IT early warning systems – State-of-the-art and promising approaches to increase resilience of critical infrastructures

Martin Brunner

Fraunhofer-Institute for Secure Information Technology - SIT

Department Secure Processes and Infrastructures - SPI

Schloss Birlinghoven 53754 Sankt Augustin, Germany

Corresponding author: Martin Brunner; martin.brunner@sit.fraunhofer.de

IT early warning systems – State-of-the-art and promising approaches to increase resilience of critical infrastructures

Abstract: Modern societies heavily depend on efficient information and communication technology (ICT) infrastructures. Due to the interdependencies between critical infrastructures and the underlying ICT malfunctions in ICT can cause cascading effects seriously damaging public life. At the same time the evolution of malware is proceeding rapidly so that the time between detection of vulnerabilities and reaction is reducing precisely. Response handling is still done by humans who can not keep up with the high processing rate of (attacking) computer-based systems. Hence the need for automated response including early warnings of emerging trends and hazards increases. This paper describes the need for IT early warning systems and provides an overview on general concepts and efforts regarding IT early warning. In this context four approaches are discussed in detail: Internet Worm Early Warning System, CarmentiS, Internet Analysis System and Agent based Early Warning System. Based on the close look at these four approaches future challenges for research and development are proposed.

Keywords: early warning system, critical infrastructures, intrusion detection, honeypots, malware

1. Introduction

Nearly all fields in modern societies, from private households to government agencies, heavily depend on efficient information and communication technology (ICT) infrastructures. Thus ICT systems became part of critical infrastructures. But the high-grade cross linking of ICT instances leads to unpredictable side-effects. In addition the extension of technical mono cultures causes an increasing vulnerability of ICT infrastructures in general. Further issues are the complexity of ICT systems (black box behaviour) as well as the human factor. Due to the interdependency of ICT systems and other critical infrastructures malfunctions in ICT could cause cascading effects damaging public life. So far the development of malware lead from exploits addressing one specific

vulnerability to polymorphic worms interconnected to botnets which become more and more sophisticated including the ability to adapt their attacks against various target systems. As an effect of this trend the time between detection of vulnerabilities and reaction is reducing precisely. This permanent race between attack and defence is aggravated by easy to use exploitation frameworks which bundle a number of exploits and payloads. It is assumed that this trend is going to intensify in future. It has to be stated that the response handling is still done by humans who can not keep up with the high processing rate of computer-based systems. Concurrently the security consciousness does not seem to keep up with the rapid technical progress. Furthermore every operator of an ICT infrastructure has simply his own local point of view. As a logical consequence attacks ironically must be faced using ICT systems, which in turn might be prone to errors again. Otherwise response will not be possible any more sooner or later. Territorial borders are blurred in this context. Hence a holistic state-of-the-art considering many (not necessarily ICT specific) factors must be done in order to make adequate statements regarding upcoming hazards. This is what future IT early warning systems (EWS) are expected to do.

2. Generic concepts for IT-EWS

The idea of integrating early warning to ICT systems is not new what is indicated by the appearance of national monitoring services like CERT networks. Due to the continuously increasing number of discovered vulnerabilities it is assumed that CERTs will be unable to handle them in the foreseeable future. Accordingly several stakeholders in and beyond Germany started dealing with the issue of IT early warning in the last years. Thus various ideas, concepts and initiatives have been already emerged taking the specific view of the stakeholders into account. They spread from focusing on a specific problem up to holistic concepts including existent organisations. Such efforts tend to cover different approaches depending on the stakeholder. To name just a few:

- Anti-Virus Information & Early Warning System (AVIEWS) [AVI02]
- Cooperative Intrusion Detection in dynamic Coalition Environments [JAH06]
- A National Early Warning Capability Based on a Network of Distributed Honeypots [HOE05]
- DShield [SAN00]
- Honeynet Project [1]
- CAIDA (Cooperative Association for Internet Data Analysis) [2]
- MyNetWatchman [3]
- Lobster [4]
- NoAH (Network of Affined Honeypots) [5]

