smau
BOLOGNA 7-8 GIUGNO 2018

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

La situazione degli attacchi digitali in Italia e di come vengono contrastati alla luce dei risultati nazionali dell'Osservatorio OAD e di altre indagini internazionali

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.malaboadvisoring.it

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA
ISSA Information System Security Association
OAD Osservatorio Attacchi Digitali in Italia
malabo ICT Advisory

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


STARTUP SAFARI
INNOVAZIONE ACADEMY
OPEN INNOVATION
FORMAZIONE ICT

AIPSI e OAD

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- **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, FidaInform, FTI, Inforav, Polizia Postale, Smau, i vari ClubTI sul territorio, ecc.

Le principali novità di AIPSI 2017-18

- → Nuovo sito web dell' Associazione
- → Nuovo sito web per OAD
- → Sedi territoriali
- → Accordo con AICA per promuove le certificazioni eCF sulle competenze della sicurezza digitale
- → Webinar
- → Nuovo Media Partner: Reportec

Milano, sabato 30/6/2018 – ore 10-13 Convegno AIPSI

Quale sicurezza digitale per il GDPR e come evitare le truffe dei millantatori

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**

OAD-OAI 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)						
	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 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:

Questionario OAD 2018 on line ancora per pochi giorni: da compilare e far compilare subito!

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

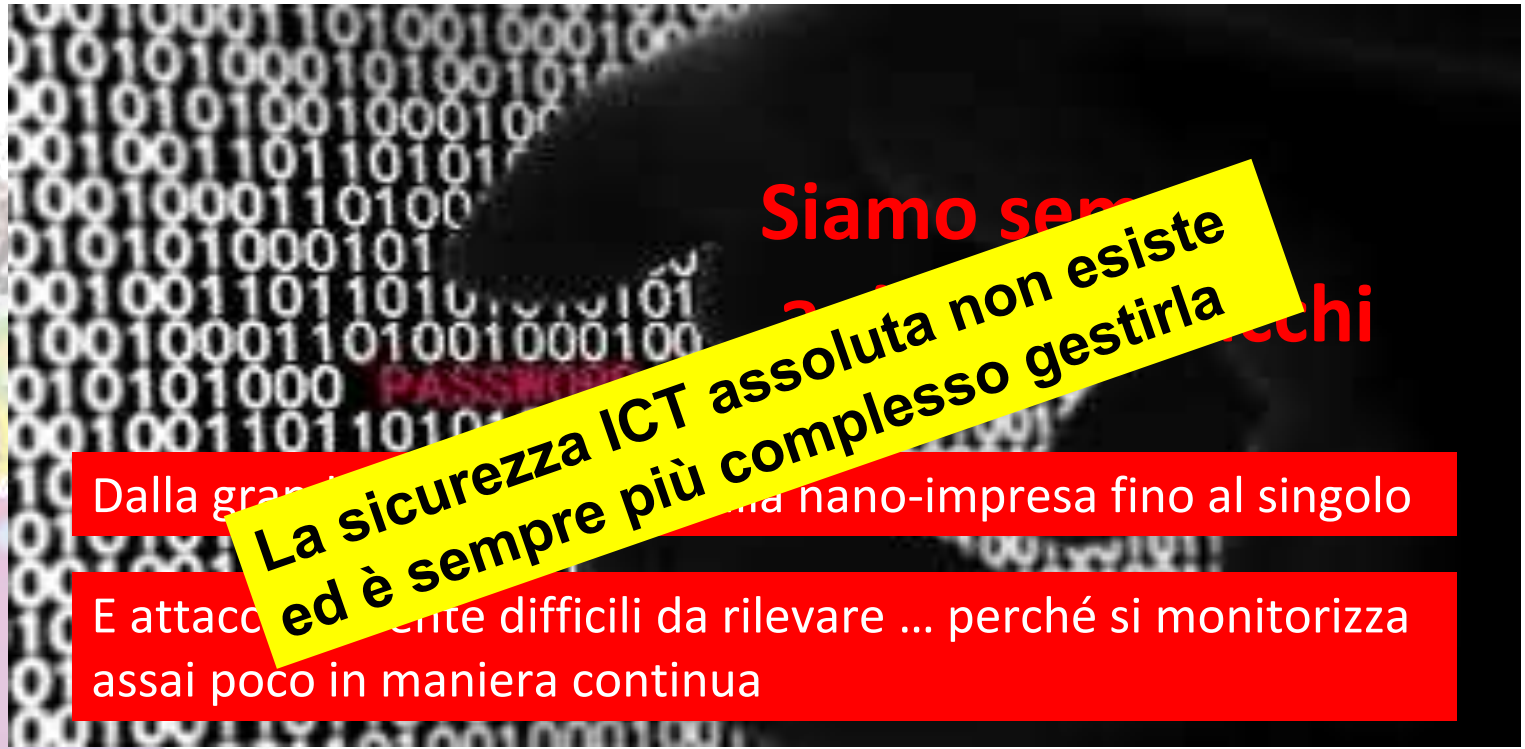
Assolutamente anonimo, risposte predefinite tra cui scegliere, rapido da compilare con il salto automatico di domande non pertinenti, include domande su attacchi a *sistemi di automazione industriale, IoT, blockchain*

