[(in) Sicurezza Informatica]

1

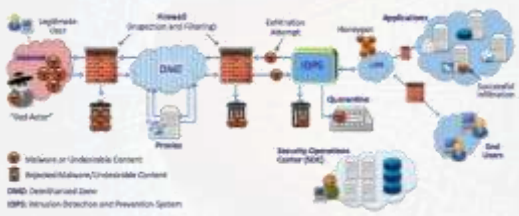
[chi sono]

Giancarlo Rosa

Perito Industriale Informatico nato con la passione per la comprensione degli algoritmi.
Dopo il diploma e una breve parentesi universitaria prematuramente interrotta, inizio a lavorare come analista programmatore nel 1994.
Nel 2000, a seguito di un primo incontro con l'informatica forense, decido di affrontare l'Esame di Stato per l'abilitazione all'esercizio della Libera Professione. Contestualmente apro una azienda (Informatica Uno) specializzata in sicurezza informatica.
La formazione continua e l'approccio sempre orientato al modello scientifico mi hanno consentito di perfezionare le competenze nell'acquisizione e analisi di dati provenienti dalle fonti più disparate. Dal 2004 sono iscritto all'Ordine dei Periti Industriali e dei Periti Industriali Laureati per le province di Sassari e Olbia-Tempio con il n°513. Sono inoltre iscritto all'albo dei CTU e dei Periti del Tribunale di Sassari. Dal 2011 sono anche amministratore della Uno Srl, società che ha inglobato una serie di realtà del mondo dei servizi informatici.
In qualità di Perito Informatico lavoro per privati, enti, aziende e autorità giudiziarie portando a frutto competenze specifiche in vari ambiti della digital forensics e della consulenza e sicurezza informatica.

2

[aspetti tecnici …]



3

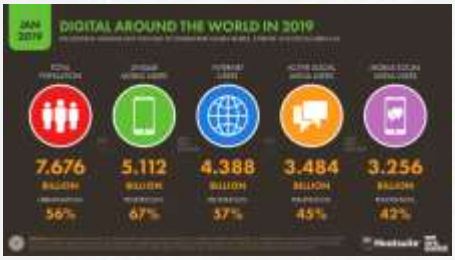
[alcune definizioni]

La **sicurezza informatica** (in inglese *information security*):

- è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici; a questi tre parametri si tende attualmente ad aggiungere l'autenticità delle informazioni;
- è anche la capacità di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi tali da compromettere i dati personali conservati o trasmessi (GDPR);
- è la capacità di adottare misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni;
- è la capacità di fronteggiare un attacco informatico e ripristinare la situazione preesistente (si noti che questo normalmente comporta un esborso di gran lunga maggiore rispetto a quello da sostenere per l'adozione di sistemi di sicurezza adeguati).

4

[il mondo connesso]



Fonte: http://wearesocial.com

5

[quali sono le minacce]

- **Esterne**
  - Cybercrime
  - Terrorismo
- **Interne**
  - Dipendenti infedeli / disattenti
- **Evoluzione Tecnologica**
  - Big Data, IoT, SCADA / ICS, Cloud Computing, Fintech / Insuretech, Cripto Valute, ecc.

6

[principali minacce cibernetiche]

- **Cybercrime**: complesso delle attività con finalità criminali come la truffa o la frode telematica, il furto d'identità, la sottrazione di informazioni o di creazioni e proprietà intellettuali;
- **Hacktivism**: perseguimento di obiettivi sociali e politici attraverso la pirateria informatica, termine derivante dall'unione delle parole hacking e activism;
- **Espionage**: acquisizione indebita di dati / informazioni sensibili, proprietarie o classificate;
- **Cyber Warfare** utilizzo della rete da parte di gruppi di «hacker» per attaccare i computer di un paese al fine di danneggiare cose, come i sistemi di comunicazione, sistemi di trasporto o le forniture di acqua ed elettricità o addirittura enti governativi



