GLI ATTACCHI DIGITALI: LA SITUAZIONE IN ITALIA E COME CONTRASTARLA

Marco R. A. Bozzetti

Presidente AIPSI, Capitolo Italiano ISSA (www.aipsi.org)
Ideatore e realizzatore OAD (www.oadweb.it)
CEO Malabo Srl (www.malaboadvisoring.it)

Marco R. A. Bozzetti e Malabo Srl

- Presidente AIPSI e CEO Malabo Srl, società di consulenza direzionale sull'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 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

AIPSI, Associazione Italiana Professionisti Sicurezza Digitale

- **AIPSI, 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**

- **Primario obiettivo AIPSI: aiutare i propri Soci nella loro crescita professionale e quindi nella crescita del loro business, fornendo servizi qualificati ed autorevoli:**
  - **ISSA Journal, webinar, workshop, convegni**
  - **formazione e certificazione eCF (EN 16234 1:2016)**
  - **Creando una comunità di professionisti**

OAD
Osservatorio
Attacchi Digitali
in Italia

2008 - 2018 : 10 anni di indagini via web

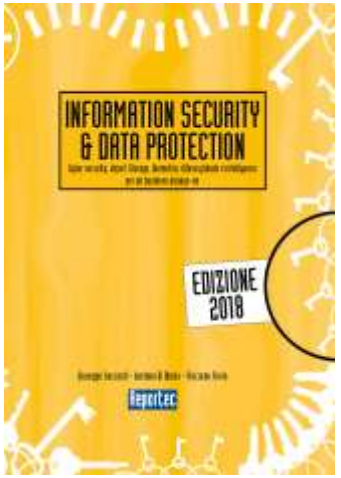
Questionario OAD 2018: da compilare subito! On line ancora per pochi giorni

https://www.oadweb.it/limesurvey/index.php/661199

Assolutamente anonimo, risposte predefinite tra cui scegliere, rapido da compilare con il salto automatico di domande non pertinenti, include domande su attacchi a *sistemi di automazione industriale, IoT, blockchain*

Come ringraziamento a chi completa il Questionario la possibilità di scaricare gratuitamente:

- **ISSA Journal di Gennaio 2018 con i migliori articoli del 2017**
- **Il volume (in pdf) di Reportec " ICT Security e Data Protection 2018"**



