

Sommario, fondamentali, informazioni



Massimo Carnevali

Il materiale di questo corso è distribuito con licenza Creative Commons 4.0 Internazionale: Attribuzione-Condividi allo stesso modo.

<https://creativecommons.org/licenses/by-sa/4.0/>

Dove note sono state citate le fonti delle immagini utilizzate, per le immagini di cui non si è riusciti a risalire alla fonte sono a disposizione per ogni segnalazione e regolarizzazione del caso.

Massimo Carnevali

posta@massimocarnevali.com

<https://it.linkedin.com/in/massimocarnevali>

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sommario

0. Sommario, fondamenti, informazioni
1. Sicurezza infrastrutturale
2. Sicurezza dei sistemi
3. Software e piattaforme
4. Attacco e difesa
5. Aspetti umani, organizzativi e legali

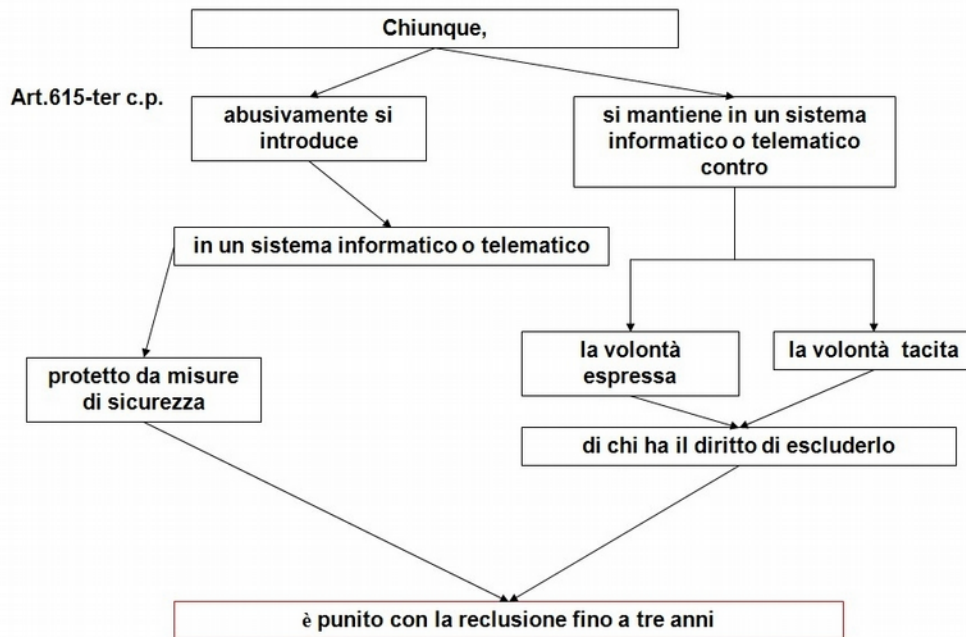
..

Sommario, fondamentali, informazioni

- Concetti base
- I livelli di Internet
- Siti utili

..

Concetti base



Concetti base

L'anello più debole della catena ...

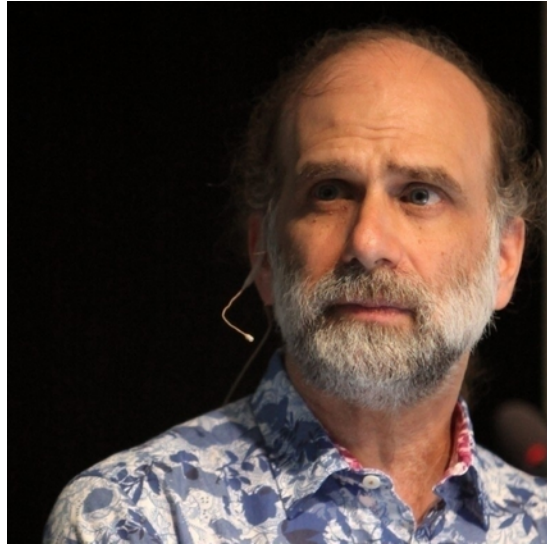


Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

5

Concetti base

La sicurezza è un
processo, non un
prodotto
Bruce Schneier



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

6

http://en.wikipedia.org/wiki/Bruce_Schneier

Concetti base

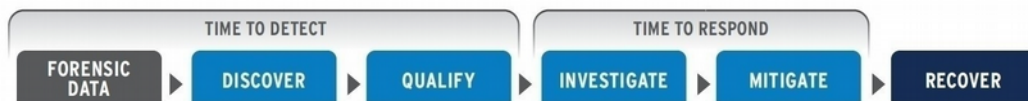
Security is never something we actually want.
Security is something we need in order to
avoid what we don't want.

