



PADOVA
22-23 MARZO 2018



Osservatorio
Attacchi Digitali
in Italia

*Quale è la situazione
degli attacchi digitali
in Italia?*

*Quali le misure di
sicurezza in atto?*



Marco R. A. Bozzetti

m.bozzetti@aipsi.org

Presidente AIPSI, Capitolo Italiano ISSA

www.aipsi.org

Ideatore e realizzatore OAD

www.oadweb.it

CEO Malabo Srl

www.malboadvisoring.it



2018



Dr. Ing. 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**

Indice presentazione

- AIPSI e OAD
- Vulnerabilità e attacchi
- Quali difese?
- Prime conclusioni: i 10 comandamenti per la sicurezza digitale

smau

PADOVA 22-23 MARZO 2018

**PADOVA
FIERE**

aipsi
ASSOCIAZIONE ITALIANI PROFESSIONISTI SICUREZZA INFORMATICA

ISSA
Information Systems Security Association

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

5



AIPSI e OAD

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

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**
 - **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 la sensibilizzazione per la sicurezza informatica agli utenti digitali**
- **Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte: AICA, Assintel, Assolombarda, Anorc, CSA Italy, FidalInform, FTI, Inforav, Polizia Postale, Smau, i vari ClubTI sul territorio, ecc.**

Le principali novità di AIPSI 2018

- Nuovo sito web dell' Associazione
- Nuovo sito web per OAD
- Sedi territoriali
- Accordo con AICA per promuovere le certificazioni eCF sulle competenze della sicurezza digitale
- Azioni in corso per essere riconosciuti dal MISE entro la fine del 2018 come Associazione rappresentativa dei professionisti della sicurezza digitale secondo la Legge 4/2013
- Webinar
- Nuovo Media Partner: Reportec

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

Indagine generale annuale 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

2008 - 2018 : 10 anni di indagini via web



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

Che cosa è attaccato	Come (tecniche attacco)					
	Raccolta Informazioni (es. social engineering,	Script e programmi maligni	Agenti autonomi/ programmi maligni	Toolkit: programmi In grado di scoprire	Strumenti distribuiti	utilizzo di due o più delle
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 access 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 Things) In uso						
Attacchi ai propri sistemi di automazione (DCS, PLC, ...) e di robotica						

per ogni tipo di attacco (che cosa) delle sotto domande che includono, se l'attacco è stato rilevato; se no si salta al tipo di attacco successivo:

- 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.

Questionario OAD 2018 on line, con attuali Sponsor e Patrocinatori



Questionario OAD 2018: da compilare subito!

<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 2017"**



smau

PADOVA 22-23 MARZO 2018

PADOVA
FIERE

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ISSA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

