La situazione sugli attacchi digitali in Italia dal Rapporto OAD 2018 e suggerimenti su come prevenirli e contrastarli

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

Marco R. A. Bozzetti e Malabo Srl

- Ingegnere elettronico al Politecnico di Milano, è Presidente AIPSI e CEO di Malabo Srl
- 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 responsabile dei sistemi informativi (CIO) dell'intero Gruppo ENI (1995-2000).
- Nella seconda metà degli anni 70 è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, partecipando alla standardizzazione dei protocolli del modello OSI dell'ISO
- È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser"
- Commissario d'Esame per le certificazioni eCF (EN 16234 - UNI 11506).
- Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

- Malabo Srl è stata creata da M. Bozzetti nel 2001
- una società di consulenza direzionale per l'ICT, che opera per Clienti lato domanda e lato offerta basandosi su una consolidata rete di esperti e di società ultra specializzate
- Obiettivo primario degli interventi di Malabo è di creare valore misurabile per il Cliente, bilanciando adeguatamente gli aspetti tecnici con quelli organizzativi nello specifico contesto del Cliente
- Dispone di un proprio laboratorio ICT con server e storage duali, virtualizzati, , collegati con switch a 10 G e connessi ad internet con fibra ottica a 100 Mbps, oltre ad uno spazio in cloud (IaaS)
- Per garantire un effettivo trasferimento di know-how, fornisce come servizio ai Clienti le proprie metodologie e gli strumenti informatici usati nell'intervento consulenziale

smau
MILANO 23-24-25 OTTOBRE 2018
fieramilanocity

Siamo presenti per tutti i 3 giorni di SMAU nella Area Community ICT

VIENI A TROVARCI !

AIPSI - www.aipsi.org

- **AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo Italiano** di **ISSA**, Information Systems Security Association, (**www.issa.org**) **che conta** >>10.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo

- **AIPSI è il punto di aggregazione sul territorio e di trasferimento di know-how per i professionisti della sicurezza digitale, sia dipendenti sia liberi professionisti ed imprenditori del settore**

- **Sede Centrale:** Milano
- **Sedi territoriali** : Ancona-Macerata, Lecce, Torino, Verona-Venezia
- **Contatti**: aipsi@aipsi.org, segreteria@aipsi.org

aipsi ISSA OAD Osservatorio Attacchi Digitali in Italia malabo ICT Advisory

smau
MILANO 23-24-25 OTTOBRE 2018
fieramilanocity

Primari obiettivi AIPSI

- Aiutare i propri Soci nella **crescita professionale** e quindi nella crescita del loro business
- Offrire ai propri Soci **servizi qualificati** per tale crescita, che includono
  - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
  - Rapporti annuali e specifici **OAD, Osservatorio Attacchi Digitali in Italia** nel nuovo sito **https://www.oadweb.it**
  - Supporto nell'intero ciclo di vita professionale
  - Formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016, in Italia UNI 11506)
- Rapporti con altri soci a livello nazionale (AIPSI) ed internazionali (ISSA)
- Contribuire alla diffusione della cultura e alla sensibilizzazione per la sicurezza digitale
- Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte

Creazione del Gruppo di lavoro
CSWI,
Cyber Security Women's Italy,
aperto anche alle Signore non Socie AIPSI

A breve disponibile il nuovo
Rapporto 2018 OAD

aipsi
ISSA
OAD Osservatorio Attacchi Digitali in Italia
malabo ICT Advisory

smau MILANO 23-24-25 OTTOBRE 2018

fieramilanocity

I Workshop di AIPSI a SMAU Milano 2018

Data	Ora	Luogo in SMAU MI	Speaker	Titolo workshop formativo
23/10/2018	15.30	**Arena ICT2**	Massimo Chirivì	Social Engineering and other Foes in the GDPR Year
23/10/2018	13.30	**Arena ICT2**	Marco Bozzetti	Privacy GDPR: ma quanto mi dovresti costare?
24/10/2018	16.00	**Arena ICT1**	Luca Bonadimani	Introduzione alla Cybersecurity dei servizi Cloud
24/10/2018	10.30	**Arena ICT3**	Marco Bozzetti	La situazione sugli attacchi digitali in Italia dal Rapporto OAD 2018 e suggerimenti su come prevenirli e contrastarli
25/10/2018	12.30	**Arena ICT2**	Tiberio Pitassi	Grafometria: significative innovazioni nell'identificazione e nella gestione documentale per grandi e piccole organizzazioni
25/10/2018	16.30	**Arena ICT3**	Giovanni Zanetti	Company Binding Rules - GDPR

aipsi ISSA OAD Osservatorio Attacchi Digitali in Italia malabo ICT Advisory

smau
MILANO 23-24-25 OTTOBRE 2018
fieramilanocity

Le principali novità di AIPSI 2017-18

- Nuovo sito web dell' Associazione: https://www.aipsi.org
- Nuovo sito web per OAD: https://www.oadweb.it
- Sedi territoriali AIPSI: Macerata, Venezia, Verona, Torino
- Accordo con AICA per promuove le certificazioni eCF sulle competenze della sicurezza digitale
- Supporto al CSCL, Cyber Security Career Lifecycle
- Azioni in corso per essere riconosciuti dal MISE, Ministero Sviluppo Economico, entro la fine del 2018 come Associazione rappresentativa dei professionisti della sicurezza digitale secondo la Legge 4/2013
- Webinar asincroni e sincroni
- Nuovo Media Partner: Reportec

aipsi
ISSA
OAD Osservatorio Attacchi Digitali in Italia
malabo ICT Advisory

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**

OAD-OAI 2008 - 2018 : 10 anni di indagini via web

smau
MILANO 23-24-25 OTTOBRE 2018
fieramilanocity

Indagine OAD 2018

Il Rapporto 2018 sarà pubblicato a breve

SPONSOR

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


BUSINESS
MATCHING
STARTUP SAFARI
INNOVAZIONE ACADEMY
OPEN INNOVATION
FORMAZIONE ICT
NETWORKING

OAD 2018

OAD 2018: tante novità dal Questionario al Rapporto

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

Che cosa è attaccato	Come (tecniche attacco)						
	Attacco fisico	Raccolta Informazioni (es. social engineering, phishing, pharming, hoax, scanning, indagini su	Script e programmi maligni (ransomware, spyware, adware, …)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente,	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit,	Strumenti distribuiti controllati centralmente (Command Control)	utilizzo di due o più delle precedenti tecniche (APT, Advanced
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 al DNS							
Uso non autorizzato risorse ICT (dal PC al 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							