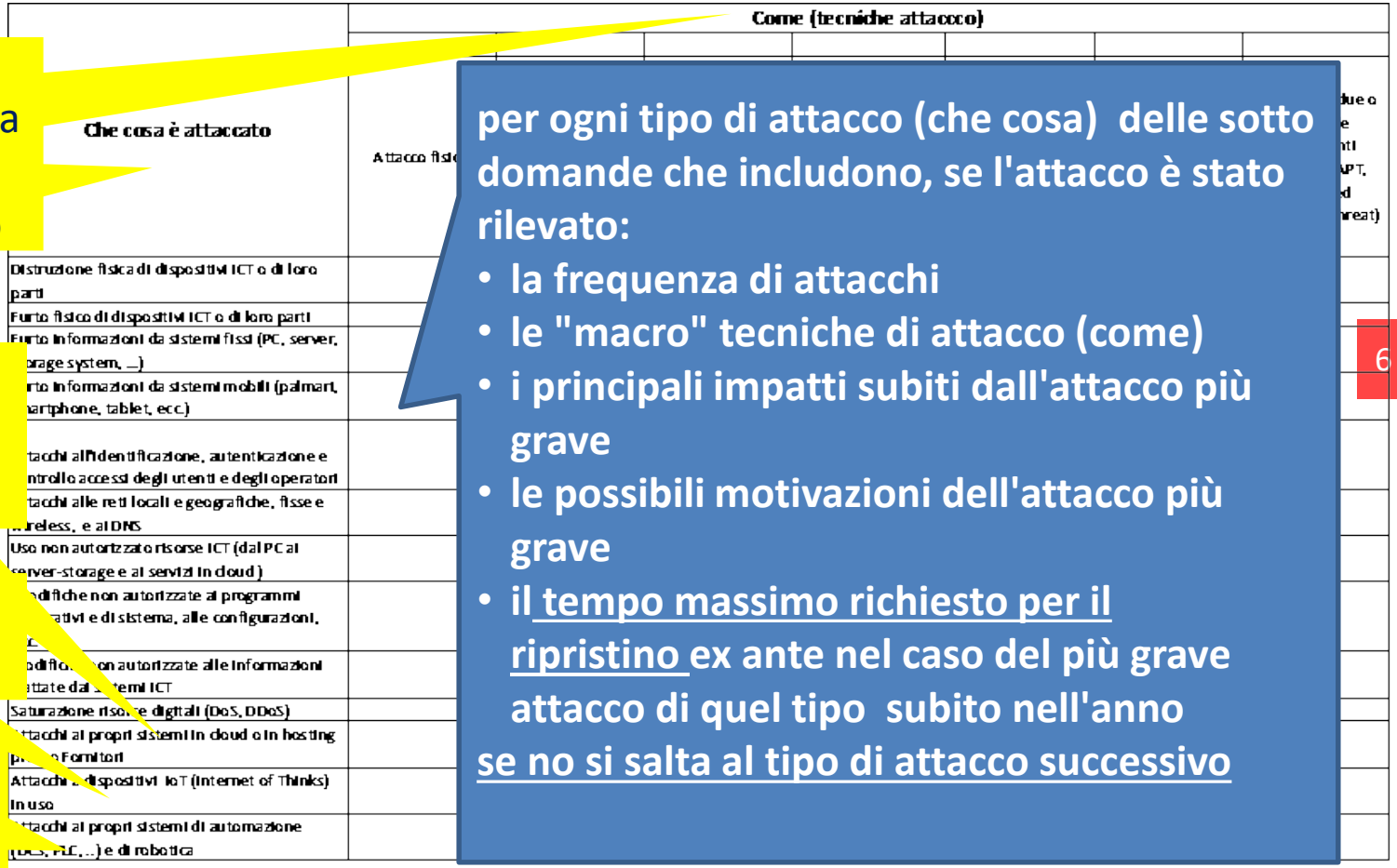
OAD 2018: tante novità a partire dal Questionario

