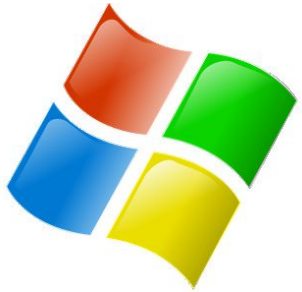
Corso di STATISTICA, INFORMATICA, ELABORAZIONE DELLE INFORMAZIONI

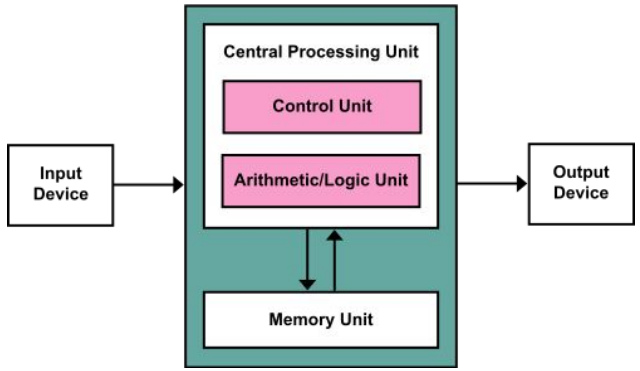
UNIVERSITÀ DEGLI STUDI DELLA BASILICATA

Modulo di Sistemi di Elaborazione delle Informazioni

Sicurezza del software

Docente:
Domenico Daniele Bloisi

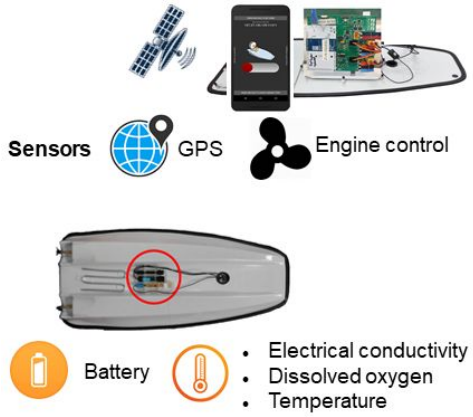


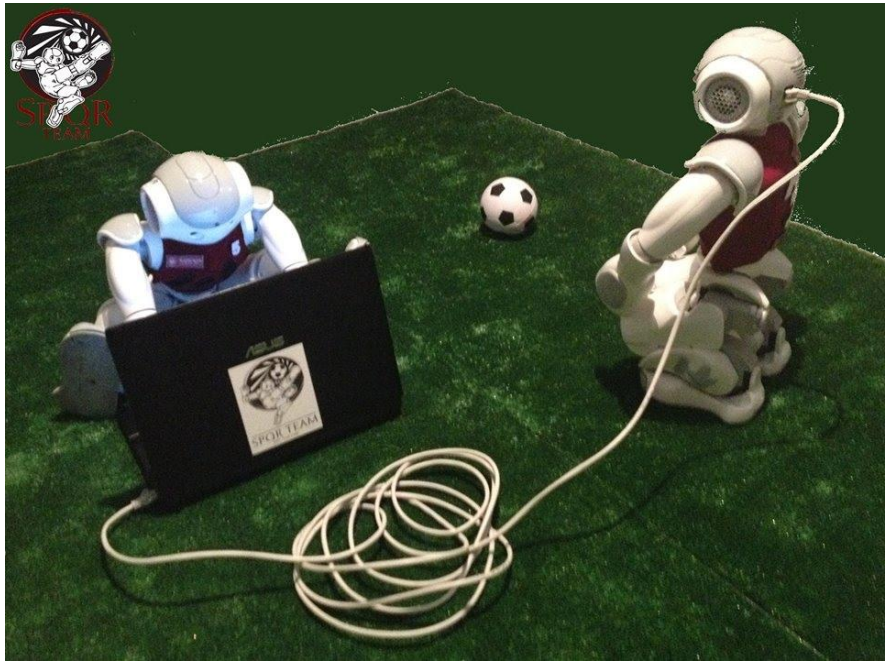


Domenico Daniele Bloisi

- Professore Associato
  Dipartimento di Matematica, Informatica ed Economia
  Università degli studi della Basilicata
  http://web.unibas.it/bloisi

- SPQR Robot Soccer Team
  Dipartimento di Informatica, Automatica e Gestionale Università degli studi di Roma “La Sapienza”
  http://spqr.diag.uniroma1.it



