AIPSI- ISSA European Security Conference 2010
Roma, 28 ottobre 2010

L'iniziativa OAI ed i primi dati raccolti per il Rapporto 2010

Marco R.A. Bozzetti
Founder OAI
Direttivo AIPSI

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

oai OsservatoriO AttacchInformatici

ISSA™
Information Systems Security Association
The Global Voice of Information Security

Indice

OsservatorIO AttacchInformatici

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**

- **Gli ideatori e realizzatori**

ClubTI Milano

La federazione dei ClubTI in Italia

L'Editore

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

OsservatorIO AttacchInformatici

Collaborazioni e patrocini Rapporto 2010

con il patrocinio di:

e in collaborazione con:

Il Rapporto OAI 2009

- **In formato elettronico**
  - Disponibile gratuitamente in vari siti web ***previa registrazione***:
    - www.aipsi.org
    - www.clubtimilano.net
    - www.fidainform.it
    - www.forumti.it
    - www.malaboadvisoring.it
    - www.soiel.it
- **Edizione cartacea**
  - 47 pagine a colori su carta patinata

oai OsservatorIO AttacchiInformatici

La tassonomia degli attacchi considerata

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 nascondibili e trasportabili contenenti dati (unità di rete, Laptop, hard disk, floppy, nastri, Chiavette USB, ecc.)
3. **Furto di informazioni** e loro uso illegale sia da dispostivi mobili (palmari, cellulari, laptop) sia da tutte le altre risorse ICT
4. **Frodi** tramite uso improprio o manipolazioni non autorizzate ed illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni, ecc.)
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 (es: se non paghi attacco il sistema e ti procuro danni, normalmente con dimostrazione delle capacità di attacco e di danno conseguente …)
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
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. **Utilizzo codici maligni** (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots , exploits, sia a livello di posto di lavoro che di server.
12. **Saturazione** risorse informatiche e di telecomunicazione: oltre a DoS (Denial of Service), DDoS (Distributed Denial of Service) e Botnet, si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc.
13. **Attacchi alle reti**, fisse o wireless, **e ai DNS**, Domain Name System