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

Attacchi ai servizi ICT terziarizzati

Attacchi a IoT

Attacchi sistemi aut. industriale e robotici



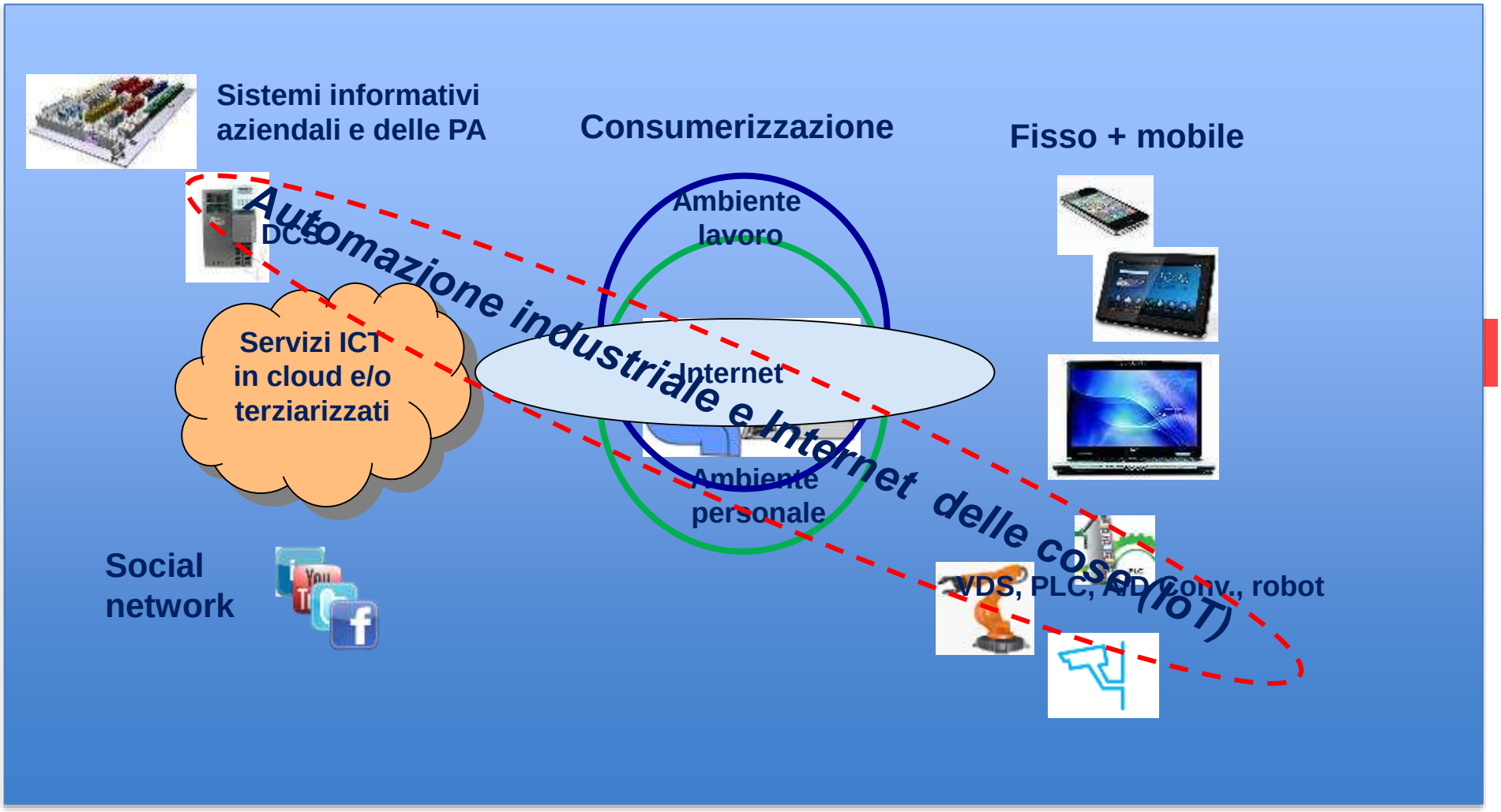
per ogni tipo di attacco (che cosa) delle sotto domande che includono, se l'attacco è stato rilevato:

- 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

6

L' attuale contesto full digital: sicurezza vo' cercando….



Gli attacchi intenzionali

dipendono da *vulnerabilità* dei sistemi ICT e degli esseri umani:

- **Degli applicativi**
- **Dei software di base - middleware**
- **Delle configurazioni e dei settaggi delle opzioni**
- **Delle architetture ICT**
- **Del comportamento degli utenti finali e degli amministratori di sistema**

Vulnerabilità causa delle minacce

Tutte si basano sulle **vulnerabilità tecniche e/o umane-organizzative**

- ***Vulnerabilità tecniche*** (software di base e applicativo, architetture e
  - 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

