Minta Darkwah Oheneba, Alessandro Scattaglia, Marco Tranaso,
Emanuele Filippo Farfariello

Agnelli
SALESIANIDONBOSCO
TORINO

Gli argomenti che tratteremo sono:

- Sicurezza di un sistema informatico: valutazione dei rischi.
- Le minacce in rete all’informazione.
- Tipologie di attacchi informatici.
- Introduzione alla crittografia: a cosa serve e come funziona un sistema crittografico.
- Regole e misure da adottare per un accesso sicuro in rete.
- Frode informatica.
- Accesso abusivo ad un sistema informatico.
- Detenzione e diffusione abusiva di codici di accesso a sistemi.
- Diffusione di hardware e software diretti al danneggiamento di sistemi.
- Intercettazione o interruzione illecita di comunicazioni informatiche o telematiche.

Sicurezza di un sistema informatico: valutazione dei rischi

La valutazione dei rischi è un’analisi del sistema informativo di un’organizzazione mirata ad individuare potenziali vulnerabilità che possono mettere a rischio la sicurezza dei dati aziendali.

I rischi sono diversi e non banali, e aumentano di pari passo con la mole di dati sensibili trattati e la complessità della infrastruttura tecnologica utilizzata.

Agnelli
SALESIANIDONBOSCO
TORINO

Fasi della valutazione dei rischi

- Analisi del perimetro
- Identificazione dei Rischi
- Analisi dei Rischi Informatici
- Prima Valutazione Tecnica da sottoporre a Valutazione definitiva del Management
- Remediation
- Ripetizione del processo di Vulnerability Assessment
- Accorpamento dei processi effettuati

Agnelli
SALESIANIDONBOSCO
TORINO

Come si svolge la valutazione dei rischi

La valutazione del rischio informatico è un’analisi che serve ad avere una visione globale della posizione di un’azienda alla perdita o alla violazione dei dati. Molte volte l’azienda non è consapevole che le loro informazioni sono già disponibili su internet. La valutazione del rischio informatico consente di mappare quante, quali e dove sono le informazioni sull’azienda e sulle persone che vi orbitano attorno. In base a questo, poi, si scelgono le azioni di mitigazione del rischio da intraprendere.

Con la metodologia dell’ISEC, all’azienda viene consegnata una relazione esaustiva e sintetica dove vengono evidenziati i rischi rilevati e le rispettive criticità dell’azienda

Per quali scopi possono essere rubati i dati di un’azienda

Gli attaccanti tendono ad acquisire le informazioni per motivi diversi. Riuscendo ad accedere alla firma, al codice fiscale e alla mail di un VIP aziendale, potrebbero simulare una sostituzione di persona, per esempio.

È importante salvaguardare anche i dati reperibili da contatti, dipendenti, CV ecc. Gli attaccanti potrebbero mirare a ottenere informazioni su questi soggetti e assumerne l’identità per fare delle truffe. Un caso frequente è la contraffazione di comunicazioni ufficiali. Questo modo di procedere è definito social engineering, o ingegneria sociale.

Le minacce in rete all’informazione

Un virus informatico/una minaccia informatica è un programma con la capacità esclusiva di riprodursi e di penetrare in qualsiasi tipo di file eseguibile. Oltre alla moltiplicazione, alcuni virus/minacce informatiche hanno un altro elemento comune: una routine di danneggiamento che trasporta la carica distruttiva. Benché a volte si limitino a visualizzare messaggi o immagini, le cariche distruttive possono anche danneggiare file, formattare il disco rigido o causare danni di altra natura.

Tipologie di minacce:Virus/minaccia informatica

- Minacce informatiche: le minacce informatiche sono dei software progettati per infiltrarsi o danneggiare un computer all'insaputa del proprietario.
- Cavalli di Troia: un cavallo di Troia è un programma dannoso mascherato da applicazione innocua. Contrariamente ai virus e alle minacce informatiche, i cavalli di Troia non si moltiplicano ma possono essere altrettanto dannosi. Un esempio di cavallo di Troia è un'applicazione che a prima vista serve per eliminare virus/minacce informatiche dai computer ma in realtà li introduce.
- Backdoor: un programma backdoor è un metodo per oltrepassare i normali processi di autenticazione così da permettere l'accesso remoto a un computer e ottenere accesso alle informazioni rimanendo, nel frattempo, nascosto.

