ERNW
providing security.

ERNW WHITEPAPER 58

INCIDENT HANDLING: FIRST STEPS, PREPARATION PLANS, AND PROCESS MODELS

Version:	1.0
Date:	1/19/2017
Classification:	Public
Author(s):	Dr.-Ing. Andreas Dewald

Matthias Luft
Digitally signed by Matthias Luft
Date: 2017.01.19 20:43:50 +01'00'

ERNW
providing security.

TABLE OF CONTENT

ABSTRACT

The number of IT security incidents in companies is still increasing every year. The impact of the incidents ranges from easy-to-fix infections of outdated clients over compromises of large portions of employees work stations and laptops with Trojans or, as a specialty of the recent years, Ransomware which did compromise the entiry IT environment. In the first place, the severity of an occurring incident is unclear, resulting in stress for all involved persons and thus raising the risk for mistakes to happen. The better a company is prepared for incidents, the better is the chance to resolve an incident as good and fast as possible. To this end, we provide a comprehensible first steps guideline, checklist, seizing and analysis strategies and explain the role and content of preparation plans as well as common incident handling process models.

1 Introduction

The number of IT security incidents we observe in companies is still increasing every year. The impact of the incidents may range from easy-to-fix infections of outdated clients over compromising of large portions of employees work stations and laptops with Trojans or, as a specialty of the recent years, Ransomware like CryptoLocker or Locky. Ransomware infections can result in the compromise of the entire company infrastructure, servers, network devices, VoIP systems and anything else. Whenever an incident is detected, it remains a priori unclear with what kind of incident one has to deal until further analysis provides first results. Thus, such situations put major stress on the involved people, raising the risk for mistakes to happen. The better a company is prepared for incidents in general and the current kind of incident in particular the better is the chance to resolve an incident as good and fast as possible. The preparation must comprise processes, the training of people/teams, and the availability of easy to read and recall documentation, guidelines, and checklists,

1.1 Motivation and Contribution

To support companies in being prepared for IT incidents as described above, in this article we want to provide a comprehensible first steps guideline for the case of an incident, seizing and analysis strategies and explain the role and content of preparation plans as well as common incident handling process models. We also provide a checklist that can be printed or kept on hand in any form and which we usually send to our customers as one of the first steps in an incident handling/analysis case. We believe that this collection of instructions supports companies in quickly performing the necessary steps, not missing important aspects, and not accidentally taking actions that might later hinder the containment, analysis, and resolution of the incident.

1.2 Outline

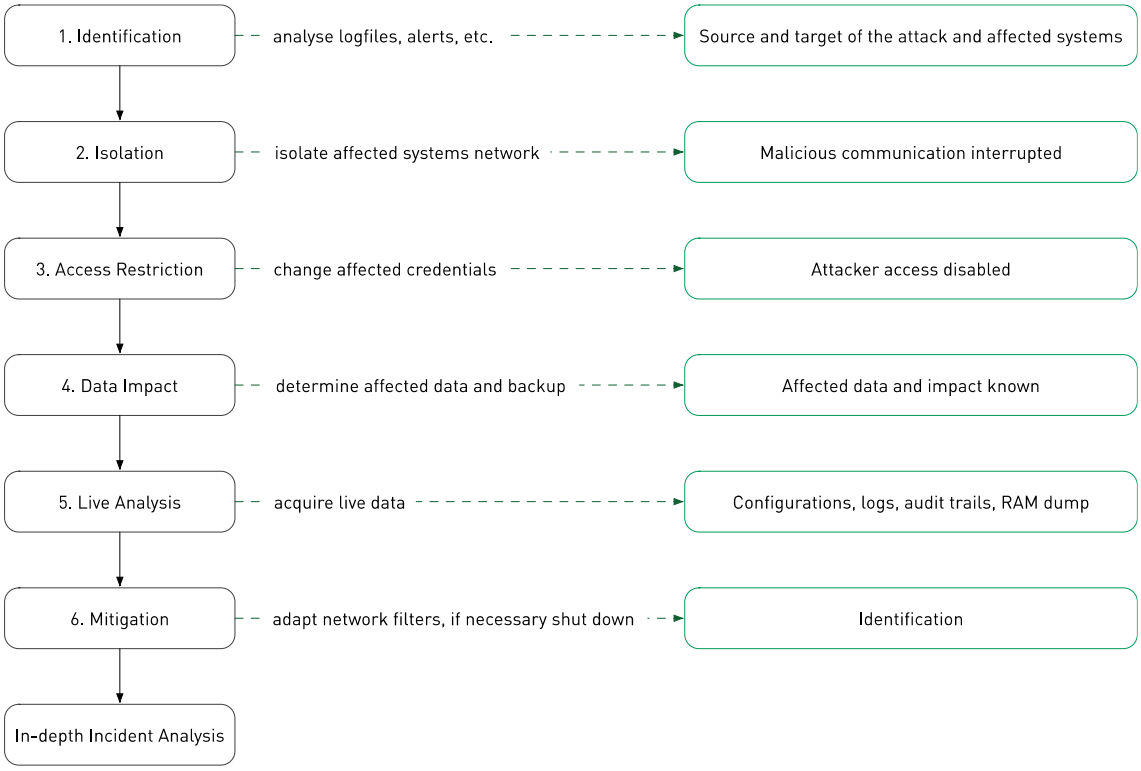
The remainder of this paper is structured as follows: In Section 2, we discuss general first steps that usually need to be performed in the very beginning after an incident has been detected. We then provide our Incident First Steps Checklist and Questionnaire as a cheat sheet and explain some basics about the Chain of Custody. Section 3 describes general seizing and analysis strategies for different types of affected systems and circumstances. In Section 4 we describe a sketch of typical incident handling preparations plans that can be prepared for specific types of incident to increase readiness for the covered incidents and in Section 5 we describe and give a short overview of incident handling process models. Section 6 concludes the paper.

