Gli attacchi ai sistemi informatici in Italia: i primi dati raccolti dall'Osservatorio 2009

A cura di

Marco Bozzetti

GeaLab Srl

VP FidaInform, Past President ClubTI

OAI, Osservatorio Attacchi Informatici in Italia

- **Che cosa è**
  - **Indagine annuale sugli attacchi ai Sistemi Informativi di Aziende e Pubbliche Amministrazioni in Italia condotta attraverso un questionario on-line indirizzo a CIO, CISO, CSO ed ai consulenti che si occupano di sicurezza informatica**
- **Chi lo attua**

FIDA INFORM

SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale

- **Con la collaborazione di**

polizia delle comunicazioni

- **I patrocinatori**

aipsa Associazione Italiana Professionisti Security Aziendale

aipsi

ASSOLOMBARDA

FTI FORUM per la TECNOLOGIA della INFORMAZIONE

Inforav Istituto per lo sviluppo e la gestione avanzata dell'informazione

Federazione Italiana Delle Associazioni professionali per l'INFORmation Management

FIDA INFORM

www.fidainform.com

www. clubtimilano.net

- **La missione di FIDA è di garantire un contributo professionale di alto livello e con caratteristiche di "terzietà" nei processi conoscitivi e decisionali chiave dell'ICT italiana, al fine di valorizzare i propri soci, la professione ICT e di migliorare, con l'uso intelligente della tecnologia, la qualità della vita nel nostro Paese.**
- **I ClubTI, e quindi la loro Federazione FIDA, si propongono come «nodo» attivo del Sistema-Paese per lo sviluppo del Settore ICT "allargato", promuovendo la professionalità dei Soci**
- **complessivamente circa 1.000 associati**
- **Rivista bimestrale ICT Professional distribuita a 7000 "decision maker" e influenzatori dell'ICT**

Obiettivi OAI

- Avere cadenza periodica annuale
- Coinvolgere tutte le Associazioni e gli Enti coinvolti e/o interessati nella sicurezza informatica
- Divenire uno strumento di ausilio nell'Analisi del Rischio ed il punto di riferimento nazionale sulla sicurezza ICT, analogamente a quanto avviene con il Rapporto CSI statunitense
- Far conoscere e sensibilizzare i vertici delle Aziende/Enti sui problemi della sicurezza ICT

- Che cosa non è e non vuole essere OAI :
  - Un'indagine criminologica estesa a tutti i crimini informatici (es. pornografia e pedofilia elettronica, pirateria prodotti software, ecc.)
  - Uno studio accademico
  - Un'indagine di mercato

La logica del questionario

- Il questionario è volutamente breve e non richiede dettagli sulle infrastrutture informatiche e sulle modalità di attacco e di difesa, sia per renderlo il più possibile anonimo sia per non appesantire la sua compilazione.
- Il primo questionario fa riferimento sia agli attacchi subiti nel 2007 che nel 2008.
- Struttura del questionario
  - La “Sezione 1” richiede informazioni atte a rilevare le caratteristiche dell’organizzazione interessata dagli eventi descritti, in termini di dimensioni (n° di addetti), settore di attività, area geografica di copertura e sistemi informativi e di comunicazione disponibili.
  - La “Sezione 2” è volta a rilevare gli attacchi informatici subiti nel corso del 2007 e del 2008.
  - La “Sezione 3” è volta a rilevare la tipologia e la frequenza con cui si sono verificate le tipologie di attacco di maggior rilievo.
  - La “Sezione 4” è volta a rilevare quali siano gli attacchi potenziali maggiormente temuti, indipendentemente da quelli effettivamente subiti e riscontrati.
  - La “Sezione 5” è volta a rilevare quali misure e politiche di sicurezza siano state pianificate o realizzate per tutelare le informazioni e i sistemi.

