Sicurezza Informatica : minacce, difese, azioni

Indice

1 introduzione

1.1 obiettivi del materiale didattico

In questa seconda mappa del Modulo dedicato alla Sicurezza Informatica ci poniamo questi obiettivi:

- conoscere le principali minacce informatiche: le loro caratteristiche, i danni che possono provocare, le strategie e i livelli di difesa
- capire come funzionano gli strumenti principali di difesa
- comprendere come agire al meglio per sfruttare gli strumenti di difesa contro i rischi informatici

Con questa mappa completeremo il quadro d'insieme della Sicurezza Informatica per questo corso base.

2 le minacce per sistemi e dati

Conoscere i rischi significa adottare gli strumenti e i comportamenti più idonei alla difesa dei sistemi e dei dati coinvolti.
Iniziamo qui l'analisi dettagliata delle minacce informatiche più diffuse e/o pericolose.
Per ciascuna seguiremo lo schema già utilizzato nella prima mappa parlando di "phishing", ovvero questi passaggi:

- **cosa è e come si presenta** il rischio analizzato
- **che danni fa** ovvero il grado di pericolosità della minaccia
- **come ci si difende** che possiamo suddividere nelle 4 componenti :
- linee guida
- informazioni e istruzioni
- strumenti e tecnologia
- aggiornamento e controllo

2.1 spam

2.1.1 cos'è e come si presenta

Lo **spam** - letteralmente "spazzatura" - è posta elettronica commerciale non richiesta, l’equivalente elettronico dei volantini e dei cataloghi che intasano le cassette della posta.
I tipi di spam più diffusi riguardano:

- truffe informatiche (hai vinto la lotteria, c'è una miniera d'oro, ..., mi serve un collaboratore per girare soldi, ...); questa è quasi una categoria di spam a parte
- farmaci senza ricetta, farmaci che ingrandiscono o potenziano alcune parti del corpo, prodotti di erboristeria o cure dimagranti
- proposte di arricchimento facile e veloce che nascondono truffe a danno di chi risponde

- servizi finanziari, ad esempio offerte di mutuo o proposte per ridurre i debiti
- titoli e qualifiche, ad esempio la possibilità di acquistare diplomi, lauree o titoli professionali
- casinò e gioco d'azzardo online
- software a prezzi stracciati o pirata

A volte lo spam è "mascherato" da un oggetto con frasi molto personali, ad esempio "Scusa per ieri", o un messaggio di tipo professionale come "Devi rinnovare il tuo account", oppure una notifica di messaggio respinto.
Gli spammer spesso "truccano" le proprie mail per evitare i software anti-spam (Spam offuscato).
L'invio di spam genera un guadagno a chi le spedisce. Gli spammer possono infatti distribuire milioni di e-mail con un unico invio a un costo trascurabile; se riescono a prendere il controllo di altri computer per la spedizione, il costo è ancora più basso.
Se anche un solo destinatario su diecimila fa un acquisto, lo spammer ha ottenuto un guadagno.

2.1.1.1 "pescare" le caselle

Ma come fa lo spammer a trovare le caselle che poi farà oggetto di "posta spazzatura"?
Ci sono molte tecniche con cui l'identificativo della propria casella postale giunge a conoscenza di chi invia SPAM e spesso sono collegate ad altre minacce informatiche "andate a segno".

- **mediante virus**: quando un PC viene colpito da un virus, tipicamente questo, nel propagarsi, utilizza quanto trova nella posta locale per mimetizzarsi meglio. E' abituale che il virus utilizzi come mittenti gli indirizzi di mail ricevute, ma alcuni giungono a "riusare" anche il soggetto o il contenuto delle mail archiviate sul PC, per confezionare una mail più credibile. Il risultato è che tutto il suo indirizzario, compresi i contatti, le mail ricevute, ... , vengono "sparsi ai 4 venti" e questo arricchisce gli archivi degli spammers
- **mediante spyware**: scaricando qualche programmino simpatico o visitando qualche sito curioso, c'è il rischio di attivare dei software che hanno lo scopo di raccogliere informazioni "utili": nel caso più innocuo si tratta dei siti visitati, gli interessi personali, ad uso di iniziative commerciali mirate; nei casi più gravi c'è il furto delle credenziali di posta, bancarie, ecc.
- **mediante "catene di S. Antonio"**, ove lunghe liste di destinatari vengono passate da persona a persona
- **forum/mailing-list internet**: usando la propria casella per interagire con forum/mailing-list in internet di fatto si forniscono i propri riferimenti: anche il malintenzionato che si iscrive a forum/mailing-list ha accesso a tutte le mail che partecipano ai dibattiti. Per questi scopi non dovrebbe mai essere usata una casella istituzionale, ma piuttosto una "usa e getta", registrata in gmail, yahoo, ecc.
- **mediante tentativi**: inviando mail con destinatari "a caso" (per esempio mescolando "nomi" e "cognomi" dell'indirizzario: non è un caso che "michela.deserio" scriva a "michela.devisu" che risulta non esistere) e vedendo se vanno a buon fine

A seconda delle proprie abitudini più o meno virtuose e quanto più la mail viene usata con l'esterno, il coinvolgimento della propria mail in casi di SPAM sarà più o meno rapido.

