Important safety-relevant information re. Miele PG 8527, PG 8528, PG 8535, PG 8536 washer-disinfectors

Dear .....,

According to our records, you are using Miele PG 8528/PG 8527/PG 8535/ PG 8536 washer-disinfectors on your premises. These machines feature a network interface for connection to an in-house network for cycle documentation purposes.

The purpose of this correspondence is to bring an IT security vulnerability to your attention affecting a machine type in use at your site which was discovered in the course of a penetration test carried out by an IT security expert. This only applies to machines which are actually connected to an in-house network. All other machines are not affected and are therefore not at risk. The following applies to machine in a network:

- In the event of an attack on the in-house network of a hospital, a laboratory or a surgery, there is a risk that data from Miele washer-disinfectors can be read out and/or replaced. This data is for the most part binary code.
- Theoretically, a hacker with criminal intent could attempt to make abusive use of this data in order to obtain access to the programme controls and to manipulate these. If pursued to the limit, hackers could even, after further data analysis and with a knowledge of instrument reprocessing, try to falsify cycle records with a view to covering up manipulation. The same applies to unauthorised actions on the part of persons with legal access to the appropriate network.
- To date, there has been no evidence indicating that such an incident has ever occurred. Such targeted manipulation of data, as described above, would require considerable effort and an in-depth knowledge of this highly specific machine software.

Miele considers the risk of a hacker successfully carrying out the multi-stage manipulation described above and causing a potential threat to the health of patients to be extremely low.

Furthermore, we would like to point out that the Miele machines listed above are not designed for direct connection to the Internet. Considering this, there is definitely no risk of a hacker using your Miele machine to obtain access to other equipment or third-party data from the Internet.

Notwithstanding this, we are concentrating all our efforts on finding a solution to stopping this security hole. Once a solution has been found, a Miele employee will contact you to discuss the next steps.

Until such a time, we recommend implementing the following measure in order to minimise risks:

- Do not enable access to the machine via the Internet (e.g. through port forwarding). If your machine is accessible via the Internet, sever any Internet connections immediately.

- Only operate these machines in a separate section of the network (physically separated or protected by access authorisation systems by configuring routers/firewalls). In this network, only operate the systems required for the documentation of reprocessing results (e.g. PC and printer).

- Access to any affected machine and access-authorised systems should be limited exclusively to persons requiring access.

- Access-authorised systems should be protected using strong passwords.
- Alter existing passwords on machines (cf. programming manual).

For the sake of completeness, we would like to remind you in this context of the necessity of routinely checking reprocessing performance alongside verifying cycle records.

The relevant authorities have been informed of the contents of this letter. Please also forward this information to network administrators and all members of staff affected.

Furthermore, we require written confirmation of receipt of this correspondence. For this reason you are requested to complete, sign and return the attached document within 14 days of receipt. Your contact at Miele – and addressee for your response form – is:

…(MPO of subsidiary)
(address, contact no, fax no. or email)

We apologise for any inconvenience, are available to answer any questions you may have, and thank you very much in advance for your cooperation.

Kind regards

…

Response form

Client

Important safety-relevant information / Urgent client information for corrective action in the field - IT security vulnerability

Dear Sir or Madam,
We herewith confirm receipt of your safety-relevant information/client information on corrective action in the field dated xx.xx.2017. We have read and understood the recommendations of the medical device manufacturer.

The machines are connected to a network:
Yes ☐
No ☐

Name/Function: _____

Hospital/Surgery/Laboratory: _____

Street/No: _____

Postal code, town: _____

Place, date_____
Signature_____