2 Incident Handling First Steps

In this section, we first provide a general first steps guideline that names important tasks that usually need to be performed in the very beginning after an incident has been detected in a plausible order. We then provide our Incident First Steps Checklist and Questionnaire as a cheat sheet to be kept on hand for the case of an incident and we explain some basics about the Chain of Custody and general solution steps.

2.1 General First Steps

The first steps that typically need to be performed as soon as possible after an incident has been detected can be summarized as follows:



In the **Identification** step, the source and target of an attack has to be determined, as well as (potentially) affected systems. This is needed as a first starting point for further steps and has to be performed as fast as possible. Although those questions can only be completely answered after performing a fully-fledged incident analysis, an initial insight should be obtained from log files, alerts from intrusion detection systems, firewalls, antivirus appliances, as well as server and host log files.

In the **Isolation** step, our goal is to isolate affected systems from a network perspective with the goal to not destroy any evidence by powering systems off on the one hand, but on the other hand disrupt data leakage, command and control traffic and potential spreading of the attack.

As the next step, we recommend to perform **Access Restriction** to avoid that a potential attacker is able to remain in control of company systems via legitimate channels by using leaked credentials. To achieve this, potentially affected credentials have to be identified and then disabled or at least changed. Further affected persons have to be informed to ask for observed unusual behavior and provide the changed credentials where necessary to not interrupt productive use of the systems more than necessary.

In the **Data Impact** step, in a similar fashion, potentially affected data has to be identified and their confidentiality has to be checked to rate the impact of the incident and the availability of (recent) backups of this data has to be verified for the case that data has been destroyed or maliciously encrypted, as for example in cases of ransomware infections.

The next step is **Live Analysis**, where we want to acquire configuration data, logs, audit trails, lists of running processes, software, potential backdoors, document system time and if possible create RAM dumps for memory forensics in the later incident analysis phase.

As a first **Mitigation** step, network filtering should be implemented where appropriate to filter known attack-related traffic, for example from compromised services on so far unknowingly affected machines. Further, if no network isolation is possible and there are no strong reasons to keep the systems running (please refer to the Seizing and Analysis Strategies in Section 3), affected systems should be powered off (only servers should be shut down properly, as explained later).

After performing those first steps to collect initial information and preserve evidence while containing the incident, an in-depth *Incident Analysis* has to be performed by a forensic specialist to answer the remaining questions for attack vector, present vulnerabilities, extent and impact of the incident, affected data and potential legal obligations and finally resolve the incident. In the following section, we show our Incident First Steps Checklist and Questionnaire to support the collection of necessary information for the Incident Analysis Phase to be handed over to the (internal, if available, or external) forensic specialist. The checklist can also be found at the end of the document as a print-out flyer.

Besides these general first steps, we provide more details about **Seizing and Analysis Strategies** for different types of affected systems in different circumstances in Section **3** and provide more information about possibilities to prepare for incidents in Sections 4 and 5.