7

[impatto]


"Ci sono solo due tipi di aziende: quelle che sono state attaccate e quelle che devono ancora esserlo."
Robert Mueller - ex Direttore FBI


+150%
2018 vs 2017
segnalazioni settore PA

+37,7%
2018 vs 2017
attacchi gravi

L'uomo è l'anello debole della catena della sicurezza


Fonte: Rapporto Clusit 2019

8

[la minaccia in numeri]

Il cyber crime a livello mondiale ha raggiunto i **500 miliardi di Euro l'anno** – poco dietro il narcotraffico.

ma...

gli attacchi di cui non si hanno notizia, sia perché non sono stati scoperti (e si continuano subire), sia perché i diretti interessati non ne danno notizia, sono invece **incalcolabili.**

In **Italia negli ultimi anni ha avuto incrementi a due cifre**.

- attacchi con finalità di spionaggio / sabotaggio (+69,09%)
- con finalità estorsive o di arricchimento diretto (+35,25%)

9

[attacco informatico]

- Un attacco informatico è una qualunque manovra, impiegata da individui od organizzazioni (anche statali), che colpisce sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite atti malevoli, provenienti generalmente da una fonte anonima, finalizzati al furto, alterazione o distruzione di specifici obiettivi violando sistemi suscettibili.
- La maggior parte degli 'utenti finali' di un calcolatore non sa esattamente cosa sia un attacco informatico.
- Si limita ad averne paura e sperare che l'antivirus scelto (?) funzioni...
- Le informazioni su Internet non aiutano a capire...

10

[principali minacce **MALWARE**]

- Definizione Malware: abbreviazione che sta per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso)
- Indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata
- Il termine malware è stato coniato nel 1990 da Yisrael Radai;

11

[principali minacce **MALWARE**]

- Il principale modo di propagazione del malware consiste di frammenti di software parassiti che si inseriscono in codice eseguibile già esistente. Il frammento di codice può essere scritto in codice macchina ed inserito in un'applicazione esistente, in codice di utility, in un programma di sistema o può inserirsi anche nel codice del sistema di boot di un computer.
- Un malware è caratterizzato dal suo intento malevolo, agendo contro le necessità dell'utente, e non include software che causa un danno non voluto a causa di qualche suo difetto.

12

principali minacce **MALWARE**

PER AUMENTARE LA LORO EFFICACIA, SPESSO I CRAKER UTILIZZANO UNA COMBINAZIONE DI PIU' MALWARE PER RAGGIUNGERE I PROPRI OBIETTIVI!!!!!!

13

principali minacce **SPAM**

Secondo una ricerca di **F-Secure**, lo **spam** rimane il metodo più comune di diffusione di Url malevoli, truffe e malware dal 1978, anno in cui è stato inviato il primo messaggio di spam.

Negli ultimi anni ha guadagnato più popolarità rispetto ad altri vettori, poiché i sistemi stanno diventando più sicuri contro gli exploit e le vulnerabilità del software.

Solo nella primavera del 2018, F-Secure ha osservato che il **23% dei casi di spam riguardava email con allegati malevoli** e il **31% conteneva link a siti web pericolosi**.

Il tasso di click è cresciuto dal 13,4% della seconda metà del 2017 al 14,2% nel 2018.

Piuttosto che usare solo allegati malevoli, lo spam attuale spesso presenta un Url che indirizza verso un sito innocuo, che poi reindirizza al sito che ospita contenuti malevoli.

14

principali minacce **PHISHING**

Truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un interlocutore affidabile in una comunicazione digitale.

Sfrutta una tecnica di **ingegneria sociale**: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.

15

principali minacce **PHISHING**

Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS o le applicazioni di messaggistica istantanea quali WhatsApp e Telegram.

