Relazione cert

Minacce e Regole di comportamento

1 giugno 2019

Accenture

Milano, Italia

# INTRODUZIONE

In seguito alla richiesta lettura del documento pubblicato dall’agenzia CERT riguardante la Sicurezza Informatica, si scrive questa relazione sulla validità e veridicità dello stesso. Si aggiungono poi note e chiarimenti sui principali argomenti affrontati sottolineando i punti salienti.

Innanzitutto, in concordanza con il testo proposto, si fornisce una definizione chiara ed esaustiva di Sicurezza Informatica:

**“La sicurezza informatica può essere definita come l’insieme delle misure, di carattere organizzativo e tecnologico, atte a garantire l’autenticazione dell’utente, la disponibilità, l’integrità e la riservatezza delle informazioni e dei servizi, gestiti o erogati in modo digitale”.**

Nell’affermazione precedente si trova riscontro delle linee guida del modello CID (confidence, integrity, disponibility) sull’utilizzo e la fruibilità di dati.

Nella realtà odierna in cui la gestione di dati personali e l’utilizzo documenti sensibili è sempre più all’ordine del giorno, è necessario prendere coscienza sia dei rischi che intercorrono nell’utilizzo di dispositivi collegati alla rete, sia delle vulnerabilità insite all’interno di software utilizzati.

Di seguito quindi vengono stilati seguendo l’ordine di apparizione nel Documento del CERT gli argomenti trattati. Lo scritto è suddiviso in quattro paragrafi. Il primo paragrafo è riguardante i malware e la loro identificazione nelle diverse tipologie. Nel secondo paragrafo si affrontano i cookies, le problematiche dovute alle reti e le vulnerabilità by design già presenti nei codici degli applicativi e nei dispositivi in commercio. Questo paragrafo è stato aggiunto perché non è stata ritenuta valida l’associazione tra malware e i possibili rischi sopracitati, in quanto essi sono difetti non dovuti a codice malevolo. Nel terzo paragrafo si riportano le principali protezioni da installare e da utilizzare per la prevenzione e la messa in sicurezza del proprio dispositivo. Nel quarto e ultimo paragrafo vengono mostrate le best practice per un utilizzo sicuro ed appropriato del sistema informatico.

# MALWARE

In questo paragrafo vengono illustrati i principali malware e le loro caratteristiche. I malware sono progettati e diffusi per causare la perdita di dati personali, in riferimento sia all’utente che al pc, ma non solo, infatti essi sono spesso usati proprio allo scopo di ottenere informazioni o abitudini, in modo da poter progettare un attacco. Nel documento preso in esame i malware vengono giustamente definiti come tutti quei tipi di programmi che puntano a danneggiare il pc e gli utenti.

Le strutture più comuni vengono illustrati di seguito.

## Virus

Il virus è un programma composto da istruzioni elementari, esattamente da codice eseguibile, che punta a danneggiare il computer in modi diversi: possono esserci fenomeni di rallentamento, danneggiamenti o la completa distruzione di file. La sua particolarità è di legarsi ad altri programmi e di restare inattivo finché il programma non viene eseguito, in quel momento il virus tende a duplicarsi e legarsi ad altri programmi.

## Worm

I worm sono similari ai virus in quanto a scopo finale, si differenziano dal fatto che essi non necessitano di un file già esistente al quale legarsi, ma sono essi stessi programmi che oltre a creare disservizi, hanno la caratteristica di duplicarsi e sfruttando la vulnerabilità del sistema puntano a auto-trasmettersi sul web per infettare altri computer.

## Trojan

I trojan (letteralmente "cavalli di troia") sono dei malware che si nascondono in altri file che l'utente scarica ed esegue inconsciamente, attivando il trojan in esso contenuto. Gli hacker spesso usano questo programma malevolo per avere un accesso in remoto, ovviamente non autorizzato, a un computer, per infettare i file e danneggiare il sistema.

## Spyware e Adware

Gli spyware sono programmi che spiano e rubano i file all'utente, per trasmetterle ad un indirizzo pre-impostato.

Gli adware sono programmi nati per uso pubblicitario che analizzando la rete e le ricerche del “consumatore”, generano pubblicità mirate, spesso in ambito di spam, o con pop-up aggressivi che portano alla reale compromissione dell'esperienza sulla rete dell’utente.