2.2 Incident First Steps Checklist and Questionnaire (by Michael Thumann)

Legend

- ! Important Information, make sure everyone knows about it and is acting accordingly!
- i Information
- ? Question to answer
- > To Do: Information/Data/Devices and so forth to provide

1. General Information
   - 1.1. ! If you are not sure what to do, ask for assistance/guidance. Don't act on your own, otherwise analysis and evidence collection might become impossible.
   - 1.2. ! Don't make changes to involved systems without being told by an authorized specialist
   - 1.3. i Collect as much information as possible (contact information, description of system behavior, involved systems, side effects and so forth)
   - 1.4. i Define and communicate single point of contact (Name, Email, Phone)
2. Contact
   - 2.1. > Provide contact information of responsible person (Name, Email, Phone)
   - 2.2. > Provide contact information of affected persons of the incident (Name, Email, Phone)
   - 2.3. > Provide contact information of person who detected the incident (Name, Email, Phone)
   - 2.4. > Inform all involved people that there might be questions by the analyst to be answered.
3. Device
   - 3.1. > What kind of devices are affected (Notebook, Server, mobile Device), provide complete inventory list as far as known including operating system information
   - 3.2. > Provide the affected employee's username(s)/-id(s).
   - 3.3. ? What privileges does the affected user(s) have (e.g. Enterprise Admin, Domain Admin, Local Admin or a standard user)?
   - 3.4. i Be prepared to provide the affected devices to the analyst
4. Detection
   - 4.1. ? How was the incident recognized? Provide all details (FW/IDS/IPS /AV Alerts/Logs and similar)
   - 4.2. ? What did the alert(s) say? Provide the original log lines, if possible.
   - 4.3. ? When was the incident recognized? Provide details in form of a timeline: When did the host get infected? When was the infection recognized? When was the host removed from the network? ...
5. Incident
   - 5.1. ? Detailed information from affected employee's perspective about what happened on the system during the infection. What did he do to get infected? What behavior did he observe during/after the infection? (Popups, system performance impact, ...)
   - 5.2. ? What actions (if any) have been performed on the affected system *at what time*, after the incident was recognized? (AV scan, removal of files, removal of autoruns, ...)
   - 5.3. i Any additional data regarding the incident is helpful (malware sample(s), mails including links/malware samples, captured network traffic, ...)
6. More required Information
   - 6.1. > Provide credentials (BIOS, Disk Encryption, local administrative accounts, ...)

2.3 Chain of Custody

Although this article is about handling and correctly reacting on incidents in a company environment, where typically the main goal is to quickly contain and resolve the incident, in some cases, it may be necessary to collect evidence in a forensically sound manner to be usable in legal proceedings. In those cases, it is most important to document each performed step in detail – especially to document how evidence has been acquired and preserved. In general, evidence should be collected according to methods that meet applicable laws and for each piece of evidence, a chain of custody should be provided, including at least the following information:

- System/Object Identification (location, serial number, model number, hostname, IP addresses, MAC addresses, photography of physical devices)
- (Safe) storage locations where the evidence has been stored at what time
- Name and contact information of every person who handled the evidence or only had access to it
- Purpose of each step
- Time and date including time zone of each step that has been performed with the particular piece of evidence

3 Seizing and Analysis Strategies

In this section, we outline some general seizing and analysis strategies depending on the circumstances of the affected devices. As a full incident analysis is quite complex, it has to be performed by a forensic specialist (a person with dedicated forensics training). Further we want to emphasize that the steps mentioned below reflect best-practices and experiences of what yields the best results for the majority of cases. However, there is no general golden rule or optimal process for all cases – given that every incident is unique in its own way. Nevertheless, we want to list the most important steps and the order in which they should be applicable for most incidents and can be adopted to a specific case. All steps lead towards a solid starting point for the actual incident analysis and collected evidence has to be handed over to the forensic specialist. The incident handling models in Section 5.2.3 also provide some details about possible incident analysis steps.

3.1 Powered-Off Device

In case of a powered-off device a forensic image (1-to-1 blockwise copy) of all storage devices in their current and unchanged state should be created. Thus the following steps and advises should to be followed:

1. Do not power the device on.
2. Disconnect all power sources and remove batteries (for example from laptops or mobile devices)
3. Create forensic images of all (writeable) storage devices, such as SDDs, HDDs, and Flash-Memory, for example.
4. Perform hard disk forensics as a part of the incident analysis phase by a forensic specialist.

3.2 Running Devices in general

If an affected device is currently running, additional steps have to be performed before the device is powered off and processed like a powered-off device as explained before. Before performing any of the following steps, check if some of the subsequent sections apply and refer to those (the more specific ones) first, as there are further requirements in cases of networked devices (which applies to most devices!) or especially servers.