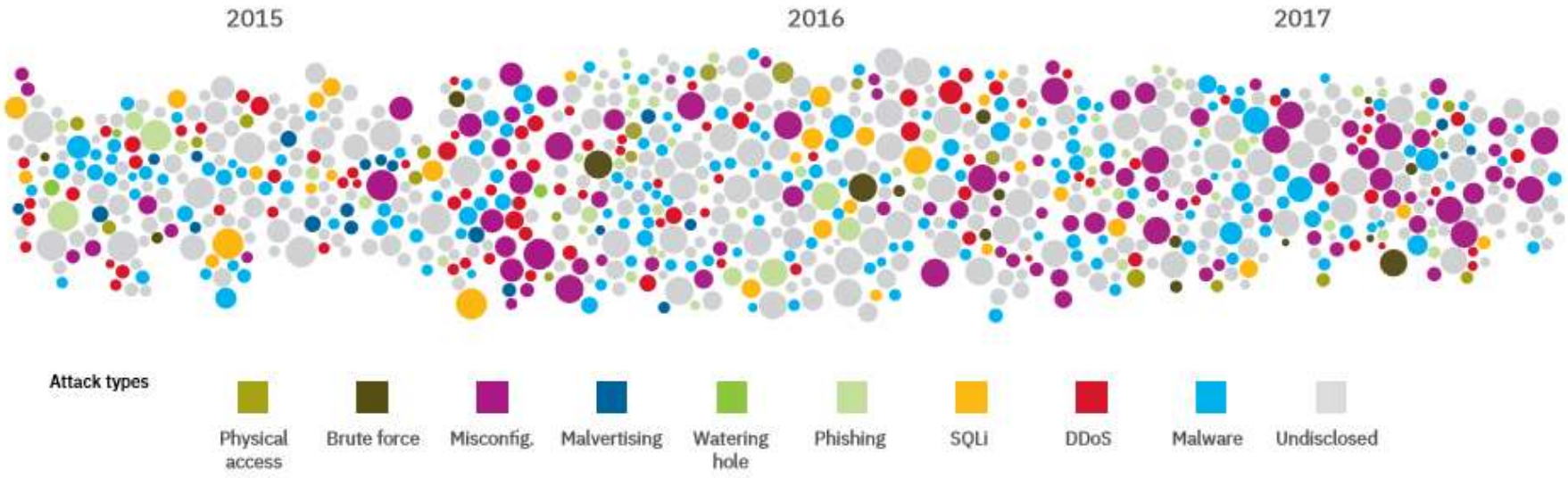
La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

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

Aggravata dalla non o inefficace organizzazione

