Metodologia di cybersecurity risk management 1/2

Gli standard di riferimento

ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA
Standard che fornisce una serie completa di principi e linee guida per aiutare le organizzazioni ad eseguire l'analisi e la valutazione dei rischi.

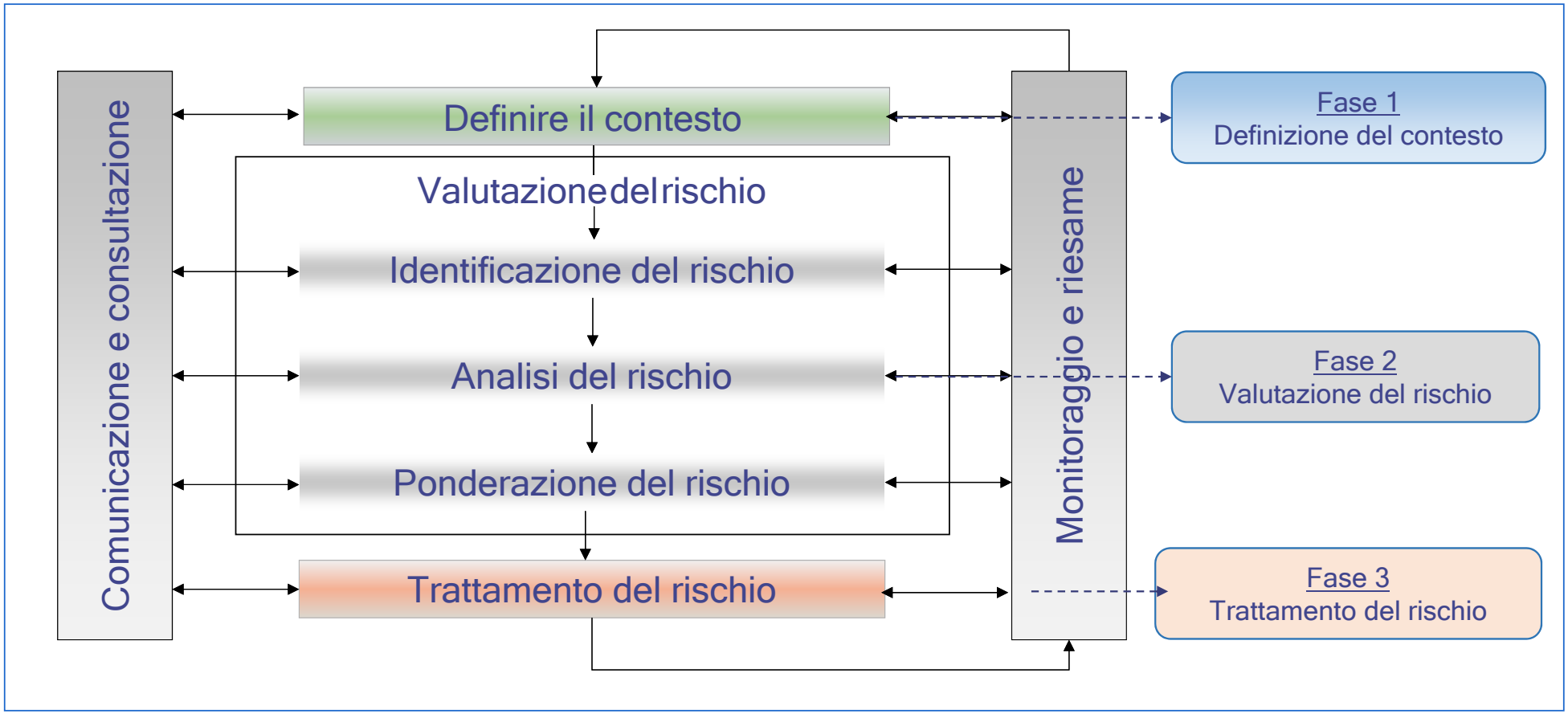
IRAM 2 (ISF): METODOLOGIA DI SECURITY RISK ASSESSMENT
Metodologia di valutazione dei rischi mediante analisi e valutazione di minacce, vulnerabilità e impatti

