitori →
- Proporre al vertice soluzioni per l'ICT e la sua sicurezza nell'ottica del business

Domande ?

RIFERIMENTI

- m.bozzetti@aipsi.org

- https://www.aipsi.org/
- https://www.oadweb.it/
- https://www.malaboadvisoring.it/