Glossario Privacy e Informatica

Glossario Privacy

Questa la divisione che è stata fatta:

- **Termini più utilizzati**: sono quelli che si è ritenuto di maggiore consultazione e più approfonditi degli altri.
- **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio del 27 aprile 2016 - Articolo 4 Definizioni
- **Decreto Legislativo 30 giugno 2003, n.196** - Codice in materia di protezione dei dati personali:
  - Articolo 121 - Servizi interessati e definizioni
  - Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica
  - Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale.
  - *(Articolo 4 - (Definizioni) – articolo abrogato)*

    Riteniamo utile pubblicare anche le "vecchie" definizioni del D. LGS. 30 giugno 2003, n.196 anche se l'articolo è stato abrogato

Glossario Informatica

Si può affermare che per questo argomento i termini, probabilmente, non finirebbero mai.

Quelli indicati sono stati presi da varie pubblicazioni in internet.

Importante! - La ricerca dei termini nel documento

La prima possibilità è quella di ricercare il testo servendosi dell'elenco degli argomenti in ordine alfabetico posto sulla sinistra del documento.

L'altra è quella di utilizzare lo strumento di ricerca del PDF digitando il testo. Ciò può essere utile se la parola può trovarsi in più argomenti.

GLOSSARIO PRIVACY

Termini più utilizzati

Accountability

Per accountability si intende il principio di "responsabilizzazione" dei Titolari e dei Responsabili del Trattamento che, nella realizzazione di un sito web, devono mettere in atto tutte le misure tecniche e organizzative adeguate, nonché in determinati casi anche le corrette politiche in materia di protezione, al fine di garantire e poter dimostrare la conformità delle modalità con cui si trattano i dati personali in relazione a quanto previsto dal GDPR .

Amministratore di sistema

Il Garante (Provvedimento del 27 novembre 2008 poi modificato il 26 giugno 2009) definisce l'"amministratore di sistema" (AdS), in ambito informatico, la figura professionale finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, facendo però rientrare in essa anche le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Anonimizzazione

Processo che rende i dati personali anonimi, in modo che la persona non possa più essere identificata.

Archivio o banca dati

Nel Codice Privacy era stata fornita una definizione di banca dati:

- “qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti”

Nel RGPD la definizione di banca dati scompare sostituita da quella di archivio:

- “qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico”

Come si vede siamo in presenza di una sostituzione di lemma ma con quasi nessuna variazione di significato: quello che era una banca dati e lo sarà sino a maggio 2018, sarà archivio a partire dal 25 maggio 2018.

Assessment

L'assessment è uno strumento che permette di **stabilire il livello di maturità del programma privacy** di un'organizzazione, è strutturato in **sette differenti ambiti** e ogni ambito contiene degli **indicatori personalizzabili** ai quali attribuire un punteggio e un eventuale peso.

La procedura di assessment è composta da sette ambiti e ognuno di questi ha un obiettivo:

1. **Indirizzo e controllo** - il programma privacy è governato in modo appropriato e il management è responsabilizzato e coinvolto. Sono presenti specifici ruoli privacy e individuate competenze per l’attuazione del programma.

2. **Valutazione del rischio** - viene effettuato un esame periodico e sono attuati presidi per identificare, valutare e mitigare i rischi per gli interessati e per l'organizzazione. Esiste un sistema per identificare le violazioni dei dati personali, valutarne l'impatto, notificarle all'Autorità e, ove richiesto, anche agli interessati.
3. **Politica, procedure e tecnologie** - sono presenti specifiche procedure per la protezione dei dati personali. Esistono meccanismi e tecnologie idonei a darne attuazione tenuto conto degli obiettivi e dei valori d'impresa e di altri aspetti di carattere etico.
4. **Trasparenza** - gli interessati ricevono le informazioni rilevanti ai trattamenti. I loro diritti, le informazioni sui benefici e i rischi ad essi correlati. L'organizzazione interloquisce con l'Autorità di controllo in merito ad aspetti rilevanti della propria politica di protezione dei dati.
5. **Formazione e sensibilizzazione** - i dipendenti e i soggetti esterni coinvolti nei trattamenti ricevono formazione e comunicazione continuativa in merito alla politica di protezione dei dati, obiettivi e misure poste in essere.
6. **Monitoraggio e verifica** - viene effettuato un monitoraggio sullo stato di attuazione del programma privacy. Vengono regolarmente effettuati audit interni sulla materia. In casi particolari (adesione a codici di condotta e certificazioni), sono effettuati audit da parte di strutture terze indipendenti.
7. **Capacità di reazione ed esecuzione** - sono istruite procedure per garantire adeguata risposta a richieste di accesso, reclami, infrazioni alla politica di protezione dei dati e altri eventi di non conformità. È favorita la collaborazione con gli enti di certificazione e con l'Autorità di controllo.

Autenticazione

La procedura di autenticazione è quella che permette di identificare l'utente di un sistema e attribuire il comportamento di quell'utente ad una persona fisica identificata.

È tale quindi la procedura che consente di accedere ai dati personali solo dopo avere inserito un nome utente e una parola chiave.

L'Allegato B al Codice Privacy prevede regole specifiche sull'autenticazione.

Autorità di controllo

Sono le autorità indipendenti presenti in ciascun Paese dell'UE, aventi i compiti di controllare, sorvegliare e raccomandare il rispetto delle norme sulla protezione dei dati personali e che hanno pure il compito di emanare norme specifiche ad integrazione di quelle esistenti.

In Italia è l'Autorità Garante per la protezione dei dati personali, detto da tutti il Garante Privacy.

Categorie particolari di dati personali

Con il decreto legislativo 196/2003 i dati personali erano stati classificati secondo due criteri convergenti che si integravano: da un lato il primo criterio era oggettivo e riferito alla identificabilità dell'interessato; esistevano così i dati personali generici e quelli identificativi che permettevano di risalire in modo non equivoco ad una persona.

L'altro criterio invece era quello della criticità dell'informazione, ovvero, la possibilità per l'interessato di essere discriminato o di perdere in dignità, qualora tali informazioni fossero state trattate in modo non rispettoso.

È facile comprendere come il criterio che rende certe informazioni critiche o meno è soggettivo.

Sono nate così le categorie dei dati c.d. sensibili e quelle dei dati giudiziari.

I primi erano i dati relativi alla salute, alle scelte relative alla vita sessuale, e quelle relative all'appartenenza ad organizzazioni di natura sindacale, politica, filosofica e culturale e religiosa, nonché i dati relativi alla salute o idonei a rivelare l'origine etnica e razziale.

I dati giudiziari erano invece quelli relativi a procedimenti penali in cui l'interessato ricoprisse la natura di indagato o imputato.

Con il regolamento il criterio della criticità viene lievemente mutato; infatti quelli che prima erano i così detti dati sensibili vengono "accorpati" ai dati relativi all'orientamento sessuale, ai dati genetici, ai dati biometrici e ai dati tesi ad identificare in modo univoco una persona (si parla quindi di impronte digitali, impronta dell'iride, riconoscimento facciale, et cetera). Articolo 9, comma 1:

"[…] dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona."

I dati giudiziari, invece sono definiti in termini meno specifici, art. 10:

"[…] dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza".

Cifratura

Non è un termine tecnico anche se è largamente usato in materia ed ha assunto un significato specifico nell'ambito degli strumenti elettronici.

Per cifratura si intende l'applicazione ad una informazione (quasi sempre rappresentata in un documento informatico), di un algoritmo di cifratura, che rende non intellegibile se non applicando la chiave dell'algoritmo, tutte le informazioni contenute.

Compliance

Come accountability, anche compliance è una parola anglosassone.

Deriva da to comply cioè accondiscendere.

A sua volta to comply deriva dal latino complere, che significa compiere.

C'è compliance quando l'azienda, l'ente o il professionista aderisce e rispetta delle regole, delle leggi o il codice deontologico.

Adesione, conformità, rispetto delle regole.

Sono tutti sinonimi che possono chiarire il significato di questa espressione così usata in ambito GDPR.

Comunicazione

La comunicazione, nel d.lg. 196/2003, è un'attività definita in modo specifico e il cui significato non è completamente intuitivo l'art. 4 del Codice la definisce infatti come:

- "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"

Pertanto qualsiasi trasmissione di dati personali tra il titolare e il responsabile o tra il titolare e

un incaricato, non è una comunicazione.

Si aveva quindi una “comunicazione” solo quando il destinatario era un soggetto terzo rispetto al trattamento.

Con il Regolamento tale nozione tecnica pare non esistere più, il concetto di comunicazione non sembra usato con tale accezione e manca tra le definizioni contenute nel Regolamento.

Al tempo stesso viene definito formalmente il concetto di destinatario (art. 4 punto 9):

- “la persona fisica o giuridica, l’autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.[…]”

Da questa definizione si comprende come la comunicazione non dovrebbe più avere il significato che ha avuto invece sino al 25 maggio 2018.

Consenso

Il consenso a uno specifico trattamento di dati personali per essere valido deve essere prestato in maniera espressa, libera e specifica.
Ciò significa che è legittimo il trattamento di dati personali solo se fondato su un consenso del singolo puntuale e specificatamente riferito alle modalità trattamentali previste.

Consenso dell'Interessato

Il consenso da parte dell'interessato è inteso come una manifestazione espressa, esplicita, libera, specifica, informata e inequivocabile della volontà da parte dello stesso, di fornire il proprio assenso.

Detta manifestazione deve necessariamente essere ricollegata a una azione positiva inequivocabile nella quale si accetti che i dati personali forniti siano oggetto di trattamento da parte del Titolare.

Consenso esplicito

Tutti gli individui devono dare il loro consenso esplicito, cioè una chiara dichiarazione scritta o orale non aperta a interpretazioni errate.

Questa dichiarazione deve specificare la natura dei dati raccolti, il tipo di lavorazione e dei suoi potenziali impatti, se le risposte sono necessarie o opzionali, i dettagli dei dati da trasferire e i rischi connessi a questo trasferimento.

Contitolari del trattamento

Laddove due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

È necessario un accordo trasparente per determinare le rispettive responsabilità in materia di trattamento dei dati personali.

Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Cookie

In programmazione, per cookie, di fatto una specie di gettone identificativo, si intende una stringa di testo di piccole dimensioni inviate da un web server a un web client (solitamente un

browser) che viene restituita, senza modifiche, ogni qualvolta il client accede alla medesima sezione di un sito web.

Ad esempio, un sito potrebbe, per il tramite di un cookie, scrivere delle preferenze di visualizzazione o semplicemente il nome dell'utente, in modo tale da riproporlo alla visita successiva.
Originariamente introdotti, dunque, per ottimizzare l'esperienza di navigazione dell'utente, memorizzare alcune informazioni o, nel caso di un e-commerce, per tenere traccia degli oggetti da acquistare (il cosiddetto "carrello della spesa"), oggi i cookie sono oggetto di massima attenzione in tema privacy, in quanto rappresentano una delle modalità per eccellenza per profilare gli utenti.

Crittografia

Operazione con la quale un messaggio da inviare, un “messaggio semplice o in chiaro”, viene convertito in un “messaggio cifrato” che è incomprensibile per un terzo e diventa così confidenziale.

Data Breach

Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l’integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l’accesso o l’acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l’impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

In caso di violazione dei dati personali, il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Data protection Impact Assessment, o Valutazione d’Impatto Protezione Dati)

La Dpia è una procedura prevista dall’articolo 35 del Regolamento UE/2016/679 (RGDP).
La valutazione d’impatto della protezione dei dati (DPIA) serve a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi.
L’obiettivo è sempre quello di stabilire misure idonee ad affrontare questi ultimi.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Data Protection Officer (DPO)

Il Data Protection Officer (DPO), o anche Responsabile per la Protezione dei Dati (RPD), è una figura introdotta dal regolamento europeo in materia di protezione di dati personali (art. 37 GDPR).

È un consulente esperto che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali e che deve fornire consulenza tecnica e legale al titolare del trattamento o al responsabile e agli addetti affinché rispettino il Regolamento europeo.

Quindi il suo compito è prima di tutto quello di informare il titolare del trattamento, gli addetti ed i responsabili esterni su come raccogliere, trattare e conservare i dati personali in modo conforme al GDPR: aiutarli a provare la loro accountability.

I suoi compiti comprendono

- l'informazione e la consulenza sia al data controller che ai dipendenti;
- la verifica del rispetto del regolamento;
- altre disposizioni di protezione dei dati;
- dare consigli, a richiesta, in merito al Data Protection Impact Assessment 'DPIA' e
- il monitoraggio della sua esecuzione; la collaborazione con l'autorità di vigilanza.

Data Protection Privacy Impact Assessment (PIA)

Un processo progettato per valutare tutti i processi e le banche dati in un determinato reparto (scopo, il periodo di conservazione dei dati, i diritti degli interessati, etc.), e analizzare i rischi per la sicurezza dei dati (accesso ai dati, frodi, ecc) e il loro potenziale impatto in materia di privacy, per determinare le misure tecniche e organizzative necessarie per proteggere i dati.

Dati personali

Qualsiasi discorso sui dati personali deve tenere conto innanzitutto della definizione di dato personale, l'Unione Europea è arrivata ad una definizione ampia di "dato personale" rendendo così le norme sugli stessi capaci di influenzare moltissimi aspetti delle attività umane.

Il diritto dell'UE invece ritiene che la definizione di dato personale è la seguente:

- "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"

Con la conseguenza che anche i dati personali non identificativi in modo indiretto (come un indirizzo IP o il numero di targa di un automobile) sono senza possibilità di equivoco dati personali.

Il principio infatti è di considerare dato personale qualsiasi dato che sia oggettivamente riconducibile ad un interessato.

Questo anche quando la chiave per la riconoscibilità passa attraverso informazioni che siano in

possesso di terzi (come avviene per l'indirizzo IP o per il numero di targa di una automobile).

Dati Personali Giudiziari

Quando si parla di dati personali giudiziari si intendono quei dati personali in materia di casellario giudiziale, quali le condanne penali, i reati e i relativi carichi pendenti o tali informazioni dalle quali si possa dedurre la qualità di imputato o di indagato di un soggetto.

Dati Personali Particolari (Ex Sensibili)

Precedentemente etichettati come "dai sensibili", i dati personali particolari sono quelle informazioni personali dalle quali si possa dedurre l'origine razziale o etnica, le ideologie politiche, l'appartenza ad un determinato sindacato, l'orientamento religioso o filosofico, nonché dati genetici, dati biometrici (intesi a identificare una persona fisica in modo univoco), dati relativi alla salute, alla vita e all'orientamento sessuale persona.

Destinatario

Già il Codice Privacy era scritto tenendo conto del fatto che i dati personali, per loro natura e, ancora di più nella società moderna, esistono per circolare, essere trasmessi e trattati da una molteplicità di soggetti.

Il destinatario è, secondo l'art. 4 al numero 9:

- la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

  Tuttavia, le autorità pubbliche che posssono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Dichiarazione di sostegno

Una dichiarazione con la quale un firmatario sostiene un'iniziativa dei cittadini europei, che può essere compilata e firmata su carta, compilata online utilizzando un modulo web, oppure firmata online con un'identificazione elettronica (eID).

Nei primi due casi le dichiarazioni di sostegno devono seguire un modello previsto dal regolamento riguardante l'iniziativa dei cittadini europei. In tutti i casi contengono una serie di dati personali del firmatario.

Diritto all'oblio / diritto di cancellazione

Il diritto cosiddetto "all'oblio" (art. 17 del Regolamento) si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per

esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1 del Regolamento).

Il Regolamento prevede che la cancellazione avvenga senza ingiustificato ritardo e impone al titolare del trattamento l'obbligo di cancellare i dati personali se, per esempio, non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, se l'interessato ha revocato il consenso al trattamento o se i dati sono stati trattati illecitamente.