16

principali minacce **PHISHING**

«C'è un rimborso per te»,
ma è solo l'ultimo tentativo
di furto di dati

Un allettante rimborso di 1,482.05 euro che però non è andato a buon fine e la conseguente richiesta di «aggiornare le informazioni dell'account fornite»: **è uno degli ultimi tentativi di phishing**

Moltissimi contribuenti hanno infatti ricevuto una mail da un indirizzo che assomiglia a quello dell'agenzia delle Entrate ma che con l'Agenzia non ha nulla a che fare. Nel messaggio si annuncia al cittadino che un «rimborso» di un'«operazione» non è andato a buon fine e lo si invita a cliccare su un link per aggiornare i propri dati.

17

esempio mail di phishing

18

[altro esempio mail di phishing]

19

[nuove frontiere del phishing]

20

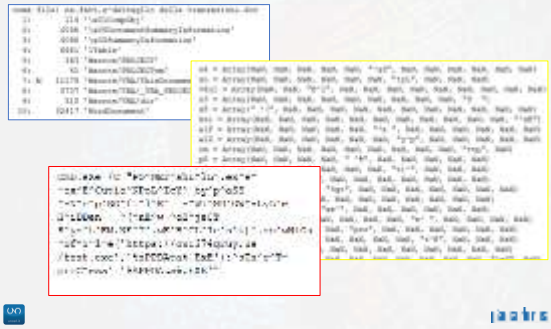
[i cavalli di troia (trojan)]

21

[i cavalli di troia (trojan)]

22

[esempi di codice]



23

[principali minacce attacco **DDOS**]

È l''acronimo di Distributed Denial of Services.
Si tratta di un attacco informatico che cerca di mettere in sovraccarico di richieste una macchina, fino a rendere impossibile l'erogazione dei servizi.
Questi attacchi vengono messi in atto generando un numero estremamente alto di pacchetti di richieste.

24

DDOS: una possibilità remota?

- Bot in rete: 6,7 milioni;
- Europa 1/5 dei bot a livello mondiale (18,7%);
- Italia: 2°posto assoluto per numero di infezioni (peggio di noi la sola Russia; meglio di noi Germania, Turchia e Spagna);
- Roma e Milano: 1° e 2° posto per presenza di dispositivi "zombie " (58,14% di tutti i dispositivi compromessi italiani - Roma 30,11%; Milano 28,03%);
- Città europee: Madrid maggior presenza di macchine compromesse
- 689 milioni di persone nel mondo, 10,2 milioni in Italia, vittime di crimini in rete;
- Qualsiasi dispositivo collegato alla rete può essere infettato da un bot (nel 2016 registrata una crescita esponenziale nell'utilizzo da parte degli hacker di smartphone e terminali IoT (Internet of Things) per il consolidamento del proprio esercito di bot;
- Vaticano: il paese più piccolo del mondo – ha il primato della maggiore densità di bot rispetto al numero di infezioni subite dagli utenti della rete.

Studio Symantec su http://www.repubblica.it/tecnologia/sicurezza/2017/09/28/news/italia_patria_dei_bot_secondi_in_europa_per_computer_zombie-176763210

25

attacco Man In The Middle (MITM)

L'aggressore trova un modo per sostituire la connessione verso il server con se stesso e comunica con il server

26

RANSOMWARE

Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.
Tipici esempi di questi ransomware sono i cosiddetti virus della Polizia di Stato, virus della Polizia Postale, virus della Polizia Penitenziaria, virus della Guardia di Finanza e virus della SIAE:

27

i numeri del 2018

Ransomware Nel primo semestre 2018 l'Italia è il Paese più colpito in Europa, con il 12,94% dei ransomware di tutto il continente intercettati, e tra i 10 più colpiti al mondo;

Malware Il numero totale di malware intercettati in Italia nella prima metà del 2018 è di 15.861.878, in flessione rispetto al 2017;

Visite a siti maligni Le visite a siti maligni sono state 6.949.860;

Le **minacce** arrivate via mail sono state 323.341.302;

Il numero di **App maligne** scaricate nella prima metà del 2018 è di 10.662;

Online Banking – Nella prima metà del 2018 sono stati 1.901 i malware di online banking che hanno colpito l'Italia. In crescita rispetto ai 1.525 del primo semestre 2017. I **malware per PoS** intercettati, sono stati invece 17.