2.1.1.2 spam offuscato

Lo **spam offuscato** è un messaggio di posta elettronica mascherato in modo da sfuggire ai software antispam.
Gli spammer sono costantemente alla ricerca di nuovi metodi per camuffare i propri messaggi e raggirare i software antispam, arrivando direttamente all'utente.
L'esempio più semplice è costituito dall'aggiunta di alcuni spazi tra le lettere di una parola, nella speranza che il software antispam non legga le lettere come un'unica parola, ad esempio
V I A G R A
Un altro metodo diffuso è quello di utilizzare un'ortografia scorretta oppure caratteri non standard, ad esempio:
V!agra
Questi trucchi sono comunque facili da individuare.
I metodi più avanzati sfruttano il codice HTML (il linguaggio utilizzato per scrivere le pagine web) all'interno delle e-mail. Questo permette agli spammer di creare messaggi che vengono visualizzati in maniera diversa dai software antispam.
Una parola può essere scritta utilizzando uno speciale codice HTML per ogni lettera. Il termine "Viagra", per esempio, può essere scritto digitando:
Viagr&#97
Il linguaggio HTML permette all'utente di vedere un determinato messaggio, mentre il programma antispam ne vede un altro che appare innocuo.
Il messaggio innocuo è dello stesso colore dello sfondo (white):
<body bgcolor=white> Viagra Hi, Johnny! It was nice to have dinner with you. </body>

2.1.2 che danni fa

Potremmo sintetizzare i danni dello SPAM in questi punti:

- lo spam fa perdere tempo alle persone, in ambito lavorativo e/o casalingo; gli utenti senza protezione anti-spam devono verificare ogni messaggio e cancellarlo
- gli utenti possono facilmente trascurare o cancellare messaggi importanti, scambiandoli per spam
- lo spam, come gli "hoax" allarmistici (vedi "hoax") e i virus via mail, occupa larghezza di banda e intasa le cartelle di posta degli utenti (fino a impedire la ricezione di nuova posta per raggiunti limiti di capienza)
- alcune messaggi spam sono offensivi; il datore di lavoro può essere ritenuto responsabile, in quanto è tenuto a garantire un ambiente di lavoro corretto e sicuro
- gli spammer usano spesso computer di altri utenti per inviare spam (vedi Zombie in "trojan-horse")

L'80% della posta elettronica in circolazione nel mondo è SPAM.

2.1.3 come ci si difende

2.1.3.1 linee guida

Azienda

- predisporre strumenti di difesa antispam e momenti formativi per il personale

Utente

- non eseguire operazioni che possano aumentare la probabilità di ricevere SPAM come ad esempio rispondere a SPAM, inserire la propria mail di lavoro in ambienti Internet visibili a tutti: gruppi, forum, ecc.
- proteggere e divulgare al minimo le caselle di posta utilizzate per scopi istituzionali o importanti, da usare per le comunicazioni che si vuole mantenere nel tempo (amici, rapporti di lavoro, ...)
- usare caselle diverse, "usa e getta", per interagire con ambienti poco sicuri (gruppi di discussione aperti o registrazione su siti in internet, ecc.)

2.1.3.2 istruzioni e informazioni

Non rispondere mai ad uno SPAM
In particolare non effettuare mai acquisti da un'e-mail non richiesta: effettuando un acquisto di questo tipo, si finanziano le attività di spamming; il proprio indirizzo di posta elettronica può essere aggiunto alle liste che vengono vendute agli spammer, quindi si rischia di ricevere molti più messaggi "spazzatura" e, cosa ancor più grave, si può essere vittima di una frode
Se non si conosce il mittente, cancellare il messaggio
La maggior parte dei messaggi spam non rappresenta una minaccia, ma causa solo fastidio. Tuttavia tali messaggi possono contenere virus in grado di danneggiare il computer all'apertura dell'e-mail
Non rispondere mai ai messaggi spam e ignorare i link al loro interno
Se si risponde allo spam, anche solo per richiedere di essere cancellati dalla mailing list, in realtà con questa operazione si conferma che l'indirizzo di posta è valido e si incoraggia gli spammer a spedire una maggiore quantità di messaggi

2.1.3.3 strumenti e tecnologia

utilizzare **un software di filtraggio** per proteggere il proprio client di posta
utilizzare un **software di filtraggio sul server di posta elettronica** per proteggere la propria azienda dallo spam e dalle minacce di virus, spyware e worm contenuti nelle e-mail

2.1.3.4 aggiornamenti e controlli

L'80% della posta elettronica in circolazione nel mondo è SPAM
Chi fa SPAM troverà sempre nuovi trucchi per inviare quantità sempre più massiccia di posta indesiderata e per superare gli strumenti automatici di difesa (sia quelli a livello server, sia quelli a livello PC).
Anche nella migliore ipotesi di ottenere un'efficacia elevatissima degli strumenti automatici e dei nostri comportamenti "corretti" (per es. il 99%), riceveremo comunque 1 o 2 messaggi di SPAM al giorno! Lo SPAM è un fastidio con cui dovremo convivere.

2.2 hoax e "catene"

2.2.1 cos'è e come si presenta

Una particolare forma di spamming è il cosiddetto **hoax** (in gergo italiano “bufala”): sono mail non richieste, inoltrate volontariamente da persone che inviano i messaggi hoax ricevuti alle caselle di amici, parenti, ecc. Possono essere notizie curiose, richieste di aiuto, evocazione di oscure disgrazie per chi avrebbe interrotto la catena degli inoltri, ecc. Quando questi messaggi invitano esplicitamente ad essere rispediti al maggior numero di persone, in modo da aumentarne la diffusione in maniera esponenziale, si parla di “**catena di Sant'Antonio**”.
Spesso gli hoax sono falsi allarmi su virus inesistenti.
Come riconoscere un falso allarme? Solitamente gli hoax sono messaggi di posta elettronica che si comportano, in tutto o in parte, in uno dei seguenti modi:

- segnalano la presenza di un virus altamente distruttivo che non può essere rilevato
- chiedono di non leggere messaggi di posta elettronica con un determinato oggetto, ad esempio “Budweiser Frogs”
- fanno credere che l’avvertimento provenga da un grande produttore di software, da un Internet Provider o da un’agenzia governativa, ad esempio IBM, Microsoft e AOL
- fanno credere che il nuovo virus possa fare qualcosa di assolutamente improbabile. Ad esempio, il falso allarme “A moment of silence” sosteneva che non era necessario alcun trasferimento di file affinché un nuovo computer venisse infettato
- usano il gergo tecnologico per descrivere gli effetti del virus. Ad esempio, “Good Times” afferma che il virus può portare il processore in “un ciclo binario infinito di ennesima complessità”
- spingono l’utente a inoltrare l’avvertimento e quindi a creare la catena

Gli hoax possono avere anche una lunga durata, dato che fermano il loro “viaggio elettronico” quando le persone non accettano di inoltrare la “bufala”. Poiché non si tratta di virus, il software antivirus non è in grado di individuarli né di neutralizzarli.
Un discorso diverso è costituito dalle richieste di aiuto, come ad esempio un bambino che ha una gravissima malattia e chiede informazioni, ecc. Queste richieste a volte sono completamente false, altre volte provengono da messaggi originariamente veri ma ... datati.