1. If the device is networked, refer to the next section, first.
2. Acquire volatile data (requires expert knowledge or at least forensic training)
   2.1. Live Analysis
      2.1.1. Make use of statically compiled forensic tools on a read-only medium
      2.1.2. Document system time, running processes, network connections, file handles, ...
      2.1.3. If there is some indication for Ransomware, try to terminate the according processes

2.1.4. Extract cryptographic keys if cryptography is applied (Bitlocker, dmcrypt, TrueCrypt, VeraCrypt, or similar, but holds true for Ransomware, too).
2.2. Acquire RAM image
2.2.1. Different hard- and software-methods are available. An appropriate method needs to be chosen based on forensic specialist knowledge (also refer to Vömel, Stefan, and Felix C. Freiling. "A survey of main memory acquisition and analysis techniques for the windows operating system." Digital Investigation 8.1 (2011): 3-22.) for an overview and classification of different available techniques.
3. Power off device
3.1. Do not shut down, but rather pull the plug instead in order to preserve the current state (except for servers, as described in the next sections)
4. Proceed with all steps for powered-off devices
5. Perform memory forensics on RAM image in case of the incident analysis phase
5.1. Especially check for potential presence of rootkit/malware in RAM
5.2. Verify all the results from the Live Analysis
5.3. Refine results of Live Analysis by scanning (carving) for old or hidden process structures, for example using modules like psscan, sockscan, ... from the Volatility or Rekall framework.
5.4. Extract cryptographic keys if cryptography is applied

3.2.1 Running Networked Device

If an affected device has network connectivity, which will probably be the case for the vast majority of devices, and the device is running, the following steps should be performed, before performing the general steps for running devices.

1. If the device is a server, please read Section 3.2.2, first.
2. Consider whether it might be relevant for the case to capture network traffic of the still compromised device. If this is the case: Do not power off the device, but instead keep it running (as long as necessary) and capture network traffic
3. Consider isolating the device/transfer it to another network for containment if necessary and possible to prevent that other devices are compromised through the device. This should be accomplished transparently to the device on the network layer.
4. Continue with all steps for running devices (see Section 3.2).
5. Perform a network forensic analysis on the captured network data later in the incident analysis phase.

3.2.2 Running Servers

For running servers, special care should be taken when determining the extent of the data that should be seized. Follow the general steps for networked devices in the previous section, but check whether the system can be shut down or if only live acquisition is possible (no creation of a forensic disk image) to not disrupt productive use of the system. If a shutdown is necessary, use the appropriate operating system options instead of pulling the plug, because the impact of a data corruption might be worse than on a non-server device.

4 Incident Handling Preparation Plans

As an addition to the previously described general first steps guideline and different acquisition strategies for specific cases, a company might consider the preparation of incident handling preparation plans to have even more specific procedures and guidelines in place to several types of incidents they already faced or consider to occur in the future.

For each considered type of incident and for different kinds of affected assets, a preparation plan containing the following information should be filled out. It is very important to not only do this work once but to keep all the information documented in the preparation plans up to date and ideally perform test exercises and incident simulations on a regular basis. This list contains a sample structure of a preparation plan that covers common relevant information, but might be complemented by any other information that is considered to be useful in case the described incident is detected:

- Assets
  - Asset Details: Asset description, relevant hosts, IP addresses, ...
  - Asset Point of contact: who is responsible for the asset.
- Communication
  - Internal point of contact for external communication
  - Relevant external communication channels: press, suppliers, providers, customers
- Legal
  - Internal point of contact for legal issues
  - External point of contact for justice/prosecution
  - Known legal obligations for the type incidents, for example if confidential or personal data is affected
- Containment steps
  - Describe step by step what should be done to contain this particular type of incident, refer to the previous sections for a general guideline and adopt to the type of incident that is addressed by this particular preparation plan.
- Analysis/Solution steps
  - Describe step by step what should be done to resolve this particular type of incident, for example:
  - Patch Requisition
    - Request patches for affected software if possible/available
  - Imaging
    - acquire storage images of affected systems for hard disk forensics
  - Preliminary Rollback
    - Restore affected systems from uncompromised backups if available
  - Incident Analysis
    - perform forensic analysis of gathered data (Live data, RAM-dump, Images)
    - This step has to be performed by a forensic expert (internal if available or external otherwise)
    - Goals: Identify attack vector, business impact, provide information to legal.
    - We provide more details about specific incident analysis steps in Section 5.2.3.
  - Mitigation
    - patch/close identified vulnerabilities (potentially again starting from clean backups)

- put controls in place that apply to this asset
- adapt configuration of existing security controls (Firewall, IDS, AV, ...)