In general efforts dealing with IT early warning aim at (global) analysis networks and distributed (intrusion detection) sensors. Thereby data is analysed locally focussing on several aspects and the results get transmitted to a central instance. Approaches often differ regarding

- design and integration of the IT-EWS infrastructure (e.g. VPN, encryption and transmission in packet headers, JIAC),
- usage of intrusion detection technologies and
- implementation of sensors (e.g. transparent proxy, IP-less bridge, interacting agents).

Furthermore there are interdisciplinary approaches concerning the operating mode which are often taken over from other sciences [BIT05], [BSI06]. That is amongst others the implementation of several warning levels (radioactivity), classification of events by space and time into ranges (medicine) as well as the question how to verify the extracted data (synoptic, syntactic). Moreover

1 http://www.honeynet.org
2 http://www.caida.org
3 http://www.mynetwatchman.com/
4 http://www.ist-lobster.org/
5 http://www.fp6-noah.org

the measurements could or should be made in several levels, like continuous (automatic) measurements, regularly measurements according to schedule or event-related measurements. Early warning (also in other fields) is based on exceedance of defined thresholds. Many known approaches for IT early warning systems focus on distributed, cross-linked sensors using intrusion detection (IDS) technologies. Manufacturer of IDS products are aware of this, too and start to use novel technologies in their products like fuzzy logic, neural networks or artificial intelligence claiming to provide protection against unknown attacks. Some outstanding examples are:

- Panda Software TruPrevent Technologies
- Behavioural DoS Protection System [RAD06]
- Non Intrusive Learning Patterns (NILP) [6]
- Mind-IDS [7]

3. Existent approaches for IT early warning systems

The following sections describe four selective approaches for IT early warning systems. Each of them aims to cover one or more aspects of IT early warning. One reason for having a detailed look at them is that they are well documented and the information is publicly available. None of the approaches is an available piece of software yet, but all of them have been developed especially to realize early warning for ICT systems.

3.1 The Internet-Worm Early Warning System (WEW) [CHE05]

focusses on TCP-based worm spread in order to derive an early detection of emerging hazards caused by worm activity. The analysis is based on specific characteristics which indicate worm activity by differing from the behaviour of a typical user profile. A worm generates a consistent

6 http://www.mwti.net/Microworld_press/MicroWorld_releases_new_version_of_eScan_Corporate.asp
7 http://www.mind-ids.org/

stream of connection failures at different hosts in a short period of time for example. Further the number of scan sources rises exponentially with an increasing number of infected hosts (worms usually scan the whole address space). Thus a worm eruption can be classified by an increasing number of hosts with an equal behaviour. The architecture of WEW determines to place the sensor at the gateway of a (corporate) network in order to monitor scan sources. Analysis is done via a monitoring station. Outgoing TCP-RESET packets and ICMP-host-unreachable packets indicate connection failures and are used to separate scan sources of worms and the typical user profile. Identified persistent scan sources are managed via a list considering temporary abnormal behaviour. This list can be used for further analysis using honeypots or as blacklist for a self-adapting firewall configuration. However details for providing the warnings are missing. The analysis of worm propagation is based on the following epidemic model:

$$\frac{di(t)}{d(t)} = \beta i(t)(1 - i(t))$$

where

i(t) is the percentage of vulnerable hosts that are infected with respect to time t and

ß is the rate at which an infected host detects other vulnerable hosts.

The reaction time $t(n_0)$ for WEW to warn an ongoing worm is

$$t(n_0) + \Delta t = \frac{N}{r \cdot V} \ln \frac{n_0(V-1)}{V - n_0} + \frac{kN}{\alpha r A}$$

where

Δt is the time it takes WEW to add an entry of an infected host to the list,

N is the size of the (IPv4) address space,

r is the rate at which an infected host scans the network,

V is the total number of vulnerable hosts,

n_0 is the number of infected hosts causing WEW to release a warning,

k is the number of connection failures causing WEW to add an entry to the list,

α is the percentage of connection failures reported by the gateway(s) and

A is the monitored address space.