ISO 27001: SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
Standard utilizzato per arricchire il framework di controlli in ambito information security

NIST
Insieme di pubblicazioni utilizzate per arricchire il framework di controlli in ambito information security

MISURE MINIME DI SICUREZZA ICT PER LE PA
Misure per valutare e migliorare il livello di sicurezza informatica della PA, al fine di contrastare le minacce informatiche più frequenti

Metodologia di cybersecurity risk management 2/2



Metodologia di cybersecurity risk management 2/2

Gentile Cliente,

siamo stati recentemente informati che uno dei nostri fornitori di servizi clienti (subappaltatore) è stato vittima di un attacco informatico nel gennaio 2026, che ha comportato un download non autorizzato di dati personali associati al Suo account cliente.

Cosa è successo?
Le nostre indagini, così come quelle del nostro subappaltatore, hanno evidenziato che nel gennaio 2026 è stata effettuata un'estrazione illecita di dati tramite l'account di un agente del nostro subappaltatore.

Quali dati sono interessati?
Le informazioni interessate includono: cognome, nome, indirizzo email, numero di telefono ed eventuali scambi con il nostro servizio clienti.
La Sua password non è interessata. I Suoi dati risultano integri e non sono stati modificati.

Cosa abbiamo fatto?
Non appena l'incidente è stato individuato, abbiamo adottato immediatamente tutte le misure necessarie per proteggere i Suoi dati.
Le analisi condotte dai nostri team di sicurezza informatica hanno permesso di identificare rapidamente l'account compromesso, che è stato bloccato il giorno stesso della scoperta dell'incidente.
Successivamente, abbiamo revocato tutti gli accessi del nostro subappaltatore ai dati dei nostri clienti. Abbiamo inoltre implementato controlli rafforzati sull'accesso ai dati, sia all'interno della nostra azienda sia presso gli altri nostri subappaltatori.
Abbiamo infine informato la CNIL (Commissione Nazionale Informatica e Libertà francese), l'ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi francese) e la piattaforma Cyber Emergency Île-de-France.

Cosa Le consigliamo di fare?
I responsabili di questa violazione potrebbero utilizzare alcuni dei dati per tentare azioni

Metodologia di cybersecurity risk management 2/2

fraudolente nei Suoi confronti o nei confronti di terzi, contattandoLa via email o telefono (tentativi di phishing tramite email, SMS o telefonate) oppure impersonandoLa (furto d'identità su Internet).
La invitiamo pertanto a prestare la massima attenzione a possibili tentativi di frode e a seguire le seguenti raccomandazioni:

- **Verifichi sempre l'origine delle email ricevute** e accerti l'identità del mittente, controllandone in particolare l'indirizzo email;
- **Non apra email o allegati in caso di dubbio sulla loro origine** e non risponda a messaggi provenienti da mittenti sconosciuti;
- **In caso di incertezza, verifichi l'identità del mittente** tramite un canale alternativo (numero di telefono o indirizzo email diverso);
- **Non comunichi informazioni riservate** senza averne verificato l'origine e non condivida alcun dato (in particolare dati bancari, codici di accesso, password o identificativi) senza aver accertato la sicurezza del messaggio e l'identità del richiedente, indipendentemente dal canale utilizzato (email, telefono, SMS o social media);
- **Non clicchi su link sospetti** presenti nelle email e verifichi l'indirizzo del sito verso cui il link rimanda prima di accedere;
- **Verifichi sempre l'indirizzo del sito** prima di inserire o trasmettere informazioni riservate;
- **Si assicuri che il software antivirus sia attivo e aggiornato** sul Suo computer;
- **Monitori regolarmente i Suoi conti bancari** per verificare l'eventuale presenza di addebiti fraudolenti;
- In caso di operazioni sospette, contatti tempestivamente la Sua banca per contestarle.