5 Incident Handling Models and Related Work

In this section, we want to summarize common existing Incident Handling / Incident Response models and highlight the differences in order to support companies to choose an appropriate one to further increase preparation for security incidents.

This section is based on our book *Forensische Informatik* (Dewald & Freiling, 2015).

5.1 General Information

For the acquisition and analysis of digital evidence, a generally accepted and approved procedure models have to be applied. In this section, we describe such common procedure models for incident handling and analysis. The term procedure models already implicates a certain abstractness. Indeed, process models provide a framework and guideline for own procedures.

There exist various incident handling process model and we want to emphasize that there is no *best* model, but the most important step for a company to be prepared for incidents is to establish at least *some* process model. Further, a process model in general is not meant to contain particular technical analysis steps, as they strongly depend on the particular case. This is in fact the purpose of the preparation plans explained in Section 4, checklists and process descriptions, which try to formalize and document the knowledge about specific incidents and can be integrated into the companies processes that follow the abstract process model.

Two characteristic representatives of such incident handling process models in the literature are the Incident Response Model by Mandia et al. (Mandia, Prosise, & Pepe, 2003).

Those two models are good candidates to show the essential aspects of incident handling process models. They have been summarized and integrated in the Common Model (Freiling & Schwittay, 2007), which we describe in detail in this section. After this, we provide an overview to some more well-known models as a starting point for further reading and customization of own processes.

5.2 The Common Model

The incident-response model has a strong focus on the management of incidents and the integration of the incident handling with the processes of an organization. Often, there is a focus on fast recovery from the incident. In contrast, the investigative process model focusses on an exact proceeding in evidence collection and incident analysis, which is therefor divided in several phases. As those models complement each other,

Freiling and Schwittay merged both to a combined so-called *common model*. The general structure of the common model, which we also use here is the following:

1. Pre-Incident Preparation (before an incident occurs)
2. Pre-Analysis Phase (after an incident occurred)
3. Analysis Phase
4. Post-Analysis Phase

Those phases are again structured into several steps, which we explain in more detail now.

5.2.1 Pre-Incident Preparation

The goal of the Pre-Incident Preparation phase is to put an organization into the position to be able to handle incidents in a well-defined way, to allow for a fast and effective resolution. This phase usually includes measures to prepare the people in the incident handling team for future incidents on the one hand, and measures to prepare the entire organization itself for incidents, such as definition and documentation of a policy that defines how different categories of incidents should be handled within the organization. It is also in this phase, where the organization decides, which pro-active measures (such as logging of any kind, preservation of network data, or similar) should be implemented. It is important to allow for proper incident handling on the one hand, but without threatening the privacy of employees or conflicting with laws on the other hand.

5.2.2 Pre-Analysis Phase

This phase includes all steps that lie between the recognition of an incident and its analysis. It is divided into the following steps:

1. Detection of incidents
2. Initial Response
3. Formulation of Response Strategy

5.2.2.1 Incident Detection

The detection of incidents step covers the deployment of guidelines for quick detection of incidents. Further, communication paths for notification about incidents, as well as the kind and degree of documentation have to be determined. This aims at a fast hand-over of the incident to the incident handling team. Incident detection usually takes place, whenever a person or security mechanism suspects an unauthorized or illegitimate activity. In fact, there exist various possible sources for such suspicions, such as employees, security personnel, intrusion detection systems or system administrators. For this reason, it is important

that the guidelines exactly state, who is to be informed in case of an incident and how it should be reacted in such situations. This is especially important in order to not unwillingly destroy potential evidence. With each notification of an incident some basic information such as date and time of detection and affected persons or systems have to be documented. For this purpose, forms have to be prepared and provided within the organization. This information has to be handed over to the incident handling team.

5.2.2.2 Initial Response and Containment

Goal of the initial response is to either confirm or discard the incident notification, e.g. determine if an incident really happened or if the suspicion was a false alert. If the incident has been confirmed, the category and extent of the incident to be able to define an appropriate strategy for tracking the incident in the following steps. Initial response also covers containment measures to limit the potential of the incident and the damage it causes. If appropriate, in this step also the logging of network traffic of affected systems is initiated in order to monitor an ongoing incident and provide further information. In specific cases, initial response may even cover steps that are normally taken during live response. In such cases, all the prerequisites that apply to live response have to be met in this earlier step of initial response. All gathered information has to be documented and is especially used in this step to estimate the impact of the incident for users, systems and business processes. This forms the basis for the next step.