14



Vulnerabilità e Attacchi



Gli attacchi digitali: sempre di più e sempre più critici

Siamo sempre

**La sicurezza ICT assoluta non esiste
ed è sempre più complesso gestirla**

Dalla grande

alla nano-impresa fino al singolo

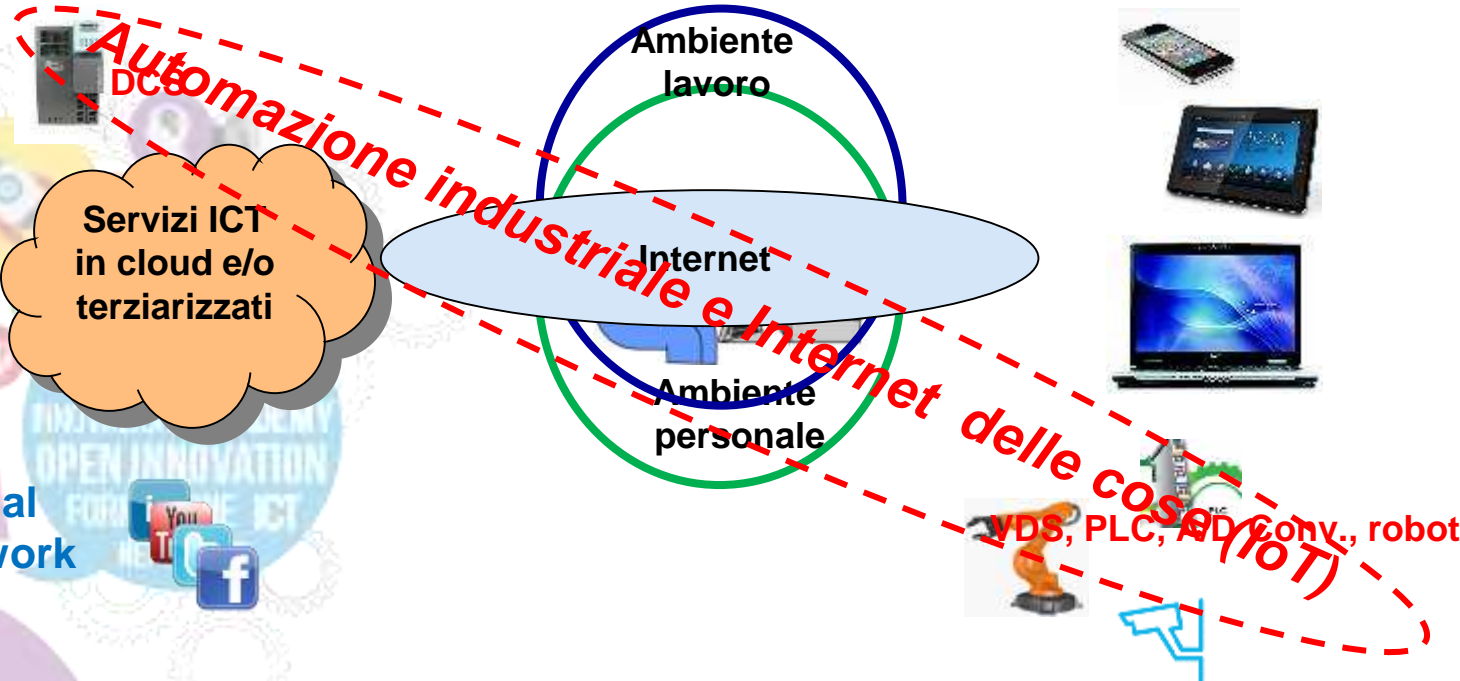
PADOVA 22-23 MARZO 2018

PADOVA

Sistemi informativi
aziendali e delle PA

Consumerizzazione

Fisso + mobile



Servizi ICT
in cloud e/o
terziarizzati

Ambiente
lavoro

Internet

Ambiente
personale

Social
network



VDS, PLC, AD conv., robot

Automazione industriale e Internet delle cose (IIoT)

Applicazione

ATTACCO

Data Center

DATI - INFORMAZIONI

Applicazioni Business Critical

Applicazioni infrastrutturali

Middleware

Infrastrutture di Elaborazione

Infrastrutture di Telecomunicazioni

Sicurezza ICT

ATTACCO

ATTACCO

Cloud

ATTACCO

INTERNET

ATTACCO

PC

SMART PHONE
TABLET, IoT

Client
Applicazione
o
browser

DATI - INFORMAZIONI

Applicazioni Business Critical

Applicazioni infrastrutturali

Middleware

Infrastrutture di Elaborazione

Infrastrutture di Telecomunicazioni

Sicurezza ICT

ATTACCO

Browser

ATTACCO

DATI - INFORMAZIONI

Applicazioni Business Critical

Applicazioni infrastrutturali

Middleware

Infrastrutture di Elaborazione

Infrastrutture di Telecomunicazioni

Sicurezza ICT

Browser

App

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 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 practice
 - 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

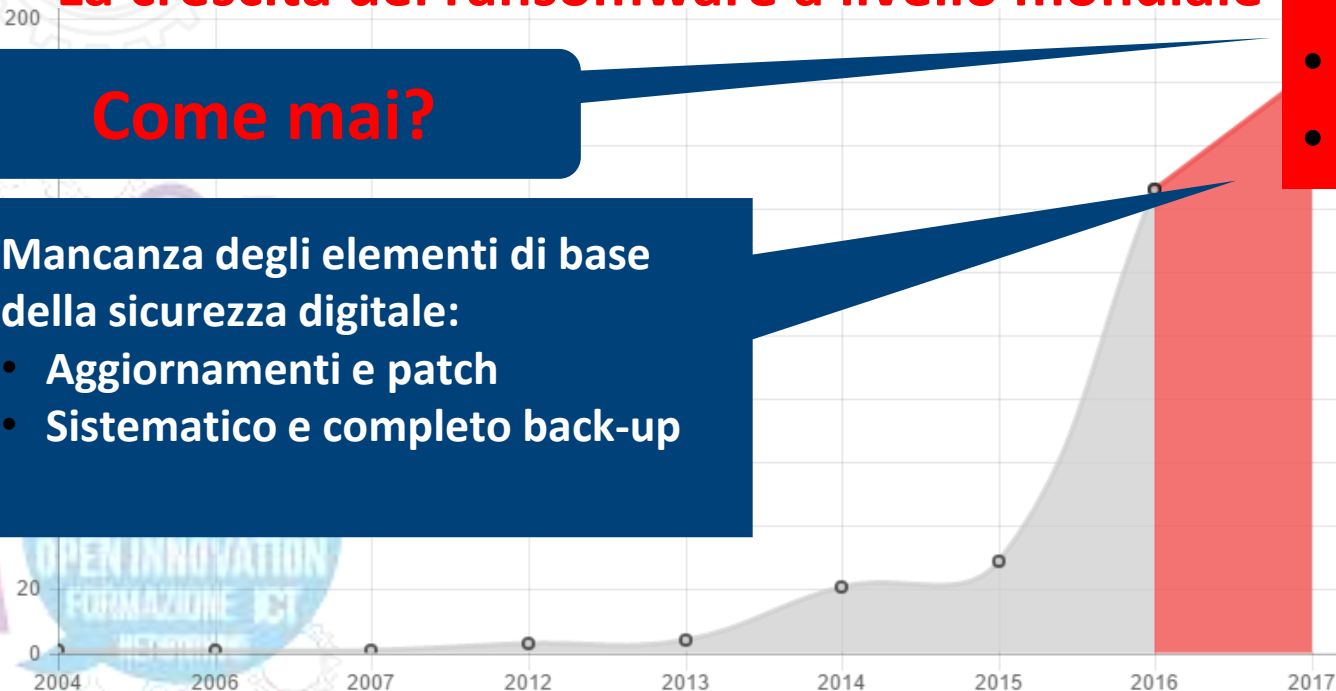
La crescita del ransomware a livello mondiale

