

OAD

Osservatorio
Attacchi Digitali
in Italia

Rapporto 2017 OAD

sugli attacchi agli applicativi in Italia

a cura di Marco R. A. Bozzetti

SPONSOR



Indagine effettuata da
in collaborazione con

Media Partner



Ringraziamenti

Si ringraziano tutte le persone che hanno risposto al questionario sugli attacchi agli applicativi, lo Sponsor F5 Network ed AIPSI che hanno aiutato alla preparazione del questionario, il Media Partner Reportec e tutti i Patrocinatori che hanno contribuito alla diffusione del questionario e che contribuiranno alla diffusione del presente rapporto.

Un grazie particolare a Francesco Zambon e ad Andrea Bozzetti che hanno aiutato l'autore nella preparazione del questionario e nella stesura del presente Rapporto.

© OAD 2017

È autorizzata la riproduzione dei grafici solo se con la citazione della fonte OAD.

E' vietata la riproduzione anche parziale dei contenuti del Rapporto senza la preventiva autorizzazione scritta dell'Autore o di Reportec Srl.

Pubblicato in maggio 2017

AIPSI

c/o Malabo srl
Via Savona, 26
20144 Milano
aipsi@aipsi.org

Malabo Srl

Sede operativa
Via Savona 26
20144 Milano
info@malaboadvisoring.it
tel. 02 39443632

Reportec srl

Via Marco Aurelio, 8
20127 Milano
info@reportec.it
tel.02.36580441

Quest'opera è distribuita con licenza Creative Commons
Attribuzione - Non commerciale
Non opere derivate 4.0 Italia

SOMMARIO

• Le ragioni di una partnership (a cura di Reportec)	pg.4
• Presentazione (a cura Marco R. A. Bozzetti, Presidente AIPSI)	pg.5
1. Introduzione	pg.6
2. Gli attacchi digitali agli applicativi	pg.7
3. Le principali vulnerabilità degli applicativi	pg.9
4. Gli attacchi digitali rilevati dall'indagine e le loro cause	pg.15
4.1 Attacchi dovuti a vulnerabilità del software applicativo	pg.16
4.2 Attacchi dovuti a vulnerabilità dei sistemi di identificazione-autenticazione-controllo accessi	pg.17
4.3 Attacchi dovuti al furto di informazioni da dispositivi mobili degli utenti e/o degli operatori ICT	pg.19
4.4 Attacchi dovuti a vulnerabilità dei sistemi infrastrutturali quali	
5. Le misure di sicurezza in atto	pg.20
5. Le misure di sicurezza in atto	pg.21
6. Gli impatti di un attacco digitale ad un applicativo	pg.26
7. Il campione emerso dall'indagine	pg.28
7.1 Chi ha risposto: ruolo e settore merceologico	pg.28
7.2 L'ambiente applicativo dei sistemi informatici dei rispondenti	pg.31
8. Prime considerazioni sui dati emersi dall'indagine	pg.32
A Allegati	pg.34
A.1 Aspetti metodologici dell'indagine	pg.35
A.2 F5 Networks	pg.36
A.3 AIPSI	pg.37
A.4 Profilo dell'Autore	pg.38
A.5 Malabo Srl	pg.39
A.6 Reportec Srl	pg.40

Le ragioni di una partnership

Reportec nasce dall'esperienza maturata dai propri fondatori presso case editrici specializzate, i quali hanno colto il bisogno di opere che aiutassero gli addetti ai lavori del mondo ICT (Information e Communication Technology) ad avere una visione d'insieme della tecnologia e del mercato cui questa fa riferimento. Nacquero nel 2001 i Report Tecnologici dedicati a specifici ambiti verticali: il primo al networking, dove già si affrontava il tema della sicurezza e il secondo allo storage. Nel 2002 è stata fondata Reportec che continua a pubblicare report, libri, white paper e riviste con un deciso taglio di approfondimento.

Questo spirito è alla base delle nostre scelte nelle partnership. In particolare della media partnership con AIPSI. Condividiamo pienamente le ragioni per cui Marco Bozzetti da tempo realizza l'osservatorio sugli attacchi digitali e riteniamo doveroso diffonderlo attraverso i nostri data base di abbonanti. Non solo riteniamo importante la condivisione dei dati che è alla base dell'osservatorio il quale mantiene l'anonimato consentendo di ricavare informazioni utili a tutti e ci produrremo sia per aumentare la base di rispondenti al questionario sia per arricchire il report di nuovi contenuti. Buona lettera e buon lavoro!

Gaetano Di Blasio
Co-fondatore e direttore editoriale di Reportec

Presentazione (a cura Marco R. A. Bozzetti, Presidente AIPSI)

Nella mia attività professionale ho sempre sentito la necessità di poter disporre di indagini indipendenti ed autorevoli sul fenomeno degli attacchi digitali in Italia. Numerosi ed interessanti sono i rapporti internazionali sugli attacchi, sulle vulnerabilità e sulla sicurezza digitale, ma forniscono ben pochi dati sulla specifica realtà italiana; e le poche indagini che trattano il fenomeno in Italia sono per lo più basate sugli input dei fornitori dei sistemi di sicurezza digitale che degli effettivi utilizzatori.

Anche in Italia il problema della sicurezza digitale diviene sempre più critico e complesso, ma è sovente sottovalutato o del tutto ignorato. Al contrario, esso dovrebbe essere conosciuto e compreso sia dagli utenti dei sistemi informatici, sia, soprattutto, dai decisori di più alto livello nelle organizzazioni, perché prendano le idonee decisioni sulle spese da sostenere per le misure di sicurezza necessarie per le loro aziende/enti. Considerando la stragrande maggioranza di aziende piccole e piccolissime in Italia, la conoscenza a livello dei vertici dei problemi della sicurezza digitale, e degli impatti sull'azienda in caso di sua inadeguatezza, è limitata.

Per questi motivi ho voluto intraprendere, insieme ad AIPSI e con il supporto di altre associazioni italiane dell'ICT, una iniziativa per produrre un rapporto annuale sul fenomeno degli attacchi in Italia, nonostante i mezzi limitati a disposizione e le ben note difficoltà realizzative, tra le quali la reticenza dei responsabili informatici nel fornire informazioni, pur in totale anonimato, su un argomento delicato come l'aver subito attacchi digitali. Dal 2010 si è pubblicato annualmente un Rapporto sugli attacchi in Italia, cercando anno dopo anno di aumentare il numero di rispondenti al questionario on line, di migliorare le analisi dei dati raccolti e i contenuti del rapporto, di diffondere il rapporto non solo tra gli addetti ai lavori. Dopo sei consecutivi rapporti annuali, che hanno cercato di fotografare la situazione degli attacchi sui sistemi informatici in Italia, ci si è accorti che quanto fatto non era ancora sufficiente, data la complessità del fenomeno e la diffusione del digitale in ogni attività lavorativa. Occorrevano maggiori approfondimenti sulle tematiche di volta in volta più critiche e di maggior interesse per i lettori, ma questo contrastava con la necessità di porre ai potenziali rispondenti poche domande e non molto tecniche. La soluzione individuata per bilanciare queste contrastanti esigenze è stata di affiancare all'ormai consueto rapporto annuale dei veloci e snelli rapporti "verticali" su specifiche tipologie di attacchi e di aspetti della sicurezza digitale. In questa ottica è stata effettuata tra la fine del 2016 e l'inizio del 2017 la prima indagine "verticale" sugli attacchi agli applicativi che ha portato alla pubblicazione del presente rapporto.

Spero vivamente di poter continuare nei prossimi anni su questa direttrice appena intrapresa, insieme ad AIPSI e con l'aiuto dei vari enti interessati: un rapporto annuale affiancato da snelli rapporti verticali, con l'impegno di estendere il bacino sia di rispondenti sia di lettori, raccogliendo ben maggiori risposte dai settori merceologici ad oggi poco rispondenti.

Perché questa sfida e questo impegno? Per poter offrire ai Soci AIPSI e a chi si occupa, direttamente e indirettamente, di sicurezza digitale un quadro autorevole, qualificato ed indipendente sul fenomeno degli attacchi digitali che realmente aziende/enti italiani subiscono e rilevano. Rendere consapevole e trasferire conoscenze a chi deve decidere in merito, per poterlo aiutare nel difendere meglio il proprio sistema informatico, e quindi il proprio business, dai crescenti attacchi digitali.

Mi auguro che il presente Rapporto possa essere di interesse e di aiuto non solo ai tecnici del settore, ma anche a tutti i decisori e le persone coinvolte a vario titolo sulla sicurezza digitale.

Buona lettera e buon lavoro!

Marco R. A. Bozzetti
Presidente AIPSI
Ideatore ed autore OAD
CEO Malabo Srl



1. Introduzione

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, evoluzione della precedente Iniziativa OAI, Osservatorio Attacchi Informatici in Italia, costituisce l'unica indagine on line via web in Italia sugli attacchi informatici per tutti i settori merceologici, incluse le Pubbliche Amministrazioni Centrali e Locali, che fornisce una specifica e concreta indicazione del fenomeno degli attacchi intenzionali sui sistemi informatici italiani. OAD è una iniziativa in collaborazione e sotto l'egida di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (www.aipsi.org, capitolo italiano della internazionale ISSAC) e, pur garantendo una totale autonomia ed indipendenza, è sponsorizzata da Enti ed Aziende, ed ha il Patrocinio di varie Associazioni del settore.

A fianco dell'indagine annuale su tutte le tipologie di attacco (si veda la tassonomia nella tabella di fig.1), nel 2017 giunta alla settima edizione attualmente in preparazione, dopo i precedenti rapporti del 2016, 2015 (2014), 2013, 2012, 2011 e del 2009-10, si è voluto approfondire con una specifica indagine il tema sempre più critico degli attacchi agli applicativi, che ha prodotto il presente Rapporto. Esso è sponsorizzato da F5 Networks, la cui scheda di presentazione è nell'Allegato 2. I Patrocinatori del presente Rapporto sono gli stessi del Rapporto 2016 ed includono, oltre ad AIPSI, AICA (Associazione Italiana Calcolo Automatico), Assintel di Confcommercio (Associazione Nazionale Imprese ICT), Assolombarda di Confindustria, AUSED (Associazione Utilizzatori Sistemi e Tecnologie dell'informazione), CDI (Club Dirigenti Informatica di Torino), CDTI (Club Dirigenti Tecnologie dell'Informazione di Roma), Club per le Tecnologie dell'Informazione Centro, Club per le Tecnologie dell'Informazione Liguria, Club per le Tecnologie dell'Informazione di Milano, FidalInform (la Federazione dei ClubTI Italiani), FTI (Forum per le Tecnologie dell'Informazione), il Capitolo Italiano di IEEE-Computer Society, Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione), itSMF Italia (information technology Service Management Forum).

Nell'iniziativa OAD il ruolo attivo dei Patrocinatori è determinante per allargare e stimolare il bacino dei possibili risponditori contattati, oltre che per far conoscere e divulgare i rapporti, quelli annuali e quelli specifici, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza ICT.

I vari Rapporti annuali OAD ed i precedenti OAI sono scaricabili gratuitamente dai siti web di AIPSI, www.aipsi.org, e di Malabo Srl che li ha realizzati, www.malaboadvisoring.it.

La presente indagine sugli attacchi agli applicativi è stata condotta via web da novembre 2016 a marzo 2017, con 14 domande con risposte predefinite tra le quali scegliere, delle quali solo 3 riguardano il ruolo del rispondente, il settore e le dimensioni della sua azienda/ente.

Un numero di domande, e delle relative risposte, volutamente limitato, ben conoscendo la difficoltà di avere risposte da persone che hanno poco o nullo tempo per far mente locale e rispondere ad un questionario on line, soprattutto se su temi delicati come l'aver subito un attacco informatico, pur con la garanzia di un effettivo e totale anonimato (si veda §A.1). E ben consapevoli di non poter approfondire in maniera esaustiva e dettagliata un tema così complesso ed articolato come quello degli attacchi agli applicativi. L'obiettivo della presente indagine verticale, che è correlata a quella annuale del 2016, è di individuare alcuni specifici trend, che riguardano soprattutto l'uso del cloud, le principali modalità di attacco, gli impatti subiti, senza ripetere domande già poste nell'indagine annuale 2016, e che sono riprese e considerate solo come indicatori di riferimento, dato che si basano su bacini di rispondenti parzialmente diversi.

2. Gli attacchi digitali agli applicativi

Come già evidenziato nei Rapporti OAD annuali e nei vari rapporti internazionali, gli attacchi agli applicativi ed ai dati/informazioni da questi trattati, sovente indicati con il termine inglese di “data breach”, sono tra i più critici e più temuti, dato che vanno a ledere il bene informativo dell’azienda/ente, bene che risulta sempre più essenziale e strategico per ogni organizzazione di qualsiasi settore merceologico.

L’attacco contro un sistema informatico è tale quando si intende violato, con un’attività non autorizzata, almeno uno dei requisiti della sicurezza ICT, definita come la “protezione dei requisiti di integrità, disponibilità e confidenzialità” delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate. Nello specifico:

- **integrità** è la proprietà dell’informazione di non essere alterabile;
- **disponibilità** è la proprietà dell’informazione di essere accessibile e utilizzabile quando richiesto dai programmi e dagli utenti autorizzati;
- **confidenzialità** è la proprietà dell’informazione di essere nota solo a chi ne ha il diritto.

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**, che consiste nell’impossibilità da parte del mittente o del destinatario di negare l’invio o la ricezione di una informazione o di un messaggio.

La tassonomia degli attacchi informatici considerata nel questionario dell’indagine OAD annuale è riportata nella Tabella di fig. 2-1, nella quale l’ordine delle famiglie di attacco non fa riferimento alla loro criticità o gravità.

Facendo riferimento al Rapporto OAD 2016, la diffusione di queste famiglie di attacchi è indicata in fig. 2-2.

Gli attacchi agli applicativi ed ai dati trattati possono essere attuati da innumerevoli diverse combinazioni delle tipologie considerate nella Tabella di fig. 2-1, soprattutto nel caso di Target Attack e di APT.

La compromissione degli applicativi può essere causata anche dagli attacchi alle reti, dal DoS/DDoS, dagli attacchi fisici ai sistemi ICT e a quelli di supporto (es. impianto di alimentazione, di condizionamento, ecc.), ma gli attacchi diretti alle applicazioni derivano prevalentemente da:

- sfruttamento delle vulnerabilità del software applicativo (si veda §3), e/o del software di base e dal middleware: dal sistema operativo ai vari driver, dalle piattaforme dei data base server a quelle degli application server;
- accessi e modifiche non autorizzate (punti 7, 8 e 9 della Tabella) per violazione dei diritti d’accesso, che possono essere a loro volta causati dal furto di identità digitale e dal suo utilizzo illegale; tale furto può avvenire con diverse modalità, dal phishing all’analisi delle informazioni su di una persona tramite i social network fino al furto (o grazie allo smarrimento) di dispositivi mobili, in particolare di smartphone e tablet; si tenga presente che in questi dispositivi i contenuti e le identità digitali sono in chiaro nella maggior parte dei casi.