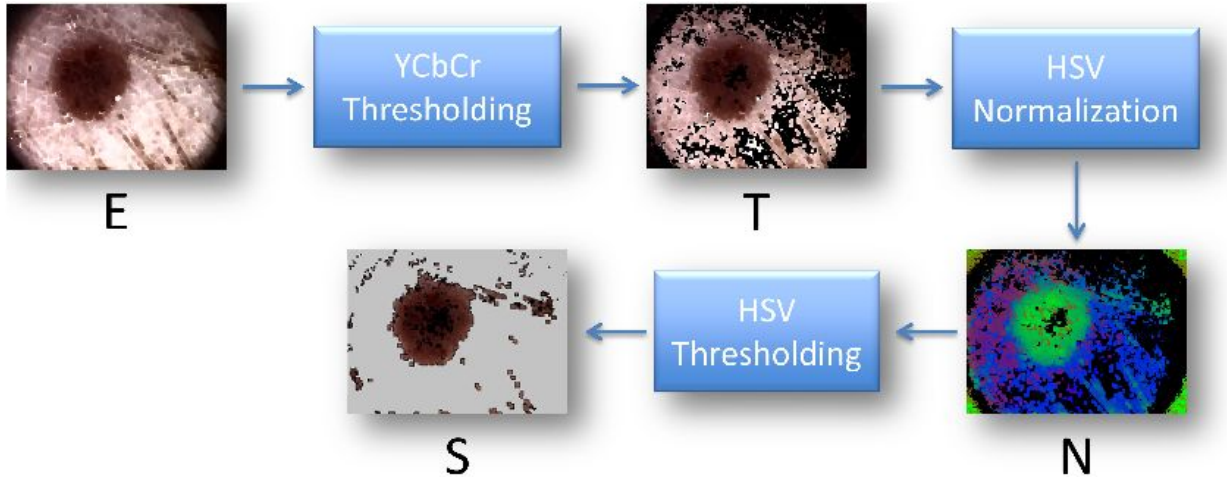


Interessi di ricerca

- Intelligent surveillance
- Robot vision
- Medical image analysis

https://youtu.be/2KHNZX7UIWQ

https://youtu.be/9a70Ucgbi_U



UNIBAS Wolves https://sites.google.com/unibas.it/wolves

- UNIBAS WOLVES is the robot soccer team of the University of Basilicata. Established in 2019, it is focussed on developing software for NAO soccer robots participating in RoboCup competitions.

- UNIBAS WOLVES team is twinned with SPQR Team at Sapienza University of Rome

https://youtu.be/ji0OmkaWh20

Informazioni sul corso

Il corso di STATISTICA, INFORMATICA, ELABORAZIONE DELLE INFORMAZIONI

- include 3 moduli:
  - SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI
    (il martedì - docente: Domenico Bloisi)
  - INFORMATICA
    (il mercoledì - docente: Enzo Veltri)
  - PROBABILITA' E STATISTICA MATEMATICA
    (il giovedì - docente: Antonella Iuliano)

- Periodo: I semestre ottobre 2022 – gennaio 2023

  - Martedì dalle 11:30 alle 14:00

Informazioni sul modulo

- Home page del modulo: https://web.unibas.it/bloisi/corsi/sei.html

- Martedì dalle 11:30 alle 13:30

Ricevimento Bloisi

- In presenza, durante il periodo delle lezioni:
  Lunedì dalle 17:00 alle 18:00 Edificio 3D, II piano, stanza 15
  Si invitano gli studenti a controllare regolarmente la bacheca degli avvisi per eventuali variazioni
- Tramite google Meet e al di fuori del periodo delle lezioni:
  da concordare con il docente tramite email

Per prenotare un appuntamento inviare una email a
domenico.bloisi@unibas.it

Sicurezza e protezione

Sicurezza e protezione

- La sicurezza misura la fiducia nel fatto che l'integrità di un sistema e dei suoi dati siano preservati

- La protezione è l'insieme di meccanismi che controllano l'accesso di processi e utenti alle risorse di un sistema informatico

Sicurezza

La sicurezza si occupa di preservare le risorse del sistema da:

- ✔ accessi non autorizzati
- ✔ distruzione o alterazione dolosa
- ✔ involontaria introduzione di elementi di incoerenza

Risorse da preservare

Le risorse da preservare includono:

- ✔ informazione memorizzata nel sistema sotto forma di dati e programmi
- ✔ CPU
- ✔ memoria
- ✔ dischi
- ✔ connessioni di rete

Il problema della sicurezza

Le violazioni della sicurezza del sistema si possono classificare come *intenzionali* (*dolose*) o *accidentali*. Nell'elenco che segue sono comprese sia le *intrusioni accidentali* sia le *violazioni dolose*.

- Violazione della riservatezza
- Compromissione dell'integrità
- Violazione della disponibilità
- Appropriazione del servizio
- Rifiuto del servizio
  DOS
  (*Denial-Of-Service*)

Il problema della sicurezza

Violazione della riservatezza

- Lettura non autorizzata di dati
- Furto di informazioni

Compromissione dell'integrità

- Modifica non autorizzata di dati
- Modifica codice sorgente

Violazione della disponibilità

- Distruzione non autorizzata di dati
- Sabotaggio di siti web

Il problema della sicurezza

Appropriazione del servizio

- Uso non autorizzato delle risorse

Rifiuto del servizio

- Blocco dell'utilizzo legittimo del sistema
- Attacchi DOS (Denial-Of-Service)

Sicurezza del sistema

Per proteggere il sistema è necessario prendere misure di sicurezza a quattro livelli:

