L'OFFERTA REPLY PER LA BUSINESS SECURITY

Reply ha composto un'offerta integrata, coerente e completa per supportare i propri Clienti nella definizione delle strategie idonee e nell'implementazione delle soluzioni appropriate per una gestione efficace della Business Security & Data Protection. La nostra missione è di consentire alle aziende nostre Clienti di stabilire relazioni di Fiducia con i loro interlocutori ed abilitare lo svolgimento dei loro processi di business affrontando ogni aspetto del rischio associato ad un Sistema Informativo.

IL MODELLO DI EROGAZIONE

Grazie all'apporto di più di 200 addetti con oltre 200 certificazioni, altamente specializzati sulle principali tecnologie e soluzioni e attivi presso i principali organismi ed istituti internazionali, l'offerta di Reply nel campo della Sicurezza delle Informazioni si articola sui seguenti ambiti:

- **Servizi professionali** per la realizzazione di soluzioni e contromisure di ICT Security di tipo:
  - Infrastrutturale, con soluzioni di Sicurezza di Rete e Sistemi
  - Applicativo, con soluzioni di SOA e Web2.0 Security, Code Review, …
  - Gestione delle Identità Digitali, con soluzioni di Identity and Access Management
- **Servizi di Consulenza** nelle aree di:
  - Security Strategy & Compliance
  - Security Governance
  - Security Awareness e formazione
- **Servizi Gestiti di Sicurezza** (Managed Security Services) erogati dal nostro Security Operation Centre H24
- **Gestione di frodi informatiche** tramite controlli Antiphishing e di Transaction monitoring
- **Security Assessment** per la verifica dei livelli di sicurezza

Il modello di erogazione si esprime tramite l'integrazione e la sinergia di questi diversi aspetti della Sicurezza Informatica che sono tra loro strettamente correlati per essere in grado di affrontare globalmente i diversi temi che compongono la Business Security.

LA BUSINESS SECURITY

GLI ASPETTI DELLA BUSINESS SECURITY. Per realizzare un Programma di Sicurezza che copra tutti gli aspetti aziendali e sia focalizzato sugli aspetti di business occorre un approccio metodologico che consenta di partire dall'analisi della situazione esistente, dei requisiti normativi e degli obiettivi di sicurezza fino ad arrivare ad una strategia implementativa della soluzione. L'esigenza è dettata dal fatto che la Sicurezza delle Informazioni copre ambiti di natura tecnologica, stragetica, organizzativa, legale ed economica.

Spike Reply, società del Gruppo Reply focalizzata sulle tematiche di Sicurezza, realizza progetti di Business Security sfruttando una metodologia proprietaria in grado di adattarsi alle specifiche esigenze dell'azienda cliente e verificata con il best of breed delle soluzioni tecniche disponibili sul mercato.

SERVIZI PROFESSIONALI DI ICT SECURITY

LA PROGETTAZIONE: Questo tipo di attività è indispensabile per progettare, valutare e selezionare le migliori soluzioni nell'ambito delle proposte disponibili sul mercato, siano esse tecnologiche che architetturali. Queste proposte sono quindi confrontate con le reali esigenze di protezione del cliente, al fine di rendere più rapido il ritorno sull'investimento nel contesto relativo alla soluzione. La conoscenza approfondita maturata sul campo permette di padroneggiare architetture particolarmente complesse in ambiente multipiattaforma ed indirizzate a diverse aree di Information Security: Network Security, System Security, Application Security, Data Security, User Profile Security sia in ambienti ad alta criticità che ad alte prestazioni.

LA REALIZZAZIONE: La policy aziendale è priva di valore se le contromisure tecnologiche definite non vengono poi realizzate in modo attento e competente. Grazie alle caratteristiche di eccellenza tecnologica ampiamente riconosciute dal mercato, Reply ha nella progettazione e realizzazione di soluzioni ICT il punto di forza principale. Reply, grazie alle competenze distintive e alle forti sinergie all'interno del gruppo, è in grado di realizzare le diverse soluzioni di Sicurezza fornendo soluzioni chiavi in mano.