Tipologie di minacce: Spyware/grayware

- Spyware: gli spyware sono software che si installano sul computer senza il consenso o la consapevolezza dell'utente per raccogliere o trasmettere informazioni personali.
- Strumenti per hacker: uno strumento per hacker è un programma o un gruppo di programmi progettato per l'attività degli hacker.
- Keylogger: i keylogger sono dei software che registrano tutte le sequenze di tasti digitate dall'utente. Queste informazioni possono quindi essere recuperate da un hacker che le utilizza per i propri scopi.
- Bot: un bot (diminutivo di "robot") è un programma che opera come agente per un utente o per un altro programma e simula un'attività umana. I bot possono essere utilizzati per coordinare un attacco automatico su computer collegati in rete.

Tipologie di attacchi informatici

Gli attacchi informatici sono un’azione offensiva rivolta alle infrastrutture, dispositivi o reti informatiche, con l’intento di rubare, modificare o distruggere dati o sistemi informatici.

Ecco dunque i principali 10 tipi di attacchi informatici più comuni:

- Malware
- Phishing
- Attacco man in the middle
- Attacco denial-of-service
- SQL injection
- Attacchi zero-day
- Password cracking

Phishing

Il phishing consiste nell'inviare comunicazioni fraudolente che sembrano provenire da una fonte affidabile, di solito una e-mail. L'obiettivo è quello di rubare dati sensibili come carte di credito e informazioni di accesso, o di installare un malware sul computer della vittima. Il phishing è una minaccia informatica sempre più comune.

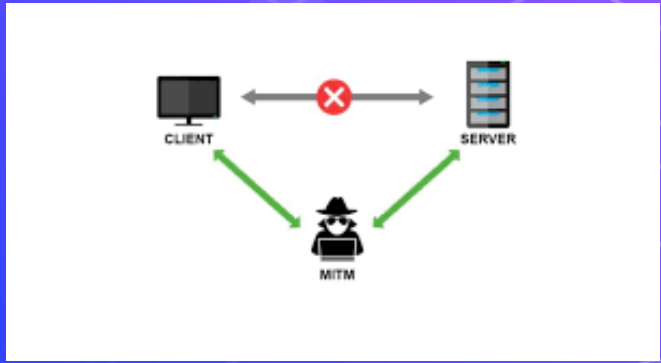
Come funziona il phishing?

I criminali informatici creano e-mail e messaggi di testo che sembrano legittimi ma in realtà contengono collegamenti, allegati o esche pericolosi che inducono i loro obiettivi a compiere un'azione rischiosa e sconosciuta. In breve:

- I phisher usano spesso le emozioni delle vittime per costringere i destinatari ad aprire allegati o fare clic sui collegamenti.
- Gli attacchi di phishing sono progettati per sembrare provenire da aziende e individui legittimi.
- Basta un solo attacco di phishing riuscito per compromettere la tua rete e rubare i tuoi dati, motivo per cui è sempre importante pensare prima di fare un clic.

Attacco man in the middle

Gli attacchi man in the middle (MitM), noti anche come attacchi di intercettazione, si verificano quando gli hacker si inseriscono in una transazione fra due parti. Una volta che hanno interrotto il traffico, i criminali possono filtrare e rubare i dati.