Sicurezza del sistema

Fisico

- Edifici
- Macchine
- Stazioni di lavoro
- Terminali

Rete

- Linee di comunicazione private
- Linee condivise
- Connessioni Wi-Fi

Sicurezza del sistema

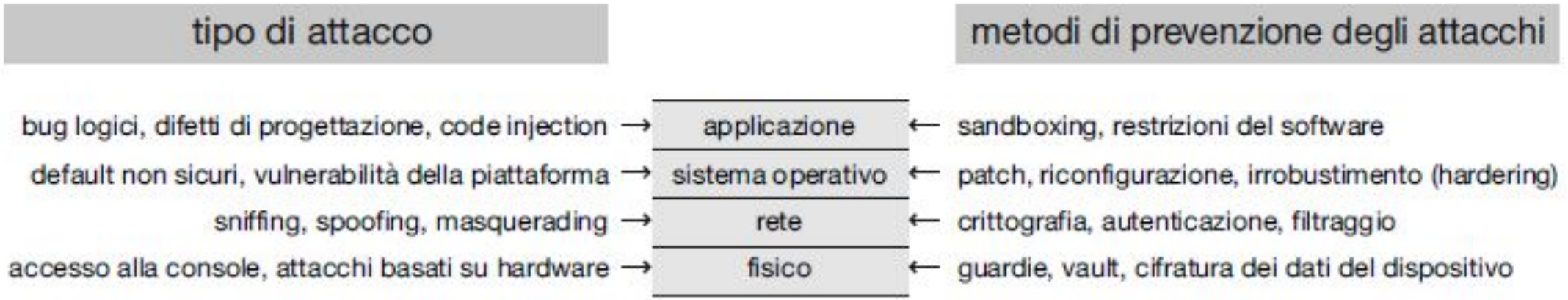
SO

- Impostazioni predefinite
- Parametri di configurazione
- Bug di sicurezza

Applicazione

- Programmi di terze parti
- Bug di sicurezza

Modello di sicurezza a quattro livelli



Il modello di sicurezza a quattro livelli è come una catena formata da anelli collegati: una vulnerabilità in uno qualsiasi dei suoi livelli può compromettere l'intero sistema.

Fattore umano

- L’autorizzazione degli utenti richiede cautela per garantire l’accesso al sistema solo agli utenti che ne abbiano diritto.

- Anche gli utenti autorizzati potrebbero essere malintenzionati oppure incoraggiati a cedere le loro credenziali ad altri volontariamente o mediante tecniche di ingegneria sociale (social engineering).

Phishing

consiste nel contraffare e-mail o pagine web rendendole simili a quelle autentiche per spingere gli utenti tratti in inganno a comunicare informazioni confidenziali

Esempio di phishing

Italia Attualità

Temi Caldi Libia Usa 2020 Piano Autostrade Taglio cuneo fiscale Debito Italia

24+ ABBONATI Accedi

ITALIA Reddito di cittadinanza, ecco che lavori faranno i percettori

MONDO L'abbattimento del Boeing 737-800 nei cieli di Teheran

IL MILANESE IMBRUTTITO L'economia spiegata dal Nano: il mutuo

23 dicembre 2019

Natale
Iban
Ing Bank
NoiPA
CONSOB

Salva
Commenta

CYBER SICUREZZA

Truffa di Natale: hacker contro NoiPA, rubati stipendi e tredicesime a dipendenti pubblici

Operazione basata su tecniche di phishing, che riguarderebbe un numero non definito di dipendenti pubblici. Un furto che lascia spazio a molti interrogativi e al pesante dubbio di non poter recuperare il maltolto

di Biagio Simonetta

Il meglio di 24+

1. OCCUPAZIONE
Lavoro, richiesta record di laureati. Quali sono i titoli più gettonati

2. 24PLUS
Auto elettriche, perché è urgente l'alternativa al cobalto nelle batterie

3. REDDITI
Negli ultimi 20 anni le pensioni italiane sono cresciute più degli stipendi

4. L'INCHIESTA DELLA DOMENICA
Quali sono le scuole che fanno trovare più velocemente il lavoro

5. INDUSTRIA SOSTENIBILE
La sfida difficile di Volkswagen, Daimler e Bmw verso l'auto elettrica

https://www.ilsole24ore.com/art/truffa-natale-hacker-contro-noipa-rubati-stipendi-e-tredicesime-dipendenti-pubblici-ACtqa77

Sicurezza del software di base

Riferimenti e Credits

- Il contenuto di questa sezione deriva dal documento Linee Guida per la configurazione per adeguare la sicurezza del software di base scaricabile al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/allegato_3_-_linee_guida_per_la_configurazione_per_adeguare_la_sicurezza_del_software_di_base.pdf

Sicurezza degli applicativi

La sicurezza del software di base ed applicativo richiede di stabilire un processo volto ad identificare rischi e contromisure di sicurezza ad ogni livello (fisico, logico e organizzativo) del contesto in cui tali software operano e sono utilizzati.

Attacchi informatici

- L’apertura delle applicazioni verso fornitori, clienti, utenti remoti e mobili ha comportato la scomparsa di un perimetro aziendale definito e un’estrema diversificazione delle minacce. In questo nuovo scenario, le applicazioni sono diventate il principale vettore di attacco ed è sempre più difficile proteggerle.

- Il Rapporto dell’Osservatorio sugli attacchi digitali (datato 2017) evidenzia come principale causa degli attacchi applicativi in Italia siano le vulnerabilità delle infrastrutture ICT, del software di base e dei middleware usati dalle applicazioni (circa il 37%). Seguono poi le vulnerabilità intrinseche all'applicativo stesso quali, ad esempio, quelle dei sistemi di identificazione, autenticazione e controllo degli accessi.

Attacchi informatici

- Il Rapporto Clusit del 2019 evidenzia un trend di crescita degli attacchi sia in termini quantitativi che in termini di gravità dei danni prodotti.

- Il rapporto riporta quanto segue “Nell’ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la Severity media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.”

Sicurezza dei Sistemi Operativi

Sicurezza di Windows

La versione di default di un server o una workstation Windows potrebbe non disporre di tutte le misure di sicurezza necessarie per essere impiegato direttamente in un contesto di produzione, anche se Microsoft negli ultimi anni ha notevolmente migliorato la configurazione predefinita in ciascuna versione del sistema operativo.