Bruce Schneier

http://en.wikipedia.org/wiki/Bruce_Schneier

Concetti base

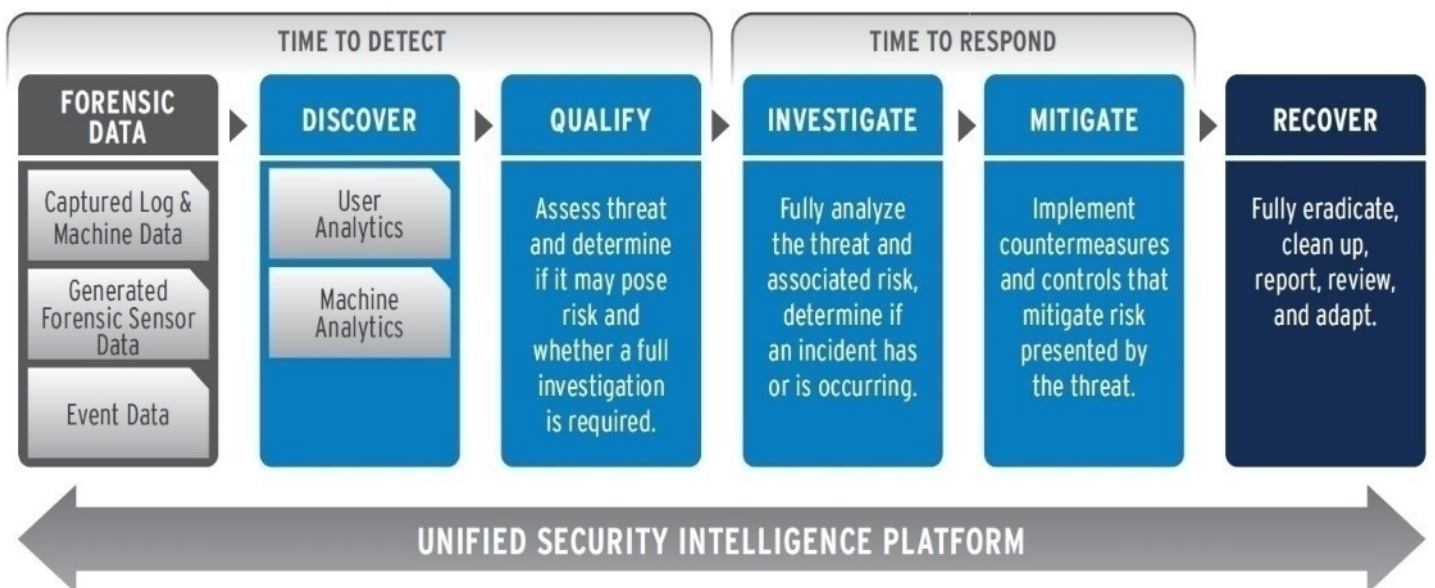
La sicurezza è un processo, non un prodotto



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

8

Surfacing Critical Cyber Threats Through Security Intelligence *A Reference Model for IT Security Practitioners*



Attacco informatico

Qualsiasi azione che comprometta la confidenzialità, l'integrità o la disponibilità di un computer o delle informazioni che contiene

<http://en.wikipedia.org/wiki/Cyber-attack>

Concetti base

Confidenzialità

Integrità

Disponibilità

Confidenzialità

Garanzia che i sistemi forniscano l'informazione solamente a chi è autorizzato a ottenerla

