An ideal Internet Early Warning System

Dominique Petersen and Norbert Pohlmann
Institute for Internet Security
University of Applied Sciences Gelsenkirchen
{petersen, pohlmann}@internet-sicherheit.de

Abstract

Today, many manufacturers advertise that they have developed the one, ultimate Internet Early Warning System (IEWS) which shall protect the customers from all the dangers on the Internet. But what does an ideal and global Internet Early Warning System need in reality? In this article, a model for the early warning is constructed and it will be shown which components need to be protected and why an early warning can only work through collaborative approaches and a variety of systems. Then some of the current research work done by the Institute for Internet Security are outlined in the area of Internet Early Warning.

1 Introduction

With the theme "Internet Early Warning Systems" in the same breath the statements are often that the critical infrastructure protection (CIP) is very necessary and a primary goal of the state is to enforce this with all technological means. In addition to the transport-, energy-, financial- or service-area also the Internet - as we know it today - is a critical infrastructure. According to the assessment of the state this critical infrastructure must be protected.

To achieve this goal it is necessary to protect the functionality of the Internet and to keep it alive. As the Internet consists of many Autonomous Systems (AS), which are connected together, special attention must be paid to the protection of the individual sub-systems of this infrastructure [1].

1.1 Relevant aspects of the early warning

Here, two aspects are crucial. Firstly, it is important to identify threats as early as possible to reduce possible damage or at best even eliminate all harm. The

containment and avoiding the damage here depends upon successful detection very much on the initiation of potential countermeasures. Secondly, it is necessary for the respective infrastructures to be adjusted and improved, so they are prepared for future requirements.

1.2 Threat scenarios

Currently, five different types of threats are distinguished and important on the Internet. In a DDoS (distributed denial of service) many requests and intense traffic is generated from multiple distributed sources, so that the narrow-band target enters an overload situation and is not longer available for a normal use. Depending on how quickly the DDoS is done: in an emergency only seconds remain for an early warning.

Another threat are exploits, that exploit current vulnerabilities in software of operating systems. In networks where the exploits occur for the first time, an early warning of single network packets is almost impossible. Depending on the degree of diffusion speed and aggressiveness of the exploit yet unaffected infrastructures could get timely warnings. Again, the time for the early warning consists of only seconds in the worst.

Malware is currently one of the most invasive threats in the Internet. Systems infected with malware automatically try to attack other systems and redistribute themselves this way. How quickly this happens depends on the design of the malware. For an Early Warning System this means that the time for a warning can be a few minutes to several days.

An equally serious threat are botnets. Sometimes they consist of hundreds of thousands of systems controlled by a unnoticed botnet and execute commands, such as a DDoS. To identify which targets are attacked at which time, it is necessary to observe the communication of the botnet and to analyze it. The time for an early warning is here defined by the communication rate of the botnet and its structure and moves within a few minutes.

The last major threat scenario is made possible by the Internet routing. It has happened in the past that wrong distribution of IP prefixes were made in the routing, and so entire Autonomous Systems, and therefore also the entire traffic to these networks, diverted to other countries. Here, the early warning time also depends on the distribution speed of routing and is only a few minutes.

1.3 Response time for early warning

Considering the threat scenarios is clear that in general very little time for an early warning is available, and that all components involved must respond as quickly and efficiently as possible. In many cases it is impossible to issue a warning before

the actual and concrete attack is launched. It will be easier however, if a warning of a potential threat is issued. Especially for a collaborative future Early Warning System infrastructures participators could be informed in time to avert possible damage.

2 Definition of an Internet warning system

Based on the basis of the goals, to improve the Internet and its infrastructures in terms of safety and reliability, and to generate a continuous situation overview of the IT infrastructure, which is carried out in cooperation with public and private partners in the sense of a collaborative early warning, a definition for a Internet Early Warning System could be as follows: Based on reliable results and results from threats or in the event of IT security incidents that affect only few infrastructures yet, an IT situation overview is continuously updated, and when an adequate and relevant incident occurs, a qualified warning to potentially affected is disseminated in order to reduce the potential damage caused or avoided altogether.

