

Ciclo di webinar in diretta

Sicurezza informatica & Protezione dei dati negli enti locali

Relatore: Dottor Antonio Guzzo

Sistemi di gestione integrata e Regolamento UE
679/2016 GDPR. I reati informatici nella pubblica
amministrazione 15-02-2024

ASMEL - Associazione per la Sussidiarietà e la
Modernizzazione degli Enti Locali

Email info@dpointrete.it

Numero Verde 800.16.56.54 (int.3)

Web: www.dpointrete.it, www.asmel.eu



Sommario

- *Le misure di sicurezza nell'era del Regolamento Europeo sul Data Protection - La sicurezza del trattamento dei dati*
- *I reati informatici*
- *La computer forensics*
- I reati informatici alla luce della legge 48/2008
- Il furto di identità digitale
- I reati informatici introdotti dal Dlgs 196/2003 così come modificato dal Dlgs 101/2018
- Le novità introdotte dal ddl cybersecurity approvato nel consiglio dei ministri del 25-01-2024

***“Le misure di sicurezza nell’era del Regolamento Europeo
sul Data Protection”***

Sommario

- Il concetto di sicurezza informatica
- Le misure di sicurezza secondo la normativa vigente ed il GDPR 679/2016
- Le minacce informatiche



La sicurezza informatica

- ▶ Per sicurezza informatica intendiamo secondo wikipedia *"quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati. I principali aspetti di protezione del dato sono la confidenzialità, l'integrità e la disponibilità"*. Ma tale definizione dataci da wikipedia non si applica al contesto ambientale in cui andiamo ad operare. Per cui la definizione di sicurezza informatica è la seguente:
- ▶ **la sicurezza informatica è quando un sistema si comporta come noi ci aspettiamo.**



La normativa – Le misure minime di sicurezza e il GDPR

Il 4 aprile 2017 è stata pubblicata, sulla Gazzetta Ufficiale n. 79, la circolare AgID n.1/2017 contenente le misure minime di sicurezza ICT che ne imponeva l'adozione al 31-12-2017.



Compliance e la circolare Agid

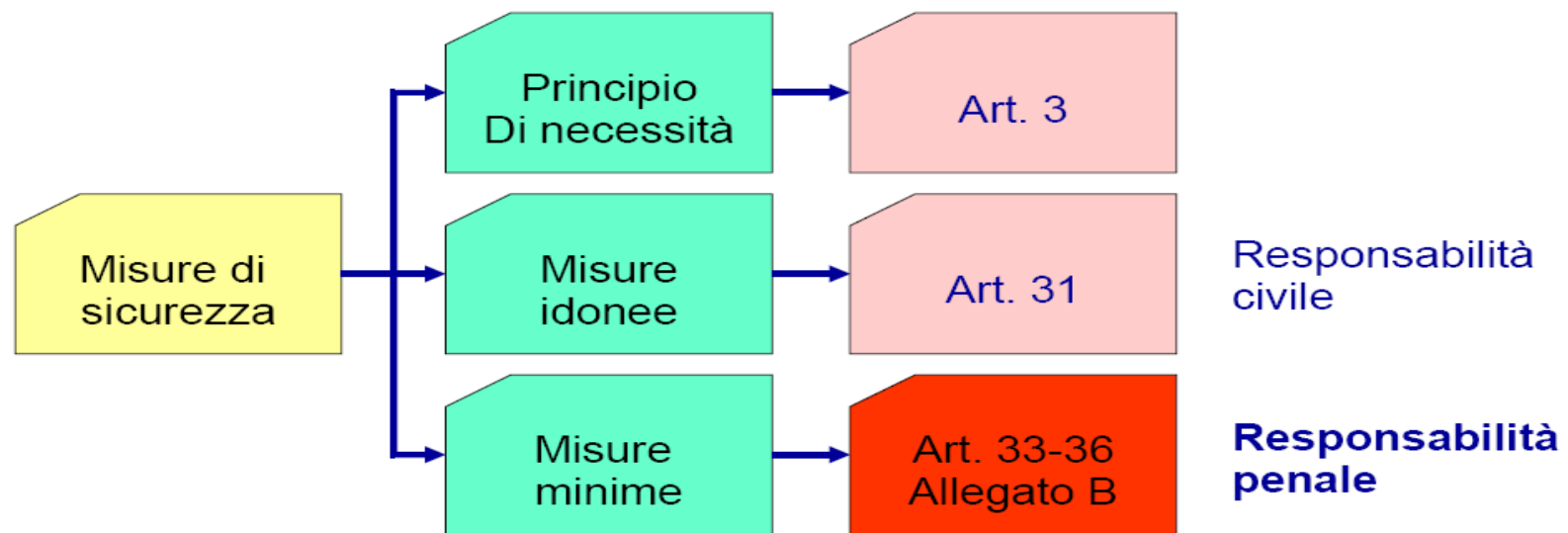
- ▶ **Compliance, la circolare Agid**
- ▶ Oggi la stragrande maggioranza degli enti locali non è “compliance” in termini di adozione di misure tecniche ed organizzative informatiche e soprattutto non ha preso coscienza del grave rischio sanzionatorio a cui va incontro. Inoltre tale compliance in termini di sicurezza informatica non fa altro che riprendere ciò che contemplava la circolare [Agid](#) del 18 Aprile 2017 n° 2/2017 così dettagliate:
- ▶ vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- ▶ impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- ▶ impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

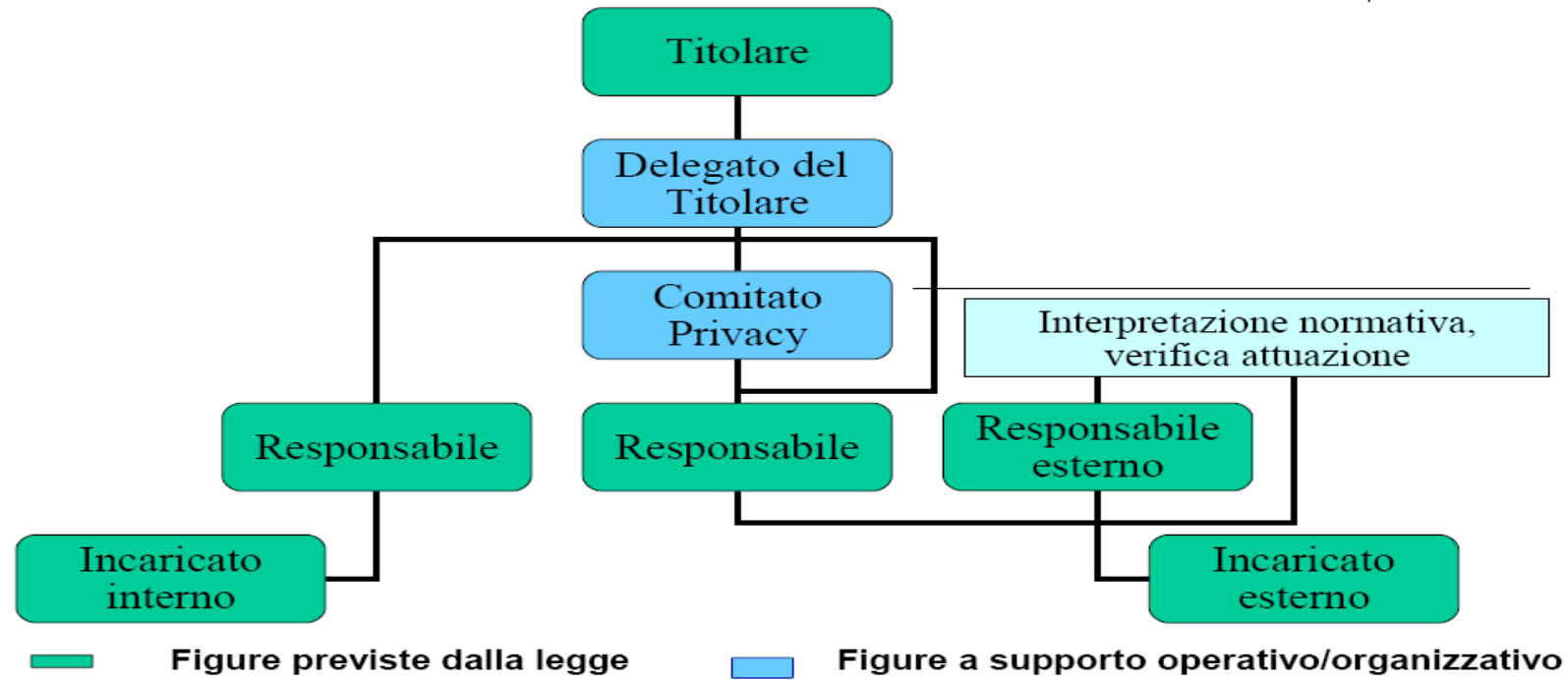


Compliance e la circolare Agid

- ▶ impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
- ▶ garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- ▶ garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
- ▶ garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- ▶ impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- ▶ garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- ▶ garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).







Misure minime di sicurezza

Dlgs 196/2003

- ▶
- ▶ Artt. da 33 a 36 del codice
- ▶ All. B: Disciplinare tecnico in materia di misure minime di sicurezza
- ▶ Sistema di autenticazione informatica (punti 1-11)
- ▶ Sistema di autorizzazione (12-14)
- ▶ Altre misure di sicurezza
- ▶ Documento programmatico sulla sicurezza
- ▶ Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
- ▶ Misure di tutela e garanzia
- ▶ Trattamenti senza l'ausilio di strumenti elettronici

Autenticazione: generalità (1/4)

- ▶ Il trattamento è consentito solo agli Incaricati con credenziali (che possono essere relative anche a più trattamenti)
- ▶ Credenziali: “ciò che si sa”, “ciò che si possiede”, “ciò che si è”
- ▶ Gestione “sicura” delle credenziali

Autenticazione: userID 2/4

- ▶ Ogni “userID” può essere assegnato a un solo Incaricato, anche in tempi diversi
- ▶ Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione

Autenticazione: password 3/4

- ▶ Nel caso di utilizzo di password:
- ▶ custodia diligente e mantenimento della segretezza da parte dell'Incaricato
- ▶ minimo 8 caratteri (o il massimo consentito)
- ▶ non deve contenere riferimenti all'utente
- ▶ modificata dall'utente al primo utilizzo e almeno ogni 6 mesi (3 mesi per dati sensibili e giudiziari)
- ▶ Politica “clear desk - clear screen”, Logoff automatico

Autenticazione 4/4

- ▶ Le credenziali non utilizzate per almeno sei mesi devono essere disattivate (tranne quelle “tecniche”)
- ▶ Le credenziali devono essere disattivate in caso di perdita dei requisiti dell’Incaricato
- ▶ Custode delle password, per garantire la disponibilità o la sicurezza del sistema
- ▶ Formazione

Autenticazione: conclusioni

- ▶
- ▶ E' opportuno, se non indispensabile, utilizzare un software per la gestione degli account (user provisioning)

Altre misure: backup 2/2

- ▶ Procedure scritte e diffuse a tutti gli interessati
- ▶ Definizione delle responsabilità
- ▶ procedure che disciplinino il ripristino dei backup (disaster recovery e business continuity)
- ▶ Modalità di aggiornamento delle procedure

Dati sensibili e giudiziari

- ▶ I dati sensibili o giudiziari sono protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici (ad es.: firewall, IDS)
- ▶ Gestione dei supporti rimovibili su cui sono stati immagazzinati i dati (accesso controllato ai dispositivi, distruzione)
- ▶ Idonee misure per garantire la disponibilità del servizio (tempo certo di ripristino, max 7 giorni)
- ▶ Dati relativi a stato di salute o vita sessuale: trattamento disgiunto dai dati identificativi
- ▶ Formazione

Misure di tutele e garanzia

- ▶ Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico
- ▶ Il Titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza

Trattamento senza strumenti elettronici

- ▶ Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali
- ▶ Aggiornamento (almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati
- ▶ Gli atti e i documenti contenenti dati sensibili o giudiziari sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione
- ▶ L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate

Obblighi di sicurezza

► Art. 31

(Obblighi di sicurezza)

- *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di **accesso non autorizzato** o di **trattamento non consentito** o non conforme alle finalita' della raccolta.*

Considerazioni

- ▶ Le “misure minime” sono tutt’altro che banali ma incomplete (protezione dei dati personali e non del patrimonio informativo complessivo)
- ▶ Occorre tendere alla sicurezza “globale” della Organizzazione seguendo metodologie standard e collaudate (es. ISO27001/17799)
- ▶ Un approccio corretto e completo alla sicurezza è “pagante” nel medio-lungo periodo

I livelli di applicazione

Minimo

È quello al quale ogni azienda/pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

Standard

Può essere assunto come base di riferimento nella maggior parte dei casi.

Avanzato

Deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Le classi di misure

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime **due classi** di misure, nonché la protezione della configurazione, che è quella immediatamente **successiva**.



Le classi di misure

La **quarta classe** deve la sua priorità alla duplice rilevanza dell'analisi delle vulnerabilità. In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.



Le classi di misure

La **quinta classe** è rivolta alla gestione degli utenti, in particolare gli amministratori.

La **sesta classe** deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.



Le classi di misure

Le copie di sicurezza, **settima classe**, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.

L'ultima classe, la Protezione dei Dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.



Il dettaglio delle diverse classi di misura

INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.



Il dettaglio delle diverse classi di misura

VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.



Il dettaglio delle diverse classi di misura

COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni Rilevanti



ABSC

**GLI AGID BASIC SECURITY CONTROL DA
IMPLEMENTARE PER OTTENERE IL LIVELLO MINIMO DI
SICUREZZA SOTTO IL QUALE OBBLIGATORIAMENTE
NESSUNA AZIENDA/PA PUO' SCENDERE**



Le famiglie di controlli

- ABSC 1 (CSC 1): Inventario dei dispositivi autorizzati e non autorizzati
- ABSC 2 (CSC 2): Inventario dei software autorizzati e non autorizzati
- ABSC 3 (CSC 3): Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- ABSC 4 (CSC 4): Valutazione e correzione continua della vulnerabilità
- ABSC 5 (CSC 5): Uso appropriato dei privilegi di amministratore
- ABSC 8 (CSC 8): Difese contro i malware
- ABSC 10 (CSC 10): Copie di sicurezza
- ABSC 13 (CSC 13): Protezione dei dati

ABSC 1 (CSC 1): Inventario dei dispositivi autorizzati e non autorizzati

Il livello minimo prevede l'implementazione, l'aggiornamento e la gestione dell'inventario di tutti i sistemi di rete (compresi i dispositivi di rete stessi) registrando almeno l'indirizzo IP.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

1.1.1 Implementare un inventario delle risorse attive correlato a quello ABSC 1.4

1.3.1 Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.

1.4.1 Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.



ABSC 2 (CSC 2): Inventario dei software autorizzati e non autorizzati

Il livello minimo prevede la realizzazione dell'elenco dei software autorizzati (e relative versioni), con regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati. L'installazione di software non presenti nell'elenco è vietata.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

2.1.1 Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.

2.3.1 Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.



ABSC 3 (CSC 3): Proteggere le configurazioni di hardware e software sui dispositivi

Il livello minimo di questa classe di controlli prevede la definizione di configurazioni standard per tutti i sistemi (server, workstation, ecc.), con il tassativo rispetto di tali standard nelle fasi di installazione o ripristino dei sistemi. Le immagini di installazione dei sistemi devono essere memorizzate offline e tutte le operazioni di amministrazione remota devono essere eseguite tramite connessioni protette.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

3.1.1 Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.

3.2.1 Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.

3.2.2 Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.

3.3.1 Le immagini d'installazione devono essere memorizzate offline.

3.4.1 Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).



ABSC 4 (CSC 4): Valutazione e correzione continua della vulnerabilità

Il livello minimo prevede la ricerca delle vulnerabilità tramite strumenti automatici ad ogni modifica della configurazione; detti strumenti devono fornire agli amministratori di sistema report con indicazione delle vulnerabilità più critiche. Non solo i sistemi devono essere aggiornati, ma anche gli stessi strumenti di scansione. Questa classe di controlli impone l'installazione sistematica di patch e contromisure idonee a contrastare le vulnerabilità riscontrate. Va inoltre implementato un adeguato piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati; tale piano deve anche prevedere le azioni da svolgere per la risoluzione delle vulnerabilità individuate.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

4.1.1 Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.

4.4.1 Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.

4.5.1 Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.



ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

4.5.2 Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.

4.7.1 Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.

4.8.1 Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).

4.8.2 Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.



ABSC 5 (CSC 5): Uso appropriato dei privilegi di amministratore

Il livello minimo della classe di controlli relativa agli amministratori di sistema definisce una specifica policy di gestione degli utenti con diritti amministrativi, che disciplini i limiti nei privilegi attribuiti e l'inventario dei profili abilitati. Tale policy prevede tutte le accortezze che si rendono necessarie per l'adeguata gestione degli amministratori di sistema, dai controlli sulle scadenze delle password alla creazione di profili nominativi e individuali (non generici). E' curioso rilevare come in questa classe di controlli, le azioni relative al tracciamento dei log degli amministratori siano definite come livello "standard", mentre rappresentano un obbligo di legge sancito da un provvedimento del Garante Privacy sugli amministratori di sistema del 2008.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

5.1.1 Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

5.1.2 Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.

5.2.1 Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

5.3.1 Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.



ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

5.7.1 Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).

5.7.3 Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).

5.7.4 Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).

5.10.1 Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.



ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

5.10.2 Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.

5.10.3 Le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.

5.11.1 Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

5.11.2 Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.



ABSC 8 (CSC 8): Difese contro i malware

Il livello minimo impone l'installazione e l'aggiornamento automatico di sistemi antimalware, firewall e Intrusion Prevention Systems (IPS). Si deve disabilitare inoltre l'esecuzione automatica di tutti quei sistemi che potrebbero inavvertitamente attivare una minaccia (es. apertura degli allegati delle email, esecuzione di macro, eseguibili lanciati da chiavette USB, ecc). Sempre in chiave preventiva, si deve prevedere l'adozione di strumenti filtraggio dei contenuti, sia sulla navigazione internet che sulla posta elettronica.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

8.1.1 Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.

8.1.2 Installare su tutti i dispositivi firewall ed IPS personali.

8.3.1 Limitare l'uso di dispositivi esterni a quelli necessari per le attività **aziendali**.

8.7.1 Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.



ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

8.7.2 Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.

8.7.3 Disattivare l'apertura automatica dei messaggi di posta elettronica.

8.7.4 Disattivare l'anteprima automatica dei contenuti dei file.

8.8.1 Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.



ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

8.9.1 Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.

8.9.2 Filtrare il contenuto del traffico web.

8.9.3 Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).



ABSC 10 (CSC 10): Copie di sicurezza

Il livello minimo di sicurezza contempla una copia almeno settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema (in linea con le misure minime di sicurezza previste dal Codice della Privacy, anche se perdere una settimana di lavoro potrebbe essere troppo penalizzante per una PA). Si pone una certa attenzione anche alla riservatezza delle informazioni contenute nelle copie di sicurezza, tramite adeguata protezione fisica o mediante cifratura delle informazioni sottoposte a salvataggio. Infine, è necessario garantire che almeno una delle copie non sia permanentemente accessibile dal sistema stesso, onde evitare che eventuali attacchi al sistema possano coinvolgere anche le sue copie di sicurezza.

ABSC 13 (CSC 13): Protezione dei dati

Il livello minimo da garantire stabilisce di effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza, ai quali applicare una protezione crittografica. Inoltre, si deve prevedere il blocco del traffico da e verso url presenti in una blacklist.

Art. 32 GDPR sicurezza dei dati personali Da misure minime di sicurezza si passa a misure adeguate di sicurezza

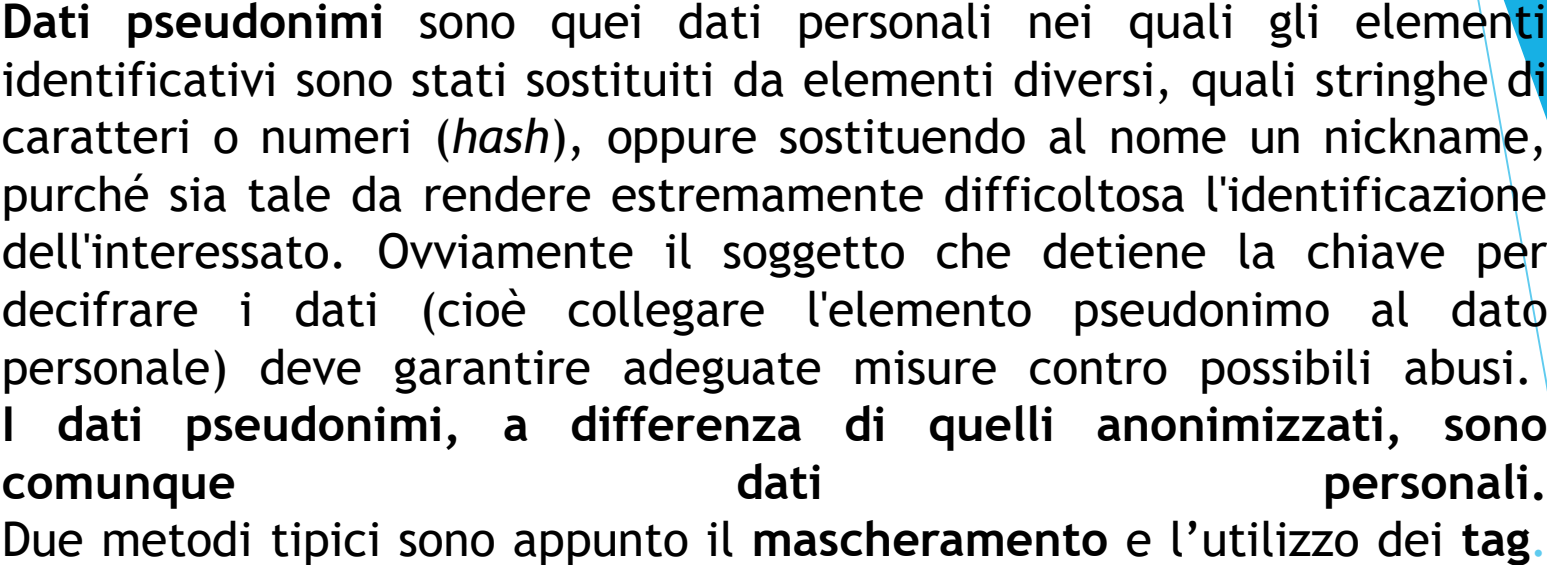
Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

► PSEUDONIMIZZAZIONE





▶ DATI PSEUDONIMI

One time Pad

Noto anche come algoritmo di password usa e getta. Usato nelle tecniche di banking on line, in cui si dispone di un codice che può essere utilizzato una sola volta.

WEP

Protocollo dello standard 802.11 dello IEEE, che significa Wire Equivalent Privacy cioè che si prefigge di garantire un livello di privacy che è equivalente a quello di una rete cablata. Una rete wireless utilizza come mezzo trasmissivo l'aria che, a differenza di una rete su cavo, non si può chiudere e circoscrivere (su una rete cablata un intruso deve comunque connettersi ad essa attraverso le prese per poter attuare i suoi attacchi).



► TECNICHE DI CRITTOGRAFIA

Algoritmi simmetrici (o a chiave simmetrica o privata) e asimmetrici (a chiave pubblica)

DES

Algoritmo a chiave simmetrica che oramai non viene più utilizzato ma che è stato utilizzato per vario tempo e quindi è stato uno degli algoritmi più conosciuti dal punto di vista di attacchi e di vulnerabilità.

Gli algoritmi a chiave simmetrica (o privata) si chiamano così perché si basano sulla condivisione della stessa chiave. Esiste un principio fondamentale, noto come *principio di kerchoff*, secondo cui la robustezza del metodo si basa sulla segretezza delle chiavi.