Indice

OsservatorIO AttacchInformatici

I primi dati parziali di OAI 2010

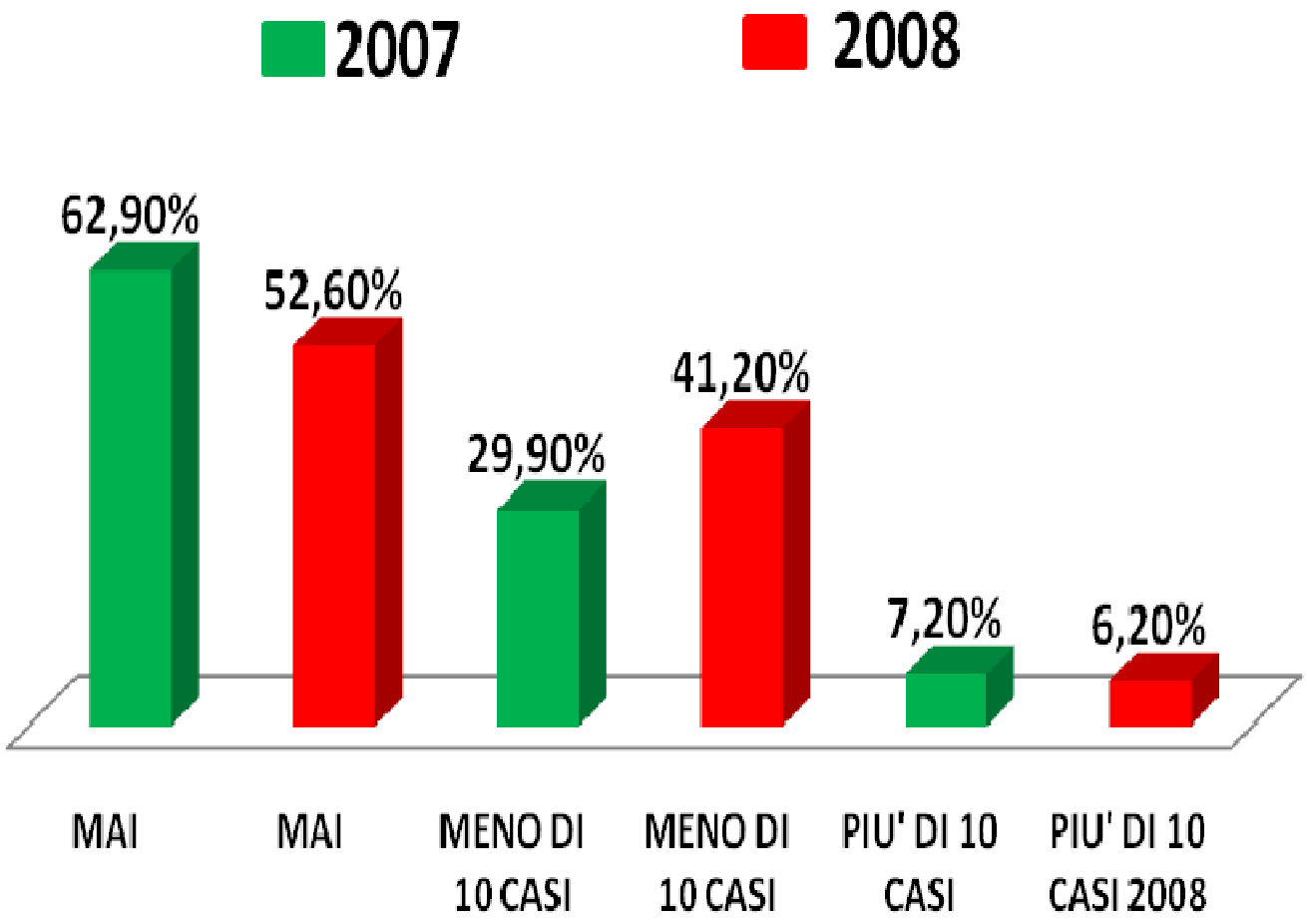
- I dati relativi al 2009 ed al 1° quadrimestre 2010 sono un anticipo parziale dei risultati dell'indagine per il Rapporto OAI 2010 che è ancora in corso

- Tali dati si basano sui primi questionari ricevuti

- I dati del rapporto finale, che contempleranno più 200 risposte "valide" e ben bilanciate tra i vari settori, potranno essere diversi da quelli oggi presentati