Mancanza di formazione e addestramento

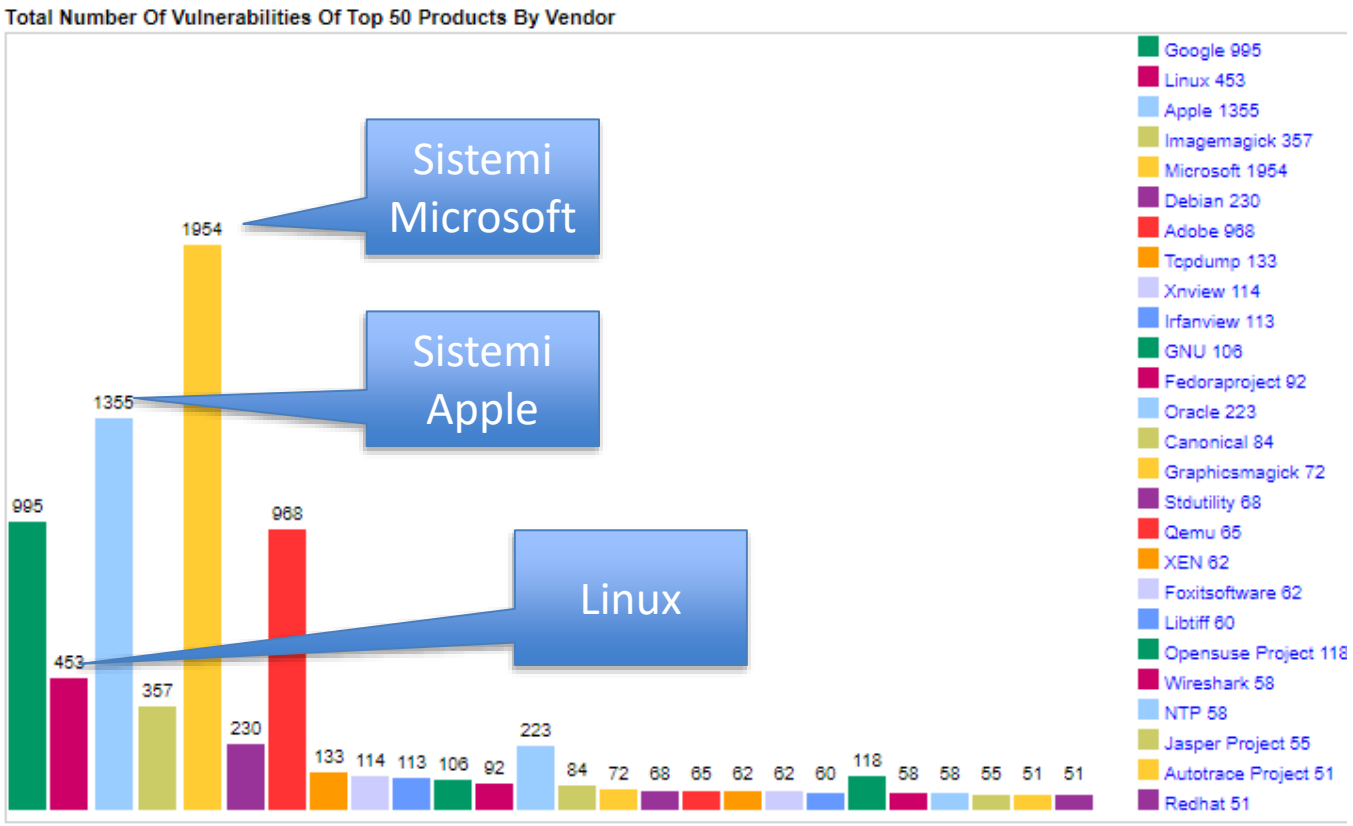
Attacchi 2015-17 per vulnerabilità tecnica a livello mondiale per tipo e durata



