Fraud Management

COMMUNICATION VALLEY
SECURITY SERVICE PROVIDER

Reply
spike

Contenuti

- Reply Security
  - SOC
    - Fraud Management

Consulting & Services

- Security Strategy
- Regulatory Compliance
- Risk Analysis & Management
- Check & Control
- Security Governance

System Integration

- Policy & Procedures
- Security Countermeasures

Managed Security Services

- Security Assessment & Early Warning
- Security Monitoring
- Device Management
- Incident Handling
- Fraud Management

Offerta Completa ed Integrata
sia in termini di copertura funzionale
che di modalità di erogazione

Communication Valley

Communication Valley è un Security Service Provider focalizzato nell'area ICT Security e specializzato nella gestione di ambienti complessi in cui è necessario garantire elevata sicurezza e alta disponibilità associati a forte flessibilità operativa.

Eroga:

- **Managed Security Services** attraverso il suo **Security Operations Centre (SOC) operativo H24**
- **Design, integration and deployment** di architetture e soluzioni di sicurezza ICT

H24 365 giorni all'anno

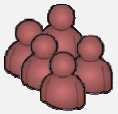
Security Operation Centre
Via Budellungo, 2
43100 – Parma

2.000 mq

Data Center

Ambiente fisico dedicato e dotato di facility ridondate (energia, CDZ, dorsali Internet). Sistema di sicurezza fisica e video sorveglianza a protezione del building

Control Room



Locale indipendente provvisto di controllo accessi, presidiato H24x365gg adibito alle normali attività del SOC

War Room

Locale indipendente provvisto di controllo accessi, adibito alle attività in situazione di "crisi" o ad attività "speciali " dedicate ad un singolo cliente eventualmente con la presenza di personale di suprto del cliente stesso

Presidi

SOC on site. Personale del SOC distaccato presso i clienti per attività "dedicate" e di coordinamento

Security Monitoring – Risorse / Organizzazione (1/2)

SOC = 50 + addetti (analisti, sistemisti, tester)

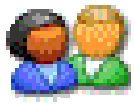
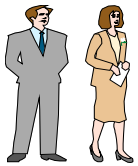
Oltre 100 certificazioni:

- **altamente specializzati sulle principali tecnologie e soluzioni**
- **attivi presso i principali organismi ed istituti internazionali**
- **centro di competenza all'interno di un team (CV + Spike Reply) di oltre 200 professionisti specializzati in ICT Security**

Vendor **Enti ed Organismi**

Security Monitoring - Risorse / Organizzazione (2/2)

Risorse

Analisti		Coinvolti nelle attività di Security Monitoring Real Time, Tuning, Reporting. (28 addetti: Junior, Expert, Senior)
Sistemisti		Coinvolti nelle attività sistemistiche di amministrazione delle piattaforme SIEM, IDS/IPS, Console Vendor Specific (Maintenance, Change, …)
Referente Tecnico		Punto di riferimento, verso il cliente e verso i team interni, sulle peculiarità tecniche del servizio verso il cliente.
Reperibili		Pool di analisti e sistemisti Senior a supporto degli analisti nel NBH, organizzati in base a matrici di competenza (ambiti – clienti – tecnologie)
Service Manager		Responsabile unico verso il cliente e verso i team interni, anche per più servizi, della gestione dei servizi erogati e relativa qualità / peculiarità organizzative.

Servizi SOC (1/2)

Security Monitoring

- Raccolta e centralizzazione dei log (multisito e multitecnologia). Analisi e Reporting
- Monitoraggio real-time degli eventi di sicurezza dell'asset
- Attivazione del processo di gestione degli incidenti verificati

System Monitoring

- Monitoraggio real-time della disponibilità di risorse, servizi di sistema e rete (Availability Monitoring)
- Misura delle prestazioni (System Performance)

Network & Security Device Management

- Manutenzione Ordinaria / Straordinaria
- Gestione dei Change
- Gestione dei Fault
- Manutenzione Evolutiva (Improvement)

