Secura
A BUREAU VERITAS COMPANY

Digital Forensics

Criminals are increasingly using computers to commit crimes. When a company becomes a victim, the consequences are often difficult to predict. Sometimes, it is only a suspicion of a crime, and it must be determined whether an incident had actually occurred.

In many cases, a digital forensic investigation is needed to determine what happened; for example, if you suspect a data breach or a potential hack. An investigation can also be used to determine whether intellectual property has been stolen, or when an employee is suspected of leaking company secrets.

Secura is registered as a Private Investigation Bureau with the Ministry of Justice and Security. In addition, Secura has employees who are qualified private digital investigators. Therefore, Secura is able to provide reports and documents that can be used in legal proceedings.

What Is Digital Forensics?

Virtually all organizations today depend on information technology (IT). These developments create potentially vulnerable systems that are often connected to each other, thus creating new risks. Just like in the physical world, it is important to protect the digital world from unauthorized use and to take measures to be able to determine what happened to a particular system. Digital forensics is the field concerning the detection and reconstruction of incidents in digital systems.

Digital investigation is essential for learning from incidents that have occurred and preventing incidents in the future. After all, users of information systems leave digital traces behind when they use the systems - whether they are computer systems, smartphones, cell phones, tablets or networks. Digital forensic tools and techniques are available for securing and analyzing digital evidence. Digital forensic tools and techniques can also be used, for example, to recover lost files or to monitor internal systems.

Digital forensics is primarily used for investigations focused on legal or law enforcement issues that may, or likely will, end up in court; hence the emphasis on legal acceptability. Digital evidence is extremely volatile and can easily be lost or altered if carelessly handled. Thus, it is necessary to preserve and handle digital evidence in a manner that ensures it is not distorted or destroyed.

Digital forensics is a field which is always in development. Digital forensics can be defined as using computer and system knowledge, in combination with legal expertise, to forensically acquire, process and analyze in a manner which complies with local legal regulations and the rule of law.

Digital Forensic Services

Secura offers a number of digital forensics services. The suitability of each service depends on specific circumstances and is determined on a case-by-case basis. In addition, advisory trajectories can also be executed, for example to determine how well your organization is prepared for a possible incident. The most common investigation methods are explained below.

DIGITAL FORENSIC INVESTIGATION

Secura has the necessary expertise to perform digital forensic trace analysis on a wide range of equipment, from laptops to workstations and phones.

A digital forensic trace investigation can provide conclusive information for the following situations:

- Has unauthorized access been gained to my systems?
- Have unauthorized activities occurred in my organization?
- Has sensitive data been siphoned off or otherwise obtained during a security incident?
- Have specific vulnerabilities in software or systems been exploited, and how was this done?

These types of investigations are also known as post-mortems, because after the incident, it is necessary to determine what happened. Using specialized software, Secura is able to identify suspicious activities such as:

- Mapping of suspicious activities through analysis on various system resources;
- Executed (rogue) programs;
- Opened files;
- Visited websites;
- Successful/unsuccessful login attempts;
- Connected USB devices such as data carriers.

During the forensic investigation, extensive contact is maintained with the stakeholders of the investigation. Upon delivery of the report, a debrief takes place; the debrief focuses on a brief summary of the investigation and relevant recommendations so that similar incidents may be prevented in the future.

INVESTIGATING MOBILE DEVICES

Smartphones and tablets have become part of everyday life and are used for various business applications. Secura has the capabilities to thoroughly examine such devices and analyze various traces. These include:

- Retrieving call history;
- Installed apps;
- Recently used WiFi networks;
- Paired devices via Bluetooth;
- Visited web pages;
- Retrieving available mail and calendar data;
- Received messages including SMS, WhatsApp and similar chat services.

It is important, however, that the device can be unlocked. Modern phones and tablets cannot be examined for all of the aspects if the device is not unlocked.

INVESTIGATING E-MAIL

Examining the e-mail of an employee can be part of the digital forensic investigation. Using specialized software, Secura is able to retrieve (deleted) emails including attachments and map the communication with various parties. This method can also be used to determine whether, for example, malware has been spread by e-mail.

INVESTIGATING CLOUD ENVIRONMENTS AWS & AZURE

The use of cloud services such as Amazon Web Services (AWS) and Microsoft Azure is becoming more commonplace in corporate IT infrastructures. Secura is able to perform forensic investigations on these environments as well. This includes the investigation of virtual machines and the associated logging of various AWS and Azure services.

