MBDA Deutschland GmbH
P.O. Box 1340 – 86523 Schrobenhausen, Germany

Suppliers of MBDA Deutschland GmbH

Date: 2024-04-23
Reference: CS-2304
Your contact: Strategic procurement
Telephone: +49 8252 996211
Fax: +49 8252 996228
E-mail: einkauf@mbda-systems.de

Guidelines for suppliers on behaviour in the event of cyberattacks - Please make available offline

Dear Sir or Madam,

Despite all the precautions we all take now, no company is immune to becoming the victim of a cyber-attack. Our shared supply chain means that our risks are also interconnected. We have therefore compiled these binding guidelines to give you an overview of how you can help minimise the risk to MBDA Germany in the event of a cyber-attack on your company. It is divided into:

1. your contact to MBDA Germany
2. which incidents you should report to us
3. what content the report should contain

1. Your contact to MBDA Germany

In the event of a cyber-attack, you may no longer have access to the contact details of your contact persons. In addition, speed is of the essence when responding to your report. We therefore ask that you send your report to this address if your e-mail system is still functional:

CERT@mbda-systems.de

If you have not received a response from us within one working day, please contact us by telephone. It could be that your e-mail was infected and was rejected by our system.

If you can no longer send an e-mail, please call the following telephone number:

Tel. IT-Security: +49 8252 99 4242 (Mon.-Thurs. 09:00-15:00, Fri. 09:00-14:00)
Plant security: +49 8252 99 6211 (manned throughout)
Fax: +49 8252 99 6228

Here you can reach our plant security team around the clock (+49 8252 99 6211), who will take your report and forward it to the appropriate department. The colleagues on the telephone number given cannot provide you with information on the status of the processing.

One of our first reactions to your report may be to restrict e-mail communication with your company. Therefore, if you need important and/or urgent information or want to give us information after you have made a report, please always use the telephone as well.

2. Which incidents should you report to us?

We have compiled a non-exhaustive list of examples to give you an idea of the type of information we ask you to provide:

- Successful attacks on your IT system
  - IT systems or the entire network have been encrypted
  - Operability of the mail server is restricted
  - No access to your data
  - Knowledge that access data has been lost
  - Detected, unintentional, outflow of data
- Indications of manipulation of the products (possibly without interfering with your IT system), e.g. untraceable interruption of transport, manipulation directly on the material, etc.

Please also report if you suspect that someone is trying to use MBDA's identity (e.g. you receive an e-mail that claims to be from MBDA but you suspect that this is not the case).

3. What information should you provide us with?

Please provide the listed content in your report whenever possible. If you do not have some of the information immediately, please notify us immediately and provide us with the missing information.

Speed before completeness

- Name of your company
- Your name and contact details. Please always include a telephone number, as e-mail communication may be restricted
- Name and contact details of the contact person for handling the incident in your company. Please also include a telephone number.
- Date and time of the attack
- What is affected (your IT system, your office automation, your product, your supply chain, your production system, etc.)?
- Is MBDA data affected, if so, which data (personal data, business data, technical data, officially classified data, strategic data)?
- Are MBDA products affected, if so, which ones?
- Please name the malware used
- Please provide the Indicators of Compromise (IoC)
- Which channel was used for the attack?
- How did you become aware of it?
- Which authorities have already been involved?

Thank you for your support and thank you for implementing this guideline in the event of a cyberattack.

With kind regards

Martin Endres
Chief Information Security Officer

Lukas Gallenberger
National Cyber Procurement Coordinator