Cyberattack – How to Protect Yourself

Checklist for Executive Management in Case of a Cyberattack

Management Summary

1. A good strategy against cyberattacks begins before an actual incident: executive management should consider in advance how to react.

2. When a cyberevent does occur, swift action is required: well-established procedures and escalation paths are crucial to keeping the situation under control.

3. After an attack is before the next attack: a systematic follow-up procedure for cyberattacks is essential.

1. Preparation

General measures by executive management:

> Is there a crisis team for a cyberattack scenario in your company? Have clear competencies and areas of responsibility been defined and gone through with the crisis team?
> Has the crisis team been assigned the necessary resources and powers? (More specifically, support in the areas of crisis management, internal and external communication, law, personnel and technical experts)
> Does the crisis team have an up-to-date manual with relevant contact details of (the competent) representatives of external partners?
> Does the team carry out regular drills in order to be familiar with each other and the roles and responsibilities within the team?
> Is the team familiar with the procedures of law enforcement, or technical consulting by police / contact persons?
> Are there personal connections between your company, or your crisis team, and law enforcement?

Legal measures:

> Are there clearly assigned responsibilities for Management, Communication and Legal regarding if and when it is appropriate to contact the police for consulting, or to request a police investigation?
> Do the responsible parties understand the difference between consulting police and prosecuting police?[1]

2. In Case of Damage

> In case of a private grievance, contacting the nearest police station is advisable.
> In case of a serious problem, i.e. an acute cyberattack against a company, it is important to find specialists as soon as possible. Contact police immediately. On the Suisse ePolice online portal (www.suisse-epolice.ch), you can find the telephone number of a police station near you.
>   > Specialised private companies may help you repair and, if necessary, restore your infrastructure.

[1] Cf. the explanations on page 2.

- The police will consult and support you during further proceedings, particularly regarding the question of whether to pay demanded ransom money.
  Basically, the police are not interested in your business secrets, or in interfering with your infrastructure. However, they do depend on an attacked company's willingness to disclose any traces left by the perpetrators on the systems of the damaged party.
  When a company is under immediate attack, it is advisable to have a technically knowledge-able employee directly contact the police specialists by telephone. It is imperative that this employee has been given internal approval, usually by Management or Legal. The company must have a policy regarding whether Legal sits in on the call.
- The Federal Reporting and Analysis Centre (MELANI) can help you assess what malware you have been affected by, and whether any other companies have been impacted.

3. Follow-up

Is there a systematic follow-up procedure for damage cases (or also "near misses") with regard to continuous improvement?

Areas of potential improvement by follow-up particularly include

- preventive or prompt detection of an incident,
- the quality and speed of incident assessment (extent of damage, criticality, etc.),
- an appropriate and timely reaction/escalation if necessary,
- incident response, both in terms of possible emergency measures for containing the extent of damage as well as identification and correction of root causes and vulnerabilities,
- measures and tools for maintaining adequate emergency operations while responding to the incident,
- internal and external communication,
- effectiveness and efficiency of organisational and technical measures, tools and processes, and also
- internal cooperation as well as cooperation with external parties.

Actively sharing experience in coping with incidents with other parties from the same industry, region or legal environment is another effective follow-up instrument. The insights gained here must be systematically integrated into the quality improvement of internal processes, documentations and exercises, and into the company management and culture.

NEDIK in cooperation with MELANI and Swiss Cyber Experts