COMPREHENSIVENESS OF COUNTERMEASURES AGAINST POTENTIAL COMPUTER AND PHYSICAL INSIDERS AT NUCLEAR FACILITIES

SERGEY ZHURIN
Federal Center of Science and High Technologies "SSPA "Eleron"
Moscow, Russian Federation
E-mail: control@eleron.org

Abstract

The countermeasures against potential physical insiders and especially computer insiders is critically important at nuclear facilities (NF). Insider may have authorization, knowledge or access including access to information, nuclear materials, NF elements and to software. That's why standard physical or data protection measures are not always enough which confirm the necessity to organize the set of preventive and protective measures for insider's risk reduction.

It is necessary to apply a complex approach for protection against potential insiders (physical and computer together):

- in the process of employment;
- in the process of work;
- during termination/reduction procedures.

This complex approach and modern measures are described in the paper in focus to prevent physical and cyber threat separately and together.

It is necessary to assess the sufficiency of counteracting against insiders using two main approaches: the method of assessing compliance with regulatory requirements and / or the method of modeling the penetration of an insider.

This approaches (with using modern models) are described in the paper. Software for implementation these methods is described also.

Commonly, countermeasures against physical and computer insiders in complex are considered in the paper.

1. INRODUCTION

The importance of protection against physical and computer insiders at nuclear facilities (NF) is reflected in many Russian regulatory documents (i.e. in 187-FL – "On Russian Federation critical informational infrastructure protection") and in IAEA Nuclear Security Series documents, for example in NSS08 (NST-041) "Preventive and protective measures against insider threats" [1] and NSS-17 "Computer security at nuclear facilities" [2].

In comparison of physical protection threats (nuclear material (NM) theft and sabotage at nuclear facilities (NF)) and computer threats (sabotage at NF using software and information theft (modification)) we may reach the conclusion that computer threats are quite serious because in sabotage at NF using software (as distinct from physical sabotage) there is no need to use any explosives, devices, force impact but need only programming skills and access to software environment and database or communication lines.

Insider's threats are confirmed by accidents presented in open sources. For example, oil dumping from turbine at Belgium NPP Doel-4 performed by insider (2015), intended change of monitoring source code at Ignalina NPP (Lithuania, 1995) or Stuxnet malicious software integration into uranium enrichment centrifuges in Natanz, Iran (2009). Those examples show the necessity of protection against insiders.

Presence of modern equipment and tools (i.e. pilotless vehicles or malware for computer attack) in a free access for physical and computer insiders increase the dangerous of their attack.

Insider may have authorization, knowledge or access including access to information, nuclear materials, NF elements and to software of Industrial&Control Systems (I&CS) of NF: I&CS of NPP, physical protection systems (PPS), nuclear materials accounting and control systems (NMAC). That's why standard

physical or data protection measures are not always enough which confirm the necessity to organize the set of preventive and protective measures for insider's risk reduction.

2. COMPREHENSIVENESS OF COUNTERMEASURES AGAINST POTENTIAL COMPUTER AND PHYSICAL INSIDERS

2.1 Common approach

It is necessary to apply a complex approach for protection against potential insider (PI):

- in the process of employment: trustworthiness testing multistage system
- in the process of work: excluding of physical, legal and ability to conduct a crime, staff prophylactic management, PI identification and detection of personnel close to discharging.
- during termination/reduction procedures: decreasing authorities of this personnel and information backup provision.

To prevent potential insider employment special comprehensive procedure concerning personnel trustworthiness shall be applied. This procedure includes interview, psychological testing, lie detector testing, social networks analysis, crime records (information) analysis, tendency to drugs or alcohol addiction shall be conducted for PI employment avoidance. This procedure shall be graded depending on position, access level and clearance level.

For periodical staff personality evaluation at workplace, both negative factors (i.e. alcoholism, attitude to security procedures) and positive factors (i.e. financial stability, moral properties demonstration, positive attitude to the job responsibilities) should be evaluated.

Besides trustworthiness testing, it is necessary to perform general security procedures against insiders: staff access limitation (e.g. physical access into site areas and informational access into information systems), identification of illicit tools carrying out and using that could be used as insider's tools (e.g. digital: laptops, mobile phones, 3-G modems, key-loggers; physical: cold steel, bench tools) etc.