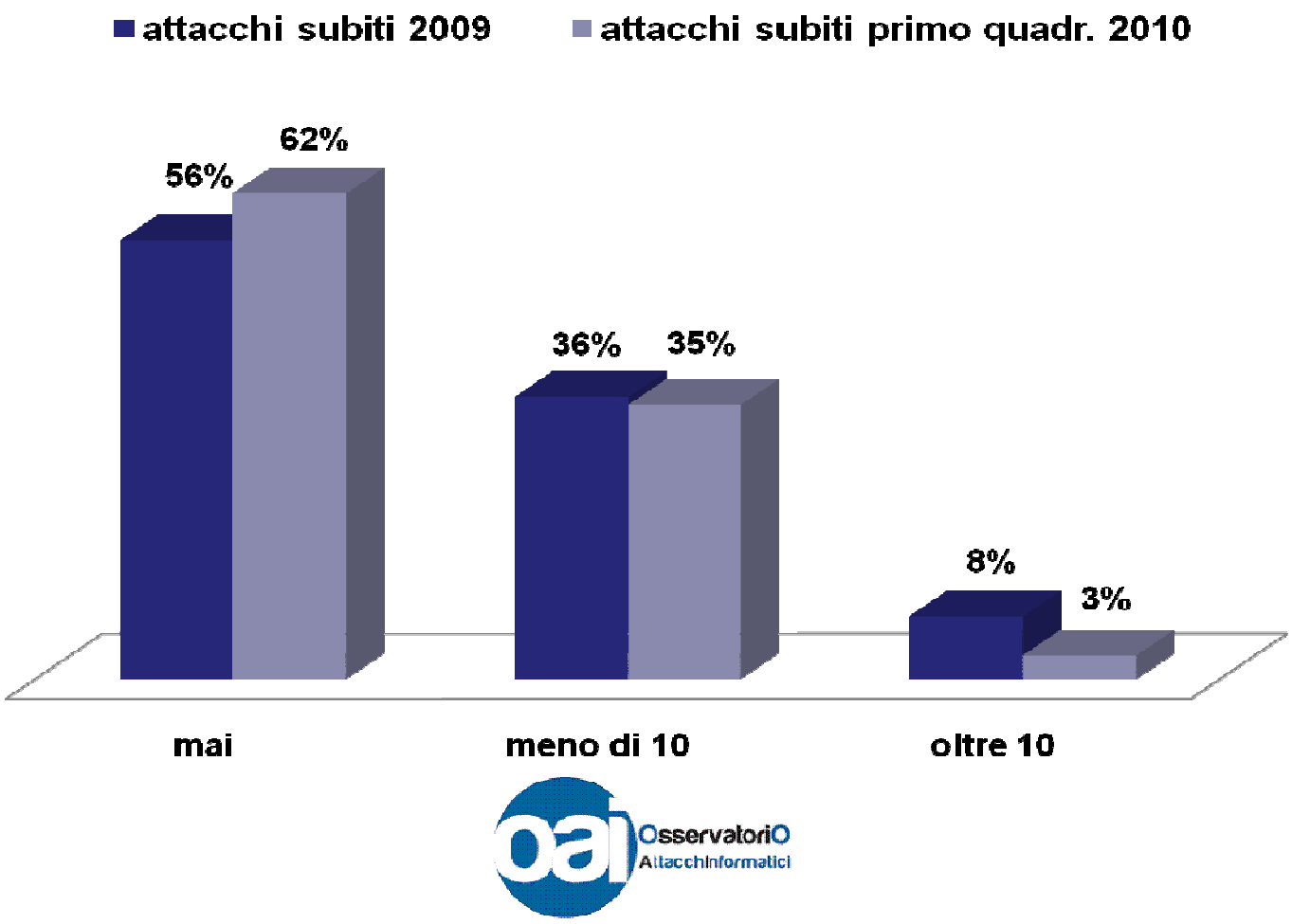
OsservatoriO AttacchInformatici

OAI 2009: % numero attacchi rilevati nel 2007 e nel 2008



OsservatoriO AttacchInformatici

Parziale OAI 2010: % numero attacchi rilevati nel 2009 e nel primo quadrimestre 2010



OAI 2009: attacchi più diffusi nel 2008

DIFFUSIONE ATTACCHI PER TIPOLOGIA 2008	COPERTURA (%)	GRADUATORIA
Utilizzo codici maligni (malware) sia a livello di posto di lavoro che di server	84%	1°
Attacchi di Social Engineering e di Phishing	58%	2°
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavett	50%	3°
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	42%	4°
Accesso a ed uso non autorizzato degli elaboratori, delle applicazioni supportate e da	34%	5°
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ec	28%	6°
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software ap	22%	7°