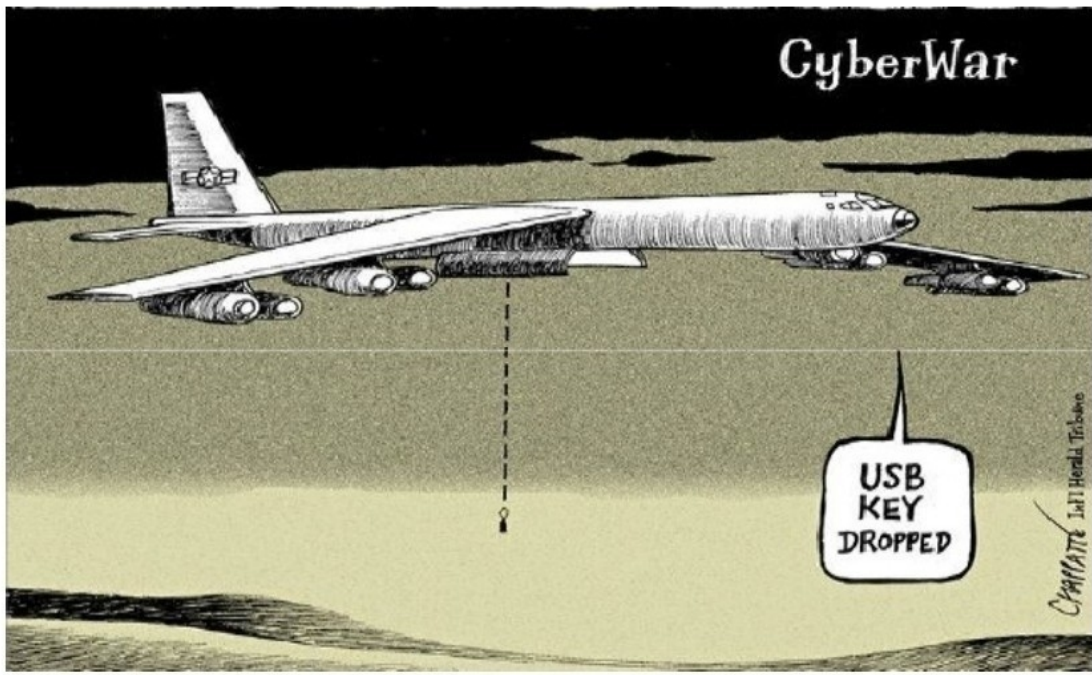
Integrità

Garanzia che l'informazione sia mantenuta e trasmessa in forma inalterata

Disponibilità

Garanzia che l'informazione risulti accessibile quando previsto a chi può e deve fruirne

Concetti base

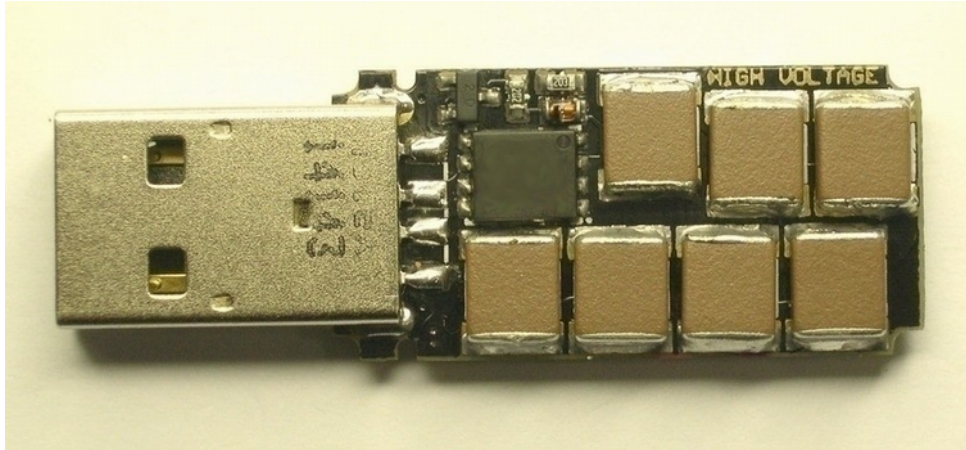


Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

11

Concetti base

Anche se



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

12

<http://kukuruku.co/hub/diy/usb-killer> Il concept iniziale, ora regolarmente in vendita:
<https://www.usbkill.com/>

Concetti base

Anche se

CRONACA

Trapani, inviata chiavetta Usb esplosiva a un'avvocata: ferito poliziotto

La penalista ha ricevuto la chiavetta in una strana lettera. Insospettitasi, ha consegnato alla polizia il pacchetto

Chiavetta contenente esplosivo e attivata dai 5v
dell'USB

Concetti base

Influenzare le elezioni in un altro paese è un atto di guerra?

Lasciare al buio e al freddo 250.000 persone due giorni prima di Natale è un atto di guerra?

Paralizzare l'economia di una nazione è un atto di guerra?

Russi all'attacco delle elezioni americane:

<https://arstechnica.com/information-technology/2018/07/from-bitly-to-x-agent-how-gru-hackers-targeted-the-2016-presidential-election/>

Dicembre 2015, Russia contro Ukraina (non rivendicato)

<https://www.wired.com/story/russian-hackers-attack-ukraine/>

Giugno 2017, ancora apparentemente Russia contro Ukraina, mai rivendicato e sfuggito di mano, attacco devastante rimbalzato in tutto il mondo.