Come mai?

Mancanza degli elementi di base della sicurezza digitale:

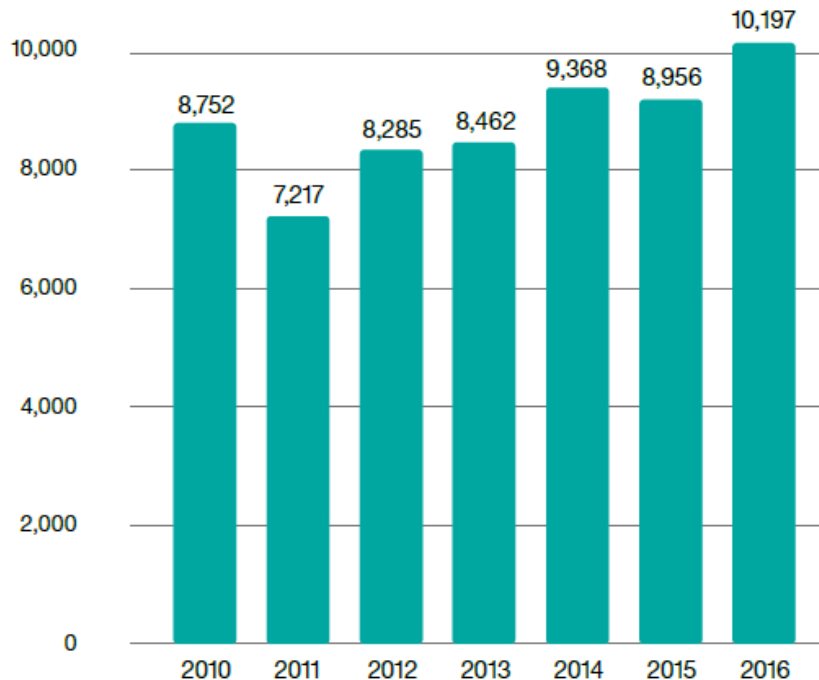
- Aggiornamenti e patch
- Sistemico e completo back-up