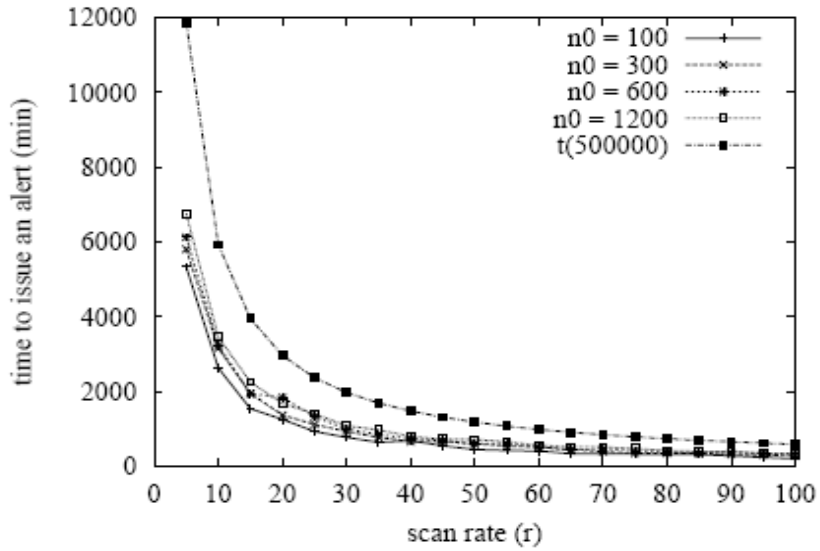

Figure 1: Time it takes WEW to report an ongoing worm attack with respect to the scan rate r and n_0

Figure 1 shows a worm attack with respect to the scan rate r and n_0 and illustrates the reaction time of WEW. The propagation of the „code red“ worm took in this context about 9 hours to infect 250.000 hosts. This approximately corresponds to the point at r=65/min. The point at t(500.000) is the time it takes the worm to infect half of all vulnerable hosts. Regarding to the statement in [CHE05] it takes WEW about four hours from the start of the worm attack to issue a warning when less than 1000 hosts are infected. WEW would further have a list containing many of the infected hosts.

3.2 CarmentiS [CER06]

was emerged from the „National Plan for Information Infrastructure Protection“ in Germany and is intended to be a sub project for a national IT early warning system. Teams of the German CERT-

network are testing the (organisational) base infrastructure for an IT early warning system. The approach focusses on the combination of meta data extracted from (technical) sensor networks in order to provide a cross-organisational platform for the analysis of arbitrary information sources. Therefore collected sensor data (e.g. extracted from IDS) are combined with further information like advisories and prepared for the corresponding stakeholder using adequate interfaces that consider the recipients specific point of view. The approach described in [CER06, p. 21ff] is based on the following idea: Organisations usually have only a local view on the status at their networks, but they don't know what is happening outside. To extend this point of view participants send data that might be interesting for others to a third, independent party. The so called CarmentiS-central, which acts as this third party, provides the necessary functions for receiving data, controlling the analysis and preparing the result for the corresponding stakeholder. It is divided into four components:

- Import Interface and Storage component:

  During import of data particularly privacy aspects, several data sources and the amount of the handled data is considered. Therefore the format used by CarmentiS for data exchange supports the definition of meta information (e.g. export policy for a specific partner, sensor configuration) and in addition state of the art authentication and encryption mechanisms.
- Main Analyze Component:

  The data for processing is correlated, analysed based on selectable profiles and either interpreted automatically or by analysts. Alarm messages are generated using incident response tools like SIRIOS[8].
- Analysts Workbench:

8 http://www.sirios.org/

The interpretation is done via a web front end, which provides several views of the data (including data of other analysts) by accessing the various databases in order to detect known attacks and new trends. Furthermore the front end includes functions for providing warnings and advisories. In addition the sensors can be updated.