Diritto alla portabilità dei dati

l diritto alla portabilità dei dati è stato introdotto dal Regolamento europeo 679/2016 all'art. 20, il quale afferma che:

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
   b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Diritto di accesso

L'interessato che ha prestato il consenso può chiedere ed ottenere in forma intellegibile i dati in possesso del titolare:

- la conferma che i dati personali sono o non sono in fase di elaborazione
- dove vengono elaborati, per ottenere l'accesso ai dati personali
- l'accesso alle informazioni sulle operazioni di trattamento effettuato con i propri dati personali
- il diritto di limitare le operazioni di trattamento
- il diritto di limitare il trattamento che l'organizzazione possa svolgere utilizzando i dati personali se il trattamento non è più giustificata.
-

Diritto di opporsi

Il diritto di opporsi ad un'operazione di trattamento dei dati personali in qualsiasi momento sulla base di motivi legittimi relativi alla vostra situazione particolare.

Diritto di rettifica

Il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti.

Double opt-in (Doppio consenso)

Per Doppio Consenso si intende la modalità di consenso che avviene in un doppio step. In una prima fase l'utente compila un form, fornendo alcune informazioni per avere accesso a determinati contenuti o servizi di un sito web.

Quest'ultimo provvederà ad inviare allo stesso una mail di conferma all'indirizzo mail indicato.

Nel secondo step dovrà, poi, confermare il consenso all'utilizzo e al trattamento dei dati che ha condiviso con il proprietario del sito.

DPIA - Data Privacy Impact Assestment

Obbligatorio per le tipologie di trattamenti che presentano rischi elevati in fatto di diritti e libertà delle persone fisiche, la DPIA è di fatto la procedura di analisi finalizzata alla valutazione dei rischi connessi al trattamento di dati con l'obiettivo di identificare le misure più idonee per affrontarli.

Elaboratore di dati

La persona fisica o giuridica, l'autorità pubblica, il servizio o organismo che elabora dati personali per conto del responsabile del trattamento.

Entità giuridica

Nel contesto dell'iniziativa dei cittadini europei, un'entità giuridica può essere creata per gestire l'iniziativa.

In tal caso, l'entità giuridica corrisponde al gruppo di organizzatori o ai suoi membri.

Può anche sostituire il rappresentante nel suo ruolo di titolare del trattamento dei dati.

Firmatario

Un cittadino dell'Unione che ha sostenuto una determinata iniziativa compilando la relativa dichiarazione di sostegno; i firmatari sono il principale gruppo di interessati cui si riferiscono le presenti indicazioni.

G29

Gruppo di lavoro europeo indipendente su dati e tutela della privacy che riunisce i rappresentanti di ciascuna autorità nazionale di protezione dei dati.

La sua missione è quella di aiutare a sviluppare standard europei adottando raccomandazioni, pareri, e così via.

Garante

Autorità di vigilanza con il compito di garantire la corretta applicazione della regolamentazione sulla protezione dei dati.

GDPR (General Data Protection Regulation)

Nuovo testo europeo sulla protezione dei dati personali applicabile dal 25 maggio 2018, che sostituisce e armonizza tutte le norme di protezione dei dati personali applicabili negli Stati membri dell'UE.

Incaricati – autorizzati al trattamento

Nel Codice Privacy è stata introdotta una figura che non può mai necessariamente mancare: l'incaricato, definito dall'art. 30, e per i quali è obbligatoria la designazione per iscritto.

La mancata designazione degli incaricati per iscritto è considerata una mancata adozione delle misure minime di sicurezza e questo provoca oltre che una sanzione amministrativa l'integrazione della fattispecie di reato prevista dall'art. 169.

Con il regolamento questa figura scompare e scompare pure l'obbligo della designazione per iscritto (detta anche lettera d'incarico).

Tuttavia la figura della persona fisica preposta alle operazioni di trattamento non può venire meno, quando il regolamento vi si riferisce usa l'espressione Autorizzati al trattamento.

Indirizzo IP (Internet Protocol Address)

In informatica e nelle telecomunicazioni, l'indirizzo Ip di fatto è un'etichetta numerica tramite la quale è possibile identificare in modo univoco un dispositivo, detto host collegato (personal computer, palmare, smartphone, router, elettrodomestico), a una rete informatica che utilizza l'Internet Protocol come protocollo di rete. In parole meno tecniche, può essere considerato come un numero di telefono senza il quale non è possibile entrare in contatto con gli interlocutori.

Informativa

È l'insieme delle informazioni che il titolare del trattamento deve fornire, verbalmente o per iscritto, ad ogni interessato nel momento in cui raccolga dati presso lo stesso oppure presso terzi.

Nell'informativa devono essere precisati in un linguaggio sintetico, colloquiale, chiaro, scopi e modalità del trattamento delle informazioni raccolte, se tali dati sono richiesti obbligatoriamente o facoltativamente, le eventuali conseguenze nel caso in cui dette informazioni non vengano fornite, nonché l'elenco degli eventuali soggetti a cui possono essere trasmessi o diffusi.

Inoltre, menzione deve essere data in merito ai diritti riconosciuti all'interessato, ai dati del titolare, ai responsabili del trattamento e le modalità con cui raggiungerli.

Le sanzioni in caso di violazione di questi obblighi possono essere estremamente salate anche perché si moltiplicano per il numero di interessati coinvolti dalla violazione.

Interessato

Colui al quale si riferiscono i dati personali. In alcuni casi si è detto, con una lieve forzatura, che è il proprietario dei dati personali, certamente è quello che su di essi ha diritti molto ampi: ha diritto a conoscere come e dove sono distribuiti i dati personali che lo riguardano e ha diritto, innanzitutto, a conoscere le informazioni che riguardano il trattamento dei propri dati, previste dal legislatore (sia nazionale che europeo), è la così detta informativa.

Limitazione di trattamento

Tale operazione di trattamento è una novità normativa introdotta dal regolamento che la definisce in modo specifico all'art. 4 e n. 3, come:

- il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Sul piano giuridico è una operazione spesso collegata all'opposizione del trattamento regolata dall'art. 21 del Regolamento.

Sul piano pratico spesso è l'apposizione di un tag ad un elemento di un database che impedisce una od un gruppo di operazioni di informatiche a tutti gli utenti o anche ad alcune categorie di utenti del database.

Mappatura dati

Una società deve prima mappare i propri processi di raccolta dei dati personali relativi ai dipendenti, clienti e candidati in cerca di lavoro.

Essa deve quindi identificare le operazioni di trattamento ad essi associati, insieme ai luoghi e formati di memorizzazione e inserire tutti questi dettagli in un apposito registro.

Misure di sicurezza

Le misure di sicurezza sono gli accorgimenti predisposti dal titolare dei trattamenti per impedire trattamenti indesiderati e illeciti.

Il Codice Privacy le classifica in misure minime di sicurezza (art. 33) e sono quelle prescritte dall'Allegato B al Codice Privacy e nelle misure idonee.

In molti casi abbiamo sentito errate distinzioni tra le due categorie di misure di sicurezza. Quella corretta è la seguente:

- Le misure minime di sicurezza sono quelle prescritte dall'allegato B, tassative, obbligatorie, che devono essere adottate così come prescritto dal testo dell'allegato B.

  Le misure minime dell'allegato B comprendono questi temi:

  - Sistema di Autenticazione;
  - Sistema di Autorizzazione;
- Le misure idonee, invece, sono obbligatorie, ma devono essere adottate:
  - A seguito di valutazione dei rischi che incombono sui dati;
  - In modo da rendere il margine dei rischi accettabile per il titolare dei trattamenti.
- Altre misure di sicurezza (aggiornamento obbligatorio della lista di utenti, dei sistemi e programmi adottati, e salvataggi obbligatori almeno settimanali);
- Ulteriori misure in caso di dati sensibili o giudiziari;
- Misure di tutela e garanzia;
- Misure per trattamenti senza l'ausilio di strumenti elettronici.

Organizzatori (gruppo di)

Persone fisiche responsabili della preparazione e della gestione di un'iniziativa dei cittadini europei durante tutto l'iter. Il regolamento riguardante l'iniziativa dei cittadini europei stabilisce che il gruppo di organizzatori gestisce diverse operazioni di trattamento dei dati (in particolare: la raccolta, la presentazione per verifica e la distruzione dei dati).

Se effettuate dal gruppo di organizzatori nel suo insieme o da membri diversi dal

rappresentante, tali operazioni di trattamento dei dati si considerano effettuate sotto il controllo del rappresentante.

Principio di legalità

I dati personali possono essere raccolti e utilizzati per uno scopo specifico e legittimo necessario per i compiti del titolare del trattamento unico.

Principio di minimizzazione

I dati possono essere raccolti e trattati solo se necessario per lo scopo per il quale vengono trattati.

Questo costringe quindi le aziende ad eliminare tutti i dati che non sono necessari per questo scopo e di rivalutare i dati che sono essenziali per le operazioni di trattamento di ciascuna applicazione.

Privacy by design

La Privacy in base alla progettazione si accompagna a qualsiasi attività umana che deve rispettare dei principi giuridici, ed è un leit motiv tipico delle società che hanno un ufficio legale ben attrezzato in una grande gruppo

I principi che reggono il sistema sono i seguenti:

- prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione, e l'applicativo deve prevenire il verificarsi dei rischi;
- privacy come impostazione di default (ad esempio, non deve essere obbligatorio compilare un campo di un form il cui conferimento di dati è facoltativo);
- privacy incorporata nel progetto (ad esempio, l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- visibilità e trasparenza del trattamento, cioè tutte le fasi operative devono essere trasparenti in modo che sia verificabile la tutela dei dati;
- centralità dell'utente, quindi rispetto dei diritti, tempestive e chiare risposte alle sue richieste di accesso.

In definitiva il sistema di tutela dei dati personali deve porre l'utente al centro, in tal modo obbligando il titolare del trattamento ad una tutela effettiva da un punto sostanziale, non solo formale, cioè non è sufficiente che la progettazione dei sistema sia conforme alla norma se poi l'utente non è tutelato.

Privacy by default

Il principio di privacy by default (protezione per impostazione predefinita) prevede, appunto, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti, in modo che l'interessato riceva un alto livello di protezione anche se non si attiva

per limitare la raccolta dei dati (es. tramite *opt out*).

Privacy Shield

Sistema di auto-certificazione UE-USA per la protezione dei dati personali che consente il trasferimento di dati personali da parte di persone situate all'interno dell'Unione europea verso aziende con certificazione "Privacy Shield" .

Profilazione

Per Profilazione si intende ogni forma di trattamento, automatizzato o non, di dati personali che si esplica nell'analisi di tali informazioni, al fine di valutare e determinare aspetti personali di una persona fisica quali, a titolo esemplificativo, il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.

Pseudonimizzazione

Introdotto con il GDPR, la pseudonimizzazione, o cifratura, è il principio in relazione al quale i dati di profilazione acquisiti vengono conservati in una forma tale (ad esempio con il mascheramento e con l'utilizzo dei tag) da impedire l'identificazione dell'utente, senza l'utilizzo di informazioni aggiuntive.

In tal caso, però, la conservazione del dato e delle stesse informazioni aggiuntive (chiavi), allo scopo di impedire un facile ricongiungimento, deve avvenire necessariamente e materialmente in zone differenti (esempio: server distinti).

La pseudonimizzazione o cifratura non è da confondere con l'anonimizzazione.

Non esistono, infatti, tecniche informatiche che possano garantire che un dato sia completamente anonimo, se non tali da rendere poi impossibile la lettura del dato originale. Vi sono due tipologie di pseudonimizzazione in base alle chiavi utilizzate:

- Pseudonimizzazione simmetrica: un'unica chiave per cifrare, o mascherare, il dato e poi renderlo nuovamente leggibile. Ovviamente, questa tecnica crea il problema di come condividere la chiave senza che questa venga scoperta.
- Pseudonimizzazione asimmetrica: si utilizzano due chiavi distinte. Una per cifrare il dato e la seconda per decifrarlo. In questo modo è possibile facilitare la condivisione, poiché si utilizza una chiave per crittografare, visibile a chiunque, e una chiave per decifrare, che conosce solo il destinatario rendendo, quindi, non necessaria la sua condivisione.

Rapporti di lavoro

Nel marzo 2007 l'Autorità Garante ha emanato delle regole per tutti i datori di lavoro che chiedano ai propri dipendenti l'uso di strumenti elettronici interconnessi in rete.

Queste regole si sono poi arricchite di altri provvedimenti speciali e decisioni che hanno contribuito a delineare un quadro normativo sul tema. Il RGPD su questo punto delinea delle regole generali ma consente ampie deroghe (*in melius* come nei contratti collettivi) da parte dei singoli stati membri.

Rappresentante

Un membro (leader) del gruppo di organizzatori di un'iniziativa dei cittadini che svolga la

funzione di titolare o contitolare del trattamento per tutte le operazioni di trattamento dei dati personali effettuate dal gruppo di organizzatori.

Laddove le presenti indicazioni fanno riferimento al rappresentante del gruppo di organizzatori in quanto titolare del trattamento dei dati, queste vanno intese come riferite all'entità giuridica che gestisce l'iniziativa, qualora tale entità sia stata creata.

Rappresentante del titolare

Il titolare dei trattamenti si è detto che è l'organizzazione nel suo complesso, e si sottintende che tale ruolo è incarnato nella persona che, secondo i principi della rappresentanza organica, ha i compiti di occuparsi di tale tema (che è quasi sempre collegato all'amministrazione dell'organizzazione in senso stretto).

Il "rappresentante del titolare" invece è un soggetto eventuale e dovuto al caso di un titolare dei trattamenti che non è stabilito nel territorio dell'Unione Europea, la nozione è definita innanzitutto nell'art. 4 al numero 17, dove si dice che il rappresentante è:

- "la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;"

Successivamente l'articolo 27 precisa alcune condizioni che rendono obbligatoria la nomina del rappresentante del titolare che, quindi, non è un altro titolare, ma un soggetto che rappresenta le posizioni, gli interessi e i doveri oltre che i diritti del titolare dei trattamenti.

Sempre l'articolo 27 spiega che il rappresentante non deve essere nominato qualora il titolare sia un 'autorità pubblica od un organismo pubblico, relegando quindi questa situazione, essenzialmente, ai gruppi imprenditoriali con impresa controllante situata fuori dall'Unione, e che abbiano scelto di mantenere la titolarità dei trattamenti in capo alla "casa madre".

Rappresentante del Trattamento

È il soggetto, persona fisica o giuridica, da designare obbligatoriamente dalle organizzazioni con sede fuori dall'UE, che rappresenti la stessa organizzazione in relazione agli obblighi imposti dal regolamento UE 2016/679 - GDPR.

Registro dei Trattamenti

E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;

- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del RGPD) e in quello del responsabile (art. 30, par. 2 del RGPD).

Regolamento dell'UE sulla protezione dei dati (EUDPR)

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'Unione e sulla libera circolazione di tali dati.

Regolamento generale sulla protezione dei dati (GDPR)

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Responsabile

Figura nata per affiancare il titolare dei trattamenti e svolgere compiti aventi limiti ed obiettivi ma liberi nelle modalità di esecuzione e spesso, con un ruolo organizzativo e di coordinazione degli incaricati (oggi con il regolamento figura scomparsa quasi del tutto).

Può essere un soggetto "interno" e quindi un dipendente dell'organizzazione titolare, o un soggetto "esterno".

Oggi è affiancato, spesso e volentieri, dal Responsabile Protezione Dati ma è comunque un soggetto imprescindibile nell'ambito della definizione delle regole per il trattamento dei dati.

Nel d.lg. 196/2003, l'articolo che si occupa di definirne le caratteristiche generali è il 29, nel RGPD si tratta invece dell'art. 28.

Riservatezza dei dati

Secondo l'Organizzazione Internazionale per la Standardizzazione (ISO), riservatezza dei dati significa garantire che i dati siano accessibili solo alle persone autorizzate, e quindi che le comunicazioni o i dati memorizzati non vengano intercettati o letti da persone non autorizzate.

