



CLUSIS

Association suisse de la sécurité des systèmes d'information
Schweizerischer Verband der Sicherheit von Informationssystemen
Associazione svizzera della sicurezza dei sistemi d'informazione
Swiss Association for the Security of Information Services

La sicurezza delle Tecnologie Informatiche e della Comunicazione in banca

Silvano Marioni, CISSP

Centro di Studi Bancari 

Lugano, 7 aprile 2004



Cosa è la sicurezza TIC

- La sicurezza TIC è la protezione dei dati, dei servizi e dei sistemi informativi da disastri, attacchi, errori e manipolazioni in modo che l'eventualità e/o l'impatto di un incidente sia ridotto al minimo.

- La sicurezza ITC si preoccupa della protezione delle risorse e servizi che utilizzano sistemi basati su TIC, ma non riguarda solo i rischi tecnologici
- La sicurezza TIC deve essere integrata nell'ottica più ampia della sicurezza aziendale e deve essere presente in modo trasversale in tutti i processi della banca

- Cifratura, password, VPN, classificazione dei dati, Single Sign-on, HTTPS, gestione del rischio, RACF, warm site, S/MIME, backup, firma digitale, RADIUS, penetration test, El Gamal, CERT, hardening, IPSec, COBIT, firewalls, LDAP, antivirus, DMZ, fault tolerance, SLA, business continuity, CCTV, smart cards, algoritmi a chiave pubblica, SSH, PKI, security policy, PGP, controllo accessi, DES, cold site, Kerberos, biometrics, SAN, eliminazione sicura, PIN, intrusion detection, proxy, CRL, separazione dei compiti, SSL, audit trail, MD5, honey pot, SET, ACF2, autorità di certificazione, RBAC, antispamming, BS7799, RAID, identity management, UPS, computer forensic, Rijndael, NAT, recovery plan, SOCKS, mirroring, TEMPEST, disaster recovery, Access Control List, certificati digitali, AES, Common Criteria, etica, Snort, IDEA, Digital Right Management, WEP

Caratteristiche di un sistema TIC sicuro

- Essere utilizzabile
- Proteggere le informazioni
- Comprovare le attività svolte
- Fornire il servizio atteso

L'importanza del fattore umano

- Attori esterni
 - Utenti sconosciuti (clienti potenziali)
 - Clienti conosciuti
 - Fornitori e Partners
- Attori interni
 - Dipendenti
 - Informatici e esperti di sicurezza TIC
 - Direzione generale e direzione TIC

- Utenti sconosciuti (clienti potenziali)
 - Nessuna possibilità di controllo
- Clienti conosciuti
 - Adeguamento ad alcune politiche di sicurezza della banca
- Fornitori e Partners
 - Adeguamento alle politiche di sicurezza della banca

- Dipendenti
 - Adeguamento alle politiche di sicurezza della banca
 - Decisioni limitate sulla sicurezza operativa
- Informatici e esperti di sicurezza TIC
 - Adeguamento alle decisioni strategiche sulla sicurezza
 - Definizione delle politiche di sicurezza
 - Decisioni progettuali sulla sicurezza dei sistemi, delle applicazioni e dei processi
- Direzione generale e direzione TIC
 - Decisioni strategiche sulla sicurezza della banca

- E' il processo di analisi delle esposizioni ai rischi e di implementazione delle soluzioni che riducono o eliminano queste esposizioni

- Valutare errori o inadeguatezze che potrebbero creare dei danni
 - Gestione del rischio per le risorse umane
 - Gestione del rischio per i sistemi TIC
 - Gestione del rischio per gli eventi esterni
- Necessità di revisione continua del processo di gestione del rischio
 - Le nuove esigenze di business
 - Le innovazioni tecnologiche
 - Le nuove esigenze legali

Progetto della sicurezza: un problema per specialisti

- Analisi dei requisiti
- Progetto della soluzione
- Implementazione
- Gestione e monitoraggio



La sicurezza non è solo un problema per specialisti

- La cultura della sicurezza deve essere diffusa in tutta la banca
- La sicurezza non deve essere un problema di un particolare settore della banca, ma di tutta la banca
- La condivisione della cultura della sicurezza tra persone con attività professionali e competenze diverse, garantisce una maggiore protezione delle risorse della banca
- Diventano quindi importanti sia l'informazione sia la formazione

L'importanza dell'informazione

- Informare sugli obblighi e le responsabilità relative alla sicurezza in azienda fornendo:
 - Conoscenza sulle security policy
 - Conoscenza sui regolamenti
- Creare nei dipendenti una coscienza dei rischi informatici che li riguardano informandoli su come:
 - Controllare gli accessi agli spazi di lavoro e proteggere le informazioni aziendali
 - Assicurarci della sicurezza delle comunicazioni con l'esterno (posta elettronica, Internet, telefono)
 - Essere sufficientemente diffidenti e ragionevolmente prudenti nei confronti di situazioni anomale

L'importanza della formazione

- La formazione è importante per chi nella sua funzione deve compiere delle scelte di tipo strategiche, progettuali o tecnologiche
 - Per riconoscere i rischi informatici e decidere le modalità di gestione del rischio
 - Per comprendere i principali aspetti sia tecnici sia organizzativi della gestione della sicurezza
 - Per esaminare i processi aziendali dal punto di vista della legislazione, della revisione e della conformità

- La sicurezza non è solo un problema tecnologico
- E' importante comprendere le caratteristiche degli attori coinvolti
- La gestione del rischio non è un'attività statica ma ha una sua evoluzione nel tempo
- Il progetto della sicurezza è un attività che richiede l'intervento degli specialisti
- La gestione della sicurezza è un'attività in cui devono essere coinvolti tutti gli attori della banca

- Corso « La sicurezza informatica nelle attività bancarie e finanziarie »
 - comprendere l'importanza della sicurezza informatica nelle attività finanziarie
 - analizzare i rischi informatici e valutare le tecniche di gestione del rischio
 - presentare i principali aspetti tecnici e organizzativi per gestire la sicurezza informatica
 - esaminare la sicurezza informatica dal punto di vista della legislazione, della revisione e della conformità
- <http://www.csbancari.ch>

Domande ?