La tassonomia degli attacchi considerata

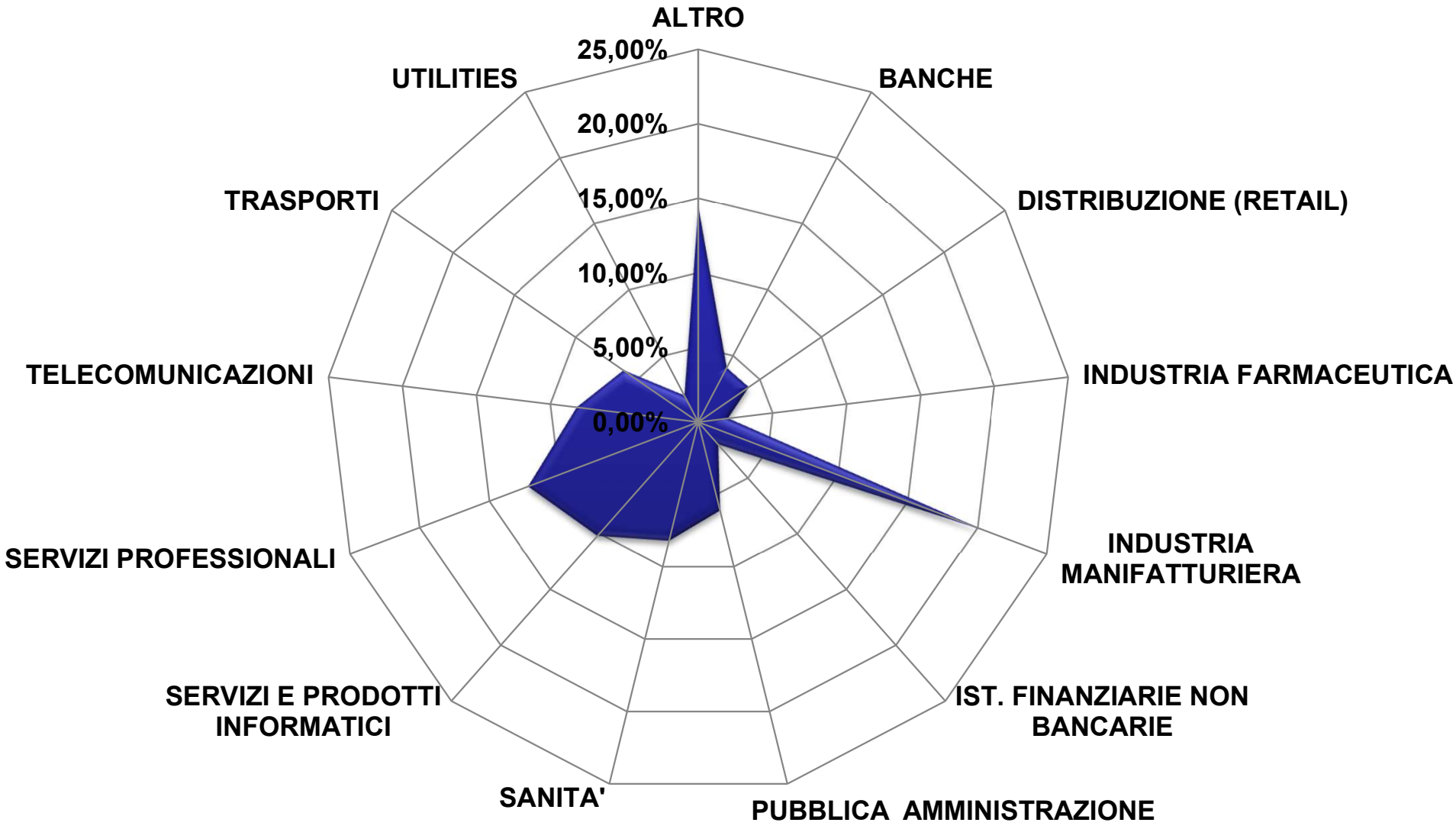
1) Accesso e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni
2) Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.
3) Modifiche non autorizzate ai dati e alle informazioni
4) Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server
5) 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.
6) Saturazione risorse informatiche e di telecomunicazione: oltre a DoS (Denial of Service) e DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, catene di S. Antonio informatiche, spamming ecc.
7) Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)
8) Furto di informazioni o uso illegale di informazioni
    a) da dispostivi mobili (palmari, cellulari, laptop)
    b) da tutte le altre risorse
9) Attacchi alle reti, fisse o wireless, e ai DNS, Domain Name System
10) Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)
11) 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 e il furto d'identità digitale
12) Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente…)
13) Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotaggi, vandalismi con distruzione di risorse informatiche.