Servizio di scambio file

Una soluzione informatica fornita dalla Commissione per consentire la presentazione sicura delle dichiarazioni di sostegno agli Stati membri per la loro verifica e certificazione, gestita utilizzando l'attuale sistema informatico S-CircaBC della Commissione.

Su questo sito l'espressione viene utilizzata anche per quanto riguarda la presentazione delle

dichiarazioni di sostegno raccolte su carta (invece di "sistema centrale di raccolta elettronica" di cui all'articolo 10, paragrafi 1 e 5, del regolamento riguardante l'iniziativa dei cittadini europei).

Sistema centrale di raccolta elettronica (COCS)

Un sistema informatico sicuro, creato e gestito dalla Commissione europea ai sensi delle apposite disposizioni del regolamento riguardante l'iniziativa dei cittadini europei (articolo 10).

Consente la raccolta delle dichiarazioni di sostegno, anche tramite moduli web e identificazione elettronica (eID), la loro conservazione e presentazione sicura agli Stati membri per verifica, nonché la raccolta e l'ulteriore trattamento degli indirizzi di posta elettronica dei firmatari.

Sistema di archiviazione

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri specifici.

Sistema informativo

Si parla da anni di sistema informativo e non di sistema informatico perché se il sistema informatico è semplicemente l'insieme degli apparati "informatici" il sistema informativo comprende tutti gli strumenti e le persone che sono in grado di svolgere la raccolta, l'organizzazione, l'elaborazione l'archiviazione e ogni utilizzo dei dati personali e delle informazioni.

Strumenti (elettronici)

Nel Codice Privacy si fa attenzione e distinzione tra gli strumenti elettronici e quelli "cartacei" o "tradizionali".

In altre parole, la norma consapevolmente è stata resa necessaria innanzitutto dall'evoluzione dell'informatica e le regole che sono ispirate dai principi di cautela e necessità si rendono doverose per le potenzialità dell'informatica e della telematica che rendono possibili operazioni di trattamento prima solo astrattamente possibili ma concretamente irrealizzabili (o realizzabili ma in modo del tutto diseconomico).

Nel RGPD invece tale consapevolezza è ormai così profonda che si da per scontato che qualsiasi informazione o dato personale sia anche presente in formato elettronico.

Nel Codice Privacy infatti si da una definizione di strumenti elettronici:

- "gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento"

Nel RGPD la distinzione e contrapposizione cartaceo/elettronico è totalmente assente, in una sola occasione si parla di "strumenti di trattamento" e mai compare la parola cartaceo.

Sub-incaricato

La persona fisica o giuridica, l'autorità pubblica, il servizio o il corpo, che è il subappaltatore del subappaltatore del titolare del trattamento.

Titolare del trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o ente che determina le finalità e gli strumenti del trattamento di dati personali.

In pratica e, in generale, si tratta di una persona giuridica nelle vesti del suo legale rappresentante.

Espressione che traduce il termine inglese controller:

- “la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell’Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri”

Trasferimento dati

Qualsiasi comunicazione, copia, circolazione dei dati personali per essere processati in un paese terzo dal punto di vista dell’Unione Europea. Semplicemente, l’accesso ai dati memorizzati in Italia da un dispositivo situato in Cina è quindi un trasferimento. I trasferimenti sono vietati al di fuori del territorio dell’UE, senza eccezioni.

Trattamento

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Trattamento (di dati personali)

Per chi si occupa della materia è una definizione ormai data per scontata dato che è interiorizzata, eppure uno degli aspetti che si sottovalutano è che quando abbiamo un dato personale abbiamo sempre almeno una operazione di trattamento, infatti è trattamento:

- “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”

URI

Con URI, si indica l’acronimo Uniform Resource Identifier e indica un elemento riconosciuto di una rete (per lo più informatica).

Con riferimento ad Internet (che è una rete) è stata definita e classificata da The Internet Society:

A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource. (da RFC2396)

Nell’ambito della protezione dei dati personali quello che deve essere sottolineato è che un elemento URI non è sempre un dato personale, sebbene, associato ad un dato personale, può sempre contribuire a determinare il profilo di un interessato.

Sono esempi di URI le URL, gli indirizzi di posta elettronica o anche, fuori dall'ambito prettamente informatico, un numero di telefono.

Valutazione d'impatto sulla protezione dei dati (DPIA)

L'art. 35 del GDPR al n. 1 precisa che

"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".

La valutazione d'impatto sulla protezione dei dati deve essere effettuata dal titolare del trattamento avvalendosi, se nominato, del responsabile della protezione dei dati (DPO).

Il principio di carattere generale prevede quindi l'obbligo soltanto se il trattamento è suscettibile di causare un rischio elevato evidenziando come elemento determinante l'uso di nuove tecnologie.

Videosorveglianza

L'attività di videosorveglianza e registrazione delle immagini è una operazione di trattamento e che comporta quindi, dati i moderni strumenti tecnologici, degli obblighi aggiuntivi e specifici, con provvedimenti generali che pongono regole specifiche e consentono particolari deroghe (tra cui le informative sintetiche tramite cartelli).

Non è prevista alcuna autorizzazione da parte del Garante per installare tali sistemi.

In base al principio di responsabilizzazione (art. 5, par. 2, del Regolamento), spetta al titolare del trattamento (un'azienda, una pubblica amministrazione, un professionista, un condominio…) valutare la liceità e la proporzionalità del trattamento, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, altresì, valutare se sussistano i presupposti per effettuare una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento

Violazione dei dati personali

Per Violazione dei dati personali si intende quella violazione della sicurezza che porta, in modo accidentale o illecito, alla distruzione, la perdita, la modifica, la divulgazione non autorizzata o all'accesso ai dati personali trasmessi, conservati o comunque trattati.

Vedere data break

WP29

È un gruppo di lavoro in seno all'Unione Europea, collegato alla Commissione Europea ma indipendente da essa, composto innanzitutto da rappresentanti delle autorità garanti di ogni Paese europeo.

Ha il compito di emanare raccomandazioni e linee guida, negli anni moltissimi sono stati gli interventi determinanti quando ancora la normativa di riferimento, in ogni Paese membro era una legge nazionale: si ricordano linee guida determinanti sulle Rfid, sul trasferimento dei dati personali verso Paesi terzi dell'Unione Europea, e sul concetto di dati biometrici.

Oggi sarà uno degli organismi che, delineando linee guida interpretative del RGPD fornirà

indicazioni alle organizzazioni e alle autorità Garanti in ciascuno stato membro.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Articolo 4 Definizioni

«archivio»:

qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«autorità di controllo interessata»:

un'autorità di controllo interessata dal trattamento di dati personali in quanto:

- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- un reclamo è stato proposto a tale autorità di controllo;

«consenso dell'interessato»:

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (C85)

«dati biometrici»:

i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)

«dati genetici»:

i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)

«dati relativi alla salute»:

i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)

«dato personale»:

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)

«destinatario»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)

«gruppo imprenditoriale»:

un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

«limitazione di trattamento»:

il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

«norme vincolanti d'impresa»:

le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

«obiezione pertinente e motivata»:

un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali

degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

«organizzazione internazionale»:

un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

«pseudonimizzazione»:

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

«rappresentante»:

la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

«impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«responsabile del trattamento»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«servizio della società dell'informazione»:

il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

«stabilimento principale»: (C36, C37)

- per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
- con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

«terzo»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«titolare del trattamento»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

«trattamento transfrontaliero»:

- trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

«trattamento»:

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

DECRETO LEGISLATIVO 30 giugno 2003, n.196 - Codice in materia di protezione dei dati personali,

Articolo 121 - (Servizi interessati e definizioni)

Definizioni trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

«chiamata»,

la connessione istituita da un servizio di comunicazione elettronica accessibil e al pubblico che consente la comunicazione bidirezionale;

«comunicazione elettronica»,

ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di

comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

«contraente»,

qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

«dati relativi all'ubicazione»,

ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

«posta elettronica»,

messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

«rete pubblica di comunicazioni»,

una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

«reti di comunicazione elettronica»,

i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

«servizio a valore aggiunto»,

il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

«servizio di comunicazione elettronica»,

i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2,

lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

«utente»,

qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

«dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica

Articolo 2 - (Definizioni)

1. Nell'applicazione del presente codice si tiene conto delle definizioni e delle indicazioni contenute nella disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni citate nel preambolo. Ai medesimi fini si intende, altresì:

per "archivista",

chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilità di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché gli archivi privati di cui al precedente art. 1, comma 4;

per "documento",

qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali.

per "utente",

chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero;

Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell’ambito del Sistema Statistico nazionale.

Articolo 2 - (Definizioni)

1. Ai fini del presente codice si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675 (di seguito denominata "Legge"), nel decreto legislativo 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni. Ai fini medesimi, si intende inoltre per:

"trattamento per scopi statistici",

qualsiasi trattamento effettuato per finalità di indagine statistica o di produzione, conservazione e diffusione di risultati statistici in attuazione del programma statistico nazionale o per effettuare

informazione statistica in conformità agli ambiti istituzionali dei soggetti di cui all'articolo 1;

"risultato statistico",

l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

"variabile pubblica",

il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

"unità statistica",

l'entità alla quale sono riferiti o riferibili i dati trattati.

(Articolo 4 - (Definizioni) – articolo abrogato)

Riteniamo utile pubblicare anche le "vecchie" definizioni del D. LGS. 30 giugno 2003, n.196 anche se l'articolo è stato abrogato

(autenticazione informatica),

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

(banca di dati),

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

(blocco),

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

(comunicazione elettronica),

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.

Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile (5);

(comunicazione),

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

(contraente),

Qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate(9);

(credenziali di autenticazione),

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

(dati giudiziari),

I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale(3);

(dati identificativi),

I dati personali che permettono l'identificazione diretta dell'interessato;

(dati relativi al traffico),

Qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

(dati relativi all'ubicazione),

Ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico(10);

(dati sensibili),

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (2);

(dato anonimo),

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

(dato personale),

Qualunque informazione relativa a persona fisica, (persona giuridica, ente od associazione,) identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale(1);

(diffusione),

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

(Garante),

L'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

(incaricati),

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

(interessato),

La persona fisica, (la persona giuridica, l'ente o l'associazione) cui si riferiscono i dati personali;

(misure minime),

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

(parola chiave),

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

(posta elettronica),

Messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

(profilo di autorizzazione),

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

(responsabile),

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

(scopi scientifici),

Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

(scopi statistici),

Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

(scopi storici),

Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

(servizio a valore aggiunto),

Il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

(servizio di comunicazione elettronica),

I servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

(sistema di autorizzazione),

l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

(strumenti elettronici),

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

(titolare),

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

(trattamento),

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

(utente),

Qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

(chiamata),

La connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale (6);

(rete pubblica di comunicazioni),

Una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti (8);

(reti di comunicazione elettronica),

I sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato (7);

(violazione di dati personali),

Violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.

GLOSSARIO INFORMATICA

0-day

Viene utilizzato per qualsiasi vulnerabilità non ancora nota pubblicamente.

Viene spesso anche utilizzato per indicare un programma informatico che sfrutta questa lacuna, un “exploit”. Grazie a questa lacuna nella sicurezza il malware sfrutta proprio il vantaggio di agire “liberamente” grazie al fattore sorpresa.

2FA

(2 Factor Authentication)

È un tipo o sottotipo dell’autenticazione multi-fattori.

Questo metodo di riconoscimento consiste nel chiedere conferma dell’identità dell’utente utilizzando una combinazione di appunto due fattori diversi.

I fattori che si utilizzano solitamente si racchiudono nel concetto di HO, SO, SONO: Qualcosa che l’utente conosce, Qualcosa in suo possesso e Qualcosa che lo definisce.

Aumentando la richieste all’utente, si aumenta il livello di sicurezza.

Questo secondo controllo viene effettuato spesso con dispositivi o applicazioni esterne e disgiunte dalla piattaforma a cui si sta accedendo.

A

Access Control

(controllo dell'accesso)

La metodologia di gestione degli accessi e delle risorse accessibili agli utenti di un sistema.

A sua volta sottoclassificato secondo la metodologia utilizzata, DAC (discretionary), MAC (mandatory), RBAC (role-based).

Account

Profilo di un utente che corrisponde ad una casella di posta e ad un indirizzo di posta elettronica.

ACE

(Access Control Entry) –

Si indica il singolo elemento di una ACL (indica il privilegio del soggetto sull'oggetto).

ACL

Si riferisce ai meccanismi ed alle politiche che limitano l'accesso alle risorse del calcolatore.

Un Access Control List (ACL), per esempio, specifica che funzioni gli utenti differenti possono realizzare sui files e directory.

Activex

È la risposta della Microsoft alla tecnologia Java della Sun Microsystems.

Un controllo activex è approssimativamente equivalente ad una Java applet.

Activex è il nome che Microsoft ha dato ad un insieme di tecnologie object-oriented.

La cosa principale che generate quando scrivendo un programma al funzionamento nell'ambiente di Activex è un componente, un programma autosufficiente che può essere fatto funzionare dovunque nella vostra rete di Activex (attualmente una rete che consiste dei sistemi del Macintosh e di Windows). Questo componente è conosciuto come controllo activex.

Address Book

È una indirizzario contenente le e-mail anche raggruppate a gruppi.

Address Resolution Protocol (ARP)

Vedi ARP

ADS

(Alternate Data Stream)

Gli ADS sono informazioni aggiuntive, attributi dei file, memorizzati su file system NTFS, creati per supportare il filesystem di Apple e quindi permettere ai sistemi operativi Windows di operare come file-server per i sistemi basati su filesystem HFS.

Nato sotto Windows NT il flusso alternativo si è evoluto nel tempo permettendo di immagazzinare sempre più informazioni.

Questo spazio essendo invisibile alla maggior parte di software è stato utilizzato come contenitore per nascondere Hack Tools e fonte di attacchi Dos.

Oltre a vari comandi è possibile visualizzare l'ads di un file tramite il semplice notepad.

ADSL

(Asymmetric Digital Subscriber Line)

Linea asimmetrica digitale ad abbonamento per il collegamento a Internet.

Come la ISDN, utilizza le comuni linee telefoniche per comunicazione di dati ad alta velocità. La velocità di trasmissione in ISDN si limita a 64 Kbps 0 128 Kbps, la tecnologia ADSL può raggiungere velocità di 640 Kbps.

Advanced Encryption Standard (AES)

L'Advanced Encryption Standard (AES) è l'acronimo di Federal Information Processing Standard (FIPS) Publication che specifica un algoritmo di crittografia usato dal governo USA per proteggere le informazioni riservate.

Adware

Molti dei software o delle applicazioni che utilizziamo ogni giorno, ci vengono solitamente proposti con qualche pubblicità interna, che provvedono a dare un guadagno, seppur minimo ma costante, agli sviluppatori che offrono gratuitamente il prodotto.

Questo servizio è possibile proprio grazie agli adware che sono software che mettono a disposizione alcune funzioni in parallelo ad un set di pubblicità consentendo per l'appunto di generare un guadagno.

Solitamente si può provvedere alla loro rimozione tramite il pagamento di un piccolo contributo monetario.

Ad oggi però la parola adware ha assunto una accezione negativa perché può succedere che, nell'atto di scaricare una applicazione o di installare un software, procediamo a darne il consenso senza leggerne le clausole, consentendo così l'installazione di terze parti che potrebbero essere malevole come spyware o malware, provocando la comparsa di pubblicità sul nostro desktop, ma soprattutto all'interno del nostro browser dove ci è più familiare trovare solitamente dei banner pubblicitari.

L'apparizione di questi banner, che solitamente nascondono spyware, provvedono a creare un aggancio tra il dispositivo e un computer remoto, osservando i comportamenti dell'utente e proponendo pubblicità mirate e stuzzicanti per lo stesso.