# VULNERABILITÀ e RETE

Le successive voci mostrano i principali rischi che si corrono nella navigazione sul web e si fornisce una definizione di vulnerabilità. Spesso gli attacchi in rete vengono accompagnati dall’utilizzo o dall’installazione di malware come trojan o worms in allegato a mail e siti apparentemente innocui.

## Social Engineering

Gli attacchi di social engineering, sfruttano la disponibilità e la buona fede e l’insicurezza delle persone per accedere a dati confidenziali o indurre le vittime a effettuare determinate operazioni. Un classico esempio è indurre l’utente a fornire informazioni personali (come le coordinate bancarie) in seguito ad un presunto pagamento non avvenuto realmente.

## Phishing

Il phishing è una forma di attacco di social engineering. Esso consiste nell’adescamento da parte di hacker di vittime inesperte, alle quali rubano asset privati (password, username, codici bancari ecc..). Solitamente il malintenzionato si presenta con un'identità fittizia tramite email, presentando servizi simili o pagine note al soggetto e l'utente ignaro, immettendo i propri dati, viene truffato delle sue credenziali.

## Hoax

L’utente viene indotto a diffondere notizie palesemente notizie (le cosiddette catene di sant’Antonio) poiché fa leva su aspetti scaramantici o emotivi. Spesso questo fenomeno viene accompagnato dallo spam.

## Spam

Lo spam vien identificato in tutte quelle mail indesiderate, ripetute e fastidioso, spediti in maniera randomica e massiva, il fenomeno associato è denominato spamming e viene usato per campagne pubblicitarie o campagne pubblicitarie. I moderni servizi di post elettronica già integrano al loro interno servizi utili al riconoscimento e all’eliminazione istantanea di questo tipo di mail.

## Vulnerabilità

I malware non sono l'unica minaccia alla sicurezza; spesso le maggiori minacce provengono dalla non curanza degli utenti, e si viene minacciati e disturbati spesso da spam, phishing, e attacchi di social engineering.

Nel file sorgente di alcune applicazioni potrebbe essere presenti alcune vulnerabilità, come scritto nel documento CERT Il software installato sui nostri personal computer comprende decine di migliaia di righe di codice: non deve quindi sorprendere che vi possano essere contenuti alcuni errori ergo vulnerabilità.

Si può consultare inoltre il documento OWASP per una maggior chiarezze delle principali vulnerabilità nei software presenti nel mercato e i test con cui verificare la sicurezza di un’applicazione.

## Cookies

I cookies sono una raccolta di informazioni estrapolate dalla navigazione sul web. Essi contengono sia dati che metadati, quali ad esempio username e password inserite, percorso di ricerca e abitudini dell’utente. Essi però non presentano solo aspetti negativi poiché essi favoriscono l’esperienza in generale dell’utente, proponendo pubblicità mirate e aumentando la velocità di navigazione.

Si distinguono i persistent cookies dai session cookies. I primi hanno una data di scadenza decisa dall’applicazione web dopo la quale verranno eliminati, mentre i session cookies vengono cancellati alla chiusura del browser.

Grazie alle leggi (GDPR) i siti web devono comunicare al consumatore l’utilizzo dei cookies da parte del sito e lui stesso può decidere se accettarli o meno.

## Chat e Instant Messaging

La comunicazione offerta tramite l’utilizzo di internet. Utilizzare canali non riconosciuti o non sicuri può comportare a un’esposizione maggiore a malware e un attacco alle vulnerabilità. Usare chat di servizi riconosciuti evita di esporsi e quindi meno rischi per i propri dati.

## Wireless LAN

La definizione data nel documento CERT è molto chiara: con l'abbreviazione WLAN (“Wireless Local Area Network”) ci si riferisce a una “rete locale senza fili” in cui un dispositivo (ad es. un personal computer) comunica senza fili con un cosiddetto WLAN Access Point (“router”), collegato a sua volta a internet o a una rete.

È opportuno configurare per limitare l’accesso a solo dispositivi e ad utenti riconosciuti. Spesso si accompagna a una cifratura delle informazioni scambiate durante la comunicazione tra i diversi dispositivi della stessa rete, per impedire ad un eventuale sniffer esterno di comprendere i dati raccolti nell’immediato. Bisogna aver comunque consapevolezza che ogni comunicazione, seppur criptata, non può considerarsi sicura al 100%.