FORENSIC READINESS

Forensic Readiness indicates to what extent an organization is able to collect, preserve, protect and analyze digital evidence so that it can be used effectively in security investigations, answering questions from regulators, internal legal departments or in a court of law. Forensic readiness focuses on the availability of various logging sources within your organization and their suitability for resolving a forensic incident. In one or more workshops, Secura will run through various scenarios and threats, working with your technical experts and administrators to analyze whether your organization is ready to properly investigate an incident. This is an important component of cyber resilience, as it can also greatly enhance recovery capability after a digital attack

The workshop can be conducted in one or more half-day sessions and will cover the various phases of a forensic incident, including detection, analysis, containment and recovery operations. It is recommended to attend a workshop with the same team that will/will be engaged in a real incident. After the workshop, noted areas of concern will be incorporated into a report.

Secura's Approach To Successful Research

OUR INVESTIGATIVE APPROACH

Within digital forensics, Secura follows a phased approach with room for different testing methodologies depending on the purpose, the environment to be investigated (architecture, platform, application etc.), industry requirements or even regulations per country.

This ensures a professional approach to projects where we meticulously and methodically investigate the security issue. This helps to be complete and accurate and provides assurance that the correct issues have been investigated.

To ensure a thorough and successful investigation it is important that Secura has access to all relevant data sources pertaining to the investigation. The number of data sources can be increased if the investigation calls for it. Adding new data sources always happens in consultation with the client. Of course, there will always be close contact during the investigation to discuss the progress of the investigation.

Prior to a forensic investigation, Secura will prepare a plan of approach, which needs to be approved by the client. Once the plan of approach is approved by the client and the required consent is given, the actual investigation begins. At the end of the investigation a written report follows with the findings such as timelines and evidence.

It is important to mention that Secura is limited in its investigations by the extent to which logging and traces are available on the to be investigated data carriers. It sometimes happens that during an investigation it must be concluded that traces have already been deleted or lost. Therefore, no guarantees can be given as to whether or not it will be possible to definitively determine what happened. It is important to note that Secura does not engage in Incident Response (IR) activities that involve fighting an active attack.

ROADMAP AND PHASES OF AN INVESTIGATION

Secura's digital forensic investigation consists of the following seven phases:

PREPARATION	The first phase of a forensic investigation involves setting up an investigative environment (crime lab). The investigation environment includes the infrastructure, hardware, software, the logbook and protocols for action, such as determining who is ultimately responsible. In this phase, the preliminary investigation also takes place and the plan of approach is drawn up. The plan of approach determines what will be investigated, what the main and sub-questions are and whether hypotheses can be drawn up. Naturally, this is always done in consultation with the client.
ACQUISITION	In this phase of the forensic investigation, the research data is obtained or secured. This is usually done by "imaging". The acquisition of data carriers is described and consent will be recorded in a statement. All further investigative activities are conducted on forensic copies. The original data carriers will remain untouched.
PROCESSING	The process steps "Processing"and "Analysis" can take place simultaneously. In these phases, data is identified, file types are recognized, files are decrypted, and duplicate files will be taken into account.
ANALYSIS	During a forensic investigation, it is customary to establish a timeline. A timeline is used to map potentially suspicious activity to performed actions within a specified timeframe. To this end, data will be indexed in specialized software for faster analysis. From this, a timeline of events will be created (e.g., who was logged into the system when, when which programs were started, when which websites were visited, etc.).
VERIFICATION	The verification phase will verify whether alleged evidence can actually be used as evidence. Data must relate back to an identifiable source and linked to a suspected or suspicious activity. In this step, the conclusions from the analysis will be validated.
PRESENTATION	At this stage, the report will be shared and findings may be presented. Any statements from witnesses will be discussed during this phase. If there is indeed a possible crime, findings will be prepared that can be used in a criminal investigation.
ARCHIVING	The final phase of the forensic process will involve archiving. Any data related to the investigation, evidence, software and hardware can be archived. If indeed a criminal investigation will take place, then the availability of this information must comply with legislation.

Secura
A BUREAU VERITAS COMPANY

Legal And Technical Frameworks

Secura complies with the applicable legal frameworks in carrying out all its assignments. For forensic investigations, the AVG and the Computer Crime Act are particularly important. This means, among other things, that no illegal methods can be used to obtain evidence, such as hacking into online accounts, without the consent of the owner of those accounts. It also means that personal data not relevant to the investigation will be anonymized in the reports.

Secura has a security management process that is certified to the ISO27001 standard. Secura's research lab is certified to the ISO17025 standard. Secura's quality processes are certified to the ISO9001 standard.

How Can Secura Help?

Are you interested in conducting a digital forensic investigation or do you have questions about what we can do for you in this regard? We would love to help you!
Call us at +31 (0) 88 888 3100 or send an email to: info@secura.com.