Air Gap

(sotto vuoto)

si dice di un sistema fisicamente isolato da altri sistemi o network, e quindi, in teoria, difficilmente raggiungibile e penetrabile.

Algoritmo

In informatica si intende l'applicazione di un metodo per la risoluzione di un problema adatto ad essere implementato sottoforma di programma.

Può essere definito come un procedimento che consente di ottenere un risultato atteso eseguendo, in un determinato ordine, un insieme di passi semplici corrispondenti ad azioni scelte solitamente da un insieme finito.

Allow-list

(lista di permessi)
una lista di utenti che gode di privilegi di amministratore o comunque di permessi specifici. Può essere usato anche genericamente per risorse e asset (es. Indirizzi IP, domini, mittenti email, numeri di telefono, ecc.)

Analogica

Grandezza che varia con continuità, non rappresenta da un valore numerico.

Antimalware

(Anti Malicious Software)
Sono programmi nati per affrontare i malware.
Bloccano la loro esecuzione prima che questa abbia avuto effetto o nei migliori casi ne rilevano la presenza prima ancora che il codice malevolo entri in funzione.
In via semplicistica si basano sulla consultazione di un database di minacce note, aggiornato costantemente, e su un'attività di anomaly detection\pattern recognition: un comportamento anomalo di un software viene segnalato e potenzialmente bloccato o isolato.

Anti-Replay Service

Col servizio anti-replay, ogni pacchetto IP ricevuto è taggato (marcato) con un numero sequenziale.
fine della ricezione, ogni numero della sequenza viene controllato e se esso ricade in un range specifico altrimenti il pacchetto IP viene bloccato.

Antispam

Sono programmi nati per impedire allo spam (ossia materiale pubblicitario indesiderato) di invadere la casella di posta elettronica degli utenti.

Antivirus

Programma che previene, individua ed elimina i virus in un computer.
Oggi, un antivirus tradizionale è spesso incapace di proteggere un computer da tutte le minacce esistenti, quali ad esempio advanced persistent threat (APT).

API

(Application program interface)
Un api è la metodologia specifica tramite la quale un programmatore che scrive un programma applicativo può fare le richieste al sistema operativo o ad un'altra applicazione.

Application Gateway Firewall

I gateways applicativi esaminano i pacchetti a livello del protocollo di Applicazione e servono come proxy per gli utenti esterni, intercettando i pacchetti e rimandandoli alle applicazioni che li hanno richiesti.
Così nessun utente esterno ha accesso a qualche risorsa che è sita oltre il firewall.

APT (Advanced Persistent Threat)

(minaccia persistente avanzata)

una violazione della sicurezza che permette a un attaccante di ottenere l'accesso o il controllo di un sistema per un periodo di tempo prolungato, di solito senza che il proprietario del sistema sia consapevole della violazione.

Spesso un APT sfrutta numerose vulnerabilità sconosciute o attacchi zero day, che permettono all'attaccante di mantenere l'accesso all'obiettivo anche se alcuni vettori di attacco sono bloccati.

Architettura Client-Server

È un tipo di architettura che prevede un computer centrale, il server, che gestisce le richieste proveniente dai pc ad esso collegati e dipendenti, client.

L'esigenza di una gestione centralizzata delle richieste nasce dalla conflittualità nell'utilizzazione delle risorse tipiche dei primi sistemi informatici.

Artificial Intelligence

(Intelligenza Artificiale, IA)

Disciplina informatica che studia il funzionamento dell'intelligenza umana, con l'obiettivo di riprodurla in maniera quanto più possibile fedele attraverso l'integrazione di sistemi hardware e software.

ASCII

(American Standard Code for Information Interchange) –

Formato internazionale dei codici per i caratteri. Standard adottato praticamente da tutti i produttori di computer, per rappresentare lettere, numeri, caratteri speciali.

Asset

Qualsiasi elemento (sistema, persona, struttura, record, file, informazione) che abbia valore nell'ecosistema da monitorare o proteggere.

Attacchi a Web app

Minacce di tipo eterogeneo, solitamente accomunate dall'impiego dei protocolli di rete HTTP / HTTPS e tese a compromettere l'integrità del sito e dei dati in esso contenuto, nonché l'accessibilità allo stesso.

Attacchi ddos

(Distributed Denial of Service)

Tipologia di attacco web utilizzato frequentemente per rendere inaccessibile un sito web.

Viene eseguito saturandone le risorse, attraverso richieste simultanee di connessione (da parte di terminali infetti) in numero largamente maggiore rispetto a quello che il sito web sarebbe normalmente in grado di gestire.

Attacchi dos

Denial of Service è il nome della famiglia di attacchi dell'ultima generazione.
Questi attacchi non mirano alla distruzione o al furto dei dati, bensì all'interruzione di un servizio, come quello di un server Web o di un sever di posta.
La loro particolarità sta nel trasmettere pacchetti che, in qualche modo, ingannano il protocollo producendo effetti imprevedibili.
Gli attacchi appartenti a questa famiglia sono diversi: alcuni si basano su errori nell'implementazione dei protocolli, altri congestionano la rete vittima con traffico fittizio. Attualmente molti dei maggiori siti Internet sono stati vittime di uno di questi attacchi (o di una loro combinazione).

Attachment

File allegato a un messaggio di posta elettronica.

Attacker

(Aggressore)
l'esecutore dell'attacco informatico.

Attribution

(Attribuzione)
È letteralmente la fase d'indagine da parte di esperti di sicurezza informatica, tesa ad identificare l'Attacker e/o il gruppo che ha eseguito l'attacco informatico.

Audit

Tecnica di monitoraggio delle operazioni o transazioni che avvengono nel sistema.
Utilizza le tracce di log.

Auditor

È il responsabile della sicurezza, il cui compito specifico riguarda l'interpretazione delle tracce di log per monitorare le operazioni che avvengono nel sistema.

Authentication

È il processo che determina l'identità di un utente che sta tentando di avere accesso ad una rete.
Le Autenticazioni avvengono tramite un botta/risposta, basato sulle sequenze di codici in un tempo massimo. Vedi CHAP e PAP.

Authorization

È il processo che determina che tipo di attività o accessi sono consentiti su di una rete.
Normalmente sono usati in un contesto di autenticazione: una volta autenticato un utente, allora può essere autorizzato ad avere accesso ad un servizio specifico.

Avatar

Alter ego virtuale che rappresenta la persona fisica in contesti variegati, come: comunità, forum,

giochi online.

B

Baseline security

(sicurezza base)

Requisiti base di un sistema o di un'infrastruttura che dovrebbero essere garantiti e verificati da un'organizzazione.

Blackhat hacker

(hacker con il cappello nero)

È un soggetto che utilizza le sue skill in ambito informatico, reti, e sociali con intento malevolo, per generare danno alle sue vittime o per arricchirsi, o entrambe le cose.

Contrapposto al Whitehat hacker.

Backdoor

Le **backdoor** in informatica sono paragonabili a porte di servizio che consentono di superare in parte o in toto le procedure di sicurezza attivate in un sistema informatico.

Queste *"porte"* possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica, e più spesso da hacker intenzionati a manomettere il sistema.

Possono anche essere installate autonomamente da alcuni **malware** (come virus, worm o trojan), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

Un esempio celebre è il programma **Back orifice**, che attiva una **backdoor** sul sistema in cui viene installato, dando la possibilità a chiunque ne conosca l'indirizzo di controllare la macchina.

Oltre ad essere molto pericolosi per l'integrità delle informazioni presenti sul sistema, le **backdoor** installate dai virus possono essere utilizzate per condurre degli attacchi di tipo **ddos**.

Backup

In informatica, operazione attraverso cui si duplica un dato (o un insieme di…) che viene poi archiviato su un supporto di salvataggio diverso da quello di provenienza.

In caso di guasto del sistema principale è così possibile ripristinare il dato dall'archivio di riserva.

Banda

Quantità di dati per unità di tempo che può viaggiare su una connessione.

Nella banda ampia la velocità varia da 64 Kbps a 1,544 Mbps.

Nella banda larga la comunicazione avviene a velocità superiori a 1,544 Mbps.

Bandwidth

Generalmente quando si parla di bandwidth (larghezza di banda) si parla di diretta

proporzionalità con la massa di dati trasmesis o ricevuti per unità di tempo. In un sistema digitale, la larghezza di banda è proporzionale alla velocità dei dati al secondo (bps, bit per second).

Un modem che lavora a 57600 bps ha la larghezza di banda doppia rispetto ad uno che lavora a 28000 bps, per esempio.

Banking Trojan

(Cavalli di Troia Bancari)

Tipologia particolare di malware, concepita espressamente per l'intercettazione di credenziali bancarie su terminali compromessi, culminante in una frode bancaria.

Bastion host

È uno specifico nodo (host) che è usato per intercettare I pacchetti di dati entranti o uscenti dalla rete interna.

BC\BCP\BCA

(continuità del business)

Parliamo di Business Continuity\Planning\Analysis pensando al piano che assicura la continuità dei servizi core di un'azienda.

BEC

(Business Email Compromise)

È un exploit col quale un attacker ottiene l'accesso a un account email, attraverso il quale imitare l'identità del possessore e riuscire così ad ingannare la compagnia, impiegati, clienti e partner commerciali.

Binario (sistema)

È il sistema di numerazione in cui si utilizzano due sole cifre, di solito indicate con 0 e 1.

BIOS

(Basic Input Output System) –

È costituito da chip a sola lettura (ROM).

Esegue test diagnostici e controlla lo stato delle periferiche collegate, raccoglie una serie di routine software per interagire con l'hardware della macchina, per esempio, la lettura dei caratteri digitati sulla tastiera, l'invio di caratteri alla stampante, l'accesso alla memoria, alle unità disco e ad altri dispositivi di inserimento (input) e di trasferimento verso l'esterno (output) dei dati.

bit

(binary digit) –

Cifra binaria, che esprime l'unità elementare di informazione. Viene indicata con la b minuscola, la B maiuscola indica invece il byte.

bit MAP

Mappa di bit per rappresentare un'immagine come sequenza di bit.

Black hat

Si contrappone a 'White Hat' ed è il tipo di hacker che opera al fine di compromettere illecitamente la sicurezza informatica di un sistema.

Gli obiettivi finali sono solitamente la sottrazione di informazioni riservate e/o l'ottenimento di un profitto economico.

Blacklist

Si tratta di un elenco di email o domini.

Il contenuto inoltrato da qualsiasi entità ad esso appartenente verrà rifiutato dal sistema. È il meccanismo di spam filtering opposto a Whitelist.

Block-List

(lista di blocco)

La lista di utenti o risorse bloccate, per motivi di sicurezza, spam, contatti indesiderati o policy aziendali in genere (es. anche un social network potrebbe figurare nella block list di un'azienda, sebbene la risorsa in sé sia perfettamente valida e sana).

Anche nota come "Black List".

Blue Team

Per definizione il gruppo di esperti cybersec a guardia di un asset\istituzione\infrastruttura. Contrapposto al Red Team in esercitazioni operative, fa parte della cultura generale del mondo cybersecurity.

Bomba Logica

Tipologia particolare di malware, "annegato" all'interno di un programma e programmato per attivarsi solo al raggiungimento di particolari condizioni.

Bookmark o segnalibro

È l'elenco degli indirizzi dei siti preferiti, da esso è possibile accedere rapidamente, senza digitarne il nome, agli indirizzi memorizzati.

Booleano (operatore)

Operatore logico tipo 'and', 'or', 'not', utilizzato nei motori di ricerca per effettuare ricerche avanzate in Internet.

L'operatore 'and' restringe la ricerca perché restituisce risultati che contengono due o più termini contemporaneamente.

L'operatore 'or' allarga la ricerca perché restituisce risultati nei quali compaiono o l'una o l'altra parola.

L'operatore 'not' restringe la ricerca, perché restituisce documenti che contengono una parola ma non l'altra.

Boot loader

Il programma che ha la funzione di inizializzare il sistema operativo.
Su un personal computer, il boot loader carica il kernel del sistema operativo dal disco fisso alla ram, permettendone così l'esecuzione da parte della CPU.

Boot Malware

(malware dell'avvio)
Un tipo di malware che si insinua nella sezione di avvio di un sistema, con il vantaggio quindi di attivarsi prima ancora che il sistema operativo e le eventuali funzioni di difesa siano attive.

Bot

Un sistema che compie azioni in modo automatico, in via programmatica o attivato da specifiche eventi o istanze.
I bot sono alla base di attacchi di grandi dimensioni.
Un intero computer compromesso a disposizione degli attaccanti viene ugualmente definito bot, o zombie.

Bot master

Un'entità o soggetto che controlla una rete di sistemi infetti e ne dispone quindi della potenza di calcolo.

Botnet

Con botnet si intende **una rete di bot**, o per dirlo più precisamente, una rete di zombie.
Con zombie si indica un PC connesso alla rete infettato da un malware che ne permette il controllo da remoto e questo può accadere senza che l'utente ne sia a conoscenza.
Un hacker o un malevolo con in mano un botnet può provvedere a fare qualsiasi azione, utilizzando singolarmente uno zombie o creare un attacco massivo tramite l'utilizzo di tutti.
Ovviamente le botnet sono comunemente sfruttate per sferrare più attacchi dos, ovvero ddos.

BPC

(Business Process Compromise)
La modifica impercettibile, da parte di un attacker, di specifici processi aziendali al fine di generare profitti illeciti.

BPS

(Bit Per Secondo) –
Unità di misura della velocità di trasmissione dei dati.

Breach

Accesso non autorizzato a contenuti riservati.

Bring Your Own Device (BYOD)

(Porta il tuo dispositivo)
Politica aziendale che ammette l'utilizzo di dispositivi (portali, smartphone, tablet, ecc) sul posto di lavoro, previo adeguamento del dispositivo ai requisiti di sicurezza necessari a garantire l'integrità del network aziendale.

Browser

Applicazione dedicata alla navigazione dei contenuti web.
Le sue funzioni principali sono: la possibilità di navigare attraverso siti e pagine attraverso dei link ipertestuali, il reperimento delle risorse remote che compongono le pagine web e, infine, la loro rappresentazione grafica.

Browser Hijacking

(compromissione del browser)
È un attacco che mira a cambiare la pagina iniziale o il comportamento di un browser (es. modificando il motore di ricerca predefinito).
É considerato un attacco di basso livello, ma che può essere il preludio a attacchi di maggiore entità.

Brute Force

Un attacco che non sfrutta processi analitici o di intelligenza (artificiale o umana), ma prevalentemente sfrutta la potenza di rete o di calcolo a disposizione degli attaccanti.
Consiste nel generare un gran numero di password o keyword o combinazioni di stringhe alfanumeriche per accedere a sistemi o reperire informazioni sugli stessi.

Buffer

Memoria tampone o di transito utilizzata per compensare la differenza di velocità di trasmissione tra due componenti del computer in comunicazione tra di loro.

Buffer overflow

In programmazione si verifica quando vengono scritti dati di dimensione eccedente la capienza di un dato buffer.
Il risultato è che la regione di memoria immediatamente successiva viene (erroneamente o intenzionalmente)! Sovrascritta, portando a malfunzionamenti e/o brecce nella sicurezza del software.

Buffer Overflow Attack

Un buffer overflow attack lavora sfruttando le vulnerabilità conosciute di alcune applicazioni che girano sul server.
Questo può causare un bypass delle aree di applicazione e far guadagnare all'attaccante i diritti di amministratore del server.

Bug

Un difetto del software.

Business Continuity

Si definisce come tale la capacità di un'organizzazione di mantenere la propria operatività e garantire così la continuità dei servizi erogati, pur a seguito di un incidente o evento distruttivo.

BYOD

(porta il tuo dispositivo)

Acronimo per Bring Your Own Device, riguarda una policy aziendale che consente agli utenti di portare in azienda i propri dispositivi e collegarli alla rete.

Questo fenomeno è salito agli onori della cronaca proprio in concomitanza con il lock-down e l'adozione in massa dello smart working.