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

Due grandi categorie di attacchi

- **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

OAD 2016: ripartizione % per frequenza attacco

Anteprima parziale OAD 2018

CHE COSA

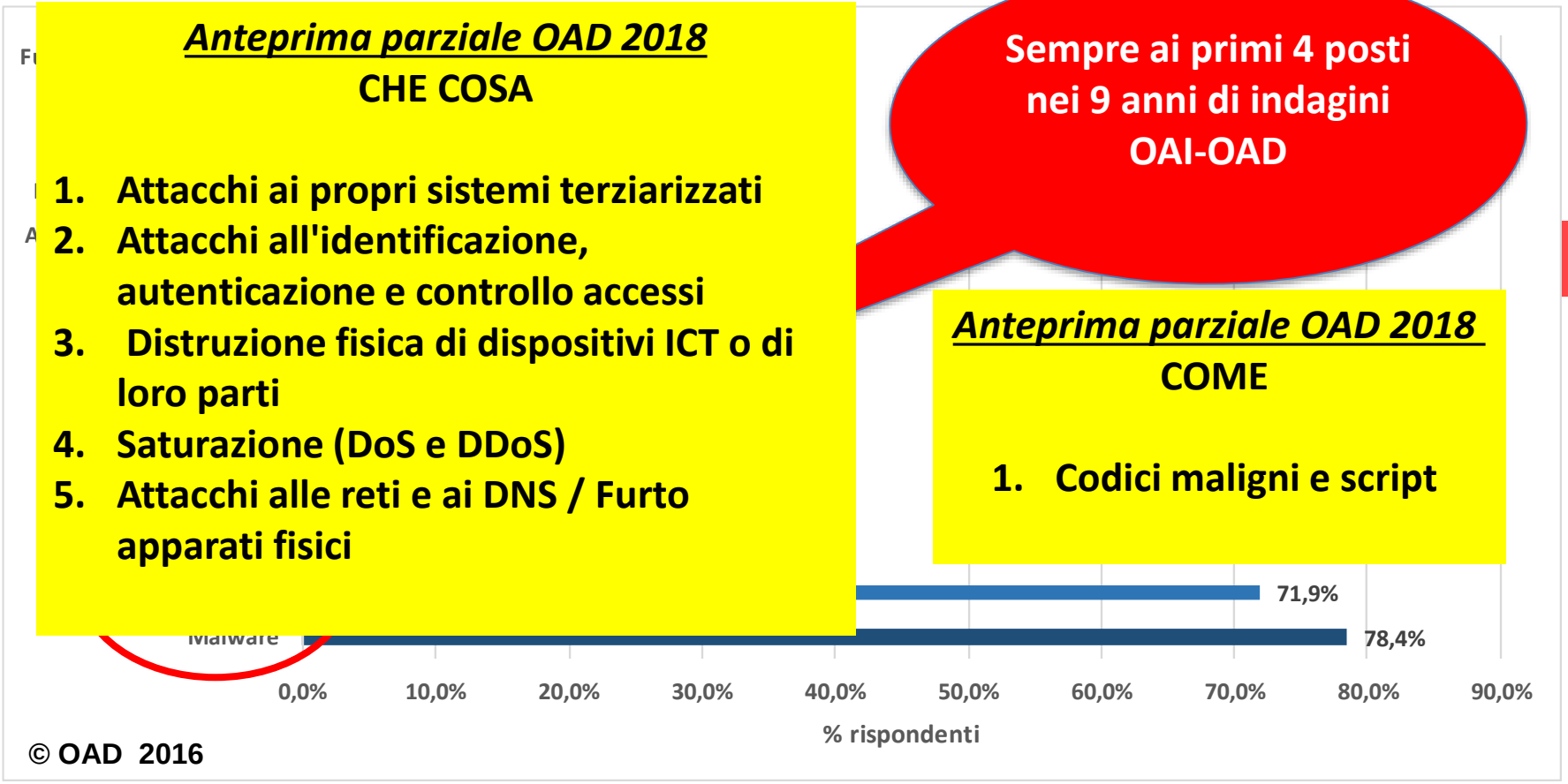
1. **Attacchi ai propri sistemi terziarizzati**
2. **Attacchi all'identificazione, autenticazione e controllo accessi**
3. **Distruzione fisica di dispositivi ICT o di loro parti**
4. **Saturazione (DoS e DDoS)**
5. **Attacchi alle reti e ai DNS / Furto apparati fisici**