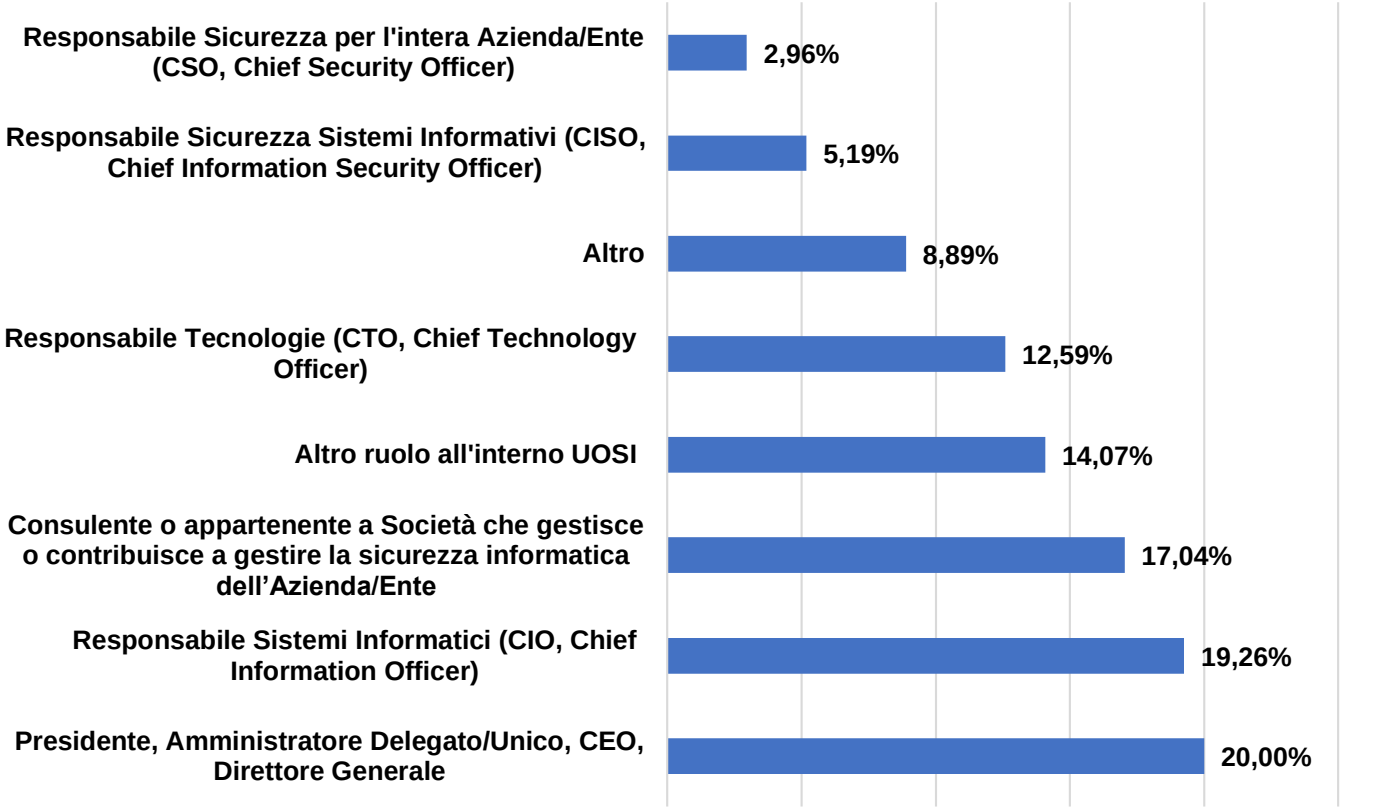
- per ogni tipo di attacco (che cosa), se l'attacco è stato rilevato appaiono delle sotto domande che includono:
  - la frequenza di attacchi
  - le "macro" tecniche di attacco (come)
  - i principali impatti subiti dall'attacco più grave
  - le possibili motivazioni dell'attacco più grave
  - il tempo 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