Byte

Raggruppamento di 8 bit che il computer considera come una singola unità di informazione. Corrisponde a un carattere di scrittura.

Viene indicato con la B maiuscola, mentre la b minuscola indica il bit.

C

CA Signature

È un codice digitale che garantisce l'autenticità del certificato digitale, esso è fornito dalla certificate authority (CA) che emette il suddetto certificato.

Cache Memory

(Memoria Cache)

Memoria di ridotte dimensioni gestita autonomamente a livello hardware (per il software è trasparente) concepita per velocizzare l'accesso agli ultimi dati utilizzati e sgravare il lavoro del bus e della ram di sistema.

Utilizzata tipicamente per rendere rapida e fluida la navigazione di contenuto online.

Ma allo stesso tempo utilizzata anche per compiere attacchi malevoli.

Carding

Acquisto illegale di beni, attraverso carte di credito trafugate.

Catfishing

Assumere false identità con lo scopo di ingannare un soggetto e indirizzarlo a compiere azioni a proprio vantaggio.

Cert (Computer Emergency Response Team)

Il CERT (Computer Emergency Response Team) è una squadra di analisti cyber che possiede le competenze per utilizzare e interpretare i sistemi di monitoraggio per l'analisi dei Big Data e scoprire e risolvere attacchi informatici.

Certificate

O anche ‘Certificato DigitalÈ, ‘Certificato SSL’.

È un documento elettronico che garantisce l’associazione univoca tra la chiave pubblica e l’identità del soggetto che rivendica come propria.

Concretamente, lo scopo di questa tecnologia è di fornire all’utente la prova incontrovertibile (e facilmente verificabile online) che, ad esempio, il sito che sta visitando è autentico (quindi sicuro) e non contraffatto.

CGI exploit

Gli exploits sono dei programmi eseguibili o compilabili scritti in C (e che lavorano nella directory cgi-bin) che aiutano l'hacker ad entrare nel server, ad avere il root o a non essere beccato.

Questi file alcune volte sono indispensabili durante un hackeraggio quando il server è molto ben protetto e non riuscite ad hackerarlo con le tecniche tradizionali.

Challenge-Response

Un forma di Autenticazione nella quale il dispositivo invia un messaggio random chiamato "challenge".

Il dispositivo che deve essere autenticato esegue una elaborazione del "challenge" e risponde con un messaggio contenente il risultato.

Nello stesso tempo il primo dispositivo calcola il suo proprio risultato.

Se i due risultati sono identici il secondo dispositivo viene considerato autenticato.

CHAP

(Challenge-Handshake Authentication Protocol) –

Diffuso protocollo di autenticazione usato nei collegamenti PPP per verificare password e username; più sicuro di PAP in quanto l'autenticazione si svolge in tre diverse fasi e può essere ripetuta anche dopo aver stabilito la connessione.

Chat

Servizi di varia tipologia che permettono ad utenti (anche anonimi) di comunicare tra loro, in tempo reale.

Circuit-level gateways

I Circuit-level gateways lavorano a livello sessione invece che a livello applicazione.

Questi non distinguono le differenti applicazioni che stanno girando sullo stesso protocollo, ma controllano solamente connessioni TCP.

Il chiamante chiama una porta del gateway con TCP che lo connette con qualche cosa all'infuori della rete.

CISO

Chief Information Security Officer, è il responsabile apicale per la sicurezza informatica di

un’azienda.

Click Fraud

(Click Fasulli)

Tipologia di frode informatica che attraverso varie tecniche (manuali, script o programmi ad hoc) simula il ‘click’ su banner pubblicitari generando compensi illeciti a favore del proprietario del sito.

Client

Programma "cliente", usato da un utente per collegarsi ad un servizio sul server.

Per esempio, Netscape e Microsoft Explorer sono client per collegarsi al servizio Web (HTTP), Eudora e Outlook sono client per collegarsi al servizio e-mail (SMTP/POP3), Cute FTP e WS-FTP sono client per collegarsi a FTP, e così via.

È in pratica un programma che viene usato per comunicare con un server.

Cloud

Paradigma di erogazione di risorse informatiche (archiviazione, elaborazione o trasmissione dati) on demand, caratterizzato da un’alta scalabilità e configurabilità.

È l’infrastruttura su cui poggia la nuova generazione di software distribuiti come servizi (e non più come pacchetti installabili).

CND

Computer Network Defense

Il perimetro di sicurezza adottato da un’entità contro gli attacchi informatici.

É normalmente definito da un protocollo e una policy di sicurezza.

Codice a barre

Sistema di rappresentazione di dati per mezzo di barre verticale di spessori differenti, possono essere letti solo con appositi lettori ottici.

Si utilizzano per contraddistinguere un prodotto in commercio e facilitano le operazioni di contabilità alle casse dei supermercati.

Codice Sorgente

È il testo scritto da un programmatore con un dato linguaggio di programmazione, che definisce le funzionalità del programma.

Prima di poter essere eseguito da un terminale, il codice deve venire elaborato (in gergo ‘compilato’) per poter essere correttamente interpretato dal processore.

COM

Abbreviazione di communication è il nome delle porte seriali per la trasmissione di dati tra computer e periferiche.

Il nome è sempre seguito da un numero: COM1, COM2.

Commodity malware

Software malevolo reperibile attraverso canali non legali.

Il lato più pericoloso di questo fenomeno è che questo tipo di software non richiede grosse competenze per l'utilizzo, risultando allettanti per soggetti senza scrupoli alla ricerca di guadagni facili.

Content blocking

È la possibilità di bloccare il traffico di rete basato sul contenuto reale del pacchetto IP.

Content filtering, scanning or screening

La capacità di rivedere le informazioni che l'utente finale vede quando usa una specifica applicazione Internet.

Per esempio il contenuto dell'e-mail.

Content virus

Vedi data driven attack.

Cookies

Sono delle entità archiviate dalle applicazioni web (lato server) che contengono informazioni relative al singolo client.

Sono file memorizzati sul proprio computer che identificano il computer quando è collegato ad alcuni siti Internet e dove detti siti possono registrare delle informazioni.

Vengono usati ad esempio per personalizzare l'accesso a un sito web a seconda delle preferenze dell'utente (si pensi ad esempio all'accesso a siti che richiedono di confermare la propria età per accedere il contenuto).

CPU (Central Processing Unit)

Unità centrale di elaborazione, è il circuito integrato che elabora i dati.

Craccare

Entrare con frode in un sistema di dati o trovare la chiave di accesso per utilizzare un software senza pagarlo.

Cracker

Il termine appropriato per riferirsi a un aggressore non autorizzato di computer, reti e tecnologia al posto dell'abusato termine "hacker".

Tuttavia, questo termine non è così ampiamente usato nei media; pertanto oggi hacker è usato come sinonimo di cracker.

Credentials

(Credenziali) Nome utente e password; vengono generate in fase di registrazione al sistema e sono utilizzate per identificare le utenze autorizzate ad accedervi.

Crimeware

È una tipologia di malware sempre più diffusa, ideata specificatamente per perpetrare furti d'identità online, dati sensibili, risorse finanziarie.

Crittografia

Metodologia atta a codificare messaggi riservati, attraverso il ricorso di varie tecnologie, permettendone la visualizzazione esclusivamente a soggetti autorizzati (dotati della tecnologia necessaria a decodificare il messaggio).

Nella computer networking, la crittografia consiste in criptazione, autenticazione, e autorizzazione.

Cryptolocker

È un malware che cripta / codifica i file presenti di un pc o uno smartphone, impedendo l'accesso ai dati e ai programmi da parte delle vittime.

L'hacker "promette" di sbloccare pc e dati dietro pagamento di un riscatto.

CTI

Cyber Threat Intelligence

Il processo di ricerca, analisi, studio delle informazioni e dati con lo scopo di strutturare una strategia di mitigazione, controllo, difesa nei rispetti di una minaccia informatica.

CVE

(Common Vulnerabilities and Exposures)

È una lista di informazioni note al pubblico che raccoglie le vulnerabilità e i rischi più comuni in rete (rif. Https://cve.mitre.org/).

CVSS

(Common Vulnerability Scoring System)

È uno standard internazionale che permette di classificare le vulnerabilità note in base al grado di pericolosità.

Cyber*

Con il prefisso cyber- vengono indicate comunemente le attività inerenti il mondo dell'information technology e delle reti.

Cyber attack

È il tentativo di violazione di un sistema informativo, attuato da soggetti o gruppi malintenzionati.

Cyber Defense

Vedi Cyber Security.

Cyber Deterrent

Contromisura di sicurezza talmente efficace da far desistere in partenza qualsiasi tentativo di attacco da parte dell'avversario.

Cyber Espionage

L'atto di accedere ad informazioni secretate senza il permesso e la consapevolezza del proprietario, attraverso varie tecniche di violazione (es. Proxy server, trojan, spyware, ecc) a terminali e reti protetti.

Cyber incident

Vedi Cyber attack.

Cyber Infrastructure

L'insieme di strumenti avanzati di calcolo, acquisizione, gestione e visualizzazione dati, reti ad alta velocità e persone.

Un esempio concreto in cui questo paradigma si realizza è nelle comunità scientifiche: l'interconnessione tra più studi di ricerca internazionali porta a risultati di ricerca altrimenti irraggiungibili.

Cyber resilience

La capacità di un sistema/organizzazione di continuare ad erogare i propri servizi anche nelle condizioni più sfavorevoli (es. Durante un Cyber attack).

Cyber security risk assessment

(Valutazione del rischio informatico)

Perizia effettuata sull'infrastruttura informatica di un'organizzazione, mirata ad individuare potenziali vulnerabilità a varie categorie di rischio (es. Network security assessments, Physical security assessments, Web application testing, ecc).

Si può definire come il complesso delle misure di protezione di tutte le risorse informatiche (hardware e software) in un'organizzazione da minacce di natura fisica (furti, calamità naturali, guasti) o digitale (attacchi informatici, furto, perdita accidentale o intenzionale di informazioni, ecc).

Cyber Service

Termine desueto con cui in passato si identificava genericamente qualsiasi servizio commerciale basato su internet, ora rimpiazzato da espressioni più specifiche.

Cyber Terrorist

Criminale che impiega la tecnologia informatica per diffondere codice malevolo, arrecare un danno, minacciare organizzazioni o persone.

Cyber Threat

Minaccia in grado di sfruttare una vulnerabilità e compromettere un sistema. Può essere intenzionale (attacco informatico) o accidentale (guasto hardware, disastro naturale).

Cyberconflict

O anche Cyberwarfare

È un'azione coordinata di attacco (o contrasto) verso un nemico, portata attraverso tecnologie informatiche e di telecomunicazione.

Cybercrime-as-a-Service (CAAS)

Un mercato nero in rapida ascesa che mette a disposizione di qualsiasi malintenzionato strumenti a pagamento (es. Ransonmware, exploit, ddos) per poter sferrare rapidamente degli attacchi informatici.

Cyberspace

Trattasi del dominio virtuale all'interno del quale la comunicazione tra persone è mediata da computer. Viene sovente utilizzato per riferirsi 'al mondo di internet'

Cyberterrorism

L'utilizzo del Cyberspace per scopi violenti o distruttivi.

Cyberwar

Vedi cyberconflict.

Cyberwarfare

Vedi cyberconflict.

Cyberwarrior

Termine di ampio utilizzo, può indicare sia un esperto di informatica incaricato di difendere sistemi critici come infrastrutture militari o statali, sia l'hacker che tenta di violare questi sistemi.

D

Dark Web

Siti web e contenuti online che esistono al di fuori della portata dei motori di ricerca e dei browser tradizionali.

Questi contenuti sono protetti da metodi di crittografia e possono essere accessibili solo con software specifici, impostazioni di configurazione o in attesa di approvazione da parte dei loro amministratori.

Da non confondere con il deep web.

DART

Detection And Response Team

Il team che nelle grandi aziende si occupa di monitorare e prevenire gli attacchi informatici.

Data at rest

Nella gestione dei dati e relativo salvataggio, sono quel tipo di informazioni archiviate che o non vengono modificate del tutto, o solo raramente. Un esempio tipico è quello dei backup su supporti esterni.
Questa tipologia di dati è spesso soggetta ad attacchi informatici.

Data breach

La distruzione, perdita, modifica o pubblicazione accidentale o intenzionale di dati personali.

Data Breach\Leak

Un dato riservato (o comunque interno) viene reso disponibile a soggetti non autorizzati.
O addirittura reso pubblico.

Data driven attack

È una forma di intrusione nella quale l'attacco è codificato all'interno di dati innocui e successivamente eseguito, inconsapevolmente, dall'utente che richiama l'applicazione contenente il codice maligno.

Database

Archivio di dati disposti in modo organizzato e correlati tra di loro.

Ddos (Distributed Denial of Service)

(Negazione del Servizio Distribuita)
È una tipologia di attacco che mira, attraverso l'utilizzo di una rete di risorse (vedi Botnet), a esaurire le disponibilità di un sistema rendendolo indisponibile.
Un attacco ddos mira a server, reti di distribuzione o data center.
Ne esistono di diversi tipi ma i principali sono due:

- *Applicativi*, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere. Non si attacca un intero sistema, ma solo un programma o un applicativo che però risulta fondamentale per il funzionamento dello stesso.
- *Volumetrici*, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse.

Un attacco ddos si differenzia da un "semplice" attacco Dos (Denial of Service) perché il primo attacca su più fronti (risorse appunto distribuite nella rete) e su scala ben più ampia.

Default

È la scelta preimpostata nel caso siano possibili più alternative.

Demoware

Software rilasciato per dimostrazione, spesso non è abilitato in tutte le funzioni.

Denial of service attack

Un programma utente che prende possesso di tutte le risorse del sistema lanciando una moltitudine di richieste che occupano il sistema.

DNS

(Domain Name System)

Ogni host che compongone Internet è contrassegnato in modo univoco da un numero, che va utilizzato per collegarsi ad esso.

Al fine di evitare agli utenti di dovere impiegare questi numeri, sostituendoli con nomi più facili da ricordare e più significativi, esiste un database (il DNS) in cui a ciascuno dei nomi è associato il numero che gli corrisponde.

Quando l'utente indica un indirizzo al proprio browser, per esempio www.ibol.it, il sistema 'interroga' dunque il DNS per conoscere il numero dell'host al quale deve collegarsi, quindi effettua la connessione.

Desktop

In italiano scrivania è la metafora di base dell'interfaccia grafica dei nuovi sistemi operativi: il monitor è pensato come un tavolo di lavoro sul quale sono posti degli oggetti da richiamare con il mouse.

Detection deficit

Il lasso di tempo che intercorre tra un attacco informatico ed il suo rilevamento.

Dialer

Piccoli programmi che hanno la funzione di creare una connessione verso internet o altri terminali, sovente utilizzati in maniera opaca per realizzare delle truffe.

Dictionary attack

(Attacco a dizionario)

Per quanto simile nella metodologia al Brute force attack, si differenzia da esso in quanto l'attacco al sistema di protezione viene eseguito basandosi su combinazioni di parole presenti all'interno del dizionario.

Le probabilità di successo sono più alte poiché tali dizionari contengono password (o porzioni di) usate frequentemente dagli utenti.

Digital footprint

L'insieme dei contributi eterogenei (da una foto postata sul social, al tracciamento dell'ip all'accesso su un sito) che un utente lascia, in maniera più o meno consapevole, nel web.

Disaster Recovery

È un protocollo di natura tecnica, parte della più ampia strategia di Business Continuity.

Definisce procedure e strumenti da impiegare in caso di disastro, per poter ripristinare sistemi e infrastrutture critiche di un'organizzazione e garantire così la ripresa delle regolari attività nel più breve tempo possibile.

Distribuzione patch

La propagazione su larga scala di patch correttive per un dato software. In termini generali, la

priorità assoluta è data alle patch di sicurezza che vadano a correggere potenziali falle sfruttabili per fini maligni, successivamente a correzioni di natura funzionale / migliorativa.