Servizi SOC (2/2)

Security Assessment

- Ricercare le vulnerabilità nelle infrastrutture IT e nelle applicazioni
- Suggerire piani di intervento per le vulnerabilità critiche, a seconda delle priorità imposte dai criteri di analisi del rischio

Fraud Management

- Individuazione e reazione dei tentativi di frode ai danni di servizi on-line
- Gestione “Shutdown” dei siti usati per il Phishing o per Brand Abuse

Early warning
PolicyCompliance

- Ricerca continua su nuove minacce e vulnerabilità
- Verifica della conformità dei sistemi agli standard adottati
- Procedure di hardening per sistemi operativi e applicazioni
- Procedura per la manutenzione delle configurazioni dei sistemi e applicazioni

Attività del SOC: i principali indicatori di sintesi

Network & Security Device Management

Generic	194
Maintenance	332
Change	2.333
Fault	770

789 apparati gestiti

3.588 ticket gestiti

Security Testing

100	PenTest
6.110	VA Network
15	VA wireless

(sedi/buildings)

Security Monitoring

114 Miliardi di eventi raccolti

94 milioni allarmi generati

c.ca 2.068 ticket di sicurezza gestiti

Oltre 2.800 apparati monitorati

C.ca 200 incidenti di sicurezza gestiti al mese

I dati fanno riferimento al periodo compreso tra il 1 gennaio e il 30 settembre 2008

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 "frodi 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 impersonificazione.***

Impersonificazione = Furto di identità

FACTA Red Flag Rules

(Fair and Accurate Credit Transactions Act)

Negli Stati Uniti sono effettive dal 1’ novembre 2008 (con alcune deroghe al 1’ maggio 2009) le regole che chiedono l’implementazione di un programma esteso di prevenzione del furto d’identità.

- Il programma deve includere ragionevoli policy e procedure per **individuare, prevenire e mitigare il furto d’identità.**

- La regolamentazione è principalmente orientata alle istituzioni finanziarie, ma è estesa anche ad altri settori secondo la seguente definizione: ciascuna azienda che fornisce beni e servizi e non richiede il pagamento al momento della erogazione di quei beni e servizi è considerata un “creditor” e quindi rientra nella regolamentazione.

- Per esempio le aziende di telecomunicazioni rientrano in questa categoria.

EUROPOL

L'Europol creerà un sistema di allarme europeo al fine di combattere e prevenire i crimini perpetrati via Internet. [*News* - 02-12-2008]

- L'Unione Europea ha deciso di impegnarsi duramente nella lotta al cybercrimine, stanziando 300.000 euro per l'Europol (l'ufficio di polizia europeo).
- Questi soldi dovranno essere usati per la creazione di un sistema di allarme che permetta di segnalare e identificare con efficacia e tempestività i crimini perpetrati via **Internet**, come le frodi informatiche e i furti d'identità, in tutti i 27 Stati membri.
- L'Europol dovrà poi impegnarsi nello scovare ogni traccia di attività illegale, sorvegliando più a fondo i sospetti, in base a una strategia quinquennale che il Consiglio dei Ministri Europeo ha preparato e approvato nella scorsa settimana.
- Inoltre l'Unione vuole vedere più **collaborazione tra le aziende e le forze di polizia**: la condivisione delle informazioni può diventare un'arma potente per prevenire e reprimere il cybercrimine, e per questo obiettivo sono state previste delle normative apposite.
- Tutto ciò servirà a rendere più sicuro l'uso della Rete in Europa, ma perché funzioni serve che si attuino *"quella tanto necessaria cooperazione e lo scambio di informazioni tra gli stati Membri"*

