IL SERVIZIO

CYBERSECURITY SERVICES

Formazione e Assessment

DESTINATARI

La cybersecurity è una priorità di tutte le Organizzazioni e le Imprese, in particolar modo per le Pubbliche Amministrazioni, i digital providers, le banche, le aziende del settore Sanitario e dei Trasporti.

IL CONTESTO

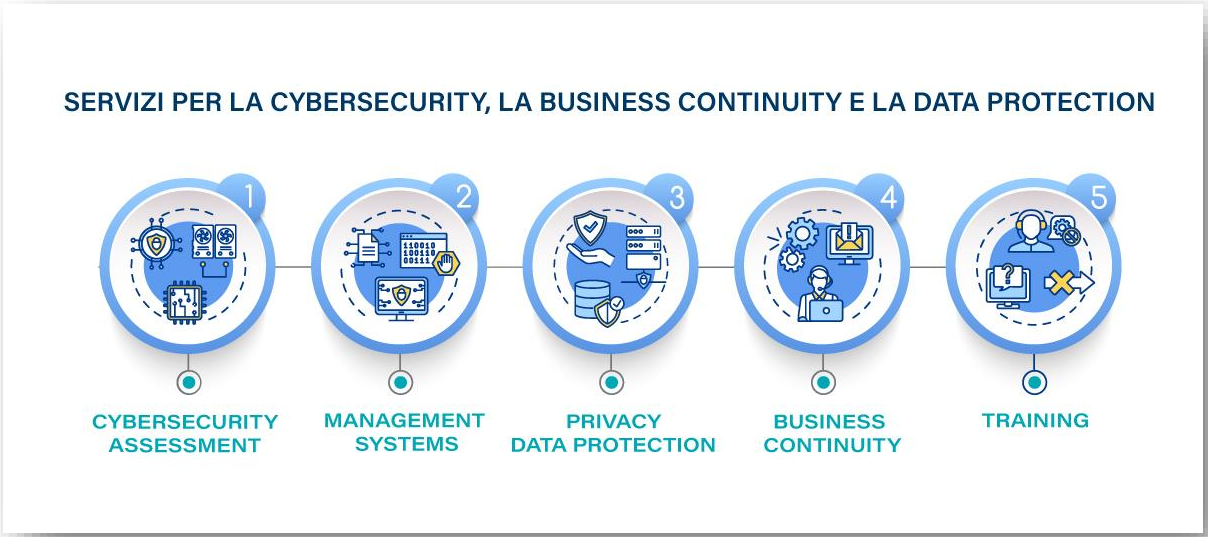
Accelerati dalla pandemia e dalla trasformazione digitale, nel mondo sono aumentati in maniera significativa gli attacchi informatici, causando impatti anche significativi, qualora si verifichi una interruzione dei servizi o una perdita di dati. L'analisi di impatto deve tenere in considerazione anche i danni dal punto di vista economico e reputazionale nonchè l'esposizione del patrimonio aziendale, sia in termini di *know how* e segreti industriali sia in termini di business continuity se i sistemi operativi venissero bloccati o danneggiati. Una cautela particolare è necessaria alle Organizzazioni che trattano **dati riservati o sensibili**. Qualora un data breach rientrasse nell'ambito del GDPR (Reg. UE 679/2016), determinerebbe un aggravio di rischio, viste le ingenti sanzioni previste in caso di mancato rispetto della normativa. L'attenzione a queste tematiche è cresciuta notevolmente negli ultimi anni, come confermato dalle iniziative sviluppate sia a livello Europeo (Cybersecurity Act, Direttiva NIS) sia Italiano (recepimento della direttiva NIS, Agenzia per la Cybersicurezza Nazionale, Piano Nazionale di Ripresa e Resilienza).

Le aziende devono dotarsi di Piani operativi da poter attivare nei casi di emergenza che riguardino non solo le infrastrutture, le reti, i dispositivi ma anche i processi, l'organizzazione, il personale, le comunicazioni, i fornitori, le parti esterne. **La complessità del tema** è tale per cui le Aziende devono necessariamente **integrare competenze multidisciplinari,** al fine di incrementare la propria resilienza.