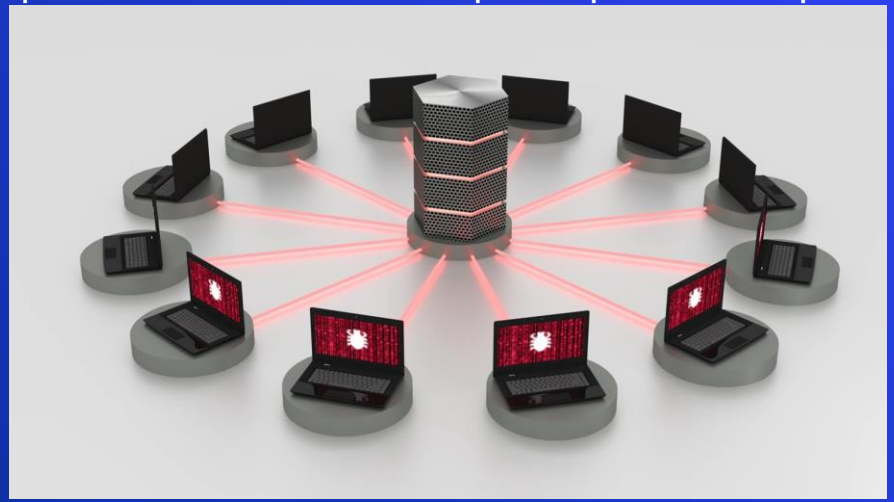
I punti di ingresso comuni per gli attacchi MitM sono due:

1. Reti Wi-Fi pubbliche, senza saperlo, il visitatore passa tutte le informazioni all'hacker.

2. Una volta che il malware ha violato un dispositivo, un hacker può installare il software per elaborare tutti i dati della vittima.

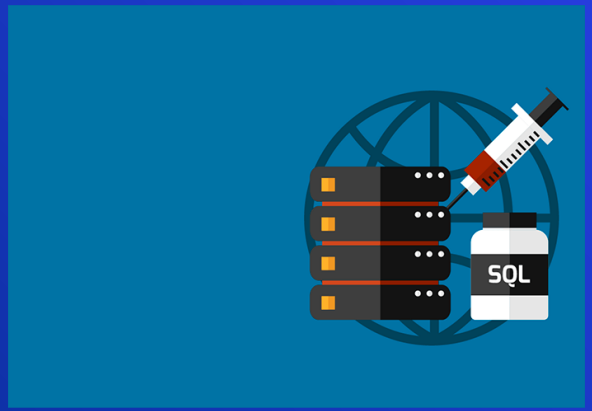
Attacco denial-of-service

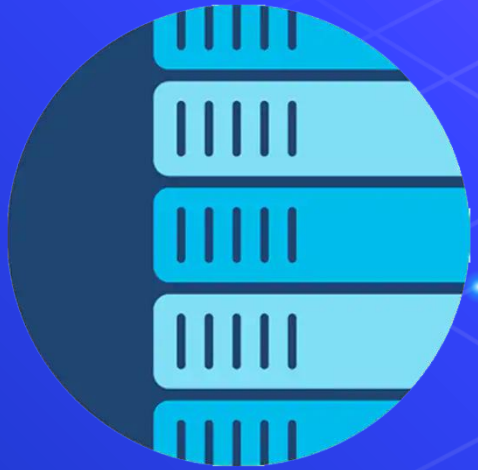
Un attacco denial-of-service invia enormi flussi di traffico a sistemi, server o reti per esaurire le risorse e la larghezza di banda. Di conseguenza, il sistema sotto attacco non è più in grado di soddisfare le richieste legittime. Per lanciare un attacco di questo tipo, gli hacker possono anche utilizzare più dispositivi compromessi.



SQL injection

Una SQL (Structured Query Language) injection si verifica quando un hacker inserisce codice malevolo in un server che utilizza SQL e lo forza a rendere pubbliche informazioni che normalmente dovrebbero rimanere riservate. Per effettuare una SQL injection, è sufficiente aggiungere del codice malevolo nella casella di immissione di un sito web vulnerabile.





Attacchi zero-day

Un attacco zero-day colpisce non appena viene scoperta una vulnerabilità nella rete, ma prima che sia possibile implementare una patch o una soluzione. Gli hacker prendono di mira la vulnerabilità rilevata durante questa finestra temporale. Il rilevamento delle minacce di vulnerabilità zero-day richiede una consapevolezza costante.

Password cracking

Il password cracking è il processo di recupero delle password da informazioni o dati che sono state immagazzinate o trasmesse da un sistema informatico. L'obiettivo dell'operazione può essere aiutare un utente a recuperare una password dimenticata, per l'amministratore serve a controllare le password semplici da craccare o può essere utilizzato per avere accesso non autorizzato in un sistema.