Modello funzionale

	Fraud Prevention	Fraud Detection & Mgmt	Fraud Analysis & Investigation
Definizione	Prevenire qualsiasi possibilità d'attacco	Identificare e contrastare comportamenti fraudolenti	Analisi su frodi a buon fine o bloccate
Cosa fare	▪ Risk assessment ▪ Predisposizione delle difese tecnologiche	▪ Dotarsi di strumenti di monitoraggio delle transazioni soggette a frode ▪ Case management	▪ Raccolta ed analisi dei dati per individuare tecniche d'attacco e di conseguenza, predisposizione delle difese
Supporto CV	▪ Consulenza Risk assessment ▪ Anti-phishing ▪ Vulnerability Assessment / Hardening sistemi ▪ Security monitoring	▪ Assicurazione dell'identità utente ▪ Verifica delle identità ▪ Transaction monitoring di insider fraud e web fraud ▪ Detection su frodi di proprietà intellettuale	▪ Semantica ▪ Intelligence di individuazione tecniche d'attacco

COMMUNICATION VALLEY SECURITY SERVICE PROVIDER

Reply spike

- **Verifica delle identità**: persona sconosciuta che chiede miei servizi
- **Assicurazione dell'identità dell'utente**: accertarmi che chi accede ai miei servizi è effettivamente il "mio utente"
- **Monitoraggio delle transazioni**: controllo delle effettive operazioni svolte e segnalazione di transazioni sospette
- **Anti-phishing**: evitare che un mio utente distribuisca le proprie credenziali

Verifica delle identità (1/2)

Scenario

Qualcuno che vuole attivare servizi online presentandosi con una falsa identità al fine di ottenere i servizi ma essere non identificabile al momento del recupero del corrispettivo

Per esempio:

- Servizi di telecomunicazioni
- Emissione Carte credito e Carte di servizio

Come difendersi

Adozione di soluzioni di sicurezza che assicurino l'identità dell'utente in real time ed aiutino a prevenire il rischio di furto d'identità e di frode.

Ciò si ottiene utilizzando un'autenticazione Knowledge-based.

In tal modo la verifica dell'identità avviene tramite una serie di domande utilizzando elementi rilevanti ottenuti con l'accesso a database di record pubblici.

Vi sono inoltre moduli che permettono una migliore accuratezza nell'autenticazione dell'utente. Ciò avviene misurando il livello di rischio associato con un'identità e permettendo al sistema di configurarsi modificando la difficoltà delle domande durante il processo di autenticazione.

Verifica delle identità (2/2)

Controlli principali

- **Data Integrity Check** : analisi della validità sintattica e semantica dei dati quali codice fiscale, carta di credito.
- **Subscription prevention tools**: controlli sulle Grey List interne (ed eventualmente controlli esterni su basi dati come Agenzia delle Entrate per il CF).
- **Alias matching**: rilevazione di pattern di informazioni simili, utile principalmente per ricondurre nuovi profili a quelli già conosciuti e ritenuti pericolosi.
- **Customer comprehension**: raccolta del maggior numero di informazioni del cliente sul web.
- **Ricerche tra record pubblici**.
- **Identity velocity**: alto volume di attività associato ad un individuo su differenti business.
- **IP velocity**: richieste di autenticazione multipla generati dallo stesso IP.

Assicurazione dell’identità dell’utente

Scenario

Persone che utilizzano in maniera fraudolenta le credenziali di un utente reale per ottenere servizi.

Come difendersi

Monitoraggio dell’accesso ai servizi valutando il maggior numero di parametri e definendo un livello di rischio legato alla connessione.

Con tale soluzione si ottiene un alto livello di protezione monitorando ed autenticando l’attività dell’utente, basandosi su livelli di rischio, policy istituzionali, segmentazione dell’utente. Con questi strumenti è possibile tracciare oltre 100 indicatori per individuare potenziali frodi.

Esempi di indicatori:

- Identificazione del device (versione browser, SO, ecc);

- IP geolocation;

- Profili di comportamento.

A ciascuna attività è associato un punteggio di rischio. Quando un’attività è considerata essere superiore al livello di rischio accettabile, si procede con ulteriori elementi di autenticazione.

