

#30



Cyber Polygon Site Project in the Framework of the MEPhI Network Security Intelligence Center

Miloslavskaya N. (ngmiloslavskaya@mephi.ru), Tolstoy A. NRNU MEPhI, Moscow, Russia



First Author



Second Author



ABSTRACT

At present, the market for information protection tools (IPTs) is much wider than a couple of years ago. But not only technology protects and carries a threat. People are still at the forefront as the most common cause of errors is the lack of experience and low competency. The only right solution is the creation of cyber polygons as specially equipped and controlled network infrastructures for developing practical skills to combat information security (IS) threats. The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) could not remain aloof from this process as the leading institute for IS training in Russia. Therefore, it was decided to create such a cyber polygon within the framework of the educational and research Network Security Intelligence Center (NSIC) for intelligent network security management established at the MEPhI Institute of Cyber Intelligence Systems in 2016. The paper describes the first results achieved in making this project a reality. It introduces the "Cyber Polygon" term, briefly analyzes a state of the current cyber polygons development worldwide, and introduces the MEPhI Cyber Polygon objectives and provision to be used within the framework of the "Business Continuity and Information Security Maintenance" Master's degree programme. Further activities in its development conclude the paper.

INTRODUCTION

At present, the market for information protection tools (IPTs) is much wider than a couple of years ago: one can buy many products of different price ranges, from antiviruses and firewalls to cybersecurity operation centers based on artificial intelligence, that allows to correlate information sources and predict how the probability of an information security (IS) event occurs and the consequences of each decision and step. These things together bring the work of IS experts to an unprecedentedly high level of reaction to an event that can only occur but has not yet occurred, while at the same time reducing the risk of the human factor to 0. But not only technology protects and carries a threat. The current problem of ensuring cybersecurity is not so much in the technological as in the personnel field. People are still at the forefront; they are known to be mistaken. The most common cause of errors is the lack of experience and low competency, while the whole business can be the price of an error. What could be done? Worthy experts cannot be taken from a school or college. Professionals in the market are expensive; there are few of them. Even if the company was lucky enough to find such a specialist, this does not mean that he will know how to deal with one attack having repelled another one. This problem is not new. The only right solution is the creation of its own "cousin of IS officers" called a "cyber polygon" (also known as a cyber range) as a specially equipped and controlled network infrastructure for developing practical skills to combat IS threats. For IS employees, it is the best tool for gaining invaluable professional experience without risking its infrastructure. For business owners, it is the best source of trained IS professional personnel, ready to face any IS threat. The analysis of the state of IS training of the Russian Infotecs company says that the average indicators in Russia are as follows: 10% have a basic education in the field of IS, 16% have completed professional retraining courses, and 74% (3/4) do not have an IS education. To remain competitive in the global cyberspace in the future, Russia needs over 20 thousand IS specialists. At the same time, the organization of such training on existing information and telecommunication systems and networks (for example, on the real Internet) where it is impossible to directly study the detection tools and prevent stew attacks is objectively difficult. It is hard to imagine classes with students on the analysis of computer viruses' spreading technologies on the Internet! In turn, within the framework of traditional computer classes, the use of technologies far from reality can ultimately negatively affect the final level of students' knowledge and skills. In this regard, for the success of the educational process, it is advisable to create a specialized environment – a cyber polygon, which would help to study the features of various computer attacks and to protect against them with the highest possible realism and at the same time safely. The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) as the leading institute for IS training in Russia could not remain aloof from the process of creating cyber polygons. Therefore, it was decided to create such a cyber polygon within the framework of the educational and research Network Security Intelligence Center (NSIC) for intelligent network security management, established at the MEPhI Institute of Cyber Intelligence Systems in 2016. The paper describes the first results achieved in making this project a reality. Further activities in its development conclude the paper.

