

Frodi interne

aspetti tecnologici

Security Summit 2010

Milano, 16-18 Marzo

Frodi interne vs. esterne

- Esterne: numerose, di impatto mediamente basso
- Interne: poche ma di impatto elevato
 - Conoscenza delle procedure
 - Maggiore rischio
 - Maggiore fiducia

Vulnerabilità?

- Nel caso di frodi interne, l'aspetto tecnologico è spesso incidentale
- Nessuna ricerca metodica di vulnerabilità
 - Trovate casualmente
 - Note internamente all'azienda
- Il rischio è alto, la “ricerca” con metodi da attacco esterno è troppo rumorosa

Contromisure

- L'aspetto tecnologico è più rilevante in termini di contromisure
 - Possibili, ma non adottate perché
 - scomode
 - Non necessarie (c'è fiducia)
- Anche queste sono sensibilmente diverse
 - Si opera su attività spesso “legittime”
 - Monitoraggio
 - Quadrature
 - Difficili da adottare se non previsti nel processo aziendale (non solo informatico)

Caso 1: manomissione dei dati in ingresso

- Se i dati sono manomessi al momento dell'introduzione nel sistema, è difficile poi fare delle verifiche
- Sistemi di telemisura: problemi di sicurezza fisica
 - Apparati
 - Postatili
 - Palmari
 - ...
- La sicurezza fisica è molto difficile da garantire
 - Sigilli, ma difficile la manutenzione
 - Monitoraggio delle variazioni/anomalie
 - Bilanci
 - Controlli a campione
- Fiducia?

Caso 2: manomissione dei controlli

- Spesso i controlli più significativi non sono “informatici”
 - es. verifica manuale/autorizzazione su cartaceo
- L'interfaccia fra il sistema informatico e le procedure cartacee è un passaggio critico
- Un problema simile si ha quando i dati vengono “estratti” per fornirli ad un'autorità di controllo
- C'è anche qui un problema di fiducia
 - Eventuali strumenti tecnologici possono poco quando l'interfaccia è umana

Caso 3: fughe di dati

- Problema molto sentito, al quale si cercano soluzioni tecnologiche
 - Personale autorizzato che fa uscire volontariamente i dati dall'azienda
- Esistono soluzioni commerciali valide (scomode, complesse?) che tutelano da chi non ha controllo amministrativo sui sistemi
 - Controllano le stampe, la copia su supporti rimovibili, l'invio per posta...
 - Appena i dati escono da questi canali, se ne perde comunque il controllo
 - Problema dei fornitori
- Trusted Computing?

Caso 4: problemi di procedure

- È stato messo in esercizio un nuovo strumento software per implementare una procedura aziendale
 - Contesto bancario, procedure dispositive
- Il vecchio strumento è stato “disabilitato” ma è ancora presente e non del tutto inefficace
- Un operatore si accorge che con il vecchio strumento è possibile stornare delle transazioni:
 - Lo storno non avviene effettivamente, ma per i controlli sì
 - L'operatore esegue delle transazioni, poi le storna con il vecchio strumento, per cui “non risultano”
- Usa le credenziali di un collega...

Caso 5: controlli non implementati