DNS

Domain Name System (Sistema dei nomi di dominio), è un sistema utilizzato per assegnare nomi ai nodi della rete, o host.

DNS

(Domain Name System)
Sistema che gestisce gli indirizzi dei domini Internet.
È un sistema utilizzato per assegnare nomi ai nodi della rete, o host.

DNS Poisoning

(o anche DNS Chache Poisoning)
Un tipo di attacco informatico indirizzato a server DNS, che ne corrompe la cache, alterando la corretta associazione tra indirizzi ip e relativi hostname. Il risultato finale è il reindirizzamento indesiderato su domini differenti rispetto a quelli aspettati.

Domain name server

È un deposito di informazioni di indirizzamento per degli Internet hosts specifici è usato per mappare gli indirizzi IP sui nodi di Internet.

Domain Name System (DNS)

(Sistema dei nomi di dominio)
È un sistema decentralizzato per la risoluzione di nomi di nodi della rete (host) in indirizzi IP e viceversa.

Dominio

Nome di un sito o di un indirizzo Web.

DOS

(Disk Operating System)
Sistema operativo che non ha interfaccia grafica.

Download

Operazione che permette di caricare o scaricare dalla rete un file sul proprio computer.

Download attack

L'utente acconsente a scaricare software (ad esempio cliccando sul link contenuto in una mail o un popup web) senza essere pienamente consapevole delle conseguenze, o in generale qualsiasi download che si aziona senza che l'utilizzatore lo abbia autorizzato.

Downloader

Applicazione pensata per accedere ed eseguire file extra.

Sono strumenti utili agli utenti per computerizzare miglioramenti di programmi importanti, inclusi miglioramenti OC, browser, software anti-virus, dispositivi anti-spyware, intrattenimento e altri programmi applicabili.

Alcuni soggetti impiegano downloader illegali per scaricare ed eseguire programmi inutili senza autorizzazione da parte dei consumatori.

Doxing

Pubblicazione non autorizzata di dati personali/sensibili sul web.

DPA

(Data Protection Authority)

Si tratta di autorità pubbliche indipendenti che vigilano, tramite i poteri investigativi e correttivi, sull'applicazione della normativa sulla protezione dei dati.

Esse forniscono una consulenza specialistica sulle questioni legate alla protezione dei dati e gestiscono i reclami presentati contro le violazioni del regolamento generale sulla protezione dei dati e delle leggi nazionali pertinenti.

Ne esiste una per ogni Stato membro dell'ue.

In Italia l'ente preposto è il Garante per la Privacy (https://www.garanteprivacy.it).

DPI

(Dot per inch)

Punti per pollice, misura della risoluzione usata per scanner e stampanti. A livello tipografico si usano risoluzioni di 300 dpi, per il monitor si usano risoluzioni di 72 dpi.

Drag and drop

È la tecnica, disponibile sui sistemi operativi, a interfaccia grafica, di trascinare file o icone con il mouse.

Drive-by download\attack

(download\attacco automatico)

Si tratta di un attacco che si innesca semplicemente visitando una risorsa web.

É ad esempio alla base dell'angler Kit.

Drive-by-Download

Vedi Download attack.

Driver

Software utilizzato dal sistema operativo per gestire un dispositivo hardware, come stampanti, modem, mouse, ecc.

Devono essere corredati dei driver di installazione per essere riconosciuti e quindi utilizzati dal

computer.

Drone ware

Software maligno progettato per impiegare il controllo remoto di un computer.

Viene impiegato per propagare mail di spam, gestire assalti ddos e diffondere immagini web insultanti. Vedi anche Botnet.

Dual-use tools

Sono strumenti nativamente installati nel sistema operativo ad alto rischio di abuso da malitenzionati poiché difficilmente tracciabili. Esempio: psexec.

E

EDI

Scambio di dati in formato elettronico.

EEPROM

(Electrically Erasable Programmable Read Only Memory)

Memoria a sola lettura cancellabile e programmabile solo elettricamente. In essa sono contenuti i dati e i programmi del BIOS.

Encryption

Vedi anche Crittografia.

Encryption

(Criptatura)

Un processo che usa la crittografia per rendere un dato non leggibile nel modo standard.

End user device

Vedi anche Endpoint.

End User License Agreement (EULA)

(Accordo di licenza con l'utente finale)

È il contratto tra l'azienda fornitrice del software e l'utente finale che definisce le modalità di utilizzo del prodotto.

Endpoint

Dispositivi ad uso personale, come: personal computer, smartphone, tablet, supporti per il salvataggio dati rimovibili.

End-to-End

(dall'inizio alla fine)
Si tratta di un dato (o di un'azione) che parte dall'origine e arriva al termine, ad esempio di un sistema, di un network, di un flusso o di un processo.

EPROM

(Erasable Programmable Read Only Memory)
Memoria a sola lettura programmabile e cancellabile.

Ethical Hacker

Definito anche come White hat e contrapposto ai cosiddetti Black hat, è un esperto di sicurezza informatica specializzato in tecniche e metodologie atte ad assicurare che i sistemi informatici di un'organizzazione siano ragionevolmente immuni ad attacchi esterni.

Exploit

(sfruttare a proprio vantaggio)
Si tratta di uno script, codice, software in grado di causare un comportamento inatteso dagli utenti ma utilizzabile a proprio vantaggio, per fini spesso legati al cybercrime.
Spesso gli exploit sfruttano bug e vulnerabilità.

Exploit Kit

Software che scansiscono risorse (reti, sistemi, computer) in cerca di potenziali debolezze o vulnerabilità.

Extranet

Utilizzo di Internet per la comunicazione tra aziende e clienti abituali.

F

FAQ

(Frequently Asked Questions)
Domande ricorrenti relative a un argomento, a un sito Internet, raccolte, assieme alle risposte, in un unico file.

File System

Il meccanismo con il quale i file sono posizionati e organizzati su dispositivi di archiviazione.

Fileless persistence

Per garantire la persistenza dei malware di nuova generazione nel sistema vengono

solitamente annidati degli script VBS nel registro di sistema o utilizzando il Windows Management Instrumentation (WMI).

Firewall

Genericamente è un dispositivo di monitoraggio e filtraggio del traffico di rete che permette di monitorare il traffico in entrata e in uscita nella rete, impedendo attività giudicate pericolose (in poche parole, facendo da “barriera”).

Ve ne sono due tipi: network firewall (dispositivi hardware che filtrano il traffico tra due o più reti) o host-based firewall (sono software installati su un host computer e hanno la funzione di analizzare il traffico in uscita o in entrata dei terminali medesimi).

Firewall denial-of service

È un firewall costruito apposta per evitare gli attacchi denial-of-service.

Firmware

Software presente nella memoria ROM che gestisce le funzioni di base del sistema.

Forensic

Termine usato in diversi contesti in ambito cybersecurity, ma che riportano all’utilizzo di una metodologia scientifica e indiziaria per il reperimento di informazioni e la loro analisi, conservazione, interpretazione, convalida.

Frame

Parti di una pagina web inserite in cornici e indipendenti l’una dall’altra.

Freeware

Software gratuito ma tutelato dalle leggi sul copyright, può essere utilizzato gratuitamente ma non può essere venduto.

FTP

(File Tansfer Protocol)

Protocollo per la trasmissione di dati su Internet.

Fuzzing

È una tecnica di test automatico che cerca di trovare bug di software hackerabili alimentando casualmente input e dati non validi e inaspettati in un programma per computer, al fine di trovare errori di codifica e falle di sicurezza.

Si tratta di un processo sempre più comune sia per gli hacker che cercano vulnerabilità da sfruttare che per i difensori che devono tutelarsi da tali minacce.

G

GARR

Autorità italiana che attribuisce gli indirizzi Internet.

Gateway

È un dispositivo di rete in grado di mettere in comunicazione due o più reti inizialmente disgiunte.
Si differenzia da dispositivi come router o switch in quanto sono in grado di operare su qualsiasi livello della scala ISO/OSI.

GB

(gigabyte)
Misura di unità di informazione, corrisponde a 1024 MB.

GUI

(Graphical User Interface)
Interfaccia grafica di un software, permette una fruizione più immediata perché utilizza immagini e icone invece di testo scritto.

H

Hacker

Una persona che ha conoscenza e abilità nell'analizzare il codice di un programma o un sistema informatico, modificando le sue funzioni o operazioni e alterando le sue abilità e capacità.
Il termine ha assunto anche il significato di pirata informatico ma, a differenza dei "crackers", gli hackers operano secondo un codice 'etico' che vieta di trarre profitto dalla violazione dei segreti informatici.

Hacking

Il processo tecnico col quale si cerca di accedere ad un sistema informatico e prenderne il controllo completo all'insaputa del proprietario o del responsabile.
Si noti che l'accezione non è necessariamene negativa, vedi anche Cracker.

Hacking Tool

Programma utilizzato per la realizzazione di un attacco hacker.

Hacktivism

Una forma di attivismo che usa attività di hacking per perseguire un obiettivo politico o sociale, spesso contro gruppi multinazionali, partiti, ideologie ecc.

Hacktivista

Soggetto che effettua un attacco informatico mosso da fini politici.

Handshake

Una fase che anticipa la connessione effettiva tra due calcolatori, durante la quale i sistemi che si stanno per mettere in comunicazione definiscono le specifiche comuni dei messaggi d'interscambio.

Hard disk

È la principale unità di memorizzazione dei dati. In esso vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer e quasi sempre i documenti creati dall'utente.

Fisicamente si presenta come un disco metallico, ricoperto di materiale magnetico.

Hardware

Insieme dei dispositivi elettronici e meccanici del computer.

Hash

Un algoritmo che trasforma un qualsivoglia input in una stringa di lunghezza costante. Le funzioni hash sono deterministiche (stesso input uguale stesso output), producono un output di lunghezza fissa, hanno un effetto valanga (minime modifiche nell'input causano modifiche drastiche nell'output).

A differenza inoltre delle funzioni crittografiche, le funzioni hash non sono reversibili (ma possono essere comunque, talvolta, decodificate ricorrendo a tavole dette Rainbow Table).

Information Security

È il reparto che si occupa del mantenimento dell'integrità dei sistemi e dei dati aziendali

Highjacking or hijacking

È la tecnica mediante la quale si prende il controllo di una connessione dopo che che l'autenticazione utente è stata stabilita.

Honey pot

Significa letteralmente "vaso di miele", un finto bersaglio utilizzato per attirare gli hacker in trappola (spesso viene impiegato per mantenere un hacker connesso ad un sistema abbastanza a lungo da rintracciare la posizione o per attirarlo in una sezione innocua di una rete, in modo che non faccia danni).

L'honeypot è configurato per registrare quante più info possibili sugli attaccanti, e creare quindi una strategia di difesa.

Hijacker

(o anche Browser Hijacking)

Software malevolo in grado di modificare le impostazioni di default del browser, solitamente forzando il traffico internet verso un portale web specifico e incrementandone così i ricavi.

Hoax

(Bufala)

Informazione falsa, spacciata per autentica. Appartengono a questa gategoria le catene di sant'antonio e le Fake News.

Host File

È un file di sistema, all'interno del quale avviene l'associazione tra hostname e indirizzo IP; determina in altre parole l'indirizzamento di un nodo all'interno di una rete.

È stato soppiantato dalla tecnologia DNS ma viene ancora usato come soluzione alternativa per configurazioni ad hoc.

Hosting

È il servizio di rete attraverso il quale vengono pubblicati i siti web su internet.

Il server che ospita direttamente il sito comprende anche tutte le risorse delle quali il sito ha bisogno per funzionare (database, web server e sistema operativo).

HSSB

(High Speed Serial Bus)

È un collegamento di tipo seriale, utilizzato per periferiche particolarmente sofisticate.

HTML

(Hyper Text Markup Language)

Linguaggio utilizzato per costruire ipertesti, ovvero documenti con zone attive per mezzo delle quali è possibile passare da un documento ad un altro.

É il formato utilizzato per costruire le pagine del Web.

Hub

Dispositivo impiegato per collegare più computer all'interno di una rete.

È una tecnologia obsoleta in quanto, amplificando il segnale indistintamente su tutte le porte (broadcasting) crea traffico superfluo, al contrario di dispositivi più intelligenti come gli switch che riescono a discriminare il segnale di rete, indirizzandolo dove effettivamente è richiesto.

I

ICS

(Industrial Control System)

Espressione che racchiude un'eterogenea tipologia di sistemi di controllo industriale (es. SCADA, PLC).

IDS

(Intrusion Detection Systems)

Dispositivo di sicurezza hardware o software (o anche ibrido) per il controllo delle reti.

Ha la funzione di monitorare qualsiasi attività sulla rete e, in caso di attività sospette, bloccarne l'accesso.

Incident

Vedi Cyber attack

Industrial Spy-Hacker

Evoluzione dello spionaggio industriale che si avvale dei più recenti ritrovati informatici.

Infosec

Information System Security, l'insieme di mezzi tecnologie protocolli dediti al mantenimento e protezione dei dati e dei sistemi informativi.

Insider\Insider Threat

(minaccia interna)
un soggetto con intenzioni malevole che appartiene però all'organizzazione stessa.

Insider risk

L'utilizzo improprio di un accesso legittimo a un sistema, condotto per arrecare danno all'organizzazione. Solitamente ad opera di una risorsa interna.

Intranet

È una rete di computer interna a un'azienda, a volte utilizza Internet per scambiare informazioni ma è protetta dall'intrusione di esterni.

IOC

(Indicators of Compromise)
In informatica forense, indica un elemento (es. Indirizzo IP, un hash MD5, ecc) che se rilevato all'interno di una rete o un computer, indica inequivocabilmente un'intrusione in atto o già compiuta.

Iot

(Internet of Things)
Neologismo che si riferisce a qualsiasi oggetto fisico che, attraverso il collegamento ad internet, vede accresciute le proprie potenzialità.

IP

Indirizzo di internet che permette di identificare in modo univoco un utente e un computer collegato a Internet.
Si suddivide in due parti, la prima individua la rete dove si trova il computer, la seconda individua il computer all'interno di quella rete.

IP Spoofing

Si tratta di una tecnica, più che di un attacco, molto complessa.

In pratica, chi attacca cerca di collegarsi a un server rubando l'identità (partendo dall'indirizzo IP) di una macchina di cui il server 'si fida'.
Questa tecnica è molto complessa, dal momento che viene dapprima 'bloccata' una macchina con un attacco dos, quindi ci si presenta alla vittima con l'identità della macchina bloccata (questo avviene simulando il traffico di ritorno che il vero host non sta più generando). Questa tecnica viene generalmente utilizzata per guadagnare l'accesso di amministratore su una rete privata.

Ipermediale

È un documento complesso che integra in modo interattivo testo, immagini, video e suoni.

Ipertesto

Indica un testo collegato tramite link ad altri testi o altri documenti, a differenza del comune testo può essere letto non in maniera sequenziale ma saltando da un documento a un altro.

IPS

(Intrusion Prevention Systems) Vedi IDS.

Irda

(infrared Data Association) –
Consente di collegare periferiche attraverso raggi infrarossi e quindi senza l'uso di cavi.

ISDN

(Integrated Services of Digital Network) –
Sistema pubblico di trasmissione dati di tipo digitale.

ISP

(Internet Service Provider, fornitore di servizi Internet)
Organizzazione che fornisce, sia a privati che aziende, servizi come l'accesso a internet, la posta elettronica, l'hosting di siti web, ecc.

J

JBOH

(Java Script Binding Over HTTP)
Hijacker che permette l'esecuzione di codice da remoto su terminali Android.
L'infezione avviene soventemente attraverso app di dubbia provenienza.

JPEG

(Joint Photographic Experts Group)
Formato grafico elaborato da un comitato di esperti di fotografia. Permette di registrare in forma digitale compressa immagini.
A differenza del formato GIF che può avere al massimo 256 colori, questo formato può avere

milioni di colori.