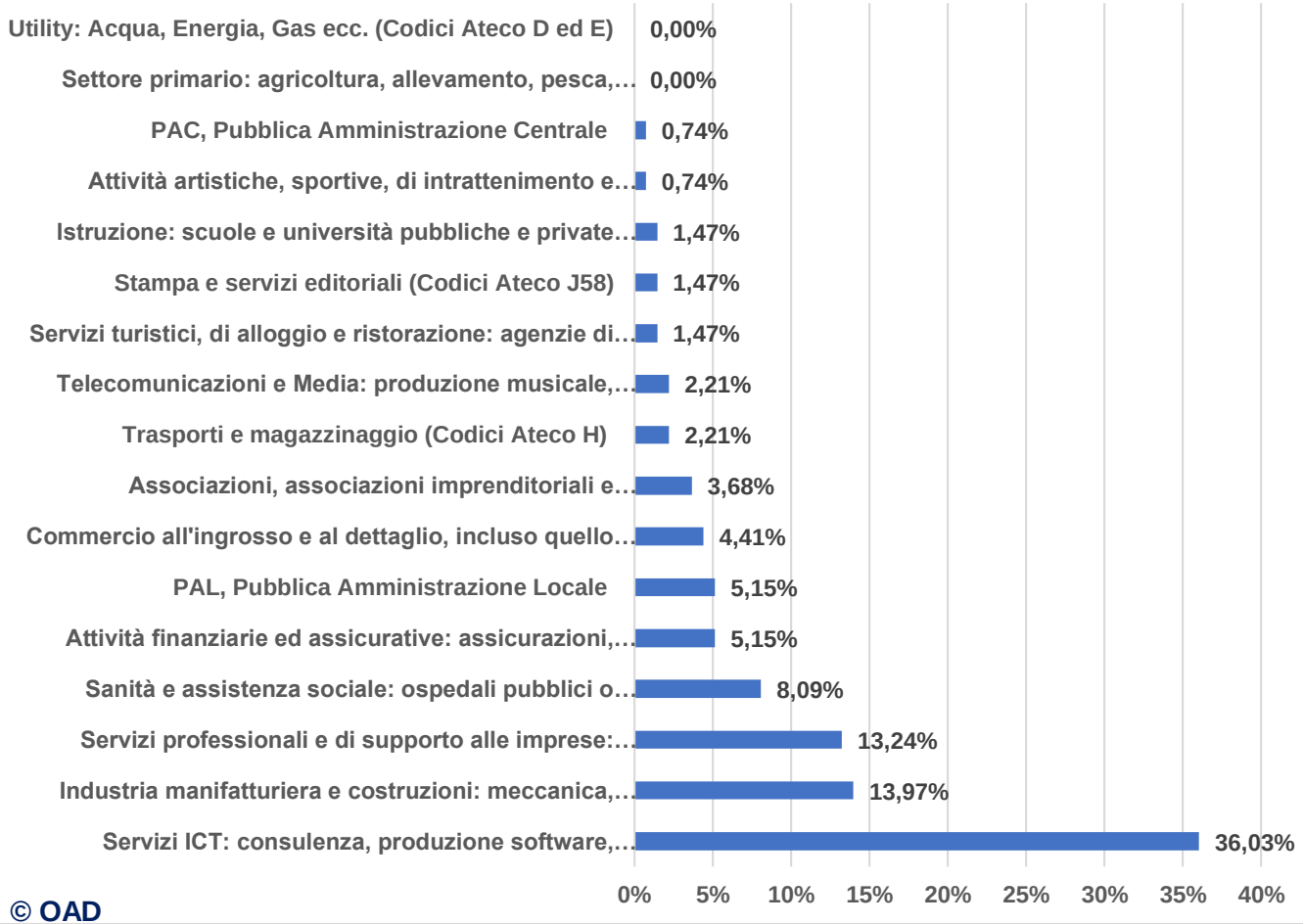
Attacchi a IoT

Attacchi sistemi aut. industriale e robotici

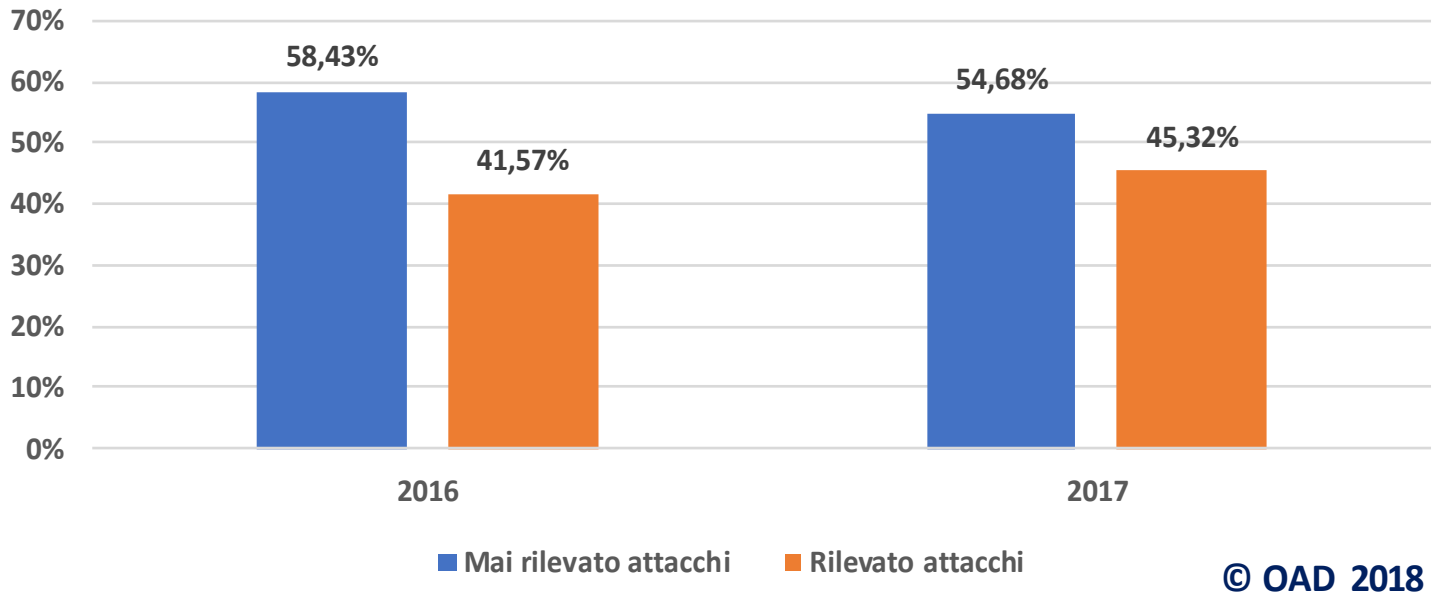
Ruolo del compilatore del questionario OAD 2018

