Cyberattack – What to Do?
Checklist for CISOs in Case of a Cyberattack

Technical Measures

> Please make sure that the system time of your network segments is synchronised in order to allow an easy alignment and analysis of various logs on the basis of matching times.
> If an incident does occur, the creation of digital images, copying large numbers of logs, etc. will quickly require a considerable volume of storage space (for example, external storage) that should already be available.
> Data are often archived for a particular time period. It is advisable that those in charge of initial provisioning know which archives exist, how they may be accessed, and the structure in which data are archived.

Organisational Measures

> Incident response is something that needs to be prepared in advance by means of clear procedures, responsibilities and communication strategies (formulated in cooperation with corporate communications).
> Internal and external communication must be regulated (with the support of corporate communications). Inform your technical team as openly as possible in order to be able to respond to incidents promptly and effectively. Also, undesired collateral damages should be avoided.
> It is recommended that an up-to-date and complete inventory of all systems, software and networks be kept. Such an inventory must be directly accessible to all involved parties.
> Establish a direct connection between incident response, vulnerability management and risk managers to ensure that all risks are known and being dealt with.
> It is crucial to know the most important internal processes and to have a plan for the continuation of operational business in case of a crisis.

Server and Client Side

System level:

> It is recommended to use dedicated systems for managing infrastructure elements. Further- more, two-factor authentication must be in use for administrators.
> Define identification rules for helper tools used by attackers, such as psexec or rexec.
> A close monitoring of the execution of binaries through the WMI interface is recommended.
> By using integrity-testing tools, you may identify unauthorised changes to system data. They are also useful for assessing the after-effects of an incident.
> Prepare solutions for the monitoring and analysis of your system memory. This increases your chances of quickly recognising complex threats and reacting to them.

Virtualisation:

> Acquire a level of forensic knowledge. This will help you determine whether a VM escape might have occurred.
> Setting up network-sniffing functions may help you in monitoring data traffic between VMs.

Active Directory:

> Have a clear understanding of the relationship of trust between various AD forests.
> Carry out close monitoring of AD logs for unusual and large-scale queries that you would not expect.
> Have emergency action plans ready that cover the possibility of a completely compromised active directory.

Network:

> Use a central and well-monitored interface through which every packet headed for the internet must pass. The same can be applied to incoming data traffic spread through different network zones. You might consider setting up central access zones with load balancers, web application firewalls and authentication gateways that would allow you to centrally monitor incoming data traffic.
> Take a close look at routing paths from the internal network to exposed network areas, for example of a DMZ. Does this traffic also pass through a central and closely monitored interface as mentioned above? If not, put sensors in place that will also monitor this traffic.
> All internet access should pass through a proxy that records every header information, including cookies.
> Collect NetFlow data, not just between the network zones, but also within a zone.
> Besides commercial solutions also use classic, signature-based IDS like Snort or Suricata. This will allow you to quickly establish self-made detection rules in case of a breach.
> Use passive DNS to make sure all domain queries go through the internet and may be quickly and easily retrieved.

Log data:

> Store log files for as long as possible. A minimum of two years is recommended, especially for important systems like domain controllers and gateways.
> Log files must be collected centrally. It is recommended to use a log management concept that covers all networks, and allows to index, search and archive all log files.
> Furthermore, a continuous log analysis needs to be implemented, allowing the automatic -alignment of these log files with known IOCs.
> Log management is an ongoing process. You need to have sufficient resources to keep adding new sources to your system, as your IT landscape will also continue to change.
> Adapt the log settings to your needs. For example, recording user agents may not be the -standard setting, but it is strongly recommended.
> Experienced employees should not only analyse the pre-processed log files, but also check the raw logs for irregularities. For that purpose, sufficient time and personnel resources should be allocated.