2.2.1.1 esempi di hoax

Ecco due esempi di hoax.

Allarme Virus! Se ricevi un messaggio con oggetto WIN A HOLIDAY non aprirlo. Formatterà immediatamente il contenuto del tuo hard disk. Si tratta di un nuovo virus non ancora conosciuto, inoltra questa informazione a tutti i tuoi amici ... (in genere sono presenti anche citazioni di fonti di conferma autorevoli come AOL, Microsoft ed altri, ovviamente fasulle)

UN POVERO BAMBINO HA UNA MALFORMAZIONE CONGENITA CON COMPLICAZIONI E NECESSITA DI UN TRAPIANTO COSTOSISSIMO: IL COSTO DELL'OPERAZIONE È DI $ 560.000. LA LEGA PER LA LOTTA CONTRO LE MALATTIE

GENETICHE PAGHERA' $0.01 PER OGNI E-MAIL INVIATA CON OGGETTO "AIUTA NICOLAS". È NECESSARIO INVIARE QUESTO MESSAGGIO IN TUTTO IL MONDO. SERVONO 56 MILIONI DI MESSAGGI PER FINANZIARE L'OPERAZIONE. NICOLAS HA BISOGNO DI NOI PER TORNARE A SORRIDERE!! SALVIAMO QUESTO BIMBO CHE LOTTA CONTRO LA MORTE ...

2.2.2 che danni fa

Se le persone inoltrano un falso allarme a tutti gli amici e colleghi, potenzialmente può generarsi una valanga di e-mail, con il conseguente sovraccarico (o addirittura il blocco) dei server di posta. In questo caso l'effetto sarebbe identico a virus che blocca i server di posta (ad es, virus "Sobig), con la differenza che l'hoaxer non ha avuto bisogno di scrivere neppure una riga di codice.
Il fenomeno delle bufale e della posta che cresce in maniera esponenziale con le catene nasce per un "eccesso di reazione" da parte degli utenti.
Il sito www.attivissimo.net – servizio antibufale - ci offre una chiave di lettura per comprendere il successo delle bufale : "siccome la notizia arriva da una persona di cui ci fidiamo o da una fonte solitamente autorevole, non attiviamo il nostro spirito critico e la accettiamo automaticamente. Inoltre molti di questi appelli fanno leva sui sentimenti o sui pregiudizi: due aspetti della psicologia umana che notoriamente annebbiano la parte razionale del nostro modo di pensare. "
Gli attacchi degli hoax a volte sono più efficaci dei virus veri e propri in termini di danno alle comunicazioni, perché impediscono l'accesso a messaggi che possono essere importanti.
I falsi allarmi distolgono inoltre l'attenzione dai virus veri e propri.
Anche rispondere a messaggi arrivata da catene "infinite" può essere dannoso per gli sprovveduti che le hanno generate.
Sempre l'utilissimo sito www.attivissimo.net ci spiega dei danni degli hoax e delle catene

Ma che male fa diffondere una catena di Sant'Antonio?
Tanto

- Quelle che parlano di sostanze tossiche presenti nei prodotti più disparati danneggiano le aziende che li producono: questo significa danneggiare inevitabilmente anche i loro lavoratori.
- Diffondere una bufala vi fa fare la figura degli ingenui che abboccano a qualsiasi storia senza prendersi la briga di verificarla e senza neppure chiedersi se sia plausibile.
- Le catene spedite dal posto di lavoro vi possono costare il lavoro! Spesso i programmi di posta aggiungono automaticamente in coda a ogni messaggio il nome del mittente e quello dell'azienda o dell'istituto presso il quale lavora il mittente. Il risultato è che una catena spedita dal posto di lavoro sembra "autenticata" dall'azienda/istituto, che difficilmente gradisce che il proprio nome venga abusato da un dipendente e associato a una bufala.
- La diffusione di false notizie può portarvi in tribunale. Sono a conoscenza di almeno un caso in Italia in cui l'incauta diffusione di un appello ha avuto conseguenze legali per chi l'ha fatto circolare. Non posso dare dettagli perché mi è stato chiesto di non darli proprio per evitare ulteriori danni alle società e alle persone coinvolte.
- Quelle autentiche che contengono appelli per curare persone malate spesso proseguono per anni dopo la morte della persona citata. Di conseguenza, i familiari

continuano per anni a ricevere offerte di aiuto che non solo sono assolutamente inutili, ma ricordano loro ogni giorno la scomparsa di una persona cara. Voi come vi sentireste, se ogni mattina vi chiamassero in tanti al telefono per chiedervi come sta vostra figlia morta di leucemia?

- Grazie all'inesperienza degli utenti della Rete, le catene viaggiano con centinaia di indirizzi di e-mail al seguito. Gli spammer (i pubblicitari-spazzatura di Internet) usano queste catene per raccogliere indirizzi a cui mandare la loro assillante pubblicità più o meno pornografica, virus e compagnia bella. Se partecipate a una catena di sant'Antonio, anche il vostro indirizzo finirà nelle liste degli spammer.
- Questi messaggi diventano spesso enormi (150 K e passa) a furia di accumulare indirizzi in coda. Questo significa che ci vuole tempo per scaricarli, e il tempo è denaro, per chi si collega a Internet con il telefono o il cellulare. In altre parole, spedire catene di sant'Antonio costa: costa a chi le riceve oltre che a chi le manda.