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 2018"**

Vulnerabilità e Attacchi

Gli attacchi digitali: sempre di più e sempre più critici



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

Sistemi informativi aziendali e delle PA

Consumerizzazione

Fisso + mobile

DCS

Automazione industriale e Internet delle cose (IoT)

Ambiente lavoro

Servizi ICT in cloud e/o terziarizzati

Internet

Ambiente personale

Social network

VDS, PLC, AD conv., robot

Vulnerabilità causa delle minacce

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

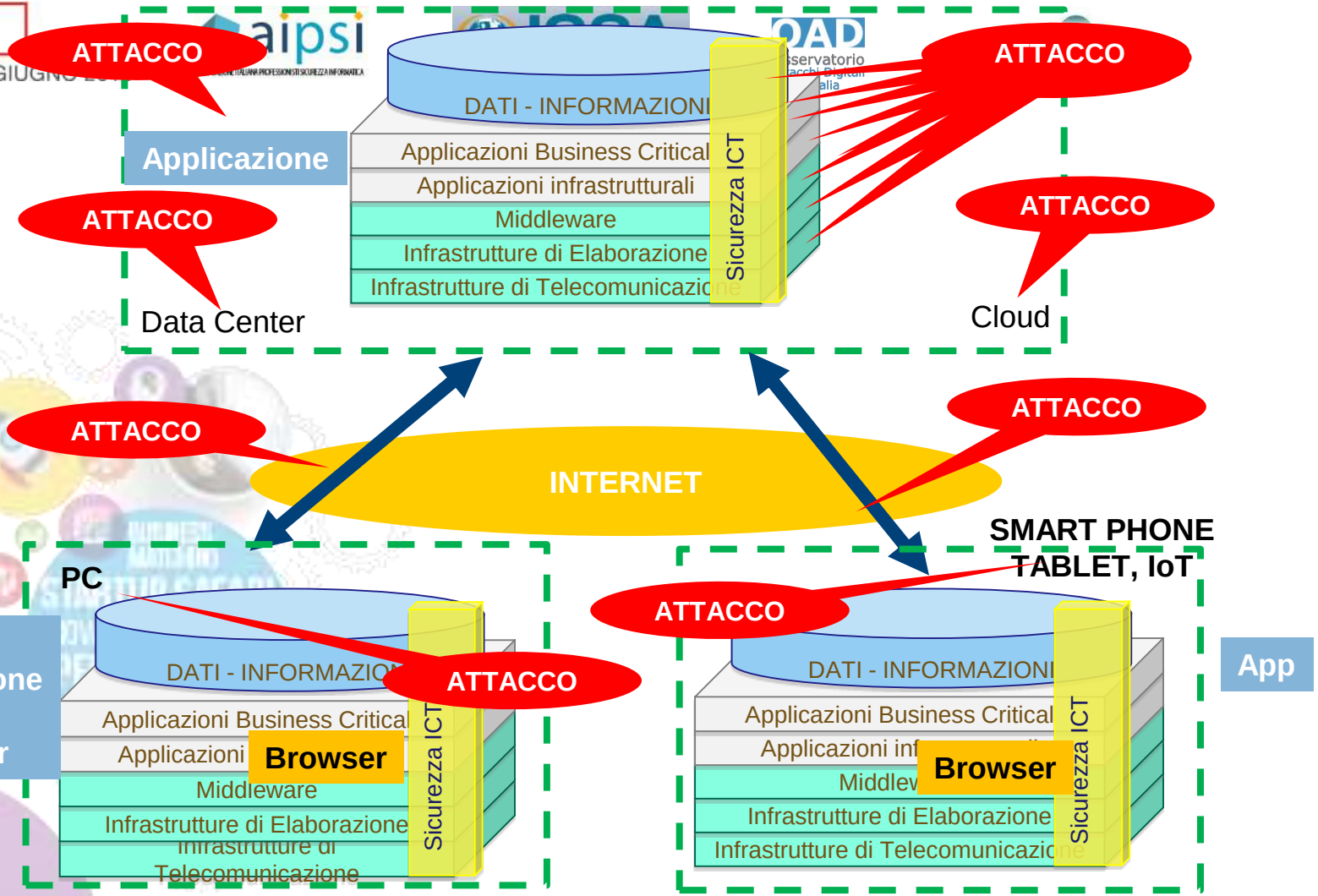
- ***Vulnerabilità tecniche*** (software di base e applicativo, architetture e configurazioni)
  - siti web e piattaforme collaborative
  - Smartphone e tablette → mobilità → **>>14.000 malware**
  - Posta elettronica → spamming e phishing
  - Piattaforme e sistemi virtualizzati
  - Terziarizzazione e Cloud (XaaS)
  - Circa il 40% e 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 practic
  - 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):