1. Attacchi fisici, quali sabotaggi e vandalismi, con distruzione di risorse informatiche e/o di risorse a supporto (es. UPS, alimentatori, condizionatori, ecc.) a livello centrale o periferico.
2. Furto di apparati informatici, facilmente occultabili e trasportabili, contenenti dati (unità di rete, Laptop, hard disk, floppy, nastri, Chiavette USB, ecc.)
3. Furto di informazioni e loro uso illegale da dispositivi mobili (palmari, cellulari, laptop)
4. Furto di informazioni e loro uso illegale da dispositivi non mobili e da tutte le altre risorse ICT.
5. Attacchi di Social Engineering e di Phishing per tentare di ottenere con l'inganno (via telefono, e-mail, chat, ecc.) informazioni riservate quali credenziali di accesso, identità digitale, ecc.
6. Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio: viene minacciato l'attacco, magari dimostrando la capacità di effettuarlo, ma non è effettuato; spesso il solo ricatto basta per effettuare la frode. Rientra in questa tipologia il ransomware)
7. Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni
8. Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.
9. Modifiche non autorizzate ai dati e alle informazioni trattate
10. Utilizzo vulnerabilità del codice software, sia a livello di posto di lavoro che di server: tipici esempi: back-door aperte, SQL injection, buffer overflow, ecc.
11. Codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots , exploits, sia a livello di posto di lavoro che di server.
12. Attacchi per la saturazione di risorse ICT: oltre a DoS (Denial of Service), DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc. Anche le botnet possono essere indirizzate a DDoS, ma richiedendo degli agenti (bot) sono considerate malware
13. Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)
14. Attacchi mirati (targeted) e APT, Advanced Persistent Threats, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco.

Fig. 2-1 Elenco delle tipologie di attacchi intenzionali considerati da OAD

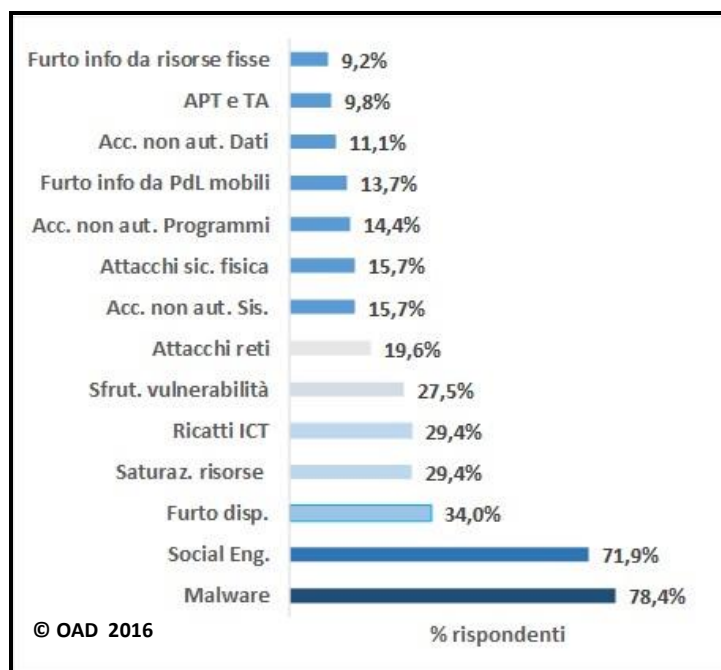


Fig. 2-2 Dal Rapporto 2016 OAD: ripartizione percentuale per tipologia di attacco (risposte multiple)

3. Le principali vulnerabilità degli applicativi

Il codice di una applicazione può contenere svariati punti deboli ed errori (intenzionali o non) che, se scoperti, offrono vulnerabilità anche molto gravi. Oggi aumentano le applicazioni che operano direttamente su Internet e queste sono spesso realizzate con tecnologie sofisticate che prevedono l'esecuzione di codice sia sul client (il browser) sia lato server: la stragrande maggioranza delle moderne applicazioni sono infatti basate sul web cui si accede via browser dal dispositivo d'utente, che può essere PC, smartphone o tablet.

Il rischio che siano presenti vulnerabilità a livello applicativo è crescente sia come numerosità sia come gravità, sia lato client sia lato server. Inoltre, si deve tener presente che, mentre il sistema operativo, il software di base ed i software middleware sono realizzati da società di alta specializzazione, che li sottopongono a test profondi e sistematici, ed hanno una vita relativamente lunga, le applicazioni, in particolare quelle web, possono essere implementate velocemente da tecnici meno competenti in termini di programmazione sicura, avere procedure di test semplificate ed una vita in genere molto più breve con il risultato di essere più a rischio, con più vulnerabilità e quindi di poter essere più facilmente attaccabili. Un caso particolare sono i software open source, che se supportati da ampie comunità di sviluppatori e di utenti, sono ad alta sicurezza e affidabilità, dati i numerosissimi test cui sono sottoposti a livello mondiale. Ben diversa la situazione di prodotti open source datati, poco o non più aggiornati, che non dovrebbero essere più utilizzati, o le personalizzazioni ed i moduli di integrazione tra applicativi costituiti da prodotti open source anche assai diffusi.

Tutti i software di base ed i middleware, anche i più diffusi ed autorevoli, presentano vulnerabilità, alcune delle quali non note nemmeno ai produttori: sono chiamate in gergo "zero day vulnerability", e per esse non esistono patch e fix correttive. E tutte queste vulnerabilità, "zero day" o non, possono essere sfruttate, intenzionalmente o non, dagli applicativi che utilizzano questi software di sistema. Anche le vulnerabilità non più "zero day" pur con la disponibilità di aggiornamenti e patch che le eliminano, risultano in vari casi utilizzate dagli attacchi, poiché non sono stati installati gli aggiornamenti o le patch di correzione. Uno dei motivi per il non aggiornamento è l'interruzione del contratto di manutenzione, causa la crisi economica e la necessità di tagliare costi: si riduce un (relativamente) piccolo costo da un lato, si apre un serio rischio di ben altri costi se un attacco basato su tale vulnerabilità avesse successo.

Le varie analisi sulle vulnerabilità applicative a livello internazionale indicano che sono relativamente poche le situazioni che causano la maggior parte dei problemi di sicurezza del software. È possibile raggrupparle logicamente nei seguenti gruppi, elencati non in ordine di criticità o di importanza:

- programmazione del codice con errori e/o inadeguati controlli, talvolta anche per uso di linguaggi di programmazione intrinsecamente poco sicuri; in alcuni casi gli "errori", chiamati in gergo "bug", sono volutamente inseriti per poter poi, grazie a loro, effettuare degli attacchi". Tipici esempi di tali errori e vulnerabilità includono:
 - **non controllo della stringa di input e injection** : se non viene accuratamente controllato dall'applicativo, l'input dell'utente può contenere codice che viene eseguito, oppure i dati non verificati vengono eseguiti come un comando: un tipico esempio è un SQL Injection, che usa comandi SQL
 - **XSS, Cross Site Scripting**: è un caso di injection nei siti web, che consente di inserire a livello "client", ossia del browser, dei codici maligni via "script" (ad esempio con JavaScript) o HTML per modificare le pagine web;
 - **directory traversal**, indicato anche come "path traversal", "directory climbing", e "backtracking": consiste nello sfruttare la mancanza o l'insufficiente verifica dei nomi dei file di input forniti dall'utente; lo sfruttamento di questa vulnerabilità applicativa consente di guadagnare accessi non autorizzati al file system locale e/o remoto;
- **HTTP Response Splitting**: la vulnerabilità dell'applicazione web (e dell'ambiente che la suppor-

ta) consente di inserire nell'header (intestazione) della risposta del protocollo HTTP una sequenza di contenuti forniti dall'attaccante, tipicamente inserendoli nei campi di input inviati all'applicazione. L'attaccante può così impostare intestazioni arbitrarie, prendere il controllo del corpo del messaggio del protocollo o suddividere la risposta in due o più risposte separate, da cui il nome della vulnerabilità;

- **non gestione dei limiti della memoria e buffer overflow:** se è possibile depositare nel buffer di memoria della applicazione una stringa più lunga del buffer stesso, allora è possibile aggiungere in questo buffer codice che, quando eseguito, compie azioni imprevedibili per l'attaccato. Questa tecnica richiede grande competenza per preparare il suo sfruttamento (il così detto exploit), ma quando questo è pronto può essere reso disponibile su internet e utilizzato anche da hacker con poca competenza tecnica;
- **back door:** nell'applicazione sono lasciati dei punti d'accesso "nascosti" che permettono di accedere al programma superando le normali procedure e barriere d'accesso. Back door sono sovente e lecitamente usate per il test ed il debug dei programmi, ma se vengono lasciate, volutamente o non, nel programma in produzione offrono formidabili punti di ingresso per innumerevoli attacchi;
- **CSRF, Cross-Site Request Forgery:** grazie a questa vulnerabilità applicativa, l'utente di un sito web nel quale è correttamente autenticato viene forzato ad eseguire azioni non volute;
- **File inclusion:** tipica vulnerabilità di applicazioni web dovuta a script operanti a run time (scripting run time); questa vulnerabilità si presenta quando un'applicazione crea un percorso per il codice eseguibile usando una variabile controllabile dall'attaccante, così che quest'ultimo può controllare quale file è eseguito al run time;
- **Code execution, indicato anche con l'aggiunta di "arbitrary" o "remote":** indica la generica vulnerabilità che consente, in maniera non autorizzata e non voluta dall'utente, l'esecuzione di un determinato programma, tipicamente di un malware;
- Vulnerabilità delle infrastrutture, del software di base e del middleware: gli applicativi operano o direttamente sopra il sistema operativo della macchina sulla quale sono installati, o sulle piattaforme server che a loro volta si basano sul sistema operativo e sui suoi driver per la gestione delle varie periferiche. Tutti questi software, operanti sia a livello del dispositivo d'utente, PC, tablet o smartphone, sia a livello server, hanno delle vulnerabilità, che quando sono individuate vengono classificate a livello mondiale: una delle principali classifiche di riferimento è fornita da CVE, Common Vulnerabilities and Exposures, si veda <https://cve.mitre.org/>. Dato che le applicazioni usano, tramite opportune interfacce ed opportune "chiamate", questi software d'ambiente, se vulnerabili rendono vulnerabile l'applicazione stessa; e tramite le vulnerabilità di questi ultimi sono attaccati gli applicativi che li usano;
- Errata configurazione dell'applicativo e/o del middleware e del software di base: molti applicativi sono pacchetti che possono operare in diversi ambienti (ad esempio sia in ambito Windows sia in ambito Linux e Unix) con innumerevoli opzioni che debbono essere opportunamente settate, alcune delle quali relative alle caratteristiche di sicurezza; in numerosi casi l'applicativo richiede che siano opportunamente configurati, settando parametri ed opzioni, gli ambienti software sottostanti, di cui al punto precedente;
- inadeguati controlli dell'identificazione, autenticazione e controllo degli accessi degli utenti e degli amministratori di sistema. Si deve considerare che il sistema di identificazione ed autenticazione è sovente un software unico e comune a tutti (o ad un determinato dominio degli) gli applicativi, si pensi ad esempio ad Active Directory e ai sistemi LDAP, mentre il controllo degli accessi è il più delle volte attuato da moduli interni al singolo applicativo; e questo comporta ovvi problemi di gestione dei controlli, crescenti al crescere del numero di applicazioni e di utenti;
- **carenze nell'autenticazione:** un punto delicato a volte lasciato a codice realizzato artigianalmente o a codice che accetta approcci semplificati e/o ingenui per semplificare la vita all'utente, un esempio password non protette memorizzate in cookie oppure URL di autenticazione che per-

mettono di effettuare un “reply attack”: se le informazioni relative alla autorizzazione alla richiesta sono contenute nello stesso messaggio, questo può essere intercettato in rete e ripresentato dall’attaccante anche con qualche variazione. Se non perfettamente implementata l’autenticazione può consentire il furto di password, il riutilizzo di credenziali, l’aggiornamento dell’autenticazione;

- **carenze nell’autorizzazione:** la profilazione degli utenti genera elevate complessità gestionali che arrivano a difficoltà di verifica e di aggiornamenti, causando possibilità di accesso a informazioni non autorizzate. Esempi di classiche carenze sono il nascondere le chiavi di accesso alle autorizzazioni dove possono essere modificate (ad esempio in cookie e variabili javascript) o consentire identificativi incontrollati alternativi di una risorsa (il nome della risorsa come ASCII viene bloccato, lo stesso nome codificato Unicode non viene riconosciuto);
- Carenze nella crittografia e nella sua gestione: la crittografia è una tecnologia complessa e specialistica, sovente poco conosciuta anche da chi la deve installare. La crittografia è la tecnica che consente di ben proteggere i file ed i dati tratti dalle applicazioni, ovunque siano archiviati. I moderni prodotti di crittografia sono relativamente semplici da usare per l’utente finale, ma debbono essere ben configurati, debbono essere correttamente scelti gli algoritmi utilizzati, e soprattutto debbono essere ben gestite le funzionalità di contorno come la memorizzazione e il riutilizzo delle chiavi, la generazione dei numeri casuali, e così via. L’uso di chiavi e di algoritmi troppo semplificati può facilmente e velocemente far mettere in chiaro le informazioni crittate e ritenute per questo inviolabili.

A livello mondiale esistono alcune banche dati che elencano, aggiornandole sistematicamente, tutte le vulnerabilità individuate a livello di software di base e di pacchetti applicativi, commerciali e open source. La più nota di queste è la già citata banca dati CVE, Common Vulnerabilities and Exposures, che alla data ha definito 668 tipi di vulnerabilità (si veda <https://www.cvedetails.com/cwe-definitions.php>), associando a ciascun tipo il numero di vulnerabilità individuate nei vari prodotti e soluzioni sul mercato. Ai primi tre posti le vulnerabilità di fig. 3-1, che riprendono i concetti illustrati all’inizio del presente paragrafo.

<i>Tipologia CVE vulnerabilità</i>	<i>Numero vulnerabilità individuate</i>
Failure to Constrain Operations within the Bounds of a Memory Buffer	8115
Failure to Preserve Web Page Structure ('Cross-site Scripting')	7208
Improper Input Validation	4402

*Fig. 3-1 Tipologie di vulnerabilità definite da CVE con il più alto numero di vulnerabilità individuate
(Fonte CVE)*

OWASP (Open Web Application Security Project – www.owasp.org) mantiene annualmente un elenco delle 10 più importanti vulnerabilità legate alle applicazioni web². Per il 2017 le principali vulnerabilità identificate sono le seguenti, elencate in ordine alfabetico, e già spiegate in precedenza:

- Broken Access Control
- Broken Authentication and Session Management
- Cross-Site Request Forgery (CSRF)
- Cross-Site Scripting (XSS)
- Injection
- Insufficient Attack Protection
- Security Misconfiguration

- Sensitive Data Exposure
- Using Components with Known Vulnerabilities
- Underprotected APIs.

CVE fornisce ³ nella tabella in fig. 3-2 l'elenco del numero più elevato di vulnerabilità indipendenti per tipo di sistema operativo (sia dispositivo d'utente che server) e per taluni ambienti applicativi, dai più diffusivi browser a sistemi multimediali come Flash. L'elenco evidenzia come taluni prodotti, da molti ritenuti sicuri, in realtà presentano numerose vulnerabilità e sono di fatto insicuri, anche se finora meno soggetti ad attacchi rispetto ad altri prodotti.