2.1 Mandatory functional requirements

An Early Warning System therefore needs a set of functional requirements: The intrusion detection must be done at a time before concrete damage occurred and early enough to minimize potential damage. Here it is important to consider both, already known and unknown, attacks are detected.

The decision-making process and the development of countermeasures have to be supported. This can e.g. performed by analysis tools and results visualization. Expert systems will help in the decision making here. Ensuring and collection of evidence for forensics must be guaranteed in order to perform legal prosecutions later.

The current status and the development of the Internet traffic must be monitored constantly. Questions, how the infrastructure needs to be extended or which technologies increase or decrease of importance in the future, are important here.

The current IT situation overview along with an overview of all security events must be generated continuously. Here, appropriate visualization methods help for the situation analysis. Other requirements follow directly from the fact that the Early Warning System itself needs to be protected. The stability and the security of the system against attacks, maintaining the privacy, the maintainability and the performance all are relevant aspects.

2.2 Asymmetric threats

Another problem is the asymmetric threats. Many attacks are carried out globally and are not aimed at a specific location. The best example illustrates a distributed denial of service attack (DDoS).

The response to a security incident occurred is currently initiated only locally and therefore concerns only the particular infrastructure which acts against these threats. All victims of a global attack must therefore execute the same or similar reactions and counter-measures to reduce the damage or avert all harm. The total cost is thus multiplied almost to the number of victims and the relevant countermeasures.

Target of an Internet Early Warning System must therefore be to initiate effective responses to incidents for all partner systems, and this preferable in an automated manner.

3 Structure of an Internet Early Warning System

Based on architecture and requirements of the particular operating company a model for an Early Warning System can be set up (see figure 1). Foremost, the system is defined by the targets that are to be achieved.

Equally important are the legal settings and conditions, in which the whole early warning is performed. Depending on how the legal conditions in the state and the company look, the Early Warning System can have more or less restrictions. Relevant here are mainly the privacy standards that need to be adhered to, the protection of the trust and the respective contract law. Not infrequently, the legal framework defines the possibilities of an Early Warning System to achieve the required goals.

Afterwards the respective company or organization, which is operating the Early Warning System, and the partners involved (concerned organizations) determine the model. The partners here may assume two different roles, active and passive. In the active role the participants are involved in the establishment and operation of the Early Warning System, e.g. by providing sensors, operating a situation awareness room or by the creation and execution of countermeasures. Passive participants consume almost all the information provided by the other Early Warning Systems. Frequently, these are home users and small businesses.

The operator of an Early Warning System usually has a precise definition of the organizational units with their respective relationships and clearly defined responsibilities. In order to act more quickly, the necessary information flows and possible responses must be clearly agreed. It is important for such a company to