K

KB

Unità di misura dell'informazione, corrisponde a 1024 byte.

Kernel

È il nucleo fondamentale del sistema operativo che ha il compito di interfacciare in maniera corretta ed efficiente il software con le risorse hardware necessarie al loro funzionamento.

Keylogger

Un **keylogger** è, uno strumento in grado di controllare tutto ciò che un utente digita sulla tastiera del proprio computer.

Esistono vari tipi di keylogger:

- **Hardware**: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera.
- **Software**: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

I **keylogger** hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza.

I **keylogger** software sono invece semplici programmi che rimangono in esecuzione captando ogni tasto che viene digitato, e poi trasmettono tali informazioni ad un computer remoto.

Spesso i **keylogger** software sono trasportati ed installati nel computer da **worm** o **trojan** ricevuti tramite Internet ed hanno in genere lo scopo di intercettare password e numeri di carte di credito.

Keystroke logger

L'attività di intercettazione degli input ricevuti dalla tastiera ad opera di un keylogger.

L

LAN

Local Area Network

Dispositivi connessi all'interno di una rete o di un network in un'area limitata (es. Un ufficio o un'abitazione).

Lateral Movement

(Spostamento Laterale)

Quando il malware ha preso possesso di un terminale vulnerabile, tenterà attraverso quest'ultimo di infiltrarsi in altri computer appartenenti alla stessa rete, cercando di acquisire

sempre più informazioni, sino ad arrivare ai sistemi/dati più critici e riservati.

Link

Collegamento tra un documento e un altro.

All'interno di un documento è una zona attiva che permette di passare a un documento collegato. Linux Sistema operativo di dominio pubblico.

Living off the Land

Attacco informatico portato per mezzo di tool già presenti nativamente nel sistema operativo dei computer, dunque senza l'aggiunta di alcun codice malevolo creato ad hoc.

Grazie a questo escamotage le operazione d'infiltrazione non lasciano tracce e i colpevoli sono difficilmente rintracciabili.

Logic Bomb

Uno script o malware che si attiva solo al verificarsi di specifiche condizioni o eventi, spesso innescati dal comportamento dell'utente.

M

Macro

Sequenza di comandi automatizzabile, eseguita all'interno di un programma.

Possono essere usate per eseguire codice malevolo, a patto che l'utente apra o esegua l'allegato (ad esempio contenuto in una malspam).

Mailbox

Casella postale, dove vengono accumulati i messaggi di posta elettronica.

Mailing list

Servizio di Internet che consente lo scambio di informazioni tra utenti mediante messaggi di posta elettronica inviati a tutti gli iscritti alla lista.

Mainframe

Computer con potenti processori, grande quantità di memoria RAM, particolarmente utile da usare in multiutenza, ossia da più persone contemporaneamente, ognuna delle quali usa un terminale collegato al mainframe.

Per le sue elevate capacità è utilizzato nelle reti come punto di smistamento.

Malspam

Email di spam contenente codice malevolo in forma di allegati o url che, una volta cliccati, portano allo scaricamento di malware di vario tipo.

Malvertising

Tecnica di diffusione dei malware su larga scala, ottenuta attraverso l'infezione di portali web legittimi. L'utenza, credendo di accedere contenuti sicuri, verrà a sua volta contagiata.

Malware

Il termine è l'abbreviazione di *malicious software* e si indica con tale **qualsiasi software indesiderato che viene installato nei dispositivi o nei sistemi informativi senza un adeguato consenso**: virus, worm ("verme", è un particolare tipo di malware in grado di autoreplicarsi sfruttando altri computer tramite mail o reti di computer), cavalli di troia ecc.

Si parla di Malware-as-a-service quando il servizio viene offerto a pacchetto da cyber criminali.

MB

(megabyte) - Unità di misura dell'informazione che corrisponde a 1024 KB.

MEGAHERTZ

(mhz) - Unità di misura della velocità della CPU, corrisponde a un milione di cicli al secondo.

Memoria cache

Memoria interna al processore, ad altissima velocità di accesso.

Memory only threats

Tipologia di attacco informatico che non lasciano traccia, essendo eseguito esclusivamente su regioni di memoria di sistema.

MFA

(Multi-factor authentication)

Metodo di autenticazione che fornisce l'autorizzazione all'accesso al sistema solo al soggetto che dimostra di essere in possesso di più requisiti combinati.

I fattori di autenticazioni tipici sono: qualcosa che l'utente conosce, possiede, impersona.

MIM

Man in the Middle (soggetto nel mezzo)

Si tratta di un attacco dove il soggetto malevolo si posiziona tra la vittima e un servizio web (o comunque all'interno del network in posizione in grado di captare i flussi dati scambiati da diversi soggetti).

MIM può dirottare le info, catturarle, o alterarle, o compiere un insieme di azioni non desiderate da parte dell'utente.

Mitigation

Il processo attraverso il quale si identificano le potenziali minacce e si definiscono procedure e azioni da applicare per ridurre il rischio di sicurezza associato.

MITM

(Man in the middle)
È un tipo di attacco informatico nel quale un attacker redireziona e/o altera la comunicazione tra due terminali che “credono” di comunicare direttamente.

Multifactor Authentication

(autenticazione a più fattori) (talvolta indicata anche come 2FA, Two Factor Authentication).
Si tratta di un processo di identificazione di un utente che si basa su più parametri, e non solo l’accoppiata classica username + password.
La prassi attuale vede un processo del genere (qualcosa che l’utente conosce AND qualcosa che l’utente ha AND\OR qualcosa che l’utente è). In tal caso, ad esempio (password AND token AND\OR impronta digitale).

Multitasking

Esecuzione di più programmi simultaneamente.
È una caratteristica del sistema operativo che consente di utilizzare diverse applicazioni contemporaneamente senza essere costretti a chiuderle per passare dall’una all’altra. Per esempio, si può lavorare contemporaneamente su diversi documenti di videoscrittura, fogli di calcolo, programmi di grafica, ascoltare musica ecc.

N

Network computer

Indica un terminale di rete intelligente che non ha memoria di massa.
Consente di elaborare in maniera autonoma i dati ma di condividere con altri computer risorse, applicazioni e dati.

Non-PE file attack

Il codice malevolo (macro o script) viene “annegato” nel codice di documenti Office.

O

Open Source

Tipologia di licenza software che permette lo studio, la modifica e la distribuzione del codice sorgente senza particolari limitazioni.

P

P2P

(Peer to Peer)

Architettura distribuita, in grado di ripartire il carico di lavoro tra tutti i nodi appartenenti alla rete.

Packer

Software provvisto di un algoritmo in grado di combinare il dato compresso con il codice di decompressione, in un singolo file.

Passive Tracking Technologies

Si tratta di tecnologie utilizzate che osservano la condotta di un consumatore o addirittura raccolgono informazioni sul consumatore.
Occasionalmente può comportare visualizzazioni individuali o ulteriori dettagli.

Password Cracking

Il processo di recupero di una password da dati salvati in un computer oppure da esso trasmessi.
Una tecnica ricorrente è quella del Brute force attack.

Patch

(toppa)
Modifica a un programma per aggiornare, correggere o migliorarne le funzionalità e la sicurezza.

Payload

È la parte di codice che definisce cosa deve fare il malware dopo che ha infettato il computer della vittima.
Ad esempio carpire informazioni riservate, danneggiare i dati, propagarsi su ulteriori terminali, ecc…

Pentest

(contrazione di Penetration Test)
È un attacco informatico autorizzato, eseguito per valutare la sicurezza complessiva dell'infrastruttura informatica e identificare eventuali vulnerabilità.

Pentesting

Penetration Testing,
Un tipo di attacco eseguito al fine di verificare punti deboli di un sistema e porvi rimedio.
É quindi parte del lavoro del whitehat hacker, ad esempio.

Pharming

Attacco informatico col quale si redirige il traffico di un sito web ad un altro sito fasullo.
Si ottiene solitamente modificando l'host file della vittima o sfruttando una falla nel server DNS.

Phishing

Il termine è una variante di *fishing,* che tradotto in lingua inglese significa letteralmente "pescare". In questo caso parliamo di una truffa realizzata sulla rete che viene effettuata a carico di un utente mirato **attraverso principalmente messaggi di posta elettronica ingannevoli**.

Tipici esempi di queste mail possono essere quelle apparentemente provenienti da istituti finanziari, poste, servizi online che richiedono dati personali, riservati e di accesso da immettere tramite una pagina indicata con un link che rimanda solo apparentemente ad un sito esterno affidabile.

Il sito esterno solitamente copia molto bene il sito originale, una volta però immessi i dati, quest'ultimi vengono resi disponibili ai criminali.

Parallelamente potrebbe essere installato un virus, tramite allegati con estensoni .exe, .doc o .pdf con diciture differenti come fatture, contravvenzioni, avvisi di consegna, accrediti ecc.

Phreaker

Un hacker specializzato nell'utilizzo di reti telefoniche e cellulari.

PII

(Personally Identifiable Information, Dati Personali)

Qualsiasi dato che si riferisca ad una persona fisica.

Ping of Death

Questo è uno degli attacchi dos più celebri (e anziani).

Il gioco è semplice: basta inviare all'host preso di mira una pacchetto ICMP (con il programma di utilità PING) con un carico di dati maggiore di 64 Kb.

La vittima, non sapendo come gestire le informazioni di frammentazione del pacchetto, produce effetti indesiderati, come il riavvio o, addirittura, il crash del sistema. Al giorno d'oggi i produttori di sistemi operativi hanno posto un rimedio a questo tipo di attacco, rendendo disponibili apposite patch.

Plaintext

Testo in chiaro, non criptato.

Port Scanner

Applicazione con la funzione di scansionare quali porte di rete sono aperte su un dato host.

Questo tipo di strumento non è necessariamente maligno, ma talvolta viene usato da un attaccante per individuare possibili vie d'accesso vulnerabili a una rete.

POS intrusion

(Point of Sale Intrusion)

Attacco remoto eseguito sui terminali POS, solitamente attraverso varie tecniche MITM e l'utilizzo di malware.

Privacy Policy

Un documento legale che definisce dettagliatamente come un'organizzazione gestisce i dati del cliente.

Privilege Escalation

(anche Privilege Elevation)
L'operazione che permette, attraverso una falla di progettazione in un sistema operativo o un software, di guadagnare dei permessi normalmente non concessi ad un utente regolare.

Proxy server

Server intermedio tra il computer dell'utente e il server web, che conserva in memoria i file e le pagine Internet maggiormente visitate, rendendo in tal modo più rapida la loro consultazione.
Sono anche un baluardo di difesa intermedio posto tra utente e network centrale verso attacchi informatici.

PUP

(Potentially Unwanted Program)
Programmi percepiti come indesiderati da un utente.
Un caso classico è quello di pacchetti d'installazione che al loro interno includono software addizionali oltre a quello richiesto, spesso di dubbia provenienza.

R

Rabbit

(anche Fork Bomb o Wabbit)
È un attacco dos nel quale un processo si replica continuamente, esaurendo le risorse del sistema che lo esegue ed, in fine, portandolo ad un blocco completo.

RAM

(Random Access Memory)
Nella RAM vengono caricati i programmi attualmente in esecuzione nel computer.
È un tipo di memoria volatile, con la caratteristica peculiare di permettere l'accesso a qualsiasi regione di memoria sempre con lo stesso tempo di latenza.

RAM-scraping malware

Malware che scansiona la memoria di dispositivi digitali (spesso usato sui POS) per raccogliere informazioni sensibili come numeri di carte di credito e PIN.

Ransomware

Il ransomware è una tipologia di malware che impedisce o limita l'utilizzo del sistema all'utente, bloccando lo schermo o i file personali e che richiede il pagamento di uno sblocco dietro pagamento.

Gli ultimi ransomware, chiamati collettivamente “crypto-ransomware”, criptano file o sistemi particolari e forzano gli utenti a pagare il “riscatto” tramite determinati servizi di pagamento online per poter ottenere una chiave di decriptazione.
É una delle tipologie di attacco più frequenti.

RAT

(Remote Administration Tool)
Strumenti di amministrazione remota di server o postazioni di lavoro, ossia di una funzionalità che permette all’amministratore del sistema o all’utente di accedere da remoto alla macchina e di eseguire operazioni sulla stessa.

RCE

(Remote code execution)
La capacità di eseguire codice arbitrario attraverso una rete.
Ciò comporta il poter prendere possesso di un terminale a distanza ed impiegarlo per fini illeciti.

Red Team

Per definizione il gruppo di esperti cybersec che simulano un attacco hacker a un asset\istituzione\infrastruttura.
Contrapposto al Blue Team in esercitazioni operative, fa parte della cultura generale del mondo cybersecurity.

Registro di Sistema

È la base dati nella quale vengono salvate le impostazioni del sistema operativo Microsoft Windows e dei programmi in esso installati.

Remote Control Software

Software che viene eseguito per abilitare l’accesso remoto e la gestione delle reti di computer.

Risk Modeling

Procedura applicata dai rivenditori anti-spyware per stabilire la classificazione di uno spyware e ruota attorno alla categoria e al rischio.

Rogueware

(malware canaglia)
un malware celato sotto spoglie di programmi di utilità (es. Antivirus, programmi di pulizia del pc).

Root Access

(accesso alla radice)
si usa per indicare i privilegi di amministratore su un sistema.

Rootkit

Un insieme di strumenti software con privilegi di accesso a livello di amministratore installati su un sistema informativo e progettati per nascondere la presenza degli strumenti, mantenere i privilegi di accesso e nascondere le attività condotte dagli strumenti.
È in grado inoltre di mascherare la propria presenza nel sistema.

Router

Dispositivo di rete che ha la funzione di distribuire i pacchetti di dati attraverso una rete di computer, indirizzandoli al corretto destinatario.

S

Saas

(Software as a service)
È un modello di licenza e distribuzione del software che si basa sul concetto di abbonamento.
Le risorse del servizio sono centralizzate e si accedono attraverso internet.

Sanitisation

La disinfezione è il processo di rimozione di informazioni sensibili da un documento o altro messaggio (o talvolta crittografandolo), in modo che il documento possa essere distribuito a un pubblico più ampio.
Quando l'intento è la protezione della segretezza, come nel trattare le informazioni classificate, l'igienizzazione tenta di ridurre il livello di classificazione del documento, producendo probabilmente un documento non classificato.
Quando l'intento è la protezione della privacy, viene spesso chiamato anonimizzazione dei dati. Inizialmente, il termine sanitizzazione veniva applicato ai documenti stampati; da allora è stato esteso anche ai media per computer e al problema della remissione dei dati.

SCADA

(Supervisory Control and Data Acquisition)
È un'architettura informatica per il controllo e il monitoraggio, attraverso un'interfaccia grafica, di macchinari e impianti industriali.
La criticità di questi sistemi ne ha fatto un bersaglio ideale per criminali informatici senza scrupoli.

Scareware

Software maligno programmato per ingannare la vittima, facendole credere che il computer sia infetto e inducendola a scaricare un falso antivirus.

Scavenging

(sciacallaggio) o anche Dumpster Dive (tuffo nei rifiuti)
L'atto di reperire info riservate e confidenziale cercando tra i rifiuti di un individuo o di un'organizzazione.

Screen Scraping

(anche Screen Capturers)
Programma in grado di scaricare grosse quantità di dati dai siti web, salvandole in un file locale o in un data base.
Possono venire usati per svolgere attività come il furto di dati, estrapolando da più siti tutte le informazioni relative alla vittima, reperibili in rete.

Script Kid

Un hacker che esegue semplicemente script e programmi altrui senza conoscerne il funzionamento nel dettaglio.
Usato, nella cultura hacker, anche in modo dispregiativo verso chi non ha conoscenza della materia.

Script Kiddie

Una persona priva di preparazione tecnica, che utilizza tool e codice maligno prodotto da altri per fini illeciti.