² Oswap Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

³ si veda <https://www.cvedetails.com/top-50-products.php>

	Nome del prodotto	Azienda	Tipo prodotto	Numero vulnerabilità individuate
1	Mac Os X	Apple	OS	1820
2	Linux Kernel	Linux	OS	1815
3	Firefox	Mozilla	Application	1437
4	Chrome	Google	Application	1425
5	Iphone Os	Apple	OS	1176
6	Flash Player	Adobe	Application	1013
7	Debian Linux	Debian	OS	1003
8	Android	Google	OS	884
9	Windows Server 2008	Microsoft	OS	846
10	Safari	Apple	Application	841
11	Internet Explorer	Microsoft	Application	840
12	Ubuntu Linux	Canonical	OS	839
13	Windows Vista	Microsoft	OS	814
14	Opensuse	Novell	OS	785
15	Acrobat	Adobe	Application	781
16	Windows Xp	Microsoft	OS	726
17	Windows 7	Microsoft	OS	708
18	Thunderbird	Mozilla	Application	703
19	Seamonkey	Mozilla	Application	698
20	Mac Os X Server	Apple	OS	641
21	IE	Microsoft	Application	631
22	PHP	PHP	Application	536
23	Solaris	SUN	OS	533
24	Acrobat Reader	Adobe	Application	515
25	Windows 2000	Microsoft	OS	507
26	JRE	Oracle	Application	491
27	JDK	Oracle	Application	480
28	Windows Server 2012	Microsoft	OS	467
29	Windows 2003 Server	Microsoft	OS	443
30	Wireshark	Wireshark	Application	441
31	Firefox ESR	Mozilla	Application	440
32	IOS	Apple	OS	436
33	JRE	SUN	Application	435
34	Database Server	Oracle	Application	421
35	Enterprise Linux	Redhat	OS	418
36	Itunes	Apple	Application	415
37	Windows Server 2003	Microsoft	OS	412
38	Acrobat Reader Dc	Adobe	Application	411
39	Acrobat Dc	Adobe	Application	411
40	Windows 8.1	Microsoft	OS	406
41	JDK	SUN	Application	405
42	Office	Microsoft	Application	399
43	Fedora	Fedoraproject	OS	397
44	Mysql	Oracle	Application	391
45	AIR	Adobe	Application	381
46	Solaris	Oracle	OS	355
47	Windows Rt 8.1	Microsoft	OS	351
48	Air Sdk	Adobe	Application	340
49	Enterprise Linux Desktop	Redhat	OS	333
50	Leap	Novell	OS	332

Fig. 3-2 Numero di vulnerabilità indipendenti per tipo di prodotto (Fonte: CVE)

La fig. 3-3 mostra il numero dei principali tipi di vulnerabilità individuati nel corso del 2015 e 2016 e quelli correnti fino alla fine del 1° quadrimestre 2017. La Tabella evidenzia in alcuni casi delle diminuzioni tra il 2015 ed il 2016, in altri casi un aumento: il numero di vulnerabilità complessive è quasi uguale. I dati per il 2017 riguardano alla data poco più del primo trimestre dell'anno, ed il numero complessivo per le vulnerabilità in colonna risulta già alto. Si noti che la colonna in bianco della tabella indica una vulnerabilità non specifica per gli applicativi, mentre quelle in giallo sono vulnerabilità degli applicativi.

Anno	# Vulnerabilità	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Indusion
2015	6452	1792	1820	1078	749	213	758	146	12	577	748	367	245	5
2016	6435	2029	1494	1326	717	94	495	98	15	444	840	601	86	7
2017 (1Q)	4540	1103	1032	786	230	99	470	73	3	205	528	138	96	4

Fig. 3-3 Le vulnerabilità individuate da CVE, evidenziate in giallo quelle specifiche per le applicazioni (Fonte: CVE)

La sintetica descrizione in questo capitolo delle vulnerabilità per gli applicativi e per il software d'ambiente e di base che utilizzano fornisce un'idea delle molteplici vulnerabilità che possono essere sfruttate dagli attaccanti e quindi della complessità e della difficoltà nell'implementare misure di sicurezza che li possano efficacemente contrastare.

4. Gli attacchi digitali rilevati dall'indagine e le loro cause

In questo capitolo sono riportati e commentati i dati emersi dalla presente indagine sugli attacchi agli applicativi rilevati dai rispondenti negli anni 2015 e 2016, e le loro macro cause, così come ritenuto dai rispondenti: vulnerabilità del codice software dell'applicativo, vulnerabilità dei sistemisti di identificazione, autenticazione e controllo degli accessi, furto di informazioni da dispositivi mobili, in particolare identità digitali, con le quali usare in maniere illegale e/o criminale gli applicativi cui si è illegalmente guadagnato l'accesso.

Il rischio di porre domande dettagliate e molto tecniche nel questionario è di non avere risposte o, peggio, di avere risposte selezionate a caso tanto per rispondere. Si è preferito pertanto porre poche domande e di carattere generale, alle quali la maggior parte dei possibili rispondenti avrebbe potuto e saputo rispondere. Si ricorda infatti che l'obiettivo dell'indagine, come già illustrato in §1, è di inquadrare e comprendere il fenomeno degli attacchi agli applicativi in Italia, e non di analizzare in dettaglio gli attacchi rilevati individuando le falle nelle misure di sicurezza.

L'indagine online di OAD sugli attacchi applicativi ha visto un totale di 173 rispondenti nell'arco di circa 4 mesi solari, da fine novembre 2016 a fine marzo 2017, periodo durante il quale il questionario è rimasto on line. Come dettagliato in §7.1, i rispondenti appartengono prevalentemente al settore merceologico dei servizi ICT e dei servizi professionali, oltre a quello manifatturiero: gli altri settori merceologici, pur tutti rappresentati, hanno avuto un numero di rispondenti molto inferiore.

La fig. 4-1 mostra, sul campione dei rispondenti, quanti hanno subito e rilevato attacchi agli applicativi e quanti no, nei due anni considerati: nel 2016 la percentuale di attacchi agli applicativi rilevati è diminuita del 4,6% rispetto al 2015, probabilmente grazie anche al miglioramento delle misure di prevenzione e di protezione (si veda §5) che le aziende/enti dei rispondenti hanno adottato.

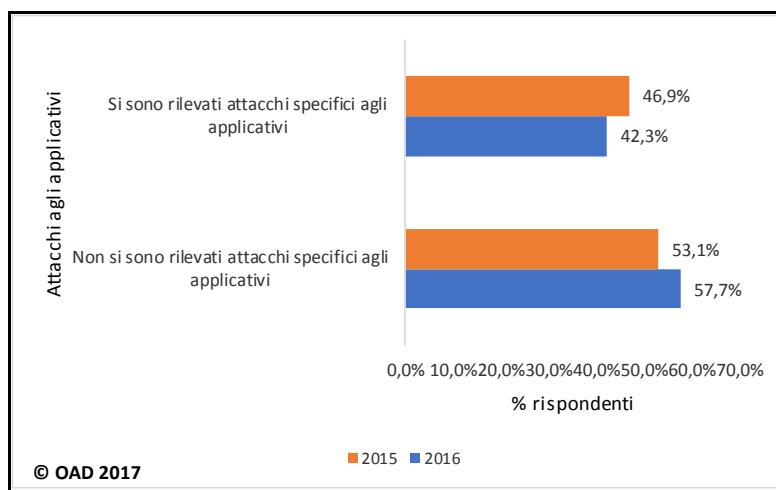


Fig. 4-1 Percentuale di rispondenti che hanno subito e rilevato attacchi agli applicativi nel 2015 e nel 2016

Il Rapporto annuale 2016 OAD riporta che il campione di rispondenti ha subito e rilevato in percentuale il 37,6% di attacchi di ogni tipo, confermando un trend consolidato negli anni per le indagini OAD-OAI: in Italia subisce e rileva un attacco digitale meno del 40% del campione dei rispondenti, dato da intendersi solo come indicazione di trend dato il campione di rispondenti parzialmente diverso nei vari anni.

Una percentuale confermata da rapporti internazionali e che è dovuta, a giudizio dell'autore, soprattutto dalla maggioranza di piccole e piccolissime imprese in Italia, che non costituiscono, singolarmente, un obiettivo di interesse per organizzazioni, spesso internazionali, di cyber criminali. Una seconda causa è sicuramente data

dalla non rilevazione, in molti casi, dell'attacco subito, ma questo significa che tale attacco non ha avuto rilevabili impatti sull'azienda/ente, al di là del possibile furto di informazioni.

Tenendo sempre presente la valenza assolutamente indicativa e non statistica di questi confronti, la fig. 4-1 mostra come gli attacchi agli applicativi, indipendentemente dalle cause che verranno approfondite nei paragrafi seguenti, sono stati rilevati da più del 40% dei rispondenti sia nel 2016 sia nel 2015.

4.1 Attacchi dovuti a vulnerabilità del software applicativo

Tra quelli che hanno subito attacchi, ¼ circa ha rilevato attacchi agli applicativi causati da vulnerabilità del codice software.

La fig. 4-2 mostra che non ci sono grandi differenze tra il 2015 ed il 2016, e che in entrambi i casi circa ¼ dei rispondenti ha subito e rilevato attacchi agli applicativi dovuti a vulnerabilità del software applicativo stesso, tipicamente per vulnerabilità del codice dovute a programmazione non accurata, che non tiene ben conto degli aspetti di sicurezza, che presenta bachi, e così via: in pratica un codice applicativo intrinsecamente non sicuro. Su questo ampio, complesso e assai dibattuto tema è opportuno fare alcune considerazioni.

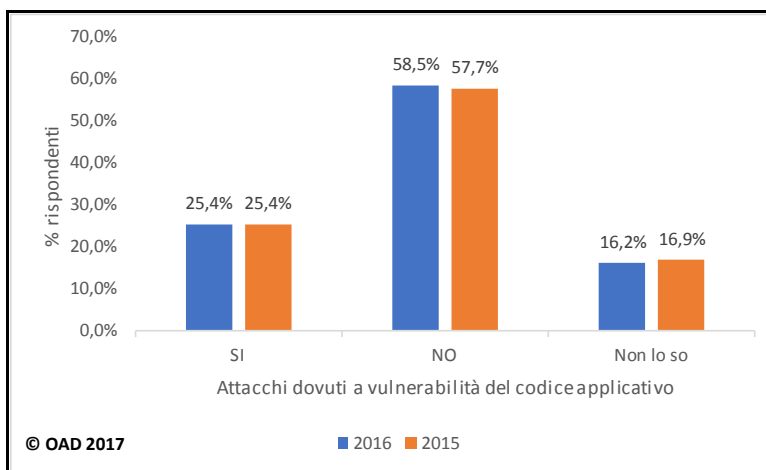


Fig. 4-2 Attacchi dovuti a vulnerabilità del codice applicativo

Le attuali tecniche di programmazione di software, al di là del linguaggio usato, si basano tutte sull'utilizzo di componenti che o sono già nelle librerie del linguaggio, o si possono acquisire via Internet. La realizzazione di un applicativo software è diventato più un assemblaggio di componenti tra loro interagenti tramite opportune API, Application Program Interface, e/o metodi quali web services. Tali componenti sono usati già compilati, conoscendo solo come interfacciarsi a loro per richiamarli ed integrarli nell'architettura complessiva dell'applicazione. Non si ha normalmente visibilità sul listato del codice, e quindi non si può sapere come sono fatti al loro interno, quale la qualità del codice ed il livello di sicurezza implementato a livello del programma. I componenti sono dei black box utilizzabili tramite la loro interfaccia, ma di cui si ignora l'effettiva sicurezza al loro interno: di fatto si usano fidandosi dell'autorevolezza associata al nome dell'azienda che li ha sviluppati.

La progettazione e l'implementazione di codice sicuro parte (o dovrebbe partire) dalla scelta di un linguaggio "intrinsecamente" sicuro nella sua impostazione, che così aiuta e talvolta forza lo sviluppatore a produrre un codice sicuro: uno di questi linguaggi è sicuramente Java, che consente di integrare commenti con la sua estensione JML, Java Modeling Language, e per il quale sono disponibili vari ambienti di sviluppo, tra i quali il ben noto e diffuso open source Eclipse.

I sistemi di sviluppo integrati (IDE, Integrated Development Environment) sono molto utili per scrivere e documentare software sicuro. Sul mercato sono presenti vari IDE, taluni in grado di supportare diversi linguaggi di programmazione, quali ad esempio il citato Eclipse, Visual Studio NET della Microsoft, IBM Rational Application Developer, altri specializzati per determinati linguaggi, quali ad esempio per Java Oracle JDeveloper e JBuilder della Borland.

Un IDE, se usato correttamente, facilita il disegno delle specifiche del programma, aumenta il livello di sicurezza nella stesura dei programmi, e consente una loro più accurata documentazione.

Un buon progetto dell'applicativo che lo contestualizzi in un ambiente di supporto a sua volta sicuro, e l'uso di IDE sono solo i primi tasselli per la produzione di software sicuro.

Un ulteriore successivo passo consiste nell'effettuare test del programma applicativo non solo funzionali ma anche tecnici, per verificare la presenza di bachi nella programmazione, di vulnerabilità tecniche, e così via. Gli standard di riferimento per il testing di software sono inclusi nella famiglia ISO 29119. Gli stessi IDE forniscono strumenti di test e debug del codice.

4.2 Attacchi dovuti a vulnerabilità dei sistemi di identificazione-autenticazione-controllo accessi

L'utente che accede ad un applicativo deve essere realmente chi dichiara di essere, altrimenti l'integrità e la consistenza dell'applicativo e dei dati trattati possono essere gravemente a rischio.

Aprire o aggirare il sistema di identificazione-autenticazione-autorizzazione per l'accesso può essere una delle principali cause di violazione intenzionale di un applicativo.

I rispondenti hanno rilevato attacchi applicativi per questa causa con percentuali molto simili per il 2015 e per il 2016, con una percentuale attorno ad 1/5 del totale del campione emerso, come evidenziato nella fig.4-3.

La percentuale emersa dal campione non è così bassa come si potrebbe pensare, considerando che numerosi rispondenti appartengono ad aziende del settore ICT (si veda §5) e si presumono pertanto competenti e dotati di idonei strumenti correttamente gestiti.

La vulnerabilità dei sistemi di identificazione ed autenticazione possono avere a loro volta diverse cause, tenendo conto che nella maggior parte dei casi sono sistemi sofisticati, complessi e con varie opzioni da scegliere e parametri da configurare.

Alcuni sistemi sono moduli integrati nei sistemi operativi o nel prodotto applicativo, altri sono contestuali a specifici ambienti, si pensi ad esempio all'Active Directory in ambito Windows Microsoft, altri ancora sono prodotti ad hoc trasversali e compatibili con i diversi sistemi operativi, ambienti ed applicazioni, per facilitare una omogeneizzazione e centralizzazione degli strumenti di controllo degli accessi, delle policy e del loro governo. Come per ogni altro codice software, anche per i sistemi di autenticazione e controllo accessi molte vulnerabilità dipendono da bachi nel programma, da uno sviluppo non sicuro, da una cattiva configurazione nell'installazione e/o da un mix di queste cause.