► TECNICHE DI CRITTOGRAFIA

Crittografia a chiave asimmetrica o pubblica

il primo sistema di crittografia a chiave pubblica passò alla storia come sistema di crittografia Diffie Hellman ma in realtà l'idea originaria fu di Merkle. L'idea è molto semplice: si usano chiavi separate per cifrare e decifrare cioè se qualcuno vuole scambiare delle informazioni le cifra con la chiave usata per cifrare e il destinatario delle informazioni le decifra con un'altra chiave, usata per decifrare



Firma Digitale

► TECNICHE DI CRITTOGRAFIA

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. **Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.**

► **ADEGUATI LIVELLI DI SICUREZZA**

Altri strumenti di prevenzione

- ▶ **SVILUPPO E MANUTENZIONE DI SISTEMI** (System Development and Maintenance)
Accertare che la sicurezza sia stata costruita all'interno delle operazioni di sistema;
- ▶ Per impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione;
- ▶ Per proteggere la riservatezza l'autenticità e l'integrità delle informazioni;
- ▶ Per accertarsi che le attività di progetto e supporto alle attività siano condotte in modo sicuro e per mantenere la sicurezza del software e dei dati del sistema

LA BUSINESS CONTINUITY

- ▶ GESTIONE CONTINUITA'OPERATIVA (Business Continuity Management)
- ▶ Neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari e dagli effetti dei guasti
- ▶ ADEGUATEZZA (Compliance)
- ▶ Evitare il mancato rispetto delle leggi civili, penali e di qualsiasi requisito di sicurezza;
- ▶ Per elevare l'efficacia e minimizzare l'interferenza per il processo di verifica del sistema

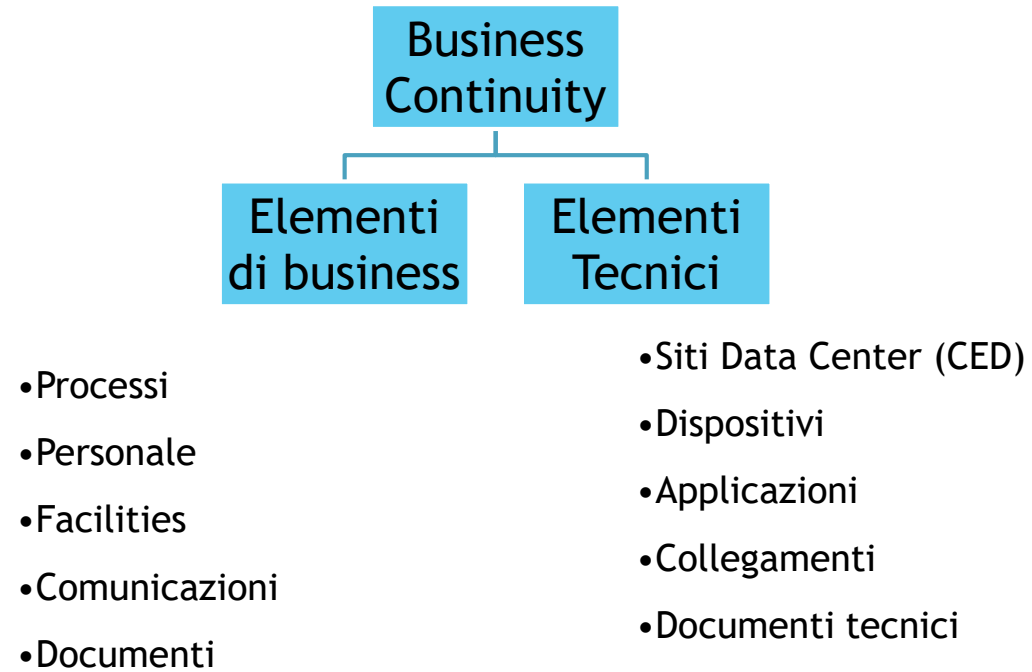
ALTRI STRUMENTI

- ▶ PRINCIPALI TECNICHE DI DIFESA
- ▶ CRITTOGRAFIA
- ▶ SISTEMA DI AUTENTICAZIONE
- ▶ FIRMA DIGITALE
- ▶ FIREWALL
- ▶ IDS (intrusion detection system)
- ▶ NIDS(network detention system)
- ▶ HONEYPOT
- ▶ STEGANOGRAFIA
- ▶ ANTI-SPYWARE

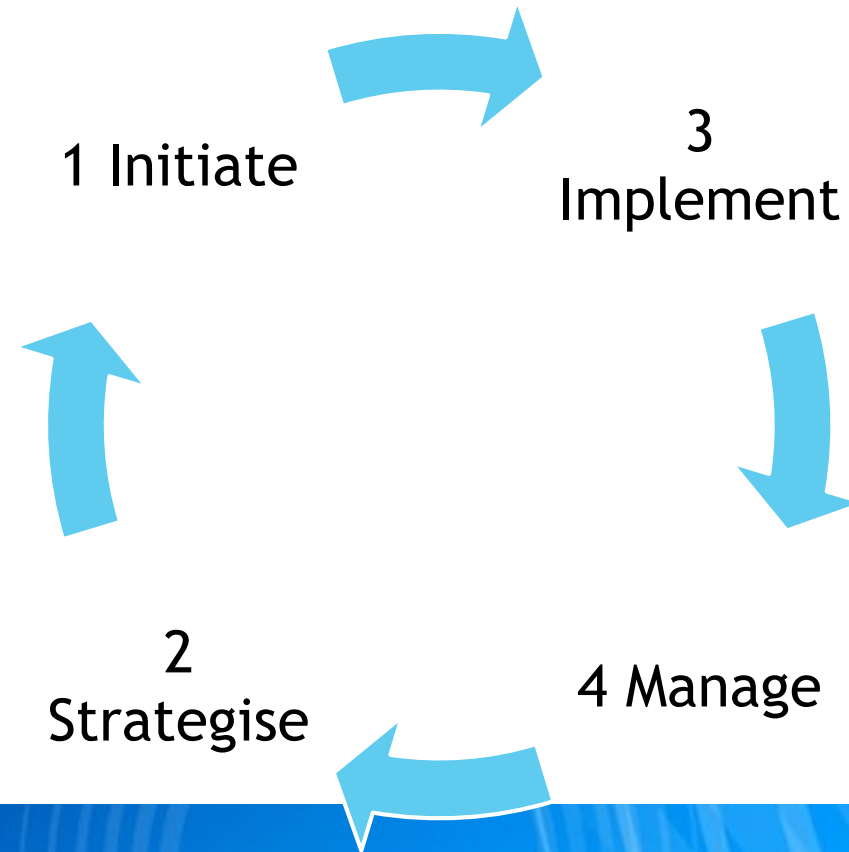
Definizione di Business Continuity

- ▶ Il ripristino dei sistemi ICT è necessario per garantire la continuità operativa dei processi e delle attività operative, ivi inclusa la disponibilità dei sistemi e dei servizi ICT che li supportano.
- ▶ Per BC (Business Continuity) intendiamo “un processo continuo che protegge il patrimonio aziendale sia in termini di infrastrutture tecniche a supporto del business, sia in termini degli asset tangibili e non, al fine di garantire la continuità delle attività operative critiche e per assicurare i flussi degli introiti di business”.

I principali elementi della Business Continuity



Le tipiche fasi di un processo di Business Continuity



Initiate e Strategise

- ▶ Nella fase 1 rientrano gli obiettivi di progetto, l'acquisizione della documentazione, pianificare il progetto, organizzazione e project management.
- ▶ Nella fase 2 rientrano il Risk Assessment, il Business Impact Analysis (BIA), la definizione della strategia

Implement e Manage

- ▶ Nella fase 3 rientrano l'organizzazione e pianificazione dell'implementazione, la predisposizione delle misure d'appoggio, definire i piani di recupero, ripristino ed emergenza, implementare misure di riduzione dei rischi, definire le procedure, collaudo iniziale
- ▶ Nella fase 4 rientrano la diffusione della cultura ed istruzione, la revisione ed audit, il testing, il change management, la formazione, la comunicazione interna ed esterna

Il Disaster Recovery

- ▶ Il Disaster Recovery è la capacità di un sistema di riprendere le sue funzionalità garantendo la corretta operatività dopo un disastro.
- ▶ Il Disaster Recovery nel mondo ICT è uno degli strumenti fondamentali per garantire la business continuity: **non si deve però fare l'errore di considerare questi due termini come sinonimi.**

Il Disastro

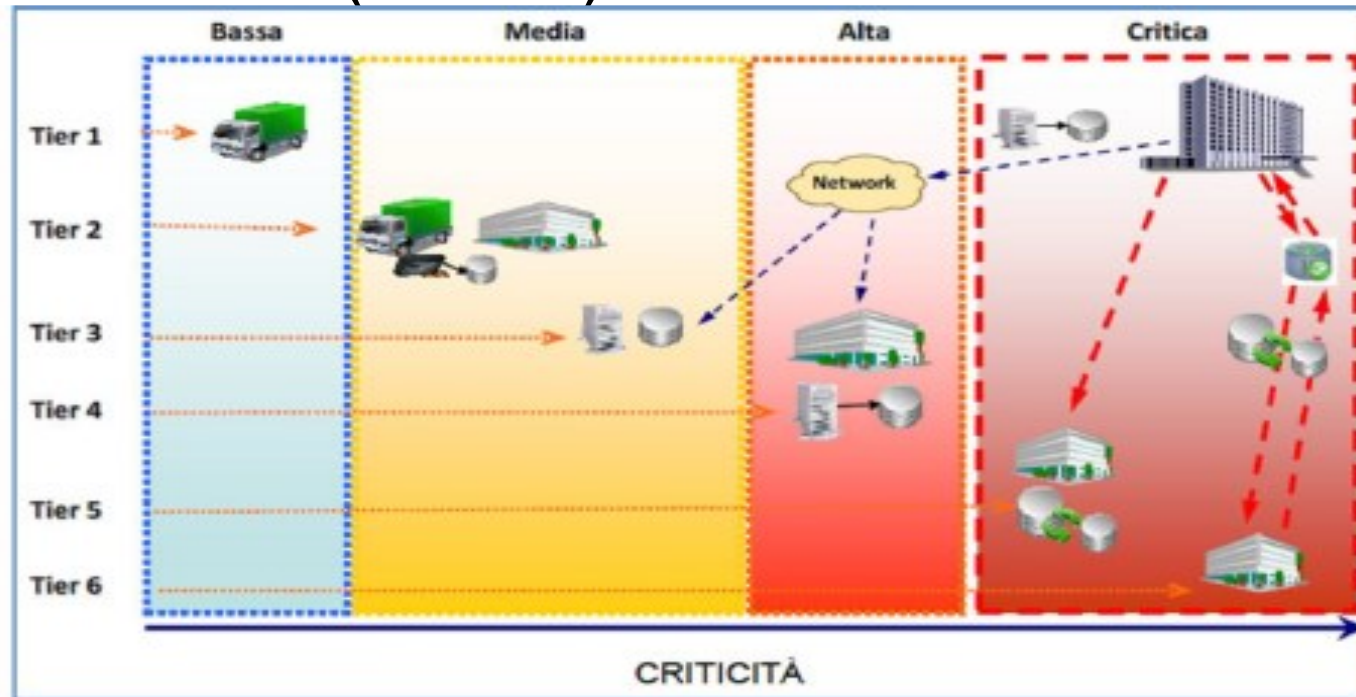
- ▶ Il disastro è un evento che rende inagibile l'utilizzo di infrastrutture, sistemi e risorse (**in genere non solo ICT**) per un tempo tale da compromettere in modo irreversibile attività, affari, produttività ed immagine di chi lo ha subito

I tre diversi tipi di disastro

- ▶ **Disastro di livello 1:** può causare la parziale ma non completa distruzione delle operazioni svolte giornalmente;
- ▶ **Disastro di livello 2:** coinvolge diverse locazioni o piani. Le operazioni di routine possono essere compromessi ed i processi critici possono dover essere eseguiti off-site;
- ▶ **Disastro di livello 3:** può coprire una vastissima zona, ad esempio una regione; tipici esempi di questi disastri sono inondazioni, terremoti o uragani.

Tipologie (TIERS)

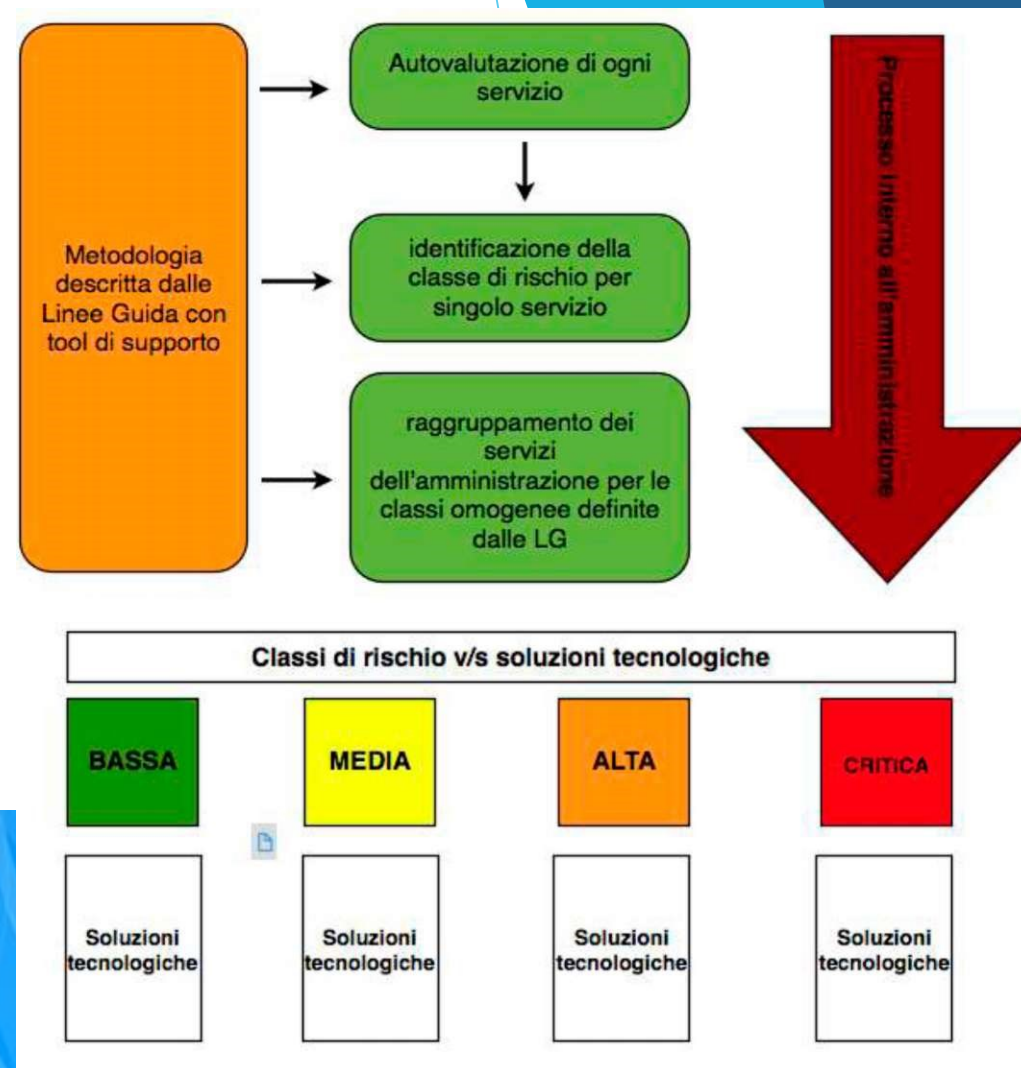
tecniche



La realizzazione della CO e delle soluzioni di DR

Dagli indicatori per ogni direttrice si giunge ad un indicatore complessivo di criticità. I livelli di criticità vengono raggruppati in 4 classi di rischio.

Alle CLASSI DI RISCHIO si associano delle soluzioni tecnologiche (o Tiers) minime



Le diverse componenti

- ▶ La Continuità Operativa investe diverse componenti e risorse strategiche di ciascuna azienda/Amministrazione: il management ad alto livello, le diverse strutture organizzative coinvolte nei processi di servizio (Direzioni/Uffici), le piattaforme tecnologiche impiegate.
- ▶ Ciò comporta che l'ente è chiamato a definire e coordinare un programma articolato in diverse fasi, che richiede il mandato dei vertici dell'Ente.

minacce informatiche

- ▶ **Virus** che è caratterizzato dal metodo di riproduzione parassitico (si allega ad altri file), infezione al boot sector ed infezione multipartito cioè sia il boot sector che il master boot record;
- ▶ **Botnet** (minacce che colpisce le reti di computer che presentino vulnerabilità);
- ▶ **Minacce dall'interno** (attacchi dall'interno da parte dei dipendenti, società di vigilanza, di pulizia, ecc);
- ▶ **Conflicker** (malware o codice maligno) che da novembre 2008 ha colpito 9 milioni di pc.

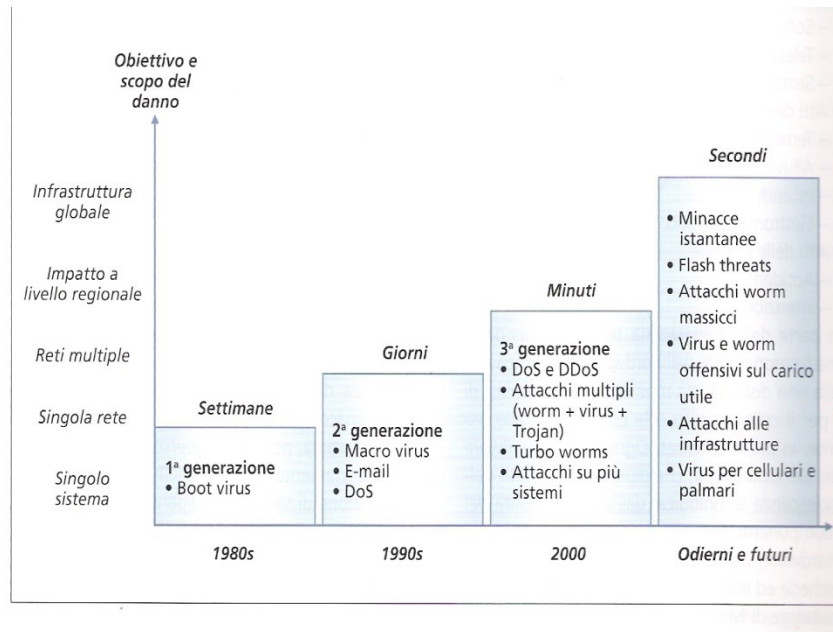
minacce informatiche

- ▶ **Skimming** (clonazione della carta di credito durante l'uso gi un'apparecchiatura di un negozio – es. pos);
- ▶ **Bin raiding** (trovare informazioni attraverso estratti conto, bollette, lettere, informazioni fiscali che sono stati gettati nella spazzatura);
- ▶ **Sniffing** (ad es. con un sms o e-mail ci viene comunicata una vincita e su un telefonino è possibile seguire un link che porta ad un'azione di phishing);
- ▶ **Phishing** il cui termine deriva da password harvesting e da fishing (furto per via elettronica tramite e-mail in cui il ladro si spaccia per banca o addetto alle carte di credito e induce a fornire dati personali, vi è normalmente un link che porta al sito solo in apparenza ufficiale)
 - ossia cercare password ed altre informazioni riservate “pescandole” con tecniche di social engineering ad utenti ingenui.

minacce informatiche

- ▶ **Social engineering:** tutte le modalità di carpire con l'inganno informatico, quali le credenziali di autenticazione per accedere illegalmente ad una risorsa informatica;
- ▶ **Mascheramento utente (IP MASQUERADING)** : può avvenire o mascherandosi da uno specifico utente, se si sono carpite le sue credenziali oppure via rete, con l'attaccante che invia pacchetti modificando l'indirizzo IP sorgente facendo credere, quindi, all'host di destinazione e alla diverse unità di rete che il pacchetto attraversa di provenire da un'altra sorgente;
- ▶ **Intercettazione**
- ▶ **Saturazione delle risorse (DOS Denial of service):** è un attacco in internet che ha l'obiettivo di saturare la risorsa obiettivo, che non è quindi più in grado di erogare un servizio.

minacce informatiche



Attacchi	Vulnerabilità
Tramite back door utilizzando una Wireless Local Area Network (Wlan)	- Il Network Service Set Identifier (SSID) non è stato adeguatamente mascherato - Un punto d'accesso non autorizzato è installato da un dipendente interno - Wired Equivalency Protocol (Wep) è debole e la relativa sessione di crittografia è interrotta
Attacco bruto (deep-crack) per scoprire identificativo d'utente e sua password	- user-id facilmente derivabile dal cognome di un dipendente - Lunghezza minima della password insufficiente - Password deboli soggette ad attacchi da dizionario
Social engineering	L'attaccante con l'inganno ha carpito user-id e pwd ad un dipendente in troppa buona fede (mancanza di sensibilizzazione dei dipendenti sulla sicurezza)
Complicità con un utente interno	Che ha deliberatamente fornito user-id e pwd
Sniffing traffico LAN	- La sequenza di autenticazione non crittografata permette intrusioni - Basso livello di monitoraggio - Trojan Horse installato in rete - possibilità di collegarsi alla LAN senza essere visti (es. come uomo delle pulizie)
Attacco di ex dipendente	- User-id e password utente non cancellate tempestivamente dopo le dimissioni - Le password di accesso sui terminali dei server-dial-in o sui punti di accesso Wlan non sono revocati dopo le dimissioni

minacce informatiche

- ▶ **Buffer e stack overflow** che consiste nel sovrascrivere in un buffer o in uno stack del programma dati istruzioni grazie alle quali il programma stesso può comportarsi in maniera diversa dal previsto, fornendo dati errati, bloccando il sistema operativo;
- ▶ **Format string exploit**, cioè attacchi basati sul formato della stringa di stampa, chiamati format string attack, derivano da una cattiva programmazione del codice;
- ▶ **Race condition e deadlock**, con il quale si indicano le situazioni derivanti da una condivisione di una risorsa comune, ad es. un file o un dato, e nelle quali il risultato viene a dipendere dall'ordine in cui si effettuano le operazioni;
- ▶ **Spamming** (posta elettronica indesiderata agli utenti);
- ▶ **Flash threats**: sono dei virus in grado di diffondersi molto velocemente sulla rete.

minacce informatiche

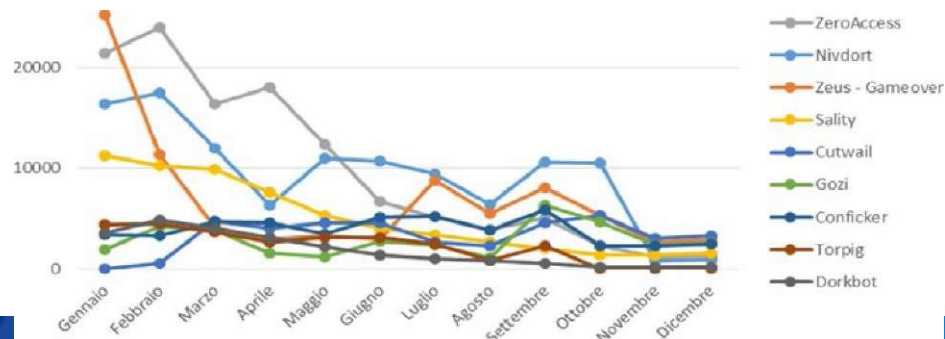
- ▶ **Adware** (advertising display software) indica un software applicativo che mostra all'utente contenuti pubblicitari (tipicamente dei box o dei banner all'interno di una pagina web) in maniera o in un contesto inaspettato e non voluto dall'utente - Tipo di **malware** che visualizza pubblicità solitamente senza il consenso dell'utente ;
- ▶ **Spyware** cioè un programma spia del comportamento di un utente collegato in rete, tramite un tracciamento delle sue operazioni senza che l'utente ne sia al corrente, senza che abbia dato il suo consenso e senza avere un controllo del tracciamento stesso;
- ▶ **Pharming** è simile al phishing, ovvero carpire informazioni personali e riservate, ma differisce per le modalità e le tecniche di attacco in quanto in questo caso sono usate tecniche sofisticate di manipolazione dei server DNS o direttamente del pc dell'utente attaccato.

minacce informatiche

- ▶ **Scam** che indica un tentativo di truffa tradizionale effettuata via posta elettronica: si segnala la vincita di somma considerevoli da ignote lotterie straniere, o la possibilità di enormi guadagni in cambio di attività sempre correlate ad un iniziale anticipo di denaro a vario titolo;
- ▶ **Blended threats**, cioè minacce mescolate, indica una famiglia di attacchi basati sull'uso contemporaneo e concatenato di più strumenti, quali virus, worm, trojan horse, exploit e denial of service, sfruttando al meglio le vulnerabilità dei server attaccati, probabilmente scoperte con uno scan in una fase pre-attacco;
- ▶ **Dialer** cioè un generico programma sul pc che compone numeri telefonici via modem. Di per sé non è un programma maligno ma può essere usato come tale, all'insaputa dell'utente, per effettuare in automatico delle chiamate a numeri a pagamento;
- ▶ **Keylogger** cioè un sistema in grado di intercettare quello che un utente digita su una tastiera di un terminale o pc.