28

i numeri del 2018

...gli attacchi scoperti da agenti esterni sono vecchi, in media, di 305 giorni mentre quelli scoperti dai team interni solo di 24,5.

Il 49% delle aziende che è stata vittima di una intrusione ad alto livello, è stata nuovamente attaccata con successo entro un anno dagli stessi criminali o da criminali "simili", mentre ben l'86% delle aziende che hanno subito più di un attacco andato a buon fine ha scoperto di avere più di un gruppo di criminali attivo nella sua rete.

29

quali sono i rischi ?

- Servizi e Dati non disponibili
- Reputazione
- Data leak (liste clienti, segreti industriali, piani di business, e-mail,…)
- Frodi Bancarie, Dati carte di credito rubati….
- Perdita di dati (Progetti, dati di clienti… perduti per sempre)

30

[quali sono le conseguenze?]

- **Ambito Privato** (Compagnie, PMI, Grandi Aziende, Micro Imprese, Professionisti….):
  - Perdita di denaro (crollo in borsa);
  - Perdita di credibilità;
- **Ambito Pubblico**
  - Dati di cittadini (sanitari, bancari,…)
  - Servizi (acqua, energia, trasporto….)

31

[come difendersi?]

- Protezione da Guasti:
  - Replicazione Dati e Backup
  - «Disaster recovery»
  - …
- Protezione dagli aggressori/ «attackers»…
  … chi sono?

32

[chi sono gli aggressori]

- Possono essere dei Competitor
- Giovani Hacker…
- Giovani Attivisti (Ex. Anonymous)
- Persone che vogliono guadagnare chiedendo un «riscatto » (ex. Cryptoloker)

33

[protezione fisica]

- Negare l'accesso non autorizzato a
  - Strutture
  - Attrezzature
  - Banche dati
  - Risorse
- Uso di più livelli di sistemi:
  - Sorveglianza
  - Guardie di sicurezza
  - Barriere protettive
  - serrature
  - Protocollo di controllo accessi

34

[gestione logica]

- La sicurezza fisica non è sufficiente
- Qualcuno potrebbe accedere attraverso la rete e ottenere o modificare i dati
- Proteggere informazioni e rete

35

[tecniche di difesa]

36

[da dove iniziare]

Clusit Associazione Italiana per la Sicurezza Informatica
https://www.clusit.it

Agenzia per l'Italia Digitale
https://www.agid.gov.it/it/sicurezza

CERT - PA
https://www.cert-pa.it/

Garante per la protezione dei dati personali
https://www.garanteprivacy.it

https://www.poliziadistato.it

https://www.commissariatodips.it

37

[avere buon senso]

- Partite dall'assunto che le richieste di credenziali o dati sensibili, collegate a una mail o a una telefonata, siano phishing;
- Nessuna attività di sicurezza richiede di contattare i singoli utenti e richiedere le loro credenziali...
- E che, soprattutto, nessuno vi voglia regalare qualcosa: "Non sono un pessimista ma un ottimista ben informato..."
- Ogni volta che venite contattati leggete attentamente il messaggio e domandatevi:
  - Ma la cosa richiesta è sensata?
    - Che senso ha inserire login e password per effettuare una verifica di sicurezza? Davvero le poste mi regalano 250 euro?
  - Sono sicuro che la richiesta sia autentica?
    - Indirizzo di email / indirizzo Web

38

[avere buon senso]

- Più in generale, ha senso inserire una password su un sito non sicuro?
  - https significa http sicuro / http non lo è e i dati viaggiano in chiaro
  - nessun sito Web serio lo usa più
- Nel dubbio non fate nulla... Difficilmente inserire username e password serve a risolvere un problema reale

39

[usare credenziali idonee]