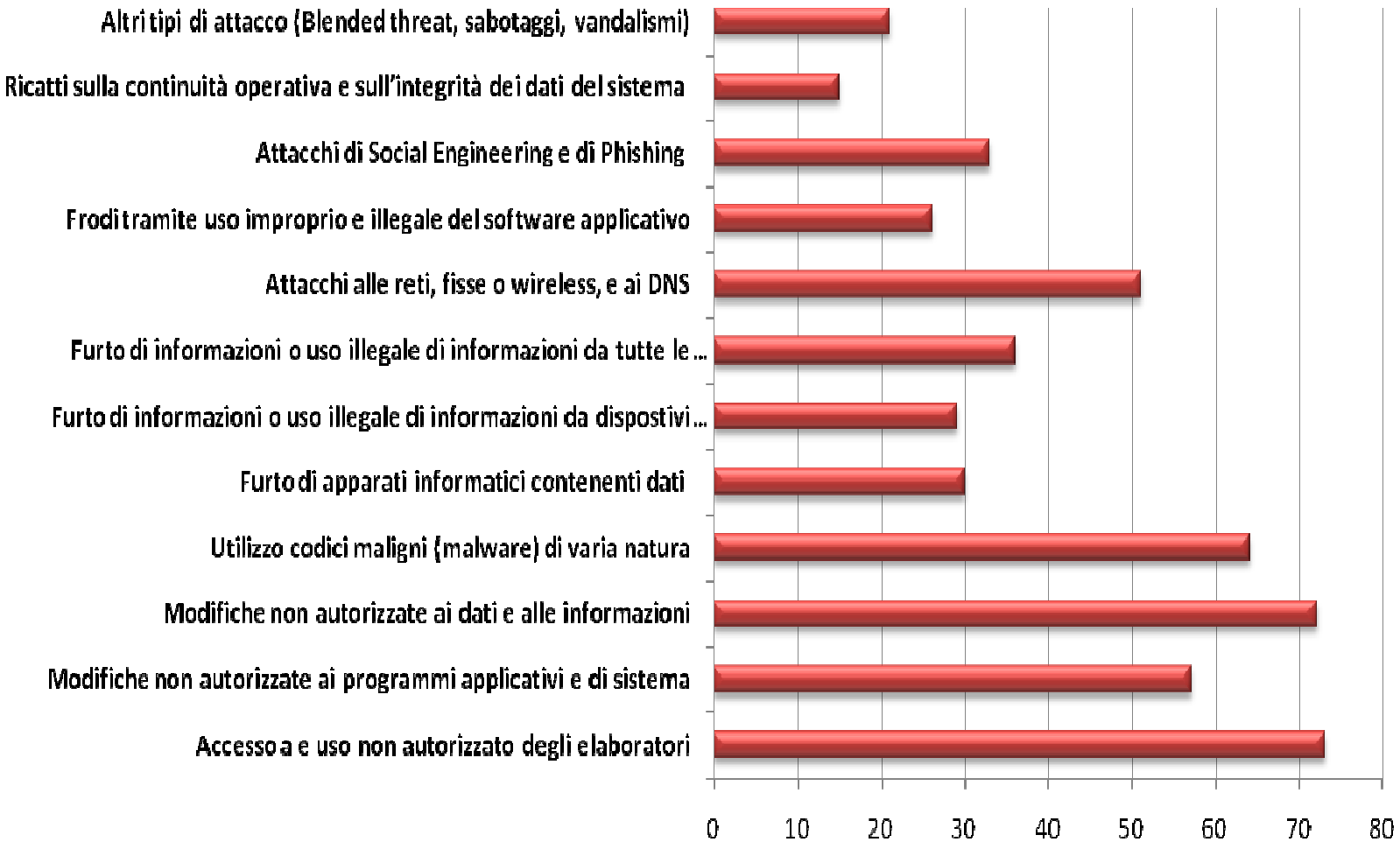
OsservatorIO AttacchInformatici

Parziale OAI 2010: attacchi più diffusi nel 2009 e nel primo quadrimestre 2010

TIPOLOGIA ATTACCHI	2009	1 quadr. 2010
Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan Horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server	63%	50%
Furto di apparati informatici facilmente nascondibili e trasportabili contenenti dati (unità di rete, laptop, hard disk, floppy, nastri, chiavette USB ecc.)	38%	37%
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.	33%	29%
Saturazione risorse informatiche e di telecomunicazione: oltre a DoS (Denial of Service), Ddos (Distributed Denial of Service) e Botnet, si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc.	25%	17%
Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni	19%	17%