Nel caso di sistemi sviluppati ad hoc (per specifiche esigenze e/o per semplificare il processo di autenticazione e/o per risparmiare i costi non sempre bassi dei prodotti commerciali), bachi e programmazione insicura possono essere più numerosi e più gravi, rispetto a prodotti seri e consolidati di mercato, offrendo così ben maggiori opportunità di attacco.

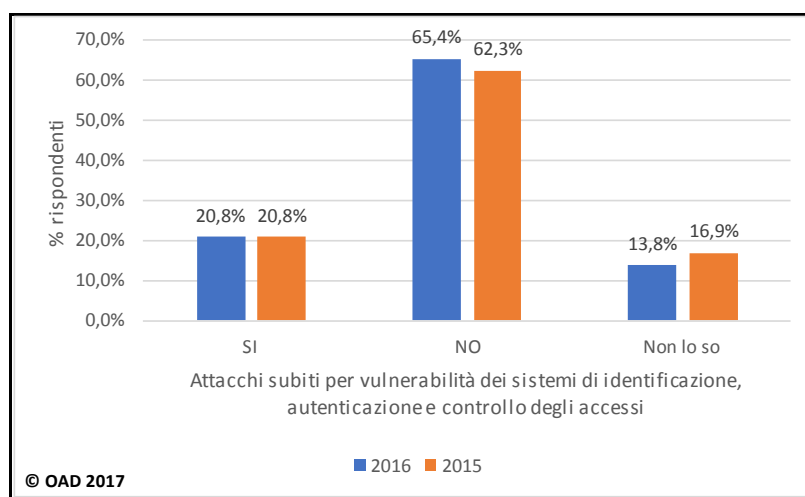


Fig. 4-3 Attacchi agli applicativi dovuti a vulnerabilità dei sistemi di identificazione-autenticazione-controllo accessi

Per l'autenticazione ed il controllo degli accessi una grave e diffusa vulnerabilità è rappresentata dal comportamento degli utenti, sia utenti finali sia amministratori ed operatori dei sistemi ICT.

Sovente in un ufficio tutti conoscono le identità digitali dei colleghi, almeno per gli account del sistema informatico dell'azienda/ente; e tale diffusione è voluta, così che una persona possa fare le veci di ed aiutare un'altra, compromettendo però l'effettiva sicurezza informatica dell'intero sistema; nel caso di amministratori di sistema questa usanza è ancor più grave, data la criticità delle operazioni che possono svolgere e dato che viene lesa la tracciabilità di chi ha fatto che cosa, obbligatoria per la privacy.

Proprio nell'ambito del controllo degli accessi l'utente finale (e sovente anche l'amministratore-operatore di sistemi ICT) riscontra una contrapposizione tra la facilità d'uso dei sistemi ICT e le misure di sicurezza per proteggerli. L'uso di autenticazione a due o più fattori, l'uso di password non banali, sovente cambiate e diverse di volta in volta e sufficientemente lunghe, la difficoltà di gestire numerosi account con identificativi e password diverse, sono considerati tutti ostacoli alla produttività personale e, appena possibile, bypassati: chi può essere interessato ai miei dati e alle mie attività? E questo è ancora più diffuso per i dispositivi mobili, in particolare gli smartphone.

Ulteriori criticità nel controllo degli accessi derivano da una loro approssimativa, se non cattiva, gestione: tempi lunghi per eliminare account di persone non più in azienda, account generici e non nominativi per fornitori e consulenti, password banali che fanno diretto riferimento a nomi ed eventi dell'utente, facilmente scopribili navigando sui social network che l'utente frequenta, e così via.

In questi casi il problema non è tecnico, ma organizzativo e comportamentale. Ed il tutto si basa, quasi sempre, su una superficiale ed approssimativa conoscenza dei problemi della sicurezza digitale, e dei gravi impatti che anche un "semplice" attacco può causare (si pensi al "ransomware"), se non ci sono almeno le misure di base della sicurezza, come per l'esempio un back up periodico e completo.

4.3 Attacchi dovuti al furto di informazioni da dispositivi mobili degli utenti e/o degli operatori ICT

Qualsiasi sistema di identificazione, autenticazione e di controllo degli accessi può essere violato, pur senza sfruttare sue eventuali vulnerabilità, se l'identità digitale di un utente autorizzato viene rubata o carpita, tipicamente da smartphone e chiavette USB, oppure grazie a tecniche di social engineering ⁴ e/o tramite un comportamento dell'utente stesso "inadeguato" alla sicurezza digitale.

Nella presente indagine è stata prevista una specifica domanda in merito.

Nei dispositivi mobili, oltre che nel proprio PC, sovente si tiene l'elenco dei propri account e relative password, e nella maggior parte dei casi totalmente in chiaro. Se si perde o se viene rubato il dispositivo mobile, chi se ne appropria può facilmente accedere a questo elenco, ed accedere agli applicativi ed ai servizi informatici aziendali e personali sostituendosi al legittimo proprietario.

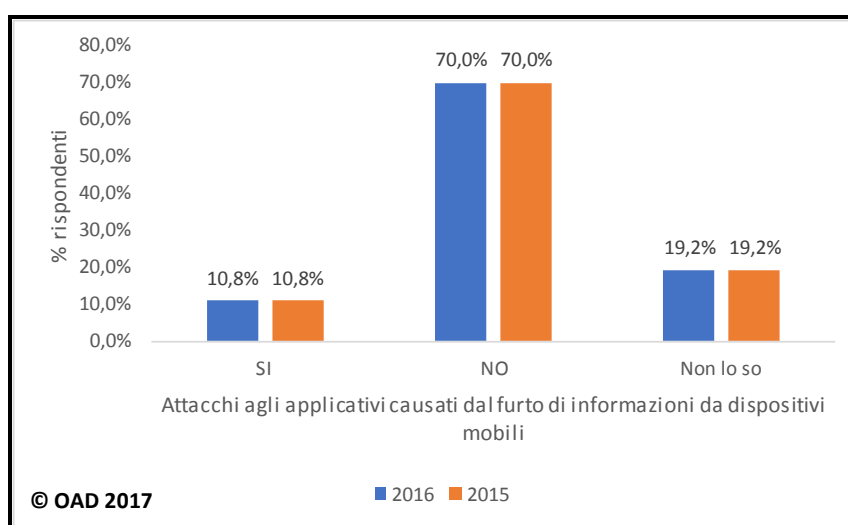


Fig. 4-4 Attacchi dovuti a vulnerabilità del codice applicativo

La fig. 4.4 mostra i risultati dell'indagine su questo punto: il 10,8% rispondenti dichiara di aver subito attacchi ai sistemi di controllo degli accessi a causa di identità digitali sottratte da dispositivi mobili, il 19,2% di non saperlo o di non averne prova.

Si deve tener conto che i dispositivi mobili non includono solo cellulari, smartphone e tablet, ma anche chiavette USB, hard disk removibili e CD/DVD; e che i dispositivi mobili sono usati non solo dagli utenti finali, ma anche dagli operatori e dai responsabili dei sistemi informatici che li gestiscono. Il furto delle identità digitali degli amministratori e degli operatori è ben più grave di quello di un utente finale: un cyber criminale, entrandone in possesso, può manomettere parte o l'intero sistema informatico.

La percentuale di poco superiore al 10% dei rispondenti che hanno riscontrato e/o ritengono che gli attacchi agli applicativi dipendano da questa causa, pur non elevato, è comunque significativo, ed è un indicatore del grave rischio che si corre mettendo, spesso senza protezioni, i propri account su dispositivi mobili, che sono veramente facile da perdere ... o da farsi rubare.

La precedente fig. 2-2, riportata dal Rapporto OAD 2016, mostra come ben il 13,7% dei rispondenti abbia subito il furto di informazioni da apparati mobili (contro il 9,2% di dati sottratti da dispositivi fissi): informazioni che sono state sicuramente usate per tentare di effettuare attacchi informatici e/o frodi.

⁴ Il social engineering è uno degli attacchi più diffusi, come rilevato nelle varie edizioni di OAD/OAI e mostrato nella fig. 2.2.

4.4 Attacchi dovuti a vulnerabilità dei sistemi infrastrutturali quali sistemi operativi, piattaforme web, ecc.

Si è in precedenza sottolineato come gli attacchi agli applicativi possano essere sferrati sfruttando anche le vulnerabilità del middleware⁵, del software di base⁶ e delle infrastrutture ICT sottostanti. Ed è significativo che tali cause siano al primo posto, con una percentuale attorno al 37% (si veda fig. 4-5), ben superiore al 25% delle vulnerabilità intrinseche del codice dell'applicazione (fig. 4-1).

Volutamente la domanda del questionario è generica e comprende i diversi componenti ed ambienti sui quali poggia l'applicazione: si rinuncia a raccogliere vari dettagli, anche importanti, ma che avrebbero richiesto più domande specifiche, alle quali forse solo pochi avrebbero voluto o saputo rispondere.

Il risultato emerso, a giudizio dell'autore, è quello più significativo ed interessante di tutta la presente indagine: la principale causa degli attacchi agli applicativi è dovuta alle vulnerabilità delle infrastrutture ICT, del software di base e del middleware utilizzati dall'applicazione attacca.

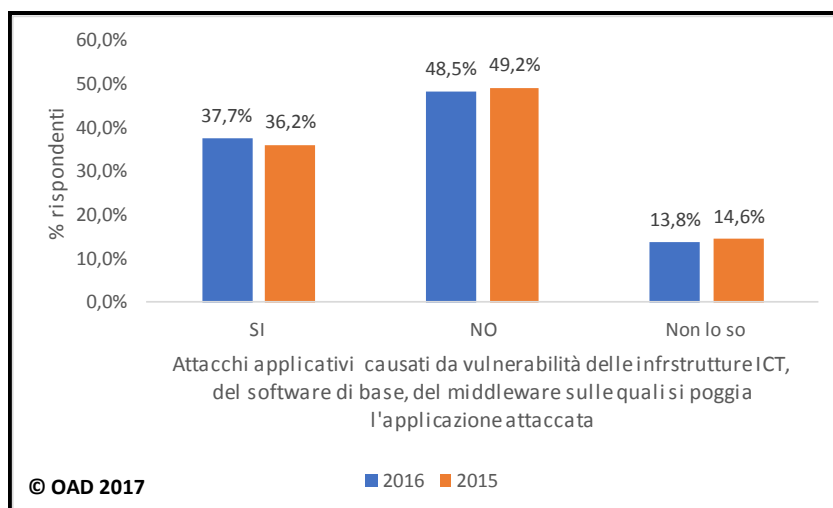


Fig. 4-5 Attacchi agli applicativi dovuti alle vulnerabilità di tutto il software ed i sistemi sottostanti all'applicazione stessa

Il risultato è ragionevole e facilmente spiegabile: le vulnerabilità del software di base e del middleware sono ben analizzate e classificate, come descritto in §3, ed un attaccante, conoscendo l'ambiente obiettivo (target), può in breve conoscere le vulnerabilità esistenti per esso, e verificare se il sistema target ha già installato gli aggiornamenti per tali vulnerabilità, e quali di esse sono ancora scoperte: e su queste ultime basare le azioni di attacco.

⁵ Termine molto usato ma senza una condivisa ed univoca definizione: fa riferimento a tutti quei moduli e componenti software che sono tra il software di base, in particolare il sistema operativo, e l'applicazione, soprattutto se distribuita.

⁶ Con il termine di "software di base" si intende normalmente il sistema operativo, i compilatori e gli interpreti, le librerie.

5. Le misure di sicurezza in atto

Nel precedente capitolo sono descritti ed analizzati gli attacchi agli applicativi subiti dai rispondenti a questa indagine OAD. In questo capitolo vengono analizzate le misure di sicurezza che i sistemi informatici dei rispondenti utilizzano e nel prossimo capitolo si forniranno brevi indicazioni su alcune caratteristiche del loro ambiente applicativo.

Sulle misure di sicurezza in essere per gli applicativi sono state effettuate alcune specifiche domande, complementari a quelle già poste nel questionario nell'indagine annuale del 2016 ed le cui risposte sono descritte nel Rapporto OAD 2016.

La classificazione delle applicazioni (e quindi dei dati trattati e dei sistemi ICT sui quali operano) critiche per il business e per le attività dell'azienda o ente è fondamentale sia per l'analisi dei rischi sia per la progettazione delle misure di sicurezza più robuste che a tali applicazioni vanno riservati.

Come mostrato in fig. 5-1, la classificazione della criticità dei dati e delle applicazioni che li trattano è svolta da circa il 70% dei rispondenti, e una così alta % indica che il campione emerso di rispondenti è nella fascia di aziende/enti virtuose/i in termini di misure ed approcci metodologici alla sicurezza digitale. Di questo 70% solo il 26,7% effettua la classificazione su tutto il parco applicativo, mentre il 43,3% effettua la classificazione solo per le applicazioni più critiche, in primis per quelle che trattano dati sensibili: significativo in questo caso l'effetto della normativa sulla privacy in Italia, normativa ora rafforzata e resa più severa dal nuovo regolamento europeo GDPR, General Data Protection Regulation.

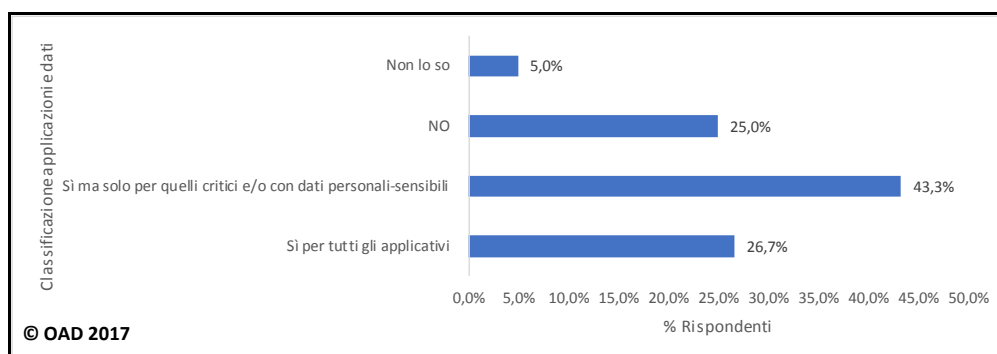


Fig. 5-1 Classificazione delle applicazioni per la criticità dei dati trattati

In §4.2 si è evidenziata l'importanza dell'autenticazione e del controllo degli accessi sicuri, e di una loro gestione sicura: una prima risposta a questa esigenza è la centralizzazione del sistema di autenticazione e controllo degli accessi.

La fig. 5-2 mostra come solo una relativamente piccola frazione dei rispondenti, quasi il 16%, non ha un unico sistema centralizzato, mentre il rimanente ha la centralizzazione, o per tutti gli applicativi o solo per una parte. Per meglio comprendere le risposte avute, si deve considerare che taluni sistemi informatici possono avere più sistemi di autenticazione, ad esempio uno per ogni dominio relativo ad ogni società del gruppo (grandi aziende multinazionali) o all'area geografica di pertinenza.