I primi dati di OAI 2009

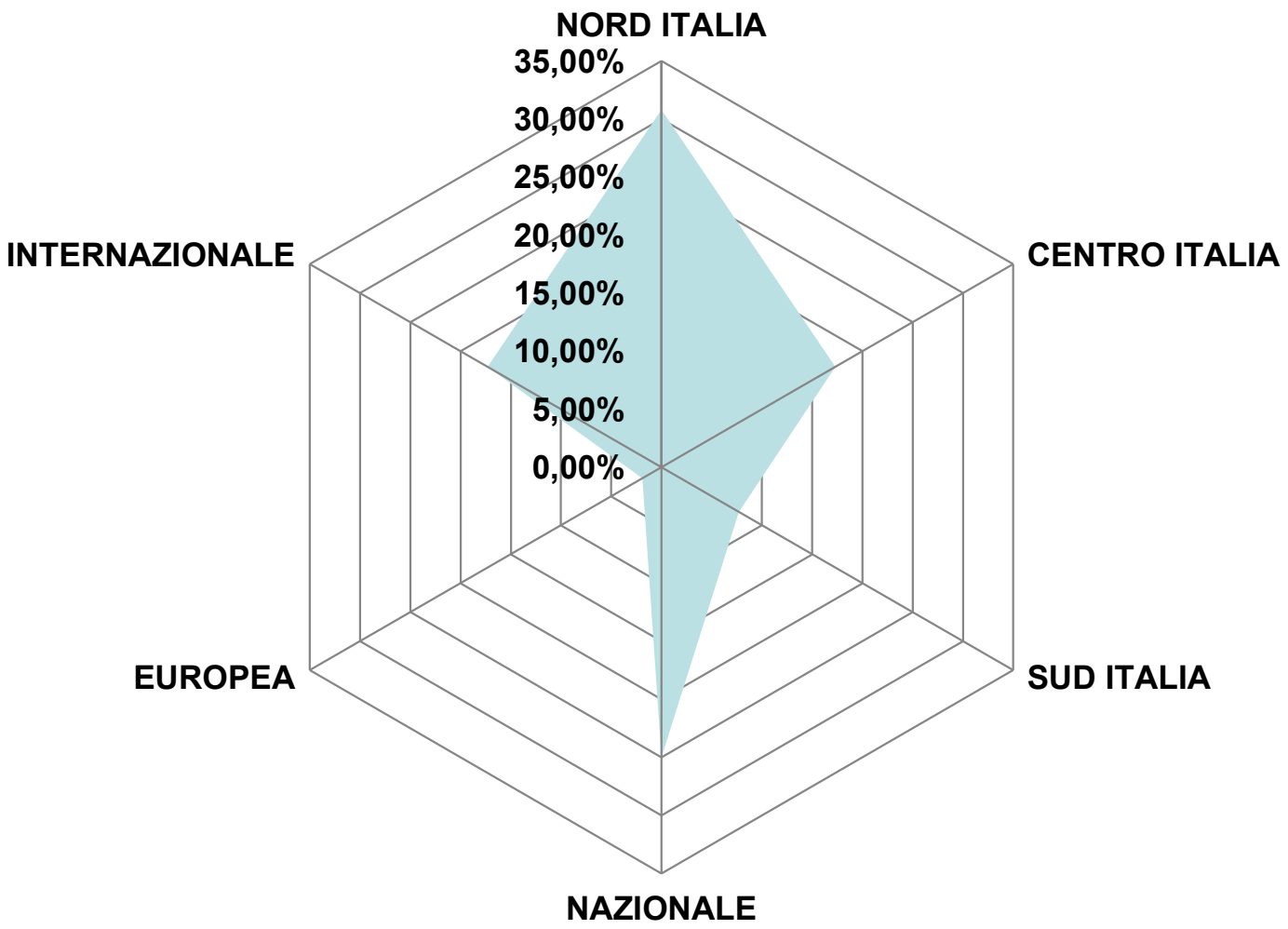
- I dati che seguono sono un anticipo parziale dei risultati dell'indagine che è ancora in corso
- I dati elaborati e presentati nel seguito si basano sui primi questionari ricevuti
- I dati del rapporto finale, che contempleranno almeno 200 risposte "valide" e significative, potranno essere diversi da quelli oggi presentati

- NB: volutamente nel presente questionario non sono state richieste stime delle perdite economiche (dirette, indirette, consequenziali) subite da chi ha subito un attacco, per la difficoltà nell'effettuare tali stime e la conseguente difficoltà o non volontà di rispondere a simili domande