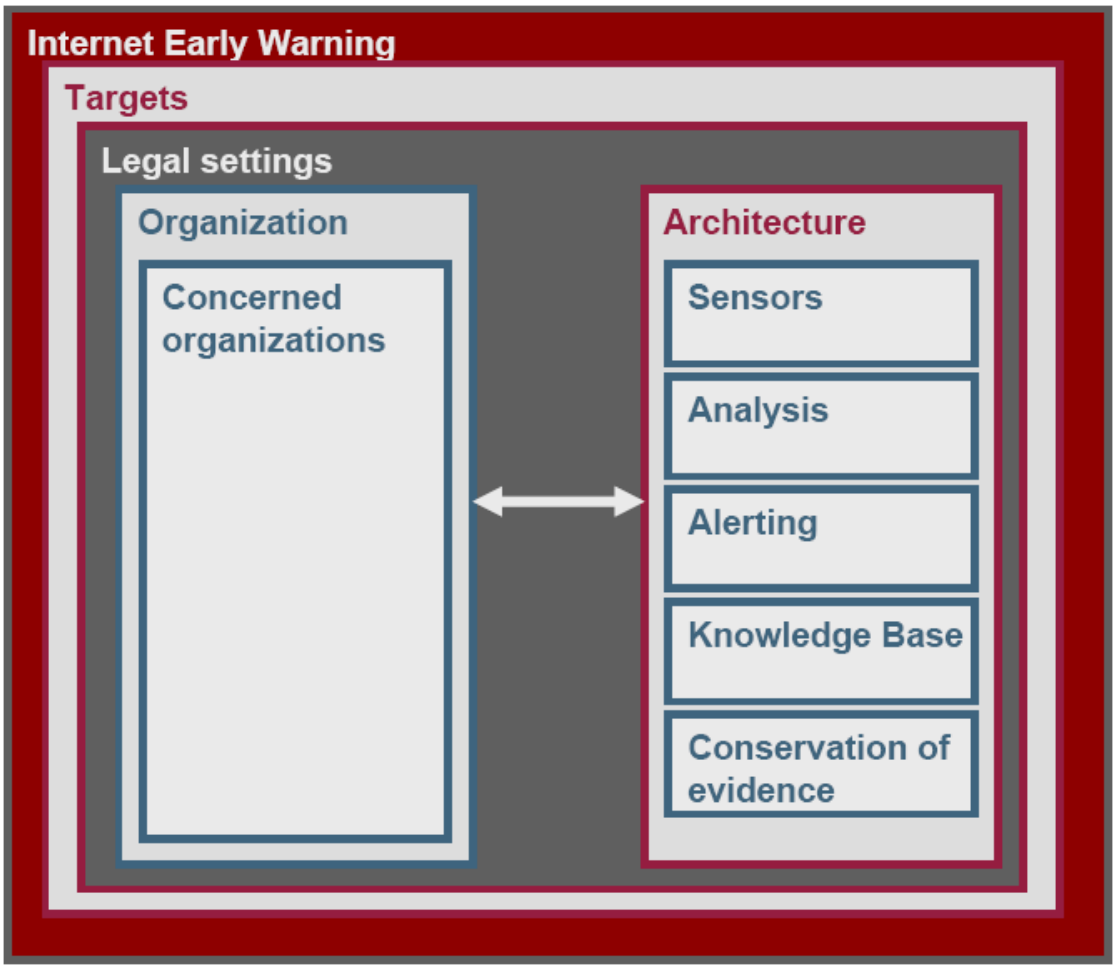

Figure 1: Model of an Early Warning System

have a very short decision process, efficient paths for the distribution of information as well as clearly defined responsibilities to warn and to react in an emergency pretty early.

3.1 Technical Implementation

The architecture inside of the early warning model represents the technical components that need to be implemented. The sensors, which are distributed to each strategic positions in the network to be monitored and set up, collect the data, which form the basis of the current status. The distribution of sensors depends on which parts of the network are critical how representative the index shall be. Several types of sensors have already been developed. It is possible to use sensors

that create a map of the total traffic, such as flow data, packet-based statistics sensors, honeypots, log and availability data or approaches that capture all traffic.

Especially with the sensors used, it is extremely important to pay attention to both, the privacy protection and the preservation of evidence. This can be achieved by methods of pseudonomisation and anonymisation. Nevertheless, it must be ensured that for the particular operation area the ideal sensors are used. For example the DE-CIX, the world's largest commercial Internet exchange (CIX) point has a peak traffic of 1.8 Tbit/s. The analysis component of the sensors must therefore be very powerful, if not the included information will be strongly reduced. Alternatively, the use of sampling can be applied, wherein in a certain time or after a certain number of packets flown through the network only a sample is taken from and then evaluated.

3.2 Core of an Early Warning System

The analysis and recognition module (Analysis) is the core component of an Early Warning System. It is responsible for identifying security incidents and to transmit these in form of alarms. In order for the threat detection works, a number of technical components is necessary (see figure 2, [2]).

The measured data of the installed sensors are sent to the signal layer. The data is then filtered for relevance and analyzed. In addition, here is the detection of abnormal and safety incidents, such as with misuse detection and anomaly detection methods. These algorithms generate events that represent a particular occurrence and include information that contributed to the construction process.

These events will now be passed to the event layer, where they are correlated. It is advisable to include more information about incidents or security flaws from external, non-technical sources (e.g. CERT's) in order to make a better conclusion. If the analysis concludes that the individual events are not only an anomaly, but a specific incident or particular threat, an alarm will be generated and forwarded to the responsible person in the company.