⁷ Regulation (EU) 2016/679

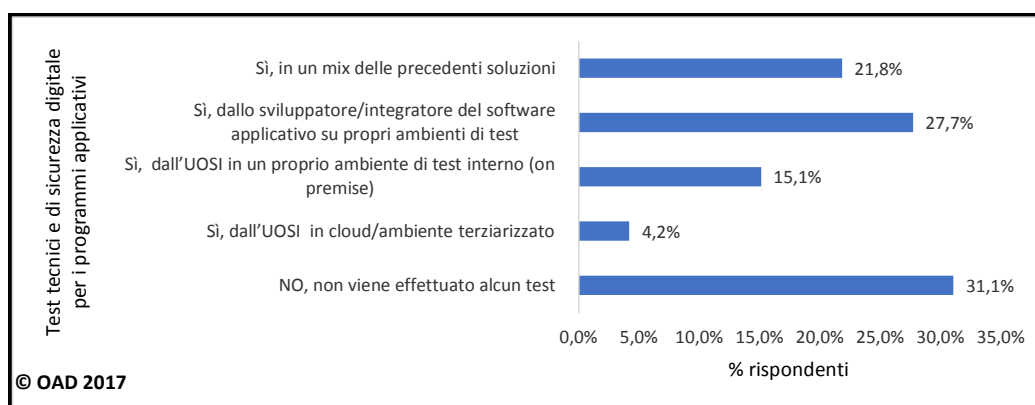


Fig. 5-2 Centralizzazione dei sistemi di identificazione, autenticazione e controllo degli accessi

Per la verifica della sicurezza dell'applicativo, sia sviluppato ad hoc sia acquisito con pacchetti commerciali, è fondamentale effettuare dei test tecnici, che includano test sulla sicurezza digitale del codice, e non solo funzionali: test che debbono essere effettuati prima di mettere in produzione il nuovo software sviluppato/comperato.

Di norma, per software applicativo sviluppato ad hoc, si fanno dei test per verificarne le funzionalità e la corrispondenza con le specifiche funzionali del committente. Sovente non vengono contemporaneamente testati gli aspetti tecnici e della sicurezza dell'applicativo, e non vengono pertanto scoperte e corrette sue eventuali vulnerabilità e difetti.

Per indagare su questi aspetti, nel questionario sono state inserite due distinte domande, una sull'effettuazione di test tecnici che includono i test sulla sua sicurezza, ed una sui test funzionali.

Le risposte raccolte sono mostrate nelle fig. 5-3 e 5-4 seguenti, nelle quali l'acronimo UOSI, Unità Organizzativa Sistemi Informatici, rappresenta la struttura interna all'azienda/ente che ha la responsabilità e gestisce il sistema informatico.

Dal confronto delle due figure emerge come si effettuino più test funzionali rispetto a quelli tecnici e sulla sicurezza del codice, ma non di molto: la differenza è di circa 12 punti %. L'autore, sulla base della sua diretta esperienza in campo, si sarebbe aspettato un maggior divario: questo dato è un'ulteriore conferma che i rispondenti appartengono ad aziende/enti di fascia alta per quanto riguarda la sicurezza digitale e la sua gestione.

Entrambe le figure mostrano come circa un terzo dei rispondenti faccia effettuare i test dagli sviluppatori: il valore è più alto per i test funzionali con un 36,7% mentre è più basso per i test tecnici, con un 27,7%.

L'effettuazione di test su ambienti dedicati all'interno dell'UOSI ha percentuali simili in entrambi i casi, ed è così anche per l'uso di ambienti di test in cloud da parte UOSI. In entrambi i casi le percentuali emerse sono basse, 4,2 e 5%, ed indicano come l'adozione di soluzioni cloud in Italia sia ancora limitata. Eppure l'IaaS⁸ e/o il PaaS⁹ in cloud sono ambienti ideali ed altamente sicuri (almeno con buoni provider) per lo sviluppo ed il test di software. Questi valori sono uno dei tanti indicatori che spiegano l'arretratezza digitale dell'Italia (si veda anche fig. 5-7), e sono più gravi se si considera che il campione di rispondenti emerso appartiene in prevalenza ad aziende del settore ICT.

⁸ IaaS, Infrastructure as a Service

⁹ PaaS, Platform as a Service

Quasi il 20% dei rispondenti dichiara di non effettuare alcun test funzionale, ed il 31% di non effettuare test tecnici e di sicurezza sulle applicazioni che mette in produzione.

Questo significa che l'azienda/ente cliente si fida, in termini funzionali e tecnici-di sicurezza, dei prodotti che acquisisce, e probabilmente non ha né le competenze né il tempo per effettuarli. E' il caso tipico delle piccolissime, piccole e medie aziende (ed enti, si pensi ai piccoli comuni) che costituiscono la stragrande maggioranza delle imprese/enti in Italia: per esse l'ICT è una "commodity" (analogamente all'energia elettrica, alla fornitura di gas e di acqua), con soluzioni standard e da acquisire soprattutto in base al prezzo, e da utilizzare, come le altri utility, in una logica "plug and play": compro, attivo/installo ed uso.

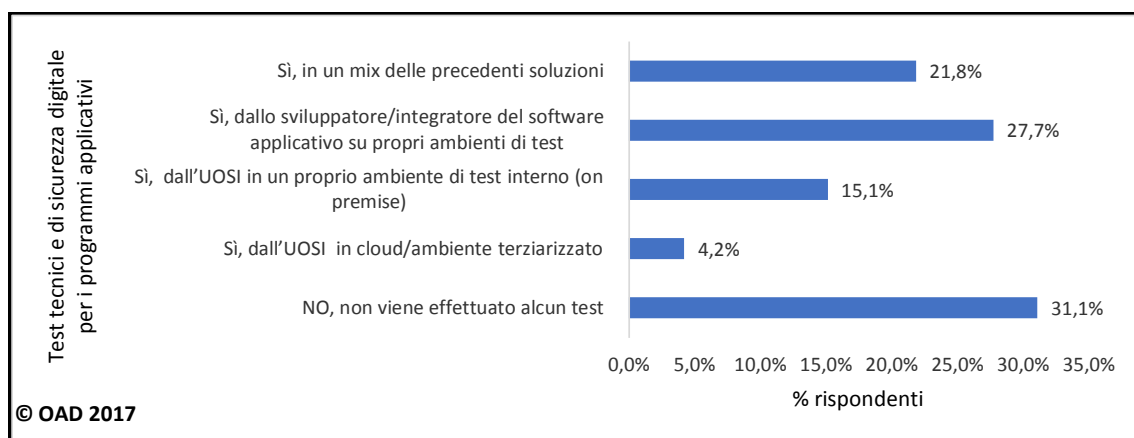


Fig. 5-3 Utilizzo di test tecnici e sulla sicurezza digitale per i programmi applicativi prima di metterli in produzione (risposte multiple)

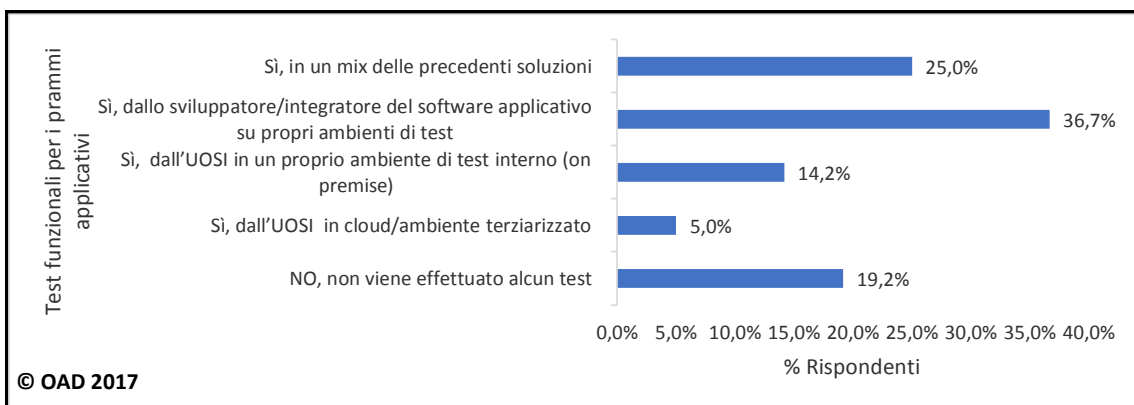


Fig. 5-4 Utilizzo di test funzionali per i programmi applicativi prima di metterli in produzione (risposte multiple)

Ma l'informatica non è ancora assimilabile ad una utility, e forse non lo potrà mai essere: estremamente dinamica ed innovativa, complessa, con un'infinità di standard, con obsolescenza (tecnologica) dei prodotti in tempi brevi (due-tre anni solari), con una miriade di fornitori-venditori per lo stesso prodotto-servizio, tra i quali è difficile scegliere anche per gli addetti ai lavori. Tutto questo disorienta il decisore con poche o nulle competenze informatiche, che non può che fidarsi dei venditori e dei fornitori, consulenti inclusi, che conosce direttamente o con un passa parola da colleghi di altre aziende/enti; ed il decisore sovente non conosce nemmeno criteri e logiche con le quali valutare e scegliere, al di là del prezzo. Ma il prezzo più basso, soprattutto per la sicurezza digitale, quasi mai è il solo criterio corretto e vincente da seguire.

Sia in produzione sia in ambienti di pre-produzione e/o negli ambienti di test, è opportuno che vengano effettuati dei penetration test sugli applicativi per verificare la tenuta delle misure di sicurezza.

La fig. 5-5 mostra le risposte raccolte. Circa il 40% non effettua tali prove, nel caso di PMI, Piccole e Medie Imprese, e di piccolissime strutture molto probabilmente per le ragioni sopra evidenziate di ICT come commodity. A tali motivazioni si aggiunge il timore di effettuare test di attacco che possano recare danno agli applicativi e soprattutto ai dati trattati, che sono l'effettivo "bene" di una organizzazione. Opportune tecniche consentono di ovviare a questo timore, ma non tutti le conoscono o le sanno usare.

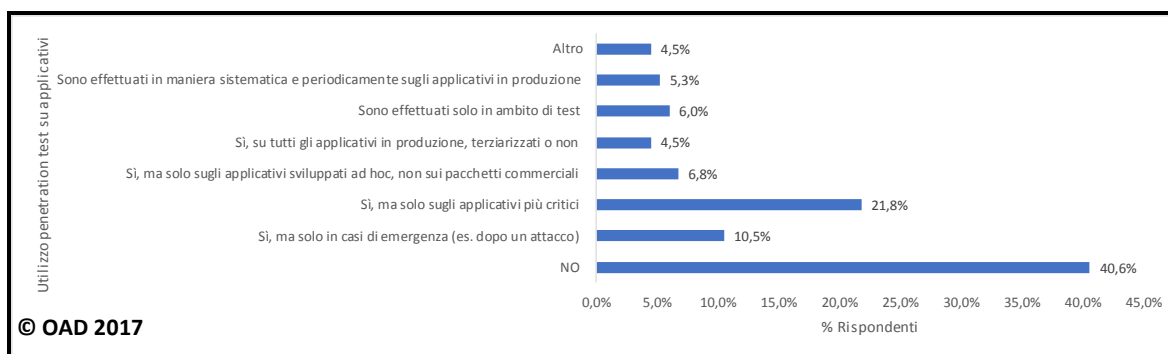


Fig. 5-5 Uso di "penetration test"

Si noti che poco più del 40% dei rispondenti non effettua penetration test ed il 10% li effettua solo in caso di emergenza, tipicamente sotto o dopo un attacco: in altri termini quando i buoi sono usciti dalla stalla, probabilmente solo per azioni legali e di computer forensic.

I dati raccolti sulle misure di sicurezza nel Rapporto OAD 2016 sono mostrati nella fig. 5-6 con risposte multiple: essi indicano con un complessivo 16,8%, al penultimo posto, le misure analizzate in dettaglio nelle fig. 5.5, 4 e 3.

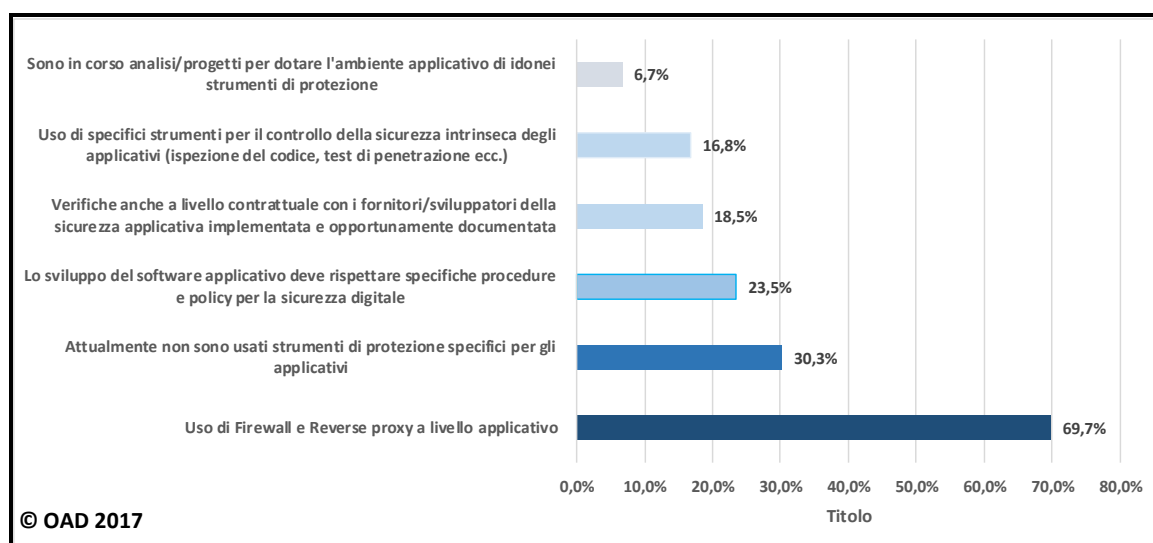


Fig. 5-6 Misure di sicurezza applicativa dal Rapporto 2016 OAD (risposte multiple)

Il 30% di quei rispondenti non sono ancora dotati di misure di sicurezza per gli applicativi, e la misura più diffusa è l'uso di firewall applicativi, attuata da quasi il 70% dei rispondenti.

Questo dato, insieme ad altri emersi dal Rapporto OAD 2016 cui si rimanda, è un significativo indicatore dell'importanza e della necessità di approcciare le misure di sicurezza digitali in una logica architetturale e ben bilanciata: per approfondimenti sull'argomento si rimanda al libro "Sicurezza Digitale" dell'autore ¹⁰.

Altre misure per la sicurezza degli applicativi della fig. 5-6 riguardano le specifiche tecniche ed i contratti con gli sviluppatori di software, perché producano codici sicuri. Le percentuali emerse non sono affatto trascurabili, ma relativamente basse considerando che la stragrande maggioranza di software o è un prodotto commerciale acquisito o è sviluppato ad hoc da aziende specializzate: ed indicano che di fatto circa $\frac{3}{4}$ del campione si fida "ad occhi chiusi" di quanto fanno i fornitori e di come lo fanno, anche perché in molti casi, e tipicamente per le PMI non del settore ICT, non hanno le competenze (e talvolta il tempo e la voglia) di specificare e di controllare poi le misure di sicurezza digitali necessarie.

La scarsa cultura informatica (in media) nelle persone al vertice di aziende/enti italiani è uno (non l'unico) dei problemi che confinano l'Italia agli ultimi posti nelle classifiche mondiali, quali ad esempio la classifica secondo l'indice DESI di digitalizzazione dell'economia e della società, riportata per il 2017 nella fig. 5-7 (si veda <https://ec.europa.eu/digital-single-market/desi>).