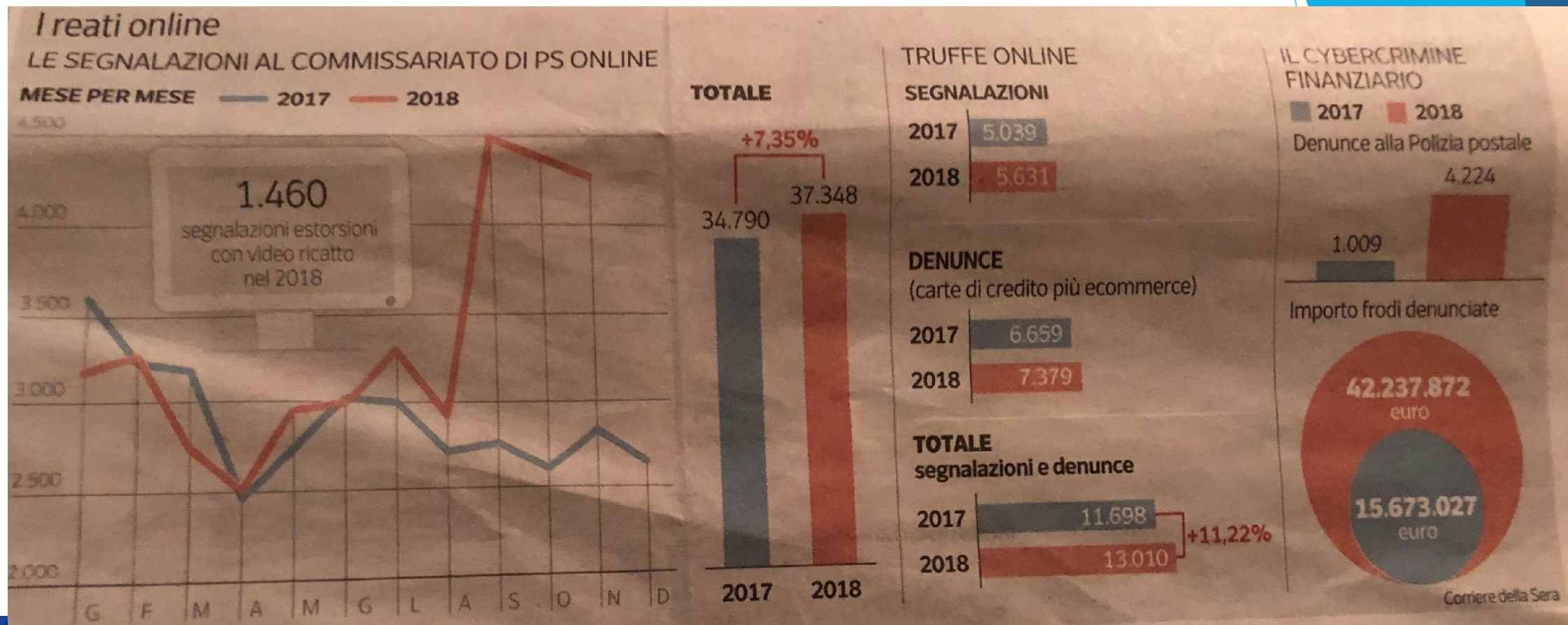
I malware

- Per malware che corrisponde alla contrazione in inglese di malicious software (programma malvagio) intendiamo dei programmi che hanno come scopo precipuo quello di danneggiare un pc ovvero di interromperne, alterarne o rallentarne il funzionamento, ovvero di cancellarne una parte della memoria o ancora di cagionare la perdita di dati, informazioni e programmi conservati all'interno di un qualsivoglia sistema informatico.



Rilevazione mensile dei malware (DATI Fastweb relativi all'anno 2016)

Alcuni dati anno 2017-2018 Fonte polizia di stato



I costi per paese 2019



**Fonte Indagine
ServiceNow.
Ponemon Institute
23-12-2019**

Nel 2019 i crimini
informatici sono
aumentati del 17%
in più rispetto al
2018

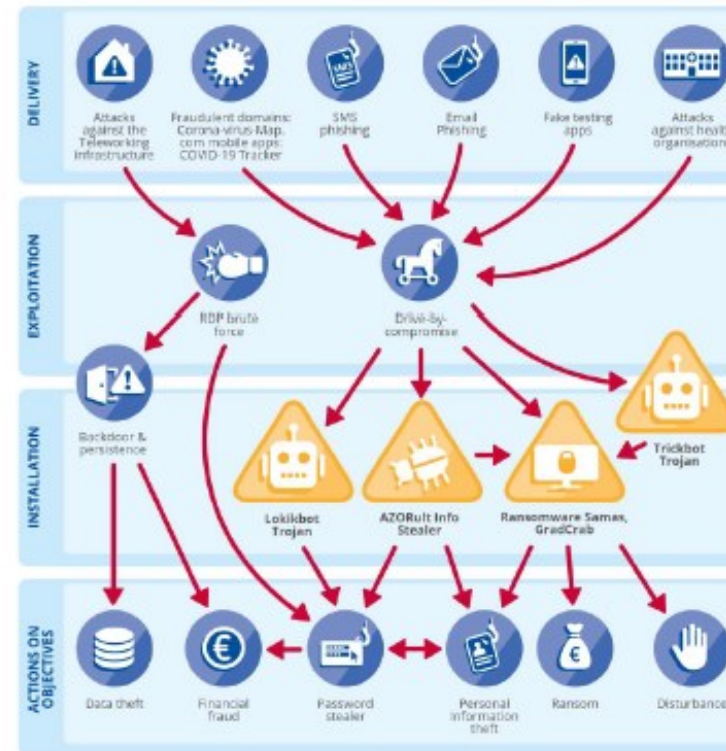
I TOP 15 CYBER ATTACCHI 2020



Fonte ENISA

COVID-19 ATTACKS

- Cybercriminals and APT groups during COVID-19 pandemic



DIRETTIVA NIS 2016/1148

- preparazione degli Stati membri richiedendo loro di essere adeguatamente attrezzati, ad es. tramite un **Computer Security Incident Response Team (CSIRT)** e un'autorità **NIS nazionale competente**
- cooperazione tra tutti gli Stati membri, mediante la creazione di un gruppo di cooperazione per sostenere e facilitare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri. Dovranno inoltre creare una rete **CSIRT**, al fine di promuovere una cooperazione operativa rapida ed efficace su specifici incidenti di cibersecurity e condividere informazioni sui rischi,
- una **cultura della sicurezza** in tutti i settori che sono vitali per la nostra economia e società e che inoltre dipendono fortemente dalle TIC, come energia, trasporti, acqua, banche, infrastrutture del mercato finanziario, sanità e infrastrutture digitali. Le imprese di questi settori che sono identificate dagli Stati membri come operatori di servizi essenziali dovranno adottare misure di sicurezza adeguate e notificare incidenti gravi all'autorità nazionale competente. Anche i principali fornitori di servizi digitali (motori di ricerca, servizi di cloud computing e mercati online) devono soddisfare i requisiti di sicurezza e notifica previsti dalla nuova direttiva. (**DIRETTIVA (UE) 2016-1148**)

LEGENDA:

 FACOLTATIVO

 CONSIGLIATO

 RICHIESTO

 OBBLIGATORIO

Precauzioni graduate

Misure di sicurezza contro gli attacchi informatici indicate dalle linee guida Iba e modulate in base alla grandezza dello studio

TIPOLOGIA	PROFESSIONISTA SINGOLO	PICCOLO STUDIO (FINO A 20 PERSONE)	MEDIO STUDIO (DA 21 A 40 PERSONE)
DOTAZIONE TECNOLOGICA			
Utilizzo connessioni internet sicure			
Implemento conservazione e sistemi di recupero dati			
Criptare dati e strumenti			
Segmentare la rete			
Utilizzo dispositivi mobili sicuri			
PROCESSI ORGANIZZATIVI			
Implemento di username e password sicure abbinate ad autenticazione multipla			
Identificazione di dati sensibili e implementazione di protocolli di protezione			
Creazione di una policy per la cybersecurity in linea con i rischi individuati			
Sviluppo di piani per la continuità aziendale in caso di attacco			
Miglioramento del controllo rischi su fornitori e parti terze			
Polizza di responsabilità per la cybersecurity			
CONTROLLI DI SICUREZZA			
Elenco dei dispositivi ammessi e vietati			
Verifiche periodiche sulla vulnerabilità e sulla protezione			
Antivirus			
Controlli degli accessi da remoto			
Software di sicurezza per le app			
LINEE DI CONDOTTA			
Indicazioni sui pericoli nell'uso dei social media			
Segnalazione di qualsiasi attività sospetta sul computer (improvvisa apertura di finestre, mouse che si muove in maniere indipendente, mail non richieste)			
No all'apertura di allegati o link in mail non richieste			
Periodici incontri formativi sul phishing			
Policy aziendali con protocolli sull'uso di sistemi mail o cloud (quali Dropbox, OneDrive, Gmail, Yahoo etc.)			

Fonte: elaborazione Il Sole 24 Ore sulle linee guida per la cybersecurity dell'International Bar Association (Iba)

Le linee guida Iba
(international bar association)
l'associazione che riunisce i
legali di tutto il mondo

Sole 24Ore 7-1-2019

Contromisure sui social network

- Corretta definizione delle «impostazioni» del proprio profilo;
- Visibilità del profilo (totale o con filtri) con restrizioni sui commenti e sui post ed anche su «like»;
- Limiti ai tag (etichetta apposta ad una foto o ad un post) e agli amici;
- Non rivelare cosa facciamo



Contromisure 1

- ▶ La miglior difesa dagli attacchi informatici è la prevenzione:
- ▶ Conoscenza dei possibili attacchi:
 - Aggiornamento continuo;
 - Valutazione impatto rispetto al proprio sistema.
- ▶ Gestione dei rischi:
 - Utilizzo di soluzioni tecnologiche;
 - Definizione di regole di utilizzo delle risorse.
- ▶ Diffusione della conoscenza:
 - Formazione e sensibilizzazione del personale interno;
 - Comunicazione ai soggetti con cui interagisce il sistema.

Contromisure 2

- ▶ ***Tutelare il bene più prezioso che circola in rete: i nostri dati personali*** (numeri di carte di credito, indirizzi, conti bancari);
- ▶ **La migliore contromisura per rispondere alle varianti del malware (malicious software) è quello di utilizzare un approccio integrato che comprenda barriere hardware e software ma anche corrette abitudini e regole ferree;**
- ▶ La somma delle contromisure è in gergo definita data loss prevention (perdita di informazioni);

contromisure 3

- ▶ Introduzione della figura del security manager che ha il compito di interagire, conciliandolo sia a livello informatico che organizzativo;
- ▶ Strumenti software di duplice protezione del software di base che hanno il compito di recuperare tutte le diverse tipologie di informazioni utili per organizzare la sicurezza e dei dati che vengono elaborati e analizzati, tramite un processo di intelligence, in modo da essere strutturati secondo valori tematici;
- ▶ Definizione dei fattori di rischio e delle componenti da monitorare a livello di sicurezza, agendo nel tempo con dei piani di correzione.

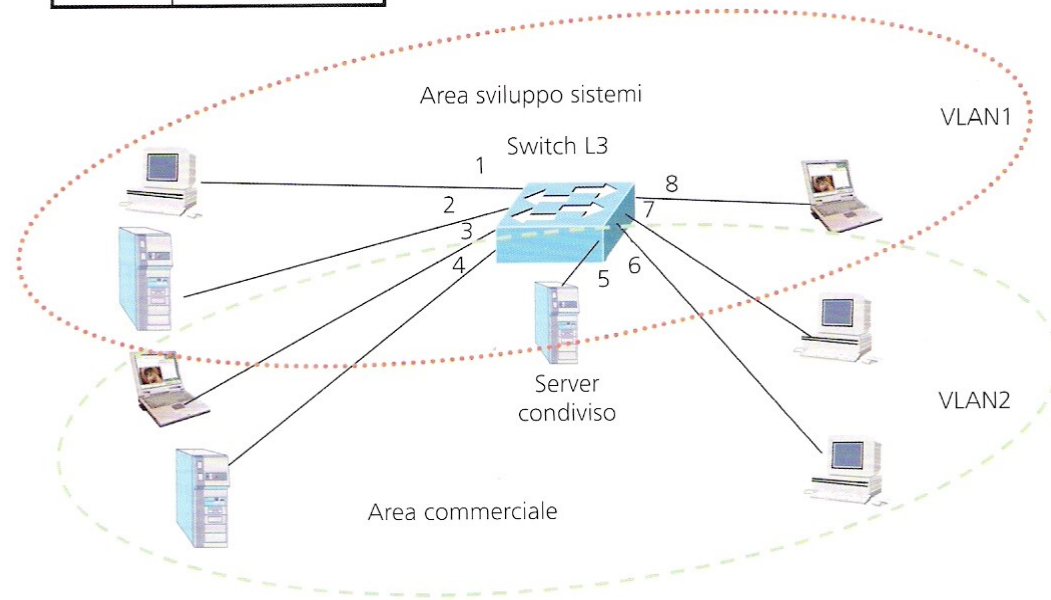
contromisure 4

- ▶ L'utilizzo di architetture di rete virtuali (vlan) che consentono di disaccoppiare le informazioni dai programmi e soprattutto dall'hardware utilizzato per trattarli, minimizzando i rischi di intrusione, sottrazione e danneggiamento;

Tecnicamente la virtualizzazione (ad es. con Symantec) viene fatta su 3 piani paralleli e cioè quello dello storage, quello dei server e quello degli endpoint (cioè i client);

vlan (Virtual Lan)

VLAN1	Porte 1, 2, 5, 8
VLAN2	Porte 3, 4, 5, 6, 7



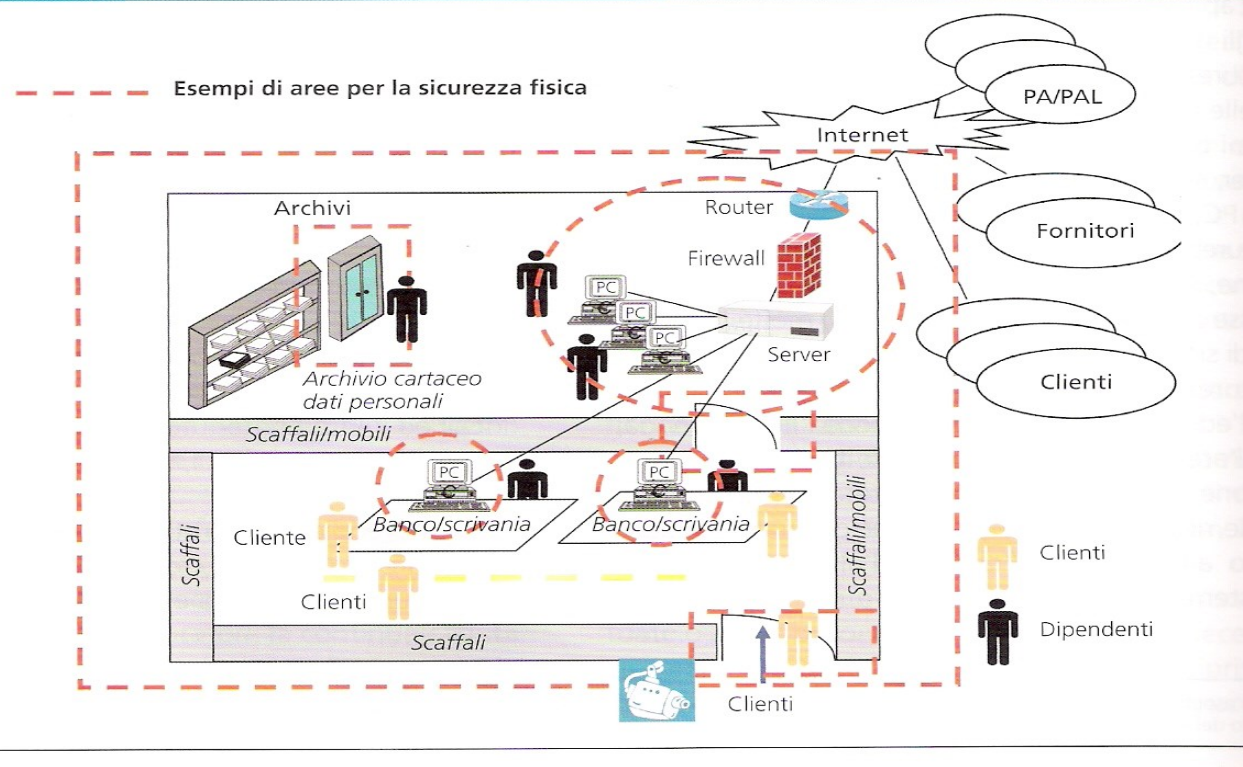
contromisure 5

- ▶ Strumenti di identificazione ed autenticazione;
- ▶ Strumenti per la gestione del controllo degli accessi e dei certificati digitali: crittografia, pki, controller di dominio;
- ▶ Strumenti per la protezione della rete e dei sistemi;
- ▶ Strumenti per la trasmissione sicura delle informazioni;
- ▶ Strumenti per la gestione delle vulnerabilità e degli attacchi (IDS, antivirus, gestione patch, aggiornamenti software, etc);
- ▶ Strumenti per la verificabilità (auditing – strumenti di gestione dei log e delle segnalazioni di malfunzionamento);
- ▶ Strumenti per il monitoraggio ed il controllo delle funzionalità e delle prestazioni dei sistemi.

contromisure: sicurezza fisica

- ▶ La sicurezza fisica ha il compito di proteggere le aree nelle quali si trovano i dispositivi informatici e di telecomunicazione, e le relative strutture ed impianti (**tale aspetto è definito sicurezza perimetrale**), i componenti hardware all'interno delle aree di cui sopra, le persone che operano nei siti ove si trovano le apparecchiature informatiche, dagli operatori agli utenti finali.

Un esempio



le misure di sicurezza fisica

- ▶ Il controllo perimetrale dell'edificio e di particolari zone all'interno o all'esterno dello stesso (parcheggi, cortili, ecc,);
- ▶ Controllo degli accessi fisici delle persone all'interno dell'edificio o di determinati locali da proteggere quali il ced;
- ▶ Il controllo e la prevenzione di mancanza di energia elettrica;
- ▶ Il controllo e la prevenzione di emissioni elettromagnetiche;
- ▶ Il controllo e la prevenzione antincendio, antifumo ed antigas;

sicurezza perimetrale

- ▶ La sicurezza perimetrale ha come misure di prevenzione i sistemi di sicurezza passiva quali sistemi di recinzione antiscavalcamiento, ed attiva, quali sistemi di allarme perimetrali a micro-onde, monitoraggio TV a circuito chiuso o con altre tecnologie.

sicurezza logica

- ▶ La sicurezza logica prevede le seguenti contromisure: identificazione dell'interlocutore, autenticazione dell'interlocutore, autorizzazione ad accedere ed operare sulla risorsa richiesta in funzione dei diritti (**in inglese chiamati access rights**) che sono stati rilasciati al richiedente e preventivamente inseriti nei sistemi da un gestore delle risorse e/o della sicurezza.

modalità di accesso alle banche dati anagrafiche: l'identificazione

- ▶ L'identificazione di un interlocutore:
- ▶ La forma più comune per identificarsi è l'inserimento di credenziali di autenticazione. Tale meccanismo di identificazione (user e pwd) è debole e dipende dalla frequenza di cambio della pwd, dalla sua casualità e dalla sua lunghezza;
- ▶ Altre forme di prevenzione sono la cd, pwd monouso (one-time pwd) che sono create ed usate per ogni singola interazione tra la persona e l'applicazione, e non possono più essere utilizzate altre volte;
- ▶ Altra forma è il **token** che si basa sull'identificazione a due o più fattori: tipicamente l'utente deve possedere un oggetto chiamato token, riconoscibile dal pc oltre al proprio user-id e pwd;
- ▶ Es. di token (carta con banda magnetica, smart card con processore con relativo lettore, chiavetta usb contenente i certificati digitali, generatore di pwd monouso, Tag RFID).