Security Analysis Software

Strumenti di vario uso e genere, impiegati per testare la sicurezza di reti e sistemi, in sessioni di pentest.

Security exploit

Vedi exploit.

Security Operation Center

Security Operations Center (SOC) è una Centrale Operativa specializzata nella sicurezza informatica.
Può essere attiva direttamente all'interno di un'azienda (di grandi dimensioni) o, più spesso, di società specializzate in Cyber Security.

Seriale

Espressione usata per indicare la trasmissione di dati inviati uno per volta.
Per esempio la trasmissione di dati attraverso il modem è di tipo seriale.

Server

Computer remoto dotato di software in grado di ricevere le informazioni e trasferirle ad altri computer collegati alla Rete.

Shareware

Software coperto da copyright distribuito gratuitamente solo per un periodo di prova.

Sicurezza Informatica Gestita

Servizio di Cyber Security che prevede la gestione della Sicurezza Informatica da parte di una società specializzata, attività non gestibile da aziende – spesso di piccole dimensioni – non strutturate e impossibilitate a effettuare investimenti massivi.

Si definisce “Sicurezza Informatica Gestita” proprio perché la soluzione è demandata a un’azienda esperta di attacchi informatici.

Skimmer

Dispositivo capace di leggere e in certi casi immagazzinare su una memoria EPROM o EEPROM i dati della banda magnetica dei badge.

Usato sempre più spesso per commettere attività criminose tramite Bancomat e distributori di Benizina self-service.

Smishing

Tipologia di phishing veicolata attraverso SMS.

Sms spoofing

Tecnologia che permette di modificare il mittente (Sender ID) originario dell’sms con del testo alfanumerico.

Non è necessariamente una tecnica maligna, ma spesso viene usata per impersonare una persona di fiducia ed ottenere informazioni riservate.

SMTP

(Simple Mail Transfer Protocol) - Standard per la trasmissione della posta in Internet.

Smurf Attack

Si tratta di un attacco molto pericoloso, diretto al router che collega la propria rete locale a Internet e che si basa sulla funzione di direct broadcast addressing.

Chi attacca utilizzando questa tecnica dirige una serie di richieste di echo ICMP (con il comando PING) all'indirizzo di broadcast della rete vittima.

Dal momento che tutto il traffico di rete generato è diretto a un indirizzo di broadcast, questo verrà inoltrato a tutti gli host della rete locale (cioè il 'broadcast domain').

Questo traffico, insieme alle risposte alla richiesta echo del comando Ping genereranno un traffico molto sostenuto, soprattutto nel caso che la propria rete sia composta da molti host. Questo traffico finisce per saturare la rete, rendendo impossibile, di fatto, la comunicazione (e, quindi, si verifica un blocco dei servizi).

Sniffing

Si definisce **sniffing** l'attività di intercettazione passiva dei dati che transitano in una rete telematica.

Tale attività può essere svolta sia per scopi legittimi (ad esempio l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il traffico, offrono funzionalità di analisi del traffico stesso.

Sniffing in reti ethernet non-switched

In questo tipo di reti ethernet il mezzo trasmissivo (cavo coassiale o, attualmente, tramite un cavo twisted ossia un cavo che al suo interno contiene 4 coppie di filo intrecciate) è condiviso tramite un hub centrale, quindi tutte le schede di rete del computer nella rete locale ricevono tutti i pacchetti, anche quelli destinati ad altri, selezionando i propri a seconda dell'indirizzo MAC (indirizzo hardware univoco della scheda di rete).

Lo sniffing in questo caso consiste nell'impostare sull'interfaccia di rete la cosiddetta modalità promiscua, che disattivando questo *"filtro hardware"* permette al sistema l'ascolto di tutto il traffico passante sul cavo.

Sniffing in reti ethernet switched

In questo caso l'apparato centrale della rete, definito **switch**, si occupa di inoltrare su ciascuna porta solo il traffico destinato al dispositivo collegato a quella porta: ciascuna interfaccia di rete riceve quindi solo i pacchetti destinati al proprio indirizzo ed i pacchetti di broadcost

L'impostazione della modalità promiscua è quindi inutile, e per intercettare il traffico si deve ricorrere a tecniche più sofisticate (ARP Poisoning, AEP Spoofing) che sfruttando alcune vulnerabilità del protocollo ARP consentono di deviare il traffico tra due **host** verso un terzo (attaccante), facendo credere ad entrambe le vittime che l'attaccante sia il loro interlocutore legittimo.

Questo tipo di attacco è definito **Man in the middle**.

Sniffing in reti geografiche

Per intercettare i dati che transitano su reti geografiche si utilizzano tecniche Man in the middle analoghe a quelle accennate in precedenza, operanti però a livello più alto: possono intervenire a livello di instradamento del traffico IP (**routing**) oppure inviare alle vittime informazioni fasulle per quanto riguarda la corrispondenza tra nomi a dominio e indirizzi IP sfruttando l'assenza di autenticazione del sistema DNS.

Modalità di difesa

- Cifratura del traffico, in particolare delle informazioni sensibili.
- Utilizzo di strumenti software in grado di rilevare la presenza di **sniffer** nella rete.
- Rafforzamento della sicurezza dei protocolli di rete.

Snoopware

Malware in grado di monitorare le attività di un dispositivo smartphone.

Può tranciare le chiamate, gli SMS, messaggi vocali e email.

È in grado anche di controllare telecamera e microfono all’insaputa del proprietario.

Social Engineering

(ingegneria sociale)

L’insieme delle tecniche (e per estensione, l’attacco stesso) che sfrutta non la tecnologia ma la psicologia e la conoscenza dell’individuo e del suo comportamento, abitudini, cerchie sociali, al fine di manipolarlo e ottenere le informazioni o i comportamenti desiderati.

Nel campo della sicurezza informatica, si adottano tecniche sofisticate di manipolazione per ottenere dati riservati, divulgati spontaneamente da soggetti informati.

Social network Poisoning

Sabotaggio su larga scala dei Social Network, compromettendone l'affidabilità attraverso la creazione di profili ed informazioni falsi.

Spamming

Lo **spamming** (detto anche fare spam) è l'invio di grandi quantità di messaggi di posta elettronica indesiderati (generalmente commerciali).

Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso la posta elettronica.

Il termine trae origine da un vecchio sketch del Monty Python's Flying Circus ambientato in un locale dove ogni pietanza del menù era a base di Spam (un tipo di carne in scatola).

Spear phishing

(pesca con l'arpione)

Un tipo di attacco phishing che sfrutta l'esistenza di un reale rapporto tra vittima e entità online che viene emulata in modo fraudolento, ad esempio una banca o un social network.

Questo tipo di attacco è molto preciso e spesso richiede un discreto effort per studiare le informazioni e abitudini della vittima.

Spoofing

Lo spoofing è la tecnica con la quale l'hacker simula un indirizzo IP privato (facente parte della LAN) da una rete pubblica facendo credere agli **host** che l'ip della macchina server da contattare sia il suo.

Con questo metodo, l'hacker riesce ad estromettere il server reale ed impossessarsi ad esempio delle userid e password dei client che tentano di connettersi al server sovrapposto.

Spyware

È un software in grado di collezionare informazioni su una persona o un'organizzazione a loro insaputa.

I dati possono venir inviati remotamente a soggetti estranei, senza il consenso dell'interessato.

SQL Injection

È un tipo di attacco che inietta del codice malevolo all'interno di un database, solitamente sfruttando una vulnerabilità del software.

Una volta avvenuta l'infezione, l'attacker può effettuare qualsiasi tipo di azione: dal dump dei dati, fino alla loro completa distruzione.

Supply chain attack

In questo tipo di minaccia il codice malevolo viene impiantato all'interno di software legittimi, ancor prima che siano distribuiti al pubblico. Infettando il canale di distribuzione alla fonte, il potenziale di diffusione è accresciuto sensibilmente.

SYN Flood

Questo attacco si basa su un difetto architetturale del protocollo e, più precisamente, sulla procedura di avvio delle transazioni TCP (tecnicamente conosciuta come three way handshake).

Questa procedura ha luogo ogni volta che due macchine stabiliscono una sessione: la prima invia un segmento che contiene una richiesta SYN (sincronia); la macchina a cui viene spedito il segnale risponde con un segmento che contiene i messaggi SYN e ACK (acknowledge); a questo punto la prima macchina dovrebbe rispondere con un segnale ACK, in modo da far partire la sessione.

Prima di inviare la risposta, le macchine che ricevono una richiesta di apertura di una sessione, accantonano in una zona della memoria la richiesta: se la procedura viene eseguita correttamente e la sessione viene stabilita, la richiesta verrà rimossa dalla memoria.

Gli attacchi SYN Flood si basano proprio su questo particolare: se si riesce a fare in modo che l'invio di numerose richieste congestioni questa zona di memoria della vittima, la macchina presa di mira andrà in blocco, nel senso che non potrà più garantire il servizio di rete fino a che le numerose richieste non vengano soddisfatte (cosa che non avverrà mai).

Con gli attacchi SYN Flood la procedura di avvio di una sessione tra due macchine viene eseguita per due terzi: invece di passare alla treza fase (ACK), chi attacca invia un nuovo segnale SYN, ricevendo una nuova risposta SYN/ACK e facendo ricominciare la procedura. Anche in questo caso, però, I produttori di sistemi operativi di rete hanno reso disponibili delle patch e quasi tutte le piattaforme Firewall attualmente in commercio permettono di difendersi da questo attacco.

Sysadmin

L’amministratore di sistema.

T

Targeted attack groups

Un tipo di minaccia nel quale gli organizzatori perseguono la compromissione dell’infrastruttura oggetto d’attacco, mantenendo l’anonimato.

TCP/IP

(Transmission Control Protocol / Internet Protocol)

Protocollo, ovvero regole, per la trasmissione di informazioni sul Web. I dati da inviare vengono suddivisi in piccoli pacchetti e poi ricomposti al momento della ricezione.

Test di vulnerabilità

Vedi Pentest.

Token

Nel mondo della cybersecurity indica un dispositivo fisico in grado di generare codici autentificativi.

Tor

(acronimo di The Onion Router)
È un software libero, che permette una comunicazione anonima per Internet basata sulla seconda generazione del protocollo di rete di onion routing: tramite il suo utilizzo è molto più difficile tracciare l'attività Internet dell'utente essendo finalizzato a proteggere la privacy degli utenti, la loro libertà e la possibilità di condurre delle comunicazioni confidenziali senza che vengano monitorate o intercettate.

Tracking Cookies

Tipologie particolari di Cookies, condivise tra più servizi o siti.
Utilizzate per fini di marketing o pubblicità, sono però spesso anche oggetto d'attacco, in quanto contenenti la cronologia delle abitudini e delle azioni di un utente sui siti che li integrano.

Tricklers

Downloader che può scaricare degli spyware in background per mascherare l'attività sospetta.

Trojan

Tipologia di malware, spesso camuffato nel comportamento e nell'aspetto come fosse un software legittimo (ad esempio un eseguibile di un videogame o di un programma).
Viene impiegato per accedere ai sistemi dell'utente, dopo che questo è stato tratto in inganno da tecniche di social engineering.

U

Underground

Aree del dark web frequentate da hacker, dove vengono effettuati lo scambio o la compravendita di strumenti illeciti per la realizzazione di attacchi informatici.

URL

(Uniform Resource Locator)
Identifica in modo univoco le informazioni presenti su Internet, un indirizzo dal quale si richiamano le informazioni.

USB

(Universal Serial Bus)
Sono i collegamenti utilizzati per connettere periferiche dotate di questo tipo di interfaccia.

User

L'utente di un sistema informatico.

UVPIE

(United Virtualities Persistent Identification Element)

Tecnologia di tracking passivo, si tratta di un'alternativa ai Cookies che utilizza come base tecnologica Macromedia Flash.

V

Virus

È un codice maligno che si propaga copiando sè stesso in un altro programma, in una partizione di boot di un computer o in un documento.

Il virus necessita che un utente, consapevolmente o meno, diffonda l'infezione.

Vishing

(Voice or voip Phishing)

Fronde elettronica nella quale la vittima è ingannata e portata a rivelare informazione finanziare o personali a soggetti estranei.

Viene eseguito non solo attraverso internet, ma anche attraverso mail vocali, voip, chiamate telefoniche su linea tradizionale e mobile.

VPN

(Virtual Private Networking)

È un sistema di hardware e software impiegato per creare una rete di dati privata utilizzando un'infrastruttura di telecomunicazioni condivisa.

In una rete privata virtuale, non è necessario che le connessioni tra computer siano dedicate o di proprietà dell'organizzazione; tramite tecnologie VPN, è possibile creare una rete privata che può essere utilizzata solo da persone autorizzate all'interno di qualsiasi struttura di rete condivisa, compresa Internet.

Le VPN utilizzano tecnologie di crittografia, quali il protocollo di tunneling point-to-point o PPTP, meccanismi di autenticazione e componenti hardware dedicati per creare una rete sicura a un costo inferiore rispetto alle reti dedicate.

Vulnerabilità

È la debolezza in procedure di sicurezza di reti di computer, controlli amministrativi, layout fisico, progettazione, configurazione, ecc., che potrebbe essere sfruttata da una potenziale minaccia per ottenere l'accesso a informazioni o per ostacolare processi cruciali.

W

WAN

(Wide Area Network)

Rete di medie grandi dimensioni che usa reti pubbliche per collegare i computer.

Water-holing

(Watering Hole Attack)
Tipologia di attacco informatico che ha come obiettivo una certa tipologia di siti web, prediletti da un gruppo di utenti ben definito che si intende danneggiare.

Web-defacement

Attacco a un sito web che ne modifica l'aspetto visivo, spesso con fini di protesta ad opera di un Hacktivista.

Whaling

(anche Whaling Phishing)
È una tipologia di attacco phishing mirato espressamente a violare account di alte figure dirigenziali all'interno di un'organizzazione (di qui l'espressione).

White Team

La squadra che supervisiona la competizione di simulazione di attacco tra team Red e Blue e giudica le sorti dell'evento.

Whitehat hacker

(hacker con il cappello bianco) è un soggetto che utilizza le sue skill in ambito informatico, reti, e sociali con l'intento di tutelare sistemi e reti e le informazioni in esso contenute.

Whitelist

(lista bianca) una lista che indica soggetti, domini, risorse liberamente accessibili o che hanno liberamente accesso a sistemi o risorse.
Il contenuto inoltrato da qualsiasi entità ad esso appartenente verrà accettato dal sistema.
È il meccanismo di spam filtering opposto a Blacklist.

Worm

I worms (i vermi) sono programmi simili ai virus che si riproducono e si copiano di file in file e di sistema in sistema usando le risorse di quest'ultimo e talvolta rallentandolo.
La differenza dai virus è che mentre loro usano i file per duplicarsi, i vermi usano i networks.

Z

Zero-day

(o anche 0-day)
Coincide con il giorno nel quale la parte interessata (un ente, la casa produttrice, ecc) viene a conoscenza di una vulnerabilità non documentata.
Lo Zero-day exploit viene utilizzato per qualsiasi vulnerabilità non ancora nota pubblicamente.
Grazie a questa lacuna nella sicurezza il malware sfrutta proprio il vantaggio di agire "liberamente" grazie al fattore sorpresa.

Zero-Trust

Principio di sicurezza usato all'interno dell'organizzazione che assume livello di fiducia zero per qualsiasi tipologia di transazione tra i sistemi aziendali, anche laddove la stessa provenga da una fonte, apparentemente, nota e sicura (es. Il computer di un dipendente).

Zip Bomb

(anche zip of death o decompression bomb)

Trattasi di un piccolo file compresso concepito per esaurire le risorse di sistema non appena viene aperto, espandendo le proprie dimensioni a dismisura ed occupando quindi completamente ram e spazio su disco.

Zombie

Un computer connesso alla rete infetto, che all'occorrenza può venire controllato da un hacker o malintenzionato e utilizzabile per un attacco ddos.