- *WannaCry*
- *Petya*
-

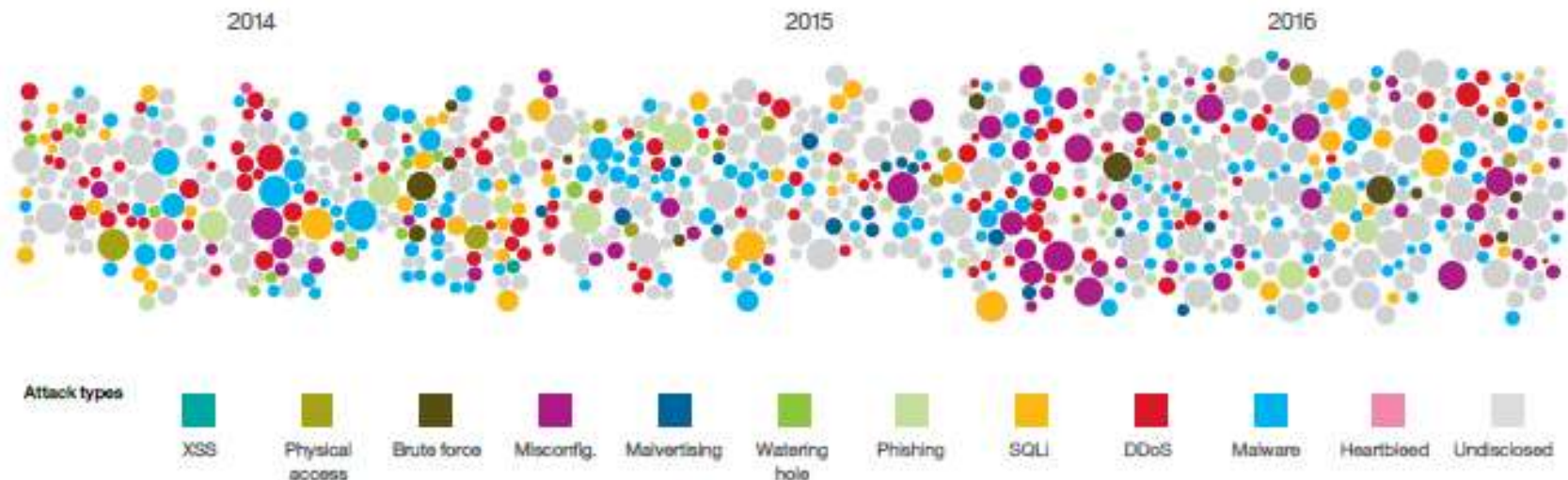


Fonte: TrendMicro

La crescita delle vulnerabilità tecniche



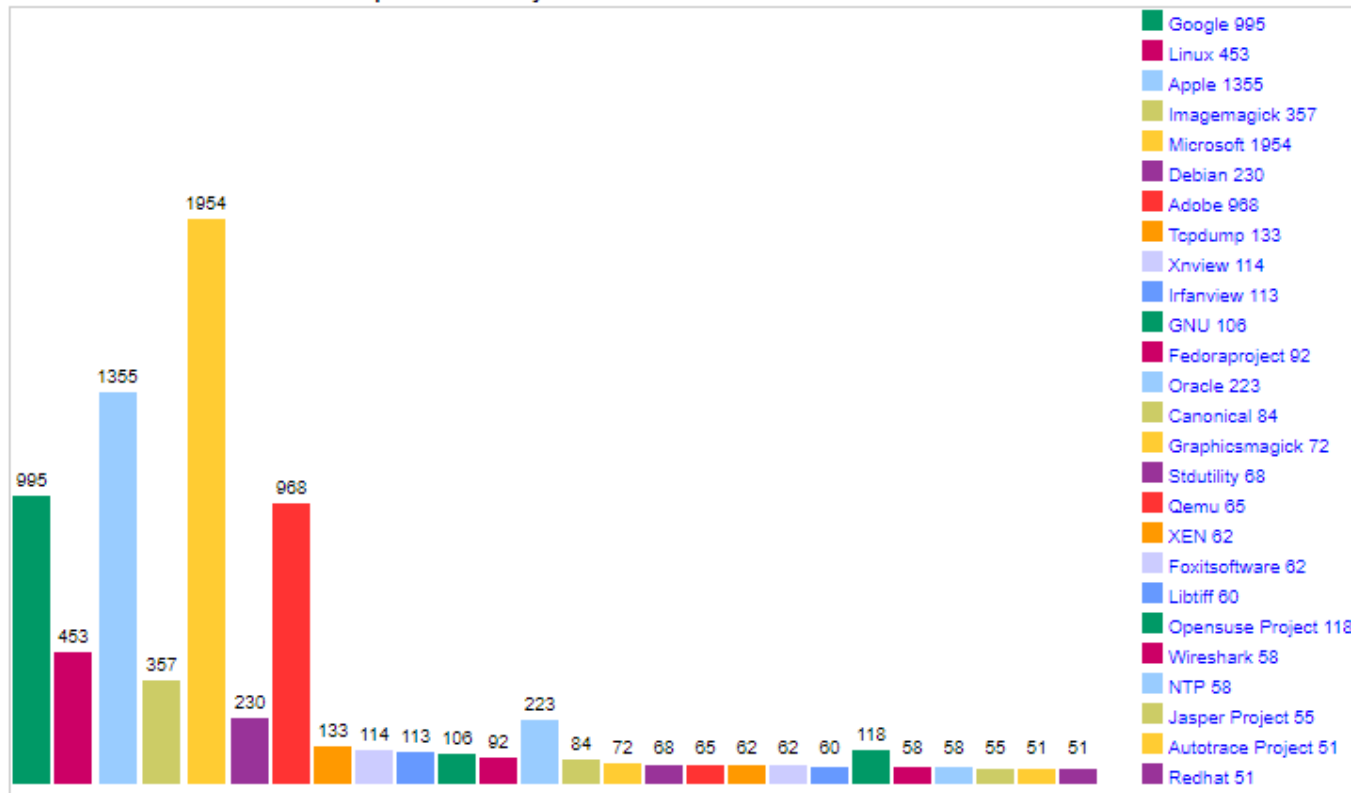
Attacchi 2014-16 per vulnerabilità tecnica a livello mondiale per tipo e durata



