Digital Forensics

The analysis after an incident.

Have you been hit by a cyber-attack and need help clearing things up? Our team of experienced computer forensic experts can help with identifying the cause, scope and perpetrator of the attack for you. Furthermore, we provide you advice regarding communication issues and create regulatory or compliance-specific reports for you, if required.

Key questions about incident investigation

Our technical incident investigation focuses on answering the following questions:

- How did the attack happen? Which vulnerabilities were exploited?
- Which systems have been affected by the attack?
- What damage was caused and which data has been stolen?
- Who was the perpetrator?
- How can future attacks be prevented?

Our computer forensic lab

Our team has a large computer forensic lab at its disposal that ensures an efficient analysis of any incident. We evaluate log files and storage devices after an attack using professional tools and methods, and identify undesirable network activities. After the incident analysis has been completed, you will receive an extensive forensic report with recommendations on how to prevent attacks in the future. Furthermore, we issue you with any regulatory notifications that might be required.

Our procedure model

Our forensic investigation comprises six phases. This procedure is based on international standards and best practices such as SANS, NIST and the BSI standards (BSI - Bundesamt für Sicherheit in der Informationstechnik – in English: German Federal Office for Information Security). All the phases and their results are documented accordingly.

Phases of the procedure model

Preparation

In the preparation phase, we discuss the current situation with you and explain our course of action. Depending on the incident, we identify and make suitable forensic tools available.

Data collection

In this step we collect all the important data of potentially affected components. For this purpose, we record the current system time and date, all the processes currently running on the system (system status), the opened network connections (sockets) and the users logged on the system, etc.

Examination

Once data collection is finished, we start examining it. In this process, we extract all the data relating to the incident. The amount of data is reduced by the fact that certain data can be excluded from further analysis (e.g. by checking against known checksums). However, it might also be required to extend the analysis to further components of the IT equipment.

Data analysis

Very often, several subcomponents are affected by an incident, thus necessitating multiple individual examinations of them. Combining the results from these examinations to a coherent timeline and logical connection is the subject of the data analysis phase.

Documentation

Formal reporting of the investigation results takes place after data analysis. In doing so, our computer forensic experts combine the individual steps that have been recorded in the course of the investigation into one or more reports. We prepare target group specific reports, which means that the technical details in the report for the management are different from those for the system administrator, for example. In this phase, we also as-

Post-processing

sist you in preparing regulatory notifications, if required. Within the scope of post-processing, we offer optional identification of processes needing improvement. We recommend and provide you with technical action plans to help prevent future attacks and develop specific proposals with you for improving the corporate response strategy, namely the process of handling incidents within the company.

This product sheet will be valid until a new version is released. *Product sheet creation date: 28/11/2018*

How to handle an emergency

Leave everything unchanged.

Of course, the primary concern in most cases is to reduce the damage and to re-establish normal operation as soon as possible after a security incident. However, from a security point of view, the affected system should not be directly reinstalled after each and every incident, because this often means that the cause of the incident remains unknown and the system is still vulnerable to new attacks. Changes to the system should therefore be avoided in order not to jeopardize the investigation of the cause.

Record everything that has happened.

Document what happened when, and what you did. This information is extremely valuable for the work of our forensic team.

Please, don't hesitate to contact us if you have any questions.
Phone: +49 6102 8631-190 | E-mail: sales@usd.de
PGP or S/MIME for secure communication