# PROTEZIONI

La protezione, in informatica, consiste nel prevenire operazioni illegittime sugli oggetti di un sistema informatico. I principali rischi sono preventivabili ed evitabili attraverso alcuni software e azioni semplici eseguibili direttamente dall’utente.

## Personal Firewall

Il firewall è un’estensione del sistema operativo utile alla difesa perimetrale di una rete informatica poiché svolge funzioni di regolatore di accessi. Grazie al firewall può essere ridotto il rischio di accesso non autorizzato da parte di hackers e minimizzato il pericolo di infiltrazione da parte di worm, trojan o spyware.

Si raccomanda quindi di installarne uno se non è già presente (solitamente i sistemi operativi più noti ne posseggono già uno di default). Il consiglio fornito dalla guida è molto valido, è buona norma attivarlo sempre prima di una connessione a internet ed avere sempre coscienza dell’impostazioni scelte.

## Software Updates

Gli aggiornamenti sono essenziali per una corretta messa in sicurezza, poiché vanno a colmare falle evidenziate all’interno dei software dopo la messa in commercio; talvolta si riscontrano vulnerabilità per le quali non esiste ancora alcun aggiornamento di sicurezza, sono le cosiddette "0-Day", esse compaiono quasi quotidianamente in molte applicazioni, tra cui anche i browser più utilizzati (Internet Explorer, Firefox, Chrome ecc.).

Una buona strategia sarebbe quella di avvalersi di un browser alternativo finché il problema non viene risolto dal provider.

## Antivirus

I precedenti metodi di protezione non sono sufficienti a garantire la completa sicurezza del sistema.

È necessario associare a quest'ultimi un software antivirus: esso mediante la scansione della memoria del computer, identifica, isola ed elimina i virus o parti di codice sospetto eventualmente presenti.

È indispensabile aggiornare costantemente l'antivirus (due o tre volte alla settimana) per cui bisogna regolarmente verificare la validità della licenza: in mancanza della stessa non avverrà l'installazione dei nuovi updates (vedi punto precedente).

## Protezione dei Dati

Come si evince dal documento CERT, per garantire la Business Continuity è utile effettuare regolarmente il backup su supporti esterni che devono essere conservati adeguatamente e controllati periodicamente. I server deputati alla funzione di backup devono essere installati in luoghi lontani o addirittura in zone geografiche totalmente diverse dalla sede di utilizzo dati. Questo è necessario per evitare tutti quegli inconvenienti, anche catastrofici, che possono colpire la sede principale, con il rischio di perdere sia i dati che i loro backup.

# BEST PRACTICE

I caposaldi di questo capitolo sono la prevenzione e la consapevolezza. Ogni azione, ogni decisone e ogni modifica, eseguita sia dall’utente che dai tecnici deve essere compiuta con un alto grado di awareness. Non bisogna mai sottovalutare, anche nella decisone più semplice, i rischi a cui si vanno incontro. Per un maggior approfondimento di questi campi si consiglia di consultare il manuale ITIL, che raccoglie le principali accortezze per quanto riguarda la sicurezza informatica.

## Password

La password deve essere di almeno 8 caratteri, meglio se di 12 o 16. Essa dovrebbe essere composta sia di caratteri alfanumerici che di caratteri speciali se consentito (alcuni Web Server non permettono l’inserimento di determinati caratteri, quindi bisogna prestare attenzione alle policy interne). A differenza di come scritto nel documento CERT è preferibile non inserire password contenenti frasi di senso compiuto. Si consiglia, in linea con quanto scritto nel documento CERT la modifica immediata dal momento in cui si presuma che essa sia stata sottratta e comunque è buona norma modificarla a intervalli regolari.

Si raccomanda che la password non deve essere MAI trascritta su documenti di testo sia virtuali che fisici, che non deve essere ripetuta in servizi differenti e deve essere facile da ricordare.

## Prudenza nella gestione delle Email

Diffidare sempre da email con mittente sconosciuto. Se la fonte non è verificata conviene non aprire gli allegati o mandare in esecuzione eventuale materiale scaricato. Per evitare eventuale SPAM si consiglia di non divulgare la propria Email a terzi non riconosciuti, e nel caso di ricezioni di email sospette evitare di rispondere per evitare di dimostrare che la propria casella di mail è attiva.