The biggest problem in identifying is firstly the vast amount of data that must be analyzed. On the other hand, the big challenge is to identify previously unknown attacks and slowly evolving trends.

To further improve the detection method, an Early Warning System has always a learning component (element). Using the information returns from the events and the results from the event layer, the algorithms are adjusted adaptively. For example, some algorithms that monitor network traffic have to be adjusted after a new service has been added, which was not previously known. The results from the learning component flow as modeled findings in the knowledge base.

Another important aspect implements the knowledge base. It contains the knowledge about the environment in which the Early Warning System is used as

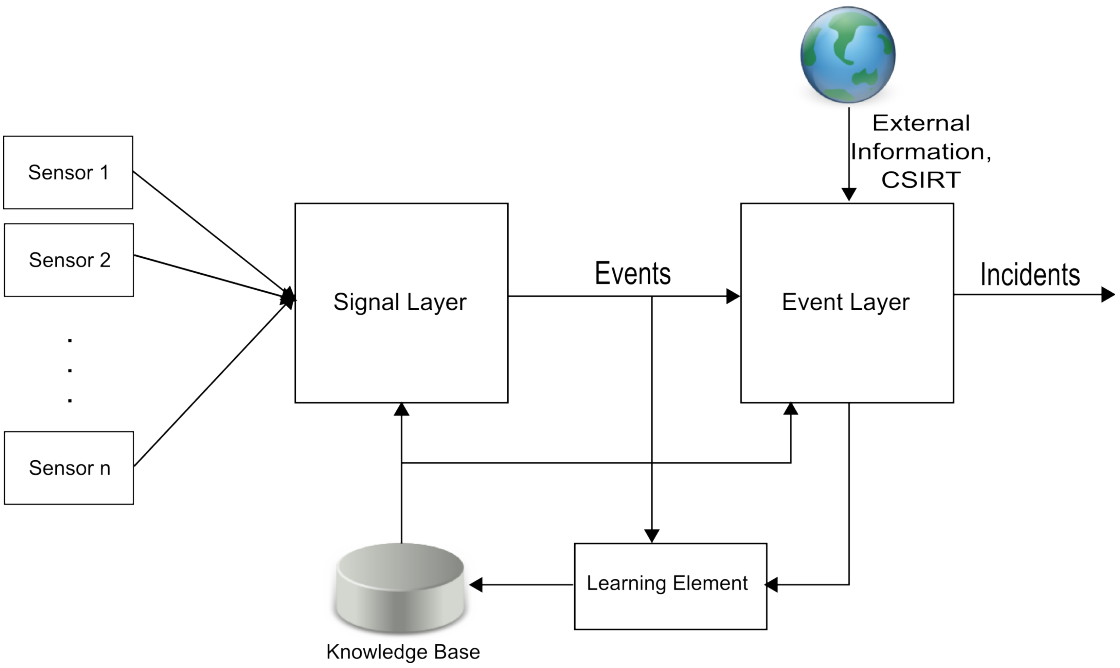

Figure 2: Technical components of the detection methods

well as information about the normal behavior of the network and attack signatures. Ideally, there are also concrete countermeasures regarding certain, already known incidents and practices when problems occur in the knowledge base. So they can really help and be supportive, the contained data must be always kept current. This can be achieved e.g. through the automatic generation of virus and attack signatures, updating the normal state of the network traffic or functioning processes to solve previously unknown problems.

The challenge with this is the continuous acquisition and storage of knowledge. As part of an expert system, the knowledge base does not only provide information for the solution of well-known problems which are available, but also provides intelligent support when editing unknown incidents in which they propose similar events and suppression instructions.

3.3 Legal consequences

If a concrete attack was detected at various levels of the recognition process and ideally successfully repelled, it is about to call the criminals legally and financially to account. To have a chance in the digital age at the court, the conservation of evidence must be carried out consistently and trustworthy.

All information about the attacker are important, his approach and the damage that the attack caused. Also these two important aspects are to be kept for further use. On the one hand, the privacy protection laws (policies) must be followed, i.e. the access to the stored data must be restricted and linked to a specific detected incident. This is to protect personal data against misuse. On the other hand, the authenticity of the evidence can be ensured by making tempering technically impossible.

