Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

INSIDE ATTACK: what prevention?
By Dr. Marco Strano

Who deals with ICT security has always to do with two potential fronts of attack (and then of defence): the attacks coming from the outside (outsiders) made by young hackers, industrial spies, crackers, etc. and the attacks coming from the inside (insiders). The outsiders front of attack is the most evident and can be opposed above all with the implementation of technological countermeasures, "logic" defences of the organization and by teaching to operators what negligences can facilitate intrusions. Instead the insiders front of attack (insiders) is the less evident but more insidious and is able to provoke the worst damages for the organization-victim. Employees in contrast to the company or simply disloyal and deceitful computer consultants are the ones who better know the ICT security architectures and can carry out, with more ease than hackers can do, "forbidden" operations of various sorts such as: frauds, information theft, data deletion or alteration, machine use for private goals, ecc. The case studies on inside computer crime gathered by the UACI (Computer Crime Analysis Unit – Communications Police Service) of The Italian State Police is extremely variegated and contains illegal operation driven by appropriation motivations (information thefts and frauds) and by emotional motivations (damaging and sabotage). Very often in cases like these an imprudence in the application of security measures emerges together with a reduced "crime perception" attitude by the security manager. Moreover the investigative experience of the Italian Communications Police indicates that the few attacks coming from the outside that provoke great damages, almost always are commited in complicity with an insider.

Possibile defences against insiders

What are the most efficient countermeasures against insiders attack? First of all a monitoring even of the operations inside the company's network (of course by informing all the employees) and the spread of procedures with proper software packages that are able to identify, with a reasonable certainty, the "*who, how, where, when and why*" of every information operation carried out within the ambit of the company. In second place, but not of secondary importance, it's necessary a risk perception and security culture assessment of everyone that uses a company PC, by using, for example, ICAA's Psychological Risk Assessment (some structured interviews and specific questionnaires). In third place it's essential a training intervention of the personnel focused on the respect of security procedures. Then, the security questions, with the advent of ICT technology and with the consequent sharing of the information sensitive resources (RIS) among all the employees of an organization, must be mastered even by company's top management and not only by security managers's technocratic élite. Some choices and countermeasures, specially the ones centered on human factor, must necessarily be elaborated and shared even by marketing and human resources management areas. In effect these considerations begin to spread more and more within the ambits of ICT security specialists. It's not a case that the risk assessment protocol of some innovative ICT consulting companies begin to include a screening focused on the human factor in addition to the one centred on the company's hardware and software, as in the case of the Spark that for this purpose has contracted an alliance with an association of psychologists and criminologists (ICAA - International Crime Analysis Association) that has its head quarter in the Net at the following URLs www.criminologia.org and www.icaa-italia.org and that is developping thorough researches on computer crimes committed by insiders, by collecting cases and administering questionnaires to employees of all ranks. In fact Dr. Roberta Bruzzone, Psychologist and Criminologist, Vicepresident of the ICAA, is coordinating a large monitoring (absolutely anonymous) of security policies's level of diffusion within the ambit of italian companies of different size and tipology. The companies that offer their collaboration to this research, after the administration, receive then a confidential report focused on their ICT security weak points connected to the human factor and a series of advices to improve their situation. The ICAA gathers some USA researchers' equipe, as for example, the one headed by the famous Prof. Marc Rogers of the Purdue University, that is considered one of the greatest experts on computer crime Psychology all over the world.

Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

To get over security procedures's changes.

Every security measure that has to be respected often represents a new dynamic to inser in the working process, in practice a new work that the operator has to add to his/her normal work and such an insertion must be "got over" by everyone. Normally the critical phases during the application of a ICT security operation are two: the first phase manifest itself at the beginning, with the introduction of the new prescription, when the individuals have to get used to the change and then they have to overcome the physiological resistences towards the change; instead the second critical phase shows itself after a certain period of time, when the routine habit and the lack of accidents that "legitimate" the measure previously adopted lower the attention and drive to not-respect of the security measure at issue. The various post-it with the password stuck to the monitor, the maintenance of the PC connected to the Net even when the operator is not present, the deactivation of antivirus or firewall "guilty" of slowing down the operations, are all signs of the danger point's reduction in the absence of events that justify and support the precautionary measure in question.
According to the most recent tendencies, a modern security policy must include a great attention even for the "human factor" and, if possible, has to include a counselling of a specialist on psychological dynamics that can suggest some strategies to overcome the critical phases and to motivate the individuals to keep a safe behavior. In fact an imprudent behavior of an employee can thwart even an highly sophisticated security system and the fear of a possible negative sanction is not always sufficient to guide his/her decisions and actions.