Per maggiori dettagli e informazioni, puoi consultare il sito dell'ACN (Agenzia per la

Metodologia di cybersecurity risk management 2/2

Cybersicurezza Nazionale) su https://www.acn.gov.it e la pagina dedicata alla cybersecurity del Garante per la protezione dei dati personali su https://www.garanteprivacy.it/temi/cybersecurity, dove troverai i rischi legati al furto di identità e le misure per proteggerti.

Il nostro impegno

Ci rammarichiamo per questa violazione della riservatezza delle Sue informazioni e stiamo facendo tutto il possibile per porvi rimedio. La sicurezza e la fiducia dei nostri utenti restano la nostra priorità.

A tal proposito, abbiamo attivato una linea telefonica dedicata, disponibile al per rispondere a qualsiasi domanda relativa a questo incidente. Il Responsabile della Protezione dei Dati di resta inoltre a Sua disposizione per ulteriori informazioni al seguente indirizzo: _ _ _____

Macro-modello di calcolo del rischio 1/2

CARATTERISTICHE SERVIZI
A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità). Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo, sicurezza logica e fisica, etc…) e dunque determinare le Vulnerabilità.

BENCHMARK
Il benchmark consente di valutare il fattore di Esposizione alla singola minaccia.

IMPATTO
Consente di valutare gli impatti per ciascun servizio erogato in caso di perdita di Riservatezza (R), Integrità (I) e Disponibilità (D). A partire dagli impatti sui singoli servizi erogati, sarà poi calcolato l'impatto R,I,D sui servizi stessi.

Macro-modello di calcolo del rischio 2/2

- Censimento dei servizi oggetto di analisi del rischio.
- Identificazione delle caratteristiche primarie e secondarie di ciascun servizio.
- Calcolo del Profilo di Criticità associato ad ogni servizio.
- Calcolo del Profilo di criticità in funzione dei profili di criticità dei servizi.

RISULTATI

- Per ciascun servizio, valutazione dell'impatto in termini di Riservatezza (R), Integrità (I) e Disponibilità (D) delle informazioni trattate dai servizi per ciascuna categoria di impatto: Economico/Finanziario, Operativo, Reputazionale e Legale/Compliance.
- Valutazione dell'impatto R,I,D in funzione degli impatti sulle singole componenti R-I-D dei servizi.

RISULTATI

- Compilazione del questionario di Risk Assessment al fine di valutare il livello di vulnerabilità dei vari domini di sicurezza (accessi logici, sicurezza SW, gestione privacy, etc).
- Implementazione di un Risk Assessment report con indicazione delle componenti di rischio risultanti per ciascuna delle minacce e relative opzioni di trattamento.