- Essendo evidente che trasmettere i dati sensibili in chiaro non è una buona idea, le applicazioni Web moderne usano crittografia e password (e.g., https)
- Ma le mail, i social (anche se lo scenario sta cambiando) e gli SMS continuano a viaggiare in chiaro...!
- A maggior ragione la crittografia dovrebbe essere applicata ANCHE alla vostra password che viaggia sul Web (controllare che il sito sia https) Quindi crittografia più una BUONA password sono un ottimo mezzo per impedire/limitare accessi indesiderati

40

[usare credenziali idonee]

- **Cosa vuol dire BUONA password?**
  - Lunga almeno 9 caratteri (lo stato dell'arte ne richiede 12/14)
  - Usa lettere maiuscole e minuscole, numeri e caratteri speciali
  - NON contiene riferimenti a cose che vi riguardano (e.g., data di nascita di un vostro figlio)
  - Non viene usata anche su siti insicuri (stessa password per molte applicazioni)
  - Non viene rivelata
  - Non viene trasmessa in modo insicuro
  - Viene cambiata con una frequenza che dipende dalla criticità dell'applicazione

41

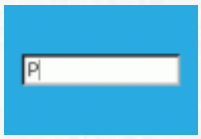
[perché usare password robuste]

- Contromisure efficaci per questo sono prese dai tecnici che si occupano della sicurezza della vostra azienda; Gli utenti finali non possono e non devono occuparsi di questo. Ma possono evitare di:
  - Usare password scontate, top 10 2018 : (123456, password, 123456789, 12345678, 12345, 111111, 1234567, sunshine, qwerty, iloveyou);
  - Usare la stessa password per applicazioni diverse...
  - Rendere la password visibile (sul Web, su un SMS, su un pezzo di carta, su un nota sul vostro schermo)
  - Usare la stessa password per decenni...

42

[proteggere le proprie credenziali]

- Utilizzare almeno tre (tipologie) password
  - Una molto robusta usata per applicazioni molto sensibili (banca, dati riservati, brevetti, etc.)
  - Una robusta per applicazioni relative al proprio lavoro
  - Una abbastanza robusta per applicazioni di poco conto
  - COMPLETAMENTE diverse nella struttura
- Utilizzare un password manager (password wallet) (e.g., lastPass) protetto da una password molto sicura
  - Utile anche contro gli attacchi di phishing: una pagina Web contraffatta NON ha l'indirizzo di quella vera e quindi la password NON viene inserita dal vostro password



43

[proteggere i nostri dati]

https://www.passpack.com

https://gnupg.org

44

[navigazione consapevole]

Firefox

Chrome

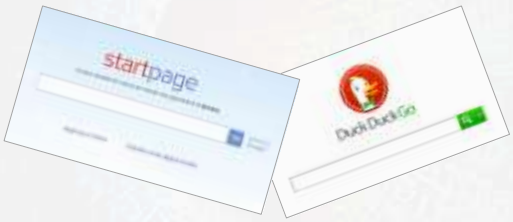
Safari

Internet Explorer

https://disconnect.me/trackerprotection

45

[i motori di ricerca]



startpage.com

duckduckgo.com

46

[monitorare i propri dati pubblici]

Firefox Monitor

https://monitor.firefox.com

';--have i been pwned?

https://haveibeenpwned.com/

DATABREACHED .it

https://www.databreached.it/

47

[dati identificativi]

48

[...sempre connessi...]

Fonte: http://thehackernews.com/2017/02/hacking-in-public.html

49

[...sempre connessi...]

Fonte: https://www.wired.it/internet/web/2019/10/25/krack-hacker/

50

[...sempre connessi...]

Fonte: https://www.lautomobile.aci.it/articoli/2019/10/24/auto-sicurezza-informatica-a-rischio.html

51

[Una sola soluzione...]

Investire in formazione!

Campione: 166 grandi imprese

52

[fine]

https://giancarlorosa.it

53