2.2.3 come ci si difende

2.2.3.1 linee guida

Azienda
Emanare direttive che vietino di inoltrare catene di S. Antonio.
Utente
Ogni mail di allarme, ogni richiesta di aiuto va ritenuta fasulla fino a prova contraria: cestinandole tutte si sbaglierebbe al più in un caso su 1000.

2.2.3.2 istruzioni e informazioni

Prima di inoltrare una possibile "bufala" si deve tentare di capire se è autentica o meno:

- Un criterio è capire se ha le caratteristiche descritte al punto precedente (come si presenta).
- Un criterio ancora più efficace è copiare alcune righe dell'appello (le più significative, perché contengono nomi o parole particolari) e incollarle nel campo di ricerca di Google. E' quasi sicuro che si perverrà ad uno o più siti che riportano un messaggio identico al nostro, già valutato come vero o falso
- si può anche consultare un sito specializzato su questo tipo di informazioni

Un sito molto completo e aggiornato, semplice e ben fatto è **http://attivissimo.blogspot.com/2004_06_01_archive.html** che riporta centinaia di mail di aiuto o allarme, quasi tutte false. Ma anche quelle vere hanno delle "avvertenze per l'uso". Non manca la sezione "umorismo".

2.2.3.3 strumenti e tecnologia

Gli strumenti ANTISPAM sulla posta possono bloccare anche buona parte degli Hoax.

2.2.3.4 aggiornamenti e controlli

elemento non significativo per hoax e catene

2.3 virus, worm, trojan-horse

2.3.1 cos'è e come si presenta

Il **virus informatico** è un frammento di software in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente a insaputa dell'utente.
L'utente può ricevere un file infetto in diversi modi:

- come allegato a un messaggio di posta elettronica
- in un download da Internet
- su un dischetto o pen drive

Non appena il file viene lanciato, il codice del virus viene eseguito. Il virus può così copiarsi in altri file o dischetti e apportare modifiche al computer.
Comunemente il termine generico "virus informatico" viene utilizzato per descrivere oggetti che hanno caratteristiche differenti. E' opportuno, quindi, vedere brevemente alcuni termini che si possono incontrare in Internet o sulla stampa e che corrispondono a diverse tipologie di virus:

- **Trojan horse (cavallo di Troia) o semplicemente Troian** : sono programmi che si spacciano per software o contenuti legittimi: un salvaschermo, un programmino utile, l'immagine della diva famosa, ovviamente nuda, ecc. Un Trojan "finge" di avere una funzione, e può persino simulare di svolgerla, ma in realtà fa dell'altro, normalmente a insaputa dell'utente. Il caso più insidioso è il **Backdoor Troian**, che sotto un aspetto innocuo, da Trojan, nasconde un insieme di funzioni che consentono il controllo del PC da remoto. Bande di malintenzionati possono arrivare controllare decine di migliaia di PC - la cosiddetta **BOT-net**: rete di roBOT o "Pc zombie" - da usare per inviare SPAM, per attaccare siti governativi, ecc. sovente senza che il proprietario si accorga di nulla
- **Virus** : in senso proprio indica un programma "parassita" che si insedia in un elemento esistente: un file eseguibile, il "boot sector" di un dischetto, le "macro" di un documento word o excel, ecc. I primi oggetti dolosi erano di questo tipo
- **Worm** : programmi che si replicano e si diffondono attraverso le connessioni Internet. I worm si differenziano dai virus perché sono in grado di replicarsi e non hanno bisogno di un programma o di un documento che li ospiti; creano semplicemente copie esatte di se stessi
- gli **internet worm** possono propagarsi da un computer all'altro sfruttando le "falle" di sicurezza presenti nel sistema operativo, ovvero i suoi punti deboli. Il worm Blaster, per esempio, sfrutta una vulnerabilità insita nel servizio di chiamata di procedura remota dei sistemi operativi Windows NT, 2000 e XP (RPC – Remote Procedure Call) e si "autoinvia" ad altri computer.
- gli **e-mail worm**, forse la categoria più diffusa, si distribuiscono automaticamente tramite i messaggi di posta elettronica. Quando l'utente apre l'allegato, manda in esecuzione il worm, che si installa sul sistema e inizia subito a propagarsi inviando una raffica di e-mail

Queste le caratteristiche principali dei diversi virus informatici; la tipologia più frequente è tuttavia utilizza una combinazione di diverse tecniche.

Trojan Email + Internet Worm backdoor : gli oggetti dolosi utilizzano spesso una combinazione di più tecniche per raggiungere la massima efficacia; possono quindi propagarsi mediante invio massiccio di mail (e-mail worm), presentando un contenuto innocente (trojan), e sfruttando poi vulnerabilità del software per mimetizzarsi, per esempio come allegato sonoro o immagine, in modo da attivarsi in automatico, oppure sfruttando altre vulnerabilità dei prodotti installati, per eseguire delle istruzioni scritte su codice nascosto.

2.3.2 che danni fa

I danni dei virus/worm possono essere vari per effetto e gravità.
[1] Diversi worm aprono una “backdoor” - una porta - che consente agli hacker di assumere il controllo dei computer. Una volta installata – via e-mail- una "testa di ponte" sul PC, la cessione del controllo del computer permette ai malintenzionati di scaricare codice doloso più pericoloso come spyware, malware, backdoors, dialers, ecc. Le macchine infette possono quindi essere utilizzate per distribuire spam.
[2] I worm sono in grado di rallentare le comunicazioni, generando un enorme volume di traffico su Internet. La creazione del traffico avviene proprio utilizzando i computer infetti; sono attacchi denominati DoS (Denial-of-service) e possono danneggiare specifici siti Web sommergendoli di richieste o di dati e le aziende collegate ai siti
[3] Un danno molto grave causato da e-mail worm è la dispersione di informazioni personali. La maggior parte dei virus di questo tipo utilizza quanto trova a bordo del PC colpito per mimetizzarsi meglio: indirizzi di posta, contenuto delle mail, ecc. Le mail infette inviate dal worm avranno mittenti e destinatari presi a caso dagli indirizzi di e-mail trovati nella rubrica del PC infettato. Alcuni virus giungono a prendere il soggetto o pezzi del contenuto di mail trovate in casella per costruire messaggi più credibili. Quello che accade molto frequentemente è qualcosa del genere:

