Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004
Articolo pubblicato sul n. di ICT Security di Gennaio 2004

INSIDE ATTACK: QUALE PREVENZIONE POSSIBILE?

Di Marco Strano

Chi si interessa di sicurezza informatica si trova sempre a che fare con due potenziali fronti di attacco e quindi di difesa: gli attacchi provenienti dall'esterno (outsiders), eseguiti da giovani hackers, spie industriali, crackers ecc. e gli attacchi provenienti dall'interno (insiders). Il fronte di attacco outsiders è quello più evidente e si contrasta soprattutto implementando le contromisure tecnologiche, le difese "logiche" dell'organizzazione e insegnando agli operatori quali negligenze possono favorire le intrusioni. Il fronte di attacco interno (insiders) è invece meno evidente ma più insidioso ed è in grado di provocare i danni maggiori per l'organizzazione vittima. Impiegati infedeli o in contrasto con l'azienda e consulenti informatici disonesti sono coloro che conoscono meglio le architetture dei sistemi di sicurezza e possono eseguire con più facilità degli hackers operazioni "proibite" di vario genere: frodi, furti di informazioni, cancellazione o alterazione di dati, utilizzo delle macchine per scopi privati, ecc. La casistica sul computer crime *inside* raccolta dall'UACI (Unità di Analisi sui Crimini Informatici) della Polizia Postale e delle Comunicazioni è estremamente variegata e contiene operazioni illegali animate da motivazioni appropriative (furti di informazioni e frodi) e da motivazioni emotive (danneggiamenti e sabotaggi). Molto spesso in tali casi emerge una leggerezza nell'applicazione delle misure di sicurezza e un quadro di ridotta "percezione del crimine" da parte del responsabile. L'esperienza investigativa della Polizia Postale indica inoltre che i pochi attacchi provenienti dall'esterno che provocano danni considerevoli, vedono quasi sempre la complicità di un insider.

LE DIFESE POSSIBILI DAGLI INSIDERS

Quali sono dunque le contromisure più efficaci per gli attacchi inside? In primo luogo un monitoraggio anche delle operazioni interne alla rete aziendale, (informando ovviamente di ciò tutti i dipendenti) e la diffusione di procedure con appositi pacchetti software che individuano con ragionevole certezza il "*chi, come, dove, quando e perché*" di ogni operazione informatica effettuata nell'ambito dell'organizzazione. In secondo luogo, ma non di secondaria importanza, è necessaria una valutazione della percezione del rischio e della cultura della sicurezza di tutti coloro che utilizzano un computer aziendale, utilizzando ad esempio lo Psychological Risk Assessment dell'ICAA (delle interviste e uno specifico questionario). In terzo luogo è indispensabile un intervento mirato di formazione/addestramento del personale al rispetto delle procedure di sicurezza. Le questioni di security, infine, con l'avvento dell'informatica distribuita e con la conseguente condivisione delle risorse informative sensibili (RIS) tra tutti i dipendenti dell'organizzazione, devono essere padroneggiate anche dalla massima dirigenza aziendale e non dalla sola elìte tecnocratica dei responsabili della sicurezza informatica. Talune scelte e contromisure, specie quelle centrate sul fattore umano, devono necessariamente essere elaborate e condivise anche dalle aree di marketing e di gestione delle risorse umane. Queste considerazioni in effetti cominciano sempre più a diffondersi negli ambienti degli specialisti della sicurezza informatica. Non è un caso che il protocollo di risk assessment di alcune innovative società di consulenza informatica cominci a prevedere uno screening del fattore umano oltre che dell'hardware e del software aziendale, come nel caso della Spark che ha stretto a tal fine un'alleanza con l'associazione di psicologi e criminologi ICAA (International Crime Analysis Association) che ha il suo quartier generale su internet all'indirizzo www.criminologia.org e che sta svolgendo approfondite ricerche sui crimini informatici ad opera di insiders, raccogliendo casi e somministrando questionari a dipendenti di ogni ordine e grado. La D.ssa Roberta Bruzzone, Psicologa e Criminologa vicepresidente dell'ICAA, sta infatti coordinando un esteso monitoraggio (assolutamente anonimo) del livello di diffusione delle policy di sicurezza nelle aziende italiane di varie grandezze e tipologia. Le imprese che offrono la loro collaborazione a tale ricerca ricevono poi un report riservato sui punti deboli della loro security informatica legati al fattore umano e una serie di consigli per migliorare la situazione. L'ICAA raccoglie alcune equìpe di ricercatori statunitensi, come ad esempio quella del famoso Prof. Marc Rogers della Purdue University che è considerato uno dei massimi esperti mondiali di Psicologia del computer crime.

Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

DIGERIRE I CAMBIAMENTI NELLE PROCEDURE DI SICUREZZA

Ogni misura di sicurezza da rispettare costituisce spesso una nuova dinamica da inserire nel processo di lavoro, in pratica una nuovo compito che l'operatore deve aggiungere al suo normale lavoro e tale inserimento deve essere "digerito" da tutti. Normalmente le fasi critiche nell'applicazione di una operazione di security informatica sono due: la prima fase si manifesta all'inizio, con l'introduzione della nuova prescrizione, quando le persone devono abituarsi alla novità e devono quindi superare le fisiologiche rigidità all'innovazione; la seconda fase critica si manifesta invece dopo un certo periodo di tempo, quando l'abitudine alla routine e l'assenza di incidenti che "legittimano" la misura precedentemente adottata abbassano l'attenzione e inducono al non rispetto della procedura di sicurezza in questione. I vari post-it con password attaccata al monitor, il mantenimento del computer connesso in assenza dell'operatore, la disattivazione di antivirus e firewall "colpevoli" di rallentare le operazioni, sono tutte dimostrazioni dell'abbassamento del livello di guardia in assenza di eventi convalidanti e giustificanti la misura preventiva.

Secondo le tendenze più recenti una moderna policy di sicurezza deve quindi prevedere una grande attenzione anche per il "fattore umano" e se possibile contemplare la consulenza di uno specialista delle dinamiche psicologiche che possa suggerire delle strategie per superare le fasi critiche e per motivare le persone al comportamento sicuro. Un comportamento incauto di un dipendente può infatti vanificare un sistema di sicurezza anche molto sofisticato e la paura di una eventuale sanzione negativa non è sempre sufficiente ad orientare le sue scelte e le sue azioni.