Tenere aggiornata l'installazione di Windows

- Probabilmente il passo più importante da fare è controllare la presenza degli ultimi aggiornamenti di sicurezza e le patch disponibili per il sistema operativo Windows.
- E' possibile in Windows ottenere automaticamente gli aggiornamenti di sicurezza.
- Dopo aver verificato la disponibilità di aggiornamenti, tenere attivo l'aggiornamento automatico al fine di scaricare e installare gli aggiornamenti maggiormente importanti che possono essere di aiuto a proteggere la postazione di lavoro/server da possibili nuovi virus o malware.

Aggiornare il software installato

- Non è necessario aggiornare solo il sistema operativo, ma anche il software in esso installato.
- Pertanto, anche in questo caso è opportuno assicurarsi che vengano installati gli ultimi aggiornamenti e le patch di sicurezza per i programmi e le applicazioni principali presenti nel sistema.

Creare un punto di ripristino

- Se si sono già installati gli aggiornamenti di sicurezza per il sistema operativo, il passaggio successivo è creare un punto di ripristino di Windows.
- Dopo aver installato Windows, è possibile creare il punto di ripristino e denominarlo "Installazione pulita" e continuare con l'installazione dei driver e delle applicazioni necessarie alla destinazione d’uso della macchina

Installare un software antivirus

- Nel prendere in considerazione l'installazione di un programma antivirus, assicurarsi di utilizzarne uno certificato da una azienda riconosciuta, in quanto si potrebbe incorrere in programmi antivirus falsi.
- È importante disporre sul sistema di una soluzione di sicurezza affidabile, che dovrebbe prevedere la scansione in tempo reale, l'aggiornamento automatico del software e delle ultime vulnerabilità/minacce nonché di un firewall.

Adottare una soluzione di sicurezza proattiva

- L'utilizzo di un antivirus tradizionale non è più la soluzione ideale, semplicemente perché non riesce a tenere il passo con l'ascesa di nuove e avanzate minacce presenti online.

- Il malware di nuova generazione di solito ha la capacità di eludere il rilevamento e aggirare il software antivirus che gli utenti hanno installato sulle proprie postazioni di lavoro al fine di mantenere i propri dati al sicuro.

Adottare una soluzione di sicurezza proattiva

- Con l'aiuto di una soluzione di sicurezza informatica proattiva, è possibile ottenere una migliore protezione contro malware di carattere finanziario e di furto di dati, come Zeus o Cryptolocker.

- Ad esempio, per migliorare il controllo finanziario di un conto bancario online, è sempre possibile impostare degli avvisi inviati dalla banca per tenere traccia dell'attività svolta sul conto, applicando questo semplice ed efficace criterio come misura proattiva di sicurezza.

Eseguire il backup del sistema

- Le pratiche precedentemente descritte hanno lo scopo di proteggere il sistema da software dannoso e minacce online, ma si potrebbero comunque riscontrare problemi hardware che potrebbero mettere in pericolo le informazioni riservate presenti nel sistema stesso.
- Per garantire che i dati rimangano al sicuro, si dovrebbe utilizzare una duplice strategia, che dovrebbe includere la combinazione di un utilizzo di un disco rigido esterno con un servizio di backup online.

Eseguire il backup del sistema

- E' opportuno sottolineare l'importanza di disporre di una soluzione di backup capace di fornire stabilità, facile da usare, che consenta di sincronizzare i file di sistema con un server di backup online e che disponga di capacità di sicurezza, come la crittografia.

- A prescindere, è sempre comunque possibile utilizzare il sistema di backup di Windows

Utilizzare account di utente standard

- Windows fornisce un certo livello di diritti e privilegi a seconda del tipo di account utente in uso.
- È possibile utilizzare un account utente standard o un account utente amministratore.
- Al fine di proteggere il sistema, è consigliabile l'utilizzo di account standard per impedire agli utenti di apportare modifiche che interesserebbero tutti coloro che utilizzano la macchina, come ad esempio la cancellazione di importanti file di Windows necessari per il sistema.

Utilizzare account di utente standard

- Con un account utente standard, si hanno diritti limitati e non è possibile, ad esempio, cambiare le impostazioni di sistema o installare nuove applicazioni software, cambiare il nome dell’utente e la relativa password.
- Per le normali attività si dovrebbe usare un account standard.
- Se fosse necessario installare un'applicazione o apportare modifiche di sicurezza, ciò lo si dovrebbe fare solo con un account amministratore.
- E' inoltre una buona pratica di sicurezza impostare una password complessa per ciascun account di Windows.

Mantenere abilitato il controllo dell’account

- Lo "User Account Control" anche detto UAC è una funzionalità di sicurezza essenziale di Windows che impedisce modifiche non autorizzate al sistema operativo.
- Spesso si ha la tendenza a disabilitarlo dopo aver installato/reinstallato il sistema operativo.
- Come si può ben comprendere, non è consigliabile disattivarlo.

Mantenere abilitato il controllo dell’account

- L'UAC controlla quali modifiche potranno essere apportate al computer. Quando viene rilevata una modifica importante, come l'installazione di un programma o la rimozione di un'applicazione, viene visualizzato l'UAC che richiede un'autorizzazione a livello di amministratore.

- Nel caso in cui l'account utente sia infetto da malware, l'UAC aiuta a impedire che programmi e attività sospette apportino modifiche al sistema.