PADOVA 22-23 MARZO 2018

CVE: vulnerabilità per prodotto

Total Number Of Vulnerabilities Of Top 50 Products By Vendor



Fonte: DB CVE 2018

Top Ten Vulnerabilità 2017 web OWASP (Open Web Application Security Project)

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Broken Access Control
- Security Misconfiguration
- Sensitive Data Exposure
- Insufficient Attack Protection
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Underprotected APIs

Due grandi categorie di attacchi

→ Attacchi a specifici obiettivi (target), con precisi obiettivi e larga disponibilità di risorse e competenze



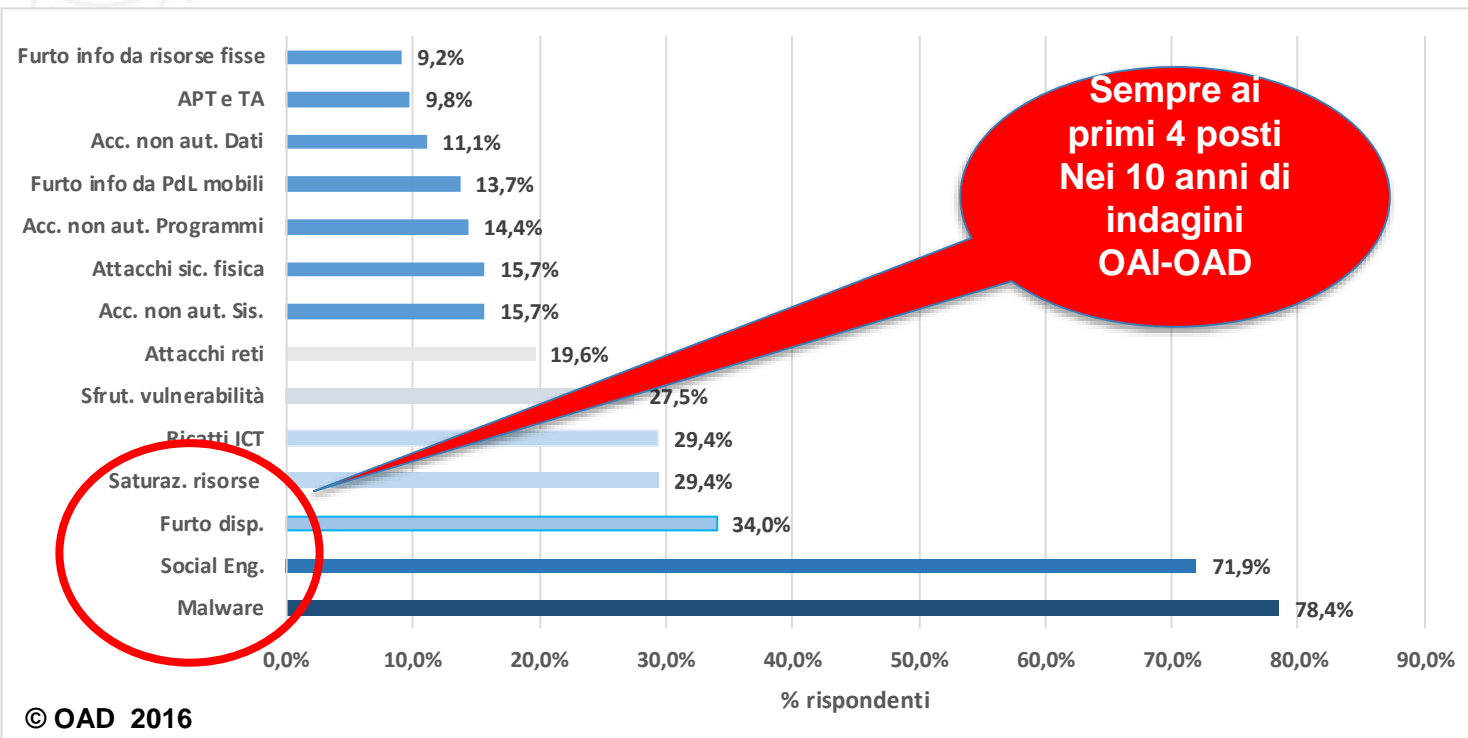
Grandi Aziende/Enti

→ 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 tipologia di attacco



PADOVA 22-23 MARZO 2018

PADOVA
FIERE

OAD AA 2017: Attacchi agli applicativi rilevati

Attacchi agli applicativi

Si sono rilevati attacchi specifici agli applicativi

46,9%

Non si sono rilevati attacchi

53,1%

57,7%

0,0% 10,0% 20,0% 30,0% 40,0% 50,0% 60,0% 70,0%

% rispondenti

© OAD 2017


 2015 2016

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