La maggior parte dei tools utilizzati per questo processo avranno sicuramente successo con password semplici, mentre se fossero complicate, si potrebbe non riuscire a trovarle. Le password possono essere di diversi tipi, in ordine di semplicità.

La crittografia

Crittografia deriva da crittologia che vuol dire **scritture nascoste.** Non permettere alle persone non autorizzate di poter vedere il *messaggio nascosto* *chiamato* ***crittogramma.***

Ma la definizione principale è: l'utilizzo di algoritmi matematici a sequenze di caratteri avvenendo su una base di una chiave segreta.

Le tipologie della crittografia

- **SIMMETRICA**
- con una chiave singola tra mittente e destinatario.
- **ASIMMETRICA**
- con due chiavi differenti chiave.
- di cifratura pubblica e decifratura privata.

I protocolli

I protocolli utilizzati dalla crittografia per oscurare le comunicazioni di dati sono:

- SSH (metodo dove dei dispositivi possono comunicare in maniera sicura).
- SSL/ TSL (metodo utilizzato per il web come protezione delle comunicazioni e degli scambi informatici tra client e server).
- HTTPS (metodo derivato dal HTTP, utilizza anche il metodo SSL/TSL per amplificare ulteriormente la protezione contro gli attacchi).

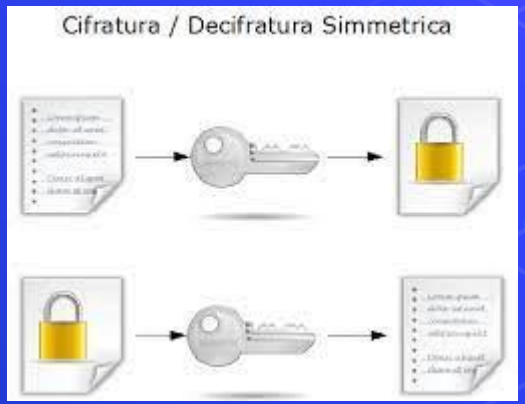
Gli algoritmi della crittografia simmetrica

Gli algoritmi più utilizzati del periodo dalla crittografia simmetrica sono:

DES (sviluppato negli Stati Uniti, per la finanza, con 64 bit)

IDEA (sviluppato in Svizzera, per il politecnico federale, 128 bit)

RC4 (sviluppato a New York, per la sicurezza informatica, con lunghezza arbitraria)

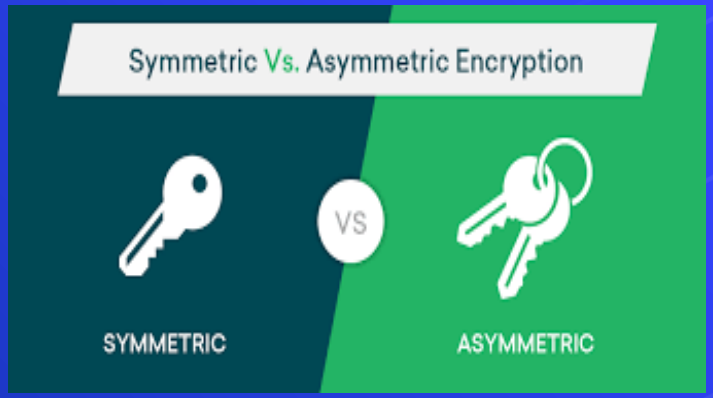


Gli algoritmi della crittografia asimmetrica

Gli algoritmi più utilizzati del periodo dalla crittografia asimmetrica sono:

RSA (sviluppato da Rivest, Shamir e Adelman, per la firma digitale, con 512/ 786/ 1024 bit)

PGP (sviluppato da Phil Zimmerman, per la chiave pubblica e lo scambio di documenti) IL PIU' USATO AL MONDO



La crittografia ai giorni nostri

L’ algoritmo di crittografia più usato è **AES** basato sulla cifratura a blocchi.

La crittografia è utilizzata in particolare per la sicurezza informatica, la protezione dei dati e dei messaggi di un dispositivo.