Crittografare il disco rigido

- Anche se si imposta una password di account per l'accesso al sistema, soggetti malintenzionati possono comunque ottenere l'accesso non autorizzato ai file e documenti privati dell'account.
- Questi vi possono accedere semplicemente avviando la macchina con un proprio sistema operativo, ad esempio Linux, da un disco esterno o un'unità flash USB. In tal caso, una delle possibili soluzioni è quella di crittografare il disco rigido in modo tale da proteggere i file sensibili in esso memorizzati.

BitLocker

- Uno strumento di crittografia gratuito che è possibile utilizzare è BitLocker, disponibile anche per le ultime versioni di Windows.
- Dopo aver abilitato la protezione BitLocker, non si noterà alcuna differenza e si potrà semplicemente accedere al sistema inserendo la normale password dell'account utente di Windows.

Vantaggi di BitLocker

I vantaggi apportati dall'utilizzo di questo strumento di crittografia sono:

1. La possibilità di cifrare l'intero disco, il che rende impossibile per i soggetti malintenzionati prelevare il laptop per rimuovere il disco rigido e leggere i file.
2. La facilità d'uso e la totale integrazione con il sistema operativo Windows, quindi non è necessario aggiungere altro software crittografico.

Proteggere il browser web predefinito

- Un'altra cosa da fare dopo l'installazione di Windows è quella di prestare particolare attenzione alla sicurezza del browser web.
- Poiché il browser Web è lo strumento principale utilizzato per accedere a Internet, è importante tenerlo al sicuro prima di connettersi online.

Proteggere il browser web predefinito

- Le vulnerabilità presenti nel browser web sono come una porta aperta verso il sistema per i criminali informatici che trovano sempre modi creativi per raccogliere dati significativamente importanti.

- Ad esempio, se si utilizza Adobe Flash, prestare attenzione alle difettosità di sicurezza di quest'ultimo e al modo in cui può esporre il sistema agli attacchi.

Proteggere il browser web predefinito

Per rimanere al sicuro durante la navigazione sul Web, attenersi in generale alle seguenti regole:

1. Scegliere l'ultima versione del browser in uso.
2. Tenere il software del browser aggiornato.
3. Scegliere una sessione di navigazione privata quando si accede a un sito Web di cui non si è sicuri. La scelta di tale modalità impedirà che le credenziali (o i cookie) di autenticazione vengano archiviate e sottratte indebitamente dagli aggressori.

Manipolazione dei cookie

- I cookie sono suscettibili a modifiche da parte del client. Ciò è vero sia per i cookie persistenti che per quelli che risiedono in memoria.
- Sono disponibili diversi strumenti per supportare un aggressore nella modifica del contenuto di un cookie residente in memoria.
- La manipolazione del cookie è l'attacco che si riferisce alla modifica di un cookie, si effettua di solito per ottenere un accesso non autorizzato ad un sito Web.

Popup

- Poiché un eventuale malware capace di sottrarre dati potrebbe diffondersi anche nei siti Web legittimi attraverso del codice dannoso presente all'interno delle finestre popup, è buona norma assicurarsi che il browser web sia preimpostato per bloccare i popup.

Sicurezza dei Web Browser

Minacce a livello Architettura

- Accesso non autorizzato al sistema
- Violazione della sicurezza, rispetto alle politiche di sicurezza dell’organizzazione
- Violazione di leggi, di regolamenti, di obblighi contrattuali.

Contromisure a livello Architettura

- Utilizzare un sistema di protezione del perimetro (Firewall), posizionato tra la rete dei client e tutte le altre.
- Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) in grado di analizzare le richieste Web.
- Impedire la manipolazione DNS: utilizzare DNS attendibile e protetto.
- Bloccare i punti di accesso wireless e utilizzare un sistema di protezione come WiFi Protected Access 2 e access point con firmware aggiornato

Contromisure a livello Architettura

- Nota Bene. Si tenga presente che i dispositivi portatili personali possono eludere tali contromisure.

Configurazione sicura (hardening)

Possibili minacce:

- Accesso non autorizzato al sistema.
- Compromissione delle comunicazioni.
- Furto di credenziali di autenticazione (es. keylogger).
- Violazione della sicurezza, rispetto alle politiche di sicurezza dell’organizzazione.

Contromisure

- Utilizzare il browser con un account utente a bassi privilegi (ovvero senza privilegi di amministratore) in modo da limitare le possibilità di un attacco (security exploit) di compromettere l'intero sistema operativo.

- Impostare il browser in modo da controllare la validità dei certificati presentati dai server, utilizzando le liste di revoca dei certificati (CRL), l'Online Certificate Status Protocol (OCSP), o altri meccanismi equivalenti.

Contromisure

Limitare/Disabilitare/Condizionare l'uso di:

- Controlli ActiveX
- Add-ons
- Estensioni del browser (plug-ins)
- JavaScript e Flash
- Java Applets e applicazioni Silverlight.
- “Mobile code” in generale.

Contromisure

- Valutare l’adozione di estensioni e plugin di terze parti create a scopo di hardening del browser.
- A titolo di esempio:
  - il software “NoScript” che consente l’esecuzione di contenuti web basati su JavaScript, Java, Flash, Silverlight e altri plug-in solo se il sito è considerato attendibile ossia è stato precedentemente aggiunto a una white list.
  - Valutare l’adozione del software “MyWOT/WOT” (Web of Trust) che fornisce un servizio di reputazione sul livello di trust dei siti web.

