Organization wide assessment for traces of a cyberattack

Compromise Assessment

FOX-IT's Compromise Assessment is an unique service that helps organizations find out if they are under a cyberattack (a compromise).
Even if you expect your security measures to be able to do what they are meant to do, advanced attackers are often able to circumvent these measures unnoticed. Not all traffic passing through your layers of security is safe: technology can fail, and personnel may ignore safety precautions and procedures. This could lead to an attacker infiltrating your network and remaining present without detection for months. FOX-IT will help you to gain insight into your IT infrastructure, determine whether your organization has been compromised, and assess the state of your IT security.

For a more secure society

FOX-IT's Compromise Assessment

- Looks for traces of current and past compromises.
- Measures your organization's overall IT security level and provides detailed insights.
- Is based on network traffic, log files and endpoints.
- Combines unique knowledge of threat actors with indicators of compromise and human expertise.
- Includes an extensive report containing all findings and recommendations.
- Can serve as the basis for a security roadmap.
- Is suited perfectly to apply within business-critical environments.

FOX-IT

Prevents, solves and mitigates the most serious threats caused by cyberattacks, data leaks or fraud with innovative solutions for governments, defense agencies, law enforcement, critical infrastructure, banking and commercial enterprise clients worldwide. FOX-IT combines smart ideas with advanced technology to create solutions that contribute to a more secure society. We develop products and custom solutions for our clients to guarantee the security of sensitive and critical government systems, protect industrial networks, defend online banking systems and secure confidential data.

Goal of the assessment

The primary goal of a Compromise Assessment is to search for traces of a compromise within your IT infrastructure, in order to determine the overall state of your IT security. The scope of the assessment is determined jointly by you and FOX-IT, establishing which groups (threat actors) pose a viable threat to your organization. In addition, the assessment enables us to construct a list of the most important assets in your network.

FOX-IT's approach

Once the scope has been established, the assessment is performed in three phases. First, preparations are taken, so that the second phase, the actual assessment, can progress smoothly. The third and final stage brings together the findings of the assessment in an extensive report, which can then also be presented to your executive management.

Phase 1 – Preparation

Before the Compromise Assessment starts, we will deploy one or more probes in your network to inspect network traffic. We also determine the type of log files that are available and their retention. Finally, we decide with you which endpoints are of key interest for a thorough forensic investigation and for checks into known traces of malware. Once all the relevant information has been collected, we can start the assessment.

Phase 2 – The assessment

FOX-IT has unique intelligence on threat actors operating worldwide and the methods they use. This information is applied to the collected network traffic, log files and endpoints. We analyze the collected data to identify traces and patterns and any anomalies in these patterns. As soon as potential indicators of a compromise are found, an in-depth analysis is performed in order to determine the severity of the situation. During the entire process, you will be kept up-to-date on the progress and status of the assessment at both technical and management levels.

Phase 3 – Reporting

Once the Compromise Assessment is complete, FOX-IT collates all the relevant findings in an extensive report. The report details the result of the assessment and how these were obtained. It also contains a number of recommendations on IT security for your environment. These recommendations are made along with suggestions for preventative, detective and response/readiness measures. The report takes any security strategies that are already in place into account, so that it can form the basis for further enhancing your security roadmap.

Expertise and flexibility

FOX-IT can carry out the assessment in the digital forensics lab at the FOX-IT headquarters in Delft. Of course if you prefer, we can also perform the assessment on-site at a location of your choice. The latter option is often preferable due to the synergy it creates between your organization and FOX-IT. It also gives us more insight into the inner workings of your organization's IT security and creates shorter communication lines. The team that performs the assessment is comprised of experts and analysts from the fields of IT security, digital forensics, incident response, network forensics and malware analysis.

More information

For more information please contact Kevin Jonkers, Manager Forensics & Incident Response, email: fox@fox-it.com, tel: +31 (0) 15 284 79 99.