I have helped implement, provided operational support for, and performed technical vulnerability testing on many HTTP applications over the past 20 years. I have also been an incident responder for many HTTP application attacks against organizational systems. My personal observation is most organizations I have worked with do not perform in-depth threat modeling of applications despite these applications being exposed to the internet.

While organizations may choose not to pursue threat modeling as a preliminary development step the concepts are mature and freely available. The NIST Secure Software Development Framework (SSDF) defines the steps a software producer should take to ensure security is included in the development process and is abstracted enough that it can be applied to popular development models like agile and waterfall while simultaneously being suitable for software created for any industry (NIST, 2020). The NIST SSDF lists threat modeling as a requirement for an organization to produce well-secured software, stopping short of defining a specific approach, links to more detailed resources are included (NIST, 2020).

The Open Web Application Standard Project (OWASP) has been promoting secure code development for HTTP based applications for more than fifteen years. Similar to other threat modeling guidance it is incumbent on the organization creating the application to identify high impact, high likelihood events that warrant mitigation (OWASP, n.d.).

Table-top discussions can be used to validate the viability of certain types of threat scenarios (Veatch, et al., 1999) , which can ensure those that know the organization best can best assess the likelihood of a specific threat having an impact on the organization. Table-tops that are focused on organizational impacts can include members of the organization outside of the I.T. department such as legal, plant operations and finance. Scenario based threat model development is dependent on the input of domain experts, limiting the view of risks to purely technical elements can result in mitigations implemented that have little value and other risks being overlooked.

Attack trees or threat trees are another approach to identifying threats, while more technical in nature due to the requirement to deconstruct the adversarial goal into a series of steps the path variations can result in hundreds of scenarios for consideration (Widel, et al., 2019). Like table-tops, an attack tree based threat modeling activity will depend on individuals to identify likelihood and impact.

References

Bolivar, H., Jaimes Paradar, H. D. & Roa, O., 2019. Modeling Cloud Computing security scenarios through attack trees. *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI),* pp. 1-6.

NIST, 2020. *Mitigating the Risk of Software Vulnerabilites by Adopting a Secure Software Development Framework (SSDF).* Available from: https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final [Accessed 26 May 2021].

OWASP, (n.d.) Threat Modeling. Available from: https://owasp.org/www-community/Threat_Modeling [Accessed 26 May 2021].

Veatch, J. D. et al. (1999) An airport vulnerabilty assessment methodology. *Proceedings IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology,* pp. 134-151.

Widel, W., Audinot, M., Fila, B. & Pinchinat, S. (2019) Beyond 2014: Formal Methods for Attack Tree–based Security Modeling. *ACM Computer Surveys,* 52(4), pp. 1-36.