LiveCD

- Considerare di utilizzare il browser all’interno di un LiveCD. I LiveCD, che forniscono un sistema operativo da una sorgente non scrivibile e sono tipicamente dotati di browser Internet.

- Se l'immagine originale LiveCD è priva di malware, tutto il software utilizzato, incluso il browser Internet, verrà caricato malware-free ogni volta che viene eseguito il boot dall'immagine LiveCD.

Ulteriori minacce alla sicurezza dei browser

- Accesso non autorizzato alle informazioni.
- Violazione della sicurezza, rispetto alle politiche di sicurezza dell’organizzazione (phishing e malware).

Contromisure

- Disabilitare la memorizzazione di password nel browser.
- Quasi tutti i browser e molti siti web in genere offrono la possibilità di ricordare le password per uso futuro.
- L'attivazione di questa funzionalità memorizza le password in un'unica posizione sul computer, rendendo più facile per un aggressore scoprirle se il sistema venisse compromesso.
- Se questa funzionalità risulta abilitata, è necessario disattivarla e cancellare le password memorizzate.

Contromisure

- Attivare il blocco dei popup del browser. Le finestre di popup sono una notevole tecnica di "phishing".
- Il blocco dei popup è oggi una funzionalità standard dei browser e dovrebbe essere abilitato ogni volta che si naviga sul web.
- Può essere utilizzata anche su siti web specifici e non su altri, dove i popup potrebbero invece essere necessari.

Privacy durante la navigazione web

Minaccia

- Divulgazione di informazioni riservate

Contromisure

Adottare le seguenti misure a salvaguardia della privacy degli utenti, rispetto ai siti Web che monitorano le attività utente:

- Impostare una routine specifica per eliminare i cookie regolarmente.
- Alcuni cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati.
- Non sempre è possibile bloccare i cookie, ma è opportuno eliminarli (diversamente i cookie possono rimanere memorizzati nel sistema per settimane o più)

Contromisure

- Attivare funzionalità “Do Not Track”.
- “Do Not Track” è un header HTTP che comunica ai siti visitati e alle terze parti i cui contenuti sono ospitati in tali siti che le proprie attività non devono essere tracciate.
- Nota Bene. L'invio di una richiesta “Do Not Track” ai siti non garantisce la protezione della privacy. I siti possono scegliere di rispettare la richiesta o continuare a eseguire attività che potrebbero essere considerate di monitoraggio anche se è stata espressa questa preferenza.

Contromisure

- Utilizzare la navigazione anonima.
- Nota Bene. Il livello di protezione è diverso a seconda dei browser. In certi casi si tratta di una difesa da attacchi locali: alcune info, come le password, la cronologia di ricerca e la cronologia delle pagine, vengono eliminate alla chiusura della scheda. In altri casi si tratta della difesa dall’attaccante esterno ossia viene protetto l'anonimato durante la navigazione.

Georeferenziazione

- Disattivare la condivisione della posizione geografica.

Metadati

Universo digitale

- Un articolo de Il Sole 24 Ore* riporta che l'intero universo digitale ha una dimensione di 44 zettabyte, cioè 44 triliardi di byte (circa 40 volte il numero di stelle osservabili nell'universo)

- Ogni giorno vengono
  - pubblicati 500 milioni di tweet
  - inviate 294 miliardi di e-mail
  - creati su Facebook 4 petabyte (cioè 4 biliardi di byte) di dati
  - inviati su WhatsApp 65 miliardi di messaggi.

*https://www.infodata.ilsole24ore.com/2019/05/14/quanti-dati-sono-generati-in-un-giorno/

Metadato

- Ai file presenti nell’universo digitale possono essere associate delle informazioni “extra”, che sono del tutto invisibili agli utenti meno esperti.

- Si tratta di informazioni che servono a descrivere il contenuto di tali file. Quindi, poiché un file contiene dei dati, le informazioni che descrivono il contenuto di un file prendono il nome di metadati (il prefisso meta- deriva dal greco e indica "qualcosa che sta sopra")

- La definizione più semplice che si può dare alla parola metadato è "dato che serve a descrivere un altro dato"