REPORT

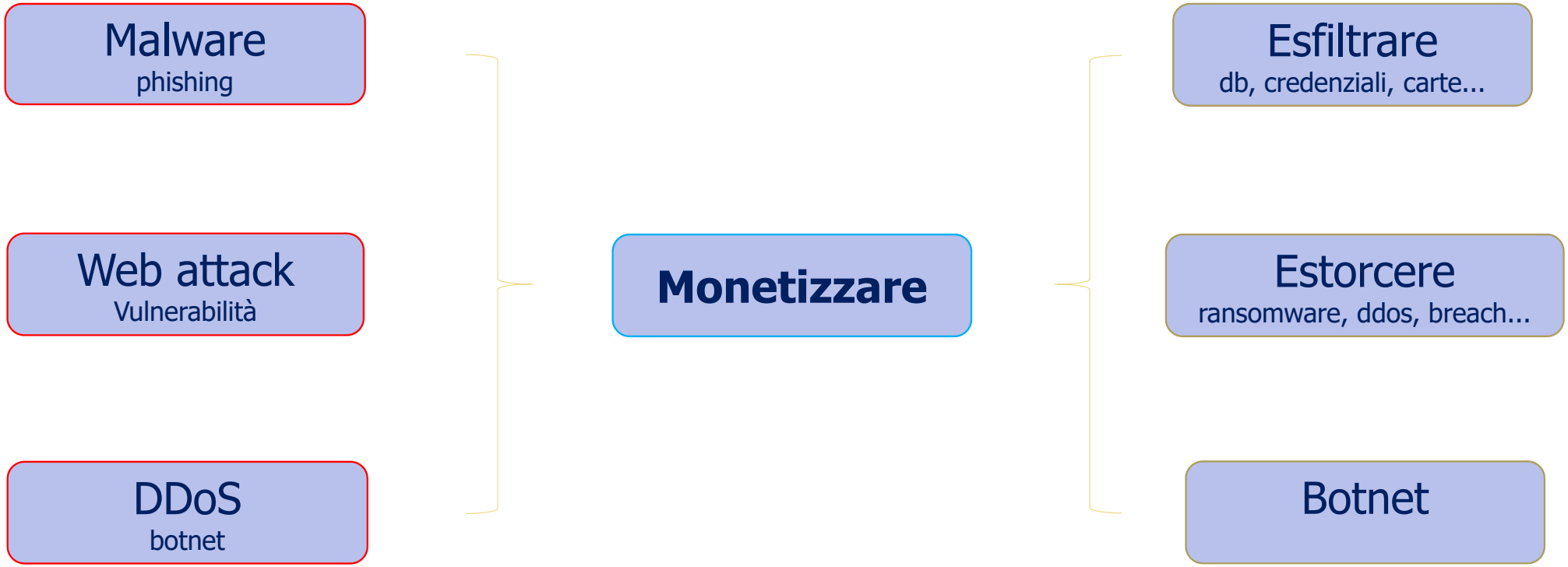
- Valutazione dei principali findings emersi dall'analisi del rischio.
- Definizione delle azioni di trattamento e mapping con le convenzioni attive.
- Implementazione di una matrice di prioritizzazione delle azioni di trattamento.
- Valutazione del Rischio Residuo.
- Definizione del Piano di Trattamento del Rischio