Esempi di token



Smart card



Chiavetta USB



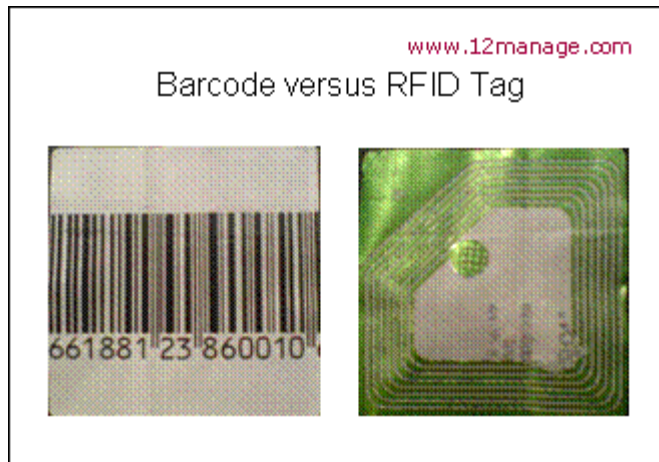
Generatore di codici casuali



Esempi di tag passivi RFID

RFID (Radio Frequency Identification)

- ▶ RFID (**Radio Frequency IDentification** o **Identificazione a radio frequenza**) è una tecnologia per la identificazione automatica di oggetti, animali o persone (AIDC Automatic Identifying and Data Capture) basata sulla capacità di memorizzare e accedere a distanza a tali dati usando dispositivi elettronici (chiamati TAG o transponder) che sono in grado di rispondere comunicando le informazioni in essi contenute quando "interrogati".
- ▶ Tale tecnologia si basa su un transponder, chiamato anche tag, un ricetrasmittitore che invia un segnale radio in risposta ad un comando ricevuto da una stazione remota)



autenticazione

- ▶ I moderni sistemi tendono ad utilizzare logiche di autenticazione a due o più fattori richiedono cioè di presentare due o più forme di identificazione per ottenere l'accesso, **tipicamente user-id e pwd associate ad un token.**

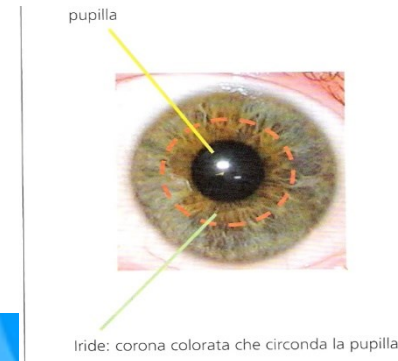
la biometria

- ▶ Per biometria, dal greco bios (vita) e metros (misura), si intende l'identificazione automatica o la verifica dell'identità di un soggetto sulla base di caratteristiche fisiche e/o comportamentali. Quando parliamo di chiavi biometriche ci riferiamo all'uso delle impronte digitali, l'impronta dell'iride, l'impronta del dna, l'impronta della pelle etc. **Da un lato si ha la necessità che mi devo identificare dall'altro che mi devo autenticare.**
- ▶ **Ad esempio l'utilizzo delle impronte digitali per entrare nell'area sicura di un qualunque CED ministeriale, in questo caso viene confrontata l'impronta con un set di impronte precedentemente dichiarate. Quindi in sostanza si passa ad effettuare un'associazione di un'identità a dei dati ed a verificare un'identità precedentemente dichiarata.**
- ▶ Un altro tema è quello dell'uso delle firme scritte come strumento di autenticazione.

tecniche biometriche



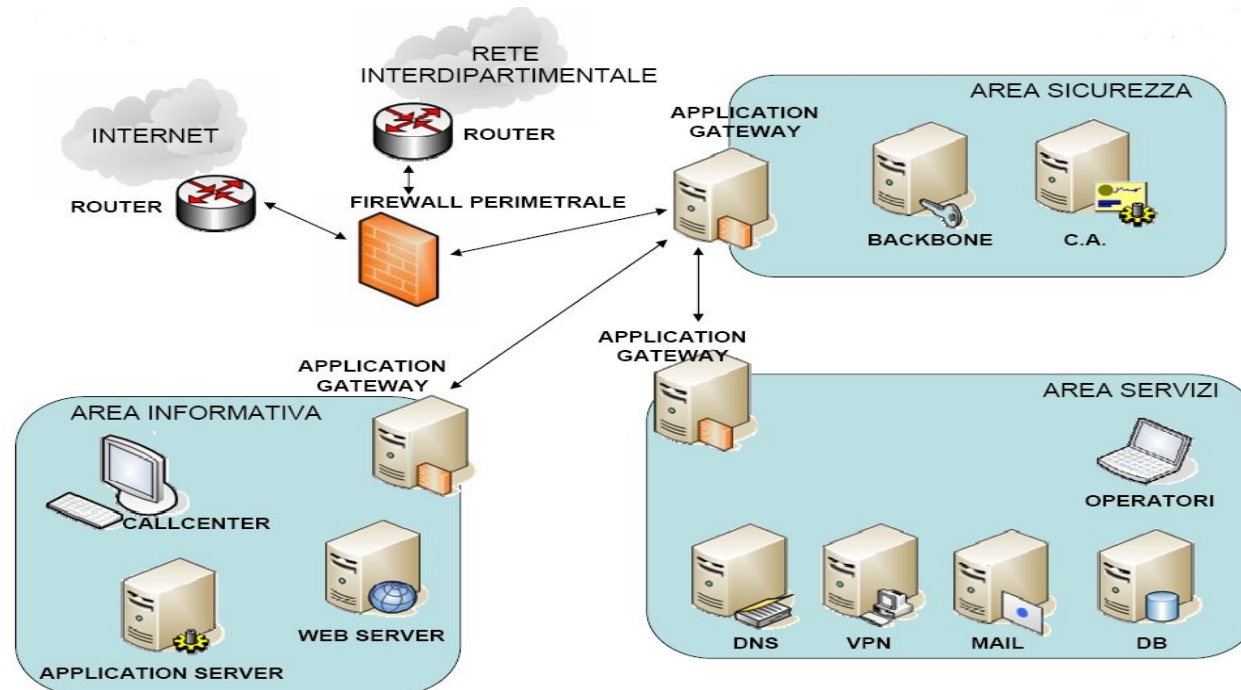
l'identificazione biometrica



modalità di accesso

- ▶ Accesso profilato mediante credenziali di autenticazione (username e password);
- ▶ Si può anche utilizzare la procedura di login disponibile sul sistema operativo della postazione di lavoro connessa in rete;
- ▶ Disattivazione dell'account in caso di prolungata assenza o fuoriuscita dall'organizzazione;
- ▶ Utilizzo di modalità sostitutive in caso di assenza del dipendente (ad es. invio automatico di messaggi di posta elettronica ad un altro recapito).

un esempio concreto



Phishing

- ▶ Phishing
- ▶ Una truffa informatica che permette agli ideatori di carpire, attraverso un'e-mail, i dati di accesso personali alla propria banca on line. Arriva nella casella di posta elettronica comunicando un imprecisato problema al sistema di "home banking".
- ▶ Invita ad aprire la home page della banca con cui avete il conto corrente gestito via web e a cliccare sul link indicato nella mail.
- ▶ Subito dopo aver aperto il sito della banca vi si apre una finestra (pop-up) su cui digitare la "user-id" e la "password" di accesso all'home banking. Dopo pochi secondi appare un altro pop-up che vi informa che per assenza di collegamento non è possibile la connessione. A questo punto qualcuno è entrato in possesso dei vostri dati e può fare operazioni dal vostro conto.

Esempi



Prevenzione

- ▶ Prevenzione
- ▶ Inserire tra i preferiti (con refresh su Proprietà) lo script:
- ▶ `javascript:alert("Direction real:"+location.protocol + "://" + location.hostname + "/")`
- ▶ Ogni volta che avrete un dubbio, utilizzatelo....

Pharming

- ▶ Pharming
- ▶ Il Pharming dirige gli utenti su server proxy, tipicamente attraverso DNS hijacking o poisoning.

Phishing

- ▶
- ▶ Phishing
- ▶ Investighiamo sul reale indirizzo della mail di phishing
- ▶

Phishing



► PHISHING

Hop	T1	T2	T3	Host	Graph	IP	Hostname	Dist	TTL	Org	Time
1	8	0	8	0.5 ms		66.36.248.2 a514381 EOPONE-DCA	c-vf02-d1 acc.dca2.hoponet.net		255	US	Unknown: 8186e1ee
2	11	0	16	0.7 ms [+0ms]		66.36.224.213 a58 [ANA-BJVD-0]	gm2.core2.dca2.hoponet.net	8 miles [+0]	254	US	Unic: 85-43:0
3	3	1	12	1.2 ms [+0ms]		66.36.224.34 a20 [ANA-BJVD-0]	gm2-0-241.core1.iad1.hoponet.net	8 miles [+0]	203	US	Unknown: 828976d15
4	29	62	2	2.3 ms [+1ms]		286.213.115.48 a20 [ANA-BJVD-0]	gm6-14.sch02.sad11.growdata.net	8 miles [+0]	252	US	Unic: 86-43:0
5	46	33	56	35 ms [+31ms]		63.218.113.18 a53481 3TH-A28	dlcgr6-2.bell.mia02.growdata.net	8 miles [+0]	243	US	Unic: 86-43:0
6	335	180	204	180 ms [+147ms]		63.218.113.2 a53481 3TH-A28	dlcgr6-2.bell.mia02.growdata.net	8 miles [+0]	244	US	Unic: 86-43:0
7	392	394	-	209 ms [+28ms]		63.171.222.6 a519429 LACBDC-19429	rwf11.cfb.net.co	8 miles [+0]	243	US	Unic: 86-43:0
8	389	-	-	209 ms [+0ms]		288.73.48.128 a519429 LACBDC-19429	[Reached Destination]climate_corpor_7549- 1206.rth.net.co	8 miles [+0]	115	CO	Microsoft: 164330436

I worms

- I worms sono dei programmi maligni che traggono giovamento dalla integrazione delle reti. Tipico è il caso dei c.d. worm (letteralmente verme), malware che modifica il sistema aggredito in modo da essere eseguito automaticamente. Esso si replica sfruttando per lo più su internet tant'è che viene in genere trasportato attraverso messaggi di posta elettronica, venendo allocato nei c.d. "attachment" o allegati. Tra i più famosi nonché pericolosi worms si annoverano Nimda che è entrato in azione una settimana dopo i tragici eventi dell'11 settembre 2001, infettò 8.300.000 pc e provocò danni stimati in circa 650 milioni di dollari.

Spyware

- ▶ Oltre a virus e worm, tra i programmi maligni è opportuno menzionare gli spyware, i trojan horse, le logic bomb e i web dialer.
- ▶ Lo spyware è un tipo di programma che raccoglie informazioni riguardanti l'attività on line di un utente (ad esempio siti visitati, acquisti eseguiti in rete, etc.). La maliziosità di tale software sta nel fatto che tali informazioni vengono carpite senza che l'utente stesso ne sia informato preventivamente e dunque senza il consenso di lui. Lo spyware poi, una volta acquisiti i dati e le notizie utili, provvederà a inoltrarli ad un database gestito quasi sempre da organizzazioni commerciali, che sfrutteranno quei dati e quelle notizie per trarne profitto. Dunque uno spyware viene realizzato non con il fine di danneggiare un sistema (anzi l'attività di reperimento di informazioni ne presuppone l'integrità) bensì per violare la privacy del cibernauta.

Il concetto

SCIENZA DELLA SICUREZZA
SAFETY
SECURITY
EMERGENCY

Sicurezza informatica

- ▶ Controllo della Sicurezza di un programma
- ▶ Semantic-Based Security model
- ▶ Security-Typed Language
- ▶ Errori di programma secondo IEEE
- ▶ ERROR
- ▶ FAILURE
- ▶ FAULT

Sicurezza informatica

- ▶ CODE OF GOOD PRACTICE Politiche di sicurezza (Security Police)
- ▶ Forniscono le direttive di gestione ed il supporto per le informazioni di sicurezza

Sicurezza informatica

- ▶ SICUREZZA ORGANIZZATIVA
- ▶ (Security Organization)
- ▶ Controllo della sicurezza delle informazioni in seno all'azienda;
- ▶ Mantenere la sicurezza e la facilità dei processi organizzativi delle informazioni anche quando accedono le parti terze;
- ▶ Monitorare la sicurezza delle informazioni quando la responsabilità dell'elaborazione dell'informazione è stata conferita in outsource

Sicurezza informatica

- ▶ CONTROLLO E CLASSIFICAZIONI DEI BENI
- ▶ (asset Classification and Control)
- ▶ Mantenere la protezione dell'assetto organizzativo e garantire che l'assetto delle informazioni riceva un appropriato
- ▶ livello di protezione

Sicurezza informatica

- ▶ SICUREZZA DEL PERSONALE
- ▶ (Personnel Security)
- ▶ Ridurre i rischi di errore, di frode o di abuso da parte degli operatori;
- ▶ Accertarsi che gli utenti siano informati delle possibili minacce e preoccupazioni sulla sicurezza delle informazioni e siano dotati a sostenere la politica della società sulla sicurezza nel corso del lavoro normale;
- ▶ Per minimizzare i danni dagli avvenimenti e dalle disfunzioni di sicurezza ed imparare da tali avvenimenti;

Sicurezza informatica

- ▶ SICUREZZA FISICA E AMBIENTALE (Physical and enviromental Security)
- ▶ Impedire l'accesso, il danneggiamento e l'interferenza dei non autorizzati all'interno del flusso delle informazioni del business;
- ▶ Impedire la perdita danni all'assetto del sistema e la interruzione delle attività economiche;
- ▶ Impedire la manomissione o il furto delle informazioni

Sicurezza informatica

- ▶ CONTROLLO DI ACCESSO (Access Control)
- ▶ Per controllare l'accesso alle informazioni;
- ▶ Per impedire l'accesso non autorizzato ai sistemi di informazione;
- ▶ Per accertare la protezione dei servizi in rete;
- ▶ Per impedire l'accesso non autorizzato nel calcolatore;
- ▶ per rilevare le attività non autorizzate;
- ▶ Per accertarsi della sicurezza delle informazioni quando sono utilizzate le prestazioni mobili rete e tele rete;

Sicurezza informatica

- ▶ GESTIONE DI COMUNICAZIONI E OPERAZIONI
- ▶ (Communications and Operations Management)
- ▶ Accertarsi del corretto funzionamento e della facilità di elaborazione dell'informazione;
- ▶ Minimizzare il rischio di guasti dei sistemi;
- ▶ Proteggere l'integrità dei software e delle informazioni;
- ▶ mantenere l'integrità e la validità dei processi di elaborazione dell'informazione e della comunicazione;
- ▶ garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto;
- ▶ Prevenire danni a beni e le interruzioni alle attività economiche;
- ▶ Impedire la perdita, la modifica o l'abuso delle informazioni scambiate fra le organizzazioni

Sicurezza informatica

- ▶ Controllo di accesso (Access control)
- ▶ Per controllare l'accesso alle informazioni;
- ▶ Per impedire l'accesso non autorizzato ai sistemi di informazione;
- ▶ Per accertarsi della sicurezza delle informazioni quando sono utilizzate le postazioni mobili rete e telerete.
- ▶ Per accertare la protezione dei servizi in rete; Per impedire l'accesso non autorizzato nel calcolatore; Per rilevare le attività non autorizzate

Sicurezza informatica

GESTIONE CONTINUITA'OPERATIVA (Business Continuity Management)

Neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari e dagli effetti dei guasti

Sicurezza informatica

- ▶ **ADEGUATEZZA (Compliance)**
- ▶ Evitare il mancato rispetto delle leggi civili, penali e di qualsiasi requisito di sicurezza;
- ▶ Per elevare l'efficacia e minimizzare l'interferenza per il processo di verifica del sistema

Sicurezza informatica

- ▶ PRINCIPALI TECNICHE DI ATTACCO (HACKING)
- ▶ EXPLOIT
- ▶ BUFFER OVERFLOW
- ▶ SHELLCODE
- ▶ CRACKING
- ▶ BACKDOOR
- ▶ PORT SCANNING
- ▶ KEY LOGGING
- ▶ SNIFFING
- ▶ SPOOFING
- ▶ TROJAN
- ▶ DOS
- ▶ INGEGNERIA SOCIALE

Sicurezza informatica

- ▶ PRINCIPALI TECNICHE DI DIFESA
- ▶ CRITTOGRAFIA
- ▶ SISTEMA DI AUTENTICAZIONE
- ▶ FIRMA DIGITALE
- ▶ FIREWALL
- ▶ IDS(intrusion detection system)
- ▶ NIDS(network detention system)
- ▶ HONEYPOT
- ▶ STEGANOGRAFIA
- ▶ ANTI-SPYWARE

Sicurezza informatica

In Italia ...

- 6° posto Computer Zombie;
- Poste Italiane: 7° posto al mondo per Phishing e Pharming.

Sicurezza informatica

- ▶ Connessioni..
- ▶ ■ Italia 43% una volta al mese;
- ▶ ■ Spagna 45% una volta al mese;

RAM

Risultati..

Il 60 % degli autori dei reati informatici
vengono individuati

Sicurezza informatica

- ▶ Strategie a difesa degli Utenti Privati
- ▶ Monitoraggio della rete
- ▶ Raccolta delle denunce
- ▶ Tutela collettiva delle vittime
- ▶ Campagna di sensibilizzazione
- ▶

Sicurezza informatica

Alcune Tipologie di attacco:

Fingerprinting

Tentativo di intrusione

Compromissione degli account

Sicurezza informatica

Alcune Tipologie di attacco:

I.P. Spoofing

D.O.S. & D.D.O.S

Sniffing

keylogging

Sicurezza informatica

- ▶ Monitoraggio della rete internet e dei suoi principali servizi

Sicurezza informatica

CHAT

BLOG

PEER-to-PEER

NEWSGROUP

FTP

Messenger

PAGINE
WEB

E-MAIL

..ecc

Sicurezza informatica

- ▶ MODALITÀ' DEGLI ACCERTAMENTI
- ▶ E-MAIL
- ▶ -Analisi dell'**header** del messaggio email
- ▶ -individuazione dell' **X-Originating-IP** del messaggio
- ▶ -analisi del **percorso** tra i server di posta dal mittente al destinatario
- ▶ -studio della "**data, ora, secondo**, e riferimento standard temporale"
- ▶ Alla ricerca di una illogicità temporale

Sicurezza informatica

- ▶ FAKEMAIL ed Mail Anonime
ESEMPIO Comandi da dare su linea di comando:
- ▶ telnet mail.serverdiposta.it 25
- ▶ Risposta server SMTP
- ▶ Hello dominiodafingere.net
- ▶ Risposta server SMTP
- ▶ Mail from: nome@dominiodafingere.net
- ▶ Risposta server SMTP
- ▶ Rcpt to:<destinatario@dominiodestinatario.net>
- ▶ Risposta server SMTP
- ▶ Data
- ▶ Risposta server SMTP
- ▶ *Testo messaggio .(punto) [INVIO]*
- ▶ Risposta server SMTP
- ▶ Magari usando un proxy per anonimizzarsi si evita di lasciare l'unica traccia (ip

Sicurezza informatica

Central Ops .net Advanced online Internet utilities

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NetLookup
- AutoWhois
- TopQuery
- AnalyzePath

Hosting metrics

- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

Domain Check See if a domain is available

www.

source code: view | download [Central Ops .net](#)

Checking domain availability...

Results

from DNS: **Taken.**

from Whois: **Taken.**

conclusion: **Taken.** The domain has been registered. However, the registrant may offer it for sale.

Web site: <http://www.interno.it/>

Whois output

```
*****
- Please note that the following result could be a subgroup of
- the data contained in the database.
-
- Additional information can be visualized at:
- http://www.nic.it/cgi-bin/Whois/whois.cgi
*****

Domain:      interno.it
Status:      ACTIVE
Created:      2001-10-05 00:00:00
Last Update: 2007-10-31 00:02:50
Expire Date: 2008-10-05

Registrant:
  Name:       Ministero dell' Interno
  ContactID:  MINIS19-IINIC
  Address:    P.zza Viminale 1
              Roma
              00184
              RM
```

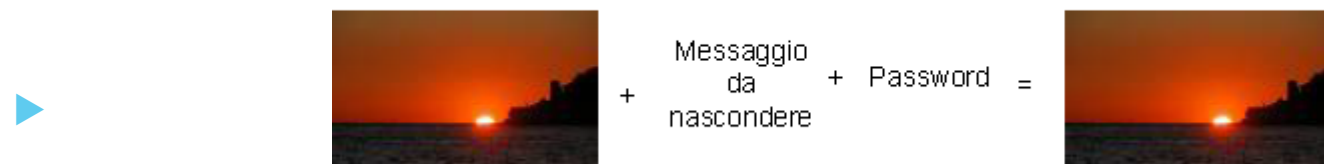

Sicurezza informatica

- ▶ Covert Channels
- ▶ Un covert Channel è un canale di comunicazione parassita che sfrutta la capacità trasmissiva di un canale di comunicazione legittimo.
- ▶ Mascheramento di scambio di informazione su traffico ordinario;
- ▶ Elusione di IDS e Firewalls;
- ▶ 2 tipologie:
- ▶ STORAGE CHANNELS: il canale informativo si instaura modificando contenitori di dati come immagini o flussi di rete; (steganografia)
- ▶ TIMING CHANNELS: il canale informativo si instaura alterando le tempistiche quali quelle tra una "request ed una "response" in un protocollo; (lenti e poca larghezza di banda)

Sicurezza informatica

- ▶ Cosa succede se si usa la STEGANOGRAFIA su WWW???
- ▶ Paradigma della steganografia

Messaggio + dato di copertura (+ chiave) = dato steganografico



- ▶ Si può nascondere l'informazione senza che il dato originale venga 'apparentemente' modificato, non facendo sorgere dubbi in chi lo dovesse analizzare
- ▶ Si riesce a distribuire l'informazione in ogni parte della terra

I reati informatici

Sommario

- ▶ *Il Concetto di reato informatico;*
- ▶ *Il bene giuridico protetto: definizione;*
- ▶ *I crimini informatici propri ed impropri;*
- ▶ *Le diverse tipologie di crimini informatici*
- ▶ *La normativa ex ante legge 48/2008*

Il concetto di reato informatico

IL CONCETTO DI REATO

Il reato è una condotta riferibile alla volontà umana in contrasto con l'ordinamento giuridico, il quale di fronte alla violazione di uno o più beni giuridici protetti, commina una sanzione di tipo penale"

Il concetto di reato informatico

- Nell'ultimo decennio c'è stata una vera e propria rivoluzione e cambiamento di tendenza nell'universo criminale. Sono apparsi sulla scena i cd. computers crime i reati informatici.
- Le peculiarità del crimine informatico sono:
 - a-territorialità del contesto di riferimento;
 - prossimità con la vittima senza la dinamica del face to face;
 - anonimità dell'autore del reato.

Caratteristiche

Tali caratteristiche determinano conseguenze sia a livello repressivo sia a livello investigativo.

L'indeterminatezza del locus commissi delicti, un reato informatico si celebra all'interno di uno spazio virtuale in cui gli utenti connessi ad internet non sono necessariamente residenti nel medesimo Stato, implica problematiche connesse alla perseguibilità del reato.

Un computer crime è un comportamento, implicante l'uso di un sistema informatico, previsto e punito come reato dalla legge. Quindi un computer crime è un reato che in qualche modo ha nella sua fattispecie un sistema informatico e che prevede l'uso di un pc.

La dottrina

- ▶ La dottrina ha di volta in volta fornito varie definizioni di computer's crime ma quella che sembra essere la più precisa definisce crimine informatico qualsiasi atto o fatto contrario alle norme penali, nel quale il computer è stato coinvolto come soggetto, oggetto o strumento. La presenza di un elaboratore deve essere ritenuta condizione necessaria ma non sufficiente, in quanto è necessario altresì valutare con attenzione anche le modalità con cui il reato viene posto in essere al fine di scartare tutte quelle ipotesi in cui l'elemento informatico, se pur presente, è assolutamente marginale ed irrilevante

La dottrina

- ▶ Dunque non ogni reato commesso con un computer può essere ritenuto informatico, ma soltanto quei reati in cui il computer rappresenta l'elemento imprescindibile della fattispecie criminosa.
- ▶ La prassi investigativa ha comunque condotto alla distinzione seguente:
- ▶ - crimini commessi ai danni della rete e dei sistemi di comunicazione (attacco ad una banca dati per carpirne le informazioni);
- ▶ crimini (per così ordinari) commessi attraverso la rete di comunicazione (invio di messaggi minacciosi o diffamatori con la posta elettronica).

I crimini informatici

I crimini informatici si dividono in “crimini informatici propri” e “crimini informatici impropri” sulla base del bene giuridico protetto.

La distinzione è connotata dal computer, a seconda che rappresenti un elemento essenziale del reato, ovvero soltanto un semplice strumento attraverso il quale viene perpetrato l'illecito.

Uno dei problemi dei computer crime è connesso alla facilità di comunicazione in quanto sulla rete si trova di tutto.

Bene giuridico informatico

► Il bene giuridico informatico

- L'introduzione dei sistemi di produzione e trasmissione a distanza di informazioni, che consentono di memorizzare, elaborare e diffondere i dati con l'impiego di un linguaggio elettronico, ha creato un nuovo bene economico, che può essere definito "*bene giuridico informatico*".
- Il bene giuridico informatico può essere venduto o ceduto in uso (ad es. il software) ma può anche essere indebitamente sottratto, danneggiato o manomesso per cui deve essere protetto non solo con accorgimenti di carattere tecnico, ma anche con adeguati strumenti legislativi ossia questa parte dell'economia ha bisogno di essere protetta dall'ordinamento. Il primo grosso problema che si è verificato è la pirateria informatica.

La pirateria informatica

- ▶ La pirateria informatica è in grado di ledere beni giuridici diversi (patrimonio, fede pubblica, ordine pubblico, inviolabilità dei segreti e del domicilio) e spazia nei settori più disparati, estendendosi dall'intrusione nel sistema di elaborazione altrui con conseguente furto di dati allo “*sniffing*” (“ascolto” e “cattura” dei dati in rete), all'illecita duplicazione del software, fino al sabotaggio delle banche dati.
- ▶ L'informatizzazione intesa come produzione e la gestione di informazioni ha agito su vari livelli sociali ed organizzativi determinando:
 - ▶ a) la formazione di un corpo normativo specifico;
 - ▶ b) la considerazione della rete come lo spazio di interconnessione tra le aziende ed i vari comparti della pubblica amministrazione, nonché il luogo dove si concentrano rilevanti interessi economici ed elevati investimenti (un luogo giuridicamente rilevante);
 - ▶ c) la modifica dei comportamenti individuali e delle categorie tradizionali delle azioni criminali.

La pirateria informatica

- ▶ Le modalità comunicative, strettamente correlate all'impiego delle tecnologie digitali, hanno migliorato l'efficienza operativa delle strutture criminali (sovente le strutture criminali sono state più veloci nell'informatizzazione di quanto non lo siano stati i soggetti, per motivi di bilancio, i soggetti demandati alla repressione di questi comportamenti) che si adattano a tutte le innovazioni e sfruttano ogni potenzialità dei nuovi mezzi di comunicazione. E' noto che esistono delle organizzazioni criminali etniche che sono specializzate su determinati reati informatici ad esempio sulle clonazioni di carte di credito, etc. La diffusione delle reti telematiche ha moltiplicato le possibilità di esposizione dei sistemi informatici ad attacchi esterni ed ha ampliato la gamma delle condotte illecite possibili.
- ▶ Negli anni settanta un comportamento illecito fu considerato quello che si verificò nell'università di Roma La Sapienza, quando alcune persone per motivi ideologici considerando i computer come strumento di controllo sociale, entrarono nel ced (Centro Elaborazione Dati) e distrussero alcune macchine. Oggi la rete consente la realizzazione di attacchi molto più semplici e potenti.