- *Pippo* invia una mail a *Pluto* (da: *pippo@aziedasana.it* a *pluto@casasua.it*)
- l'email di *Pippo* viene memorizzata sul Pc di *Pluto*, assieme a quelle di cento altre persone
- quando il Pc di *Pluto* è colpito da virus, questo invia centinaia di mail usando come mittente l'email di *Pippo*
- una di queste mail dolose viene inviata anche a *Paperino* (*paperino@chissadove.eu*); il server di posta di *Pluto* tuttavia rileva un errore (per es. rileva il virus, oppure la casella di *Paperino* non esiste più, oppure è piena, ...) e invia un messaggio di errore a *pippo@aziedasana.it* cioè il presunto mittente del messaggio
- *Pippo*, completamente estraneo all'attacco del virus che ha colpito *Pluto*, riceve per es. una mail che la accusa (erroneamente) di avere inviato virus oppure un avviso che la "sua" mail non è stata consegnata a *paperino@chissadove.eu*
- da notare che *Pippo* e *Paperino* non si conoscono assolutamente
- L'unica cosa che *Pippo* può fare è cestinare la mail

Purtroppo le infezioni da virus informatici sono molto frequenti e possono danneggiare anche chi non ha nulla a che fare con il virus, con conseguenti perdita di tempo e disorientamento.

2.3.3 come ci si difende

2.3.3.1 linee guida

Azienda
Organizzare un sistema di difese efficienti: antivirus aggiornati, backup delle stazioni di lavoro per essere pronti a "ricostruirle" in caso di distruzione da parte di virus; promuovere la consapevolezza del personale sui danni derivanti da queste minacce.
Utilizzare la posta elettronica certificata quando è importante dare un'immagine di una garanzia e di autenticità delle mail inviate dall'Azienda o Ente: il problema descritto nell'esempio di Pippo, Pluto, Paperino è possibile perché la normale posta elettronica non fornisce alcuna garanzia di autenticità del mittente, e tanto meno del contenuto.
Utente
Diffidare di quello che non si conosce; non aprire gli allegati sconosciuti!

2.3.3.2 istruzioni e informazioni

E' utile un'adeguata e ripetuta formazione del personale per dare le conoscenze per gestire eventi anomali come la ricezione di e-mail con virus

2.3.3.3 strumenti e tecnologia

E' indispensabile disporre di strumenti **antivirus** e **antispam** su

- server di posta centrale
- stazione di lavoro
- tutti i server che forniscono servizi locali: aree condivise di appoggio files, installazione o lancio di applicazioni, ecc.

La protezione dei server dove gli utenti possono scrivere files è fondamentale: il primo PC infetto passerà l'infezione sull'area condivisa e questa colpirà nel giro di pochissimo tempo tutti i PC del gruppo. Inoltre la copertura e l'aggiornamento di questi strumenti deve essere totale (vedi “aggiornamenti e controlli”).
Un **firewall** può proteggere i servizi di sistema esposti agli "Internet worms": il firewall è assolutamente necessario sul PC di casa, mentre in una rete interna aziendale il firewall perimetrale fornisce una protezione rispetto alle fonti esterne di infezione.
Nello schema della rete camerale - nella mappa precedente - appare visivamente evidente il ruolo di protezione del firewall, rappresentato dal muro rosso che separa rete interna e rete internet.

2.3.3.4 aggiornamenti e controlli

Le contromisure più importanti per affrontare virus e worm appartengono alla categoria degli aggiornamenti e dei controlli:

- **aggiornamento costante dei sistemi operativi e delle applicazioni** : molti virus e worm per infettare il PC usano vulnerabilità del sistema (Windows, Outlook, Internet Explorer) oppure delle applicazioni coinvolte nell'apertura degli allegati (pacchetto di Office, PDF Reader, Flash player, media player o simili); perciò è importante installare in tempi brevi gli aggiornamenti di sicurezza (le cosiddette “patches”) quando i fornitori di sistemi e applicazioni – Microsoft e altri – li rendono disponibili (anche se è opportuno prendersi il tempo per verificare che l'aggiornamento stesso non sia carente – in gergo "bucato" - a sua volta)

- **aggiornamento e copertura degli antivirus**: nuovi virus compaiono di continuo. **IMPORTANTE**: un antivirus che non è aggiornato ALMENO una volta al giorno diventa un antivirus estremamente scadente. TUTTE le stazioni devono essere protette.
- **da solo l'antivirus non basta**: è essenziale la consapevolezza che comunque l'antivirus non basta. In genere passano almeno otto ore da quando compare il nuovo virus fino al momento in cui i più rapidi ed efficienti fornitori di antivirus rilasciano l'aggiornamento in grado di bloccare le ultimissime minacce (l'aggiornamento viene detto “pattern”). Ma nelle prime otto ore tutti gli antivirus sono uguali, ovvero INUTILI! L'unica difesa è la prudenza dell'utente e la sua capacità di cogliere i segnali di pericolo nelle mail ricevute: ad es. contenuti o mittenti non usuali, allegati eseguibili o comunque strani.
- **presto o tardi** (se siamo prudenti: molto tardi) il **nostro PC** sarà danneggiato da un virus: è importante avere pensato al “dopo”, ovvero aver predisposto il salvataggio frequente dei dati, saper a chi rivolgersi per supporto, ecc.

2.4 phishing

Il “phishing” consiste nell’uso di e-mail e di falsi siti Web per indurre gli utenti con l’inganno a fornire informazioni confidenziali o personali. Questa minaccia informatica è stata trattata nella prima mappa “La sicurezza: strumenti, comportamenti e obiettivi”.

2.5 altre minacce

Vediamo brevemente altre minacce informatiche e/o termini che potrebbe essere utile conoscere.