Cyber Polygon Definition

In our research, based on the related work analysis, we define a Cyber Polygon as a specially equipped and controlled network infrastructure for online cyber training sessions on ways security professionals can engage in national or even international cooperation to combat IS threats. Figuratively speaking, the cyber polygon is a "virtual country" that repeats the infrastructure of companies in various industries. Thus, cyber polygons are mainly designed to develop practical skills in identifying and responding to IS incidents via cyber exercises, as well as to conduct stress tests of hardware and software. Today, technology allows one to create a complete emulation of any infrastructure, from a small office to a space ship flight control center or even a smart city, to fill this infrastructure with real network devices and tools of any manufacturers and developers for monitoring, control and protection, and to enclose it all in an isolated "vacuum" and "freeze" it in the "all-is-well" state. It typically includes all necessary hardware and software for simulating some of the most common types of attacks and training of participating parties, as well as multiple geographically distributed sites for simulating remote access to the cyber polygon. Modern cyber polygons can also be created using cloud technologies. Cyber polygons allow the instructors to create for each student its own separate virtual laboratory environment, which can include tens or even thousands of virtual network resources. In this environment, the student gets the opportunity to complete regardless of colleagues his tasks, to save his results from lesson to lesson, and to carry out additional preparation for them during his independent work. This is not just a "sandbox"; it is a cyber polygon for training future IS officers who are ready to repel an attack of any complexity. All sorts of viruses and various attack scenarios can be launched in the cyber polygon, which future or current IS experts will have to fend off with the available set of IPTs. Like chess players, IS experts can at first understand and follow all the steps of well-known attack scenarios and try to repel them in different ways, and only then to run arbitrary random scenarios, gaining experience and understanding of the most effective actions and tools of dealing with them. This approach will allow not only to grow from a theoretician into a real expert but also to maintain a high level of preparedness for meeting new urgent IS threats. Such actions will help future IS specialists to form a system-integrated vision of IS problems, to get an idea of how common IS threats are implemented by attackers, and to learn how to effectively counteract them. The level of their success can be monitored by observers in real-time via a web site, specially designed for these purposes. After the "hostilities" end, the cyber polygon can be returned to its original state and will be ready for a new launch. Hence, the cyber polygon arms the students with skills, problem-solving, and critical thinking capabilities for ensuring network security in the best possible way. Besides, it is also possible to conduct IS competitions and create centers for testing software and hardware security, including IPTs, at cyber polygons.

MEPhI Network Security Intelligence Center as a Framework for Cyber Polygon Developing

As modern businesses face numerous targeted network attacks, the well-known "Detect-Investigate-Respond" triad must be added by the fourth "Adapt" critical component, which should be based on Security Intelligence (SI) approaches. For this purpose, we have already started in 2016 to build at MEPhI a Network Security Intelligence Center (NSIC) as a combination of SI Center (SI) and Network Operations Center (NOC) with their unique and joint toolkits and techniques. NSICs empower the autonomy of network security management within one organization, change the IS ensuring model from reactive to proactive, support more effective responses to IS incidents, enhance communications between the network and security teams, management and board members, drive IS investment strategies, and more directly connect IS priorities with business risk management priorities. Therefore, on the basis of this particular center, it is necessary to develop the MEPhI Cyber Polygon.

In the infrastructure of the NSIC, the Cyber Polygon is the fourth virtual one, combining the three already established laboratories, and interacting with the Center's Network Security Management tools (Fig.1). The first laboratory, as the core, has the Palo Alto Next-Generation Firewall (NGFW). The second laboratory is based on the Positive Technologies' MaxPatrol Security Information and Event Management (SIEM) system. A third lab is built around the SearchInform's Data Loss and Prevention (DLP) system. Continuing our research on designing NSICs we allocate five zones in the Cyber Polygon's security zone infrastructure, namely untrusted (not included into the NSIC itself), demilitarized (semi-trusted) (DMZ), trusted, restricted and management with their specific subzones and special sandboxing component (Fig.2). This approach separates coming from outside suspicious untrusted software from unverified third parties, users, web site and so on and will allow detecting previously unseen IS threats and alert Cyber Polygon's staff who can quickly take action. DMZ is a physical or logical Cyber Polygon's forefront subnetwork for external-facing servers and services that are externally shared by the NSIC and MEPhI intranet as well as remote and infra services (like Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), etc.). Its purpose is to separate the Cyber Polygon from the Untrusted Zone and, hence, to add a layer of security. Users from Untrusted Zone only have direct access to the DMZ, but not to any other "deeper" NSIC's part.