3.4 Overall architecture of the Ideal Early Warning System

The previous explanations help to identify a number of important aspects that significantly determine the overall architecture (see figure 3).

For instance, even at the local systems the incident management and the countermeasures are defined by different rules. In addition to that, due to the different environments, not every countermeasure can be applied to any network. Moreover, in several countries, there are different legal frameworks which must be observed.

If a threat is detected in a situation awareness room, it is important for an early warning to communicate the threat description to all participants involved, and this preferably faster than the spread of the attack. Finally, it's the Early Warning System itself which has to be robust in order to perform its actual task.

In order to respond to the threats today it is needed to act globally and collaboratively. Large enterprises and governments need to operate sensors throughout the Internet and analyze this data locally. If incidents are identified, that must be as soon as possible spread to both active and passive participants involved by an efficient information distribution network. Also, certain countermeasures must be carried out collectively within the early warning participant network.

Also important is a distributed knowledge base, in which already occurred incidents are stored and can be accessed by all partners for a quick and ideal response.

4 Developments of the Institute for Internet Security

The Institute for Internet Security - if (is) of the University of Applied Sciences Gelsenkirchen has been working for more than seven years of applied research of Internet Early Warning Systems. Within this project several technical implementations have been developed, of which three selected projects will be presented.

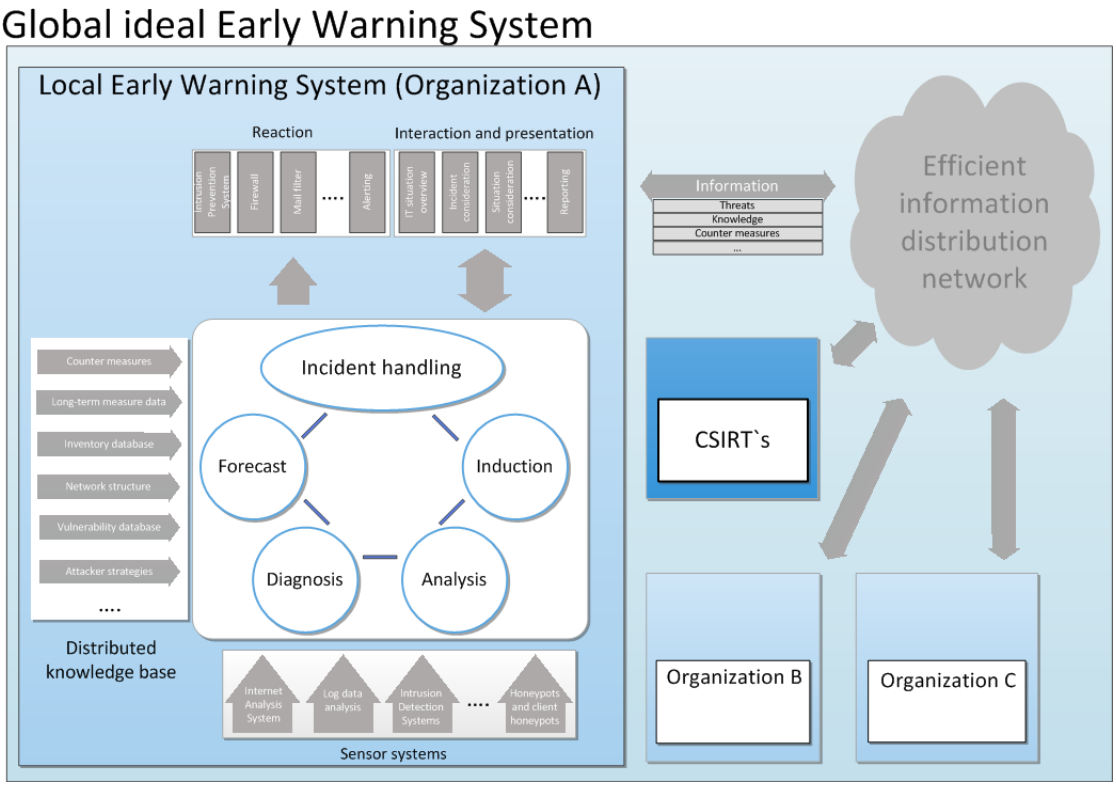

Figure 3: Structure of a global, ideal Early Warning System

4.1 Internet Analysis System

Using the sensor-based Internet Analysis System (IAS), which was developed as a research and development project of the if(is) in collaboration with the Federal Office for Information Security (BSI), local and global overviews can be created and analyzed in order to generate early warnings ([3]). The Internet Analysis System provides the core component of the Internet Early Warning Systems of the if(is) ([4]).