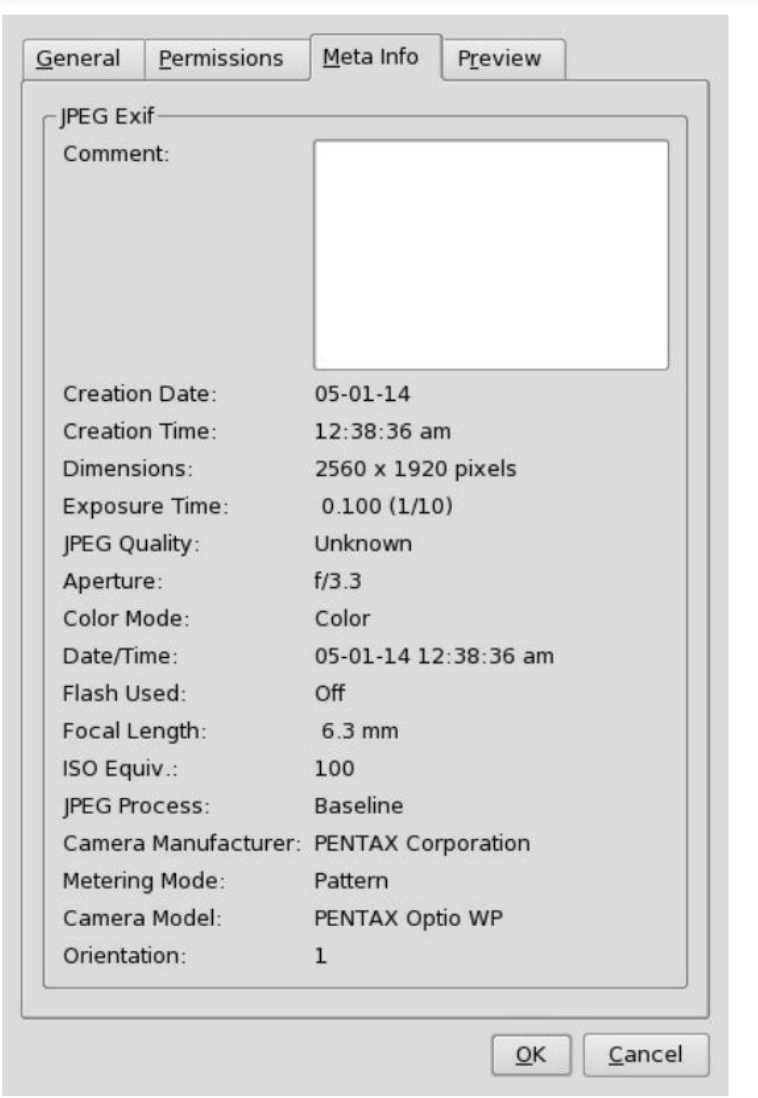
Tipologie di Metadato

I metadati sono raggruppabili in tre macro-categorie:

1. Descrittivi. Sono metadati che descrivono il contenuto del documento.
2. Strutturali. Sono una tipologia di metadati che contengono informazioni sulla persistenza fisica e logica del documento, la loro mappatura permette di tenere sotto controllo dove fisicamente risiedono i file.
3. Gestionali. Sottendono alla gestione dei documenti e alla loro amministrazione. Possono contenere informazioni sui diritti d'accesso, su quando e come procedere allo scarto quando sarà il momento, su chi sia il custode di quei file.

Esempio Metadati

- Le tipologie di metadati, a causa della loro eterogeneità, non hanno uno standard.
- Per esempio, le immagini hanno tre formati diversi di metadati (EXIF, IPTC e XMP), ognuno con una propria funzione specifica.



Importanza dei metadati

- I metadati ricoprono un ruolo essenziale laddove i dati sono esposti a utenti terzi e a software

- I metadati, infatti, consentono una maggiore comprensione e rappresentano la chiave attraverso cui abilitare più agevolmente la ricerca, la scoperta, l'accesso e quindi il riuso dei dati stessi

Il caso REPORT

- Un’indagine della trasmissione Report ha portato alla luce un retroscena sconvolgente sulla gestione della pandemia in seguito alla diffusione del COVID-19.

https://www.rai.it/programmi/report/inchieste/Il-parafulmine-a7d91226-ac48-408b-bb43-35ef5992817b.html

Il caso REPORT

- Tramite la lettura dei metadati del documento pubblico intitolato PIANO NAZIONALE DI PREPARAZIONE E RISPOSTA AD UNA PANDEMIA INFLUENZALE, disponibile al momento dell'indagine di REPORT sul sito del governo, è stato possibile evincere che, nonostante la data di caricamento del file fosse 15 dicembre 2016, la data di ultima modifica del documento pdf prima del caricamento risaliva al 10 febbraio 2006.

Il caso REPORT

- il documento quindi non era mai stato aggiornato dal 2006, nonostante la data di caricamento risalisse al 2016.

- Questo potrebbe aver contribuito a farci trovare impreparati nell'affrontare una pandemia come quella del 2019/2020.

Proprietà	Valore
Title	Microsoft Word - PIAN...
Author	Paolillo
Subject	
Keywords	
Creator	PScript5.dll Version 5.2
Producer	Acrobat Distiller 5.0.5 ...
Trapped	
Creation Date	2006.02.10 at 15:02:1...
Modification Date	2006.02.10 at 15:05:3...

Il caso Aaron Schock

- Il politico repubblicano dell'Illinois Aaron Schock era conosciuto come il deputato "più fotogenico" d'America.

- Sul suo account Instagram postava foto in pose eccentriche e bizzarre in luoghi esotici.

Il caso Aaron Schock

- Aaron Schock ha pubblicato foto di se stesso sulla neve, su spiagge esotiche e su aerei privati.
- Questo ha portato gli elettori a chiedersi se fossero viaggi di lavoro oppure vacanze.

Il caso Aaron Schock

- L'Associated Press (AP) ha avviato un'indagine che ha estratto i metadati di geolocalizzazione dalle foto che Schock ha pubblicato e taggato insieme alla sua posizione sul suo account Instagram.
- I metadati sono stati confrontati con le spese di viaggio che Schock stava dichiarando come spese della sua campagna.
- In particolare, l'AP ha comparato le registrazioni degli scali aeroportuali con i dati estratti dal suo account Instagram e ha scoperto che i soldi dei contribuenti e i fondi della campagna erano stati spesi per voli con aerei privati.