5.2.2.3 Formulation of Response Strategy

In this step, an optimal strategy for incident handling in the specific case should be formulated. Especially, the incident handling team has to decide, whether a full-fledged forensic investigation of the incident should be performed. Thereby, a variety of different factors have to be taken into account. For example, it has to be considered, how critical the affected system is for the organization with respect to business processes on the one hand and with respect to the importance and confidentiality of the contained data on the other hand. Also the expected abilities of the attacker have to be taken into account, as well as financial impact. Also political decisions, risk management and regulatory restrictions are of importance.

5.2.3 Analysis Phase

In the analysis phase, the actual analysis of the affected systems takes place. The scope of the analysis is determined by the strategy that has been developed in the previous step. First of all, the Live Response (in our notation also called Live Analysis) is performed on the still running system, if applicable. The remainder of the analysis phase is then performed as a post-mortem analysis on the "dead" system. If in the prior

phase the decision has been made to perform a full forensic analysis, all steps of the analysis phase have to be performed without exception. If such a deep investigation is not needed, some of the steps can be left out or shortened, which we remark in the following description of the steps. Specific strategies (that have been decided beforehand) might even include to skip the analysis entirely and proceed with the Resolution Phase.

The analysis phase is divided into the following steps:

1. Live Response
2. Forensic Duplication
3. Data Recovery
4. Harvesting
5. Reduction and Organization
6. Analysis

We now explain each of those steps of the analysis phase in detail in the following sections.

5.2.3.1 Live Response

Live Response (or Live Analysis) describes the acquisition of data from running systems. This means that devices that need to be analyzed stay powered and running and are analyzed (to a certain extent) in the running state. The goal of Live Response is to gather volatile data that are lost after shutting down the device. In many cases in practice, it is further useful to already acquire some persistent data, too, to get a quick insight. However, all steps that are performed on the running system should alter the system as little as possible to avoid to many modifications to the original evidence. Specific volatile data, such as running processes or existing network connections, can nevertheless only be obtain in the Live Response due to the fact that they are usually only kept in RAM. The information gathered in the Live Response is often of great value to the analyst to estimate the extent of the incident and plan appropriate analysis techniques in the further steps.

5.2.3.2 Forensic Duplication

In the Forensic Duplication step (also called *imaging*), exact copies of all storage media that are related to the incident are created. The original evidence hereby has to remain unaltered. A chain of custody (see Section 2.3, too) is started for each piece of evidence and the original evidence is stored in a safe location (evidence room) alongside with (a copy of) the image.

5.2.3.3 Data Recovery

The Data Recovery step is about recovering data that is not accessible in the current state of the image that has been created in the previous step. This includes the recovery of hidden, lost, deleted, destroyed, or corrupted data or data that has been made inaccessible in whatever way or hidden in unallocated space.

5.2.3.4 Harvesting

In the Harvesting step, the analysis starts to collect meta data (data about the data), such as timestamps, file sizes, or file types) of all data das is directly accessible or has been made accessible in the previous step. The goal is to structure the mostly unorganized set of data following several criteria, like for example time spans, file types or other meta data. This structure might be useful in the next steps, as is many cases, specific properties of data (or files in particular) might indicate a connection to the incident, for example all binary files (programs) that have been modified in the specific time span in which the incident happened, in case of a malware/Trojan infection.

5.2.3.5 Reduction and Organization

While Reduction and Organization, all data that can be classified as not relevant to the case, can be excluded from the further analysis. The goal of this step is to reduce the big amount of structured data from the previous step to the smallest possible set of data with the biggest potential to carry all/the most relevant data. The remaining data is organized to ease the later access, for example by indexing textual files to enable a fast keyword search, numbering and naming data to easy referring to it, or similar.

5.2.3.6 Analysis

Now that all data with a potential relation to the incident has been recovered, collected, reduced and organized, in this step, the actual Analysis by the analysis takes place. An investigator develops hypotheses about what might have happened and who might be responsible for it. When examining the actual content of all the data, the different pieces of (digital) evidence are put in relation to each other. All activity (events) that is documented is verified as far as possible on all pieces of evidence that might mirror the particular event, leading to an as complete as possible reconstruction of the entire incident, based on dispassionate and scientific principles.