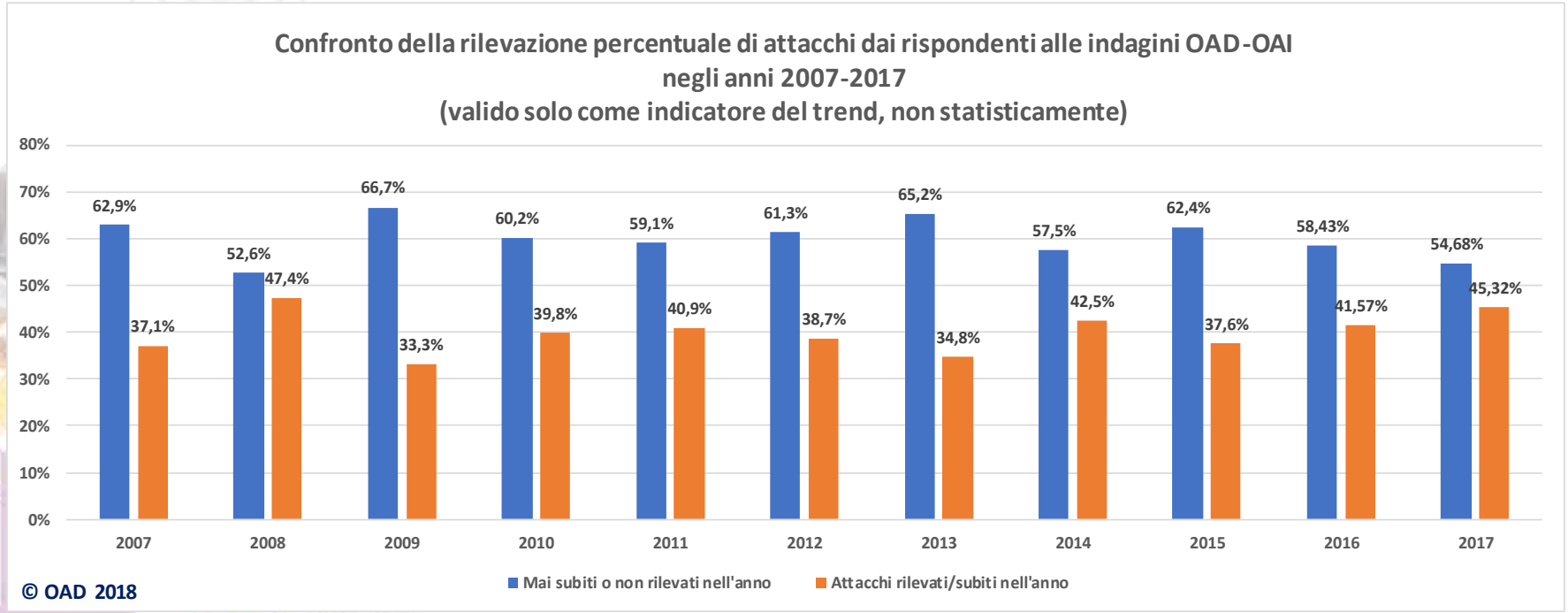


Settore merceologico di attività dell'Azienda/Ente rispondente

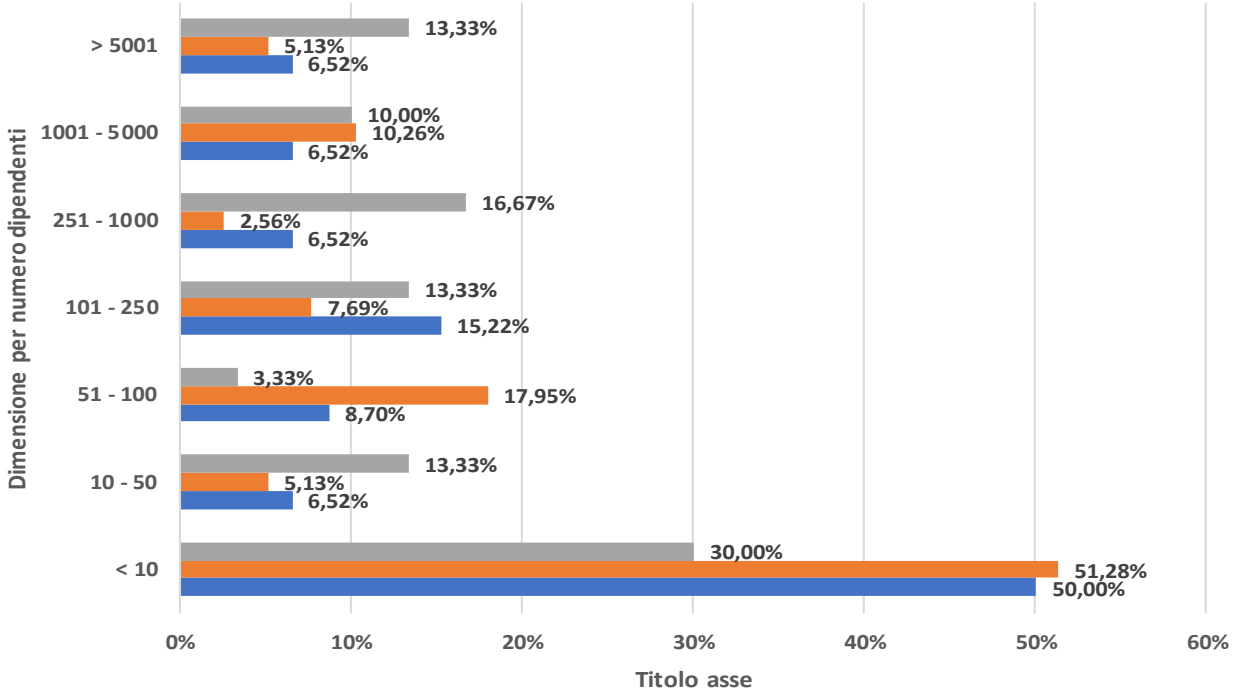


Numero di attacchi rilevati nel 2016 e nel 2017 dai rispondenti OAD 2018

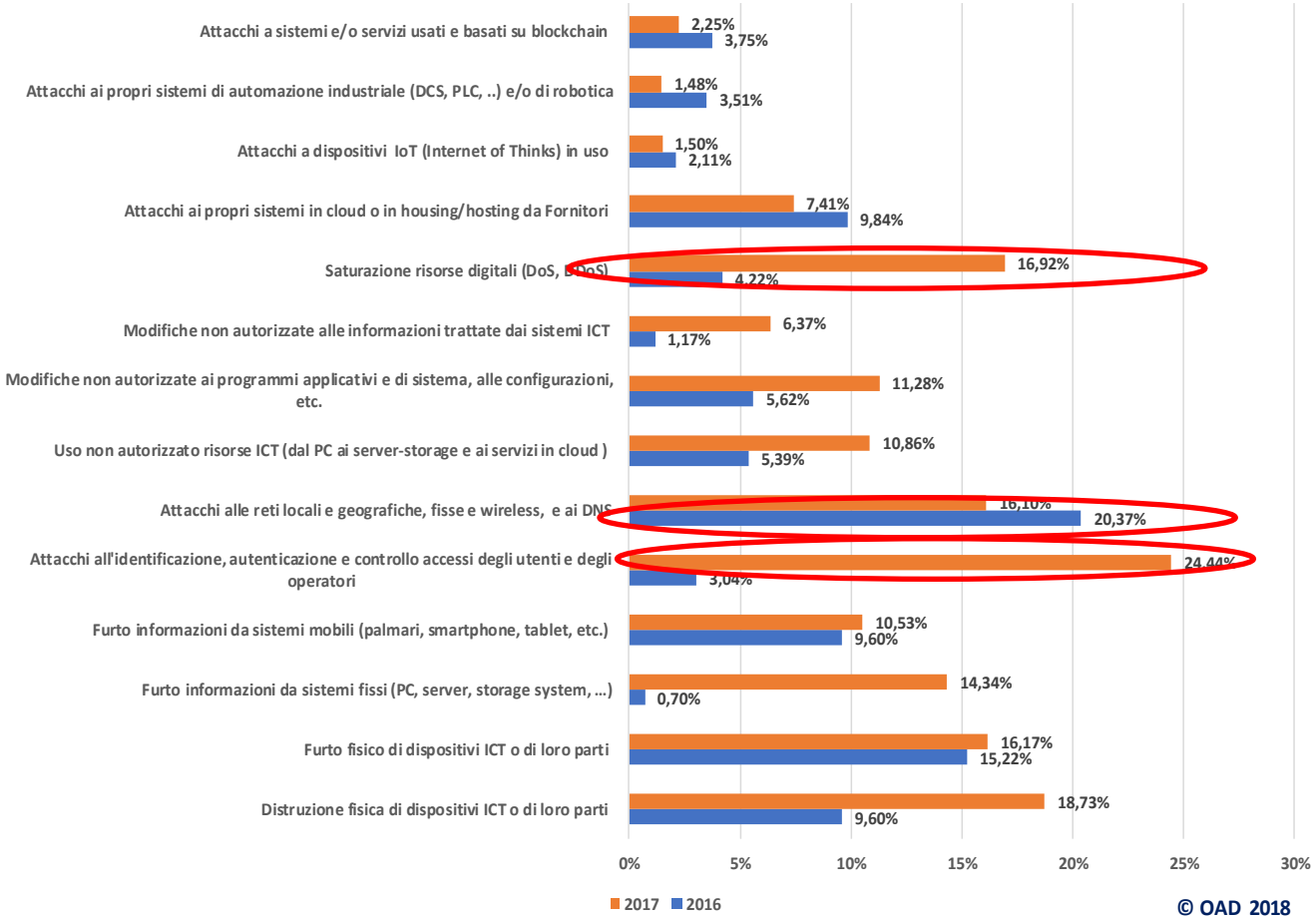



Confronto della rilevazione percentuale di attacchi dai rispondenti alle indagini OAD-OAI
negli anni 2007-2017
(valido solo come indicatore del trend, non statisticamente)
80%
70%
60%
50%
40%
30%
20%
10%
0%
62,9%
37,1%
52,6%