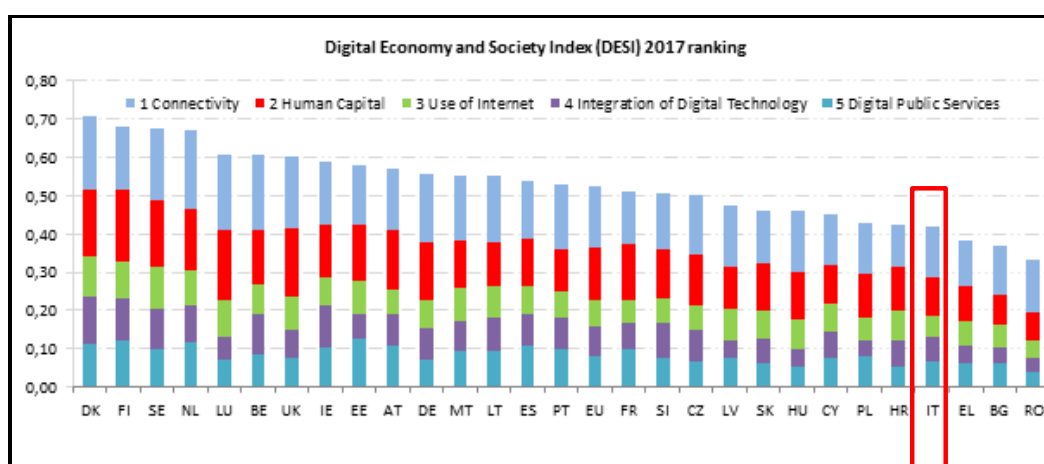


Fig. 5-7 Classifica europea indice DESI (Fonte: Comunità Europea)

Formazione e sensibilizzazione sul tema della digitalizzazione e della sicurezza digitale, non solo per i tecnici ma anche per i decisori sul tema e per chi ne è coinvolto direttamente o indirettamente, ad esempio per taluni avvocati, magistrati e commercialisti, sono attività che devono essere svolte molto più frequentemente e diffusamente a tutti i livelli. Solo così si potrà gradualmente diffondere una cultura della sicurezza digitale, e così migliorare il livello di sicurezza dei sistemi informatici italiani.

AIPSI da sempre sta operando in tal senso con un insieme di eventi: i prossimi per il 2017 sono elencati ed aggiornati sulla pagina web: <http://www.aipsi.org/eventi/calendario-eventi-2017.html>

¹⁰ M. R. A. Bozzetti, F. Zambon: "Sicurezza Digitale- una guida per governare un sistema informatico sicuro", Giugno 2013, Soiel International Editore, ISBN 9788890890109

6. Gli impatti di un attacco digitale ad un applicativo

Il vero problema di un attacco per un'azienda/ente è il danno che può causare. Le misure di sicurezza, oltre che prevenire e contrastare i possibili attacchi, hanno il compito di ridurre l'impatto che l'attacco può causare, a livello funzionale e prestazionale dei sistemi ICT, a livello economico e legale, di immagine e di reputazione. L'importanza di tale fattore è al centro dei questionari e dei rapporti OAD: nell'ultima indagine annuale, quella del 2016, è stato richiesto, a seguito degli attacchi subiti, quali impatti hanno avuto, se poco o molto significativi. Per non appesantire il questionario, non si è voluto dettagliare il tipo di impatto, lasciando al compilatore la libertà di rispondere considerando qualitativamente l'intera valenza del termine "impatto" per la sua azienda/ente. Rimandando per i dettagli al Rapporto 2016, il dato complessivo emerso è che, fatto 100 il numero complessivo di attacchi, solo il 14,6% del totale li ha considerati molto significativi: e questo considerando tutti i diversi tipi di attacco.

Con la presente indagine verticale, la focalizzazione è sugli impatti degli attacchi agli applicativi, considerando come indicatore di riferimento della gravità dell'impatto il tempo richiesto per ripristinare la situazione ex ante dell'applicativo dopo che ha subito l'attacco ritenuto più grave e critico, ossia nella presunta condizione peggiore. Le risposte emerse sono riportate nella fig. 6-1.

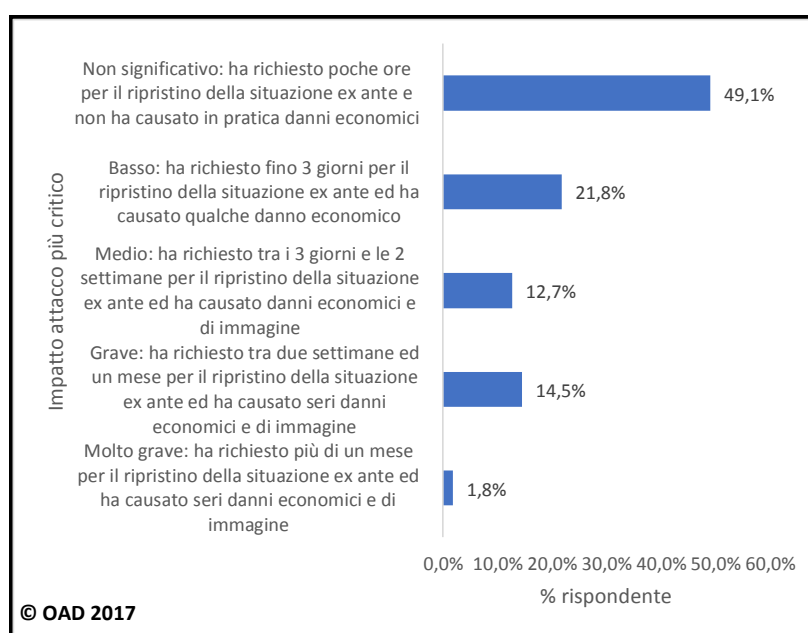


Fig. 6-1 L'impatto dell'attacco più grave e critico all'applicativo

Tra quelli che hanno subito attacchi agli applicativi, poco meno della metà dei rispondenti, la maggior parte (49,1%) è riuscita a ripristinare l'applicativo dopo l'attacco peggiore entro poche ore nel giorno stesso, e il 34,5% ha ripristinato l'applicativo entro due settimane. Tempi di ripristino tra 2 settimane ed un mese solare (sempre per l'attacco considerato più grave tra quelli occorsi nell'anno) riguardano il 14,5% dei rispondenti: una percentuale non piccola, anche se riguarda il peggior attacco subito, e che conferma come alcuni attacchi riusciti abbiano conseguenze veramente pesanti sull'azienda/ente che li subisce. Criticità ulteriormente confermata dai pochi, 1,8%, che hanno impiegato più di un mese a ripristinare.

I dati della fig. 6-1, confrontati con gli analoghi dati del Rapporto OAD 2016 che riguardano però tutti i tipi di attacchi (non solo quelli agli applicativi), confermano che taluni attacchi agli applicativi nel 2016 hanno avuto

impatti più gravi di quelli rilevati (dal campione dei rispondenti) nel 2015: allora non ci fu nessun ripristino che richiedesse più di un mese.

Gli altri dati sugli impatti del Rapporto OAD 2016, pur facendo riferimento a tutti i tipi di attacco e basati su un campione in parte diverso, sono logicamente congruenti con quelli emersi per gli attacchi agli applicativi: nel 44% dei casi la situazione “ante” è ripristinata in meno di un giorno e, complessivamente, in quasi l'80% dei casi, la situazione ex ante riprende entro 3 giorni dall'attacco.

Questi tempi per il ripristino indicano che, da un lato, gli strumenti di prevenzione, protezione e ripristino usati sono sufficientemente diffusi ed efficaci, dall'altro che la maggior parte degli attacchi, almeno per il campione della presente indagine, non ha serie conseguenze. L'indagine conferma ulteriormente che gli attacchi seri con forti impatti sono prevalentemente portati ai sistemi informatici ed agli applicativi di grandi strutture, dove il ritorno per il cyber criminale può essere significativo, in termini sia economici sia mediatici. E nell'Italia con milioni di piccole e piccolissime aziende l'attrattiva per un attaccante si limita a poche migliaia di aziende o enti pubblici di grandi dimensioni e con marchi conosciuti a livello mondiale. E queste grandi strutture hanno normalmente un livello di sicurezza digitale adeguato.

7. Il campione emerso dall'indagine

Le risposte avute sono state 173, un numero di risposte basso rispetto alle aspettative ma comunque sufficiente a fornire delle concrete indicazioni sugli attacchi agli applicativi dei sistemi informatici in Italia.

Come illustrato nel seguente §7.1, il campione emerso è molto simile a quello del Rapporto OAD 2016, sia per ruolo dei rispondenti, sia per dimensioni di aziende/enti, sia per settore merceologico.

7.1 Chi ha risposto: ruolo e settore merceologico

Come per il Rapporto OAD 2016, la quota maggiore di rispondenti è responsabile del sistema informatico e della struttura interna che lo supporta, indicata come UOSI, Unità Organizzativa Sistema Informatica: il CIO, Chief Information Officer, per le medio-grandi organizzazioni, l'Amministratore di sistema per quelle piccole, dove normalmente non esiste nemmeno una minima struttura UOSI, e l'Amministratore di sistema, se c'è, opera in questo ruolo talvolta a tempo parziale.

Significativo che, come per il Rapporto 2016, al secondo posto risultano come rispondenti le persone al vertice di aziende, per lo più di piccole e piccolissime dimensioni. Sono loro infatti i decisori sull'informatica e la digitalizzazione per le loro aziende. Il ruolo di responsabile della sicurezza digitale, il CISO, Chief Information Security Officer), ha ancora una limitata diffusione in Italia: è definito ed operativo in medie e grandi strutture, ed infatti solo 6.8% dei rispondenti si è qualificato con tale ruolo. Nella presente indagine il CISO è superato in percentuale dal responsabile delle tecnologie, il CTO, Chief Technology Officer, che in alcune grandi manifatturiere include nella propria struttura organizzativa anche il CIO e l'UOSI.

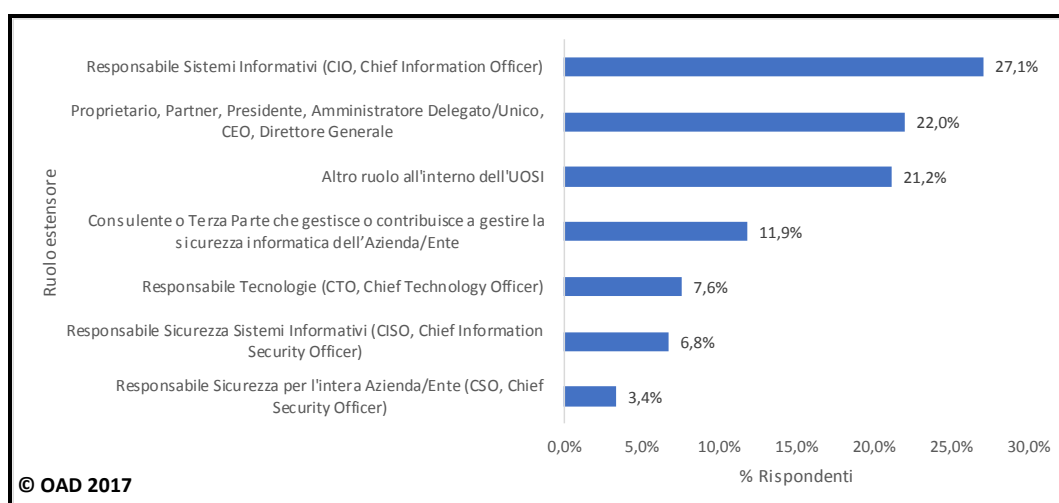


Fig. 7-1 Ripartizione % dei rispondenti per ruolo svolto nell'azienda/ente

Pure per dimensioni dell'azienda/ente, indicata come numero di dipendenti, il campione emerso è molto simile a quello del Rapporto OAD 2016, e risulta abbastanza ben bilanciato rispetto alla realtà italiana, con quasi la metà dei rispondenti appartenente ad aziende/enti con meno di 50 dipendenti, più di ¼ ad aziende/enti tra 51 e 250 dipendenti (250 è il numero massimo di dipendenti per una PMI), il restante ad aziende/enti di grandi dimensioni, a loro volta suddivise in tre fasce: un 16% ad aziende/enti tra i 251 ed i 1000 dipendenti, e poco più del 6% a testa tra quelle che hanno tra i 1000 ed i 5000 dipendenti, e quelle che superano tale numero.

Le percentuali emerse non sono ovviamente proporzionali al numero di aziende esistenti in Italia per numero di dipendenti, dato che le più recenti indagini CGIA di Mestre su dati Infocamere – Movimprese del 2012 (gli analoghi ultimi dati ISTAT pubblici risalgono ad un anno prima) evidenziano che:

- le aziende fino a 49 addetti risultavano essere 5.246.179;
- quelle da 50 fino a 249 risultavano 25.359;
- quelle oltre i 250 risultavano 3.977.

Non considerando le Pubbliche Amministrazioni centrali e locali, le PMI a quella data erano circa 5,5 milioni, contro circa 4.000 aziende grandi e grandissime. E tra le PMI la stragrande maggioranza è di aziende sotto i 5 dipendenti: una nazione, l'Italia, di "nano" imprese, che ben difficilmente può competere a livello internazionale, e purtroppo non solo sul fronte digitale.

Come più volte ripetuto, la ripartizione dei rispondenti non è statisticamente significativa, ma copre in maniera ben bilanciata aziende/enti di varie dimensioni, fornendo così dati utili per gli obiettivi dell'indagine.

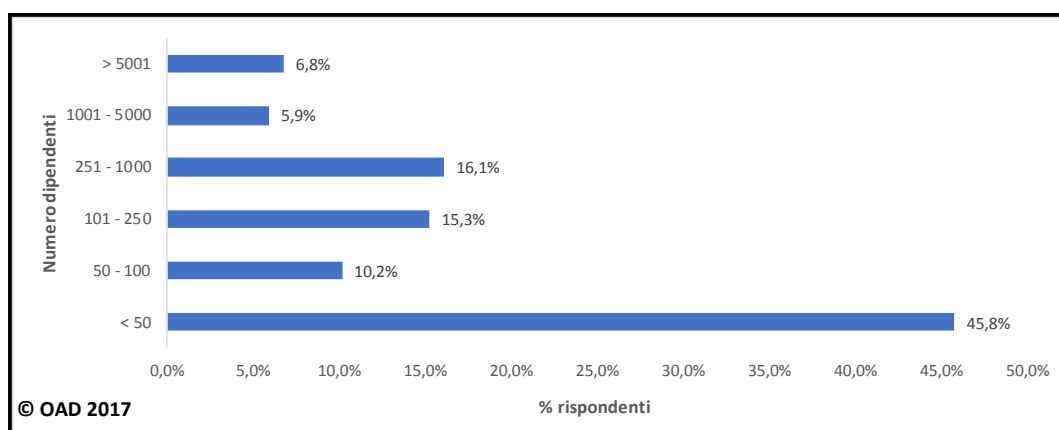


Fig. 7-2 Ripartizione % dei rispondenti per dimensione d'azienda

La fig. 7-3 mostra la distribuzione dei rispondenti per settore merceologico, secondo la classificazione ATECO riportata nella tabella di fig. 7-4.