To ensure such a dispassionate analysis and interpretation of the results, scientific methods have to be applied. This includes that an investigator has to figure out all possible hypotheses that might have led to

the incident and then try to disprove each of them (NOT proving them) by the available evidence. By excluding hypotheses and theories that cannot be brought together with the already obtained knowledge from the evidence, it is harder to be biased and drive the investigation in a single (maybe wrong) direction. The remaining hypotheses (the ones which cannot be disproven) have a higher probability to be a correct reconstruction of the incident.

Another important property of the Analysis Phase's results is the repeatability. This means that every analyst has to be able to make the same observations as the investigator, if applying the same methods. To this end, each applied technique and every tool that is used has to be documented precisely (and ideally in the moment it is used). Same holds true for the results and their meaning or interpretation for the assumed hypotheses and the hypotheses themselves – everything has to be written down.

5.2.4 Post-Analysis Phase

The Post-Analysis phase starts after all activities for collecting and analyzing digital evidence are finished and the goals that have been formulated in the strategy have been fulfilled (all questions have been answered) in the analysis phase.

The Post-Analysis phase consists of the following steps:

1. Report
2. Resolution

5.2.4.1 Report

This step included the writing of a precise report that describes the details of the incident in a comprehensive manner so that it can be understood by non-technical readers, too. The report contains the entire documentation that has been created in the Pre-Analysis and the Analysis Phase and puts a comprehensive overview of the entire case on top, that includes the most important results of the analysis and their meaning for the (re)solution of the incident.

5.2.4.2 Resolution

The goal of the resolution is to identify (all) the problem(s) that has led to the incident, solve it, and find appropriate controls to prevent another incident of this kind in the future. In case of a still ongoing incident, those measures should already be taken as soon as they are known (for example already during the Analysis Phase), but if possible only after all potential evidence has been acquired. To verify that the identified

controls perform in the considered way, their implementation should be observed and the effectiveness of the measure should be tested afterwards.

5.3 More Models

There exist various other Incident Handling models in the literature. A good overview is provided in the work of Pollitt (Pollitt, An Ad Hoc Review of Digital Forensic Models, 2007).

The following list shows a selection of incident handling process models from this overview (Dewald & Freiling, 2015), that also includes a more current model. All models can more or less be mapped to the model we introduced here, but there are different focusses and emphasis on specific tasks, as well as the order of the described steps may vary. However, from reading this article, the main idea of incident handling process models should be clear and we encourage to customize it to an own process model that matches best and reading through the other models to incorporate some more ideas. To this end, we believe that the following selection be a good starting point for further development and customization of an individual model:

- (Pollitt, Computer Forensics: An Approach to Evidence in Cyberspace, 1995)
- (Carrier & Spafford, 2003)
- (Baryamureeba & Tushabe, 2004)
- (Beebe & Clark, 2005)
- (Gong, Kai Yun Chan, & Gaertner, 2005)
- (Kent, Chevalier, Grance, & Dang, 2006)
- (Kiltz, Hoppe, Dittmann, & Vielhauer, 2009)

6 Closing

In this section, we want to summarize the contents of this paper and end up with an overall conclusion and outlook.

6.1 Summary and Conclusion

In this paper, we motivated the advantages of incident preparation and provided different pieces of information and documentation to support especially companies to improve IT security incident readiness. We first explained the from our perspective and experience most important first steps in case of an incident, as there often happen mistakes that hinder further analysis in Section 2,. We then provided our Incident First Steps Checklist and Questionnaire as a cheat-sheet to be printed out and explained some basics about the Chain of Custody to be kept in mind for the further reading. In Section 3, we described general seizing and analysis strategies for different types of affected systems and circumstances, such as running vs. powered-off devices, networks devices, and servers in particular and named important steps that depend on further circumstances such as if some kind of encryption is used. Section 4 described a sketch of typical incident handling preparations plans that can be prepared for specific types of incident and finally in Section 5, we incident handling process models in general and described the Common Model in detail. We also provided a reading list for further literature on incident handling models.

6.2 Limitations

As limitation of this work (and a disclaimer), we again want to emphasize that this paper provides a general guideline with the goal to support companies to improve their preparation for incidents, for such that do not have much preparation done so far, but also for those that already are well-prepared and might find some ideas to still improve their line-up. It is important to modify and customize the guidelines, plans, checklists and models described in this work to own needs and circumstances, but we hope and believe that our general recommendations can be useful as a starting point and can then be modified over time. The most important point is to invest in preparation, from our point of view.