Not-Petya "THE MOST DEVASTATING CYBERATTACK IN HISTORY Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world."

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Concetti base

Confusione di termini

Hacker = smanettone buono
(white hat)

Cracker = smanettone cattivo
(black hat)

Cracker = cibo

Non tutti concordano con questa classificazione.
(poi ci sono i “gray hat”...)

[https://en.wikipedia.org/wiki/Hacker_\(term\)#Hacker_definition_controversy](https://en.wikipedia.org/wiki/Hacker_(term)#Hacker_definition_controversy)

https://en.wikipedia.org/wiki/Hacker_culture

https://en.wikipedia.org/wiki/Security_hacker

[https://en.wikipedia.org/wiki/Cracker_\(food\)](https://en.wikipedia.org/wiki/Cracker_(food))

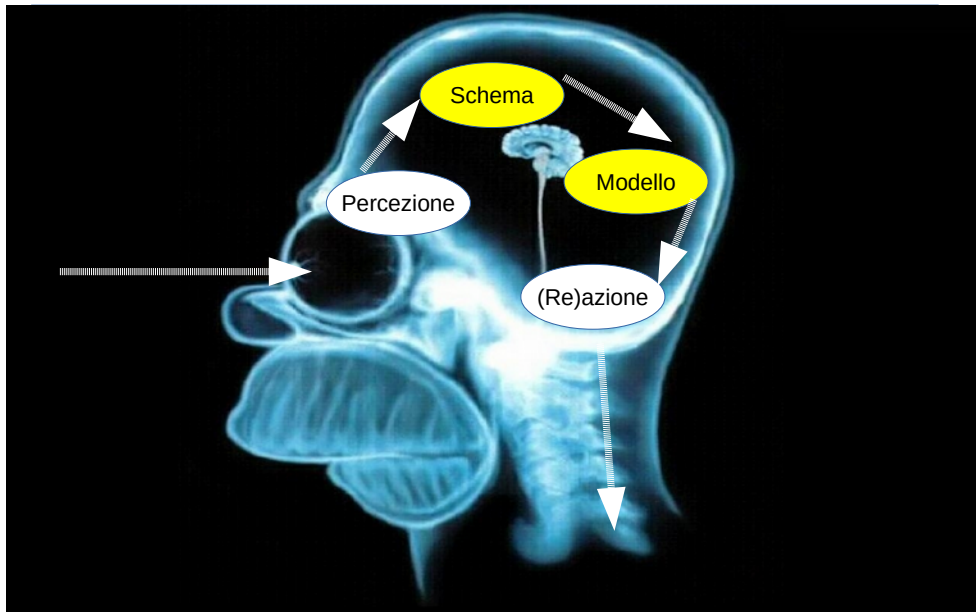
Misdirection

Alla base di tutto c'è il concetto di “misdirection”,
[http://en.wikipedia.org/wiki/Misdirection_\(magic\)](http://en.wikipedia.org/wiki/Misdirection_(magic))

L'arte di distrarti per fregarti

http://www.ted.com/talks/apollo_robbins_the_art_of_misdirection

Concetti base



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

17

Percepiamo l'input, gli applichiamo uno schema, lo correliamo con un modello noto e reagiamo di conseguenza.

(es. preda-predatore)

Schema e modello sono funzione dell'esperienza, del contesto, del task che sto svolgendo, dei condizionamenti sociali ecc.

Si applica anche alla "sicurezza" in senso lato.

I livelli di Internet

Non esiste solo Google

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

18

Esiste tutta una parte di Internet che normalmente ci è nascosta (nel senso che non è indicizzata da nessun motore di ricerca, però c'è).

Molte chiacchiere e molta mitologia su questo tema.

I livelli di Internet

(una delle classificazioni)

- › La superficie
- › Le reti aziendali protette (VPN)
- › Deep Web (nascosto)
- › Dark Web

Ma di quanti soldi stiamo parlando?

I livelli di Internet (una delle classificazioni)

La superficie. Tutto ciò che è indicizzato.

Le reti aziendali protette. VPN (sarà spiegato in seguito)

Deep Web. Pagine non indicizzate, ad accesso ristretto, protette da password, accessibili solo conoscendo URL complicate, bloccate da DMCA (OK queste non proprio protette ma non ve lo spiego io). A volte basta conoscere la strada giusta e ci si arriva.