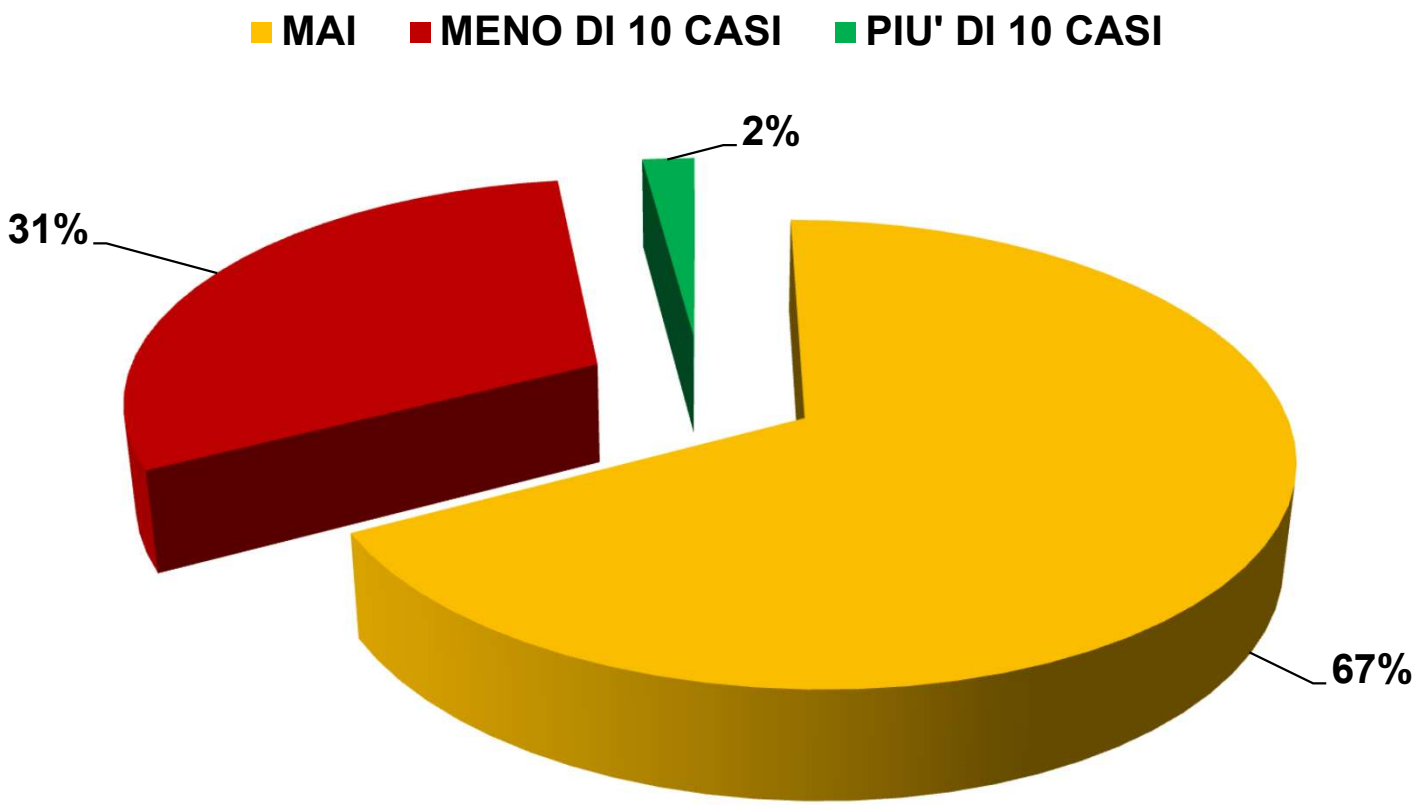
OAI 2009: settori merceologici di attività dell'insieme dei soggetti censiti



