DIVISIONE CYBER SECURITY

ATTRIBUZIONI PRINCIPALI:

La Divisione agisce nell'ambito del «Cyber Space» costituito da tutti i dati digitalizzati e da tutte le infrastrutture informative della comunità interna o "constituency" di LAZIOcrea costituita dalle strutture Aziendali e dalle strutture della Regione Lazio.

- definisce e ne cura l'aggiornamento e l'evoluzione nel tempo del piano strategico di Cyber Security aziendale che contiene riferimenti normativi, ruoli e responsabilità, risorse e asset, processi e attività operative relative alla Cyber Security;
- collabora, con le strutture preposte alla Sicurezza delle Informazioni, alla gestione del rischio e con il DPO Aziendale, nello svolgimento delle attività:
    - necessarie a proteggere da minacce la riservatezza, l'integrità e la disponibilità delle informazioni memorizzate nei sistemi informativi gestiti da LAZIOcrea, nel rispetto della corretta e necessaria fruibilità, definendo ed implementando le misure organizzative (definizione ruoli e responsabilità) più idonee;
    - di supervisione e controllo sull'impiego delle procedure e degli strumenti atti a garantire il rispetto delle normative sulla tutela dei dati;
- definisce e diffonde le policy e linee guida attinenti la Cyber Security, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale e della constituency, e con il contesto normativo e legislativo in materia di sicurezza informatica, riportando all'Azienda ed agli Stakeholder in merito allo stato di attuazione e copertura delle politiche, procedure, e degli standard aziendali relativi agli aspetti di Cyber Security;
- è responsabile della gestione del registro degli incidenti informatici e della risposta e ripristino degli incidenti critici di tipo cyber, abilitando e coordinando le comunicazioni interne (stakeholder ed altre strutture aziendali) ed esterne (ad es. con i CERT nazionali) per consentire il rapido ed efficace ripristino dell'operatività sulla base di regole e procedure definite da attivare in risposta all'attacco;
- è responsabile della progettazione e successiva gestione di una struttura centralizzata di Security Operation Center (SOC) che assiste le organizzazioni nel monitoraggio e nell'identificazione (raccolta, analisi e correlazione) degli eventi di cyber security nonché svolge attività di security alerts volta a notificare alle organizzazioni coinvolte, avvisi di sicurezza in modo tale che possano essere prese per tempo le dovute contromisure atte a mitigare o annullare gli impatti delle nuove vulnerabilità cyber.

La mission e gli obiettivi principali del SOC saranno:

- gestione dei sistemi e strumenti di monitoraggio (SIEM, EDR, ecc..);
- analisi delle minacce;

SEGUE

DIVISIONE CYBER SECURITY

  - verifica delle componenti infrastrutturali alla ricerca delle vulnerabilità;
  - emissione di bollettini di sicurezza e/o segnalazioni (IOC, early warning, ecc..);
  - gestione del servizio di threat intelligence.

- E' responsabile della progettazione di una struttura di Computer Emergency Response Team (CERT) dedicata alla gestione degli incidenti di sicurezza informatica, in grado di cooperare e coordinare gli interventi necessari per contenere il loro impatto e rispristinare le normali o accettabili condizioni operative nell'erogazione dei servizi. La mission del CERT sarà:
  - fornire supporto ed assistenza specialistica alla constituency nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
  - facilitare la risposta agli incidenti dichiarati attraverso il coordinamento delle risorse e la definizione di tempestive ed appropriate contromisure;
  - agevolare la notifica degli incidenti alle Autorità preposte;
  - incentivare la collaborazione e la cooperazione con altre organizzazioni nazionali al fine di creare un legame volto a condividere (infosharing) le informazioni, i metodi e le esperienze in ambito di gestione degli incidenti;
  - ottimizzare la gestione operativa delle tecnologie a supporto dei servizi, nonché la manutenzione e i cambiamenti, dei componenti di sicurezza quali firewall, IPS/IDS e piattaforme di raccolta, aggregazione ed analisi dei dati (SIEM); nonché offre supporto specialistico nel recepire ed applicare i cambiamenti delle policy di sicurezza;
  - accrescere le competenze specialistiche in tema di cyber security nonché promuovere attività di sensibilizzazione (awareness) sulle medesime tematiche.
- Progetta e gestisce l'erogazione di servizi di prevenzione, formazione e sensibilizzazione per la propria comunità di riferimento sulle tematiche di cyber security.
- Progetta e gestisce l'esecuzione di test e verifiche di sicurezza anche mediante l'erogazione di servizi di Vulnerability Assessment e Penetration Test volti ad identificare e valutare i potenziali punti deboli di sistemi, applicativi e infrastrutture che ne potrebbero compromettere il livello di sicurezza.

SEGUE

DIVISIONE CYBER SECURITY

Chief Information Security Officer (CISO)

Tra le attività in carico alla Divisione vi è l'incarico di Responsabile della Sicurezza Informatica – Chief Information Security Officer (CISO), le cui funzioni principali sono:

- supporto all'applicazione, alla gestione ed al miglioramento dei processi di gestione del rischio informatico;
- definizione della politica della sicurezza dei sistemi informativi;
- supporto alla valutazione dei rischi connessi all'uso di specifici strumenti informatici;
- controllo e supervisione dell'infrastruttura tecnologica aziendale per gli aspetti relativi alla sicurezza delle informazioni da questa gestite;
- verifica che tutte le informazioni disponibili siano correttamente fruibili, rimanendo al contempo protette da qualsiasi tentativo di accesso non autorizzato;
- supporto alla definizione del processo di gestione del rischio aziendale per le componenti attinenti la sicurezza informatica;
- supporto all'integrazione dei processi, in particolare per i piani di Continuità Operativa e di Disaster Recovery, per quanto attinente la sicurezza informatica.