Es. Crimini propri

- ▶ Esempi di crimini propri
- ▶ Appartengono alla categoria dei reati informatici propri tutte quelle fattispecie che, sulla base della definizione di computer's crime, vedono nel computer l'oggetto o il soggetto del reato che, di fatto, non potrebbe essere perpetrato in sua assenza

Esempi

- ▶ A titolo di esempio si pensi alla diffusione di programmi diretti a danneggiare un elaboratore (reato disciplinato dall'art. 615 - quinquies codice penale), all'accesso abusivo ad un sistema informatico o telematico (disciplinato dall'art. 615 - ter c.p.)



► I CRIMINI INFORMATICI PROPRI E IMPROPRI

I crimini propri

- ▶ **Crimini Informatici Propri**
- ▶ Il Legislatore ha introdotto nuove norme per i reati compiuti contro i computer. In genere per i crimini informatici propri si è generata una normativa ex-novo.

Crimini impropri

- ▶ **Crimini Informatici impropri**
- ▶ Il Legislatore ha inserito i reati compiuti per mezzo dei computer (crimini informatici impropri) all'interno delle vecchie disposizioni, ritenendo il computer un mezzo simile ad altri. Per quanto concerne i crimini informatici impropri si è adeguata la normativa precedente a questo nuovo mezzo.
- ▶ Un altro problema importante connesso all'impatto dell'informatica sul diritto penale affianco a quei reati che minacciano la sfera privata, il patrimonio, etc è quello relativo alla rapida circolazione delle informazioni. I reati informatici minacciano non solo la sfera privata ed il patrimonio, ma possono agevolare la rapida circolazione delle informazioni, venendo a costituire un efficace mezzo di comunicazione utilizzato anche per scopi illegali.

Altre tipologie

Crimini con finalità di profitto per l'autore e di danno per la vittima (*appropriazione o manipolazione di programmi ed informazioni, frodi elettroniche, ecc.*);

Crimini diretti contro il computer (contro il sistema informatico) in cui il sistema informatico è l'oggetto materiale del reato per provocarne la distruzione o l'inservibilità (*sabotaggio, vandalismo, danneggiamento informatico*);

Crimini correlati all'uso del computer che così diviene cosa pertinente al reato o strumento necessario per agevolare o per consumare la condotta illecita ossia vi sono una serie di reati la cui realizzazione viene facilitata dall'utilizzo di un pc (pensiamo ad esempio al traffico di materiale pedo-pornografico su internet).

Alcuni esempi

- ▶ I reati informatici sono in genere reati commissivi, di condotta o di evento (vuol dire che non sono in genere reati omissivi, ossia perchè possa essere configurata questa fattispecie reato ci deve essere sempre un "*facere*" o un "*agere*"), e possono essere di condotta o di evento, cioè può essere sufficiente che l'agente ponga in essere su un determinato comportamento, una determinata condotta a prescindere dall'evento che si verifichi oppure possono essere reati di evento ossia che sia necessario perché si configura la fattispecie penale che si verifichi un determinato scopo e che si raggiunga lo scopo che l'agente si è prefissato (ossia che a sua volta causa un evento pericoloso o dannoso per la persona offesa o per il titolare del sistema oggetto di intrusione, sabotaggio o danneggiamento).

La querela di parte

Il concetto della querela di parte è un grosso handicap nel ristabilimento della legalità in questo ambiente. Nelle fattispecie non aggravate da particolari circostanze (articoli del codice penale che richiamano le cosiddette circostanze aggravanti), la perseguibilità del reato è generalmente a querela di parte cioè affinché possa intervenire l'autorità giudiziaria ci deve essere la parte danneggiata che deve denunciare questo fatto cioè deve chiedere essa la tutela dell'autorità giudiziaria. Questa opzione legislativa ha però evidenziato alcuni grossi limiti per quanto concerne la sicurezza generale del sistema perché accade spesso che i soggetti attaccati non ritengano conveniente richiedere l'intervento dell'autorità giudiziaria perché la notorietà che consegue all'intervento dell'autorità giudiziaria è per loro un danno maggiore di quello subito dall'attacco criminale.

La querela di parte

Ovviamente questa omertà da parte delle vittime facilita il ripetersi degli attacchi criminosi. Uno dei limiti del nostro sistema è quello di prevedere quasi sempre la querela di parte sottovalutando gli interessi generali alla sicurezza informatica che probabilmente travalica e va oltre quello che può essere l'interesse della singola persona o della singola azienda a vedere tutelato il proprio sistema informatico.

Questa opzione legislativa ha però evidenziato alcuni limiti e spesso la querela non c'è. Accade infatti spesso, ad esempio, che imprese vittime di attacchi al proprio sistema informatico preferiscono non denunciare il fatto all'autorità giudiziaria per timore di diminuire la propria immagine o la parvenza di efficienza ed affidabilità sul mercato. Ciò facilita il ripetersi di fatti criminosi.

Esercizio arbitrario delle proprie ragioni

1) Esercizio arbitrario delle proprie ragioni normata dall'art. 392 c.p. che testualmente così recita:

“Chiunque al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo mediante violenza sulle cose è punito, a querela della persona offesa con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorchè la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. Si ha, altresì, violenza sulle cose allorchè un programma informatico viene alterato, modificato o cancellato in tutto o in parte viene impedito o turbato il funzionamento di un sistema informatico telematico.”

Articolo 392 c.p.

Sarebbe come dire che se un soggetto fosse stato introdotto per dolo o per errore in una centrale di rischio inserisce un virus nel computer di questa centrale e distrugge tutto.

In tale fattispecie criminosa il soggetto attivo del reato di esercizio arbitrario delle proprie ragioni mediante violenza sulle cose può essere anche chi esercita il preteso diritto pur non avendone la titolarità. Può anche essere persona diversa dal titolare del diritto illecitamente tutelato, quando questa abbia agito secondo lo schema della *negotiorum gestio* cioè una fattispecie relativa a condotta di violenza sulle cose attuata per esercitare il presunto diritto di proprietà di un figlio dell'agente. Infine può essere anche colui che non abbia la titolarità del diritto arbitrariamente esercitato, ma che agisca quale mero *negotiorum gestor* dell'effettivo titolare (fattispecie relativa all'arbitrario esercizio di un diritto del quale è risultato essere titolare il coniuge del soggetto agente).

Articolo 392 c.p.

Inoltre affinché tale fattispecie criminosa si verifichi è necessario, da un lato, quale elemento essenziale di carattere oggettivo, che la pretesa fatta valere dall'autore del fatto possa formare oggetto di una contestazione giudiziaria, senza che abbia, tuttavia, decisiva rilevanza la fondatezza o non della pretesa stessa, e, dall'altro quale essenziale elemento di carattere soggettivo, che l'imputato abbia agito nel ragionevole convincimento della legittimità della sua pretesa. Tale reato richiede oltre che il dolo generico anche quello specifico, rappresentato dal fine particolare di esercitare un proprio diritto: detto fine, se può non essere esclusivo, non può tuttavia concordare con scopi diversi incompatibili, che escludano, cioè prima ancora che il fine specifico voluto dalla norma, l'intento di farsi, sia pure arbitrariamente, ragione da se medesimo, come quando, ad esempio, si pongano in essere violenza sulle cose o minacce di una gravità eccezionale che esorbitano da quel fine o rendono comunque palese la concomitanza di un fine diverso come quello di rappresaglia o di vendetta.

Attentato ad impianti di pubblica utilità

2) **Attentato ad impianti di pubblica utilità** normato dall'art. 420 c.p. che così testualmente recita :
"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. La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni".

Articolo 420 c.p.

Nello sostanza tale fattispecie criminosa stabilisce di punire chiunque commetta un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità o dati, informazioni e programmi in essi contenuti o pertinenti.

Dopo il 1993 il legislatore con una nuova formulazione ha inteso introdurre una nuova figura di reato diretta ad una più estesa tutela dell'ordine pubblico, sanzionando penalmente qualsiasi attività diretta a distruggere o danneggiare impianti di pubblica utilità o di ricerca o di elaborazione di dati, attività considerata di per se stessa idonea a turbare la serena e ordinata convivenza sociale indipendentemente dal verificarsi in concreto del relativo turbamento.

Articolo 420 c.p.

Affinchè tale reato possa configurarsi è necessaria la presenza di un impianto inteso concettualmente come il complesso di strutture, apparecchi, attrezzature e congegni concorrenti ad uno stesso scopo ed indispensabili per un determinato fine.

Di fondamentale importanza è anche il concetto di pubblica utilità con il quale si intende un'attività pubblica cioè non limitata a singoli soggetti (ad es. una centralina computerizzata dei semafori in una città, un portale web di un ministero).

Un esempio di attentato ad impianti di pubblica utilità ci viene dato da azioni di sabotaggio effettuate da determinati soggetti che manomettano i dischi software in uso presso l'elaboratore elettronico di un centro di calcolo universitario.

Accesso abusivo ad un sistema informatico o telematico

3) **Accesso abusivo ad un sistema informatico o telematico** normato dall'art. 615 *ter* c.p. che così testualmente recita :

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero si mantiene contro la volontà espressa o tacita del titolare, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso 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, 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;

Articolo 615

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 in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio ([1])".

[1] • Articolo aggiunto dall'*art. 4, L. 23 dicembre 1993, n. 547*

Articolo 615

- ▶ Questo articolo è stato redatto su ricalco di un altro articolo che prevede la violazione di domicilio, per cui è stato individuato un domicilio informatico al quale sono state date le stesse tutele date al domicilio fisico. Il concetto di introduzione ha dato luogo a qualche difficoltà interpretativa. Chiunque abusivamente **si introduce** in un sistema informatico o telematico **protetto da misure** di sicurezza 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.
- ▶ Con tale articolo il legislatore ha teso fornire tutela ad un luogo virtuale, quale quello costituito dalla memoria di un elaboratore elettronico, adottando parametri analoghi a quelli della violazione di domicilio. In tal modo, sanzionando l'intrusione non autorizzata, si tutela il diritto degli utenti di un pc, cittadini privati o amministrazione pubblica, a regolare l'accesso al proprio "domicilio informatico".

Articolo 615 quater c.p.

4) Un'altra fattispecie criminosa ci viene data dall'art 615-quater c.p. ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*** che così testualmente recita:

“Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, 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, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma *dell'articolo 617-quater*[1]”.

[1] Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

Articolo 615 quater c.p.

- ▶ Questa fattispecie è caratterizzata dal procurare a se un profitto o recare ad altri un danno (abusivamente cioè se si procura questo mezzo per accedere in modo non legato ad una posizione che gli consente di farlo). In tema di criminalità informatica, l'art. 615 quater c.p. si applica anche all'ipotesi di detenzione o diffusione abusiva delle pics-card, schede informatiche che consentono di vedere programmi televisivi criptati attraverso la decodificazione di segnali trasmessi secondo modalità tecniche di carattere telematico. Nello specifico tratteremo sia questa fattispecie criminosa sia quella in materia di clonazioni di cellulari.
- ▶ Esaminiamo ora la fattispecie in materia di clonazioni di cellulari. Questo reato è importante perché l'acquisizione di codici ci consente di accedere a dei sistemi informatici.

La diffusione di programmi

- ▶ 5) Un altro reato è quella della ***diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*** normata dall' art. 615 *quinquies* c.p.[1] che così testualmente recita: “Chiunque diffonde, comunica o consegna un programma informatico (da lui stesso o da altri redatto) avente per scopo o per effetto il danneggiamento (art. 635 bis c.p.) di un sistema informatico o telematico o dei dati e programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329.”
[1] Articolo aggiunto dall'*art. 4, L. 23 dicembre 1993, n. 547*

Danneggiamento sistemi informatici

- ▶ 6) Un altro reato informatico è quello inerente il ***danneggiamento di sistemi informatici o telematici*** normato dall'art. 635 bis c.p. [1] che così testualmente recita:
- ▶ “Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.”
[1] Articolo aggiunto dall'art. 9, L. 23 dicembre 1993, n. 547.

Art. 635 c.p.

- ▶ A norma di tale articolo viene punito chiunque distrugga, deteriori, renda inservibili in tutto o in parte sistemi informatici o telematici altrui oppure dati, programmi e informazioni di terzi. Esaminiamo ora l'interpretazione giurisprudenziale data dalla Cassazione Penale. Antecedentemente all'entrata in vigore della legge 23 dicembre 1993 n. 547 (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi dell'art. 635 cod. pen. in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore. (*Sez. U., sent. n. 1282 del 13-12-1996 (cc. del 09-10-1996), Carpanelli (rv 206844).*)

Art. 635 c.p.

- La Corte di Cassazione con tale sentenza ha precisato che tra il reato di cui all'art. 635 c.p. e l'analoga speciale fattispecie criminosa prevista dall'art. 9 legge n° 547 del 1993, la quale ha introdotto l'art. 635bis c.p. sul danneggiamento di sistemi informatici e telematici, esiste un rapporto di successione di leggi nel tempo, disciplinato dall'art. 2 c.p. Questo articolo 635 bis è un caso di ostruzionismo del legislatore perché il danneggiamento (art. 635) prevedeva che si danneggiasse qualcosa di materiale mentre il software non è materiale. Però la cassazione ci dice che evidentemente per punire qualcuno che aveva compiuto qualcosa prima del 1993, danneggiare il software rendeva inutilizzabile l'hardware per cui era una forma di danneggiamento dell'hardware.

La frode informatica

- ▶ 7) Un altro reato informatico è quello relativo alla **frode informatica** normato dall'art. 640 ter c.p. [che così testualmente recita: “Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante .”]

Art. 640 c.p.

- ▶ Si può notare che nella fattispecie semplice, cioè nella quale non ricorrono aggravanti, la sanzione è piuttosto modesta (è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032). Per una cosa molto grave, invece, il danno anche qui si procede a querela di parte (la querela della persona offesa potrebbe non venire mai perché il danno per la persona offesa potrebbe essere maggiore se si affronta il cosiddetto streptus fori (cioè si viene a sapere) che non quello che ha subito. Passiamo ora ad esaminare il momento consumativo del reato secondo la Cassazione Penale. Il reato di frode informatica (art. 640-ter cod. pen.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa (la truffa funziona in questo modo io raggrò una persona ed ottengo un vantaggio per me ed un danno per la persona raggrata) dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

Art. 640 c.p.

- ▶ Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui. Nella specie, l'agente, utilizzando il sistema telefonico fisso installato in una filiale della società italiana per l'esercizio telefonico, con la veloce e ininterrotta digitazione di numeri telefonici, in parte corrispondenti a quelli per i quali il centralino era abilitato e in parte corrispondenti a utenze estere, riusciva ad ottenere collegamenti internazionali, eludendo il blocco predisposto per le chiamate internazionali per le quali il sistema non era abilitato, così esponendo debitoriamente la società italiana per l'esercizio telefonico nei confronti dei corrispondenti organismi esteri autorizzati all'esercizio telefonico. (Sez. VI, sent. n. 3065 del 14-12-1999 (ud. del 04-10-1999), De Vecchis (rv 214942)).

Violazione, sottrazione e sopp.

- ▶ 8) Altra fattispecie criminosa è quella concernente la *violazione, sottrazione e soppressione di corrispondenza* normata dall'art. 616 c.p. che così testualmente recita: "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è previsto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza."

Articolo 613 c.p.

- ▶ Tale norma punisce chiunque prenda cognizione del contenuto di una corrispondenza chiusa a lui non diretta, ovvero sottragga o distrugga una corrispondenza chiusa o aperta a lui non diretta (anche informatica o telematica). In tale fattispecie criminosa oggetto della tutela penale non è il segreto, che eventualmente sarà affidato alla corrispondenza, ma la corrispondenza in sé, la quale è dalla legge per se stessa ritenuta segreta indipendentemente cioè dalla segretezza o non segretezza del suo contenuto. A tal proposito si veda *Cass.*, 10 luglio 1997, *Realai*, CP 98, 1378 nt. *Gallucci*; *invi* 98, 2361, nt. *Larizza* nella quale la suprema corte ha precisato che è inibito a prendere visione della corrispondenza diretta al coniuge, senza il consenso espresso o tacito di quest'ultimo. Passiamo ora ad esaminare in tale fattispecie criminosa il concetto di giusta causa esaminato dalla cassazione penale. In materia di violazione, sottrazione e soppressione di corrispondenza, la nozione di giusta causa, alla cui assenza l'art. 616, secondo comma, cod. pen., subordina la punibilità della rivelazione del contenuto della corrispondenza, non è fornita dal legislatore ed è dunque affidata al concetto generico di giustizia, che la locuzione stessa presuppone, e che il giudice deve, pertanto, determinare di volta in volta con riguardo alla liceità -sotto il profilo etico e sociale dei motivi che determinano il soggetto ad un certo atto o comportamento. Nel caso in esame la Corte ha ritenuto sussistere la giusta causa relativamente alla rivelazione del contenuto della corrispondenza del coniuge in un giudizio civile di separazione. (Sez. V, sent. n. 8838 del 01-10-1997 (cc. del 10-07-1997), *Reali* (rv 208613)).

Intercettazione

- ▶ 9) Un altro reato informatico è quello inerente *l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* normata dall'art. 617 quater c.p. che così testualmente recita: “Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque 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.”

Art. 617 quater c.p.

- ▶ Tale norma punisce chiunque fraudolentemente intercetti, impedisca o interrompa comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, nonché mediante qualsiasi mezzo di informazione al pubblico ne riveli il contenuto.
- ▶ L'interesse tutelato dalla norma è chiaramente la riservatezza delle comunicazioni e la libertà e regolarità delle stesse che devono essere libere, complete e senza interruzioni. Com'è ovvio la particolarità del mezzo informatico non incide sul fine delle comunicazioni telematiche, che è comunque la trasmissione di dati tra soggetti in forma riservata. In proposito, sembra opportuno segnalare che tale previsione è il luogo parallelo informatico di quanto già previsto per le comunicazioni e conversazioni telefoniche o telegrafiche (art. 617), stante il fatto che il concetto di "intercettazione", assunto nell'art. 617 quater, corrisponde a "presa di cognizione della comunicazione" di cui all'art. 617.

Art. 617 quater esempio

- ▶ **Un esempio di tale fattispecie criminosa ci viene dato ad esempio da un esercizio commerciale che utilizza, mediante un terminale POS in sua dotazione, una carta di credito contraffatta, atteso che il titolare dell'esercizio commerciale è ben legittimato ad utilizzare il POS e l'accesso abusivo genera un flusso di informazioni ai danni del titolare della carta contraffatta diretto all'addebito sul suo conto della spesa fittiziamente effettuata (*si veda Cass. Sez. V, 14 ottobre 2003 – 19 novembre 2003, n° 44362, CED 227253; CP 05, 1580, nt. Aterno*)**

Installazione

- ▶ 10) **Altra fattispecie criminosa è quella concernente l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche** normata dall'art 617 quinquies c.p. che così testualmente recita: "Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater." Tale norma punisce chiunque fuori dai casi consentiti dalla legge installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi. La circolazione internet di reti wireless si configura in questa fattispecie criminosa. Altro esempio ci viene dato secondo la cassazione (Cass., sez V, 5 dicembre 2006 – 30 gennaio 2007, n° 3252, CED 236035) dall'installazione di una fotocamera digitale su un "postamat" di un ufficio postale.

Falsificazione

- ▶ 11) Un altro reato è quello della *falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche* normato dall'art. 617 sexies c.p. che così testualmente recita: “Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma *dell'articolo 617-quater* .”

Art. 617 sexies c.p.

- ▶ Tale norma punisce chiunque al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, formi falsamente, alteri o sopprima in tutto o in parte il contenuto (intercettato anche occasionalmente) di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Falsità informatica

- ▶ 12) Altra fattispecie criminosa è quella della *falsità informatica* normata dall'art. 491 bis c.p. che così testualmente recita : “Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.”

Art. 491 bis c.p.

- ▶ Con tale articolo si equipara il supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi al documento cartaceo ai fini delle disposizioni sulle falsità documentali relative agli atti pubblici ed alle scritture private. Infatti l'archivio informatico di una pubblica amministrazione deve essere considerato alla stregua di un registro tenuto da un soggetto pubblico, con la conseguenza che la condotta del pubblico ufficiale che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici della pubblica amministrazione, confezioni un falso atto informatico destinato a rimanere nella memoria dell'elaboratore, integra una falsità in atto pubblico, a seconda dei casi, materiale o ideologica. In ordine alla falsità degli atti, essa può essere di due forme: la falsità materiale, ossia la non genuinità del documento e la falsità ideologica, ossia la non veridicità dello stesso. Si ha dunque falsità materiale quando "vi è una divergenza tra autore apparente e autore reale del documento o quando quest'ultimo è stato alterato successivamente alla sua formazione"; si ha falsità ideologica quando "il documento contiene attestazioni o dichiarazioni non veritiere".

Comunicazioni e conversazioni

- ▶ 13) Un altro reato informatico è rappresentato dalle altre **comunicazioni e conversazioni** normato dall'art. 623 *bis* c.p. che così testualmente recita: “Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati.”
- ▶ L'art. 623 *bis* c.p. assimila le comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche a qualunque altra trasmissione a distanza di suoni, immagini o altri dati.

Altri crimini informatici

- ▶ Altri crimini informatici sono stati introdotti dalla legislazione speciale
- ▶ Ad esempio:
 - ▶ 1. l'art. 4 della Legge 13 dicembre 1989 n. 401 (Svolgimento di attività organizzata per l'accettazione e la raccolta, anche per via telefonica e telematica, di scommesse o per favorire tali condotte in assenza di concessione, autorizzazione o licenza);
 - ▶ 2. la Legge 3 agosto 1998 n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù);
 - ▶ 3. la Legge 18 agosto 2000 n. 248 (Norme di tutela del diritto di autore) e successive modificazioni;
 - ▶ 4. l'art. 12 del d.l. n. 143 del 1991 (Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante);
 - ▶ 5. il D.lgs 30 giugno 2003, n.196 (Codice in materia di protezione dei dati personali).

La legge 547/1993

- ▶ LA NORMATIVA EX Ante legge 48/2008

I reati informatici sono stati disciplinati dalla legge n° 547 del 23 dicembre 1993, che ha introdotto figure nuove di reato ed ampliato gli strumenti a disposizione delle forze di polizia, attraverso la modifica di alcuni articoli al codice penale e di procedura penale, nonché l'introduzione di nuovi. La normativa, all'epoca dell'emanazione esaustiva, ha recepito positivamente segnali provenienti dal mondo della telematica e da quello delle investigazioni, individuando profili nuovi di responsabilità penale e disciplinando condotte di reato che già si erano evidenziate nella realtà criminale emergente

La legge 547/1993

- ▶ Prima della legge n° 547 del 1993, i comportamenti illeciti realizzati mediante, nonché quelli aventi ad oggetto comunque interessanti il computer, potevano assumere rilevanza penale solo in quanto riconducibili ad una figura di reato, per così dire, tradizionale ossia ad una fattispecie criminosa ideata prima che l'informatica assumesse la rilevanza e la diffusione che tutti conosciamo.
- ▶ La soluzione percorsa dal legislatore con l'adozione della legge 547/1993 è stata quella di modificare ed integrare l'impianto del codice penale inserendovi, in punti diversi, le nuove figure criminose. Peraltro, in coerenza con la scelta operata dal legislatore del 1930 che ha raggruppato i reati secondo l'unità dell'oggetto giuridico, si è preferito ricondurre le nuove fattispecie a figure già esistenti, piuttosto che procedere all'introduzione di un nuovo titolo nel codice penale.