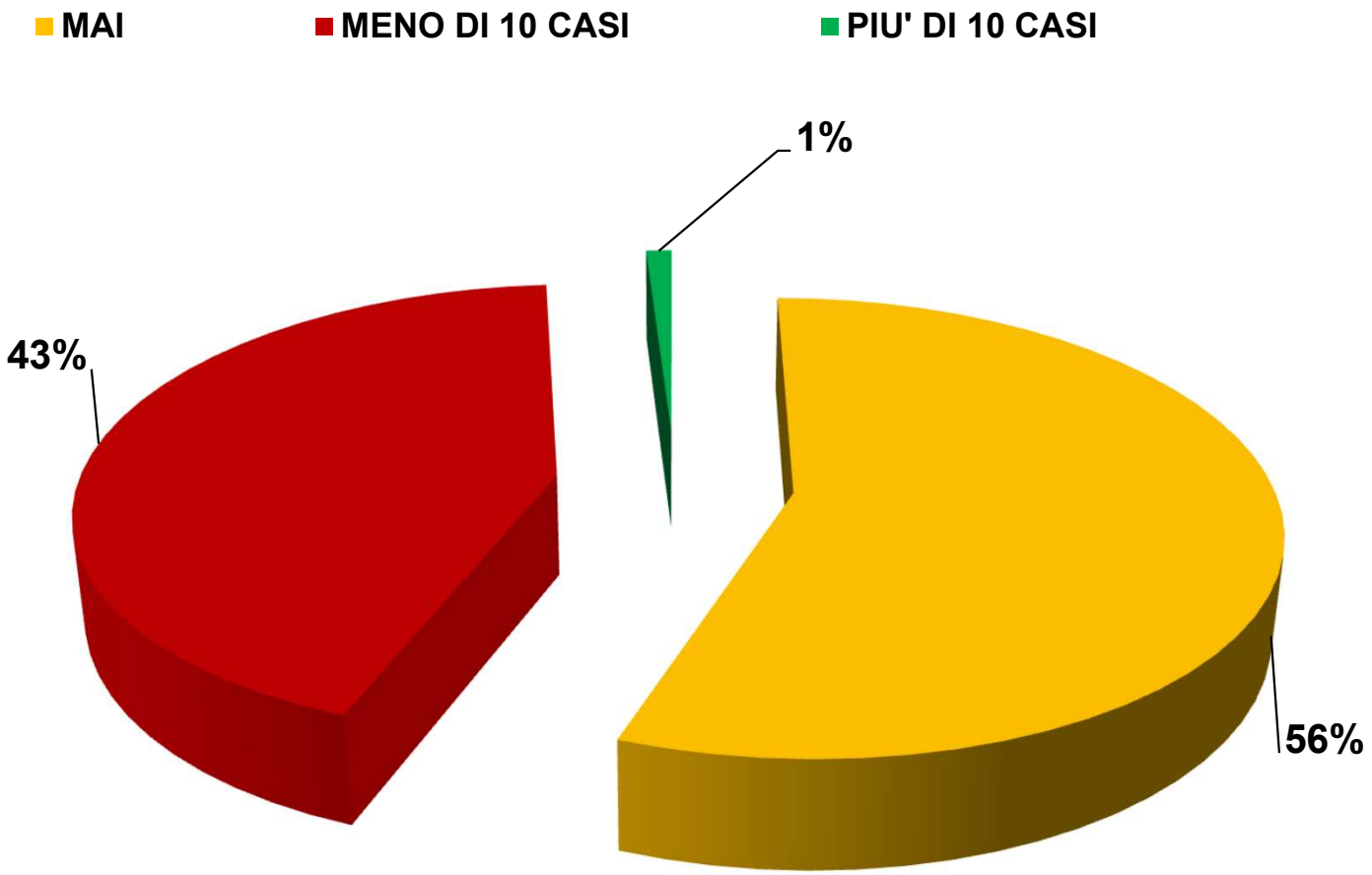
OAI 2009: area geografica di estensione dell'insieme dei sistemi ICT censiti