Il caso Aaron Schock

- Non è stato solo l’account Instagram di Schock a incastrarlo.
- Il post di uno stagista di Schock che mostra un’immagine di un concerto di Katy Perry con lo slogan "Non puoi dire di no quando il tuo capo ti invita", è stato collegato a una fattura da 1.928 dollari pagata al servizio di biglietteria StubHub.com indicato come "evento di raccolta fondi" a spese di Schock.
- L’AP ha pubblicato i suoi risultati il 24 febbraio 2015
- Il 17 marzo 2015 Schock ha annunciato le sue dimissioni dal Congresso

Tag di geolocalizzazione

- Questo cartello è stato affisso dai ranger che hanno il compito di proteggere le specie a rischio estinzione dai bracconieri
- si chiede ai visitatori di disattivare la geo-localizzazione dei propri dispositivi prima di scattare le foto

- se pubblicate sui social, quelle foto potrebbero fornire informazioni ai bracconieri sui luoghi solitamente visitati dai rinoceronti

Tag di geolocalizzazione

- Conoscere i metadati e utilizzarli al meglio è fondamentale per l'autotutela e la tutela del proprio lavoro.

- È importante saper tutelare se stessi e il proprio lavoro in relazione ai metadati che generiamo, in particolare se si ha a che fare con dati sensibili.

- Che siano esposti, eliminati o aggiunti e verificati, utilizzati da soli o incrociati con altri dati trovati attraverso altre fonti (convenzionali o meno), i metadati possono diventare una potente fonte di informazione di cui è bene avere comprensione.

Buone pratiche

Alcune buone pratiche

- Non fare clic su collegamenti senza considerare i rischi che ne potrebbero derivare (evitare di cliccare su link sospetti presenti nelle pagine).
- Prestare attenzione al fatto che gli indirizzi di pagine Web potrebbero essere mascherati e portare in un sito imprevisto.
- Considerare che ogni volta che un sito web richiede che vengano abilitate determinate funzionalità o installati software e aggiornamenti, si mette a rischio il computer. Ad es. non aggiornare mail il Flash Player su richiesta di una pagina web ma solo da pannello di controllo.

Alcune buone pratiche

- Non riutilizzare la stessa password per siti diversi.
- Non fornire mai online informazioni personali a meno di non essere certi che il sito sia valido e le transazioni sicure
- Prima di inserire qualsiasi informazione personale, controllare la barra degli URL del browser al fine di accertarsi che il sito sia quello atteso e che sia presente la dicitura "https:" e un'icona a forma di lucchetto ad indicare che la connessione al sito è protetta e che il certificato server è valido.

Alcune buone pratiche

- Evitare Wi-Fi pubblici o gratuiti: l’attaccante spesso utilizza sniffers wireless per rubare le informazioni degli utenti quando vengono inviate su reti non protette.

- Il modo migliore per proteggersi da questo attacco è evitare di utilizzare queste reti, oppure utilizzarle solo con una VPN che incapsuli tutto il traffico in un tunnel cifrato.

Alcune buone pratiche

- In caso di individuazione di una “falsa” pagina di autenticazione segnalarla al team di sicurezza interna all’organizzazione per procedere all’oscuramento della medesima e possibilmente all’individuazione dei responsabili.

Introduzione al Mobile e al Cloud Computing

Riferimenti e Credits

- Il contenuto di questa sezione deriva dal documento Manuale di abilitazione al cloud scaricabile al seguente link: https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/bozza/index.html

Cloud computing

- Il cloud computing (in italiano nuvola informatica), più semplicemente cloud, è un modello di infrastrutture informatiche che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, risorse di archiviazione, applicazioni software) che possono essere rapidamente erogate come servizio.

- Questo modello consente di semplificare drasticamente la gestione dei sistemi informativi, sia eliminando la gestione relativa ad applicativi fruibili direttamente online, sia trasformando le infrastrutture fisiche in servizi virtuali fruibili in base al consumo di risorse.

Strategia cloud della PA

- Cloud First: le PA devono, in via prioritaria, adottare il paradigma cloud prima di qualsiasi altra opzione tecnologica per la definizione di nuovi progetti e per la progettazione dei nuovi servizi nell'ambito di nuove iniziative da avviare
- Modello Cloud: si compone di infrastrutture e servizi qualificati da AgID sulla base di un insieme di requisiti volti a garantire elevati standard di qualità per la PA
- Cloud Enablement Program: il programma che abilita un'organizzazione a migrare il proprio patrimonio IT esistente (infrastrutture e applicazioni) utilizzando infrastrutture e servizi cloud all'interno del modello Cloud della PA.

Vantaggi del cloud

Il modello cloud consente di:

- usufruire delle applicazioni da qualsiasi dispositivo in qualsiasi luogo tramite l'accesso internet
- avere importanti vantaggi di costo nell'utilizzo del software, in quanto consente di pagare le risorse come servizi in base al consumo ("pay per use"), evitando investimenti iniziali nell'infrastruttura e costi legati alle licenze di utilizzo
- ridurre i costi complessivi collegati alla location dei data center (affitti, consumi elettrici, personale non ICT)
- avere maggiore flessibilità nel provare nuovi servizi o apportare modifiche, con costi accessibili

Vantaggi del cloud

- effettuare in maniera continua gli aggiornamenti dell’infrastruttura e delle applicazioni
- ridurre i rischi legati alla gestione della sicurezza (fisica e logica) delle infrastrutture IT

Corso di STATISTICA, INFORMATICA, ELABORAZIONE DELLE INFORMAZIONI

UNIVERSITÀ DEGLI STUDI DELLA BASILICATA

Modulo di Sistemi di Elaborazione delle Informazioni

Sicurezza del software

Docente:
Domenico Daniele Bloisi