Legge 547/1993

- ▶ Determinante in tal senso è stata la considerazione delle condotte da incriminare, non quali aggressioni ad un nuovo oggetto unitario, bensì come nuove forme di aggressione di beni giuridici già tutelati da preesistenti norme del c.p.

Normativa

- Legge 1 aprile 1981, n. 121 (Nuovo ordinamento dell'Amministrazione della pubblica sicurezza).
- ▶ Legge 2 gennaio 1991, n. 1 (Disciplina dell'attività di intermediazione mobiliare e disposizioni sull'organizzazione dei mercati mobiliari).
 - ▶ Legge 5 luglio 1991, n. 197 (Conversione in legge, con modificazioni, del decreto-legge 3 maggio 1991, n. 143, recante provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio).
 - ▶ Decreto legislativo 12 febbraio 1993, n. 39 (Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm, della legge 23 ottobre 1992, n. 421).
 - ▶ Legge 23 dicembre 1993 n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica).
 - ▶ Legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali);

Normativa

- ▶ Legge 31 dicembre 1996, n. 676 (Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali).
- ▶ Legge 15 marzo 1997, n. 59 (Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa).
- ▶ Legge 31 luglio 1997 n° 249 (Istituzione dell'Autorità per le garanzie sulle comunicazioni e norme sui sistemi di telecomunicazioni e radiotelevisivo)
- ▶ Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59).
- ▶ Decreto legislativo 31 marzo 1998, n. 114 (Riforma della disciplina relativa al settore del commercio, a norma dell'art. 4, comma 4, della legge 15 marzo 1997, n. 59).
- ▶ Legge 3 agosto 1998 n° 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù)

Normativa

- ▶ Decreto Legislativo del 8 giugno 2001 n° 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000 n° 300);
- ▶ Decreto Legislativo 30 giugno 2003 n° 196 (Codice in materia di protezione dei dati personali)

La Computer Forensics

Sommario

- ▶ *Il Concetto di computer forensics;*
- ▶ *La prova e le sue caratteristiche;*
- ▶ *L'analisi del disco;*
- ▶ *Tecniche investigative;*
- ▶ *Phishing.*

Il concetto

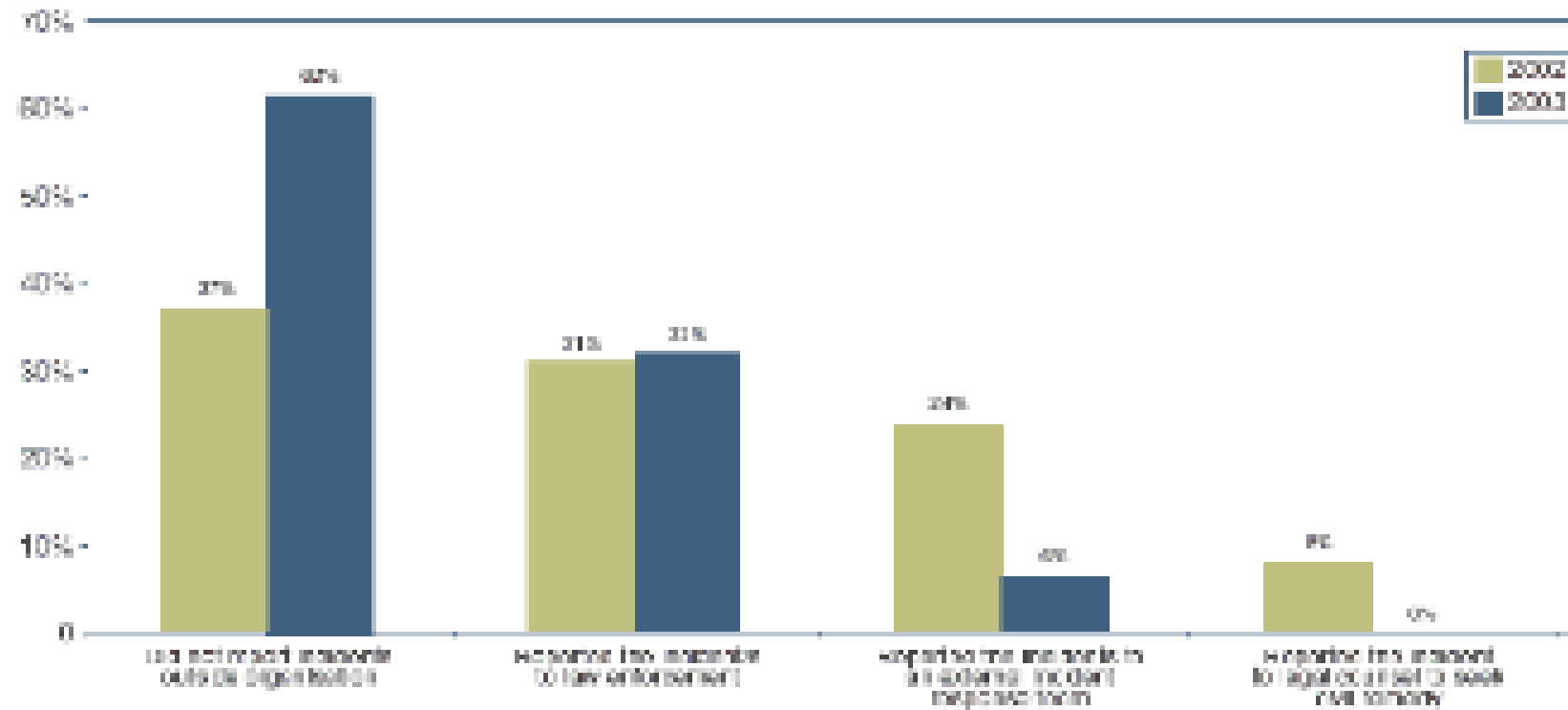
Cosa è Computer Forensics?

La Computer Forensics è l'applicazione di tecniche scientifiche ed analitiche ai Sistemi Operativi ed ai Filesystem al fine di recuperare prove utili (e valide) nell'attività processuale.

La prova



► L'approccio aziendale



Source: 2003 Australian Computer Crime and Security Survey
2002 and 2003 percentages may not add to 100% due to rounding.

La dottrina

- ▶ PROCEDIMENTO A 4 PASSI
- ▶ Acquisizione
- ▶ Identificazione
- ▶ Valutazione
- ▶ Presentazione

I crimini informatici

Chi ha bisogno della Computer Forensics?

- ▶ La vittima
- ▶ Le forze di polizia
- ▶ Assicurazioni
- ▶ Le aziende
- ▶ Il sistema giudiziario

Le vittime

- ▶ Aziende
 - ▶ Governo
 - ▶ Individui
- ▶ Chi sono le vittime?

Obiettivi

- ▶ Obiettivi della Analisi Forense
- ▶ Identificare il colpevole;
- ▶ Identificare il metodo/la vulnerabilità della rete della rete che ha consentito al colpevole di guadagnare l'accesso al sistema;
- ▶ Condurre un assessment del danno della rete colpita;
- ▶ Conservare correttamente la prova per l'azione giudiziaria;

Le richieste

- ▶ Tipi di richieste forensi
- ▶ Analisi delle intrusioni
- ▶ Assessment del danno
- ▶ Esame del sospetto
- ▶ Tool Analysis
- ▶ Analisi dei file di log
- ▶ Ricerca della prova

Intrusioni

- ▶ Analisi delle intrusioni
- ▶ Chi si è introdotto?
- ▶ Cosa ha fatto?
- ▶ Quando è accaduto?
- ▶ Dove è andato?
- ▶ Perché ha scelto questa rete?
- ▶ Come ha fatto?

Danno

- ▶ Assessment del danno
- ▶ Che cosa ha visto l'intrusore?
- ▶ Cosa ha preso?
- ▶ Che tracce ha lasciato?
- ▶ Dove è andato?

Crimini propri

▶ CARATTERISTICHE
DELLA PROVA

▶ ANALISI

La prova

- ▶ La prova informatica deve essere...
- ▶ ...come ogni altra prova:
- ▶ ammissibile
- ▶ autentica
- ▶ accurata
- ▶ completa
- ▶ convincente per il giudice

La prova

- ▶ La prova informatica deve essere...
- ▶ Essere convincente
- ▶ Avere un valore probatorio
- ▶ Un test pratico di presentazione
- ▶

Procedure forensi

Procedure Forensi

"Congelare la scena del crimine"

Procedimento formale

imaging

Mantenere la continuità della prova

controlled copying

controlled print-out

Raccolta testimonianze

ACPO

Catena di custodia

- ▶ Catena di custodia
- ▶ Una volta in possesso della copia originale del dispositivo, occorre documentare come si conserva
- ▶ Dove è memorizzata
- ▶ Chi ne ha avuto accesso
- ▶ Che operazioni sono state effettuate su di essa
- ▶ Questa è la catena di custodia, che fornisce la documentazione provante che l'integrità dei dati è stata preservata e non c'è stata alcuna modifica, seppur casuale.

Catena di custodia

- ▶ Catena di custodia
- ▶ Tecnicamente, si ottiene con:
- ▶ documentazione,
- ▶ hashes,
- ▶ timestamps

I dispositivi

- ▶ Tipi di dispositivi
- ▶ CD-RWs
- ▶ DVD-RWs
- ▶ Floppies
- ▶ Hard drives
- ▶ Flash ram (smart media, memory stick, mmc, secure digital)
- ▶ PDA
- ▶ Telefoni cellulari

ANALISI DEL DISCO

Analisi del disco

- ▶ Richiami sul procedimento forense
- ▶ Preparazione
- ▶ Protezione
- ▶ Imaging
- ▶ Esame
- ▶ 11
- ▶ Documentazione

Analisi del disco

Extract, process, interpret

Lavorare sull'immagine o sulla copia sicura

Data extracted may be in the binary form

Process data to convert it to understandable form

Reverse-engineer to extract disk partition information, file systems, directories, files, etc

Software available for this purpose

Interpret the data - search for key words, phrases, etc.

Analisi del disco

Problemi aperti

Problemi sull'uso di tool proprietari per forze di polizia

disclosure del metodo

Open source?

"Parità di armi" con la difesa

Es: Pedofilia rilascio del materiale alla difesa

Analisi del disco

- ▶ Network Monitoring
- ▶ Consentito quando:
- ▶ Il sistema è compromesso e si sta monitorando per localizzare ed identificare un intrusore
- ▶ Quando il monitoraggio è esplicitamente consentito dagli utenti (AUP)
- ▶ Dove le leggi lo consentono

Analisi del disco

Sporcare le prove

- La prova informatica è "modificabile"

Un intrusore potrebbe aggiungere/rimuovere/modificare il contenuto dei log

Possono compromettere i componenti del sistema che ospita i log

Potresti modificare qualcosa durante l'investigazione

Analisi del disco

- Recupero di file
- File cancellati
- File nascosti
- Slack Space
- Bad Blocks
- Steganografia
- File cifrati
- Partizioni nascoste

Analisi del disco

Bit Stream Backup

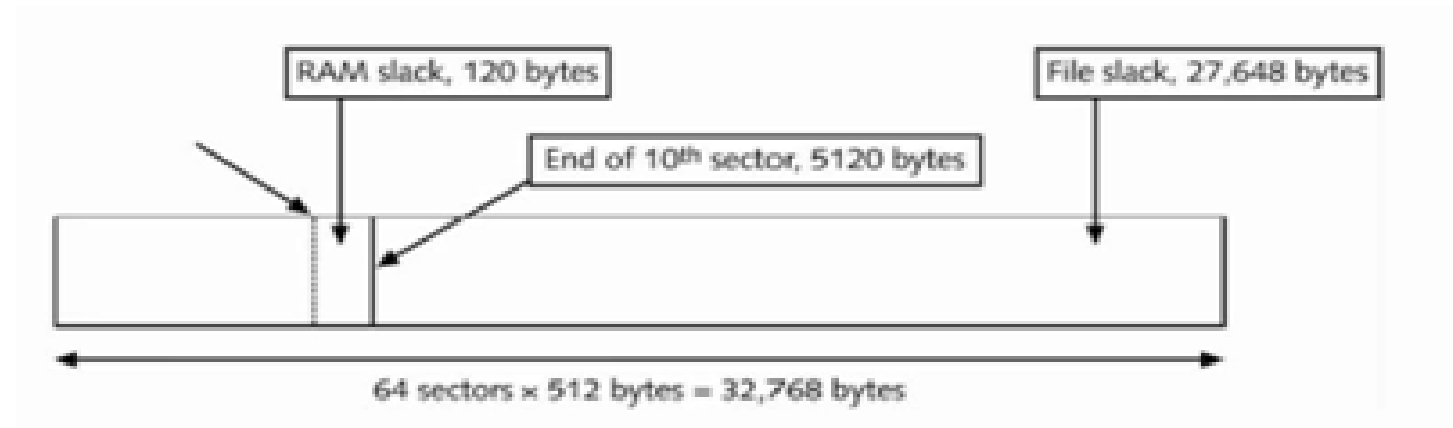
- Settore per settore
- Mappa il drive originale
- Recupera existing files, RAM slack, file slack

Analisi del disco

- ▶ Identificare la prova
- ▶ Hard disk nella forma di
- ▶ Swap files
- ▶ Temporary files
- ▶ Spazio del disco non allocato
- ▶ Spazio del file slack
- ▶ Memoria e Processi in piedi
- ▶ Floppy Disks, CD-ROMS, DVDs, Zip e dischi Jaz, Nastri di backup
- ▶ File di Log
- ▶ RAID, Backup
- ▶ informatico”.

RAM

RAM E FILE DI SLACK

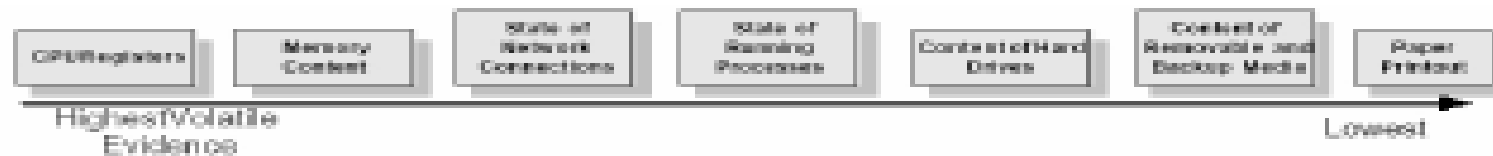


Come conservare

- ▶ Come conservare
- ▶ Bypassare il Sistema operativo per creare backup bit-stream di tutta la prova
- ▶ Duplicati sono riportati su HD, CD-ROM, etc.
- ▶ Tutte le analisi sono fatte su queste immagini
- ▶ Documentare ogni cambiamento che comporta il cambiamento dell'immagine
- ▶ Autenticare le immagini rispetto agli originali usando CRC o hash MD5

Volatilità

- ▶ Ordine di volatilità
- ▶ Registri, cache, memoria delle periferiche
- ▶ Memoria(kernel, fisica)
- ▶ Stato della rete
- ▶ Processi in esecuzione
- ▶ Dischi



Analisi

- ▶ Analisi dei File di Log
- ▶ Eventi
- ▶ Quali eventi sono monitorati?
- ▶ Cosa rivelano I record degli eventi?
- ▶ File di log di Firewall/IDS/Router/Server?
- ▶ TripWire Database?
- ▶ Modem/FTP/Telnet/RAS

Steganografia

Steganografia

Creata per proteggere i diritti d'autore

Usata, generalmente, per nascondere dati o file nella grafica

Programmi per intercettarla

Stegdetect

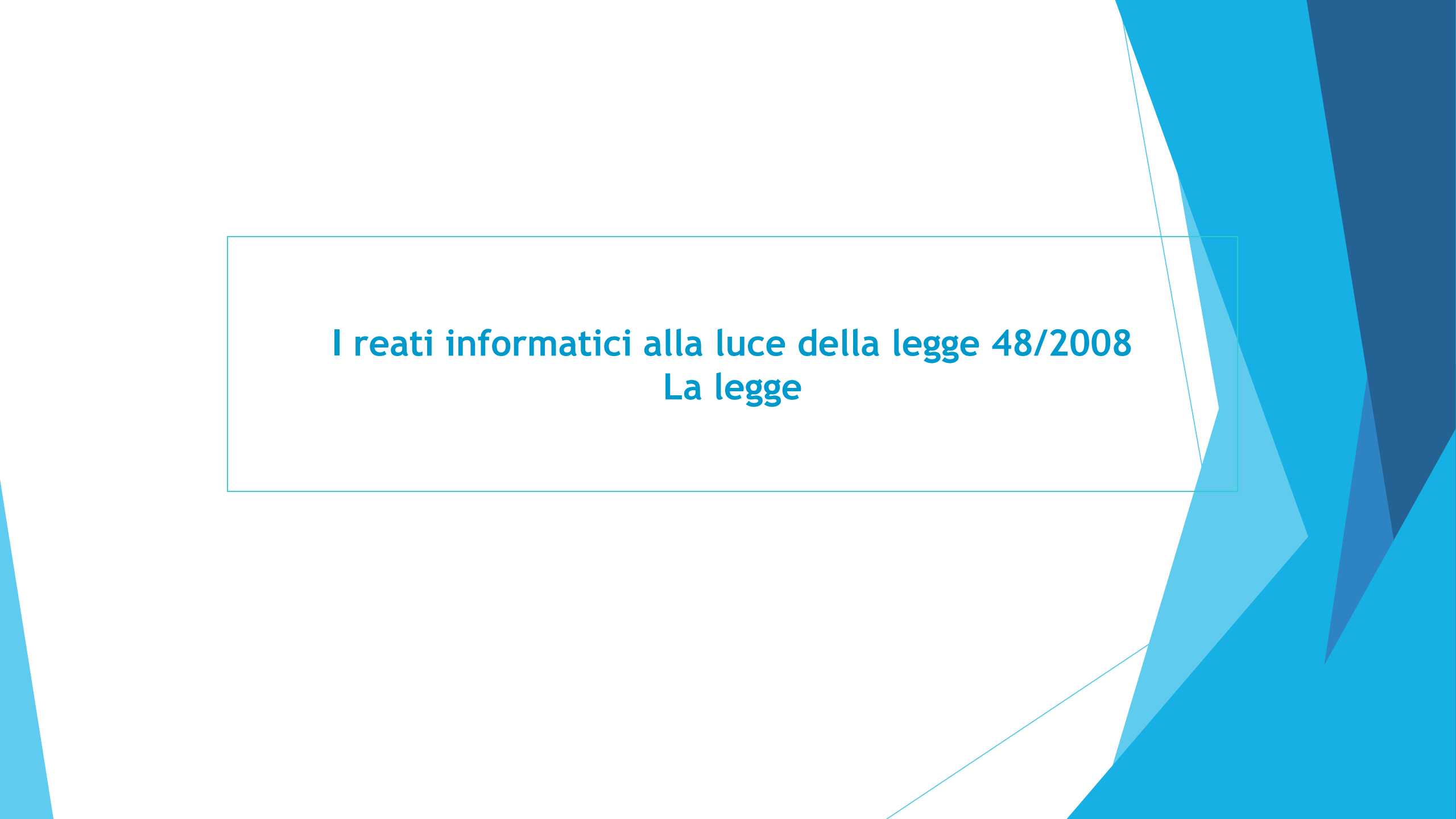
Stegbreak

Usata per proteggere le informazioni da persone in regime non libero.



▶ Example:

▶ Investigation techniques for phishing



I reati informatici alla luce della legge 48/2008

La legge

Sommario

- ▶ *La ratifica della convenzione di Budapest;*
- ▶ *Le novità legislative;*
- ▶ *I nuovi reati informatici;*
- ▶ *Il freezing dei dati;*
- ▶ *Conclusioni*

La ratifica

- ▶ In data 27 febbraio 2008 è stata ratificata dal Senato la legge di ratifica alla Convenzione di Budapest del 23 novembre 2001 del Consiglio d'Europa; dopo un'appassionata ed elaborata analisi della normativa presso le Commissioni riunite di Giustizia e Senato si è arrivati, frettolosamente anche grazie ad un accordo fra maggioranza e opposizione, sul finire della legislatura all'approvazione del testo definitivo contenuto nella [legge 18 marzo 2008, n. 48](#)

La convenzione di Budapest

- ▶ La convenzione del Consiglio d'Europa sulla criminalità informatica costituisce un passo importante normativo nel progresso normativo in questo settore ed è ***il primo agreement internazionale che riguarda i crimini commessi attraverso la Rete Internet o altri network informatici***

La convenzione di Budapest

- ▶ Il classico **computer crime** si allarga elasticamente fino a ricomprendere tutte le condotte illegali poste in essere attraverso un sistema informatico e quelle per l'individuazione delle quali si debbano o possano raccogliere elementi probatori in formato elettronico.
- ▶ La convenzione di Budapest ha l'obiettivo di:
- ▶ Conformare la politica degli Stati membri sul fronte di una così ampia e crescente minaccia;
- ▶ Giungere ad un concreto ed efficace coordinamento degli sforzi tesi a contrastare il crimine tecnologico nelle sue più diverse manifestazioni

IL DPR

Successivamente il 4 aprile 2008 è stata promulgata dal Presidente della Repubblica la Legge 18 Marzo 2008 n° 48, recante la ratifica della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001. Tale normativa ha introdotto significative modifiche al Codice Penale, al Codice di procedura penale, al Decreto legislativo 8 giugno 2001 n° 231 e al Decreto Legislativo 30 giugno 2003 n° 196 (codice della Privacy)

L'aspetto più delicato

- ▶ L'aspetto più delicato ruota attorno all'esigenza di garantire la genuinità della prova digitale, come già traspariva nella Raccomandazione R (95) del 13 settembre 2001 firmata dal Comitato dei Ministri del Consiglio d'Europa, antesignano della Convenzione, nella quale si sottolinea l'esigenza *“to collect, preserve, and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity (...) should be recognized”*(art. 13).

La legge come valutazione e innovazione

- ▶ La legge 48/2008 è frutto di una valutazione di sostanziale adeguatezza del nostro sistema penale che ha riconosciuto dal 1993, con la legge n. 547, l'esistenza dei delitti informatici e ha via via modificato il quadro normativo con disposizioni sulla tutela dei dati personali (legge 675/96), sulla pedopornografia in rete (legge 269/98), sulla pirateria informatica (legge 248/2000).
- ▶ In questo senso il recepimento della Convenzione rappresenta forse un'occasione perduta. *Sul piano sostanziale, infatti, la legge introduce alcune condotte inedite come la diffusione di virus informatici, ossia di programmi che diffusi nei computer danneggiano irrimediabilmente i programmi installati, i dati immagazzinati e i sistemi operativi degli elaboratori.*

Difesa dei sistemi informatici e la privacy

- ▶ Tra le altre fattispecie illecite trova posto un nutrito arsenale a difesa dei sistemi informatici, non solo privati, ma anche di pubblica utilità, da ipotesi di danneggiamento. Con la possibilità poi di sanzionare, con l'intero ventaglio delle misure previste dal decreto 231/01, le imprese quando abbiano tratto un vantaggio dal reato informatico commesso da propri dipendenti. Più significativa è la parte che introduce disposizioni per agevolare la fase investigativa. In questo senso spicca la modifica al Codice della privacy, in base alla quale i fornitori e gli operatori di servizi informatici possono essere costretti a conservare e proteggere per un periodo massimo di 6 mesi i dati relativi al traffico telematico (ma non al suo contenuto).

La perquisizione

Misure specifiche sono poi introdotte per agevolare le operazioni di perquisizione e sequestro di dati informatici detenuti dagli operatori ma anche da altri soggetti: per esempio viene esplicitamente introdotta la possibilità di rintracciare materiale informatico detenuto da banche.

