Intrusion Detection and Intrusion Prevention Systems

Security professionals are facing a growing risk of data breaches and compliance fines while battling budget constraints and corporate policies. In 2020, IBM has written a report estimating the total cost of a data breach amounts to around $3.86 million on average, globally. Within the report, IBM cites automation technologies as the primary way to cut down on cost (IBM, 2020). Two of such security technologies are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both parts of the network infrastructure. An intrusion detection system (IDS) is a network security system that detects malicious activity in a network. If a detection occurs, the event is logged and reported to an administrator. Intrusion Prevention Systems (IPS) also act as a monitoring device, but depending on the type of attack detected, an IPS furthermore can also help prevent the attack. An IPS acts as a control system that can prevent the delivery of a packet based on its contents (Petters, 2020).

Typically, the following methods are employed in these systems to detect intrusions and enhance network protection (Barracuda, N.D.):

- **Signature-based detection**: the system uses previously defined attack signatures of known network threats for detection. This is similar to what an Antivirus does for software security. Signature-based systems can efficiently detect known threats; however, these systems cannot detect new attack vectors.
- **Anomaly-based detection**: the system detects abnormal or unexpected network behaviour by comparing network events to a trust model. The trust model is established through machine-learning and defines trustworthy, legitimate activity that occurs in the network.

Both systems can detect occurring threats and report on them. The difference is that with an IDS, a human or another system must assess the results and determine what actions to take. With an IPS, on the other hand, the threat response is automated by the system itself. An IPS can drop suspicious packets, block traffic from a specific source or to a specific destination, and interrupt or reset connections (Barracuda, N.D.).

IDS and IPS systems provide companies and organisations with an additional layer of protection for their network infrastructures. They ensure that attempted attacks and unwanted data transmissions are quickly reported and ideally also prevented. The type of protection that should be deployed ultimately depends on the size and architecture of the network in question, as well as on the security requirements set by the management and key stakeholders.

Reference List

Barracuda (N.D.) What is a Intrusion Detection System? Available from: https://www.barracuda.com/glossary/intrusion-detection-system [Accessed 27 October 2020].

Barracuda (N.D.) What is an Intrusion Prevention System? Available from: https://www.barracuda.com/glossary/intrusion-prevention-system [Accessed 27 October 2020].

IBM (2020) Cost of a Data Breach Report 2020. Available from: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ [Accessed 27 October 2020].

Petters, J. (2020) IDS vs. IPS: What is the Difference? Available from: https://www.varonis.com/blog/ids-vs-ips/ [Accessed 27 October 2020].

Post-Discussion Summary:
Intrusion Detection and Intrusion Prevention Systems

Within the scope of the discussion, additional key topics and potential issues concerning Intrusion Detection and Prevention Systems have been highlighted.

Firstly, focusing on false positives that may occur when using these systems offered an insight into the downside of both systems. A false positive state is when a legitimate activity is falsely identified as an attack. In short, a false positive is a false alarm (OWASP, N.D.). In the case of an IDS, this would result in wasted time and resources due to unnecessary logs and notifications created for legitimate activity. The IPS, having the ability to specifically prevent attacks, would even go as far as to block legitimate traffic and thus could result in website functions being disabled or removed for non-malicious users when a false positive occurs.

Furthermore, a closer look at the two methods that are employed in the systems to detect intrusions, namely signature-based and anomaly-based detection, allows us to consider limiting factors for each. With the signature-based detection, which is reliant on a database that stores attack signatures of known network threats for detection, the database needs to be updated continuously to reflect the latest known threat signatures. Even then, a signature-based detection system will not be able to identify and protect against zero-day threats. Anomaly-based detection, on the other hand, requires a certain amount of system data to establish a trust model for legitimate activity. This data might not always be available in the required volume and, further, if available, might include sensitive data that cannot be disclosed.

As a possible solution, Artificial Intelligence and Deep-Learning prove to mitigate the issues of false-positives occurring in IDS/IPS systems, as well as offer capabilities to adapt to new threat patterns. However, for that to be the case, a big enough dataset containing both standard system data and attack data is required for machine learning to be effective.

Reference List

OWASP (N.D.) Intrusion Detection. Available from: https://owasp.org/www-community/controls/Intrusion_Detection [Accessed 13 November 2020].