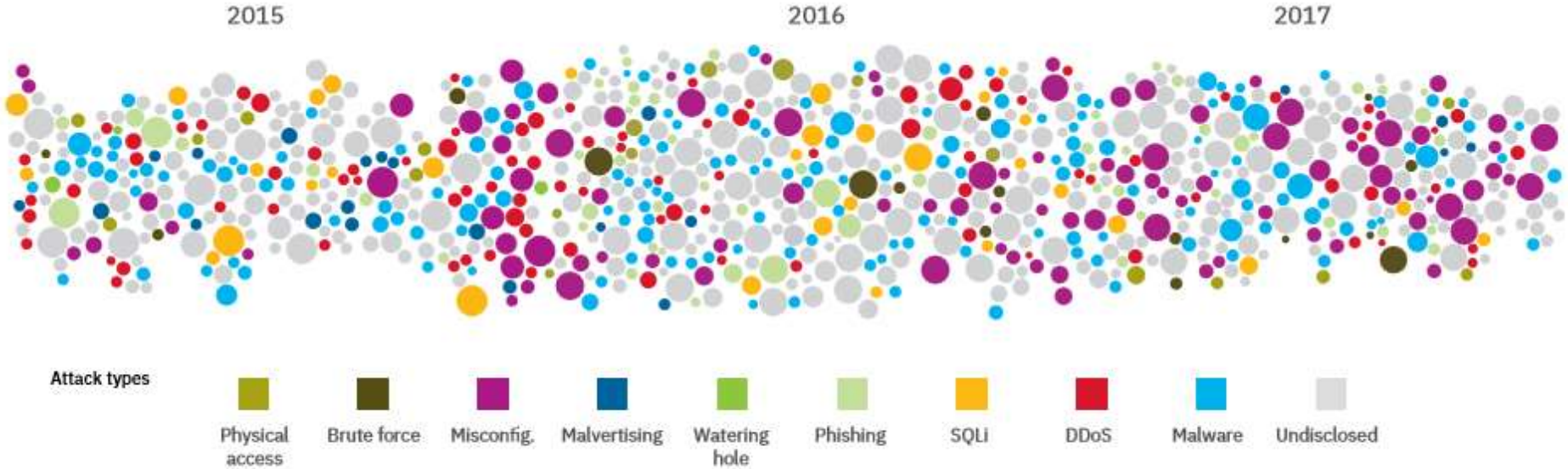
- **Inconsapevolezza**
- **Imperizia**
- **Ignoranza**
- **Imprudenza**
- **Dolo**