Fonte: Enisa
Threat landscape 2022

I SERVIZI

Certiquality ha sviluppato nuovi servizi altamente qualificati in materia di Data Security, Data Protection e Cybersecurity anche grazie a nuove partnership con società specializzate in sicurezza informatica. Si tratta di servizi di Testing &Verification per individuare le vulnerabilità delle imprese e servizi di formazione per la crescita delle competenze e della consapevolezza dei rischi rivolti al personale aziendale.



CYBERSECURYTY ASSESSMENT

I servizi di assessment possono includere:

> Email security

- Verifica del livello di security compliance dei sistemi e-mail aziendali, ossia la loro conformità a standard, protocolli e best-practice di sicurezza
- Verifica della vulnerabilità dei sistemi email e verifica della conformità agli standard di sicurezza
- Verifica dell'adozione di pratiche **anti-phishing**

> Assessment rischi da fonti aperte

Questa verifica indaga, tramite l'utilizzo di sistemi **OSINT (Open Source Intelligence), indicatori di compromissione,** quali ad esempio utilizzo improprio del brand per attivazione campagne di phishing o credenziali dei dipendenti rubate. Si tratta di una verifica di primo livello della vulnerabilità dei sistemi public-facing, ovvero **esposti su Internet** (come siti e piattaforme web di vario tipo). Verrà condotta una verifica della presenza dell'azienda sul Deep Web e sui motori di ricerca, in maniera impropria / illegale, insieme al rilevamento di attacchi alla **reputazione di un brand.**

> Penetration Test

effettuare attività di penetration testing sui servizi public-facing fondamentali per l'operatività dell'azienda

> Reporting

I report di ispezione evidenzieranno il livello di maturità in termini di Cybersecurity delle imprese. I report contengono il dettaglio delle vulnerabilità riscontrate, l'identificazione di caratteristiche e impatti (scoring di severità) delle differenti vulnerabilità, le azioni di rimedio e controllo suggerite. Sono utilizzati standard di classificazione riconosciuti a livello internazionale.

PRINCIPALI OBIETTIVI:

- Rilevare i rischi di esposizione del brand aziendale ed eventuali data breach (**furto dati sensibili, informazioni business critical,** etc.)
- Identificare eventuali **account compromessi**, **informazioni** e **account** esposti sul Deep Web ossia **rubati**, che potrebbero essere utilizzati per accedere in maniera non autorizzata ai sistemi aziendali e creare danni all'operatività (**blocco sistemi, cancellazione dati, …**)
- **Prevenire** fenomeni di **Social Engineering**, quali il **Phishing** (ossia frodi basate sul tentativo di **furto di informazioni sensibili** degli utenti) e lo **Spoofing**, frode attraverso la quale più genericamente l'attore malevolo invia false comunicazioni
- Identificare azioni di **remediation / mitigazione** , dando strumenti di scelta delle priorità degli interventi da mettere in atto (scoring).

Management Systems

A fianco dei servizi specifici di Cybersecurity Assessment, riteniamo fondamentale **una efficace implementazione ed attuazione dei sistemi di gestione a fronte delle norme ISO**, ovvero i riferimenti internazionali più rilevanti in materia di quality management. Da un lato la **ISO 27001** (International Security Management Systems), insieme alle Linee Guida della famiglia ISO 27000. L'ISO/IEC 20000 è lo standard internazionale sviluppato specificatamente per la gestione dei servizi IT (IT Service Management).

Data and privacy protection

Grazie alla nuova norma **ISO/IEC 27701** è possibile certificare il processo di gestione delle informazioni personali, dei rischi per la privacy e la conformità alle norme vigenti.

Business Continuity

La norma ISO 22301 - Business Continuity Management- fornisce l'approccio sistemico e gli strumenti necessari per la gestione della continuità operativa, predisponendo un adeguato piano di prevenzione e di emergenza per affrontare le situazioni critiche.

Formazione

- Corso introduttivo Cybersecurity
- Percorso formativo - Cybersecurity Expert
- Corsi sulle norme ISO dedicate ai Sistemi di gestione

VANTAGGI

I servizi Certiquality per la Cybersecurity consentono di:

- Aumentare l'affidabilità aziendale e la continuità operativa;
- Incrementare la fiducia degli stakeholder per l'adozione di un sistema affidabile, efficiente e sicuro nella gestione, confidenzialità, disponibilità e tutela delle informazioni e dei dati nei processi aziendali.
- Migliorare la reputazione aziendale
- Migliorare la consapevolezza e la formazione del personale