► IL CASO DELLA PERQUISIZIONE ON LINE

Il caso tedesco

- ▶ A seguito della sentenza della Corte Costituzionale Tedesca (*Bundesverfassungsgericht*) del 27 febbraio 2008 è esplosa una nuova questione legata alla legittimità circa l'utilizzo di tecnologie sempre più evolute e invisibili in sede d'indagine, rappresentate nel caso concreto dalle cd perquisizioni *online*.
- ▶ La vicenda ha per oggetto una norma di legge contenuta all'interno della Legge sulla protezione della Costituzione del *North Rhein Westfalia* (VSG), in particolare il § 5 co. 2, n°11 che autorizzava il *Verfassungsschutzbehörde*, organismo di intelligence a "protezione della Costituzione", a effettuare due tipi di attività:
- ▶ un monitoraggio segreto su quanto accadesse in *Internet* e l'accesso a sistemi informatici attraverso un meccanismo di intrusione a mezzo *Trojan*, sempre in modalità silente.
- ▶ A livello tecnico, esistono essenzialmente due modelli di monitoraggio delle attività che più si avvicinano al concetto di perquisizione virtuale:
- ▶ la cd **online search o one time copy ovvero la online surveillance**. La prima si caratterizza per consentire l'acquisizione mediante copia di dati contenuti all'interno delle memorie dei dispositivi oggetto di attenzione;
- ▶ la seconda permette un **monitoraggio costante delle attività in rete poste in essere da un soggetto associato a un determinato account**.
- ▶ Grazie all'utilizzo di cd *sniffer* o attraverso l'intrusione di "programmi spia", come appunto il *trojan-horse* oggetto della vicenda, tali operazioni sono rese tecnicamente possibili. È ben evidente come tali strumenti siano fortemente invasivi nella sfera privata e di libertà dei soggetti sottoposti a tale misura, tenuto conto, fra l'altro, della loro caratteristica peculiare rivestita dal fatto di essere, informaticamente parlando, innocua.

Il caso tedesco

- ▶ La vicenda della *Online Durchsuchung* può essere assimilata, volendo tentare un parallelismo con la disciplina processuale italiana, alle attività di contrasto alla pedopornografia *online*, pur rappresentandosi come “*tertium genus*” fra ispezione e perquisizione

Le novità

- ▶ Il provvedimento introduce le seguenti novità:
- ▶ Sanzioni più pesanti per i reati informatici
- ▶ Norme di contrasto più efficace alla pedopornografia in rete
- ▶ Sanzioni anche a carico della società
- ▶ Possibilità per le forze dell'ordine di chiedere al provider il congelamento dei dati telematici per 6 mesi
- ▶ Maggiori tutele per i dati personali

ex ante legge 48/08

- ▶ Prima della legge di ratifica della convenzione di Budapest non esisteva una norma in Italia che indicasse dei requisiti sulla computer forensics.
- ▶ Oggi invece un aspetto importante ed anche per certi versi critico è il concetto di non alterazione del reperto informatico.

perquisizione ed ispezione

- ▶ Gli articoli 244 (perquisizione) e 247 (ispezione) del codice di procedura penale sono stati modificati, imponendo alla polizia giudiziaria di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
- ▶ Queste modifiche pongono fine a un dibattito che da anni si trascinava nelle aule di giustizia e che vedeva contrapposto chi, tipicamente, le forze di polizia, riteneva di poter sequestrare e analizzare computer senza adottare particolari cautele tecniche a chi - gli avvocati - chiedeva il rispetto dei principi fissati dalla computer forensics.

Il nuovo art. 244

- ▶ **Art.244 Casi e forme delle ispezioni** (codice procedura penale)
- ▶ 1. L'ispezione delle persone, dei luoghi (103) e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato (354 1 e 2 comma, 364).
2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359). anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione

Il nuovo art. 247

- ▶ **Art.247 Casi e forme delle perquisizioni (codice procedura penale)**
- ▶ 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato (253), è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione
- ▶ 2. La perquisizione è disposta con decreto motivato.
- ▶ 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria (57) delegati con lo stesso decreto.

i sequestri informatici

- ▶ Dall'entrata in vigore della legge, le forze di polizia sono obbligate ad adottare questi sistemi. Il che implica decidere quali sono quelli che hanno un qualche valore giuridico, e stabilire regole tecniche per l'esecuzione delle operazioni. Cambiano parzialmente anche le norme sui sequestri informatici registrando un piccolo passo avanti e confermando la validità di quanto associazioni per la tutela dei diritti civili online stanno sostenendo, in Italia e all'estero, da oltre dieci anni. Le autorità devono sequestrare (senza alterarli) i soli file di interesse di indagine (e non i supporti che li contengono, o le macchine) quando questi risiedono presso operatori telefonici lsp e uffici postali. Mentre nel caso intervengano presso un provato cittadino sono ancora liberi di sequestrare interi computer



► IL SEQUESTRO

Il sequestro probatorio

- ▶ Altra importante modifica va segnalata nel settore del sequestro probatorio, istituto anch'esso interessato dall'intervenuta evoluzione tecnologica. In particolare all'art. 260 c.p.p. si prevede la possibilità da parte delle autorità di assicurare le cose sequestrate anche attraverso l'apposizione di sigilli *di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia*. Tale previsione recepisce anche a livello processuale la certificazione fra copia e originale tramite procedure informatizzate, ossia le cd *hash functions*; inoltre, al 2° comma, estende la presunzione di deperibilità e alterazione prevedendo la possibilità di effettuarne copia *che deve essere realizzata su adeguati supporti mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*. Il sequestro rappresenta l'istituto processuale che più ha fatto discutere, e, che continua tutt'oggi a generare profili di maggior criticità.

La falsa dichiarazione

- ▶ Viene infine estesa anche alle perquisizioni informatiche la possibilità per la polizia giudiziaria di procedere anche in presenza di misure di sicurezza. La norma potrebbe quindi essere interpretata nel senso che sarebbe addirittura legittimo “bucare” un sistema, se non se ne possiedono le password, pur di accedervi e prendere le prove.
- ▶ Dal punto di vista dei reati, viene introdotto quello di falsa dichiarazione al certificatore di firme elettroniche: è sanzionato con la reclusione fino a un anno il furto d'identità o l'uso di false generalità nei confronti di chi deve certificare l'identità del titolare di una firma elettronica

La falsa dichiarazione

- ▶ Simmetricamente la legge punisce il certificatore di firma elettronica che non rispetta le regole normative per il rilascio dei certificati di qualificati. Inoltre la legge tenta di realizzare i reati che puniscono il cracking di sistema e il danneggiamento di informazioni.

I reati di danneggiamento

Sono previsti, in successione, i reati di:

- Danneggiamento di dati, informazioni e programmi
- Danneggiamento di sistemi informatici (che punisce esplicitamente gli attacchi DoS) anche di pubblica utilità

Ulteriori modifiche sono state apportate anche per la disciplina dei dati personali per quanto riguarda la data retention dei dati di traffico.

Su semplice disposizione delle autorità di polizia che esegue indagini preventive, e anche su richiesta di autorità straniere, operatori e ISP sono obbligati a conservare i dati di traffico per almeno 90 giorni

La legge in dettaglio

- ▶ Nel dettaglio la legge di ratifica consta di 14 articoli, divisi in 4 capi. Tre in sostanza sono i campi di intervento finalizzati rispettivamente al rafforzamento degli istituti rilevanti in sede di cooperazione internazionale, ad una migliore armonizzazione e disciplina in ambito di diritto sostanziale relativo al cybercrime e, in ultimo, alla predisposizione di strumenti processuali comuni e condivisi atti all'acquisizione e conservazione delle evidenze elettroniche.

- 
- ▶ Capo II
 - ▶ MODIFICHE AL CODICE PENALE E AL DECRETO
LEGISLATIVO 8 GIUGNO 2001, N. 231

- ▶ Art. 3 (Modifiche al titolo VII del libro secondo del codice penale)
- ▶ 1. All'articolo 491-bis del codice penale sono apportate le seguenti modificazioni:
 - a) al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»;
 - ▶ b) il secondo periodo è soppresso.
- ▶ 2. Dopo l'articolo 495 del codice penale è inserito il seguente:
«Art. 495-bis. - (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri). - Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno».

- ▶ Art. 4 (Modifica al titolo XII del libro secondo del codice penale)
- ▶ 1. L'articolo 615-quinquies del codice penale è sostituito dal seguente:
«Art. 615-quinquies. - (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico). - Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

Il nuovo art. 615

- ▶ **Art. 615 quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**
- ▶ Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Il nuovo art. 635

Art. 5 (Modifiche al titolo XIII del libro secondo del codice penale)

1. L'articolo 635-bis del codice penale è sostituito dal seguente:
«Art. 635-bis. - (**Danneggiamento di informazioni, dati e programmi informatici**). - Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».

2. Dopo l'articolo 635-bis del codice penale sono inseriti i seguenti:
«Art. 635-ter. - (**Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**). - Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Il nuovo art. 635 e 640

Art. 635-quater. - (***Danneggiamento di sistemi informatici o telematici***). - Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635-quinquies. - (***Danneggiamento di sistemi informatici o telematici di pubblica utilità***). - Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

Dopo l'articolo 640-quater del codice penale è inserito il seguente:
«Art. 640-quinquies. - (***Frode informatica del soggetto che presta servizi di certificazione di firma elettronica***). - Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

Art. 6 (Modifiche all'articolo 420 del codice penale)

1. All'articolo 420 del codice penale, il secondo e il terzo comma sono abrogati.

Art. 7 (Introduzione dell'[articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231](#))

1. Dopo l'[articolo 24 del decreto legislativo 8 giugno 2001, n. 231](#), è inserito il seguente:
«Art. 24-bis. - (Delitti informatici e trattamento illecito di dati). - 1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».

- 
- ▶ Capo III
 - ▶ MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

Art. 8 (Modifiche al titolo III del libro terzo del codice di procedura penale)

1. All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».
2. All'articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente: «1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».
3. All'articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».
4. All'articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni: a) il comma 1 è sostituito dal seguente: «1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;
b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti: «o alterarli».

- ▶ 5. Dopo l'articolo 254 del codice di procedura penale è inserito il seguente:
«Art. 254-bis. - (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). - 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immutabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».
- 6. All'articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così è ordinato,» sono inserite le seguenti: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,».
- 7. All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».
- 8. All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:
 - a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «, anche di carattere elettronico o informatico,»;
 - ▶ b) al comma 2 è aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immutabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

- ▶ Art. 9 (Modifiche al titolo IV del libro quinto del codice di procedura penale)
- ▶ 1. All'articolo 352 del codice di procedura penale, dopo il comma 1 è inserito il seguente:
«1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previste, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».
- 2. All'articolo 353 del codice di procedura penale sono apportate le seguenti modificazioni:
 - a) al comma 2 sono aggiunte, in fine, le seguenti parole: «e l'accertamento del contenuto»;
 - ▶ b) al comma 3, primo periodo, le parole: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» sono sostituite dalle seguenti: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica,» e dopo le parole: «servizio postale» sono inserite le seguenti: «, telegrafico, telematico o di telecomunicazione».
- ▶ 3. All'articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

Art. 10 il freezing dei dati

- ▶ Art. 10 (Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196)
- ▶ 1. Dopo il comma 4-bis dell'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sono inseriti i seguenti:
«4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati.

Art. 10 il freezing dei dati

- ▶ Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. 4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. 4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

Art. 10

- ▶ IL FREEZING DEI DATI - articolo 10 legge 48/2008

Il freezing

- ▶ L'art. 10 della [legge n. 48/2008](#) è intervenuto altresì su una norma molto travagliata, spesso ritoccata da legislatore nazionale, estranea al codice di procedura penale ma che assume estrema rilevanza in ordine alla tutela della *privacy*, in particolare in ambito di *data retention* ex art. 132 del d.lgs. n. 196/2003. Si è intervenuti attraverso l'introduzione del comma 4-ter, 4-quater, 4-quinquies, istituzionalizzando il **cd congelamento dei dati per ragioni urgenti**, il quale conferisce ampi poteri alle forze di polizia e ai servizi segreti. Tale potere sembra limitato ai casi eccezionali e urgenti di cui all'art. 226 del dlgs n. 271 del 1989 in tema di indagini e intercettazioni preventive, anche se in realtà si aggiunge una formula di fatto generica indicante “*finalità di accertamento e repressione di specifici reati*”.

Il freezing: gli obblighi

- ▶ Questa apertura mal si concilia con tale previsione che assume carattere eccezionale, rappresentandosi come eccessivamente fluida in un settore così delicato come quello delle comunicazioni salvaguardate come sopra ricordato dall'art. 15 della Costituzione.
- ▶ Gli obblighi previsti possono essere così riassunti:
- ▶ a) obbligo di conservazione dei dati di traffico per un periodo di novanta giorni prorogabile fino a sei mesi, su richiesta dei soggetti indicati al comma 4-ter per finalità di indagine essenzialmente preventiva;
- ▶ b) applicabilità nei confronti del *Service Provider* dell'art. 326 c.p. in ipotesi di rivelazione del segreto connesso all'ordine di conservazione ricevuto;
- ▶ c) convalida di detto provvedimento entro 48 ore da parte del Pubblico Ministero.

Il sogg. processuale

- ▶ L'ultimo punto merita un'ulteriore riflessione sulla scelta del soggetto processuale a cui affidare la convalida del provvedimento ex art. 132, comma 4-ter: trattandosi di indagini (o intercettazioni) preventive ex art. 226 disp. att. c.p.p. fa presumere l'insussistenza al momento di un procedimento penale in corso con conseguente assenza di un P.M. deputato all'indagine. Sarebbe forse stato più opportuno delegare tale funzione al giudice del luogo dell'esecuzione del congelamento dei dati ovvero del luogo in cui i dati sono conservati in funzione di giudice per le indagini preliminari, così da assicurare la necessità di tale strumento valutata da un organo terzo.

Art. 11 (Competenza)

1. All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma:

«3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

1-bis. Le disposizioni di cui al comma 3-quinquies dell'articolo 51 del codice di procedura penale, introdotto dal comma 1 del presente articolo, si applicano solo ai procedimenti iscritti nel registro di cui all'articolo 335 del codice di procedura penale successivamente alla data di entrata in vigore della presente legge.

► LE MODIFICHE ALL'ARTICOLO 51 C.P.P. LA Competenza

La competenza

- ▶ L'art. 11 prevede la modifica all'art. 51 del codice di procedura penale in materia di competenza.
- ▶ *Si è deciso di dar vita alle cd “Procure Informatiche Distrettuali” con l'intento di creare pool investigativi specializzati perseguendo lo schema vincente delle procure antimafia sorte negli anni '90.*
- ▶ *Da più parti si è sostenuto come tale modifica risulti “priva di alcuna utilità sostanziale” che porterà nel futuro sicuramente problematiche serie rappresentate dal carico di lavoro sproporzionato cui saranno sottoposte le procure. L'eterogeneità dei reati informatici richiamati non permette lo sviluppo di modalità investigative comuni ma al più settoriali, peraltro già in via di sviluppo e sostenute da alcune importanti procure italiane come quella milanese. Inoltre la mancanza di organi interni di raccordo simili alla DNA, DDA o alla DIA ostacolano lo sviluppo di una vera e propria rete nazionale dedicata a tali aspetti.*
- ▶ All'indomani della modifica legislativa si segnalò altresì la difficoltà di individuare l'Ufficio del Giudice per le indagini preliminari territorialmente competente e non considerato dal legislatore della novella. Per fortuna vi si provvede velocemente con gli artt 2 e 12-bis della [l. n. 125 del 2008](#) in cui venne formalizzato il corretto raccordo delle norme interessate

Es. del 2010

- ▶ Si vedano sul punto le perplessità espresse dal coordinatore del *pool* reati informatici di Milano, il quale in occasione dell'inaugurazione dell'anno giudiziario 2010 scriveva:
- ▶ *“Parlando di reati informatici non può tacersi il grave e ingiustificato aggravio di lavoro per questa Procura della Repubblica determinato dall'introduzione dell'art. 51 quinquies del codice di procedura penale a seguito del quale una qualsiasi intrusione informatica (per esempio quella di un marito geloso di Sondrio che “sbircia” nel computer della moglie), una qualsiasi frode informatica commessa a Pavia, Varese, Como, una qualsiasi captazione di dati da un qualsiasi apparecchio Bancomat di Busto Arsizio dovrà essere trattata, investigativamente parlando e senza alcuna seria e plausibile ragione, da questa Procura della Repubblica di Milano. Il disegno normativo avrebbe forse potuto avere una sua ragion d'essere solo ove finalizzato a migliorarne le attività di contrasto nei confronti di fenomeni di criminalità informatica riconducibili alle attività di gruppi organizzati strutturati in ambito associativo.”*

La pedopornografia

- ▶ Art. 12 (Fondo per il contrasto della pedopornografia su internet e per la protezione delle infrastrutture informatiche di interesse nazionale)
- ▶ 1. Per le esigenze connesse al funzionamento del Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di cui all'[articolo 14-bis della legge 3 agosto 1998, n. 269](#), e dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione per le esigenze relative alla protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, di cui all'[articolo 7-bis del decreto-legge 27 luglio 2005, n. 144](#), convertito, con modificazioni, dalla [legge 31 luglio 2005, n. 155](#), è istituito, nello stato di previsione del Ministero dell'interno, un fondo con una dotazione di 2 milioni di euro annui a decorrere dall'anno 2008.
- ▶ 2. Agli oneri derivanti dal presente articolo, pari a 2 milioni di euro annui a decorrere dall'anno 2008, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 2008-2010, nell'ambito del fondo speciale di parte corrente dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2008, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia.
- ▶ 3. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.



► CONCLUSIONI

Conclusioni in pillole

- ▶ L'intervento del legislatore, benché apprezzabile non è stato del tutto soddisfacente e convincente.
- ▶ In altri Stati si è paragonato l'impatto della *digital evidence* in ambito giudiziario pari all'uragano *Katrina*.
- ▶ È ormai cosa nota il fatto che le forze dell'ordine faticino a trovare fondi da destinare a specifiche attività di formazione, quando già le odierne attività d'indagine sono a rischio.
- ▶ Il legislatore, dal canto suo, ha dato un segnale: con la [legge n. 48/2008](#) si è cercato di andare incontro a quella parte della dottrina che da tempo sollecitava un intervento a causa dei fenomeni distorsivi che si registravano, segno inequivocabile della concretezza con cui si manifesta l'argomento.

Conclusioni in pillole

- ▶ Si è persa l'occasione per regolamentare fenomeni che di fatto e alla luce della legge a commento non trovano una loro collocazione né disciplina specifica: si pensi alla captazione di comunicazioni vocali tramite sistemi VoIP (es. *Skype*), all'acquisizione in tempo reale della posta elettronica, alle problematiche relative ai limiti del sequestro nei confronti dell'indagato o del terzo fino all'emergente fenomeno del *cloud computing*, nonché al peso e al ruolo assunto dai *social network* come *Facebook*, *Twitter* veri e propri focolari informativi da cui attingere elementi utili alle ricostruzioni processuali.

Le problematiche

L'impianto normativo della legge in realtà si è rivelato di insufficiente nell'attività di contrasto a reati che vengono segnalati in costante crescita.

Perché a dovere essere modificato è innanzitutto il Codice penale per adeguarsi a forme di reato in continuo cambiamento, per cui se appena ieri l'emergenza era costituita dalla donazione delle carte di credito, **oggi è il phishing e domani potrebbero essere le lottery scams (truffe legate alla falsa vincita di una lotteria online).**

Le problematiche

A testimoniare le difficoltà i dati forniti dalla polizia postale, il soggetto più spesso chiamato a intervenire sul versante delle truffe telematiche. **Negli ultimi 14 mesi, per quanto riguarda il phishing, a fronte di oltre duemila denunce è stato possibile effettuare solo quattro arresti.**

Le problematiche

- ▶ Lo scarso numero di arresti è frutto di un'evidente carenza del nostro Codice penale che permette di perseguire il phishing solo come sostituzione di identità, illecito sanzionato con la pena massima di un anno di reclusione, insufficiente a permettere l'esecuzione dell'arresto. A meno che non sia possibile contestare nello stesso tempo anche l'associazione a delinquere, elemento però non sempre facile da provare.

La mancanza di presa di coscienza

- ▶ Ciò dimostra come finora non vi sia una vera e propria presa di coscienza da parte delle istituzioni interessate circa l'impatto sociale e giuridico derivante dall'utilizzo dei nuovi media e delle tecnologie ad esse connesse: già a oggi, e sempre più nel futuro, nel divenire processuale le prove informatiche faranno sentire la loro voce, lasciando agli interpreti l'arduo compito di definire i contorni di una realtà giuridica tuttora troppo mutevole

The background of the slide features abstract, overlapping geometric shapes in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are primarily located on the right side and bottom of the frame, creating a modern, dynamic feel. A thin, light blue rectangular border is positioned around the central text area.

I reati informatici alla luce della legge 48/2008 Il furto di identità digitale

Sommario

- ▶ *Il Concetto di furto di identità;*
- ▶ *I vari tipi di autenticazione;*
- ▶ *Lo pseudonimo digitale*

Cos'è

Il furto di identità si concretizza nell'acquisire, spesso in modo fraudolento, "pezzi" di informazioni personali relative ad una persona (n° di carta di credito, n° di tessera sanitaria, patente di guida, etc) e nell'utilizzare tali informazioni per ottenere un vantaggio, spesso di tipo economico (ma non solo)

Statistiche (Experian e Gallup)

- ▶ Un americano su 5 dichiara di avere subito il furto di dati bancari (numero di conto corrente o di carta di credito), e uno su 7 di dati o documenti personali (certificati, patente, codice fiscale, dati previdenziali)
- ▶ Nel complesso il 26% degli americani afferma di aver subito almeno un furto di dati sensibili, 10 punti percentuali in più rispetto al 2005.

Statistiche (Experian e Gallup)

- ▶ In più del 10% dei casi, i furti di dati personali sono finalizzati ad atti criminosi e in parte anche ai furti di identità
- ▶ il 21% dei furti di dati personali è effettuato da conoscenti;
- ▶ più della metà degli americani (51%), comincia a temere di subire non solo furti di dati personali, ma anche furti di identità;
- ▶ il 70% degli americani non ha ancora adottato misure preventive contro i furti di dati personali e i furti di identità
- ▶ il 75% della popolazione crede che le truffe con la carta di credito e il furto d'identità siano la stessa cosa.