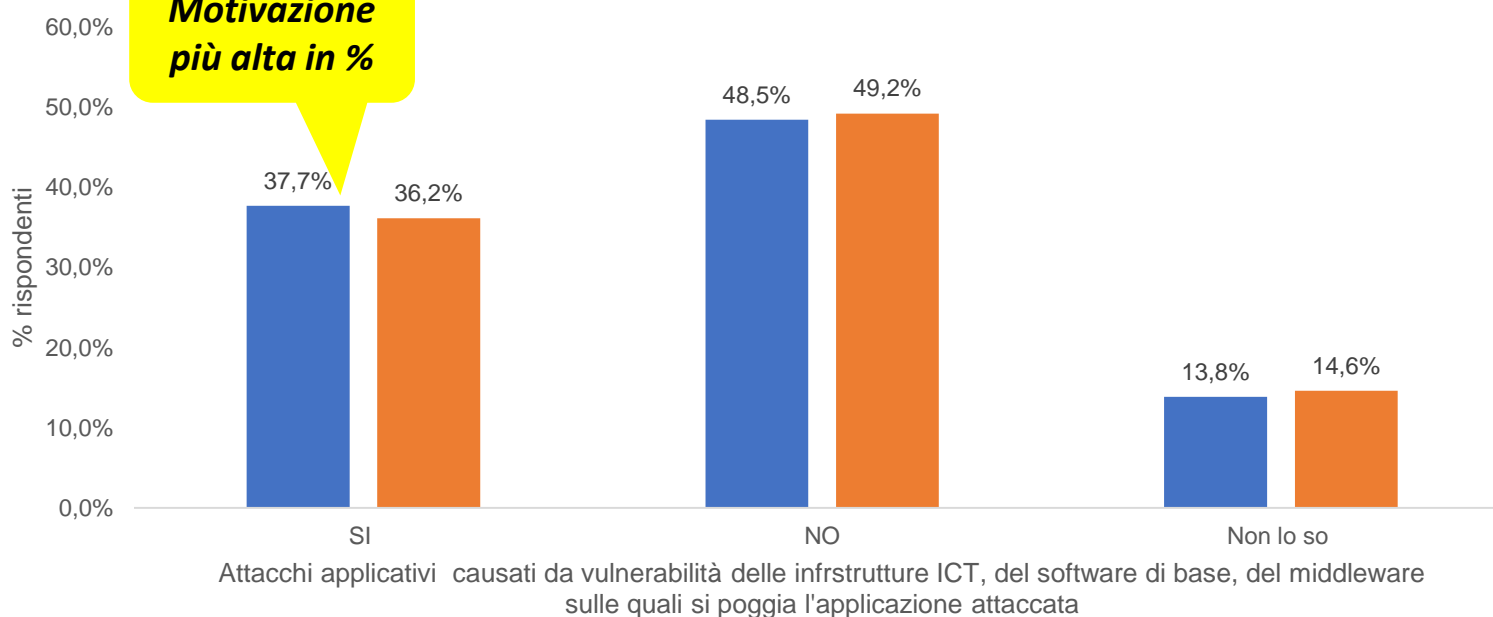


PADOVA 22-23 MARZO 2018

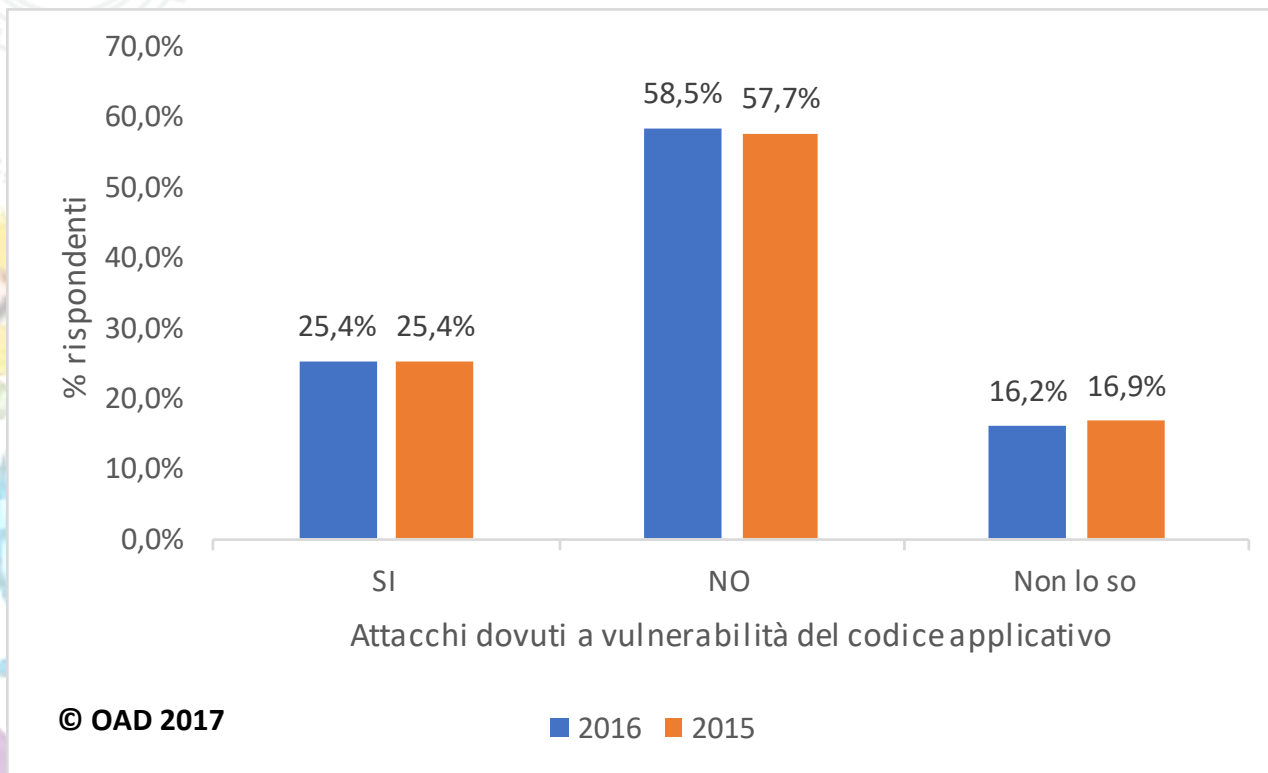


OAD AA 2017: causati dalle vulnerabilità sw

**Motivazione
più alta in %**



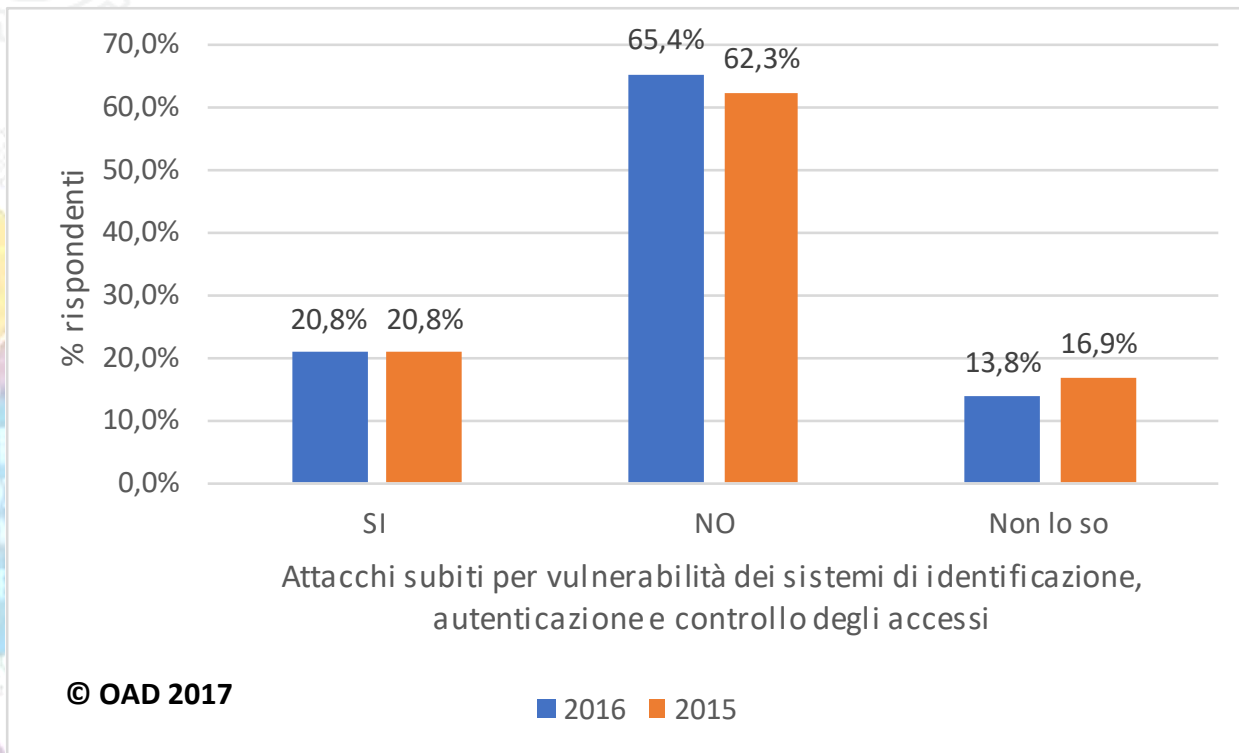
OAD AA 2017: causati da vulnerabilità del codice



PADOVA 22-23 MARZO 2018

PADOVA
FIERE

OAD AA 2017: Attacchi da ident.-auten.-controllo accessi



smau

PADOVA 22-23 MARZO 2018

**PADOVA
FIERE**

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ISSA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

31



Quali difese?

