"Hafnium": potential impact on processing relationships

Article by Dr. Carlo Piltz, Stefan Hessel and Karin Potel

The Federal Office for Information Security (BSI) continues to warn about critical "Hafnium" security vulnerabilities in Microsoft Exchange servers: companies with unpatched Exchange servers face the threat of attacks from the internet. German companies are affected as well.

From the viewpoint of data protection law, companies acting as controllers are required, at a minimum, to document security updates pursuant to Article 33(5) of the GDPR. In cases where a potential risk cannot be ruled out, notification of the competent supervisory authority is required in accordance with Article 33(1) of the GDPR and, in case of high risk, the circumstances must be communicated to the data subjects in accordance with Article 34(1) of the GDPR.

But not infrequently, Exchange servers are operated not by the controller, but rather by outside service providers, i.e. processors. In such cases, the processors are responsible for checking and monitoring their servers and are required, pursuant to Article 28(1) of the GDPR, to provide sufficient guarantees to ensure that processing conforms to the requirements of data protection law by implementing appropriate technical and organizational measures. In accordance with Article 28(3)(f) of the GDPR, processors are required to assist the controller in ensuring compliance with the obligations specified in Articles 32 to 36 of the GDPR. This requirement particularly applies in the case of the "Hafnium" security vulnerabilities.

Consequences for processing relationships

If the processor does not patch the servers and check if they are compromised, or if its efforts to do so are unsuccessful or come too late, it may be necessary for controllers to notify the data protection authority or even communicate the matter to the data subjects, with the processor's assistance. Regardless of whether notification or communication is required, the breach has to be documented in accordance with Article 33(5) of the GDPR, and in this as well the processor is required to assist. For the controller, documenting the breach is also important with regard to possible recourse claims based on misconduct on the part of the processor, so that it is in both parties' interest for documentation to be as detailed possible.

In addition, the processor's handling of the current vulnerabilities may lead the controller to conclude that the processor is not in a position to guarantee appropriate technical and organizational measures, as required in accordance with Article 28(1) of the GDPR. For example, if the processor is days or weeks late in installing updates or if the processor fails to check if systems are compromised, or does so only inadequately, even though these measures are absolutely required, the controller may conclude on this basis that it can and must no longer rely on the processor's expertise. At the very least, controllers should examine the organizational measures taken by the service provider in this case and request changes if necessary.

If, in the end, there are continuing deficiencies in the processor's measures to ensure compliance with the GDPR, the processing relationship may no longer be permissible and data processing by the processor may have to be discontinued.

Processors which are affected by these circumstances, particularly those which were late in installing updates or failed to check if the system was compromised, are advised to furnish documentation to their controllers demonstrating that they have nevertheless provided sufficient guarantees for the security of processing and/or that the necessary improvements are already underway. Controllers, for their part, should contact affected processors and request the relevant information and documentation so as to comply with their supervisory duties. Sensible documentation may include e.g. full documentation of the handling of an incident, bringing in outside experts or the development of concepts which demonstrably raise the level of security. As things stand, far-reaching consequences are only conceivable in case of a grave breach.

Further action and conclusion

In light of possible recourse claims and the threat of consequences for processing relationships, affected controllers and processors should take immediate action to ensure that "Hafnium" security vulnerabilities are addressed by installing the available updates. In addition, the systems they use should be checked to determine if they have may have been compromised. If they need assistance, valuable resources are available from BSI (only in German) and, in particular, in the self-help guidance from HiSolutions (only in German).

In addition to technical aspects, controllers and processors should also devote more attention to the legal consequences of the security vulnerabilities, which may go well beyond the notification and communication requirements which have been the subject of intense discussion lately.

The Cybersecurity & Data Protection team at reuschlaw Legal Consultants will help you resolve the "Hafnium" security vulnerabilities and provides advice in all legal questions relating to IT security.

[March 2021]

Company contact: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E > melanie.schaumann@reuschlaw.de