2.5.1 spyware

spyware
oggetti software dolosi che si installano nel computer con tecniche di tipo "troian horse" e successivamente “spiano” l'attività dell'utente, rubando per esempio le userid/password del sito di home banking, i codici della carta di credito, e ogni altra informazione che può risultare "remunerativa" per chi sta compiendo la frode

2.5.2 dialer

dialer
piccoli programmi molto pericolosi sulle connessioni casalinghe, fatte via modem: disconnettono il modem e lo riconnettono chiamando numeri telefonici (anche internazionali) a tariffe onerosissime

2.5.3 mouse trapping

mouse trapping
il “mouse-trapping” impedisce all’utente di uscire da un determinato sito Internet; si viene indirizzati su un falso sito Web dal quale non si è più in grado di uscire utilizzando i normali pulsanti INDIETRO (back) del browser e/o o CHIUDI FINESTRA. Per sfuggire alla trappola “mouse-trapping” si seleziona un indirizzo dall’elenco “Preferiti” (o Segnalibri) oppure si apre la Cronologia e si seleziona il penultimo indirizzo visitato, o ancora si premono i tasti Ctrl+Alt+Canc e si utilizza il Task Manager per terminare il browser o, se necessario, riavviare il computer.

3 gli strumenti per la difesa

Analizziamo ora i principali strumenti di difesa informatica.
Cerchiamo di comprendere di ciascuno il funzionamento generale senza entrare in dettagli tecnici che competono i sistemisti di rete e di sistema.
Inoltre capiremo che questi strumenti di difesa operano in sinergia fra loro.
Senza dimenticare quanto detto più volte in questo corso che gli strumenti vanno accompagnati da comportamenti “sicuri”.

3.1 software antivirus

Il **software antivirus** protegge i sistemi e le stazioni di lavoro da virus, Trojan, worm e – a seconda dei prodotti – anche da spyware e altri tipi di malware.
Il software antivirus può essere attivato su diverse apparecchiature:

- **server di posta**: in questo caso l'antivirus controlla il contenuto di tutte le mail consegnate al server, agendo quindi PRIMA che la minaccia giunga sul PC dell'utente
- **stazione di lavoro (workstation)**: in questo caso il software riesce ad analizzare meglio il virus e il suo modo di operare; quindi, per così dire, ha a disposizione più elementi per decidere. Di contro però l'antivirus sul PC agisce quando il virus ormai è "salito a bordo"; alcuni virus particolarmente subdoli si attivano prima che il prodotto antivirus possa fermarli, anzi, sono loro che "fermano" l'antivirus
- **filtro antivirus sulla navigazione internet**: stanno crescendo le possibilità di abbinare al proxy la funzione di antivirus per l'analisi del traffico internet e la difesa da files (virus) e pagine scaricate (codice javascript, activex, ecc.)

NOTA BENE: si ottiene un maggior livello di sicurezza installando, nei diversi sistemi, software antivirus di fornitori diversi. Perché questa attenzione? Bastano due piccole considerazioni: dove l'antivirus di un fornitore è carente, è possibile che l'altro possa sopperire, perché già pronto ad affrontare una nuova minaccia; infatti se l'antivirus per il server di posta di un certo fornitore non è pronto di fronte a una certo attacco, difficilmente l'antivirus per la workstation dello stesso fornitore sarà pronto alla difesa.

Tutti i moderni antivirus operano basandosi su **più strategie**:

- **Virus conosciuti** : l'antivirus ha una funzione denominata “scanner” che confronta i file del computer con una libreria di “identità” di virus conosciuti. Se trova una corrispondenza con un virus noto, manda un avvertimento e blocca l’accesso al file. La qualità di rilevamento di virus conosciuti dipende dalla frequenza di aggiornamento del software con le ultime identità dei virus.
- **Virus sconosciuti / files sospetti** : lo scanner dell'antivirus analizza il comportamento probabile di un programma. Se ha le caratteristiche di un virus, l’accesso viene bloccato anche se il file non corrisponde ad alcun virus noto. L'efficacia di questa modalità non è sempre garantita; vi è il rischio che blocchi per errore programmi validi; il vantaggio di questa tecnica è che ha la possibilità di bloccare nuovi virus ancora prima che venga aggiornato l'archivio dei virus conosciuti

Esistono scanner "real time", cioè sempre in esecuzione, e scanner su richiesta (su tutto o parte del disco). La maggior parte dei software antivirus offre entrambe le possibilità.

3.2 software antispam

I **programmi antispam** hanno l'obiettivo di individuare le **e-mail indesiderate** evitando che raggiungano la casella di posta destinataria.
Questi programmi utilizzano una combinazione di metodi per stabilire se un messaggio è spam e quindi deve essere bloccato.

I principali metodi sono:

- **bloccare i messaggi che corrispondono esattamente a determinate caratteristiche**: si tratta di una modalità simile all'antivirus che blocca i virus noti. Il sistema antispam si basa su diversi criteri:
- blocca la posta in arrivo da indirizzi presenti nell'elenco di indirizzi vietati; può essere una lista generale che è possibile acquistare, oppure una lista locale di indirizzi dai quali in passato è stato spedito spam all'azienda e che è stata mano a mano incrementata
- blocca le e-mail che contengono determinati indirizzi Web, determinati mittenti, soggetti o contenuti noti e catalogati con certezza come SPAM
- **bloccando i messaggi che corrispondono a regole generali e che quindi con elevata probabilità sono SPAM**. In questo metodo l'antispam:
- ricerca parole o espressioni chiave che ricorrono nei messaggi spam (ad esempio "carta di credito" o "dieta dimagrante")
- ricerca alcuni tipici "trucchi" utilizzati dagli spammer per mascherare le parole chiave all'interno del messaggio (ad esempio, "hardc*re p0rn").
- ricerca codice HTML superfluo ma utilizzato dagli spammer per nascondere i messaggi e confondere i programmi antispam

Il programma utilizza tutte le informazioni raccolte per stabilire la probabilità che un messaggio e-mail sia spam. Se la probabilità è abbastanza alta, il software blocca l'e-mail o la cancella, a seconda delle impostazioni prescelte.
Anche il software antispam deve essere aggiornato frequentemente con nuove "regole" per poter riconoscere le tecniche più avanzate usate dagli spammer.
Il sistema antispam attivo nella rete camerale opera su due livelli:

