CASE STUDY

Summary

The client is a holding company, which unites more than 10 businesses of different profiles - manufacturing, trade, construction, insurance, services and other.

Installation covers up to 100 VLANs.

Challenge

Based on threat's testing and modeling approach, applied to different segments of the customer's infrastructure, weak points in event detection within the network perimeter were identified.

These events were classified as those that are related to the stages of network exploration by the attackers and attempts to exploit the obtained network services in the local network segments.

It was also determined that an additional layer of protection was required at the workstation level, in the form of file honeypots for attackers who had already gained access to the station, for example, through a phishing attack.

To improve the quality of incident investigation, it was essential to reduce the amount of response time, while diverting the attackers' attention as much as possible from real IT assets.

Realization

The Labyrinth system was deployed in a configuration with multiple Worker VMs, because there was a need to cover several distributed network segments: offices and data centers.

During the deployment process, all available types of network honeypots (Points) were used and two-way integration with SIEM was performed.

For the majority of internal Web services, our team created web honeypots based on UniversalWebPoint.

Solution

Deployment of the Labyrinth system and coverage of the Client's infrastructure was provided in few directions:

1. Critical for business processes, internal Web applications were identified, and several network honeypots for each of them were created on the basis of UniversalWebPoint aiming to increase the likelihood of detecting an attacker who is focused specifically on finding and exploiting internal Web resources.
2. All available types of network decoys (Points) were deployed to create the largest possible attack surface. The majority of the client's network segments were covered with decoy networks.
3. SIEM and Labyrinth dual sided integration is configured. Based on this integration, additional procedures have been deployed and formalized to be used in the investigation and response to incidents. Labyrinth incidents handling process was integrated into common Security Incident Management process within Organization.
4. On actual hosts, many different types of decoy files are distributed to detect an attacker at the post-exploitation stage (if the intruder anyways gains access on an actual host by using phishing, physical access, etc.).

Results

With the Labyrinth system's functionality, it was possible to increase visibility within the network perimeter, to identify any possible attempts to conduct unauthorized access and research within the structure and composition of hosts in network segments. Due to the use of the Web-deception functionality, attackers' sequence of actions on internal Web applications were spot-on detected and carefully classified.

Based on the data gathered by the Labyrinth system, informational value of detected incidents has been significantly increased, which has led to faster decision making for each of the investigated cases.

Labyrinth is a team of experienced cybersecurity engineers and penetration testers, which specializes in the development of solutions for early cyber threat detection and prevention.