Dark Web, reti anonimizzate (Tor ecc.), onion links, p2p.

Domini .onion Difficile da accedere, traffici illeciti, criminalità, e-commerce illecito (droga, armi). Silk Road (RIP). Meglio evitare. Ma anche libertà di parola, fuga dalla censura ecc. C'è anche Facebook ad esempio.

<http://f3magazine.unicri.it/?p=889>

I livelli di Internet



Black Markets

A successful Business Model

2012

- Silk Road realized \$22 Million In Annual Sales only related to the drug market. (Carnegie Mellon 2012)
- USD 1.9 million per month Sellers' Total revenue
- Silk Road operators earned about USD 143,000 per month in commissions.

2015

- Principal Dark 35 marketplaces raked from \$300,000 to \$500,000 a day.
- About 70% of all sellers never managed to sell more than \$1,000 worth of products. Another 18% of sellers were observed to sell between \$1,000 and \$10,000 but only about 2% of vendors managed to sell more than \$100,000

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

20

Fonte: **Pierluigi Paganini – Cyber Threat Summit 2015 – Dublino Ottobre 2015**

Dal 2016 al 2019 Wall Street Market è stato un mercato, una sorta di eBay, nascosto sulle darknet, dove si potevano vendere e comprare molti tipi di narcotici, software malevoli, dati rubati, merci contraffatte. Nell'aprile 2019 il sito era uno dei più grossi del suo genere per quantità di transazioni, con 5400 venditori e oltre un milione di account clienti complessivi. Arrestati due tedeschi e un olandese, si stavano preparando ad una "exit scam".

I livelli di Internet

The screenshot shows the UTOPIA website, a marketplace for various substances. The header includes the logo "UTOPIA" with the tagline "A BRIGHT STAR IN THE SHADOWS OF THE DARKNET". The user is logged in as "ads" and the currency is set to EUR. The main navigation bar includes links for "Main page", "My account", "My wallet", "My favorites", "My orders", "PM", "Forum", and "Logout". A search bar is also present.

The "Product Highlights" section displays a grid of items for sale:

- drzheng (3)**: Pure MXE with FREE worldwid... €888,50 (฿1.45287154)
- pocketscale (3)**: Super Bud strong indica €12,59 (฿0.02114901)
- Pharma Jack (3)**: 50 x Diazepam 5mg tablets (... €144,96 (฿0.24357219)
- xinhai2 (3)**: CAVIAR €40,72 (฿0.06842328)
- hollandonline (3)**: 10x 150ug Dutch Premium Tw... €66,68 (฿0.11203729)
- PureFireMeds (3)**: High Purity MDMA Crystal Po... €36,28 (฿0.06095992)
- dimitry (3)**: 5* LSD BLOTTER - SHAMROCKS... €55,53 (฿0.08330447)
- moremanu (3)**: well bleached pure MDMA 84%... €165,00 (฿0.27723984)

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

21

Fonte:

<https://medium.com/@jasisrad/journey-into-the-dark-8c7922a48265>

I livelli di Internet

The screenshot shows the homepage of DEEP.DOT.WEB, an official hidden service. The header includes the site name and logo, and a navigation menu with links for HOME, NEWS & ARTICLES, MARKETS LIST (highlighted), MARKETS CHART, VPN'S CHART, BITCOIN CASINOS, and DARKNET SEARCH. Below the navigation is a breadcrumb trail: HOME » FEATURED » UPDATED: LIST OF DARK NET MARKETS (TOR & I2P). The main content area features the article title 'UPDATED: LIST OF DARK NET MARKETS (TOR & I2P)' in large bold letters. Below the title, it states 'POSTED BY: DEEPDOTWEB' and 'OCTOBER 28, 2013' in a smaller font. Further down, it lists 'Last update: 18.4.17', 'Listing: ~53 Live Markets & Vendor Shops!', and a link to 'See the most recent changes in the Changelog'. At the bottom of the article preview, it says 'Welcome to our Updated List of Dark Net Markets! Can our list be Improved?'.