Aggravata dalla non o inefficace organizzazione

Mancanza di formazione e addestramento


ATTACCO
ATTACCO
Applicazione
DATI - INFORMAZIONI
Applicazioni Business Critical
Applicazioni infrastrutturali
Middleware
Infrastrutture di Elaborazione
Infrastrutture di Telecomunicazione
Sicurezza ICT
ATTACCO
ATTACCO
Data Center
Cloud
ATTACCO
ATTACCO
INTERNET
SMART PHONE
TABLET, IoT
PC
ATTACCO
ATTACCO
Client
Applicazione
o
browser
DATI - INFORMAZIONI
Applicazioni Business Critical
Applicazioni
Browser
Middleware
Infrastrutture di Elaborazione
Infrastrutture di Telecomunicazione
Sicurezza ICT
DATI - INFORMAZIONI
Applicazioni Business Critical
Applicazioni inf
Browser
Middlev
Infrastrutture di Elaborazione
Infrastrutture di Telecomunicazione
Sicurezza ICT
App

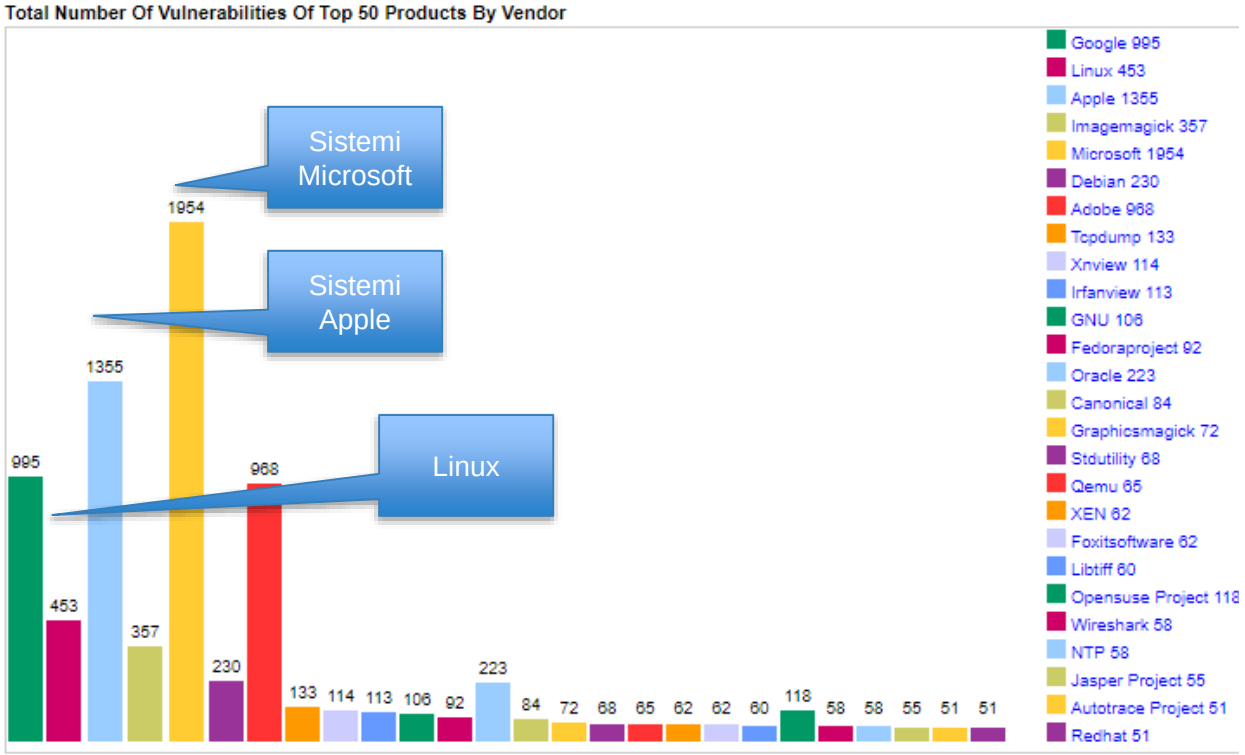
Attacchi 2015-17 per vulnerabilità tecnica a livello mondiale per tipo e durata