47,4%
66,7%
33,3%
60,2%
39,8%
59,1%
40,9%
61,3%
38,7%
65,2%
34,8%
57,5%
42,5%
62,4%
37,6%
58,43%
41,57%
54,68%
45,32%
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
Mai subiti o non rilevati nell'anno
Attacchi rilevati/subiti nell'anno

Ripartizione % attacchi rilevati nel 2017 per dimensione azienda/ente del rispondente



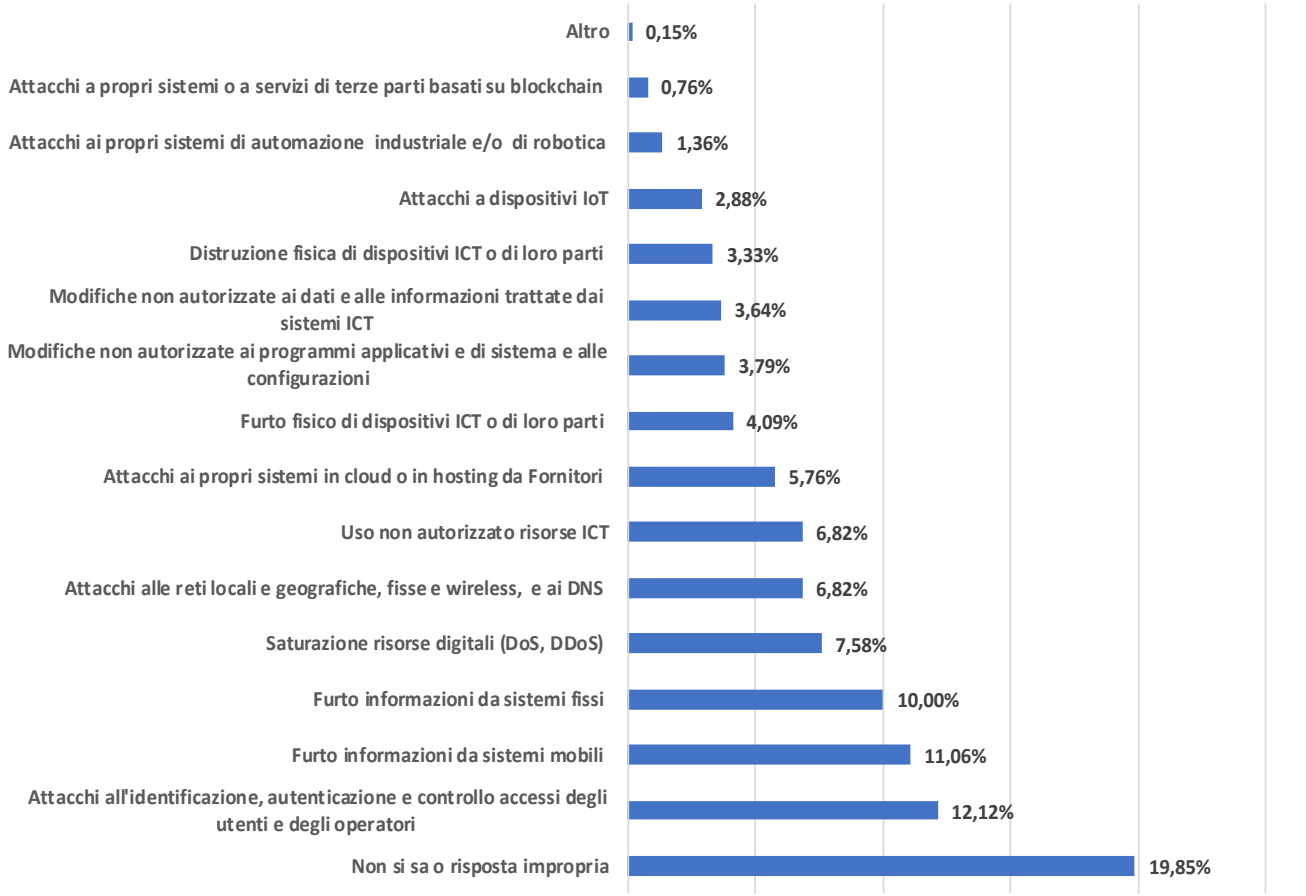
Diffusione % tipologia attacchi (che cosa attacco) rilevati dai rispondenti nel 2016 e nel 2017 (risposte multiple)