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

22

Ci sono parti del Deepweb che ogni tanto affiorano.
<https://www.deepdotweb.com/>

Siti utili

Siti di riferimento
(oltre a Google e Wikipedia ovviamente)
<http://imgtfy.com/>

Se proprio ve lo chiedono:

<http://imgtfy.com/>

Siti utili

Usi malevoli di Google (dorks)

Usando le query avanzate si trovano cose interessanti

`inurl:https://trello.com AND intext:@gmail.com AND intext:password`

Un elenco qui:

<https://www.exploit-db.com/google-hacking-database/>

https://www.google.it/advanced_search

CERT/CC

<http://www.cert.org/>

CERT non è un acronimo, ma un marchio di Carnegie Mellon University e ne è ora una divisione.

Il CERT Coordination Center è stato il primo computer incident response team, fondato dal DARPA nel 1988.

- Come gestire un incidente
- Cosa fare, chi contattare, cosa comunicare
- Come fare vulnerability reports
- Come ottenere informazioni sulla sicurezza
- Attività correnti, advisories, incidenti, vulnerabilità, sommari, CVE

http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

- Mailing list
- Fonti di informazione

Siti utili

SANS

<http://www.sans.org/>

SysAdmin, Audit, Network, Security institute

La più grande fonte per la sicurezza informatica.

Raccoglie, sviluppa e pubblica:

- Documenti
- Certificazioni
- Mailing lists
- Sans Newsbyte (Biweekly executive security summary)
- @RISK (Weekly Vulnerability Digest)
- Ouch! (Monthly security awareness report for end users)
- Internet Storm Center (Early Warning System)
- Training, webcast
- Reading Room: Free Resources
- <https://www.sans.org/critical-security-controls/>

Akamai

http://www.akamai.com/html/technology/visualizing_akamai.html

Internet non è nata per il business. Akamai fornisce un “overlay” su Internet composto da una piattaforma hardware distribuita e software intelligente allo scopo di fornire contenuti e applicazioni il più vicino possibile a chiunque e a qualunque cosa.

“If you’re using the Internet to shop, download music, watch TV, play a game, check the news, book a flight, upgrade software or conduct a business transaction, you’re probably using Akamai.”

- Kona Dashboard (web app firewall)
- Real Time Web Monitor
- Network Performance Comparison
- Visualizing the Internet

Center for Internet Security

<http://www.cisecurity.org/>

Aiuta le organizzazioni a gestire i rischi legati alla sicurezza informatica.

Fornisce metodologie e tool per misurare e migliorare lo stato dei sistemi connessi a Internet.

Pubblica benchmarks per la verifica di configurazioni di sicurezza di molti sistemi.

Security Focus

<http://www.securityfocus.com/>

E' una comunità di professionisti della sicurezza.

Si rivolge a tutti i profili coinvolti: utenti, hobbisti, amministratori, manager.

- BugTraq
- Vulnerability database (bid)
- Letteratura (Adv., Vulns., Infocus)

Siti utili

Sectools

<http://www.sectools.org/>

Dai creatori di Nmap <http://nmap.org/>

Top 125 Network Security Tools

Catalogazione iniziata intorno al 2001,

poi passato a classifica annuale, ora

aggiornati praticamente in tempo reale.

CLUSIT

CLUSIT: Dal 2000 al servizio della sicurezza delle informazioni

<http://clusit.it/>

La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per far fronte ai problemi della sicurezza informatica.

Il CLUSIT nasce sulla scorta delle esperienze di varie associazioni europee per la sicurezza informatica che costituiscono un punto di riferimento nei rispettivi paesi da oltre 20 anni.

Il CLUSIT è aperto ad ogni persona e organizzazione che manifesti un interesse per la sicurezza informatica.

Siti utili

Open Threat Exchange

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

32

<https://otx.alienvault.com/>

Raccolta di dati in tempo reale su attacchi in corso.

“online threat intelligence among more than 47,000 participants in 140 countries who contribute more than 4 million threat indicators daily”

Log di vari honeypot in giro per il mondo e su diverse piattaforme.

Siti utili

Altri 1000 ...

SenderBase <http://www.senderbase.org/> The world's largest Email and Web traffic monitoring network

Lonerunners <http://www.lonerunners.net/> Information security and security tools.

Packet Storm <http://packetstormsecurity.com/> Global Security Resources

CIRT <http://cirt.net/> “Suspicion Breeds Confidence”

Matteo Flora <https://mgpf.it/>

EFF Electronic Frontier Foundation <https://www.eff.org/>

“The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world.”

(IN)secure Magazine <http://www.net-security.org/> Free digital security publication discussing some of the hottest information security topics.

Progetto Winston Smith <http://www.winstonsmith.info/>
Privacy, tecnocontrollo, censura, anonimato, controllo informazione.