criminal convictions and thus goes some way to protect us from such insider threats.

Incident management

Incident management is the process of responding appropriately to security incidents by detecting, reporting, assessing, responding to, dealing with, and learning from said incidents (ISO/IEC 27000, 2018). At my school, we have the ability to remotely wipe a user's hard drive if a device is lost so that company information is kept secure.

References

Pillai, AB. (2017). Software Architecture with Python : Architect and Design Highly Scalable, Robust, Clean, and Highly Performant Applications in Python. Packt Publishing.

ISO/IEC 27000. (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 4 August 2024].

OWASP Foundation. (2017) OWASP Top 10. Available from: https://owasp.org/www-project-top-ten/ [Accessed 4 August 2024].

Permalink Add your comment

Managing Human Risk in Cybersecurity: Key Terms and Strategies

Sunday, 11 August 2024, 5:02 PM

by Lauren Pechey

Visible to participants on this course

In cybersecurity, human factors play a pivotal role in the overall security of an organisation. Drawing from the ISO/IEC Standard 27000 (2018), this blog post explores five key terms—Threat, Vulnerability, Threat, Attack and Performance—and how they relate to mitigating cybersecurity risks.

A **Threat** is an unwelcome incident which occurs when employee(s) accidentally or purposefully tries to breach security or access sensitive data (ISO/IEC 27000, 2018). As a solution, Elmrabit et al. (2020) proposed the Bayesian Network-based model, which predicts malicious threats before the organisation's security is compromised. This model helps identify potential attack paths and security breaches, thereby providing proactive threat management.

An **Attack** is one step further than a threat, where a user maliciously exploits a system's weaknesses to compromise the organisation (ISO/IEC 27000, 2018). Inside attacks are particularly challenging because they bypass external security measures. To prevent this, user activities need to be monitored, alongside the implementation of regular security audits and strong access controls (Fonseca-Herrera et al., 2021).

Vulnerability is when an organisation has systematic weaknesses, like poor training or policy gaps, making them exploitable (ISO/IEC 27000, 2018). Minimising these vulnerabilities includes conducting frequent assessments and security protocols (Sharma & Bawa, 2020). This will reduce the organisation's weaknesses and strengthen their safety against cybercriminals.

Information Security is the protection of an organisation's information from being accessed, edited or deleted by unauthorised users (ISO/IEC 27000, 2018). Fonseca-Herrera et al. (2021) proposed a recent model that alerts organisations of their information security status, and enables them to systematically incorporate strict policy adherence and regular employee training. Adopting these kind of models can safeguard systems from cyberattacks.

Finally, **Performance** is how well an organisation's security system is protecting their assets (ISO/IEC 27000, 2018). To ensure security performance is at its peak, companies need to regularly assess, review and update their security software (Fahrurozi et al., 2020). This requires diligent maintenance and ensures an organisation's security status remains strong.

By focusing on these key terms, organisations can better manage the human elements that contribute to cybersecurity risks.

References:

Elmarit, N., Yang, S., Yang, L., Zhou, H. (2020) Insider threat risk prediction based on Bayesian Network. *Computers & Security* 96: . DOI: **https://doi.org/10.1016/j.cose.2020.101908**

Fahrurozi, M., Tarigan, S., Alam Tanjung, M., & Mutijarsa, K. (2020) 'The Use of ISO/IEC 27005: 2018 for strengthening information security management (A case study at Data and Information Center of Ministry of Defence)', *12th International Conference on Information Technology and Electrical Engineering (ICITEE).* Yogyakarta, Indonesia, December. 86–91.

ISO/IEC 27000. (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 6 August 2024].

Fonseca-Herrera, O., Rojas, A., & Florez, H. (2021) A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science* 48(2): [no pagination].

Sharma, A, & Bawa, R. (2022) Identification and integration of security activities for secure agile development. *Springer* 14(2): 1117-1130. DOI: https://doi.org/10.1007/s41870-020-00446-4

Permalink Edit Delete Add your comment

HT

Preventing Internal Cyber Security Attacks Via People Management

Sunday, 11 August 2024, 4:04 PM