Impact Factor: 9.9 ISSN-L: 2544-980X

Security Threats in Information Systems Classification

Fazlitdinov Muhammadali Khatamjonovich [1]

Abstract: Information in systems safety threats of information confidentiality , integrity and existence to break directed different risks own into takes Threats right classification information systems efficient protection in doing important important have This threats basically technical , software and a person factors with dependent being them one how many to groups separate possible : external attacks (hacking , malicious programs), internal attacks (of employees wrong works or sabotage), technical malfunctions (of equipment from work output) and natural disasters (fire , water floods). Each threat type prevention get for safety measures and protocols work exit necessary Information systems safety in providing of threats classification important of the system protection level increase and information to be lost to minimize help gives .

Key words: information systems , security threats , hacking , malicious programs , internal attacks , technical failures , naturally disasters , security measures.

Information and communication of technologies development and to the internet access of possibilities increase with organizations different different to threats relatively weak being they stay . In fact , theirs information cyber to attacks subject to will be and of this as a result damage sees Threats different from sources comes , for example , of employees activity or of hackers attacks . Safety violation as a result come coming out financial losses usually sure to determine possible not because big in quantity losses smaller scale safety incidents come comes out and information system safety risk enough level to evaluate take will come So managers their own to assets effect who does threats they know and belongs to against measures choose through of attacks prevention get for what to do need to determine for their effect determinations need

Threats classification principles

Taxonomy islearning in the field more to understand for used of reality is an approximation. Literature seeing exit information safety of classification the following principles compliance to do need shows:

- Reciprocal exclusive : Each threat one in the series classified if , another all risks an exception because it does categories to each other suitable does n't come
- Full : In classification categories all options (all threat samples) own into take need
- Clear : All categories sure and sure to be it is necessary , then classification sure will be
- Repetitive : Repetitive applications who from classification strict nazar , one different to classification take will come
- Accepted: All categories logical, intuitive and practices the majority by easy acceptance will be done.
- Useful : From it request field about to understanding have to be for use can
- Security threats classification : general appearance

Threats classification important important have because they are basically of threats features and system assets protection to do sources to determine and to understand enable gives From this except , it is this to systems threat puter safety risks represents and opportunities to understand and safety solutions to choose help gives The threat is that of the opponent purpose or rival to the system what to

[1] Muhammad al- Khorazmi TATU named after Ferghana branch assistant

do to be can It is also the opponent 's to the system attack to do ability as is described . So making a threat two road with determination possible: intruders system in the components from weaknesses use for which uses methods or of threats to your assets effectThreats classification approaches for two our separation can:

- Attack to the technique based on classification methods
- Threats to the effect based on classification methods

Offer model being developed

Safety threats a lot classifications usually threats classification for one or two from the criterion use with limited , others while of threats complete didn't happen the list present will (all threats in classification cover not taken) and their categories each other an exception does not This is security threats relatively stable has been stable environment (small organization) for enough to be possible , but permanent variable in the environment organizations internal from threats protection do it ca n't From this except , available threats at work main problems to determine can Ours our model behind main the idea many threats classification criteria combine and their potential effect is to show . Above given common from the view received criteria classification list:

- Security threat Source : Internal or external of threat come output
- Security threat agents: threats cause emits agents and we are three main class we found out: human , ecological and technological .
- Security threat motivation : Harmful or harmful didn't happen in the system of attackers purpose
- Security threat intention: on purpose or random the threat cause released of a person intentionThis criterion attack behavior and his intention to understand for complete harmful behavior again to build enable gives This is to the investigators work high precision with in conclusion help to give for prophecy to be done factor present is enough and therefore for risks reduces and real the agent to the hand get according to decision acceptance to do accelerates .
- Threats effect: Threat effect threat movement as a result surface coming safety is a violation.

Used literature

1. Lindqvist U, Jonsson E. How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy; 1997. 154163. 2.
2. Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Computer Crime and Security Survey – 2006. 11th Annual CSI/FBI Computer Crime and Security Survey; 2006.