- User Workbench:

  The results of analyses will be published on a web portal in future considering the point of view of various stakeholders.

Privacy concerns, which occur during operation of an IT early warning system, are met by separating the sensor data into connections and attacks. Connection data must fit a defined policy. Only data that were classified as attack data will be further analysed. Additionally the sensor data (respectively the source) are cryptographically pseudonymized. So CarmentiS claims to be the first project allowing CERT-networks a common analysis of sensor data. Extensions allowing efficient early warning using the base infrastructure are planned. This includes currently (march 2007) the combination of IDS data and net flow or the extension of automated analysis using thresholds and statistical methods.

3.3 The Agent-based Early Warning System [BSU06]

was developed in the DAI-labor of the Technical University of Berlin in order to detect emerging problems, generate warnings and share them with other critical infrastructures. The architecture of A-EWS focusses on networks as well as on particular hosts. A-EWS deals mainly with the technical aspects of IT early warning including the detection of attacks. Privacy aspects are expected to be handled basing on the results of the technical considerations. The basic idea is to treat incidents not only locally but also to inform further networks and infrastructures. Hence this architecture does not provide immidiate advantages for operators of A-EWS regarding the defence of attacks but

improves the security of other critical infrastructures by exchanging information. This contributes to an improvement of security of the entire critical infrastructures. The Agent-based Early Warning System is intended to be a network consisting of distributed sensors which forward their analysed data to a central instance. The deployed sensors are placed in various critical infrastructures like telcos, traffic systems, water- and energy supply and public administration. Sensors are represented by agents that use services for the interaction with A-EWS. There should be several types of sensors in an A-EWS which can be implemented as wrapper for common security products or as honeypots. Additionally the authors of [BSU06] focus their research on three further types of sensors:

- Anomaly sensors:

  These are (currently) used for monitoring particular hosts. There are two approaches for anomaly detection. On the one hand so called self organisation map (SOM) algorithms are used in order to learn the "typical" behaviour of hosts. There specific properties of systems are measured whereas their behaviour should not diverge significantly from the typical behaviour (e.g. The host should be used by one person only). On the other hand host based artificial immune systems (AIS) are used. Both approaches focus on the same specific properties and can monitor a host simultaneously. The results of SOM and AIS get correlated in so called supervisor agents. In order to determine the threat level of a host also the results of neighbour hosts are considered. Thus supervisor agents represent the anomaly sensor for a critical infrastructure, whereas their results could be forwarded to a global A-EWS system again. But this sensor type allows only the detection of attacks that have already taken place. Furthermore the significance concerning the global threat status is negligible for attacks on a low number of hosts.
- Sensors for network analysis:

Observations on network level allow the detection of emerging attacks before they have reached their target (completely). One the one hand this can be reached by simply monitoring the net flow and allows the detection of DoS-attacks. On the other hand this approach can consist in analysing the payloads in order to identify (known) signatures of malware, whereas privacy aspects have to be notably considered. Analysing traffic between every possible server and router seems to be impracticable from the technical point of view. Further is has to be considered that the performance of the corresponding critical infrastructure does not suffer from the analysis.

- Sensors for detecting attack patterns

  can be used for monitoring particular hosts as well as for monitoring network segments. They are primarily deployed to detect advanced attack techniques, which pass several steps. As a result every step causes certain effects (e.g. IP-fragmentation). Such sensors offer a formal description language for particular steps and their effects.

Locations where the sensors should be placed must be found using adequate placing algorithms. Further it has to be found out if/how sensors should be communicating among each other and how to handle privacy aspects. The implementation of A-EWS is intended to be done using the JIAC-frameworks [FRI01] which already provides various requirements regarding the architecture of such a system. The organisational handling is widely open in this approach as well as the incident handling.