LE PRINCIPALI TEMATICHE: Le principali tematiche coperte in questo ambito sono:

- Network & System Security:
  - Sicurezza perimetrale e IDS/IPS
  - Hardening
  - Sistemi ad alta affidabilità
  - Log management e Audit (SIEM)

- Application Security:
  - Safe Coding
  - Code Review

  - Firma digitale / PKI
  - SOA Security
  - Web2.0 Security
  - Application e Web Firewall

- Data Security:
  - Content Filtering
  - Cifratura dati
  - Desktop security
  - Database security
  - Data Masking
  - DLP (Data Loss Prevention)

- User Profile Security: Analisi e Disegno delle soluzioni di Identity and Access Management a partire dal modello profilativo e dei processi sino all'implementazione dei servizi tecnologici a supporto quali:
  - Identity Management, Role Management, User Provisioning
  - Enterprise e Web Single Sign on, Strong Authentication
  - Federation

SERVIZI DI CONSULENZA

LA CONSULENZA: La capacità consulenziale di Reply si applica in tutti i progetti da noi condotti in quanto la migliore architettura di sicurezza rischia di essere inefficace se non accompagnata e gestita da persone che condividono gli stessi principi, le stesse procedure e che si comportano in modo coerente, complementando le tecnologie e le misure fisiche adottate nello sforzo di protezione delle informazioni critiche dell'azienda contro minacce interne ed esterne. Reply lavora a stretto contatto con l'azienda cliente ed il suo ambiente per definire i principi, le politiche generali e gli obiettivi di sicurezza, nonché l'organizzazione funzionale della sicurezza, individuando quali sono le figure organizzative coinvolte e dettagliando i relativi ruoli, responsabilità e procedure specifiche.

LE PRINCIPALI TEMATICHE: Le principali tematiche coperte in questo ambito sono:

- Security Strategy & Compliance**:**
  - Risk Analysis / Business Impact Analysis
  - Piano Integrato della Sicurezza (Security Blueprint, Security Roadmap)
  - Piani e Sistemi di Business Continuity & Disaster Recovery (BS25999)
  - Sistemi di Gestione della Sicurezza delle Informazioni (ISMS; ISO27001)
  - Impianto documentale (Politiche Generali e Procedure Operative di Sicurezza)
  - Adeguamento Privacy (D.Lgs 196/03): definizione del DPS e impianto normativo
  - Conformità a leggi, normative e best practices (SOX, L.231, ABI, Basilea II,

PCI-DS, ITIL ...)
- Definizione e implementazione Competence Centre e/o Security Operation Centre interni

- Security Governance:

  - Secure Application Building (SSDLC; supporto team di sviluppo SW; Code Review)
  - Cruscotto monitoraggio e indicatori di Sicurezza (Security KPI/KRI/KPO)
  - Vulnerability & Patch Management
  - Gestione Incidenti Informatici
  - Security Awareness e Formazione con corsi personalizzati sulle esigenze specifiche del cliente

SERVIZI GESTITI DI SICUREZZA

SECURITY OPERATION CENTER (SOC). Il Security Operation Center (SOC) di Communication Valley, consociata di Spike Reply, è una struttura fisica e logica, l'unica in Italia, specializzata nell'erogazione di servizi gestiti e professionali di sicurezza informatica, che lavora per una pluralità di organizzazioni e che come centro di competenza vanta più di cento certificazioni. Si tratta di una vera e propria "torre di controllo", presidiata H24hx365gg da un security team composto da analisti, sistemisti e tester, specializzati rispettivamente in attività di monitoraggio real time, gestione degli apparati di sicurezza e security assessment. Il SOC si avvale di una infrastruttura esclusiva (Enterprise Security Management), costituita da un insieme di applicazioni, per la gestione di eventi di sicurezza, il riconoscimento di pattern d'attacco, il mantenimento delle tecnologie ed il Knowledge and Asset Management. Il SOC interagisce e condivide con il cliente gli output dei servizi attraverso un portale web-based facile e ricco di contenuti. Dal SOC vengono erogati i principali servizi di sicurezza informatica che compongono la nostra offerta di Managed Security Services:

- **Security Information and Event Management**, per la progettazione e realizzazione di soluzioni di raccolta e correlazione di dati affidabili sull'utilizzo della rete e delle sue componenti, nonché di tutte le informazioni necessarie per ottimizzare le risorse, correggere le configurazioni e inibire comportamenti che possano compromettere l'efficienza del Sistema Informativo
- **Security Monitoring**, per le attività di controllo e di rilevazione delle anomalie nella rete.
- **Network and Security Device Management**, per la gestione operativa degli impianti di rete e della sicurezza.
- **Early Warning,** per la gestione tempestiva delle escalation al verificarsi degli eventi significativi.
- **Policy Compliance,** per conformare i sistemi IT al fattore di rischio scelto per rispettare regolamenti aziendali, standard e normative.
- **Security Policy,** per controllare periodicamente e minimizzare l'esposizione dei sistemi IT rispetto al loro grado di vulnerabilità.

GESTIONE FRODI INFORMATICHE

FRAUD MANAGEMENT. La frode è un inganno intenzionale perpetrato per i propri interessi, per ottenere quindi benefici non autorizzati (denaro, proprietà, ecc) e possono riferirsi ad ambiti giuridici, commerciali, fiscali, valutari, sportivi alimentari e bancari. Con il termine "frode online" ci si riferisce a qualsiasi tipo di frode svolto con l'utilizzo di strumenti informatici. La gran parte dei casi di frode può essere ricondotta per quanto riguarda i settori, creditizio, del commercio, assicurativo e sempre più anche per le telecomunicazioni, a casi di furto d'identità ed impersonificazione.

