Blog Post – Michael Geiger – ISO 27000

Studies show that at 58%, more than half of all security incidents are due to insider threats (Giandomenico & Groot, 2020).
It therefore appears to be a poor approach to restrict security aspects to external influences only. To prevent internal threats, a satisfactory authentication system is required to ensure that information is only available to authorized personnel (3.10 confidentiality)(ISO, 2018). An access control (3.1) based on the "least privilege principle" is ideal for this, in order to only provide necessary information for the employees. This approach increases the security aspects of a software infrastructure, since a malicious employee has to invest more effort in order to be able to carry out a defective action and in the event of a security breach the extent of the damage can be reduced (ISO, 2018).
However, since an attack (3.2) on a company from the inside offers more options for an attacker than an external attack, it is the task of the information security management system (ISMS) professional (3.33) to also recognize this threat and identify suitable countermeasures (ISO, 2018). With regard to this aspect, an intrusion and altering detection system should be implemented, which registers unexpected intrusions into the system and its information (Nagano et al., 2006). In this way, the central pillar of non-repudiation (3.48) can be significantly strengthened and it can be determined at an early stage from which source an intervention in the system was made and whether the infrastructure was weakened as a result (ISO, 2018).
The embedding of the information security management system professional of an intrusion and altering detection system with the approach of the least privilege principle can therefore contribute to greater security in the internal network, since on the one hand hurdles are created for potentially malicious internal staff and on the other hand in the case of an undesired event can occur be recognized early.

References:

Giandomenico, N. & Groot, J. (2020) Insider vs. Outsider Data Security Threats: What's the Greater Risk? Digital Guardian. Available from: https://digitalguardian.com/blog/insider-outsider-data-security-threats [Accessed 13 March 2022].

ISO (2018) Information technology – Security techniques – Information security management systems – Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 13 March 2022].

Nagano, F., Tatara, K. & Sakurai, K. (2006) An intrusion detection system using alteration of data. 20th Internatinal Conference on Advanced Information Networking and Applications. Available from: https://ieeexplore.ieee.org/abstract/document/1620199 [Accessed 14 March 2022].