- **server di posta esterno** : è il server posto al di là del firewall che riceve posta da Internet; su questo sistema vengono bloccati e cancellati definitivamente tutti i messaggi che sono CERTAMENTE spam, in base alle regole del primo tipo cioè quando c'è esatta corrispondenza delle caratteristiche con campioni di SPAM catalogati
- **server di posta interno** : è il server interno alla rete camerale che riceve la posta internet dal server esterno e la posta di tutta la rete camerale; anche su questo sistema viene applicata la regola di eliminazione dello SPAM "certo". Invece tutti i messaggi e-mail che, in base alle regole generali, risultano "molto probabilmente" SPAM (ma non certamente spam), vengono messi in stato di "quarantena" ma non cancellati. Periodicamente il sistema invia all'utente un elenco delle e-mail in quarantena: l'utente può consultare le e-mail poste in quarantena, può decidere di "sbloccarle" e riceverle come e-mail normali o di cancellarle. Dopo un certo intervallo di tempo le e-mail in quarantena non sbloccate vengono comunque cancellate.

Oltre ai servizi antispam attivi sul server di posta - che bloccano la stragrande maggioranza di SPAM - ci sono programmi “utilities” che operano sul PC, in abbinamento al client di posta come Outlook, Mozilla, Thunderbird, Questi programmi operano in modo "adattivo" cercando cioè di determinare cosa è spam sulla base di regole generali, e poi affinano il metodo "imparando" in base alle azioni di blocco/sblocco fatte dal"utente.

3.3 firewall

Il firewall è un sistema di protezione e difesa di una rete.
Come suggerisce il nome – firewall letteralmente significa “parete tagliafuoco” - questo apparato funziona come barriera: il firewall viene installato in corrispondenza del confine di due reti, solitamente fra Internet e la rete aziendale, e sorveglia il traffico di rete, in entrata e in uscita fra le due reti (o diverse parti di una rete), per stabilire se soddisfa determinati criteri di sicurezza.
Il firewall può essere un’apparecchiatura hardware o un software installato su un computer che funge da gateway per la rete aziendale; basa il suo funzionamento sulle regole di filtro che sono impostate. Grazie a queste regole di difesa e protezione il firewall impedisce l’accesso non autorizzato a un computer o una rete, blocca il traffico ritenuto pericoloso e respinge gli attacchi degli hacker. Questo firewall è detto “perimetrale”.
Anche sul PC di ciascun utente è presente un firewall software che protegge (solo) la stazione di lavoro, in modo simile al firewall di rete. Ne deriva l'importanza di NON disattivare il firewall locale (client).
Il firewall, sia perimetrale che locale, **sorveglia il traffico, sia in entrata sia in uscita**, per stabilire se soddisfa determinati criteri di sicurezza.
Se il traffico soddisfa i criteri di sicurezza viene autorizzato, altrimenti il firewall lo blocca.
Il firewall può filtrare il traffico in base a:

- indirizzi di provenienza e destinazione e numeri di porta (filtro indirizzi)
- tipo di traffico di rete, ad es. HTTP o FTP (filtro protocollo)
- attributi o stato dei pacchetti di informazioni inviati.

Inoltre un firewall client può avvisare l’utente quando un programma tenta di stabilire una connessione e chiedere all'utente se la connessione deve essere autorizzata o bloccata. Il software è in grado di apprendere gradualmente in base alle risposte dell’utente, imparando a conoscere il tipo di traffico autorizzato dall’utente stesso.

3.4 agenti anti malware

Il **malware** è un software creato con il preciso scopo di causare danni più o meno gravi al computer su cui viene eseguito. E' un termine che comprende varie tipologie di minacce già analizzate, come virus, worm, spyware.
Fra gli strumenti di difesa ci interessa qui accennare agli **Agenti anti Malware** ovvero quei programmi che **proteggono le risorse del nostro computer** dai tentativi di accesso alle parti vulnerabili del sistema.
Gli agenti anti malware si basano sulla tecnica di “resource shielding” - letteralmente “schermatura delle risorse” - che analizza il comportamento di tutti i programmi già attivi sul computer e blocca qualsiasi attività che venga giudicata dannosa per le parti vulnerabili del computer.

Il “resource shielding”, ad esempio, verifica tutte le modifiche apportate al registro di Windows, che possono indicare che un malware si sta autoinstallando per avviarsi automaticamente ogni volta che si accende il computer.
I prodotti di resource shielding consentono solitamente di impostare regole proprie sulle risorse da proteggere.

3.5 convergenza di strumenti

L'orientamento attuale della sicurezza informatica è **far convergere strumenti diversi di difesa in una suite di prodotti e agenti di sicurezza integrati** in modo coerente e in sinergia.
Ecco ad esempio che:

- i firewall locali più recenti integrano anche un agente che controlla le modifiche al registro o alle parti critiche del sistema
- gli antivirus sono diventati anche anti-malware e integrano un firewall e/o un antispam della posta elettronica

4 altri strumenti

4.1 cos'è il certificato digitale

Uno strumento di sicurezza è dato dall'autenticazione attraverso smart card e certificato digitale di autenticazione.
Prima di vedere le applicazioni d'uso del certificato digitale usiamo un paragone per capirne il funzionamento.
Un certificato digitale opera in modo simile ad un documento di riconoscimento:
Facciamo l'esempio della patente di guida, che è caratterizzata da:

- il viso del conducente: un elemento unico e irripetibile
- la foto sulla patente: si può riprodurre in molte copie
- un metodo di confronto che permette di stabilire con certezza che foto e viso corrispondono
- la dichiarazione della Prefettura, che certifica che la foto corrisponde ad una precisa persona (nome e cognome, indirizzo, ...)
- un insieme di abilitazioni: in base al tipo di patente (A, B, C, D, ..) corrispondono abilitazioni a condurre veicoli differenti