In questo caso è usato per i login online per proteggere password e nomi utente.

La crittografia **END TO END** ad esempio è un sistema di comunicazione cifrato che impedisce l’accesso ad altre persone non autorizzate.

L’hash per la crittografia

Una funzione molto importante ed essenziale della crittografia è l’**HASH** che rende un file o un messaggio un breve stringa fissa (hash value).

Utilizzato soprattutto per controllare l'autenticità del messaggio e che non sia stato modificato.

Anche solo una modifica nel messaggio modifica il valore dell’hash. L’hash non deve essere semplice da modificare per conoscere il messaggio.

MD5 e SHA - 1 sono i vecchi algoritmi più in uso un tempo, ma ad oggi **SHA - 2** è l’algoritmo più “di voga”.

Per un accesso sicuro:

Le regole da utilizzare per un buon e sicuro accesso:

- avere un atteggiamento serio e vigilante
- tenere attive le funzioni privacy
- navigare in posti sicuri
- navigare in connessione sicura
- vigilanza nei dati che si scaricano
- fare compere in luoghi sicuri e certificati

Modulo 1
ICT NELLA VITA DI OGNI GIORNO

1. Concetti di sicurezza
2. Malware
3. Sicurezza in rete
4. Controllo di accesso
5. Uso sicuro del Web
6. Comunicazioni
7. Gestione sicura dei dati

Agnelli
SALESIANIDONBOSCO
TORINO

MALWARE

Il termine **malware** definisce software malevoli (spyware, ransomware, virus e worm). Il malware viola è una rete che sfruttando una vulnerabilità, in genere quando un utente seleziona un link pericoloso o apre un allegato ricevuto via e-mail installa il software dannoso. Una volta all'interno del sistema, il malware può:

- *Bloccare l'accesso* ai componenti principali della rete **(ransomware)**
- *Installare malware* o altri software dannosi
- *Acquisire informazioni* di nascosto trasmettendo dati dal disco rigido **(spyware)**
- *Interferire con alcuni componenti* e rendere il sistema inutilizzabile

Come difendersi dalle minacce in rete

1. **Firewall e antivirus**

Il fatto che ci stiamo digitalizzando sempre di più ha portato al fatto che molto spesso le minacce sono derivanti da Internet. Filtrare i dati e le informazioni che in continuazione passano per il sistema informatico aziend

2. **Misure di cybersecurity**

Firewall e antivirus sono dei punti di partenza. La cybersecurity di un’azienda deve assicurarsi di:

- **Modificare le password**
- **Backup** (per poter avere il salvataggio dell’ultimo lavoro)
- **Conservare i backup** (rischio basso di non avere un backup funzionante)
- Fare controlli di struttura generale **(manutenzione)**
- **Protezione delle reti**

3. **Data Center**

Un centro di elaborazione dati viene chiamato CED, parte essenziale e importantissima di una azienda che si assicura che la parte informatica in utilizzo sia protetta dai malintenzionati.

Firewall

Il FIREWALL (dall'inglese tagliafuoco) è un dispositivo utilizzato per la protezione e la sicurezza della rete, con il compito di controllare il traffico di dati di entrata ed uscita.

Il firewall si trova sia nella rete esterna (Internet) che nella rete interna (dell'azienda), e usa due criteri in particolare:

Default - deny: nel quale viene permesso solo quello che è autorizzato.

Default - allow: nel quale viene bloccato solo chi viene vietato.

Frode informatica con pos

Ci sono molti modi per commettere delle azioni illegali tramite l’informatica, penetrando in un PC. Si possono attuare queste azioni tramite POS (apparato elettronico) usato per rubare dati delle carte di credito. I metodi in particolare con il POS sono:

- Intercettazione dei dati: dove vengono rubati i dati di carte di credito rubate o false grazie al POS.
- Dirottamento dei dati: dove vengono falsificate le coordinate dell’accredito del negoziante e viene dirottato l’importo.

Frode informatica alterando un sistema operativo

Alterare il funzionamento di un sistema operativo e qualsiasi dati a sé collegati è un reato. In particolare queste azioni illegali sono:

- Il modificare il normale funzionamento del sistema operativo con l'elaborazione e trasmissione dei dati.
- Agire senza diritto su dati ed informazioni di un sistema operativo.
- Agire sulle informazioni collegate fra loro, passando da un' informazione all'altra.

