DIVISIONE CYBER SECURITY

ATTRIBUZIONI PRINCIPALI:

- 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 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;
- gestisce il CSIRT regionale che gestisce gli incidenti informatici, la risposta ed il ripristino degli incidenti critici di tipo cyber, abilitando e coordinando le comunicazioni interne (stakeholder ed altre strutture aziendali/regionali) 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;
- 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 al management aziendale ed agli Stakeholder in merito allo stato di attuazione e copertura delle politiche, delle procedure e degli standard aziendali relativi agli aspetti di Cyber Security;
- è responsabile della 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 e 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.
- è responsabile della gestione della struttura di Cyber Security Incident Response Team (CSIRT) 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 al fine di:

SEGUE

DIVISIONE CYBER SECURITY

  - supportare e prestare 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 in ambito cyber; nonché offrendo 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 Testing volti ad identificare e valutare i potenziali punti deboli di sistemi, applicativi e infrastrutture che ne potrebbero compromettere il livello di sicurezza.