Il campione emerso, così come quello del Rapporto 2016, risulta fortemente concentrato su aziende dei servizi ICT, su aziende manifatturiere, e su aziende di servizi professionali. Tutti gli altri settori merceologici sono coperti, ma con un numero di aziende/enti troppo basso perché le loro risposte possano essere rappresentative (anche non in logica strettamente statistica) dei settori di appartenenza. Forniscono comunque delle indicazioni interessanti per l'inquadramento del fenomeno degli attacchi alle applicazioni, ma, dato il loro piccolo numero, non si ritiene significativo elaborare ed analizzare ripartizione e cause degli attacchi per settore merceologico. L'indagine risulta pertanto più significativa per alcuni settori, meno per altri. Sarà compito di AIPSI e di Malabo effettuare ulteriori sforzi nelle prossime indagini per aumentare il numero di rispondenti per i settori merceologici ora meno rappresentati, pur conoscendo le difficoltà di ottenere risposte, pur anonime, su argomenti delicati come l'aver subito attacchi digitali.

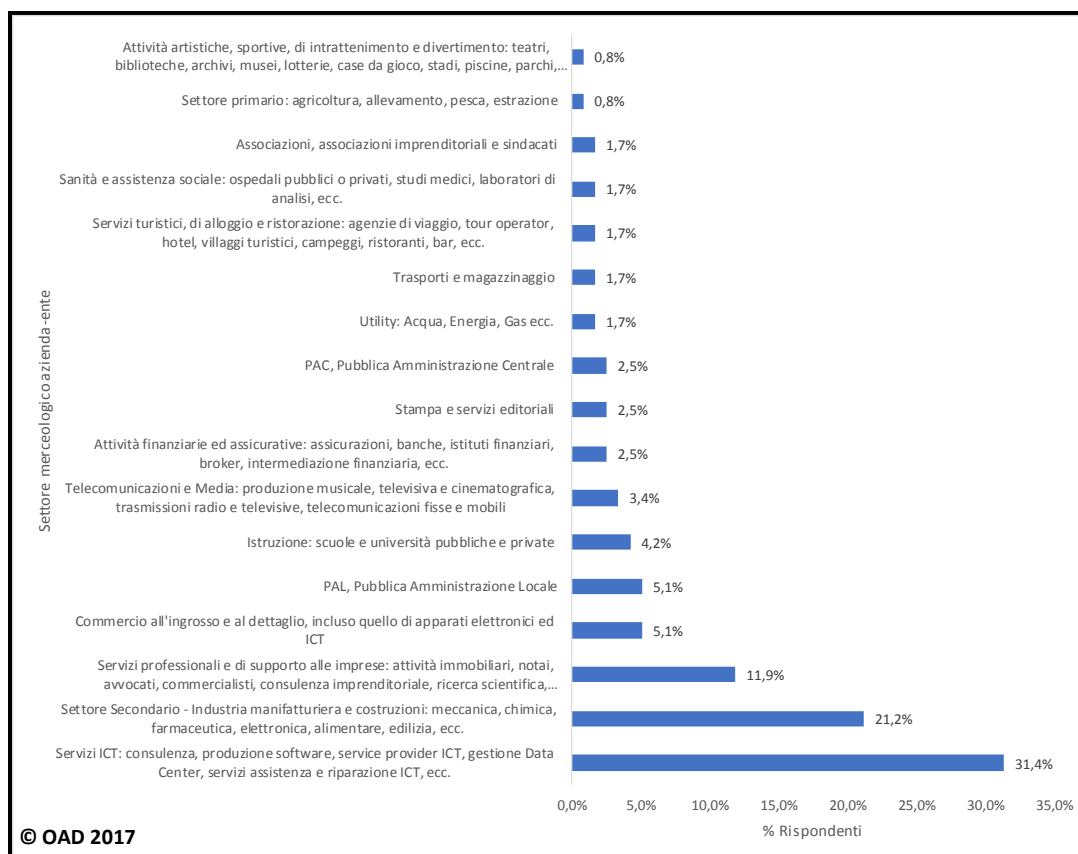


Fig. 7-3 Ripartizione % dei rispondenti della presente indagine per settore merceologico

1. Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B)
2. Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
3. Utility: Acqua, Energia, Gas ecc. (Codici Ateco D ed E)
4. Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
5. Trasporti e magazzinaggio (Codice Ateco H)
6. Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, ecc. (Codice Ateco M)
7. Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, ecc. (Codice Ateco I e N79)
8. Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, ecc (Codice Ateco R)
9. Stampa e servizi editoriali (Codice Ateco J58)
10. Servizi professionali e di supporto alle imprese: attività immobiliari, notai, avvocati, commercialisti, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, ecc. (Codici Ateco L, M, N77, N78, N80, N81, N82)
11. Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, ecc. (Codici Ateco J62, J63, S95.1)
12. Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
13. Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, ecc. (Codice Ateco Q)
14. Istruzione: scuole e università pubbliche e private (Codice Ateco P)
15. Associazioni, associazioni imprenditoriali e sindacati (Codice Ateco S94)
16. PAC, Pubblica Amministrazione Centrale
17. PAL, Pubblica Amministrazione Locale

Fig. 7-4 I settori merceologici ATECO considerati nei questionari delle indagini OAD

7.2 L'ambiente applicativo dei sistemi informatici dei rispondenti

Come già evidenziato in §1 e in §A.1, per poter velocizzare e facilitare le risposte al questionario si sono poste solo 2 domande sull'ambito applicativo dei rispondenti, nell'ottica di considerare (in modo puramente indicativo) le caratteristiche tecniche dei sistemi informatici dei rispondenti rilevate nell'indagine annuale del 2016, e per le quali si rimanda al Rapporto OAD 2016.

La prima domanda della presente indagine fa riferimento al numero di applicativi complessivi del sistema informatico, numero che fornisce un sintetico indicatore della potenziale area di attacco.

La fig. 7-5 sintetizza in % le risposte ricevute: più della metà dei sistemi informatici dei rispondenti utilizza un numero limitato di applicazioni, fino a 20, tipico per le organizzazioni piccole e piccolissime, ed un non trascurabile 15,6% ha più di 100 applicazioni, prevalentemente di medie-grandi organizzazioni.

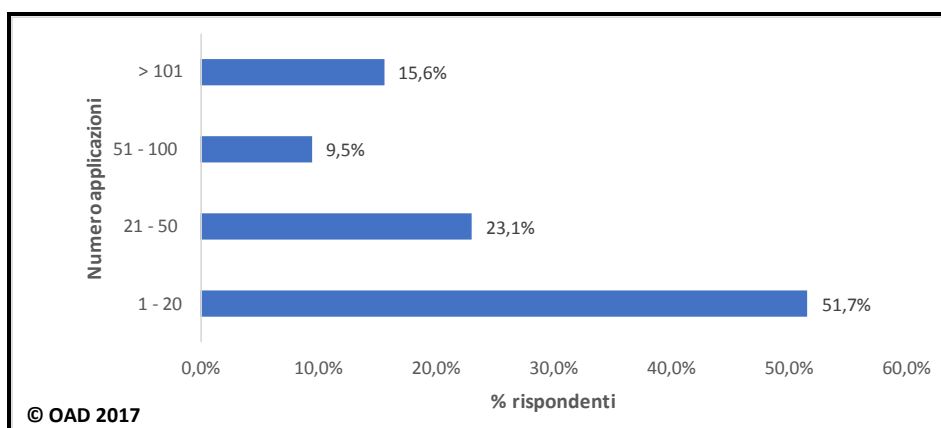


Fig. 7-5 Numero degli applicativi del Sistema Informatico dei rispondenti

La seconda domanda fa riferimento a quanti degli applicativi utilizzati siano in cloud, sia usando IaaS, ossia applicativi dell'azienda/ente operanti in produzione su infrastrutture in cloud, sia direttamente come SaaS¹¹, ossia applicativi erogati come servizi dal fornitore in cloud.

La fig. 7-6 mostra le risposte: la quasi totalità delle aziende/enti utilizza almeno qualche (fino a 10) applicativo in cloud, tipicamente alcuni social network o specifiche applicazioni come posta elettronica, siti web, piattaforme collaborative, e-commerce, ecc.

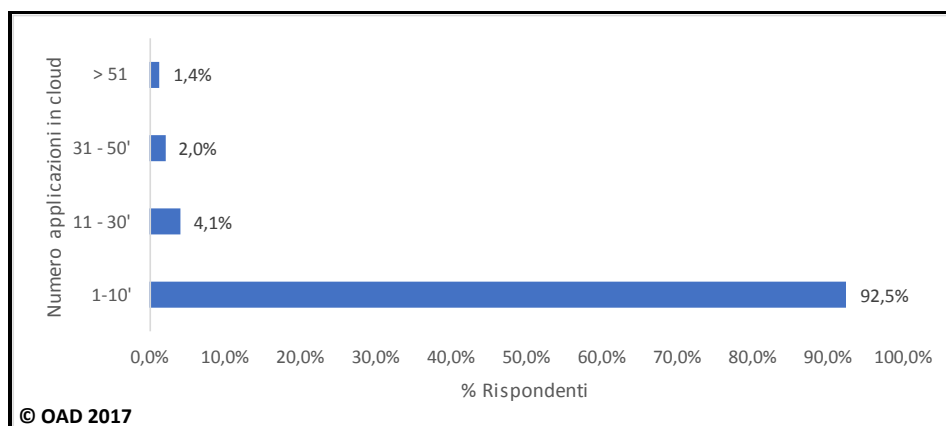


Fig. 7-6 Numero di applicativi in cloud

¹¹ SaaS, Software as a Service

8. Prime considerazioni sui dati emersi dall'indagine

Numerose analisi e considerazioni possono essere effettuate sui dati emersi dalla presente indagine, soprattutto correlandoli tra loro e, almeno come indicazioni di massa, con i dati del Rapporto OAD 2016.

Nel seguito sono riportate le principali considerazioni emerse da una prima analisi dei dati raccolti.

- **Il contesto: tipologia dei rispondenti e dei loro sistemi informatici**
 - così come per il Rapporto 2016, le aziende dei rispondenti appartengono in maggior parte a 3 settori merceologici: servizi ICT, manifatturiero, servizi professionali alle imprese; tutti gli altri settori ATECO considerati hanno avuto dei rispondenti, ma in numero limitato. La ripartizione per dimensioni come numero di dipendenti è ben bilanciata tra piccole, medie grandi e grandissime strutture. Il ruolo dei rispondenti è prevalentemente quello di Responsabile/Amministratore del sistema informatico e di responsabile di vertice dell'azienda/ente, soprattutto per quelle più piccole;
 - il numero totale di applicativi nel sistema informatico dipende dalle dimensioni e dal tipo di azienda: poco più della metà ha fino a 20 applicazioni, tipicamente le PMI, le grandi e grandissime aziende/enti ne hanno anche più di 100;
 - quasi tutti i rispondenti hanno applicazioni in produzione in cloud, ma solo pochi usano il cloud per i test alle applicazioni, sia funzionali sia tecnici.
- **Vulnerabilità degli applicativi:** innumerevoli sono i tipi di vulnerabilità, sfruttabili e sfruttati dagli attaccanti, dai bachi nel codice dovuti ad una programmazione non sicura al non settaggio dei parametri di sicurezza nelle configurazioni. Il grande numero di vulnerabilità degli applicativi e dei software che utilizzano, dai sistemi operativi al middleware, rende complessa e difficile l'analisi dei rischi (pratica ancora limitata ed effettuata prevalentemente da grandi aziende/enti) e la progettazione e realizzazione di efficaci ed efficienti misure di sicurezza, ma rende più facile portare attacchi agli applicativi con impatti sul business anche molto gravi.
- **Attacchi agli applicativi e relativi impatti:** poco meno della metà dei rispondenti, 46,9%, ha subito e rilevato attacchi agli applicativi, confermando che questo è uno dei principali problemi della sicurezza digitale (insieme al comportamento degli utenti). Gli impatti dell'attacco peggiore subito nell'anno, misurato dal tempo necessario per ripristinare l'applicazione, sono stati nella maggior parte dei casi non gravi e l'applicazione e i suoi dati sono ripristinati in poche ore: ma per un significativo 14,5% dei rispondenti è occorso fino ad un mese solare per ripristinarla e per un piccolo, ma non trascurabile, 1,8%, più di un mese. Si rileva quindi che nel 2016 alcuni degli attacchi agli applicativi sono stati i più critici e difficili da ripristinare rispetto a tutti gli attacchi, non solo agli applicativi, occorsi nel 2015 ai rispondenti alle indagini OAD.
- **Principali cause degli attacchi agli applicativi:** dall'indagine è emerso che la causa più rilevante e diffusa è dovuta alle vulnerabilità dei software e delle infrastrutture usati dall'applicazione (36,2% nel 2016); al secondo posto la vulnerabilità intrinseca dell'applicativo stesso (25,4% nel 2016), dovuta allo sviluppo del codice in maniera non sicuro e/o con linguaggi non sicuri; seguono come causa le vulnerabilità dei sistemi di identificazione, autenticazione e controllo degli accessi (20,8% nel 2016).
- **Misure di sicurezza in essere per gli ambienti applicativi dei rispondenti:** i sistemi informatici dei rispondenti appartengono in gran parte alla fascia alta per le misure di sicurezza, grazie anche al fatto che molti sono di aziende di servizi ICT, e chi quindi hanno (o dovrebbero avere) sistemi informatici e relativa sicurezza allo stato ultimo dell'arte (ma anche tra le aziende ICT ci sono casi di "ciabattino con le scarpe rotte"). Il 70% dei rispondenti classifica dati ed applicazioni; più dell'84% gestisce in maniera centralizzata l'autenticazione ed il controllo degli accessi; prima di passare un'applicazione in produzione, l'80% effettua test funzionali e quasi il 69% test tecnici e sulla sicurezza del codice; quasi il 55% effettua penetration test.

In conclusione, pur su un campione emerso di aziende/enti che in gran parte ben conosce e gestisce la sicu-

rezza digitale, la difesa degli applicativi risulta sempre più difficile e complessa, viste anche le innumerevoli vulnerabilità cui gli applicativi possono essere soggetti.

Attacchi alle applicazioni, quando riescono, posso avere impatti devastanti in termini di continuità operativa, di perdite economiche e di immagine-reputazione, di aspetti legali, e così via. Le applicazioni trattano i dati, che costituiscono il bene più prezioso dell'azienda/ente nell'attuale epoca digitale: attacchi alle applicazioni implicano attacchi ai dati che esse trattano, per rubarli, manipolarli, cancellarli, con tutti i danni che così si possono causare all'azienda/ente.

Il grandissimo numero di piccole e piccolissime imprese, ed anche di piccole amministrazioni pubbliche, che caratterizza l'Italia e la sua economia riduce fortemente l'attrattiva per cyber criminali, soprattutto per attacchi alle singole aziende/enti di piccole dimensioni. Per queste ultime rimane potenzialmente assai critico (a parte attacchi tipo ransomware e ricatti informatici efficaci per chi non ha le minime misure di sicurezza) un eventuale attacco di massa, capace di coinvolgere centinaia di migliaia di soggetti, e che sconfina più nel cyber terrorismo (anche di valenza politica) e nella guerra informatica. Per identici motivi anche le Pubbliche Amministrazioni, piccole o grandi, locali o centrali, sono un target appetibile. Un simile attacco, paralizzando contemporaneamente buona parte delle attività delle PMI, potrebbe veramente mettere in ginocchio l'economia italiana.