OAI 2009: % num attacchi 2007



OAI 2009: % num attacchi 2008



OAI 2009: tipologia attacchi rilevati 2007/2008

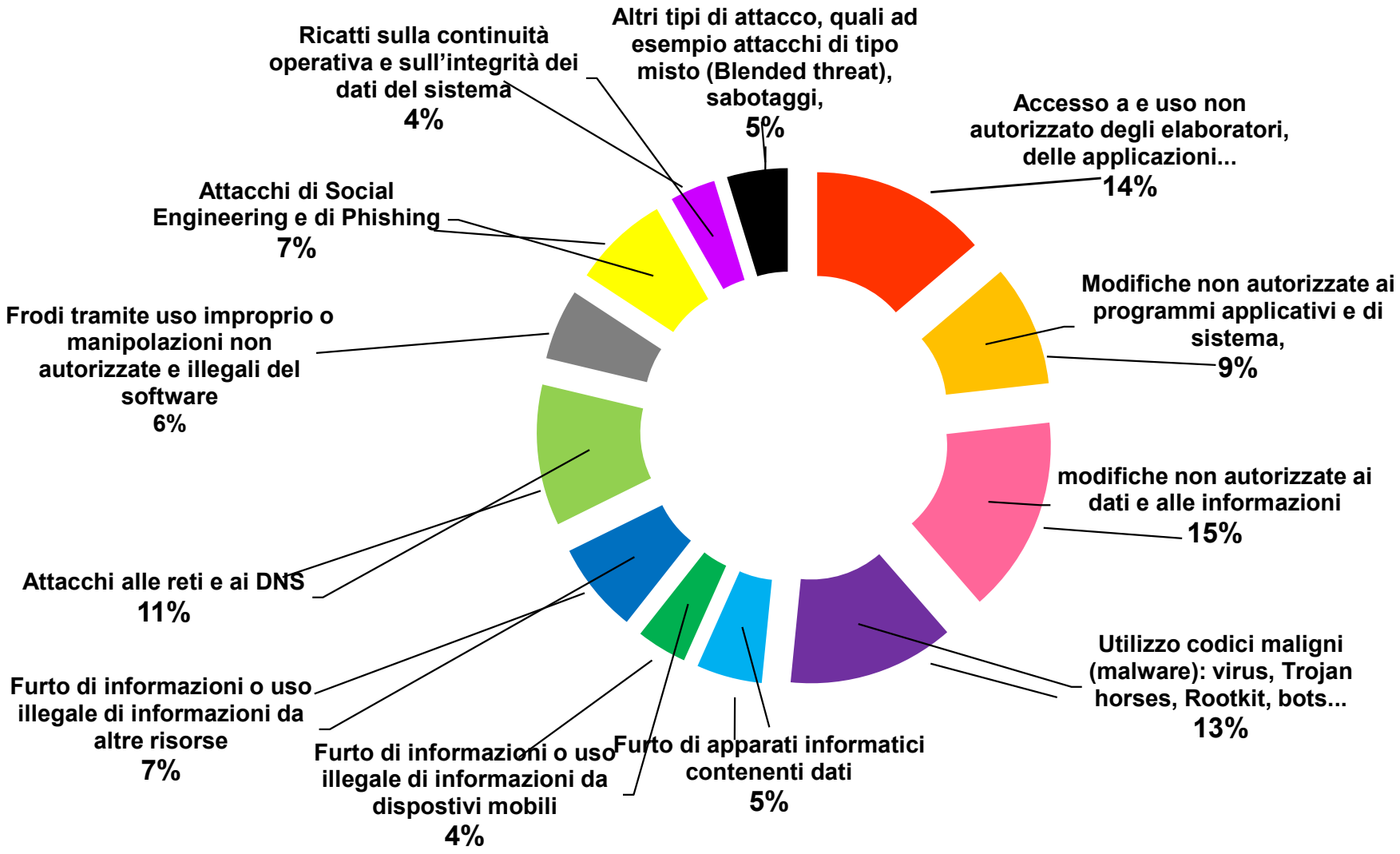
TIPOLOGIA DI ATTACCO	DA 1 A 5		DA 1 A 5		OLTRE 10	
	2007	2008	2007	2008	2007	2008
Accesso a ed uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni	5	5	1	1		
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.	3		1			
Modifiche non autorizzate ai dati e alle informazioni	1					
Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server	1	1				
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)	1	1				
Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellulari, laptop)						
Furto di informazioni o uso illegale di informazioni da tutte le altre risorse						
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	1					
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)	1					
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 e il furto d'identità digitale		1				
Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente…)						
Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotaggi, vandalismi con distruzione di risorse informatiche. Se individuato, segnalare il tipo di altro attacco subito (specificare):						