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

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

Fonte: OWASP, Open Web Application Security Project

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

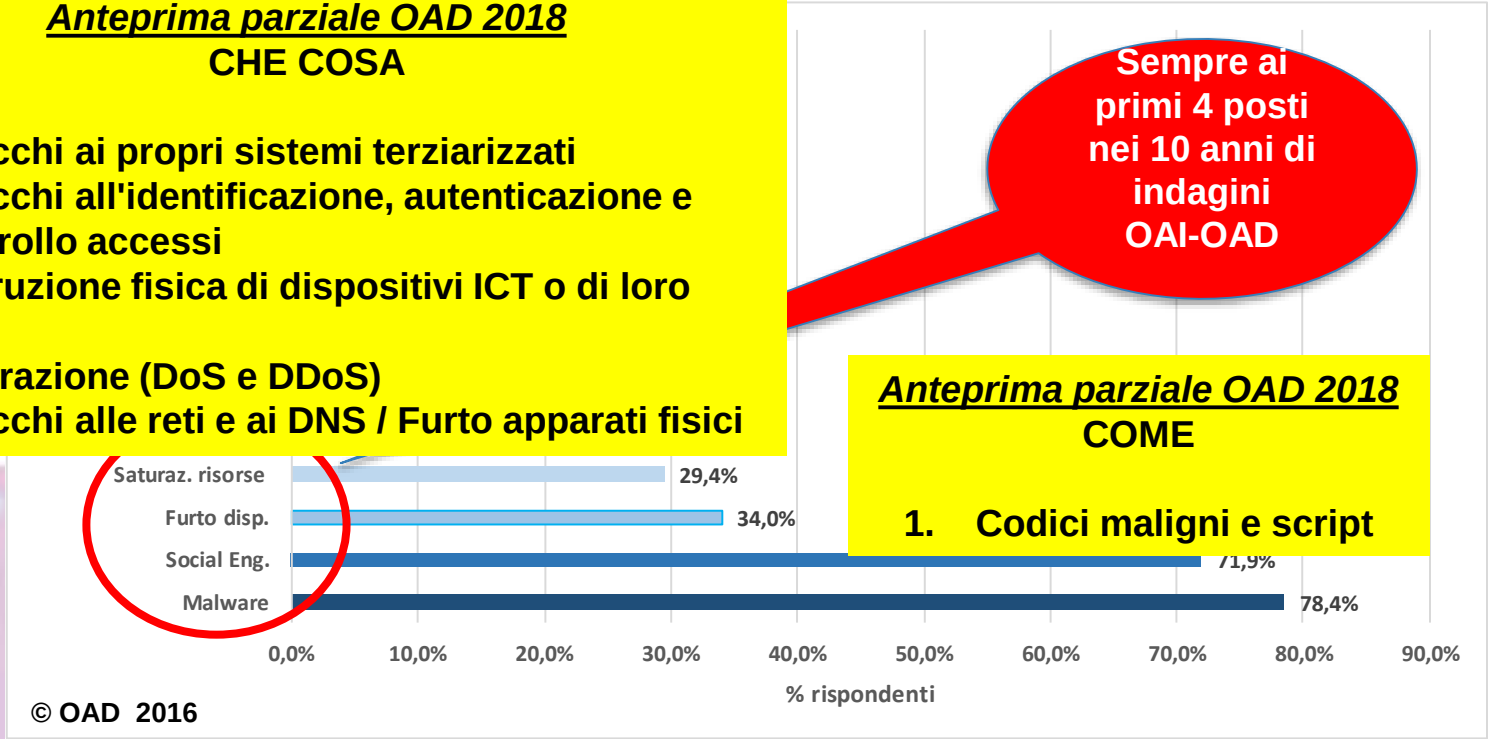
Anteprima parziale OAD 2018
CHE COSA

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**

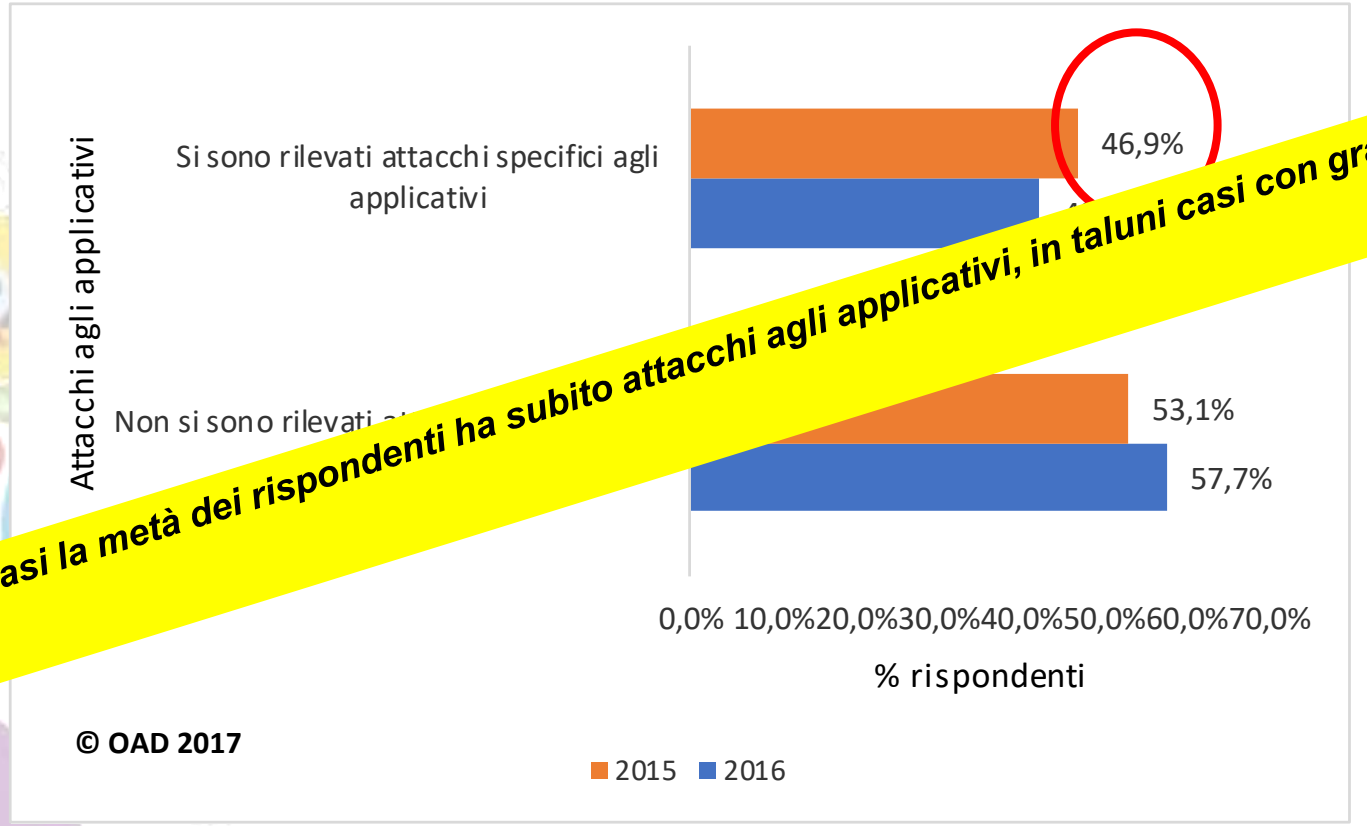
Sempre ai primi 4 posti nei 10 anni di indagini OAI-OAD