In addition to measures mentioned above, it is necessary to analyze breaches of procedures and measures both physical (attempting to access into restricted area, attempting to carry out illicit tools) and digital (attempting to passwords brute force, malware installation, attempting to carry out mobile devices, flash drive, notebooks, copying of sensitive information) including different types of security systems testing.

The abovementioned methods of data collection, psychological characteristics, types of violations will be used in the IAEA research project J02010 "Preventive and protective measures against insider threats at nuclear facilities". Within this project, the IAEA SNPO "Eleron" conducts a study of negative parameters of PI, methods for their identification, model of formation and identification of PI.

2.2 The specifics of preventing insider threats in Russian Nuclear Facilities

The specifics of preventing insider threats in Russian NF consist of an nuclear safety culture system, an anti-corruption system, the work of a security department and the work of a laboratory for conducting psychophysiological examinations.

Comprehensiveness approach to information security in Russian NF, in particular, isolation of networks and automated workstations (AWS) of NF, the use of registered information storage devices, port blocking, a closed software environment, access control, certification and attestation of automated systems make it possible to exclude an internal computer insider in NF.

Comprehensive protection against insiders in Russian NF includes compartmentalization of access (in protected areas to nuclear materials and in computer programs to sensitive information) and authorities,

selective control, audit, monitoring, the complexity of the emergency by using the automatic control, the impossibility of critical masses of NM. This approach allows protection from the actions of an physical and computer insiders.

It is advisable to consider together the physical and computer insiders in relation to nuclear facilities during the theft of nuclear material or sabotage at Nuclear installation, as NM is identified and taken into account in automated systems, I&CS of NPP contain an increasing amount of automated components, and the adversary will use all possible paths to minimize the risk of detection both during the preparation of the action and during its execution. Therefore, when implementing protective measures, it is necessary to consider and evaluate the protection as a whole.

3. THE SUFFICIENCY OF COUNTERACTING COMPUTER AND PHYSICAL INSIDERS: TWO METHODS

The sufficiency of counteracting insiders can be assessed using two main approaches: the method of assessing compliance with regulatory requirements and / or the method of modeling the penetration of an insider (in computer simulation or real penetration).

In comparison of PPS and information security system effectiveness assessment methods it can be found that a time-line analysis method modeling of adversary penetration have implemented since 1980's (in addition to deterministic approach) using software Vega-2 (Russia), Assess (USA).

A modeling assessment method for effectiveness assessment in IT-area been applying (in addition to deterministic approach using ISO standards and using in Russian software Grif and Condor for assessing level of information security) since 2010's (MITRE (https://attack.mitre.org/) and CTF models (https://www.dni.gov/index.php/cyber-threat-framework)).

The MITRE model began to be used in 2019 in the Max Patrol program (in the SIEM system of a computer network) of the Russian company Positive Technologies. The penetration simulation analysis method or modeling is useful for evaluating effectiveness because it allows you to analyze all the paths of attack development and identify places with insufficient security.

It is noteworthy that deterministic approach on security systems conditions assessment is not able to assess level of protection correctly due to the fast change of technologies (physical and digital) because of upgraded requirements of regulatory documents (and documents itself) been developed only in 2-4 years after new threats identification.

When modeling, it is also advisable to combine computer and physical insiders based on the scenarios of their actions, as indicated in the new version of NSS-10 (Development, use and maintenance of the basic design threat) [3]. The integration of computer and physical penetration was implemented in 2014 in a unified mathematical approach and was implemented in the PACRAT computer program in 2015.

4. CONCLUSIONS

Thus, for a comprehensive countermeasures against computer and physical insiders, it is necessary to perform:

- preventive measures (including including personal verification, maintaining an adequate level of reliability),
- protective measures that minimize the capabilities of the adversary (access control, verification of the passage of prohibited items),
- measures to respond to unauthorized actions,
- measures to verify, analyze violations and possible signs of possible crimes,
- measures for periodically check compliance with both the requirements of regulatory documents and conduct an assessment of the effectiveness of existing systems.

REFERENCES

[1] Preventive and protective measures against insider threats. IAEA Nuclear Security Series, №8.
[2] Computer security at nuclear facilities. IAEA Nuclear Security Series, №17.
[3] Development, use and maintenance of the basic design threat. IAEA Nuclear Security Series, №10.