Collaborative Discussion 1 – Initial Post – Michael Geiger

The European parliament and the council (2016: 1) declared that: “the protection of natural persons in relation to the processing of personal data is a fundamental right”, as well as of intangible and physical property. To uphold this fundamental right, it is the task of companies, but also government organizations, to take care of the safety of customers and citizens. A breach of this duty of supervision can not only result in reputational damage, but also massive financial damage to people and companies, the leak of personal information, intellectual property or infrastructural damage.

In March 2021, Microsoft's email transport server software, Microsoft Exchange, fell victim to a cyber breach (Morgan, 2021). Microsoft Exchange is a groupware and e-mail transport server software from Microsoft, which is also part of the Office 365 service. It is used for the central storage and management of e-mails, appointments, contacts, tasks and other elements for several users and thus enables collaboration in work groups, which makes the service particularly interesting for companies (Microsoft, 2021a). The program enables internal company planning and communication to be carried out so that sensitive data is stored on the servers (Microsoft, 2021b). The cyber attack on Microsoft Exchange infected more than 120,000 systems (Turton, 2021). The hack was so significant that the United States Federal Bureau of Investigation (FBI) stepped in and removed the vulnerability without the companies' knowledge (Collier, 2021).

The Cyber Security Breaches Survey of 2019 shows that the priority of Cyber Security has increased compared to previous years. Between 2017 and 2019 the costs to companies in the United Kingdom from cyber breaches roughly doubled (Department of Digital, Culture, Media and Sport, 2019: 53). This indicates that cyber attacks are becoming increasingly important and not only companies but also government agencies are interested in Cyber Security. VanSyckel (2018:7) notes that absolute security in cyber space is not possible. It can be concluded from this that cyber security will continue to gain in importance in the future, as further networking with the Internet can lead to new and potentially more dangerous cyber attacks.With this in mind, the designated president of the United States of America Joe Biden, indicated that: “it is more likely we were going to end up in a war, a real shooting war, when a major power it is going to be as a consequence of a cyber breach of great consequence is increasing exponentially” (Bose, 2021).

References:

Bose, N. (2021) Biden: If U.S. has 'real shooting war' it could be result of cyber attacks. REUTERS. Available from: https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/ [Accessed 13.08. 2021]

Collier, K. (2021) The FBI might have gone ahead and fixed your Microsoft email server. NBC News. Available from: https://www.nbcnews.com/tech/security/fbi-might-gone-ahead-fixed-microsoft-email-server-rcna680 [Accessed 13.08.2021]

Department for Digital, Culture, Media and Sport (2019) Cyber Security Breachers Survey 2019. Available from: https://drj.com/wp-content/uploads/2019/04/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF [13.08. 2021]

Microsoft (2021 a) Reimagine productivity with Microsoft 365. Available from: https://www.microsoft.com/en-gb/microsoft-365/business/compare-all-microsoft-365-business-products-b?=&ef_id=a7f984cb17fa1f183b54e5de348dc87f%3AG%3As&ocid=AID2200004_SEM_a7f984cb17fa1f183b54e5de348dc87f%3AG%3As&lnkd=Bing_O365SMB_Brand&msclkid=a7f984cb17fa1f183b54e5de348dc87f [Accessed 12.08.2021]

Microsoft (2021 b) Exchange architecture. Available from: https://docs.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019 [Accessed 13.08.2021]

Morgan, L. (2021) IOTW: Microsoft Echange, The FBI & A Lack Of Patching. Cyber Security Hub. Available from: https://www.cshub.com/executive-decisions/articles/iotw-microsoft-exchange-the-fbi-a-lack-of-patching?preview=1882a995f678930583a8722943f42babe42f1e92 [Accessed 12.08.2021]

The European parliament and the council (2016) Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 12 August 2021]

Turton, W. (2021) Thousands of exchange server still compromised after patches. Bloomberg. Available from: https://www.bloomberg.com/news/articles/2021-03-22/thousands-of-exchange-servers-still-compromised-after-patches [Accessed 12.08.2021]

VanSyckel, L. (2018) Sealevel Systems White Paper – Introducing Cybersecurity. SEALEVEL. Available from: https://www.sealevel.com/support/white-paper-introducing-cybersecurity/ [Accessed 12.08.2021]