PIANO DI TRATTAMENTO

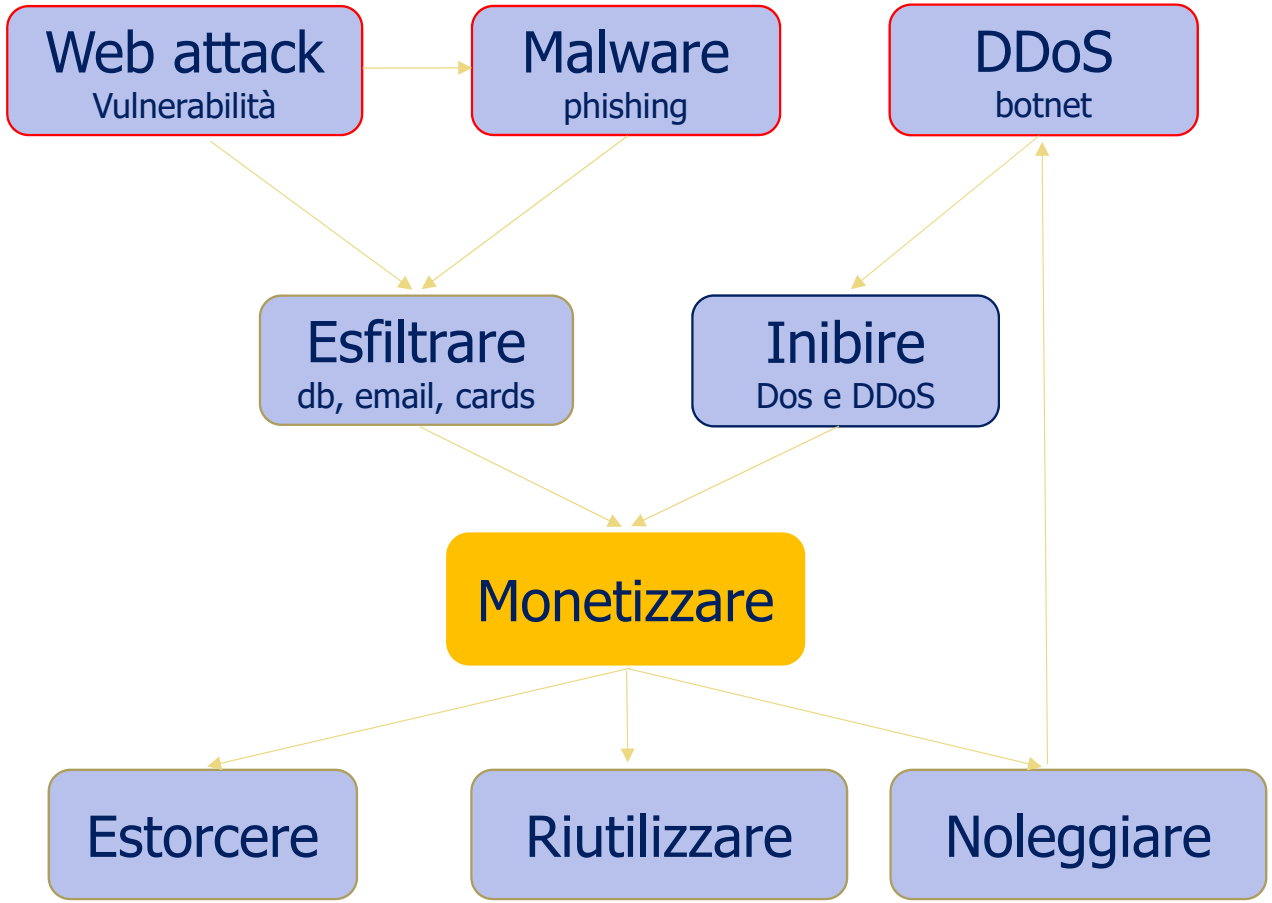
Gli attacchi informatici

Attività ostili nei confronti di una componente informatica, spesso compiute sfruttando le debolezze della componente umana.

Panorama delle **minacce** principali



Flusso della minaccia in dettaglio



Gli attori

Le vittime

- Scelte o casuali
- Sistemi informatici esposti e vulnerabili
- Personale non adeguatamente preparato
- Eventi di interesse nazionale

Gli attaccanti

- Criminali di strada, assoldati o in autonomia, singoli o in gruppo
- Hacktivisti
- Terroristi
- Paesi (ostili?)

Vittime scelte o casuali?

Scelte

- Target mirato
- Selezione per brand e per categoria

Casuali

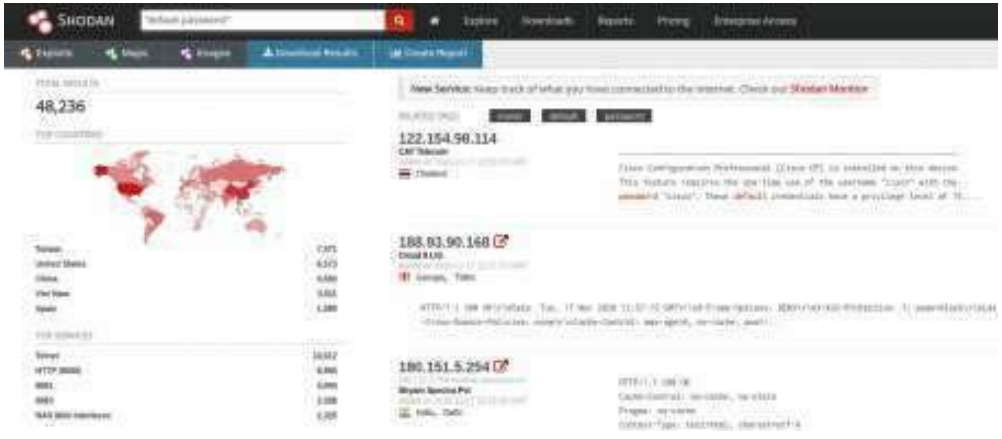
- Non esiste un target specifico
- Attacchi massivi

Vittime scelte o casuali?