3.4 Internet Analysis-System [PET06]

The R&D-project “Internet Analysis System” (IAS) - which was developed by the Institute for Internet Security at the University of Applied Sciences in Gelsenkirchen in cooperation with the Federal Bureau for Information Security (BSI) – is the foundation for an IT early warning system

particularly in combination with the “Internet Availability-System”. IAS deals with the consolidation of several local views of networks to a holistic (global) view of the internet in order to generate early warnings based on the analysis of the global data. The architecture of IAS consists in several peripheral sensors, which tap the traffic in defined subnets and one (central) analysing system, which interprets and formats the data considering various aspects. The interface between both components is a so called raw data transfer system, whereas raw data is transmitted via a (specially defined) secure raw data transfer protocol (RDTPs). The functions of IAS include

- pattern generation,
- description of the current state,
- alerting and
- forecasting.

The task of the sensors is information retrieval regarding the state of the transmission line and the network behind. Additionally the amount of necessary information has to be minimized and privacy aspects have to be considered. Therefore a sensor taps the connection passively and counts the parameters of the corresponding protocols on network level. The resulting counter reading is transferred to the raw data transfer system in defined time slices. So a preferably high amount of raw data (many aggregated counter readings of various parameters and communication levels) is necessary in order to produce significant results, because the analysis of IAS is based on that raw data. During the gathering of raw data the incoming packets are successively tapped in their random order. Every packet passes several analysis (depending on protocol) whereas the protocol header of the corresponding communication level is evaluated. Depending on the header information the assigned counters are incremented. As mentioned in [PET06 p.14] the processing time of one packet is less than 1 millisecond. Regenerating the context of particular packets or parameters

respectively (e.g. Sessions) is not possible, because the raw data extracted in this way are simply a statistical modelling of the communication data. Hence privacy aspects are accommodated and the necessary memory requirements are minimized. The analysis of the collected raw data is done in several modules of the analysing system. The modules get their information from the raw data and the corresponding results only. The aim of the analysis consists in the generation of contexts, statistics, profiles and the detection of threshold exceedings. For instance IAS “knows” a certain profile from the past including its standard aviation and is therefore able to derive atypical behaviour. A standalone client is used to prepare the data from IAS, but front ends like pictured visualisations (analog to a traffic jam chart), web clients or PDAs are possible as well. Using IAS transport protocol distribution as well as dependencies between protocols can be illustrated very well. One example is the proportional protocol distribution between TCP and UDP that can be referred to the dependency between HTTP and DNS [PET06 p. 16]. The significance of the data produced by IAS depends essentially on amount and placement of the sensors (type of network, geographical location, etc.). Thus IAS finally depends on the existence of preferably much raw data, which in turn can only be gathered by a high number of partners respectively sensor operators. Getting a better overview on the status of their networks could offer an incentive for potential partners. However IAS does not offer any IDS functionality so malware signatures can not be detected. Hence it is not a replacement of existing security measures, but rather an extension to them. Moreover detailed time data regarding early warning is missing. For instance the theoretical / practical duration until a certain event or trend causes an alert. In [PET06, p.17] is simply stated, problems would be relayed “in time”.

4 Comparison of the selected approaches

The four approaches mentioned above differ in many respects and have often very different objectives. Insofar finding an objective base for comparison is difficult. For the sake of overview the following table lists various characteristics of the four approaches.