Transaction monitoring

Monitoraggio estremamente potente nell'individuazione di attività fraudolente

- Individuazione di attività ad alto rischio, segnalazione e raccomandazione di azioni appropriate
- Monitoraggio trasparente delle attività online

Due scenari possibili:

1. **Monitoraggio delle transazioni finanziarie**
2. **Correlazione eventi**

Sorgenti di rischio:

Interne

Risorse interne all'azienda che sfruttano le proprie permission per effettuare atti illeciti

Esterne

Soggetti esterni che

- *accedono agli account dei clienti effettuando operazioni fraudolente*
- *utilizzano servizi erogati dall'azienda in maniera fraudolenta*

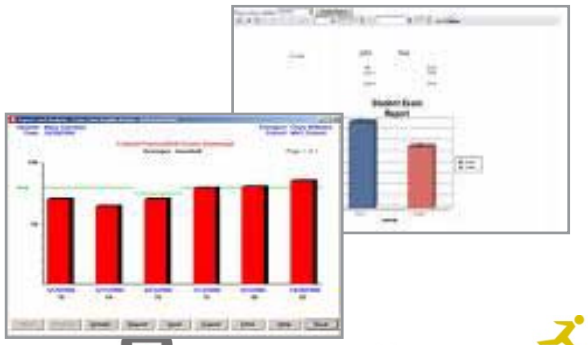
Transaction Monitoring per transazioni finanziarie

I sistemi di Transaction Monitoring valutano ogni attività online (login, impostazione di nuovi beneficiari, trasferimenti di denaro, ecc) in tempo reale, tracciando su centinaia di indicatori per individuare le frodi.

Gli indicatori monitorati includono sia indicatori di frode predefiniti, sia indicatori multidimensionali legati ai profili che facilitano l'anomaly detection.

Per esempio:

- **Internet data profiling**: IP address, ISP, geo-location, connection type, etc.
- **Device data profiling**: Browser version and configuration, optional device ID, operating system, etc.
- **User behavioral profiling**: Transaction amounts, time, type, velocity, etc.



COMMUNICATION VALLEY
SECURITY SERVICE PROVIDER

Reply
spike

Transaction monitoring – Correlazione eventi

- Possibilità di monitorare attività tramite correlazione di informazioni ed eventi provenienti da sorgenti distinte

- Attraverso motori di correlazione che accedono ad eventi provenienti da diverse sorgenti, anche database, e sono in grado di individuare e segnalare in **tempo reale** situazioni anomale secondo **business rules** definite.

- Per esempio: correlazione di registrazioni dati di traffico con log applicativi.

Transaction monitoring – Correlazione eventi

Altre caratteristiche

- Correlazione degli eventi raccolti in un ampio arco temporal
- Severity degli eventi calcolata dinamicamente sulla base di:
  - importanza dell'asset
  - vulnerabilità riscontrate sull'asset
  - frequenza dell'evento
- Il dato viene collezionato e mantenuto inalterato in modalità nativa
- Il dato viene cifrato rendendolo fruibile e leggibile soltanto attraverso l'utilizzo e l'accesso al sistema di correlazione
- L'accesso ai dati viene gestito attraverso adeguate policy di sicurezza differenziando gli accessi per utente e gruppo sia dal punto di vista applicativo che sistemistico
- L'attività di monitoraggio può essere svolta sotto forma di servizio remoto mantenendo i dati all'interno dell'azienda.

Il phishing è una frode on-line ideata per sottrarre con l'inganno numeri di carte di credito, password, informazioni personali e sensibili.

Attuato mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici

- **Lotta al phishing: la rilevazione delle esche inviate agli utenti e il blocco tempestivo dei siti utilizzati per raccogliere informazioni personali.**

Cosa deve essere fatto

1. Raccolta eventi
2. Analisi incidenti
3. Risposta e shutdown
4. Analisi forense
5. Report

Come

- Strumenti sempre aggiornati rispetto alle tecniche correnti
- Risorse competenti nell'analisi degli incidenti e disponibili H24
- Processi flessibili per adattarsi alle specifiche esigenze del cliente e per rispondere ad ogni incidente nella maniera appropriata

Contatti

www.reply.eu
info@reply.it