La criminalità informatica, prevalentemente internazionale, ha come obiettivi frodi e guadagni economici-finanziari, e il suo target principale, per l'Italia, è il sotto-insieme più appetibile delle quasi 4000 imprese di medie e grandi dimensioni: ed un'area d'attacco è proprio l'ambito applicativo con tutte le sue vulnerabilità dirette ed indirette.

Un'ultima considerazione riguardo alla consapevolezza sui rischi informatici e sulla sicurezza emersa, seppur in maniera indiretta, dalle risposte raccolte: questa consapevolezza è carente e/o insufficiente, ed in particolare per le persone di vertice delle aziende/enti. La sicurezza digitale non è solo un problema tecnico ed organizzativo: è un problema di business nel quale deve essere coinvolta l'intera struttura organizzativa, dal vertice, che deve prendere le idonee decisioni in merito, a tutti i livelli e a tutti i ruoli delle persone che devono utilizzare gli strumenti informatici in maniera sicura, operando ormai in un mondo digitale e per questo sempre più soggetto ad attacchi.

Allegati

A.1 Aspetti metodologici dell'indagine

Il presente "Rapporto OAD 2017 sugli attacchi agli applicativi" si basa sull'elaborazione delle risposte al questionario online ricevute dai rispondenti la cui tipologia è descritta in §7.

AIPSI, il suo Media Partner Reportec, l'azienda dell'autore Malabo Srl, i Patrocinatori hanno invitato, con specifiche pagine sui loro siti web e con messaggi di posta elettronica, a compilare il questionario dell'attuale edizione tutte le persone con i profili sopra elencati delle loro "mailing list" sia lato domanda sia lato offerta ICT. Sono stati inoltre sollecitati i partecipanti a vari "social network" inerenti l'ICT e la sicurezza digitale.

Il Questionario è rimasto accessibile on line via web da fine 2016 al primo trimestre 2017, e in questo arco temporale i potenziali rispondenti hanno ricevuto vari inviti e solleciti a compilare le 14 domande del questionario on line con risposte predefinite tra cui scegliere.

Nel complesso il numero delle persone contattate si è aggirato attorno ai tremila, appartenenti ad un ampio insieme di aziende di ogni dimensione e settore merceologico, inclusi enti pubblici centrali e locali. Questa specifica indagine, analogamente a quella annuale, non ha (e non può e non vuole avere) valore strettamente statistico, basandosi su libere risposte via web-Internet da parte di un campione di rispondenti non predefinito che partecipa su base volontaria. Come descritto in §7, il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico sia per dimensione, è comunque significativo e sufficiente per fornire attendibili indicazioni sul fenomeno degli attacchi agli applicativi in Italia e sulle sue tendenze.

Nel presente Rapporto sono ripresi taluni dati, soprattutto sugli ambiti applicativi, emersi dal Rapporto 2016 OAD: i campioni di rispondenti sono diversi, anche per il loro numero, ma dal punto di vista del mix e a livello qualitativo e indicativo sono confrontabili. In tali confronti si deve comunque considerare che, oltre ai campioni diversi, le percentuali variano in funzione del numero di rispondenti, risposta per risposta, e nel caso di risposte multiple.

Il questionario è totalmente anonimo: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene nemmeno specificata la data di compilazione.

Tutti i dati forniti vengono usati solo a fini di analisi complessiva e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente. Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario.

L'Autore, AIPSI, Malabo garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per la presente indagine, la produzione del presente Rapporto e l'eventuale presentazione dei risultati in eventi.

A.2 F5 Networks



F5 Networks offre soluzioni per il mondo applicativo, aiutando le organizzazioni a scalare con semplicità i deployment cloud, i Data Center, le reti di telecomunicazioni e il Software-Defined Networking (SDN), per offrire con successo applicazioni a chiunque, ovunque e in qualunque momento.

Le soluzioni F5 ampliano il raggio d'azione dell'IT attraverso un framework aperto ed estensibile e un ricco ecosistema di partner che include le aziende leader nella tecnologia e nell'orchestrazione.

Le più grandi organizzazioni, i service provider, le amministrazioni pubbliche si affidano a F5 per essere al passo con le tendenze in ambito cloud, security e mobility.

- **Sicurezza delle applicazioni:** F5 aiuta le organizzazioni a ridurre al minimo i rischi e salvaguardare le proprie reti, le applicazioni, le proprietà intellettuali e gli utenti dalle minacce alla sicurezza provenienti sia dall'esterno della rete, sia dagli utenti interni inconsapevoli e da quelli che operano da mobile utilizzando reti pubbliche non protette.
- **Abilitatore del Cloud:** Grazie al supporto delle piattaforme cloud di player come Amazon, VMware e Microsoft, F5 offre la flessibilità che consente alle aziende di adottare il modello d'infrastruttura che meglio risponde alle proprie esigenze.
- **Ottimizzazione delle prestazioni della rete e delle applicazioni:** Le applicazioni enterprise migliori risultano inutili se non sono disponibili, affidabili in grado di offrire le prestazioni che gli utenti si aspettano. F5 comprende la logica applicativa nella sua profondità e utilizza questa conoscenza per ottimizzare le prestazioni della rete e delle applicazioni.
- **Servizi applicativi:** Tutte le applicazioni hanno bisogno di servizi che ne garantiscano la sicurezza, le prestazioni e la disponibilità, ma spesso solo le applicazioni mission-critical ne sono fornite. Con F5 Software-Defined Application Services, non è più necessario scegliere quali applicazioni ottimizzare e proteggere ma è possibile fornire servizi essenziali a tutte le applicazioni ovunque esse risiedano.
- **Tecnologie abilitanti e supporto nel mondo:** Le soluzioni F5 includono una serie di tecnologie di supporto per la visibilità globale sulla rete e sulle applicazioni, la flessibilità e il controllo, che consentono di estendere le operazioni dal Data Center al cloud. Queste tecnologie consentono di distribuire anche a tempi da record le applicazioni aziendali dei principali vendor come IBM, Microsoft, Oracle e VMware, massimizzando il ROI. F5 è nota anche per i suoi servizi di supporto completi, con clienti che indicano come grado di soddisfazione "9 su 10". DevCentral, la comunità tecnica online di F5, conta 240.000 architetti di rete, professionisti della sicurezza, e sviluppatori di applicazioni che supportano i clienti con know-how tecnico necessario sul codice, nelle configurazioni e nelle discussioni tecniche, fornendo white paper, video e articoli a firma.

Per maggiori informazioni, visitate il sito www.f5.com

A.3 AIPSI



AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, è il capitolo italiano di ISSA, l'organizzazione internazionale no-profit di professionisti ed esperti praticanti. Con l'attiva partecipazione dei singoli soci, AIPSI, in qualità di capitolo italiano di ISSA, è parte della più grande associazione non-profit di professionisti della sicurezza che ne vanta oltre 10000 a livello mondiale. L'organizzazione di forum e di seminari di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, la formazione per le certificazioni europee eCF per la sicurezza informatica, oltre all'interazione fra i vari professionisti della sicurezza contribuiscono concretamente ad incrementare le competenze e la crescita professionale dei Soci, oltre che promuovere più in generale la cultura della sicurezza ICT e della sua gestione in Italia. L'appartenenza al contesto internazionale ISSA, permette ai soci AIPSI di interagire con gli altri capitoli europei, americani e del resto del mondo. Il comitato direttivo di AIPSI e di ISSA International è costituito da rappresentanti influenti nell'ambito della sicurezza con rappresentanze che provengono da alcune delle principali aziende della domanda e dell'offerta e da consulenti con competenze anche in ambito legale. ISSA è focalizzata nel mantenere la sua posizione di "Global voice of Information Security".

Benefici per i Soci AIPSI-ISSA

- Ricevimento di ISSA Journal, la rivista mensile di ISSA, e della Rubrica AIPSI nella rivista elettronica mensile Security&Business di Reportec.
- Accesso/ricevimento newsletter di ISSA e newsletter italiana di AIPSI.
- Partecipazione ai webinar ISSA ed a quelli AIPSI (in preparazione).
- Formazione ed aggiornamento continuo sulla sicurezza digitale per l'aggiornamento e la crescita professionale.
- Rappresentanza dei Soci professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate (in preparazione).
- Corsi per le certificazioni professionali per le competenze sulla sicurezza, in particolare per eCF.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Accesso e sconti a seminari, conferenze, training a carattere nazionale e internazionale.
- Possibilità di redigere articoli per conto di AIPSI/ISSA e loro pubblicazione nel sito web AIPSI.
- Pubblicazione e ricerca di curricula vitae per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web di ISSA e di AIPSI.
- Visibilità nazionale ed internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare come oratore a seminari e conferenze per conto di AIPSI/ISSA.

Per maggiori informazioni: www.aipsi.org e www.issa.org

A.4 Profilo dell'Autore



Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è amministratore unico di Malabo Srl, società di consulenza e servizi sull'ICT ed ideatore e curatore di OAD, Osservatorio Attacchi Digitali in Italia. Attraverso la sua società Marco conduce interventi consulenziali lato sia domanda sia offerta ICT ed offre alcuni servizi on line a supporto dei suoi interventi consulenziali. I suoi campi di intervento includono la gestione di progetti informatici di medie grandi dimensioni e complessità, la governance ICT, la sicurezza digitale, il disegno di architetture ICT, la razionalizzazione e la gestione del sistema informativo, la definizione di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto alla compliance alle varie normative, dalla privacy alla safety.

Marco 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 Consulenti di Direzione, oltre ad essere stato il primo responsabile dei sistemi informativi dell'intero Gruppo ENI a livello mondiale.

È stato Presidente e VicePresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.

È attualmente Presidente di AIPSI, nel Consiglio Direttivo di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio del ClubTI di Milano, di AIPSI. È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser".

E' "assessor" e commissario d'esame per le certificazioni eCF.

Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, le architetture ICT, gli scenari e gli impatti dell'ICT.

A.5 Malabo Srl



Malabo Srl opera dal 2001 nell'ambito della consulenza e dell'erogazione di servizi ICT, basandosi su una rete consolidata di esperti "senior" e di società ultra specializzate, per clienti lato sia offerta sia domanda ICT. Malabo dispone di un piccolo laboratorio ICT con il quale può installare e testare qualsiasi tipo di sistema operativo e/o applicativo.

La consulenza

Lato domanda l'intervento principale è di aiutare il cliente nell'uso efficace ed efficiente dell'ICT in modo da creare per lui un effettivo e misurabile valore; lo stesso obiettivo si applica per le aziende dell'offerta ICT, per le quali gli interventi spaziano da quelli per il miglior uso dell'ICT, a quelli più strategici per una reale crescita, per incrementare immagine e guadagni, per meglio posizionarsi sul mercato italiano e internazionale.

Gli interventi sui sistemi informatici includono la loro razionalizzazione, la riduzione dei costi, la gestione operativa, la definizione e gestione dell'ICT Enterprise Architecture anche con terziazioni e cloud, l'ICT governance, la sicurezza digitale, l'analisi e la gestione dei rischi. A livello organizzativo gli interventi includono l'assessment delle competenze e dei ruoli del personale ICT con riferimento agli standard europei EUCIP/eCF ed all'italiano UNI 11506, la riorganizzazione dei processi ICT con intelligente e contestuale riferimento a ITIL e a COBIT, l'effettivo allineamento tra sistema informatico e business, la gestione delle compliance e delle certificazioni.

I servizi

Grazie al cloud e al proprio laboratorio ICT, Malabo è in grado sia di provare software per verificarne funzionalità, facilità d'uso e sicurezza, sia di fornire ai propri Clienti alcuni servizi personalizzati, che sovente derivano dagli interventi consulenziali svolti. Esempi di servizi erogati on line includono:

- SLA Watch per il monitoraggio da remoto delle funzionalità e delle prestazioni di ogni risorsa ICT indirizzabile da Internet; per approfondimenti si veda <http://www.sla-watch.com/>
- ICT Inventory: individua automaticamente tutte le risorse fisiche e logiche ICT, con i loro componenti, di un sistema informativo, creando una banca dati centralizzata (CMDB)
- ICT TT, Trouble Ticketing system: consente la centralizzazione di tutte le segnalazioni e le richieste degli utenti, tracciando puntualmente il loro ciclo di vita e rendendolo visibile a ciascun utente
- GOSI, Gestione Operativa Sistema Informatico: integra i servizi sopra elencati e viene supportata anche da interventi in loco, con una contestuale applicazione delle buone pratiche ITIL e COBIT
- Strumenti di supporto all'analisi dei rischi e dei loro impatti, basati sui più consolidati standard e best practice (ISO 27001-2-5, NIST 800, Octave Allegro)
- Kit autovalutazione del ritorno economico e dell'analisi del valore di un sistema informatico: può essere usato sia a livello di sistemi o di parti di sistemi già in produzione (post) sia a livello di analisi di fattibilità (ante).
- Kit per la stesura guidata del DPS, Documento Programmatico Sicurezza (normativa privacy) e del DVR, Documento Valutazione Rischi per la sicurezza sul lavoro.

Per maggiori informazioni: www.malboadvisoring.it

A.6 Reportec srl



Dal 2002 Reportec è attiva nell'editoria specializzata, in particolare per il settore ICT, realizzando e pubblicando riviste, report, survey, e-magazine, Webinar, video, libri sull'ICT e prodotti personalizzati per aziende.

La redazione, composta da giornalisti professionisti, è anche impegnata nell'alimentare siti Web specializzati con notizie quotidiane pubblicate su www.reportec.it e <https://www.tomshw.it/business/>

Testate di riferimento sono Direction, dal 2003 la rivista per il Cio e i manager aziendali alle prese con i processi di business alimentati dalle tecnologie digitali, e Partners, la rivista per i manager del canale trade ICT.

Security & Business, dal 2005, informa professionisti e manager sulle problematiche relative alla sicurezza informatica e alla protezione dei dati e degli asset aziendali.

Reportec possiede un database con oltre 50mila nominativi di manager di alto livello in aziende end user e operatori di canale di tutte le dimensioni: dalla grande impresa alla medio piccola azienda, su tutto il territorio nazionale e in vari settori. Un database "abituato" a ricevere pubblicazioni di alto spessore e a essere coinvolto in indagini e analisi sul mercato e le tecnologie.

Reportec è in grado di interpretare specifiche esigenze di informazione nel settore dell'Information e Communication Technology professionale, attraverso l'impiego di mezzi funzionali ai bisogni del marketing e adatti anche a soddisfare i nuovi paradigmi di comunicazione multicanale.

Reportec interpreta in un modo nuovo sistemi di comunicazione specifici per il Canale e per coloro che al Canale vogliono fare arrivare il loro messaggio con un approccio innovativo e qualificato.

Nel 2015 Reportec ha costituito una nuova divisione dedicata al mondo agroalimentare, food e beverage, che realizza e pubblica notizie e approfondimenti su www.de-gustare.it, un sito dedicato agli appassionati di enogastronomia e agli addetti al settore, risultando spesso fonte per le stesse agenzie stampa, come ANSA..

Per maggiori informazioni: www.reportec.it

Patrocinatori