Prestare attenzione a mail contenenti allegati con due estensioni, solitamente sono sinonimo di truffa. Esempio “palla.jpg.exe”

## Prudenza nella navigazione in internet

Durante la navigazione bisogna prestare sempre molto attenzione ai siti web visitate e ai link a cui si viene reindirizzati. Seguendo le norme contenute nel documento CERT si suggerisce di:  
-Non scaricare mai programmi sconosciuti da internet prima di averne accertato la provenienza.  
-Scaricare gli aggiornamenti di software e driver esclusivamente dalla pagina web dei relativi produttori.  
-Non comunicare MAI le proprie credenziali, i provider di servizi hanno nei loro database le credenziali degli utenti, quindi è molto improbabile che vi vengano richieste.  
-È preferibile avvalersi di siti con protocollo HTTPS.  
-Effettuare sempre il logout prima della chiusura di un servizio.

Nel documento viene consigliato anche di disattivare le funzioni di Javascript. Questa indicazione rende alquanto limitante l’esperienza in rete, per questo si consiglia di non seguire questa ultima indicazione per evitare eventuali errori nel caricamento delle pagine.

## Configurazione del sistema

Come scritto nel documento CERT è opportuno assegnare una password efficace ad ogni utente disponibile. Prestare molta attenzione nel rilascio dei privilegi, è fondamentale minimizzare i privilegi per evitare accessi liberi e non autorizzati.

## Prudenza nella navigazione sulle reti “peer-to-peer”

Nel modello “peer-to-peer” ogni computer è contemporaneamente client e server, ossia offre e riceve prestazioni di servizi dagli altri computer della rete. L'utilizzo di questo metodo di comunicazione per lo scambio di files comporta alcuni rischi e un suo uso improprio avviene solitamente in diverse azioni illegali come la violazione dei diritti d'autore (la cosiddetta pirateria internet), la presenza di virus o l'involontario scambio di dati confidenziali.

Per questo si consiglia di avere molta prudenza nell’utilizzo di questo strumento e utilizzarlo solo per scopi legittimi e legali.

## Wireless LAN (reti “Wi-Fi”) e Reti Bluetooth

Come per le reti WiFi è opportuno seguire determinate indicazioni: attivare il Bluetooth e la visibilità dell'apparecchio solo quando necessario, adoperarlo solo in ambienti sicuri, e attivare le opzioni di sicurezza come l’autenticazione e la cifratura (meglio chiave WPA2 piuttosto che WEP, quest’ultima è completamente superata e infatti ritenuta non sicura).

Per quanto riguarda la configurazione del router, si consiglia di impedire che il router emetta regolarmente la propria identificazione di rete (SSID). Bisogna quindi disabilitare l’opzione Broadcast se possibile. Inoltre è buona norma modificare la password del router ad intervalli di tempo regolari.

**Sommario**

[INTRODUZIONE 1](#_Toc10127622)

[MALWARE 2](#_Toc10127623)

[Virus 2](#_Toc10127624)

[Worm 2](#_Toc10127625)

[Trojan 2](#_Toc10127626)

[Spyware e Adware 2](#_Toc10127627)

[Social Engineering 3](#_Toc10127628)

[Phishing 3](#_Toc10127629)

[VULNERABILITÀ e RETE 3](#_Toc10127630)

[Vulnerabilità 3](#_Toc10127631)

[Hoax 3](#_Toc10127632)

[Spam 3](#_Toc10127633)

[Cookies 3](#_Toc10127634)

[Chat e Instant Messaging 3](#_Toc10127635)

[Wireless LAN 4](#_Toc10127636)

[PROTEZIONI 5](#_Toc10127637)

[Personal Firewall 5](#_Toc10127638)

[Software Updates 5](#_Toc10127639)

[Antivirus 5](#_Toc10127640)

[Protezione dei Dati 5](#_Toc10127641)

[BEST PRACTICE 6](#_Toc10127642)

[Password 6](#_Toc10127643)

[Prudenza nella gestione delle Email 6](#_Toc10127644)

[Prudenza nella navigazione in internet 6](#_Toc10127645)

[Configurazione del sistema 6](#_Toc10127646)

[Prudenza nella navigazione sulle reti “peer-to-peer” 6](#_Toc10127647)

[Wireless LAN (reti “WiFi”) 6](#_Toc10127648)

[Reti Bluetooth 6](#_Toc10127649)