Frodi con le aste online

Le aste online sono un altro modo per commettere frodi informatiche.

Le aste online sono soprattutto utilizzate negli e-commerce dato che si basano su una reciproca fiducia, e per questo i siti per le aste sono dotati di un’iscrizione gratuita per assicurarsi di poter eseguire un controllo sui dati da te registrati.

Queste operazioni sono necessarie per una protezione elevata nelle transizioni finanziarie e per la sicurezza dei partecipanti.

Accesso abusivo ad un sistema informatico

Articolo 615 ter Codice Penale

L’articolo 615 del Codice Penale dice che:

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza(password) ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La reclusione può essere da 1 a 5 anni se:

1) se il fatto è commesso da un pubblico ufficiale, con abuso dei poteri, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema.
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato.
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi che contiene.

Invece se i danni erano riguardanti l’ordine pubblico o interesse digitale, la pena può arrivare fino a 8 anni di reclusione.

L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, ovvero la password. L'art. 615-ter c.p. punisce la semplice intrusione ancor prima di valutare l'ipotesi di danneggiamento o furto dei dati.

Il reato può anche essere causato da soggetti legittimati all'uso del sistema, autorizzati ad accedere solo ad una parte dei dati contenuti in memoria.

In tal caso il sistema protetto diviene quella parte di memoria a cui l'accesso non è autorizzato.

Detenzione e diffusione abusiva di codici di accesso ai sistemi

La detenzione o diffusione abusiva di codici di accesso è un reato informatico previsto dall’articolo 615-quater del codice penale

“Chiunque, al fine di procurare a sé o ad altri un danno, abusivamente si procura, riproduce, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo”

L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo.

Può infatti trattarsi di una password, di un codice d'accesso o semplicemente di informazioni che consentano di eludere le misure di protezione.

Non rientra l'acquisizione illegittima di carte di credito telefoniche in quanto l'illecito utilizzo permetterebbe solo di usufruire delle prestazioni telefoniche dell'apparecchio.

Le condotte punite se realizzate abusivamente dall'art. 615-quater c.p. sono molteplici:

- l'utilizzo non autorizzato di codici d'accesso;
- la diffusione che si manifesta nel rendere disponibili tali codici ad un numero indeterminato di soggetti;
- la comunicazione che consiste nel rendere disponibili tali codici ad un numero limitato di soggetti;
- la consegna che riguarda cose materiali come può essere un token di accesso ad un servizio di home banking(banca online);
- la comunicazione o diffusione di istruzioni che permettono di eludere le protezioni di un sistema.

Resta irrilevante il fatto che i codici siano stati procurati abusivamente o mediante l'autonoma elaborazione.

Esistono anche gli accessi abusivi ai social network o account di e-banking mediante le credenziali del proprietario dell'account ma, ovviamente, a sua insaputa. Il reato è commesso quando si esegue l'accesso, indipendentemente dalle azioni successive, che possono comportare l'infrazione di altre norme e, di conseguenza, altri reati informatici.

La Corte di Cassazione ha stabilito che per dimostrare la sussistenza del reato può bastare l'identificazione dell'indirizzo IP di chi ha eseguito l'accesso abusivo.

L'articolo 640 ter del codice penale rende perseguibili l'accesso abusivo a un sistema informatico o telematico protetto da misure di sicurezza.

Diffusione di hardware e software diretti al danneggiamento di sistemi.

L'art. 635 bis prevede espressamente che la sua applicazione non avvenga quando fattispecie simili costituiscono *più gravi reati*. Viene, infatti, considerato reato autonomo quello previsto e punito dall'art 420 Codice Penale Attentato a impianti di pubblica utilità *Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.*

Intercettazione o interruzione illecita di comunicazioni informatiche o telematiche

Articolo 617 quater Codice Penale

“Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.”

Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

GRAZIE PER L'ATTENZIONE

Agnelli
SALESIANIDONBOSCO
TORINO