STARTUP SAFARI
INNOVAZIONE ACADEMICA
OPEN INNOVATION
FORMAZIONE ICT
NETWORKING

- 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, ...
- ... gestione delle patch e delle release del software (→ licenze)
... informazione e addestramento, operation (ITIL v3), help-desk/contact center, ERT, ..

Crittografia ... richiesta anche dal GDPR

- Simmetrica: un'unica chiave per criptare/decriptare, che deve essere nota ad entrambi gli interlocutori. Un algoritmo di crittografia simmetrica consente di crittografare in modo efficiente grandi quantità di dati
- Asimmetrica: ogni interlocutore ha due chiavi, una pubblica ed una segreta., non correlate tra loro. L'informazione può essere criptata con una chiave e decriptata con l'altra. Si evita in questo modo il problema di scambiare la chiave tra i due interlocutori. Si realizzano canali sicuri tra due attori, risolvendo anche il problema della condivisione della chiave simmetrica che cripta il canale.

- Algoritmi troppo semplici di crittografia e/o una sua cattiva gestione possono rendere
- Fare riferimento agli algoritmi standard ed usare chiavi di opportuna lunghezza

Back to the basic

- **Classificazione dei dati** critici, che includono quelli personali → GDPR
- **Analisi dei rischi**
- **Bilanciamento** tra le diverse misure tecniche di sicurezza
- **Aggiornamento** software di base ed applicativo
- Misure di **Back-up e ripristino**
- **Misure organizzative:**
 - Definizione chiara **ruoli e responsabilità**, separazione compiti (SoD)
 - **Procedure organizzative**
 - **Sensibilizzazione e formazione del personale**

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

- Le misure di sicurezza sono sempre più complesse e sofisticate a causa degli attacchi e della loro complessità. Sono necessarie ...
- Sistematica applicazione di tecniche di *intelligenza artificiale*, *fuzzy logic* e *machine learning*.
- Scannerizzazioni e analisi di grandi volumi di dati.
- Correlazioni in tempo reale di eventi.
- Tecniche euristiche e di apprendimento automatico.
- Evoluzione algoritmi di crittografia: curve ellittiche, crittografia quantistica (viene usato un canale di comunicazione segreto basato sullo scambio di fotoni polarizzati su fibra ottica)



L'effettiva sicurezza ICT dipende da come viene gestita

- Sia dal punto di vista tecnico
 - Può essere terziarizzata
- Sia dal punto di vista organizzativo e del personale
 - Deve essere gestita internamente
 - Forte commitment dal vertice aziendale
- Fondamentale avere strumenti di misura e controllo, usati sistematicamente
- Fare riferimento agli standard ed alle best practice consolidate: ISO 27000, NIST SP 300, Cobit 5, Itil 2013, ecc.

Il problema delle effettive competenze sulla sicurezza digitale

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

- professionisti **certificati**
- **Iscritti** ad Associazioni riconosciute dal MISE (entro il 2018 lo sarà anche AIPSI)

- 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 (riconosciute da un Ente accreditato Accredia)
 - AIPSI collabora con AICA (Ente accreditato Accredia)
- possono valorizzare i titoli conseguiti
- si basano su standard europei

partecipa al webinar **sincrono gratuito** AIPSI-AICA
 del **27/3/2018** ore 17
 Qualificazioni e Certificazioni eCF nel percorso di crescita professionale
 per la sicurezza digitale

Per iscriversi: http://www.aicanet.it/dettaglio_evento/2059859

Security Manager

Competenze più importanti nella cybersecurity dall'indagine ISSA-ESG 2017

Survey Respondents Identify Three Areas Where Cybersecurity Skills are Most Acute

CISOs should be ready to compete for talent in the following areas.



31%

Security analysis
and investigations



31%

Application security



29%

Cloud computing
security

smau

PADOVA 22-23 MARZO 2018

**PADOVA
FIERE**

aipsi
ASSOCIAZIONE ITALIANI PROFESSIONISTI SICUREZZA INFORMATICA

ISSA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

40



**Per
concludere**



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**