N.B. campione iniziale di 49 risposte

OAI 2009: % strumenti e metodologie in uso

STRUMENTI E METODOLOGIE DI PROTEZIONE IN USO	%
Antivirus and antispyware	100%
Firewall e DMZ	91,80%
Identificazione dell'utente con identificativo d'utente e password	91,80%
VPN (Virtual Private Network)	79,60%
Strumenti di gestione delle autorizzazioni (Active Directory, Ldap, Access Control List, policy server)	75,50%
Monitoraggio e controllo funzionalità e prestazioni dei sistemi	61,20%
Uso di strumenti per la gestione delle patch, degli aggiornamenti, delle release	61,20%
Archiviazione e gestione dei log	59,20%
Politiche (policy) tecnico-organizzative di sicurezza ICT	55,10%
Rete Wireless hardened (ad esempio reti chiuse)	53,10%
Uso sistemi ad alta affidabilità	53,10%
Firewall e Reverse proxy a livello applicativo	44,90%
Crittografia dei dati in transito (https ecc.)	44,90%
Sistemi di individuazione delle intrusioni (IDS, Intrusion Detection System)	34,70%
Disaster Recovery Planning	34,70%
Uso di procedure organizzative formalizzate nel supporto ai processi inerenti la sicurezza informatica	32,70%
Sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention Systems)	30,60%
Vulnerability assessment – scansioni della rete e dei sistemi - Hardening	30,60%
Sistemi di PKI (Public Key Infrastructure)	24,50%
Identificazione dell'utente "forte" con certificati digitali	24,50%
Uso di strumenti informatici per il supporto dei processi inerenti la sicurezza informatica	18,40%
Identificazione dell'utente anche tramite opportuni "token" quali chiavi USB, smart card, dispositivi One Time Password ecc.	16,30%
Software di sicurezza End-Point e NAC, Network Access Control	16,30%
Utilizzo di un SGSI, Sistema Gestione Sicurezza Informatica, integrato e centralizzato	16,30%
Crittografia dei dati archiviati (hard disk, chiavi USB ecc.)	14,30%
Uso di specifici strumenti per il controllo della sicurezza intrinseca degli applicativi (ispezione del codice, test di penetrazione ecc.)	8,20%
Identificazione dell'utente biometrica	6,10%
Archiviazione remota e sicura dei backup	2%

OAI 2009: % tipologia attacchi più temuti



Prime considerazioni sugli attacchi subiti dal campione iniziale e parziale considerato

- un maggior numero di attacchi tra 1-10 nel 2008 (43%) rispetto al 2007 (31%)
- un minor numero di attacchi >10 nel 2008 (1%) rispetto al 2007 (2%)
- Il tipo di attacco più riscontrato è l'"*accesso a ed uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni*"
- Molto ridotti gli attacchi da virus e codici maligni

Prime considerazioni sugli strumenti in uso

- Il campione di Aziende/Enti che per primo ha risposto è in media “ben strutturato” ed organizzato,e comprende quindi strutture di medie-grandi dmensioni. Infatti:
  - **Praticamente tutti** usano sistemi **antivirus, firewall, DMZ**, e strumenti di identificazione dell’utenza tramite un suo **identificativo** e **password**
  - L’uso dei **certificati digitali** si attesta interno al **24,5%,** ma l’uso di “token” quali smartcard e chiavette scende al **16,3%**; **l’identificazione biometrica** è usata dal **6%** del campione
  - **Diffusi** strumenti anche abbastanza “sofisticati” quali **VPN, gestione log, monitoraggio e controllo sistemi ICT**
  - Si riduce la percentuale di chi ha **sistemi per la gestione della sicurezza ICT** ed utilizzo di strumenti per **l’analisi delle vulnerabilità**, **IDS/IPS**, ma rimane comunque su valori non trascurabili tra il **30** ed **16%**
  - La **crittografia** è usata per circa il **45%** nella **trasmissione** dei dati e per il **14,3%** per l’**archiviazione** di dati
  - Il **34%** afferma di avere pianificato soluzioni di **Disaster Recovery**

- Stranamente in tale contesto il valore basso per l’”**archiviazione remota e sicura dei backup**” pari a solo un **2%**

Prime considerazioni sugli attacchi più temuti

- l'attacco "killer" più temuto risulta la **modifica** non autorizzata (o per errore) **ai dati ed ai programmi** , che arriva al **24%**

- Seguono vari tipi di attacchi tutti ritenuti significativi, tutti > **10%** ma **< 15%,** tra i quali:
  - accessi non autorizzati
  - codici maligni
  - attacchi alle reti ed al DNS

- Altri attacchi significativi , ma **< 10%** , includono:
  - phishing e social engineering
  - furto di informazioni (si pensi alla facilità con chiavette USB …)
  - furto di apparati
  - frodi

Si è ancora in tempo per rispondere al questionario…

- L'accesso al questionario è disponibile da parte di vari siti, in particolare sulle home page dei siti:
  - **Soiel** : www.soiel.it
  - **ClubTI di Milano**: www.clubtimilano.net
  - **AIPSI** : www.aipsi.it

- dove trovi il banner

- Oppure accedi direttamente a :

  http://www.soiel.it/FIDA/pagina1.html