The next Snowden Case can be Prevented

Almost none of the world's security companies is concerned with the question of how to prevent another case of a leak like the Edward Snowden case. Will the implementation of the HFTIM method provide the solution?

By Shabtai Shoval

Illustration: shutterstock

One of the existing cyber measures intended to prevent an "insider threat" would have stopped Edward Snowden, or Mordechai Vanunu for that matter. Moreover, all of the IT-oriented solutions designed to prevent an "insider threat" within the organization are incapable, by definition, of preventing a sophisticated employee from carrying out his evil schemes. This serious allegation will most certainly enrage all of those IT executives who spend millions each year on technologies offering only limited effectiveness.

Edward Snowden inflicted a strategic damage on the US that was more substantial than the damage inflicted by all of the cyber attacks staged by terrorist elements against the American government in the last ten years. Mordechai Vanunu revealed the secrets of Israel's nuclear program (according to foreign sources) and the information leaked by Anat Kamm could have resulted in the loss of lives. Beyond those prominent cases at the government level, there are dozens of cases at the business level where employees or sub-contractors of various business organizations caused massive damage.

Failing to Identify the Enemy Within

The existing ways for coping with insider threats include three basic loops: screening of potential employees during the hiring process, monitoring the employee's computer usage patterns after he/she had been hired and receiving intelligence concerning suspicious behavior from external and internal sources.

In Israel, the screening of potential employees before they are hired relies on the references of the candidate's acquaintances and on information provided by specialist companies that conduct personality tests. In the USA, personality testing is not so widely used and some employers run background checks that include an investigation by private investigation firms regarding the candidate's past and whether any suspicious information has been found about him/her.

After the employee was lucky to be accepted by the organization, the options available to the employer for identifying a certain employee as posing the risk of an insider threat are very limited. Normally, the primary cyber tool available to employers consists of systems that monitor the computer usage patterns of the employee.

Monitoring this behavior is based primarily on the (groundless) assumption that in order to commit a serious violation against the work place, the employee has to deviate from the conduct expected of him/her. Several systems operating according to this concept are currently available on the market, for example the SEIM systems that collect data from the IT systems and enable analysis of computer usage patterns and deviations from those patterns, DLP systems that enable tracking of documents in an attempt to prevent abuse by employees and outsiders and so forth.

All of these technologies are used as an "inevitable" measure, namely – every organization must use them either owing to compulsory regulation or in order to provide minimum protection against various threats. Unfortunately, the probability of these technologies identifying a sophisticated insider threat is embarrassingly low, for a number of reasons. Technologies for monitoring computer usage patterns are normally characterized by an extreme abundance of false positive identifications, in some cases as many as 99% or more. In other words, alerts generated by systems such as the SEIM systems, which claim to be able to locate external and internal attacks, "bombard" the controllers with massive amounts of false alarms with absolutely nothing behind them. The controllers on behalf of the information security layout tire of keeping track of these false alarms ("latent dysfunction") and eventually ignore them as a matter of routine.

Additionally, technologies for monitoring the computer usage patterns of the employees attempt to spot the trivial behavior of an insider threat, namely – such behavior as downloading too many files to electronic media such as a disk-on-key or DVD, printing of numerous documents, attempting to access unauthorized files or servers, making repeated attempts to enter passwords, working at irregular hours, irregularly using the organizational computer resources, executing irregular transactions and so forth. Sophisticated insider threats will not fall into such traps, so the false negative attacker identification rates of these technologies are also very high.

Employees choosing to damage the organizational interests or rules possess two primary characteristics: intent/motivation and ability/opportunity. The "attacker" employee will act when his intent and an opportunity coincide. The existing technologies assume that the insider threat is stupid enough to operate in a manner that would automatically trigger the known irregular behavior control mechanisms. These existing technologies completely ignore the element that is by no means less important, and possibly even more important – the very intent or motivation of the insider threat to act in a manner that would damage the organization. The simplest and most basic rule of security applies to this case as well – when there is motivation, opportunity is just a matter of time.

Do we possess a conceptual and technological alternative capable of filling the gap and spotting the attacker according to his/her intentions and human behavior, beyond his/her computer usage patterns? There is currently a method that has a high potential of spotting an insider threat according to his/her intentions or non-computer-related behavior: the Human Factor Insider Threat Mitigation Method, or HFTIM.

This method is based on technologies that focus on the human factor and on employee behavior, according to a methodology that is similar to the one developed in the field of aviation security for El-Al Airlines in the 1980s: assembling a profile of potential attackers with a derivative reference to the actual prevention of an attack in accordance with that profile. Three assumptions provide the foundation for this method: the detection and prevention resources will always be limited; in order to make the most of the limited resources, the resources should focus on employees with the most substantial intent/opportunity/damage potential; it is possible to predict, with a high degree of probability, what individuals within the target population possesses the most substantial attack and damage potential.

The derivative implication of these principles is that employees should be cataloged according to risk potential, which differs from one employee to another and is affected by a critical mass of synergistic factors. The subjective (baseline) profile of the employee, which consists of the results of a dedicated test (the P300 test) along with information from the field of human resources available to the organization. Additionally, the method uses an objective risk potential profile of the employee, which is based on the employee's actual access to critical systems and secrets of the organization. The third basic component consists of information from the existing IT alert systems that monitor the employee's computer usage patterns.

The basic element of this technology is the P300 test, which employs the "guilty knowledge" methodology. These tests measure the subject's responses to a series of stimulations in the form of a questionnaire. The questionnaire is very similar to a standard questionnaire intended to reaffirm that the employee had not committed various violations (A sample question: Have you passed confidential information to company competitors?).

The employee is required to take the test as the result of an irregular act on his/her part, or pursuant to a specific alert generated by the organizational computer usage pattern monitoring systems, or on a regular basis, in the context of routine tests the employees have to take. The results of the test are compared to the employee's past results and to the results of his fellow employees. The employee's psycho-physiological responses are measured by dedicated software.

The complete subjective profile includes the findings of the test and the data provided by the human resources department, cross-referenced with the employee's risk element: his/her formal and informal access to sensitive information or to organizational resources

Catch the Leak in Time

The uniqueness of the method and technology proposed herein stem from the fact that they make it possible to identify employees who intend or who actively endeavor to damage the employer based on their tested and compared human behavior. In this way, Edward Snowden, Anat Kamm, Mordechai Vanunu and thousands of employees who damage their countries or their employers would have been caught in the earliest stages of their activity, or would have come under the watchful eyes of the information security directors as early as during the stage when they only had an unfulfilled intent.

Moreover, in the event of alerts generated by the SEIM system or the organizational authorization management system and so forth, the HFTIM concept can be used to minimize the amount of false alarms to a manageable number of meaningful alerts only. Beyond the effectiveness in identifying threats from within the organization and significantly reducing the number of false alarms, the HFTIM method provides an equally substantial value – a deterrent effect vis-à-vis the employee. When the employee has to pass dedicated tests occasionally, either because of company policy or pursuant to an irregular act he/she had committed, the psychological deterrent effect is very significant.

The implementation of the HFTIM method may be measured empirically: the number of false alarms generated by the IT systems will decrease immediately following the implementation of the method. Pursuant to the implementation of the method, the organization will experience a miraculous and dramatic decrease in inventory losses including office stationery, private telephone calls and absenteeism.

"Ideological" insider threats like Edward Snowden as well as "self-serving" criminal threats would, in most cases, have avoided acting if they had known that it was highly probable that they would be spotted by the system even before they made their move.

The author is the founder of SDS Suspect Detection Systems Ltd. and a fellow research associate at IDC Herzliya