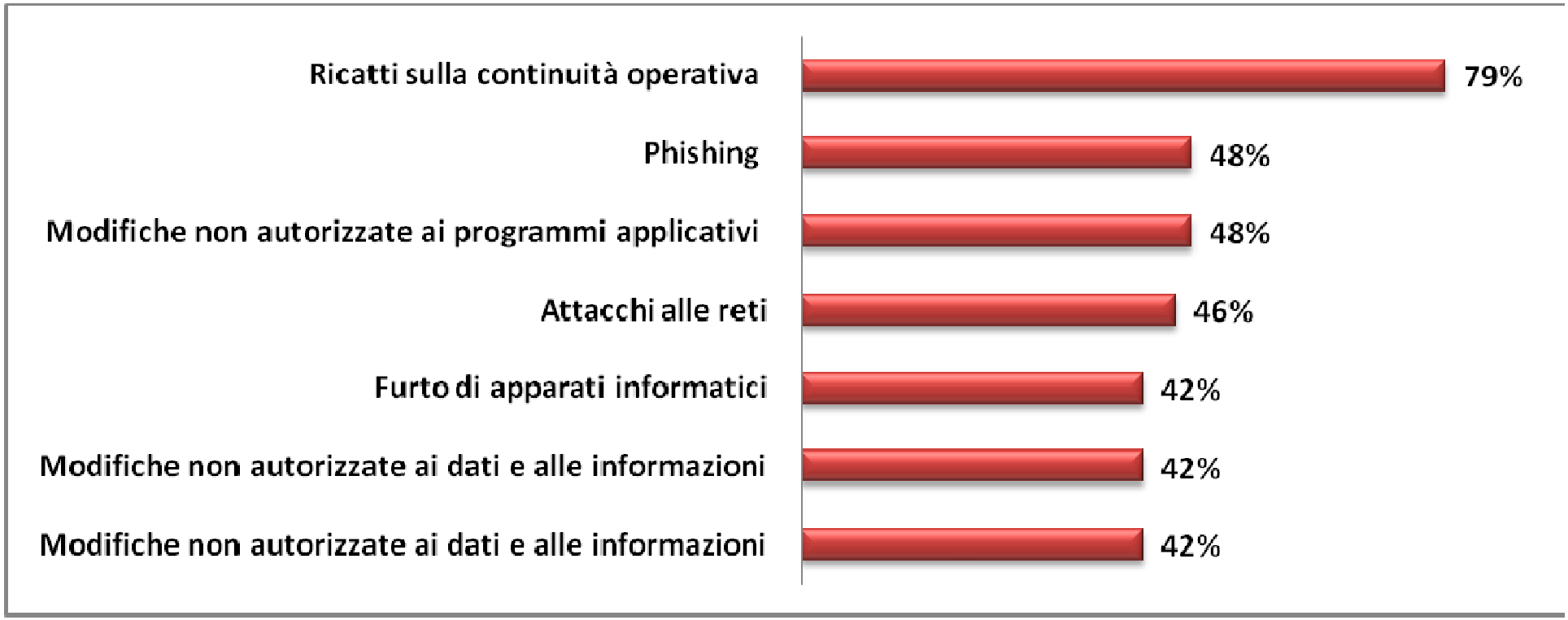
OsservatoriO AttacchInformatici

OAI 2009: % tipologia attacchi più temuti



OsservatoriO AttacchInformatici

Parziale OAI 2010: % tipologia attacchi più temuti



OsservatorIO AttacchInformatici

Parziale OAI 2010: % 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%

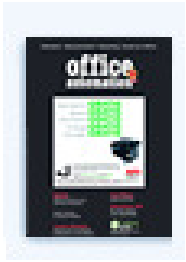
OsservatoriO AttacchInformatici

La rubrica mensile OAI sulla rivista Office Automation

Da marzo 2010 sulla rivista **Office Automation** tengo una rubrica fissa mensile per OAI sugli attacchi informatici, con un taglio più manageriale che tecnico.

Attacchi informatici: non si scherza più

Da questo numero prende il via una rubrica mensile sugli attacchi ai siste
collegata all'OAI (Osservatorio Attacchi Informatici in Italia) voluto da Fi
e dal ClubTI di Milano insieme a Soiel International, con il patrocinio di



Non esiste sicurezza senza l'utente finale

Secondo appuntamento con la rubrica OAI (Osservatorio Attacchi Informatici).
Il comportamento di utenti e operatori è determinante per la sicurezza aziendale.
Nonostante i progressi tecnologici, se si sottovalutano aspetti di formazione
e sensibilizzazione, i rischi continueranno a crescere.

OsservatoriO
AttacchInformatici

Ancora in tempo per compilare il questionario on-line !!

- Per chi non l'avesse già effettuato, **è ancora in tempo per compilare il questionario all'indirizzo**

  http://www.soiel.it/questionarioOAI2010/pagina1.html

- Il Rapporto OAI completo sarà gratuitamente disponibile in forma elettronica entro fine 2010. Tale disponibilità sarà segnalata sui siti:
  - www.soiel.it
  - www.malaboadvisoring.it
  - www.clubtimilano.net
  - www.fidainform.it

  oltre che sui siti di tutti i Patrocinatori

OsservatorIO AttacchInformatici