Il problema

- ▶ L'aumento dei furti d'identità è dovuto principalmente al fatto che nel mondo digitale le procedure di autenticazione sono meno sicure che nel mondo reale (si fa quello che si può ... e spesso anche meno)
- ▶ Autenticazioni deboli danno luogo ad autorizzazioni "potenti"
- ▶ Algoritmi di verifica "interni" (carte di credito fino al 2001)
- ▶ Nel mondo digitale vengono "trasferite" le procedure esplicite ma non quelle implicite o contestuali (sono nella mia banca?)
- ▶ Fiducia eccessiva nella tecnologia che dovrebbe "pensare a tutto" anche senza il nostro impegno personale

Le soluzioni

- ▶ **Il problema dell'autenticazione è interdisciplinare. Coinvolge aspetti**
- ▶ **Giuridici**
- ▶ **Sociali ed economici**
- ▶ **Tecnologici**

I vari tipi di autenticazione

Autenticazione di una persona da parte di un sistema IT

- ▶ Autenticazione di un sistema IT da parte di una persona
- ▶ Metodi per manipolare l'autenticazione

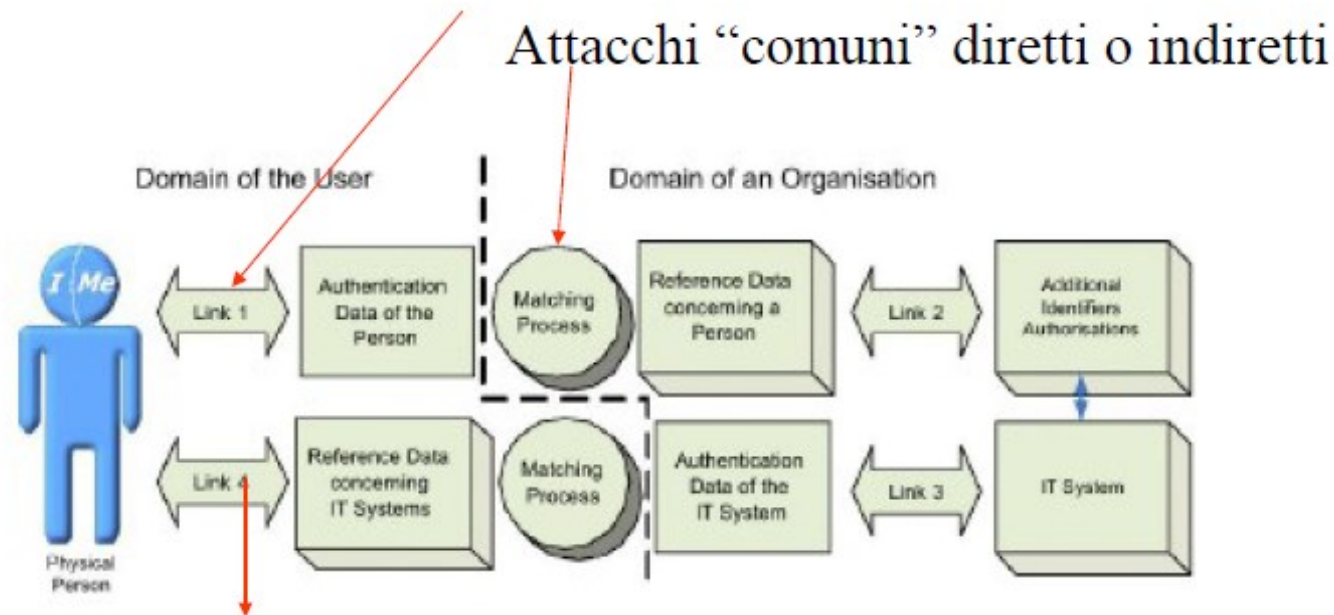
Autenticazione di una persona da parte di un sistema IT

- ▶ • La verifica è finalizzata a concedere accesso al sistema IT (è il tallone d'Achille della sicurezza informatica)
- ▶ Ciò che si ha (debole, economico, di facile sostituzione, è possibile "bloccare" l'accesso, può essere rubata e/o condivisa, "one shot" o continuativo nel tempo)
- ▶ Ciò che si conosce (stesse caratteristiche)
- ▶ Ciò che si è (forte?, costoso, non di facile sostituzione, è difficile "bloccare" l'accesso, non può essere rubata e/o condivisa?, solo "one shot")

Autenticazione di un sistema IT da parte di una persona

- ▶ L'autenticazione consiste nel verificare
- ▶ Cos'è il SI
- ▶ Cosa conosce
- ▶ Dove è collocato
- ▶ La fiducia che una persona ripone in un SI è altrettanto importante della fiducia che un SI concede a una persona

Metodi per manipolare l'autenticazione



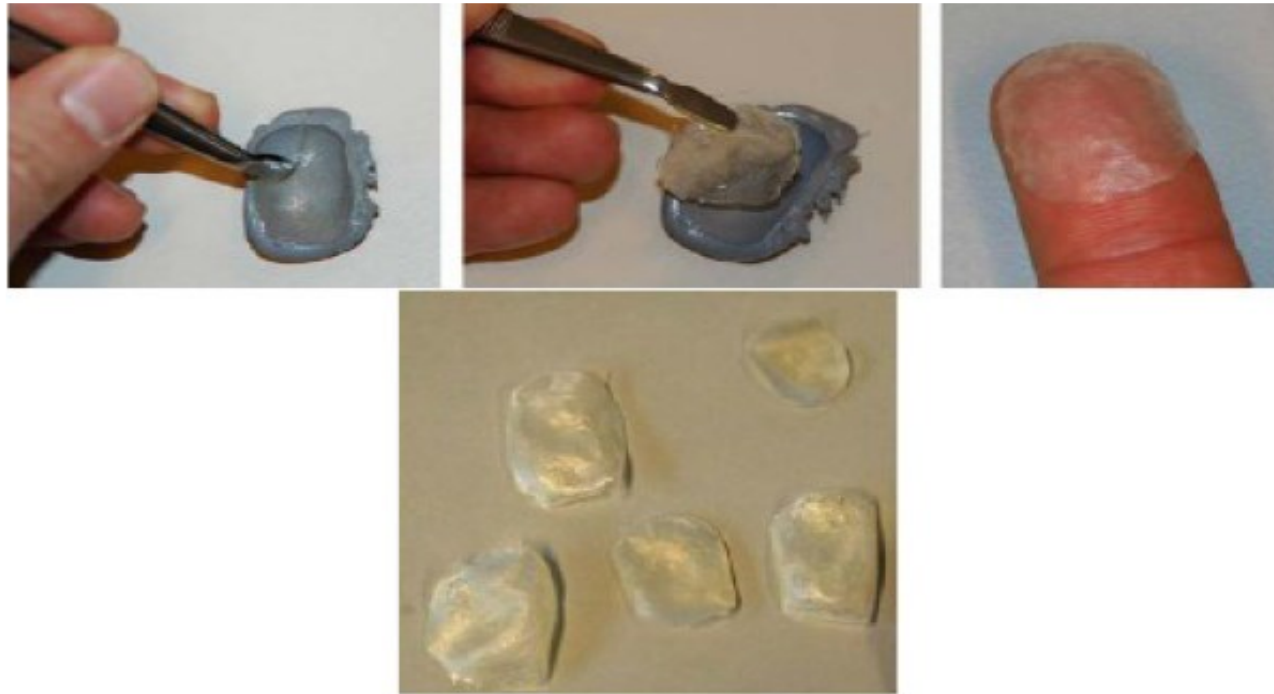
Attacchi diretti

- ▶ Worms (key logger). Attacco non selettivo 1:n Social engineering. Attacco selettivo 1:1 Cavalli di Troia/key loggers spediti via email
- ▶ (1:n)
- ▶ Spoofing dei sensori biometrici senza la cooperazione del soggetto interessato (1:1)

Attacchi indiretti

- ▶ Rivelazione degli identificatori, delle autorizzazioni e dei dati di riferimento di una persona, ottenuti attaccando i database centralizzati (1:1 e 1:n)
- ▶ Manipolazione dei dati di riferimento di una persona
- ▶ Phishing
- ▶ Man in the middle (attacchi replay, DNS spoofing)
- ▶ Abuso delle credenziali con la cooperazione del soggetto "titolare"
- ▶ Creazione di una nuova identità (non reale)

Biometria più sicura ?



Linee Guida (sociali)

Diffondere la consapevolezza degli impatti sociali ed economici delle frodi basate sul furto di identità

Utilizzare dei controlli "feedback" per bilanciare il sistema di autenticazione-autorizzazione. Utilizzare nuove tecnologie senza aver propriamente analizzato gli aspetti di sicurezza e privacy aumenta la sfiducia degli utenti (ciclo di sfiducia)

Linee Guida (sociali)

- ▶ Il ciclo di sfiducia deve essere rallentato, per esempio:
- ▶ Usando schemi di autenticazione proporzionali al contesto
- ▶ Utilizzando metodi di autenticazione socialmente accettati e accettabili
- ▶ Migliorare la sicurezza dei processi di autenticazione sulla base di una analisi causa-effetto (passaporto "biometrico" contro il terrorismo???)
- ▶ Nel caso sia necessaria una elevata sicurezza, utilizzare più sistemi di autenticazione paralleli disaccoppiati tecnologicamente

Linee Guida (tecniche)

- ▶ Minimizzazione dei dati personali necessari ("biometria"). Dove possibile si deve usare l'anonimato
- ▶ Usare autenticazioni "attive", dove l'utente decide dove, quando e per quale proposito usare l'autenticazione
- ▶ Usare metodi socialmente e psicologicamente accettabili (pw lunghe, con cambi frequenti non sono accettate)
- ▶ Non usare dati di autenticazione "irrevocabili" Usare metodi di autenticazione senza verifica interna Non usare metodi difficilmente aggiornabili

Requisiti per autenticazione "sicura"

- ▶ Usare autenticazioni ad almeno due fattori, verificati da sistemi diversi
- ▶ Non usare sistemi di autenticazione centralizzati "multipurpose"
- ▶ Usare autenticazioni "one time"
- ▶ Usare autenticazioni "two ways", ogni parte autentica la controparte

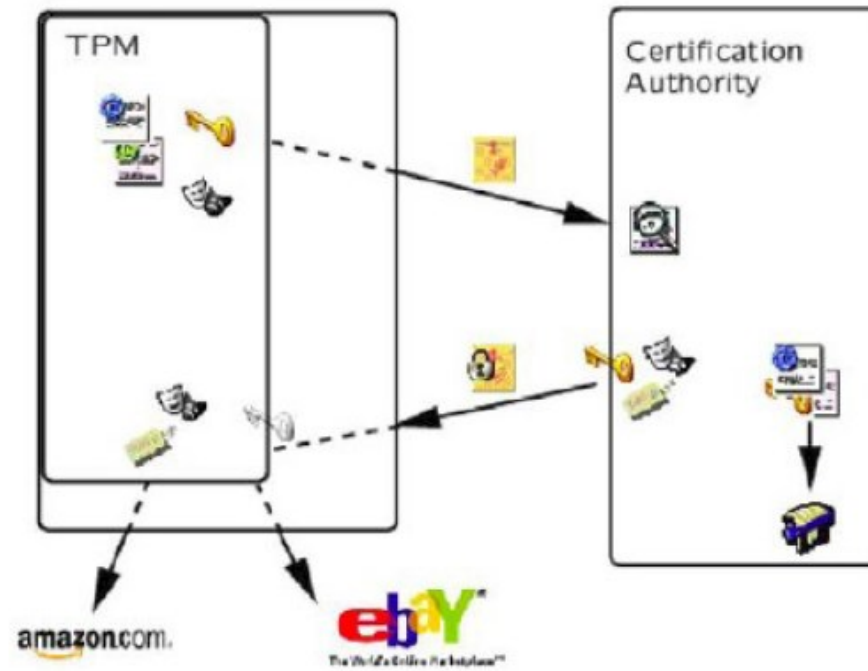
Soluzione "sicura" per la privacy online

La soluzione migliore per garantire la privacy online sembra essere quella di usare identità digitali parziali identificate da pseudonimi digitali

Pseudonimo digitale: caratteristiche (desiderabili)

- ▶ Deve essere unico (almeno con una elevata probabilità)
- ▶ Deve poter autenticare il possessore (chiave pubblica PKI, uso di PGP)
- ▶ Ogni soggetto deve avere un numero limitato di pseudonimi
- ▶ Gli pseudonimi non devono essere collegabili tra loro da parte di soggetti "non fidati"
- ▶ Trasferibilità (controllata) ad altri soggetti
- ▶ Trasferibilità di attributi da uno pseudonimo ad un altro
- ▶ Validità certa (tempo di "expire")
- ▶ Possibilità di blocco o revoca

Certificazione degli pseudonimi



The background of the slide features abstract, overlapping geometric shapes in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are primarily located on the right side and bottom of the frame, creating a modern, dynamic feel.

**I reati informatici introdotti dal Dlgs 196/2003
così come modificato dal Dlgs 101/2018**

Il sistema sanzionatorio

- ▶ **Il sistema sanzionatorio alla luce del nuovo Dlgs 101/2018 che ha modificato il codice sulla privacy (Dlgs 196/2003)**
- ▶ Il sistema sanzionatorio del Regolamento UE 679/2016 contempla sia sanzioni amministrative che penali stabilito ed è regolato dagli articoli 83 e 84 e distingue tre diverse sanzioni ai paragrafi 4,5 e 6 dell'articolo 83. Inoltre il Dlgs 101/2018 ha introdotto i seguenti illeciti penali prevedendo:
 - ▶ **Il trattamento illecito di dati personali;**
 - ▶ **L'acquisizione fraudolenta;**
 - ▶ **Le false dichiarazioni rese al Garante**

Il sistema sanzionatorio

- ▶ **Le sanzioni amministrative**
- ▶ La mancata adozione di tali misure di sicurezza informatica prevede la comminazione di sanzioni amministrative ed illeciti penali tra cui per quanto concerne le sanzioni amministrative ai sensi dell'articolo 42 del suddetto decreto sono le seguenti:
 - ▶ - Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, la violazione delle disposizioni di cui all'articolo 3, comma 1, lettere a), b), d), e) ed f), all'articolo 4, commi 2 e 3, all'articolo 6, commi 3 e 4, all'articolo 7, all'articolo 8, e' punita con la sanzione amministrativa del pagamento di una somma da 50.000 euro a 150.000 euro. La medesima sanzione amministrativa si applica al trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale in assenza della decisione di adeguatezza della Commissione europea, salvo quanto previsto dagli articoli 33 e 34.
 - ▶ - Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, è punita con la sanzione amministrativa del pagamento di una somma da 20.000 euro a 80.000 euro la violazione delle disposizioni di cui all'articolo 14, comma 2. Con la medesima sanzione e' punita la violazione delle disposizioni di cui all'articolo 17, comma 2, all'articolo 18, commi 1, 2, 3 e 4, all'articolo 19, all'articolo 20, all'articolo 21, all'articolo 22, all'articolo 23, all'articolo 24, commi 1 e 4, all'articolo 26, all'articolo 27, all'articolo 28, commi 1 e 4, all'articolo 29, comma 2.
 - ▶ Nella determinazione della sanzione amministrativa da applicare secondo quanto previsto dai commi 1 e 2 si tiene conto dei criteri di cui all'articolo 83, paragrafo 2, lettere a), b), c), d), e), f), g), h), i), k), del regolamento UE.

Il sistema sanzionatorio

- ▶ Le sanzioni penali
- ▶ Trattamento illecito di dati articolo 167 del Dlgs 196/2003
- ▶ 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
- ▶ 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
- ▶ 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

Il sistema sanzionatorio

- ▶ **Le sanzioni penali**
- ▶ **Trattamento illecito di dati articolo 167 del Dlgs 196/2003**
- ▶ 4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
- ▶ 5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
- ▶ 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

Il sistema sanzionatorio

- ▶ **Le sanzioni penali**
- ▶ **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala articolo 167 bis**
- ▶ 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.
- ▶ 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.
- ▶ 3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Il sistema sanzionatorio

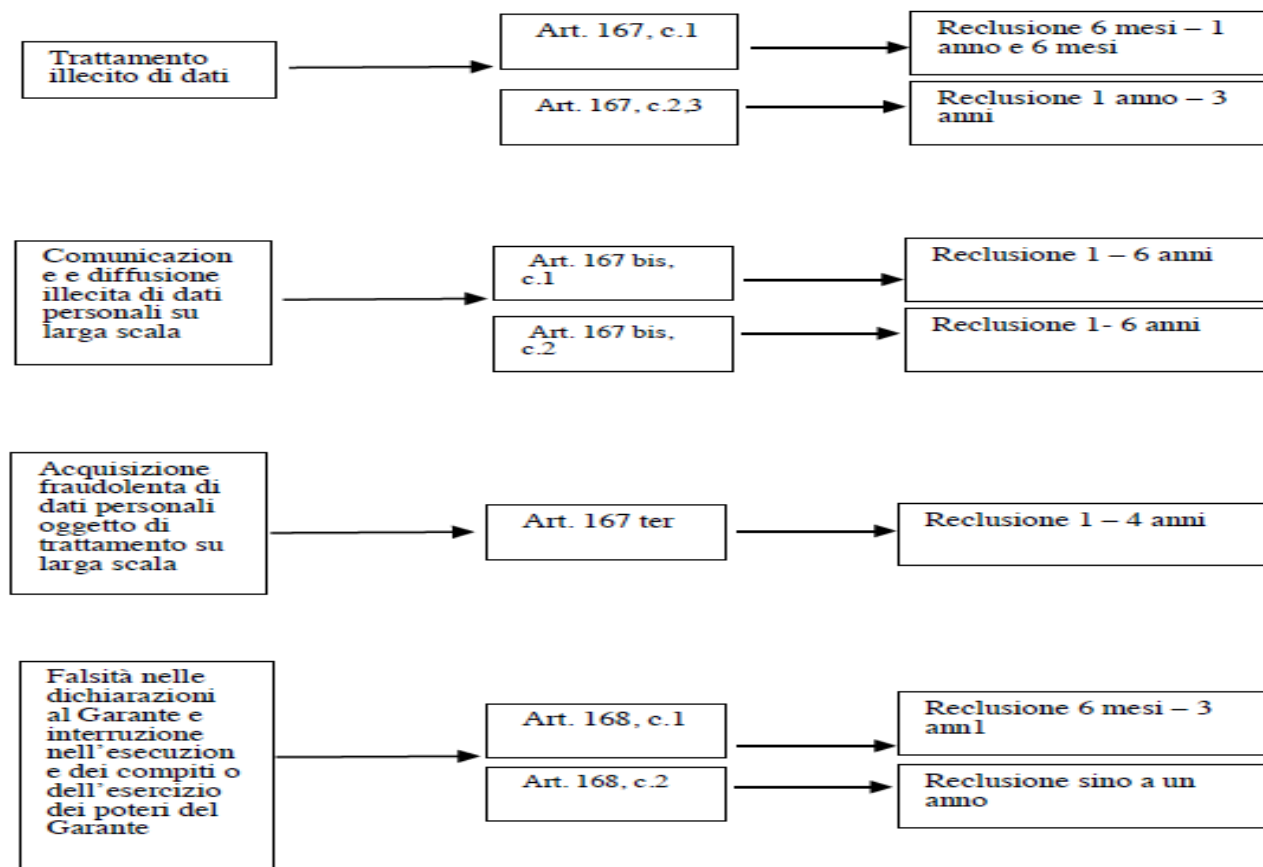
- ▶ **Le sanzioni penali**
- ▶ **Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala articolo 167 ter**
- ▶ 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.
- ▶ 2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.
- ▶ **Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti di esercizio dei poteri del Garante articolo 168**
- ▶ 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
- ▶ 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

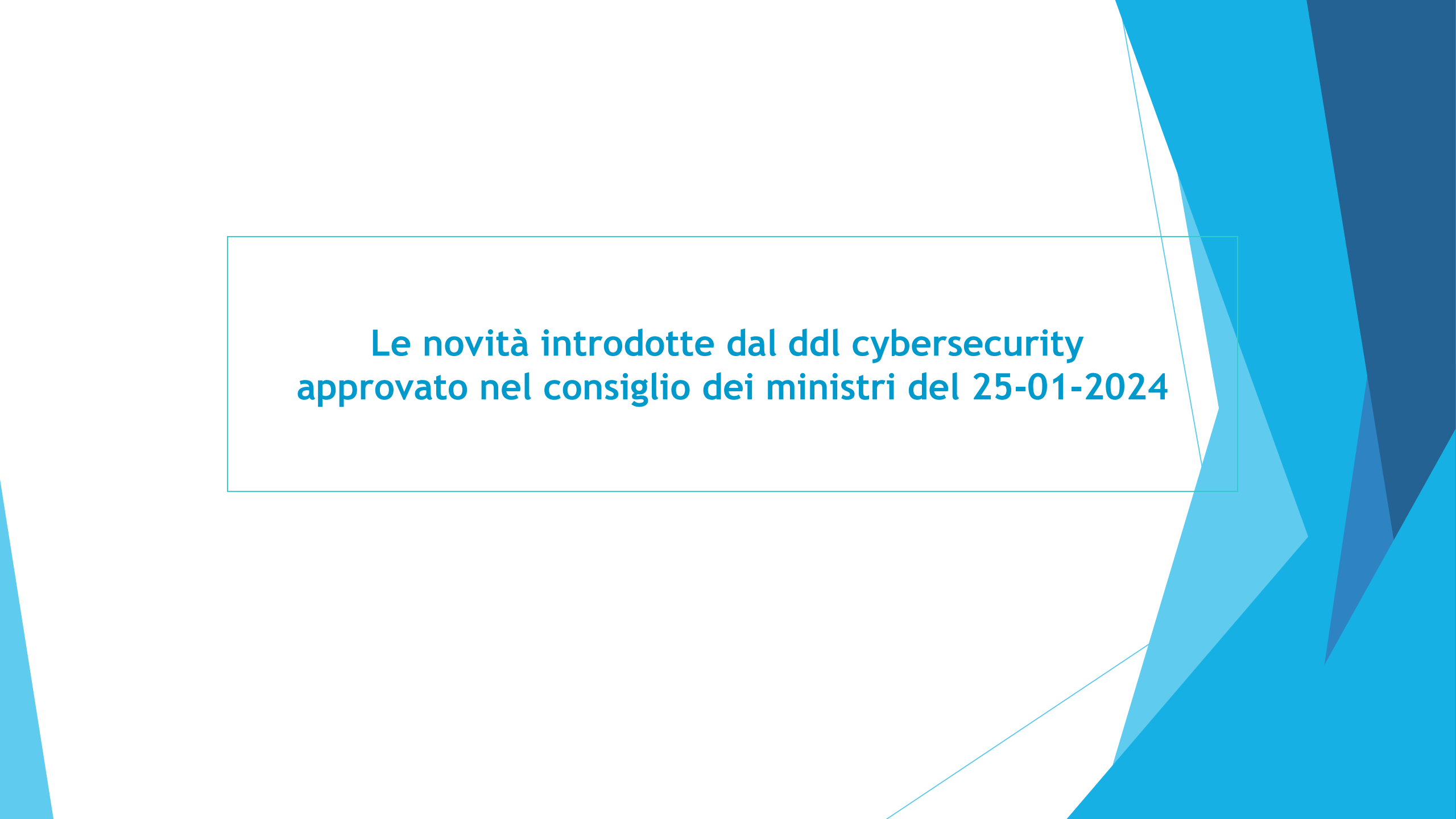
Il sistema sanzionatorio

- ▶ **Le sanzioni penali**
- ▶ **Inosservanza di provvedimenti del Garante articolo 170**
 - ▶ 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni.
- ▶ **Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori articolo 171**
 - ▶ 1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

Il sistema sanzionatorio

3. Diagramma sanzioni penali - D.Lgs. n. 101/2018



The background of the slide features abstract, overlapping geometric shapes in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are primarily located on the right side and bottom of the frame, creating a modern, dynamic feel. A thin, light blue rectangular border is positioned around the central text area.

**Le novità introdotte dal ddl cybersecurity
approvato nel consiglio dei ministri del 25-01-2024**

Inasprimento delle pene

- ▶ Le pene, dunque, si inaspriscono sia sul fronte reclusione per l'accesso abusivo ai sistemi informatici che introducendo maxi sanzioni pecuniarie anche per chi detiene o fornisce programmi in grado di danneggiare sistemi informatici. Inoltre lo scopo principale del ddl è stato quello di proporre, al passo con i tempi, un adeguamento ad una normativa non più attuale, e un'indicazione della direzione in cui si sta muovendo il governo, che può rappresentare un anticipo dell'impatto certamente più ampio che dovrà avere il recepimento della Direttiva NIS2. L'estensione del periodo detentivo vuole essere in deterrente importante e correttamente inasprisce le pene per coloro che attaccano sistemi informatici o telematici di interesse militare o di settori ritenuti critici.
- ▶ Lo schema del ddl applica anche un inasprimento sanzionatorio per alcuni reati già esistenti, tra cui:
- ▶ **accesso abusivo ai sistemi informatici (art. 615 ter c.p.)** e punito con il carcere da 1 a 5 anni, ora viene raddoppiato con la pena da 2 a 10 anni;
- ▶ **accesso abusivo a sistemi informatici di interesse militare, della P.A. e della sanità (art. 615 ter, co. 3, c.p.)**, viene innalzato da 3 a 10 anni e da 4 a 12 anni.
- ▶ **per chi detiene oppure fornisce programmi idonei a sabotare i sistemi informatici**, viene disposto il carcere fino a 2 anni e una sanzione pecuniaria oltre 10.000 euro.
- ▶ Il caso di reati contro “sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico”, le pene, rispettivamente, passano “da tre a dieci anni” e “da quattro a dodici anni”.

Inasprimento delle pene

- ▶ Il Ddl prevede norme di carattere penale che non sono solo l'innalzamento sanzionatorio ma anche la configurazione di **figure autonome di reato, come l'estorsione cibernetica**. Non ci sono solo modifiche di carattere penale sostanziale, ma anche di carattere procedurale in quanto questi reati rientrano nella disciplina dei reati di criminalità organizzata e quindi permettono non soltanto l'utilizzo di strumenti più efficaci di indagine e accertamento ma anche di quel coordinamento che passa dalla Direzione distrettuale antimafia e dalla Procura Nazionale Antimafia, perché sono reati senza territorio.