It is further of great importance, to inform people about processes, guidelines and everything that is prepared for the case of an incident to ensure that this preparation is really made use of in the case of an incident even under major stress. To this end, workshops, training, and exercises are good instruments to really implement this knowledge.

6.3 Future Work and Outlook

As we observe more and more cases every year, we want to keep our checklists and guideline up to date to cope with arising new types of attacks that we see in the wild, but also new technologies or paradigms. Thus, we plan to accordingly publish updated versions of this article (or material in other formats) as soon as substantial parts of our suggestions made in here change. We further might include a short description of other incident handling models, too, if we recognize that some of them are more appropriate to cover the real word.

7 References

Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *DFRWS.*

Beebe, N., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*(2).

Carrier, B., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. *Int. Journal of Digital Evidence, 2*(2).

Dewald, A., & Freiling, F. (2015). *Forensische Informatik* (2nd Edition ed.). Germany: BoD.

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *IT-Incidents Management & IT-Forensics (IMF).* Stuttgart, Germany: GI.

Gong, R., Kai Yun Chan, T., & Gaertner, M. (2005). Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. *Int. Journal of Digital Evidence*.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensics into Incident Response.* National Institute of Standards and Technology (NIST), Computer Security Division Information Technology Laboratory. NIST.

Kiltz, S., Hoppe, T., Dittmann, J., & Vielhauer, C. (2009). Video surveillance: A new forensic model for the forensically sound retrival of picture content off a memory dump. *Informatik 2009: Im Focus das Leben, Beitraege der 39. Jahrestagung der Gesellschaft fuer Informatik e.V. (GI).* Luebeck: GI.

Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident Response & Computer Forensics* (2nd Edition ed.). McGraw-Hill.

Pollitt, M. (1995). Computer Forensics: An Approach to Evidence in Cyberspace. *Proc. 18th NIST-NCSC National Information Systems Security Conference.* NIST.

Pollitt, M. (2007). An Ad Hoc Review of Digital Forensic Models. *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE).* Seattle, Washington, USA: IEEE Computer Society.

Incident Checklist & Questionaire

by Michael Thumann - mthumann@ernw.de

	Actions/To Dos/Questions
1 General Information	1.1 If you are not sure what to do, ask for assistance/guidance. Don't act on your own, otherwise analysis and evidence collection might become impossible. 1.2 Don't make changes to involved systems without being told by an authorized specialist!!! 1.3 Collect as much information as possible (contact information, description of system behavior, involved systems, side effects and so forth) 1.4 Define and communicate single point of contact (Name, Email, Phone)
2 Contact	2.1 Provide contact information of responsible person for the incident (Name, Email, Phone) 2.2 Provide contact information of affected persons of the incident (Name, Email, Phone) 2.3 Provide contact information of person who detected the incident (Name, Email, Phone) 2.4 Inform all involved people that there might be questions to answer provided by the analyst.
3 Device	3.1 What kind of devices are affected (Notebook, Server, mobile Device), provide complete inventory list as far as known including operating system information 3.2 Provide the affected employee's username(s). 3.3 What privileges does the affected user(s) have (Enterprise Admin, Domain Admin, Local Admin or a standard user)? 3.4 Be prepared to provide the affected devices to the analyst
4 Detection	4.1 How was the incident recognized? Provide all available details (Firewall/IDS/IPS/Proxy/AV/... Alerts?) 4.2 What did the alert(s) say? Was it a malicious file, suspicious traffic, ...? Provide the original log lines, if possible. 4.3 When did the incident got recognized? Provide details in form of a timeline: When did the Laptop get infected (according to the user)? When was the infection recognized? When was the Laptop removed from the network? ...
5 Incident	5.1 Detailed information from affected employee's perspective about what happened on the system during the Infection. What did he do to get infected? What behaviour did he observe during/after the infection? (Popups, system performance impact, ...) 5.2 What actions (if any) have been performed on the affected Laptop _at what time_, after the incident was recognized? (AV scan, removal of files, removal of autorun functionality (e.g. registry keys), ...) 5.3 Any additional data regarding the incident is helpful (malware sample(s), mails including links/ malware samples, captured network traffic, ...)
6 More requried Information	6.1 Provide credentials for local access (BIOS password, HD Disk Encryption Passwords, local administrative account credentials, ...)
7 Legend	Important Information, make sure everyone knows about it and is acting accordingly! Information Question to answer To Do: Information/Data//Devices and so forth to provide