Special key aspects of the project are a privacy-friendly collection of network information and optimizing the amount of information data to store long-term, thus to enable the analysis of trends and developments over long periods.

4.2 Goals and objectives of the IAS

The task of the Internet Analysis System is on the one hand the analysis of local communication data in defined subnets of the Internet (networks), and on the

other hand the creation of a global view ([5]) on the subnets or the whole Internet with the help of combining the many local views by the network operator ifself or an independent party, such as the Institute for Internet Security.

The functions of the Internet Analysis System can be divided into four sections: Build-up of the knowledge base, description of the current status, alerting, and forecasting.

The main task of building up the knowledge base is a comprehensive analysis and interpretation of the communication parameters of the Internet traffic with the goal of discovering technology trends, relationships and patterns that represent different states and views of the Internet. Based on this knowledge base anomalies are found with actual measurements and reasons for the state changes which are analyzed and interpreted. This happens, inter alia, with methods of artificial intelligence (AI) such as probabilistic neural networks (PNN), which can be implemented on graphic processing units (GPU) ([6]). It is important to find out whether the state anomalies are of natural origin, such as through a technology change, or whether a malicious attack is responsible. If such a malicious attack is present, the patterns can be identified which characterize the attack, in order to detect these faster in the future.

By the exact knowledge of the current state of a communication line and the aid of historical, i.e. previously collected information from the knowledge base a warning message will be generated, if there are are significant changes in traffic or communications data. After that measures can be taken to protect and preserve the functionality of the Internet.

Another important function is to show the status with a visual representation of the state of the Internet, similar to a weather chart or traffic jam map. It is important to make urgent decisions - especially at risk - easier and faster than ever in order to explain complex issues to a third party. Here, it is not only warned of dangers, but also the positive situation when the monitored networks are alright is illustrated. In addition to a simplified view of complex structures the visualization system must be supportive in order to signal anomalies, such as spam attacks or malicious malware attacks, early enough so that preventative arrangements can be taken and risks can be minimized.

By studying and analyzing the collected data from the IAS, the technology trends, the relationships and the patterns, it is possible through a process of evolution of the results obtained, to make predictions about changes in state of the Internet (e.g. with the help of neural networks). In this way, attacks and major changes can be identified pretty early to forcast damage effects and capacity bottlenecks.

4.3 Functionality of the IAS

The Internet Analysis System consists of sonsors, which passively tap the network traffic of communication lines of different networks and count communication parameters on different levels of communication (OSI model). In an evaluation system the communication parameters are evaluated from different perspectives and displayed well-arranged.

In order to deliver results for a meaningful situation overview, the Internet Analysis System requires a very large amount of raw data, i.e. many counters of different communication parameters on all communication levels (OSI layers 2 to 7). All analyses, which the evaluation system performs, are based upon these raw data.

The sensors can send the raw data to one or more evaluation systems. Each organization is able to monitor their communication with the Internet and perform their own analyses with its evaluation system. To achieve a global and representative view of the Internet, sensors have to be placed in different types of networks, such as Global Tier One providers, transit providers, Eyeball Internet Service Providers (DSL providers), content providers and large enterprise networks, as well as in different regions.

4.4 FIDeS as intelligent correlator

The Institute for Internet Security was involved in another research project called FIDeS (Early Warning and Intrusion Detection System on the basis of combined methods of artificial intelligence), which is primarily a smart event correlation.

Intrusion Detection Systems (IDS) are widely used to protect corporate networks. Because they detect attacks against computer systems, among other things, they help to discover the theft of important corporate know-how and to stop this. These systems, however, currently still suffer from two major problems: First, they work mostly signature-based and can therefore only detect attacks that are already known and for which a signature exists. The second problem: Due to the high false positive rate and the mass of the resulting events provided by these systems, security managers are not able to process all events sufficiently.