L'autenticazione mediante certificato digitale opera in modo simile; le rispettive componenti sono:

- la "chiave privata" registrata dentro la smart-card: un elemento unico e irripetibile
- la "chiave pubblica": è incorporata nel certificato digitale, che si può distribuire e inviare in N copie a tutte le persone o server con cui interagire
- il confronto tra chiave pubblica e chiave privata, che viene fatto dal software di firma o dal colloquio SSL del browser: un metodo di confronto che permette di stabilire con certezza che chiave privata e chiave pubblica corrispondono, ovvero che che la smart-card è proprio quella corrispondente al certificato digitale
- la dichiarazione della Certification Authority, che certifica che il certificato digitale corrisponde ad una precisa persona (nome e cognome, indirizzo, ...)
- un insieme di abilitazioni: in base al tipo di certificato (di firma, di autenticazione, ...) corrispondono abilitazioni a eseguire operazioni differenti

Una differenza fra patente e certificato digitale è questa:

- la patente non può essere "fotocopiata" senza perdere validità
- nel mondo digitale gli oggetti possono essere copiati e risultano al 100% identici all'originale; non esiste il concetto di "originale" nel senso che diamo ai documenti cartacei

Il meccanismo di riconoscimento mediante certificati digitali (la parte "visibile a tutti") e chiavi private (la parte "unica e irripetibile" che va protetta con cura) avviene in molte operazioni che svolgiamo con il computer. Ora ne vediamo alcune.
[alcuni concetti di questo argomento sono ricavati da http://www.firma.infocert.it/]

4.1.1 la crittografia

Il sistema di cifratura si basa sulla **crittografia**
La crittografia, o cifratura, è la tecnica fondamentale per la generazione della firma digitale, e viene utilizzata per assicurare la riservatezza, l'autenticazione e il non ripudio delle informazioni archiviate o inviate attraverso reti di computer. Con la crittografia, un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica, ecc.) è trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "chiave" giusta per decifrarli.

4.2 autenticazione ed e-mail

Vediamo il caso in cui il certificato digitale di autenticazione viene usato per accedere a un indirizzo web: il server si accerta dell'identità della persona che utilizza il browser, verificando le credenziali dell'utente (smart-card e PIN) e il suo certificato di autenticazione.
In base a tale conoscenza il server consentirà l'accesso ad aree di informazioni riservate piuttosto che ad altre. I dati scambiati sono cifrati.
Quando il certificato di autenticazione viene usato per firmare un messaggio di posta elettronica, esso risulta associato al messaggio stesso, arricchendolo di informazioni anagrafiche sul mittente (IUT, cognome, nome) che permettono di stabilirne con certezza la provenienza. Il certificato di autenticazione, infatti, abbina, da una parte, i dati del mittente ad un indirizzo di posta elettronica; dall'altra riporta i dati dell'Ente Certificatore che lo ha rilasciato. Infine, viene specificato che si utilizzano i protocolli di posta S/MIME e quelli di accesso sicuro SSL.

4.3 siti protetti

Vediamo ora il caso in cui il gestore di un sito web voglia erogare servizi internet garantendo la riservatezza dei dati trasmessi, instaurando un canale sicuro, cifrato, esclusivo tra il computer dell'utente e il sito.
La versione sicura del protocollo di trasmissione HTTP è l' **HTTPS** , dove la "S" finale significa appunto "secure".
Si tratta di un protocollo sicuro grazie al quale il traffico web di tipo HTTP è incapsulato con modalità denominate SSL/TSL e basate su sistemi di crittografia.

- L'SSL (Secure Socket Layer) è un protocollo di sicurezza che fornisce riservatezza nelle comunicazioni internet. Il protocollo permette di comunicare in una modalità progettata per evitare l'intercettazione, la modifica o la falsificazione dei messaggi.

- TSL (Transport Layer Security) è il protocollo di sicurezza per il trasporto dei pacchetti di dati.

E' bene accertarsi che i siti con i quali scambiamo dati delicati, come ad esempio i servizi di Home Banking, utilizzino il protocollo HTTPS per la protezione delle informazioni trasmesse via internet.
Basta verificare che l'indirizzo web – URL – sia preceduto dalla scritta https:// anziché htpp://
In questo modo è garantita la riservatezza dei dati, instaurando un canale sicuro, cifrato, esclusivo tra il computer dell'utente e il sistema informativo del sito (banca o altro).
Per erogare un servizio web utilizzando il protocollo sicuro HTTPS, il gestore del sito deve possedere un certificato digitale.

4.3.1 il certificato web

Il certificato digitale è rilasciato da un Ente Certificatore che svolge la funzione di garante dell'autenticità del certificato e dell'identità del proprietario.
Il certificato digitale di un Web Server offre al visitatore garanzie di sicurezza:

- autenticazione del sito tramite un certificato digitale riconosciuto da ente preposto
- cifratura di tutte le informazioni scambiate tra il server web e il browser dell'utente

Quando apriamo una pagina web https il browser ci chiede se ritenere affidabile e quindi accettare, oppure no, il certificato del proprietario. Fra le scelte possibili vi è quella di accettare in modo permanente il certificato digitale del web server.
NOTA BENE: il protocollo https e i certificati web sono strumenti di sicurezza per il traffico internet che impediscono di fatto il reindirizzamento inconsapevole verso siti “fantasma” creati per scopo di frode informatica.

5 conclusioni

5.1 riepilogo del materiale didattico

Con questa mappa abbiamo completato la conoscenza di base della Sicurezza Informatica conoscendo i rischi informatici (cosa sono, che danni fanno, come ci difendiamo) e i principali strumenti di difesa informatica (come funzionano, cosa possiamo fare noi per utilizzarli al meglio).
Abbiamo seguito un approccio diffuso in questa disciplina dell'informatica: cercare anzitutto di conoscere ciò da cui dobbiamo difenderci e, solo in seguito, capire cosa possiamo utilizzare per garantire la sicurezza dei sistemi e dei dati.