Approach for IT EWS	WEW	CarmentiS	A-EWS	IAS
Monitoring of networks	Yes	Yes	Yes	Yes
Monitoring of hosts	-	-	Yes	-
Covered aspects:				
Technical	Yes	-	Yes	Yes
Organisational	-	Yes	-	Yes
Incident Handling	partial.	Yes	-	partial.
Privacy aspects	Yes	Yes	-	Yes
Handling of data amount	-	Yes	-	Yes
Technologies:				
Anomaly detection[9]	Yes	-	Yes	Yes
Attack patterns	-	-	Yes	-
Analysis of network traffic[10]	-	-	Yes	-
„Self learning“	-	-	Anomaly-based	statistical base
Correlation of various:				
Data sources (sensors)	Yes	Yes	Yes	Yes
Data types / formats	-	Yes	Yes	Yes
Results / measurements	available	available	not specified	available
In use	not specified	test mode	not specified	test mode

Table 1: Comparison of the four selected approaches

5. Conclusion

As malware will continue to evolve, IT EWS must be able to do it as well. The existence of several approaches dealing with IT EWS shows, that ICT is understood as part of critical infrastructures by now. None of the discussed approaches is perfect yet, but some of them could complement each

9 relates to (statistical) network based as well as to user based anomalies

10 including analysis of payloads

other in technical and/or organisational aspects. However some issues still require R&D-needs. So far most of the known approaches are missing a solution for incident handling like counter measures in case of attack. This is one of the future challenges. As most of such systems are prone to a undesirable high false positive rate, a further challenge will consist in reducing this. Additionally the most important requirement for an appropriate early warning is that preferably many stakeholders from various fields participate and run a sensor. This concerns stakeholders in economy like ISPs as well as those in research and government agencies including their willingness to share information.

References

[AVI02] „Anti-Virus Information & Early Warning System (AVIEWS)“, URL: http://www.aviews.net/

[BSU06] Karsten Bsufka, Olaf Kroll-Peters, and Sahin Albayrak: „Intelligent Network-Based Early Warning Systems”, Proc. Of Critical Information Infrasturctures Security First International Workshop, CRITICS 2006, Samos Island, Greece, August 31 - September 1, 2006. URL: http://www.dai-labor.de/fileadmin/files/publications/IntelligentNetwork-BaseEarlyWarningSystems.pdf

[BSI06] Bundesamt für Sicherheit in der Informationstechnik: “Tagungsband BSI-Workshop IT-Frühwarnsysteme“, Wissenschaftszentrum Bonn, 12. Juli 2006.

[BIT05] BITKOM: „Ein nationales IT-Frühwarnsystem für Deutschland“ Positionspapier der ITK-Wirtschaft, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 10117 Berlin-Mitte, Stand 1.8.2005

[CHE05] Shigang Chen and Sanjay Ranka: „Detecting Internet Worms at Early Stage“, Department of Computer & Information Science & Engineering Universityof Florida, April 2005, URL: http://www.cise.ufl.edu/~sgchen/papers/JSAC2005.pdf

[CER06] CERT-Verbund: „CarmentiS - Frühwarnung in Deutschland“, URL: www.carmentis.org

[FRI01] Stefan Fricke, Karsten Bsufka, Jan Keiser, Torge Schmidt, Ralf Sesseler, and Sahin Albayrak: “Agent- based telematic services and telecom applications”, Communications of the ACM, 44(4):43–48, April 2001

[JAH06] FGAN: „Kooperative Intrusion-Detection in dynamischen Koalitionsumgebungen“, Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie 53343 Wachtberg, URL: http://www.fgan.de/fkie/fkie_c46_f5_de.html

[HOE05] Cristine Hoepers, Klaus Steding-Jessen, Luiz E. R. Cordeiro, Marcelo H. P. C. Chaves: “A National Early Warning Capability Based on a Network of Distributed Honeypots”, NIC BR Security Office – NBSO, Brazilian Computer Emergency Response Team

[PET06] Institut für Internet-Sicherheit : „Internet-Analyse-System“, Fachhochschule Gelsenkirchen 45887 Gelsenkirchen, URL: http://www.internet-sicherheit.de/ias- summary.html

[RAD06] Radware: “Adaptive Behavioral DoS Protection - Technology White Paper” 15. Jänner 2006, URL: www.radware.com