Critical vulnerabilities in Microsoft Exchange mail servers

03/12/2021

privacy

press release

In a press release dated March 5, 2021 [1], the Federal Office for Information Security (BSI) informed about existing critical security vulnerabilities in thousands of Exchange servers and requested operators to install the security patches provided by Microsoft. It must be assumed that vulnerabilities have already been used by a group of attackers ("Hafnium") to compromise systems. In addition to the urgent need to install the security patches immediately, operators are required to take specific testing and protective measures according to the recommendation of the BSI [2] and according to Microsoft [3]. If, after a self-examination of the Exchange server, operators find indications of a compromise or a data leak and thus a violation of the protection of personal data, there is an obligation under Article 33 of the General Data Protection Regulation (GDPR) to report the facts to the responsible data protection supervisory authority. In addition to describing the underlying violation, the report must also describe the countermeasures taken in each case in this context. If the data processing body comes to the conclusion after its own examination that the requirements for reporting the facts according to Art. 33 GDPR are not met, this must at least be documented internally according to Art. 33 Para. 5 GDPR. For reports for responsible persons based in Saarland A reporting form [4] is available on the website of the Independent Data Protection Center. [1] BSI press release: BSI - Critical vulnerabilities in Exchange servers - BSI warns: Critical vulnerabilities in Exchange servers (bund.de)[2] BSI recommendations: BSI - Federal Office for Information Security - Several vulnerabilities in MS Exchange[3] Notes from Microsoft: HAFNIUM targeting Exchange Servers with 0-day exploits - Microsoft Security[4] Reporting form

return