La nostra risposta alle frodi online è svolta su due fronti principali:

- Anti-phishing per ridurre al minimo il rischio di furto d'identità;
- Monitoraggio delle transazioni per bloccare attività fraudolente compiute con dati di identità ottenuti illecitamente.

ANTI-PHISHING. Il phishing è una tecnica di frode online che si avvale di vari metodi per ingannare l'utente e indurlo a fornire informazioni personali e sensibili (nome utente, password, numero di carta di credito ecc.). Le attività antiphishing sono realizzate con una serie di strumenti proprietari specializzati e nel supporto 24x7 degli specialisti del nostro SOC (Security Operations Center). La nostra soluzione include i seguenti benefici: analisi preventiva delle registrazioni di dominio, rilevazione degli incidenti di phishing H24, analisi di ogni incidente, risposta mirata al takedown della rete di phishing, dilution delle credenziali e inserimento di credenziali esca.

TRANSACTION MONITORING. Il monitoraggio delle transazioni è un potente strumento per:

- monitorare le attività online in maniera trasparente (sia in fase di login, sia di post-login);
- individuare le attività ad alto rischio, segnalare e raccomandare azioni appropriate;
- abilitare le istituzioni finanziarie ad investigare con efficacia le attività segnalate ad alto rischio;

Gli indicatori utilizzati dal sistema e che determinano il calcolo del livello di rischio durante una transazione riguardano:

- Profilo utente;
- Profilo IP;
- Profilo del dispositivo.

Raccogliendo un elevato numero di indicatori su ciascun tipo di profilo, il sistema determina un livello di rischio cui può essere associata un'azione.

SECURITY ASSESSMENT

L'ASSESSMENT: Una volta scelta e realizzata la migliore soluzione, è indispensabile esercitare un continuo controllo dell'esistente tramite sessioni di Assessment. La scoperta di nuove tecniche d'intrusione e di nuovi metodi di risposta per arginare gli attacchi, rendono la verifica periodica della sicurezza del sistema informativo una delle attività necessarie per il corretto mantenimento dei parametri di riservatezza, integrità, disponibilità, autenticità, non ripudio, privacy. Questa verifica viene condotta in modo diverso a seconda degli obiettivi che si intende perseguire: verifica esterna dei sistemi e/o delle applicazioni (EthicalHacking); verifica interna delle configurazioni; test passivo del sistema informativo, tramite verifica dei files di configurazione ed interviste con gli amministratori ed i progettisti; test di verifica delle procedure operative ed organizzative, dei manuali e della loro effettiva applicazione. Questo percorso porta in modo naturale alla gestione complessiva del mantenimento del livello di sicurezza raggiunto tramite l'erogazione di servizi di sicurezza gestita (Managed Security Services) da parte del nostro Security Operation Center (SOC).

LE PRINCIPALI TEMATICHE: Le principali tematiche coperte in questo ambito sono:

- ICT Security Assessment – Security Check-Up (verifica generale degli aspetti di sicurezza (LOFTA))
- Vulnerability Assessment (identificazione delle vulnerabilità di sicurezza informatica)
- Ethical Hacking / Penetration Test (identificazione e verifica pratica delle brecce informatiche)

All'interno del Gruppo Reply SpA, Spike Reply e Communication Valley sono le società specializzate sulle tematiche relative all'area della Sicurezza e della tutela dei Dati Personali. Reply ha definito un'offerta completa, integrata e coerente per affrontare ogni aspetto del rischio associato ad un sistema informativo: dall'individuazione delle minacce e delle vulnerabilità, alla definizione, progettazione e di implementazione delle relative contromisure tecnologiche, legali, organizzative, assicurative o di ritenzione del rischio. La consociata Communication Valley è un Managed Service Provider specializzato nella gestione della sicurezza di sistemi complessi. Le soluzioni offerte si applicano alle reti dati e voce, in tutte le loro modalità: wireless e wired, tradizionali e VoIP. Il portafoglio comprende attività di security assessment, gestione di apparati di sicurezza, monitoraggio in tempo reale. Communication Valley vanta un Security Operations Center in grado di fornire servizi in modalità H24x365 presidiato da specialisti di sicurezza.

La missione di Reply è di permettere ai propri clienti di effettuare il loro business in condizioni di Sicurezza, supportandoli nello sviluppo delle idonee strategie e nella implementazione delle appropriate soluzioni per una gestione efficace della Sicurezza delle Informazioni.

Spike Reply
www.reply.eu