	Opportunistico	Mirato
Selezione vittima	Casuale	Specifica
Automazione	Alta	Limitata
Preparazione	Minima	Approfondita
Obiettivo	Monetizzazione rapida	Informazione strategica / sabotaggio
Attori tipici	Cybercriminali	APT, stati, gruppi organizzati

Sistemi esposti e vulnerabili

Heartbleed

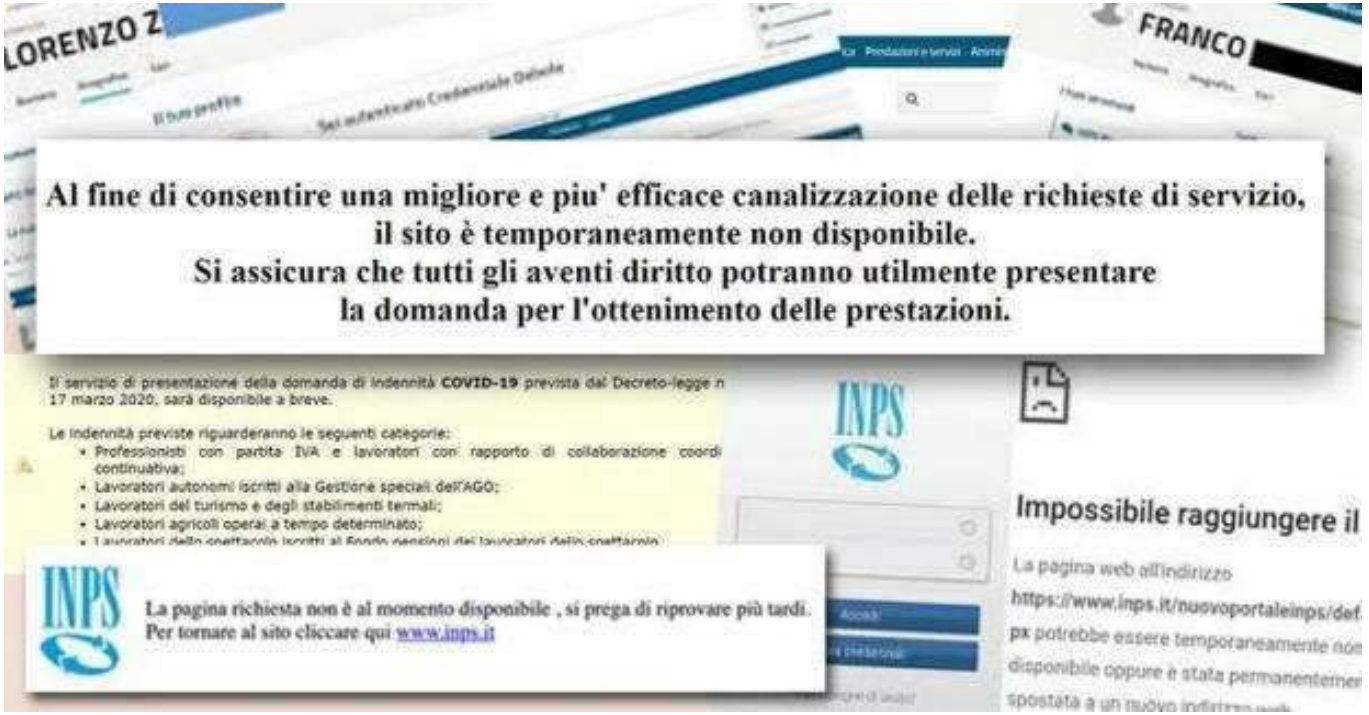


Default password

Sistemi esposti e vulnerabili

Heartbleed	Default password
Vulnerabilità di codice	Vulnerabilità di configurazione
Complessa da scoprire	Banale
Richiede patch	Richiede policy
Dipende dallo sviluppatore	Dipende dall'utente/amministratore