Anteprima parziale OAD 2018
COME

1. **Codici maligni e script**

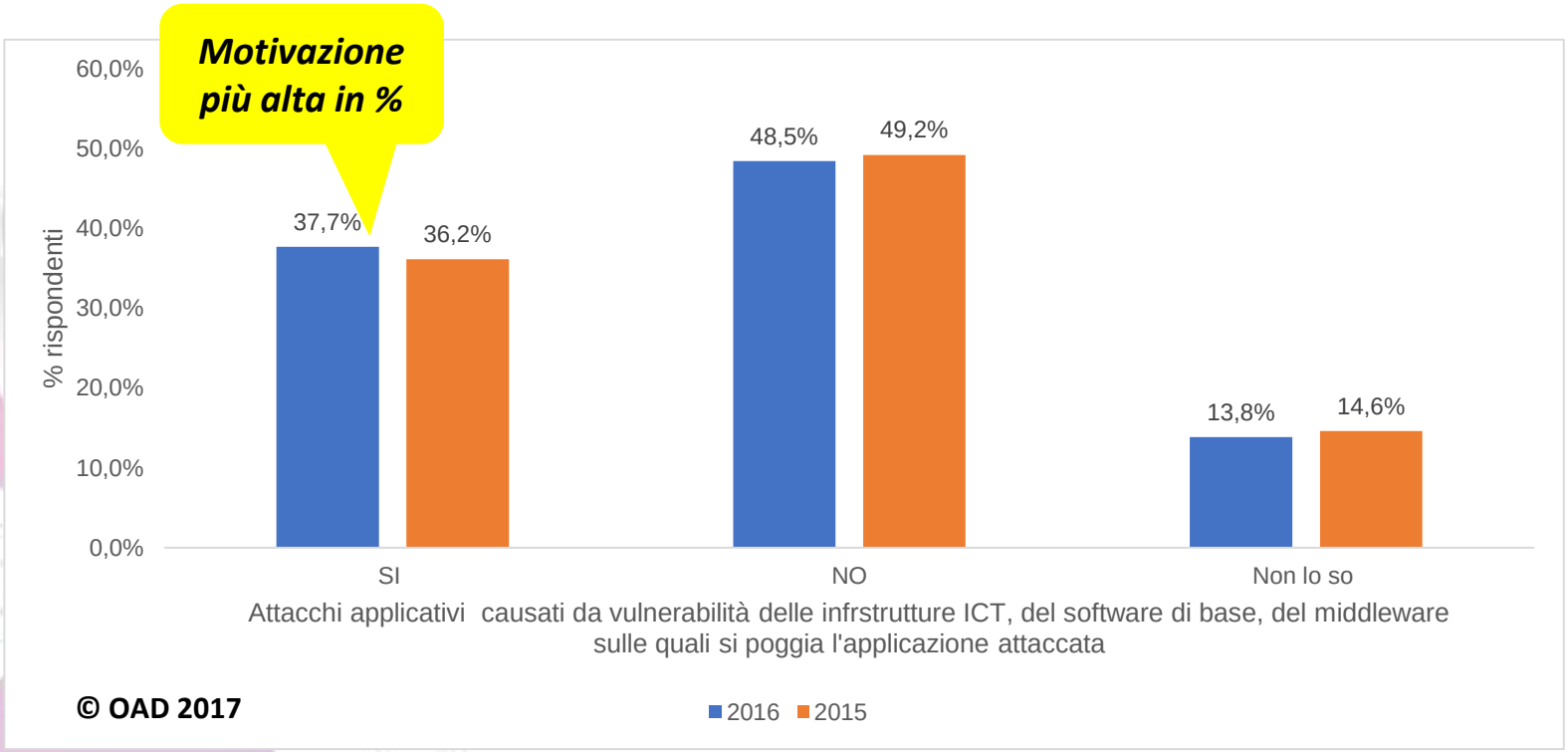


OAD AA 2017: Attacchi agli applicativi rilevati



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



Quali difese?

- **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)

…ttiva: formazione 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**

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

- → **Le misure di si… …gli attacchi e della loro complessi… …no sempre necessarie … r…**
- → Sistematica ar… …di ***intelligenza artificiale, fuz…***
- → **Scannerizzazi… …ni e di dati**
- → **Correlazioni *in*… …oli eventi**
- → **Tecniche euris…**
- → **Evoluzione algoritmi di crittografia: curve ellittiche, crittografia quantistica (viene usato un canale di comunicazione segreto basato sullo scambio di fotoni polarizzati su fibra ottica)**

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'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?