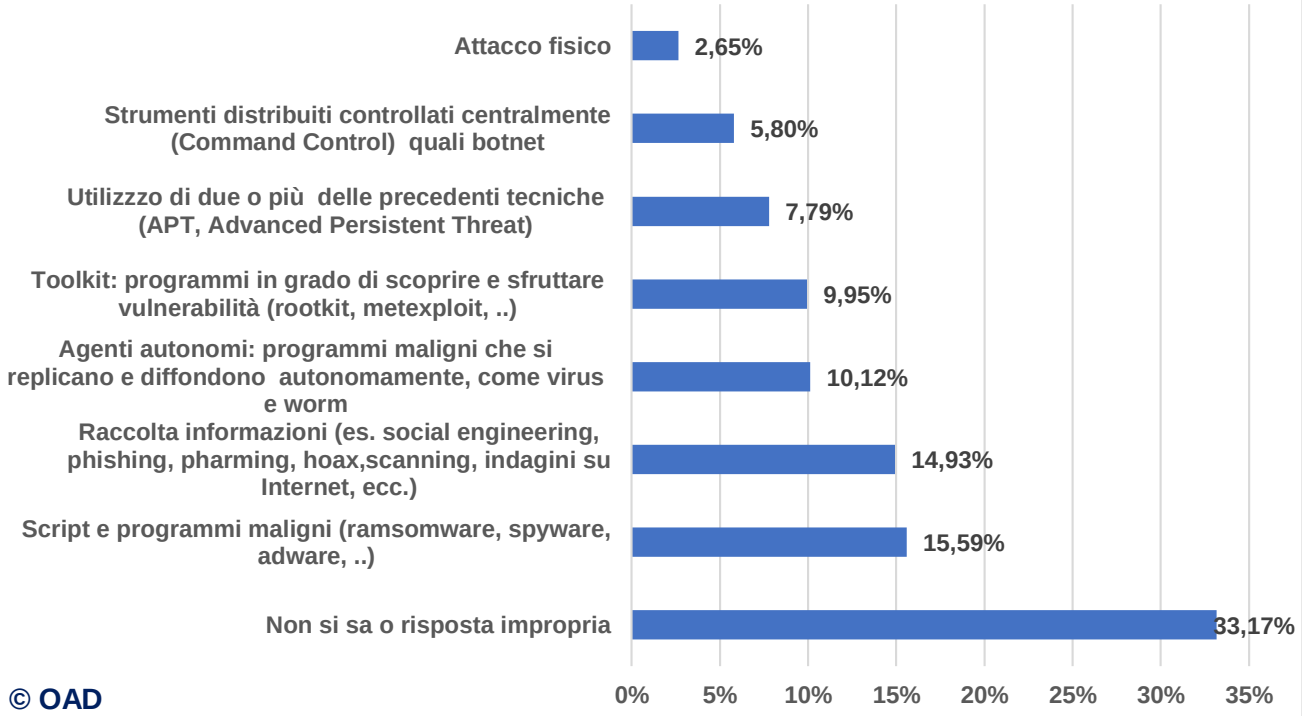
% tecniche di attacco su tipologie di attacco 2017

Tipologia attacchi	Attacco fisico	Script e programmi maligni	Raccolta informazioni	Agenti autonomi	Botnet e simili	Toolkit
Attacchi a dispositivi IoT (Internet of Thinks) in uso	0,00%	18,18%	0,00%	18,18%	18,18%	27,27%
Attacchi a sistemi e/o servizi usati e basati su blockchain	0,00%	13,33%	0,00%	26,67%	20,00%	13,33%
Attacchi ai propri sistemi di automazione industriale (DCS, PLC, ..) e/o di robotica	0,00%	15,38%	0,00%	15,38%	23,08%	23,08%
Attacchi ai propri sistemi in cloud o in housing/hosting da Fornitori	0,00%	25,00%	3,13%	18,75%	9,38%	15,63%
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS	6,76%	24,32%	20,27%	10,81%	8,11%	12,16%
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori	1,96%	25,49%	24,51%	15,69%	4,90%	13,73%
Distruzione fisica di dispositivi ICT o di loro parti	100,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Furto fisico di dispositivi ICT o di loro parti	100,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Furto informazioni da sistemi fissi (PC, server, storage system, …)	2,53%	32,91%	20,25%	18,99%	7,59%	10,13%
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)	7,50%	22,64%	20,75%	11,32%	9,43%	7,55%
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.	1,72%	29,31%	12,07%	18,97%	8,62%	13,79%
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT	0,00%	21,21%	21,21%	15,15%	9,09%	15,15%
Saturazione risorse digitali (DoS, DDoS)	0,00%	19,12%	10,29%	10,29%	19,12%	16,18%
Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)	0,00%	24,49%	20,41%	16,33%	10,20%	10,20%
Diffusione tecnica di attacco (come) nelle tipologie (che cosa)	**220,47%**	**271,38%**	**152,89%**	**196,53%**	**147,70%**	**178,20%**

Attacchi (che cosa) più temuti nel prossimo futuro (risposte multiple)