Sempre ai primi 4 posti nei 9 anni di indagini OAI-OAD

Anteprima parziale OAD 2018

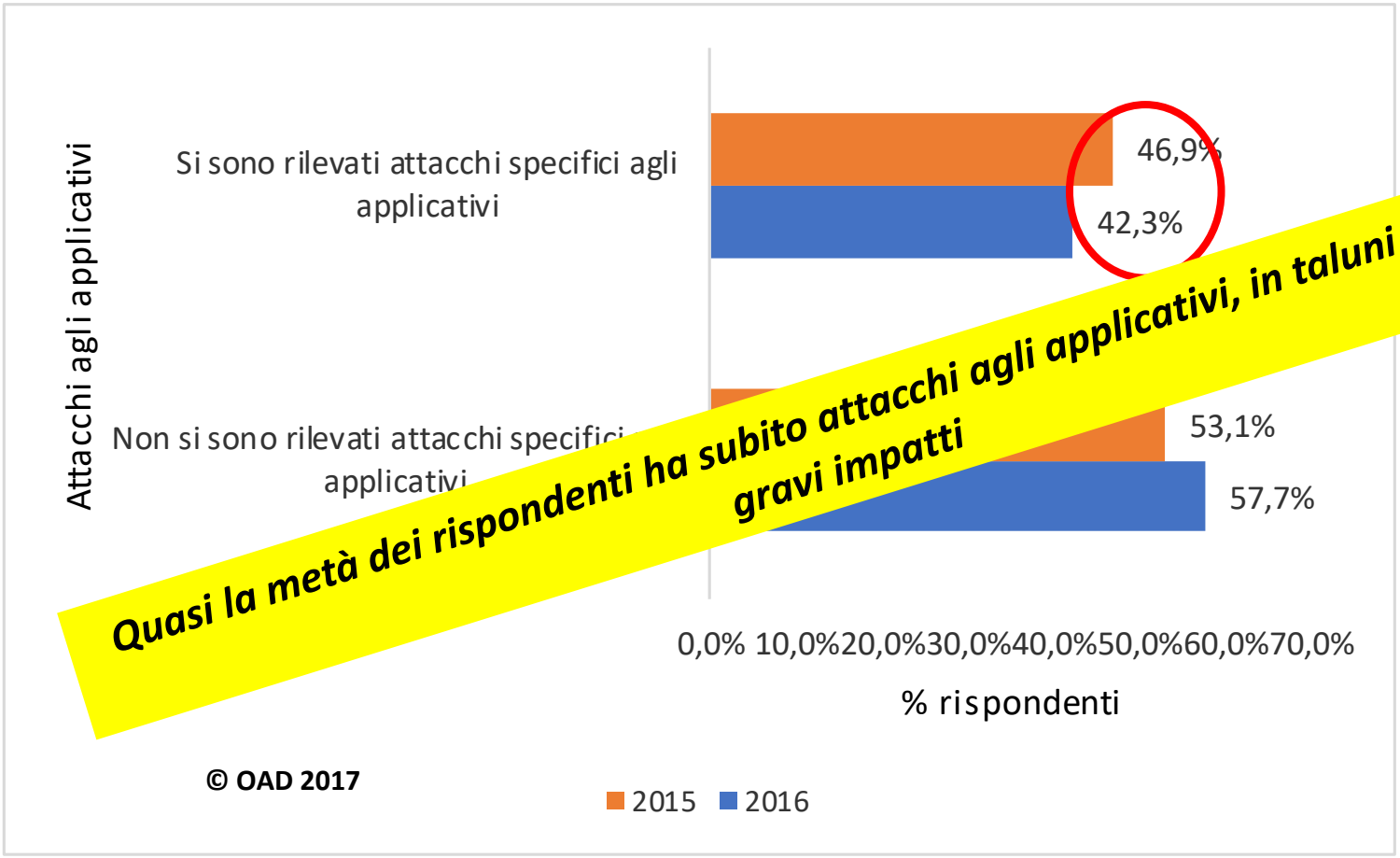
COME

1. **Codici maligni e script**



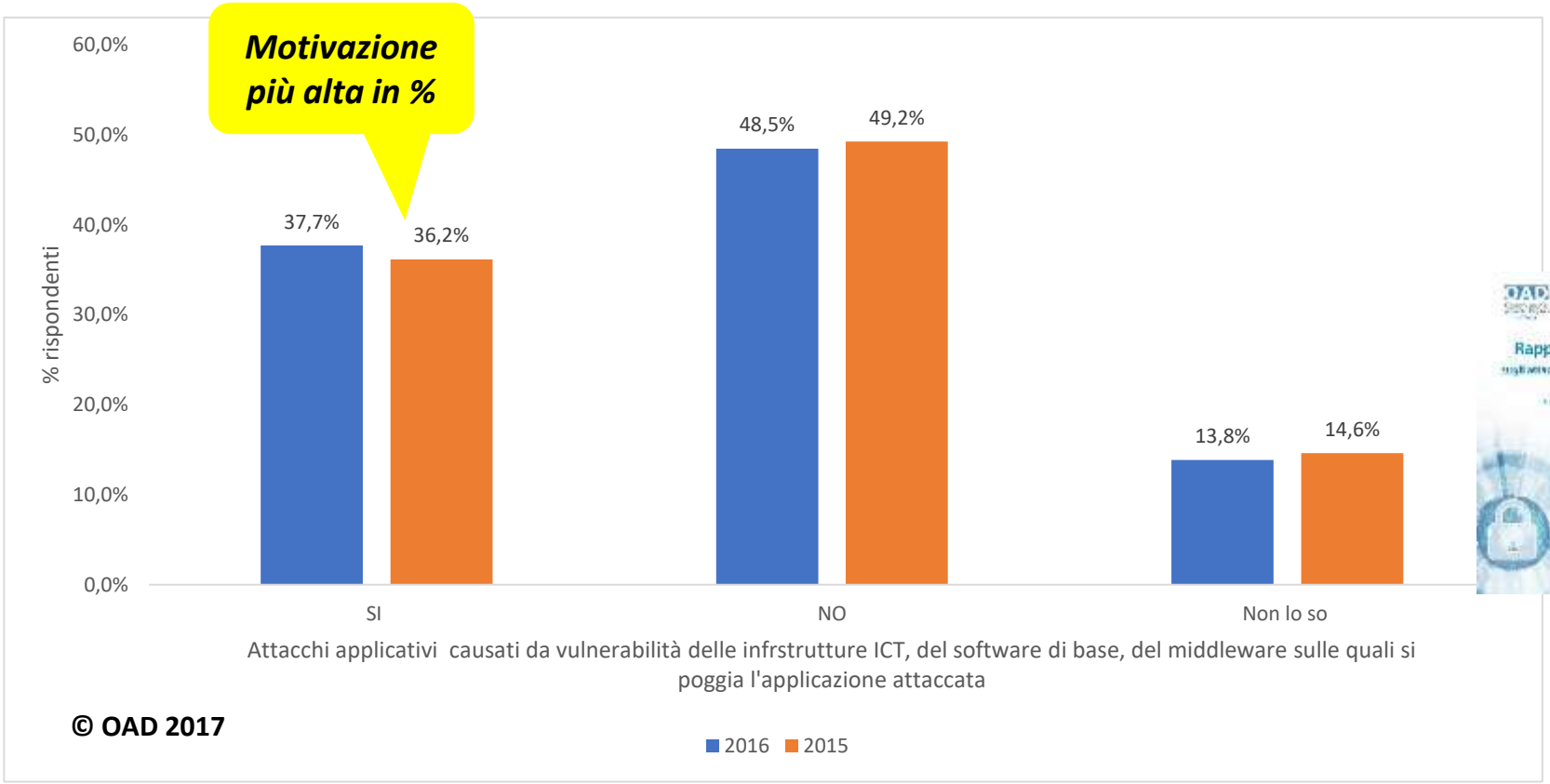
© OAD 2016

OAD AA 2017: Attacchi agli applicativi rilevati



Quasi la metà dei rispondenti ha subito attacchi agli applicativi, in taluni casi con gravi impatti

OAD AA 2017: causati dalle vulnerabilità del sw di base e delle infrastrutture



I principali strumenti di difesa

- ***di prevenzione e protezione***
  - Crittografia, Stenografia
  - Periodiche anali…
  - …
- ***di ri…***
  - …
  - …
- ***di ge…***
  - …
  - …

- **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, …**

…one,

…AP,

…licenze)

…(ITIL V3), help-desk/contact center, ERT, ..

GDPR: le misure di sicurezza richieste (da Art. 32)

- Non sono specificate misure minime come quelle del Codice Unico, ma indicate più ampie misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono:
  - la **pseudonimizzazione** e la **cifratura dei dati personali**;
  - su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - **una procedura** per testare, verificare e valutare regolarmente **l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.
- In più:
  - Si devono registrare (e possibilmente gestire) i log almeno degli Amministratori di Sistema per 6 mesi (Raccomandazione Garante del 2008 che rimane valida)
  - si dovrebbe essere in grado di rilevare la violazione dei dati personali, in pratica degli attacchi, per denunciarla all'Autorità (Garante) → tecnicamente un problema non semplice

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

- **Le misure di sicurezza digitale evolvono con l'evolversi degli attacchi e della loro complessità. Le «tradizionali» misure, se esistenti, sono sempre nec**
- Sistematica a … che di *intelligenza* …, ecc.
- **Scannerizza…** …ssioni e di dati
- **Correlazioni** …revoli eventi
- **Tecniche eu…**
- **Evoluzione a… …ittografia quantistica (viene usato un canale di comunicazione segreto basato sullo scambio di fotoni 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 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)**
- **qualificano il professionista considerando l'intera sua carriera e le competenze ed esperienze maturate nella sua vita professionale**

I 10 comandamenti per la sicurezza digitale

1. La sicurezza assoluta non esiste
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
- ***Compilate e fate compilare il Questionario OAD 2018***