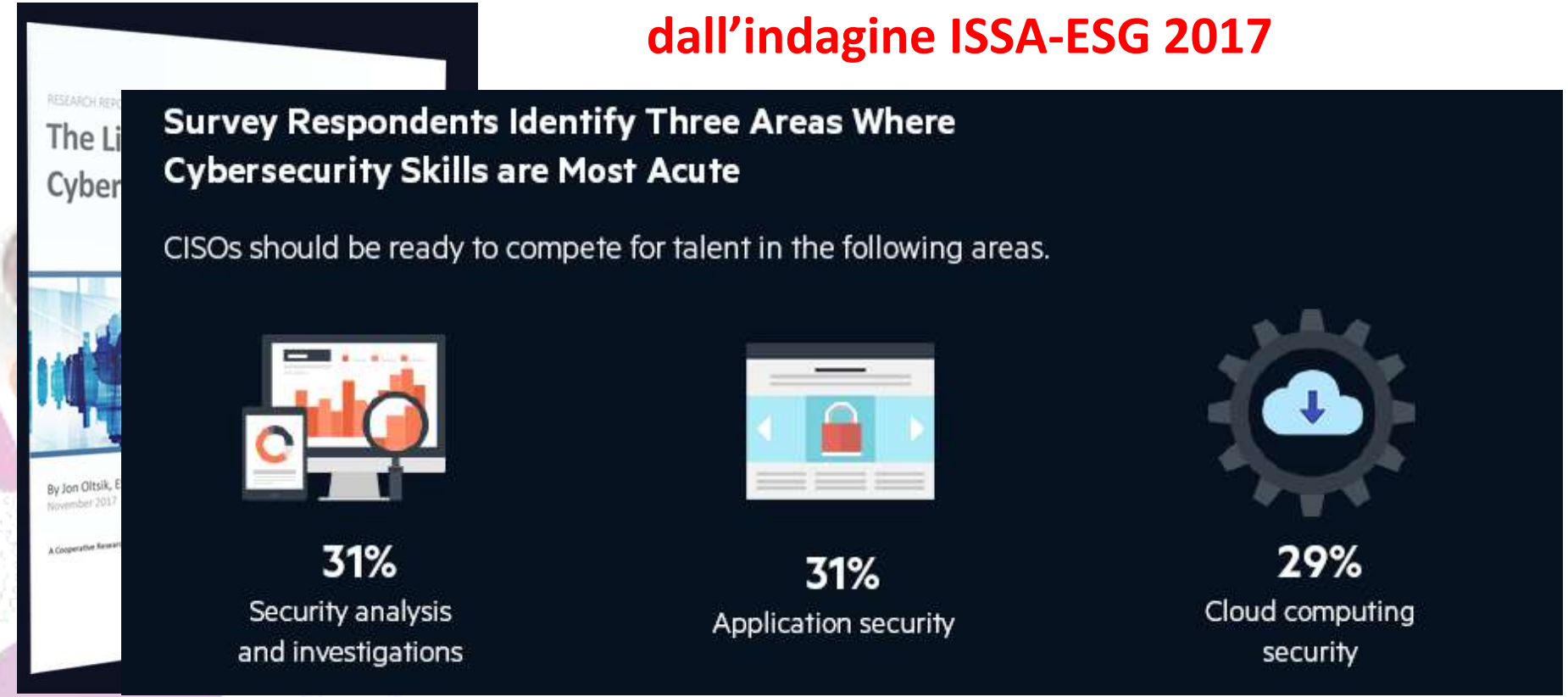
Le certificazioni eCF (EN 16234 1:2016)

- **Sono le uniche ad avere valore giuridico** in Italia e in Europa (se erogate da un Ente accreditato Accredia)
  - AIPSI collabora con AICA, Ente Certificato
- possono valorizzare alcune altre **co**
- si basano sulla **provata** professionista
- qualificano il **sua biografia**
  - esperienze maturate nella sua vita
  - per aver seguito un corso e superato un esame)
- Il Framework digitale eCF prevede due profili:
  - Security Specialist
  - Security Manager

Milano, sabato 30/6/2018 – ore 10-13 Convegno AIPSI

Quale sicurezza digitale per il GDPR e come evitare le truffe dei millantatori

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



Per concludere

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
- *Compilate e fa[illegible]ilare il Questionario OAD 2018*

SUBITO !!!