Cyberattack – what to do?
Checklist for CISOs in the event of a cyberattack

Technical measures

> Ensure that the system time of your network segments is synchronised to allow easy matching and analysis of different protocols based on the same times.
> If an incident occurs, you will quickly need a large amount of storage space (for example external memory) for creating digital images, copying a large number of logs, etc. This should already be available.
> Data is often archived for a certain period of time. It is advisable for those responsible for initial care to know which archives exist, how to access them and the structure in which data is archived.

Organisational measures

> Incident management must be prepared in advance with clear procedures, responsibilities and communication strategies (developed with corporate communications).
> Internal and external communication must be regulated (with support from corporate communications). Inform your technical team as transparently as possible in order to respond to incidents promptly and effectively. Furthermore, unwanted collateral damage should be avoided.
> It is recommended to keep an up-to-date and complete inventory of all systems, software and networks. This inventory must be directly accessible to all parties involved.
> Establish a direct relationship between incident response, vulnerability management and risk managers to ensure that all risks are known and addressed.
> It is essential to know the key internal processes and have a plan for maintaining operations in the event of a crisis.

Server and client side

System level:

> It is recommended to use dedicated systems for the management of infrastructure elements. Furthermore, administrators should use two-factor authentication.
> Define detection rules for attacker's "helper" tools such as PsExec and rexec.
> It is advisable to closely monitor the execution of binaries via the WMI interface.
> Integrity monitoring tools can be used to detect unauthorised changes to system files. They are also useful for assessing the impact after an incident.
> Prepare the means to monitor and analyse your system memory. This increases your chances of quickly identifying and responding to complex threats.

Virtualisation:

- Acquire a certain level of forensic knowledge. This will help you to determine whether a VM escape may have occurred. > Preparing packet sniffing functions can help you monitor traffic between VMs.

Active Directory:

- Develop a clear understanding of the trust relationship between different AdForests.
- Monitor AD protocols closely for unusual and large queries that you would not expect.
- Have contingency action plans in place that provide for a fully compromised Active Directory.

Network:

- Use a centralised and well-guarded interface through which every internet-bound packet must pass. The same can be done for incoming traffic distributed across different network zones. You may consider setting up central access zones with load balancers, web application firewalls and authentication gateways that allow you to centrally monitor incoming traffic.
- Look closely at the routing paths from the internal network to exposed network areas, such as a DMZ. Does this traffic also pass through the central and well-guarded interface mentioned above? If not, you should place sensors that also monitor this traffic.
- All internet access should pass a proxy that logs all header information, including cookies.
- Collect netflow data, not only between network zones, but also within the zone.
- In addition to commercial solutions, use a classic signature-based IDS such as Snort or Suricata. This gives you the possibility to quickly apply custom detection rules in case of an intrusion.
- Use Passive DNS so that all domain queries run over the internet and can be found quickly and efficiently.

Log files:

- Save the log files for as long as possible. A minimum of two years is recommended, especially for important systems such as domain controllers and gateways.
- Log files must be collected centrally. It is recommended to have a log management concept that covers all network zones and allows indexing, searching and archiving of all log files.
- Furthermore, it is advisable to implement continuous log analysis, which enables an automated comparison of these log files with known IOCs.
- Log management is an ongoing process. You must have sufficient resources to add new sources to your system on an ongoing basis. This is because your IT landscape is also constantly changing.
- Tailor the log settings to your needs. For example, although user agent logging may not be the default setting, it is strongly recommended.
- Experienced employees should not only analyse the pre-processed log files, but also check the raw logs for irregularities. Sufficient time and personnel resources should be allocated for this.