Eventi nazionali

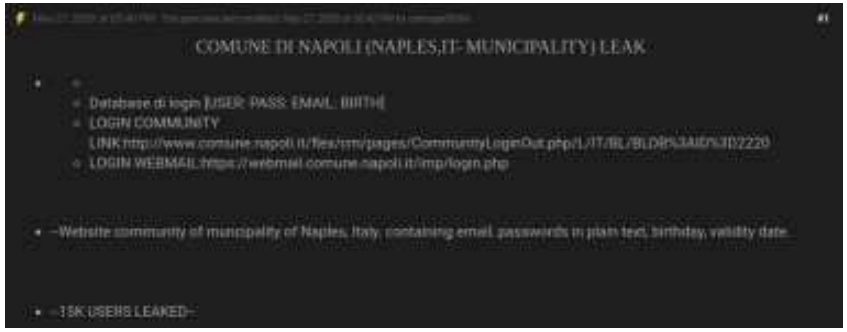


Data leak

- Sono sempre esistiti ma oggi è diventata una moda
- È nato un mercato di nicchia in forte crescita
- I blackmarket sono migrati dal darkweb al deepweb
- Prezzi sempre più accessibili

Quali dati in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito

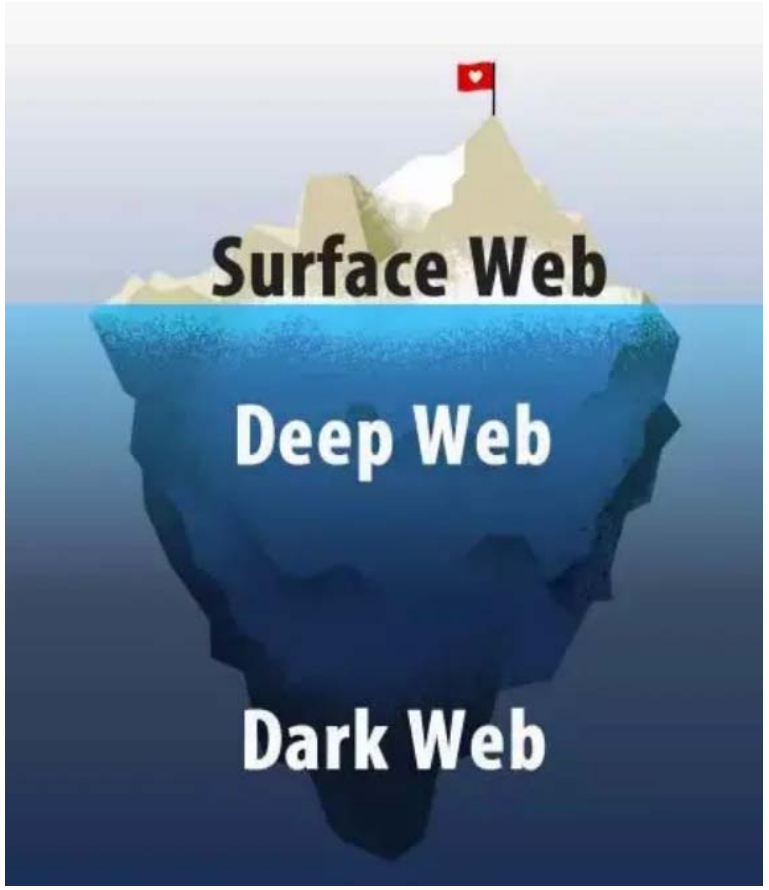


Data leak

- Sono sempre esistiti ma oggi è diventata una moda
- È nato un mercato di nicchia in forte crescita
- I blackmarket sono migrati dal darkweb al deepweb
- Prezzi sempre più accessibili

Quali dati in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito



Leak con pubblica minaccia di estorsione