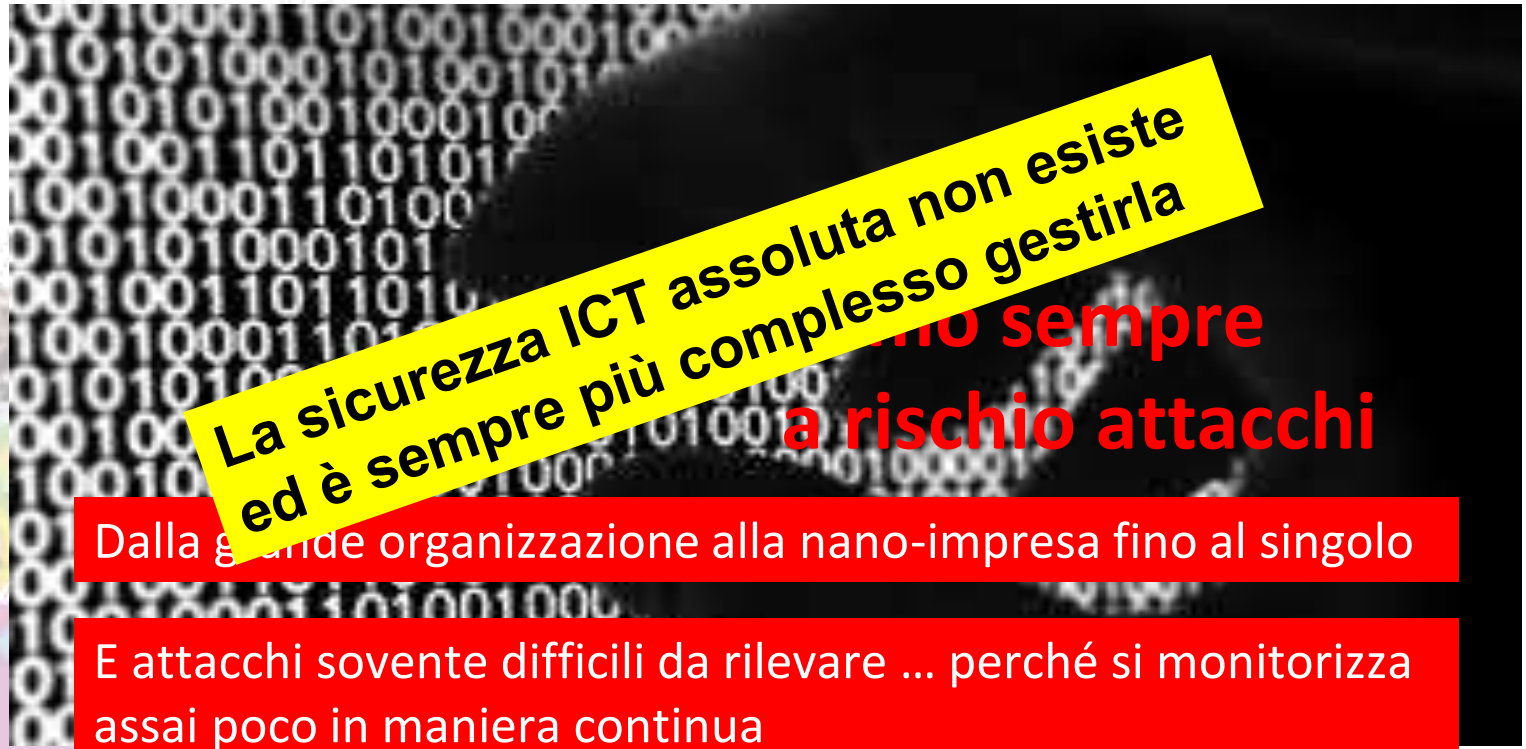


Tecniche di attacco (come) più temute nel prossimo futuro (risposte multiple)



Ma quali rischi a livello ICT?

Gli attacchi digitali: sempre di più e sempre più critici



Dalla grande organizzazione alla nano-impresa fino al singolo

E attacchi sovente difficili da rilevare … perché si monitorizza assai poco in maniera continua

Due grandi categorie di attacchi digitali

- **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

Vulnerabilità causa 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

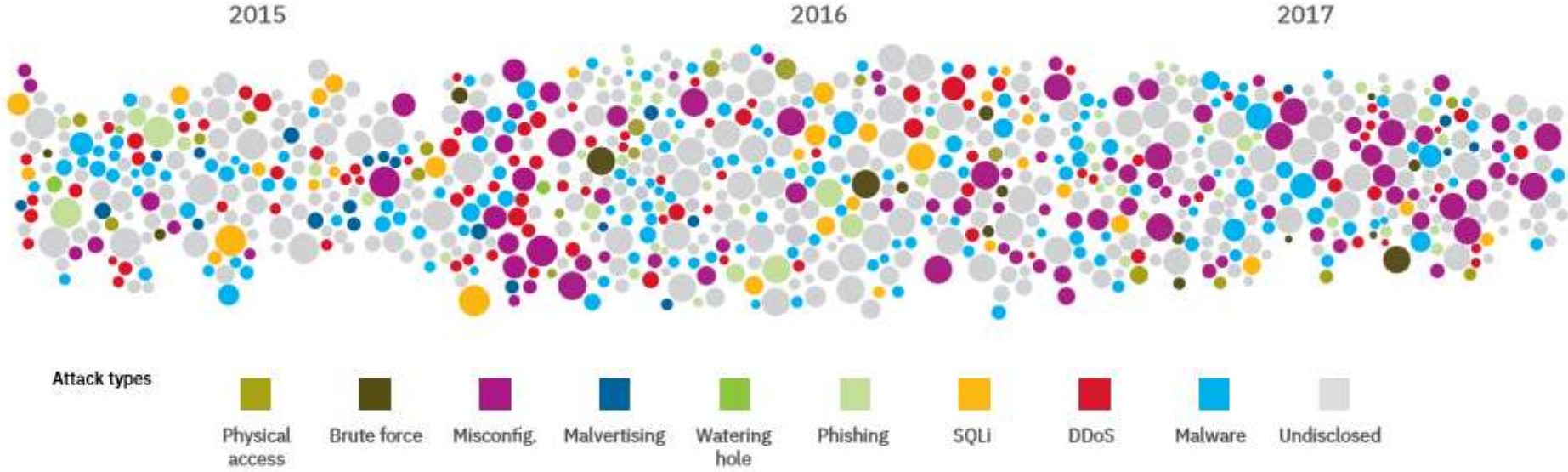
La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