In order to identify the attackers, a huge and ever-growing expertise is needed. Only in this way related scenarios can be taken to events together and correlated with other information such as vulnerability or inventory databases. FIDeS want to solve these two problem points based on past research projects and new ideas, to help security managers in their daily work. The aim is to improve the intrusion detection and the subsequent forensic analysis. If possible even predictions shall be taken to prevent critical incidents from the outset. Using these results, information can then be analyzed across the enterprise in order to detect attack scenarios, that

may not have been noticed in one location, but maybe on a larger scale.

4.5 Technical implementation of FIDeS

FIDeS uses as many well established and standardized open-source systems and open formats for data exchange as possible. Thus, further sensors or other components connected to the base architecture can be implemented with any programming language. The core sensor used here is the privacy-compliant Internet Analysis System.

The focus at FIDeS is the user who should to be supported in his daily work, the monitoring of the security situation. For this reason, special attention is given to the user interface. Large amounts of information can thus be detected quickly and intuitively, in order to take decisions for actions in time.

Current technologies in the field of Web 2.0 help for this purpose in making the system easy to handle and well configurable.

4.6 iAID with flow-based detection for very high Internet connectivity nodes

In the research project iAID (innovative Anomaly- and Intrusion Detection) an innovative anomaly detection and a new generation of IT Early Warning System shall be realised, which has a high recognition rate for threats, taking current privacy protection aspects into account, and shall be able to also analyze large quantities of data in real time. It will be investigated, how it can respond appropriately to threats using information fusion and creation of taxonomies of anomalies.

It must be developed a suitable way of collecting information about the network traffic. This is to fulfill the three properties: Highly detailed description of network traffic at all layers of the communication stack, resource-efficient collection and storage of useful meta-information from the communication data and observing and complying with privacy protection issues.

Once an optimal information collection system was implemented, in the next step a methodology for the evaluation and classification is developed. The focus here is to reduce the number of messages.

An important component of the new anomaly detection system (or Early Warning System) will be a feedback module, which will allow the analyst to review the decisions of the anomaly detection system and thus improve future decisions.

Thus only major anomalies to reach the administrator, an intelligent filter use the feedback of the analyst to filter out all flows or anomalies, which have similarity to those who were considered unimportant. The filter shall also use methods of artificial intelligence to perform this classification.

5 Summary

This article has presented the importance of Internet Early Warning regarding current threats and how much time there is to protect the infrastructure in case of an attack.

Furthermore, a definition of an Internet Early Warning System was described and demonstrated the functional requirements.

Based on the definition and requirements the structure and the technical realization of such an Internet Early Warning System have been carved out. Finally, it was shown what an ideal Internet Early Warning Systems should contain.

The article was rounded off with the presentation of three projects in the area of early warning, which the authors have realized in the recent years.

References

[1] Sebastian Feld, Tim Perrei, Norbert Pohlmann and Matthias Schupp, *Objectives and Added Value of an Internet Key Figure System for Germany*. In Proceedings of the ISSE 2011 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2011 Conference, 2011.

[2] Sascha Bastke, Mathias Deml and Sebastian Schmidt, *Internet Early Warning Systems - Overview and Architecture*. In 1st European Workshop on Internet Early Warning and Network Intelligence (EWNI 2010), 2010.

[3] Malte Hesse and Norbert Pohlmann, *Internet situation awareness*. In eCrime Researchers Summit, 2008, 1–9., 2008.

[4] Dominique Petersen, Kilian Himmelsbach, Sascha Bastke and Norbert Pohlmann, *Measuring and warning*. In kes – Professional journal for information security, issue 5/2008, 2008.

[5] Norbert Pohlmann and Marcus Proest, *Internet Early Warning System: The Global View*. In ISSE 2006 Securing Electronic Business Process, Vieweg, 2006.

[6] Sascha Bastke, Mathias Deml and Sebastian Schmidt, *Combining statistical network data, probabilistic neural networks and the computational power of GPUs for anomaly detection in computer networks*. In Workshop Intelligent Security (SecArt 2009), 2009.