Trusted Zone with the controlled environment after the internal back-end NGFW is designed for internal-exposed systems (like internal load balancing/performance optimization, device testing, and troubleshooting platforms, application services and management, services with limited access to Cyber Polygon's staff only, etc.). Restricted Zone contains Cyber Polygon's high risk and/or mission-critical systems (critical services and servers, Data Center with a knowledge base and other DBs with sensitive data, etc.). Management Zone with Cyber Polygon's assets such as infrastructure services, network devices, traffic telemetry, storage, Data Center with certain computational power and applications supports its centralized functioning, big data processing, virtualization, configuration, changes, patch, backups and IS management, including IS centralized real-time logging, monitoring, reporting, IPTs like NGFW, SIEM and DLP systems, security scanners, analytical tools, regulatory compliance, etc. We propose to design several subzones within trusted and restricted security zones that enable special cases, listed above under the description of their functional components and additional subzone boundary control. Sandbox can be regarded as an isolated highly controlled quarantine (a specific example of virtualization), which is used to analyze unknown users' behavior, activity in the CPU of sandboxed hosts and its execution flow at the assembly code level or unverified programs with possible viruses, malicious code or targeted attacks evaded traditional signature-based defense. The main aim is to see if something triggers anything beyond what was normally expected. Hence, in the Cyber Polygon, sandbox appliances support a safe and sheltered environment, where the behavior of processes, programs, memory, files, file descriptors, file system space, unknown users, etc., can be carefully and constantly observed without compromising the entire Cyber Polygon. Bearing in mind this infrastructure of the Cyber Polygon, we will further describe the site design at MEPhI for its implementation for educational purposes.

FIGURES

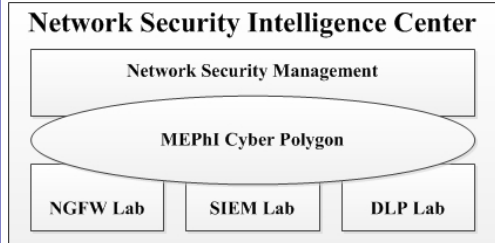


Fig. 1. MEPhI Cyber Polygon in the NSIC infrastructure

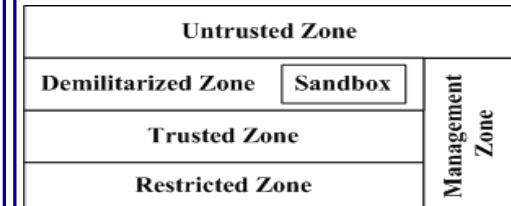


Fig. 2. Cyber Polygon's security zone infrastructure

CONCLUSIONS

After a detailed study of the issue put at the beginning, it is obvious to us that creating a cyber polygon for educational purposes is the urgent need of today for any university, teaching network security. As is clear from the paper, the experience of its wide practical use is not yet available, but soon we hope to get results that we will definitely share with the public. Based on this study, the following features of cyber polygons can be distinguished:

- ✓The use of cyber polygons is an educational process, not a show;
- ✓They must fill in the gaps in technical and organizational knowledge;
- ✓They should provide an opportunity to look at attacks from different angles: both attacking and defending;
- ✓They should give an experiment with IDPSs and IPTs;
- ✓They should provide reasonable metrics for assessing network security.

✓The next steps in improving the existing MEPhI Cyber Polygon are to develop the widest possible set of typical scenarios of the studied network attacks, as well as various scenarios of its use for students to learn how to counteract network attacks and respond to IS incidents. After this, it is advisable to start using samples of not only widely used at present but also promising systems in the educational process. As the MEPhI Cyber Polygon is being improved, the creation of a project and regulations for connecting it to the FEPU will be required. In addition, the development of the short-term professional refresher courses for obtaining additional professional competencies and retraining programs for developing trainees' competencies related to a new type of professional activity is seen as a necessary direction. And in a more global perspective, the MEPhI Cyber Polygon's infrastructure already tested in practice may be of interest as a promising software and hardware platform for the deployment of competency assessment centers for network security.