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

Aggravata dalla non o inefficace organizzazione

Mancanz di formazione e addestramento

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

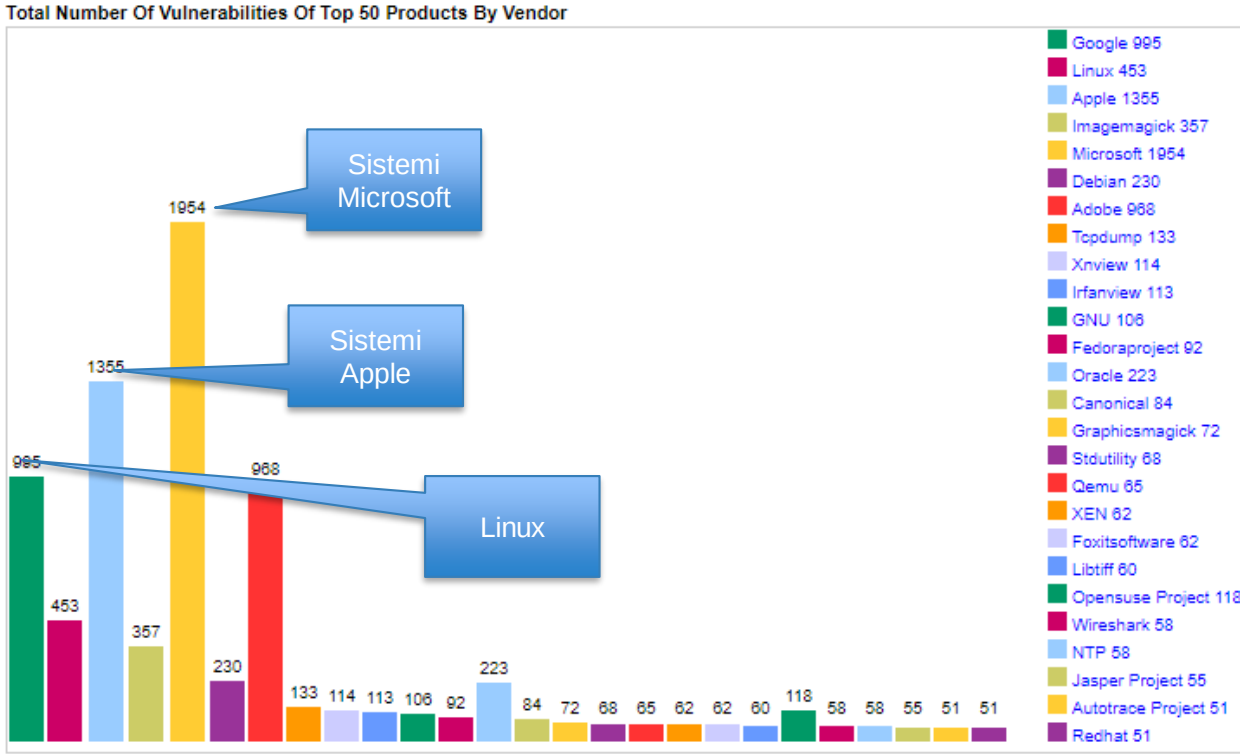


Cover Image: Sampling of security incidents by attack type, time and impact, 2015 through 2017.

Fonte: IBM Xforce, aprile 2018

CVE: vulnerabilità per prodotto

Fonte: DB CVE 2018



Quali difese ?

I principali strumenti di difesa

→ *ORGANIZZATIVI*

- da approccio reattivo a proattivo
- contestualizzare misure tecniche ed organizzative alla propria realtà

→

- Analisi dei rischi e degli impatti
- approccio architetturale ben bilanciato
- riferimento ai principali standard e alle best practices ben consolidate: OSA, ITIL v3, Cobit, ISO 27000, NIST SP, …

Le misure di sicurezza digitale per il GDPR

- Le misure richieste di sicurezza digitale riguardano:
  - Le misure generali atte a garantire riservatezza, disponibilità, integrità, resilienza
  - Misure specifiche sui dati personali per
    - Pseudonimizzazione e Cifratura
    - L'individuazione di data breach
    - La gestione degli accou[illegible]nte nominativi) e dei log
  - Misure di gestione [illegible] delle misure stesse per il controllo e la verifica d[illegible]isure sicurezza
- Tutte l[illegible] misure di sicurezza debbono essere individuate ed attuate dal [illegible]ontestualizzate sulla realtà delle sue attività, dei suoi sistemi informatici e dei suoi rischi

Sono necessarie e vitali per la continuità operativa aziendale

L'evoluzione delle misure di sicurezza digitale …
…. la sfida tra guardie e ladri continua …..

- Le misure di sicurezza digitale evolvono con l'evolversi degli attacchi e della loro compl… bastano a preve…
- Siste… *artificiale, fuzzy …*
- Scann…
- Correl…
- Tecni…
- Nuove…
- Nuove…
- Nuova…
- Evoluz… ica (viene usato … i polarizzati su fibra ottica)

Il problema delle effettive competenze sulla sicurezza digitale

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

- professionisti **certificati**
- **Iscritti** ad **Associazioni** professionali **qualificate**

- La sicurezza digitale è **multi-disciplinare** e richiede una vasta gamma di competenze e di esperienza sul campo
- Difficilmente un'Azienda/Ente può avere al proprio interno specifiche e aggiornate competenze di 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 si può fidare? Come può garantirsi sulle reali competenze dei Fornitori e dei Consulenti?

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

I 10 comandamenti per la sicurezza digitale

1. La sicurezza assoluta non esiste, **e la sicurezza ha un costo: ma quale è il costo della non sicurezza?**
2. La Legge di Murphy è sempre vera, prima o poi qualche guaio arriva: bisogna essere preparati al ripristino
3. Il peggior nemico: la “falsa” sicurezza
4. La sicurezza è un processo continuo, sia per la parte tecnica che per la parte organizzativa
5. La sicurezza “globale” deve essere calata nello specifico contesto dell’Azienda/Ente: i suoi processi, i suoi sistemi, la sua organizzazione, la sua cultura
6. Sensibilizzare, formare, addestrare in maniera continua sia gli utenti finali sia gli operatori-amministratori di sistema
7. Qualunque siano le soluzioni e le modalità di intervento prescelte, è sempre il top management che deve dare un forte commitment, che deve guidare i fornitori, che deve dare il buon esempio
8. Prevenire, prevenire, prevenire: ma per far questo occorre misurare e controllare sistematicamente
9. La velocità e la complessità degli attuali attacchi è tale che i processi di gestione della sicurezza devono essere automatizzati
10. La sicurezza ICT è come una catena: tanto sicura quanto il suo anello più debole. Essa deve quindi essere “ben bilanciata” tra le varie misure e strumenti

Grazie per l'attenzione e ..

- **Visitate il sito AIPSI e OAD, e seguite i nostri eventi**
- **Iscrivetevi ad AIPSI-ISSA**