Availability

Availability within the context of cybersecurity is the quality of information or information systems being accessible to and usable by authorized users whenever demanded. (Joint Task Force Interagency Working Group, 2020). Availability is part of the CIA triad, a conceptual model used to define policies relating to information security within organizations. The CIA triad serves as a high-level checklist in the evaluation of information security processes and tools used by an organization. (Fortinet, n.d.) All three attributes of Confidentiality, Integrity and Availability are complementary to each other but an argument is made by Qadir & Quadri (2016) that the other attributes may not matter if there is no Availability. Figure 1 below presents a modified CIA triad proposed by the authors:

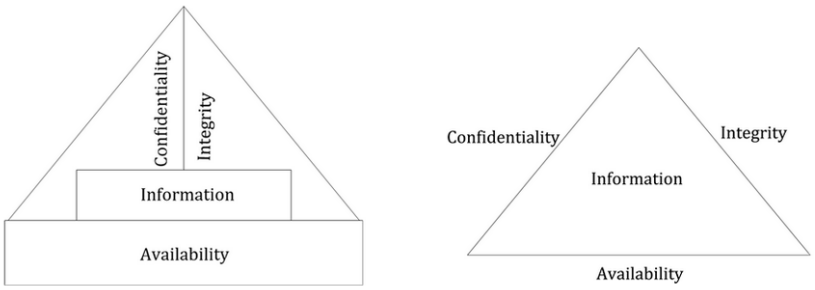

Figure 1. Proposed modified CIA triad versus classic CIA triad (Qadir & Quadri, 2016)

Whenever the information or information systems are unavailable, a denial of service is said to have occurred. Denial of service attacks are the greatest threat to Availability, causing legitimate users to lose access to crucial resources needed to perform tasks.

Scenario

A scenario illustrating the importance of the principle of Availability is considering a Distributed Denial of Service (DDoS) attack on a fictional online fast fashion retailer Vandress.com. Vandress.com is an online-only electronic commerce (e-commerce) business with world a global annual turnover of three billion euros. Customers utilize their website and mobile applications to browse and order clothing items after which the order information is sent to their third-party logistics partners for delivery fulfilment. Several of their logistics partners' networks were breached and malware installed on various endpoints within their networks to make them into a botnet. (Kaspersky, n.d.-b)

With the botnet that has been created from the malware infection, a distributed denial of service attack is launched on Vandress.com, rendering the website unavailable to shoppers worldwide. The outage lasts 36 hours, resulting in two hundred million euros in lost revenue and recovery costs for Vandress.com. Their enterprise resource planning systems used to coordinate operations with their various partners was affected by the outage also.

The immediate impact of this attack is the lost revenue for the period of the outage. Vandress.com is also a wholesale provider of clothing items for certain brands that rely on them for merchandise and order fulfilment. Revenue for these brands also

negatively impacted by the non-availability of the systems, straining business relationships and potentially impacting future revenues.

Phishing

Phishing is a form of social engineering that attempts to trick unsuspecting victims into divulging confidential data or credentials by impersonating a trusted entity through messages and email. (Cybersecurity and Infrastructure Security Agency, 2023)

Dzuba & Cash (2023) in a 2023 report on phishing, estimated that 90% of successful cyber attacks start with email phishing.

Business email compromise attacks aim at inducing the victim to make a financial transaction. An estimate by the Federal Bureau of Investigation (2023) on the cost to victims of global business email compromise attacks between October 2013 and December 2022 is 50 billion U.S. dollars.

Impact on a system

Successful phishing attempts allow malicious actors unauthorized access to critical systems. These malicious actors may use this unauthorized access to install malware allowing them lateral movement onto or infection of other systems within the network they are on, compromising more systems. Such malware can include ransomware, which is malicious software that prevents or blocks access to a victim's files or systems usually by encryption. The malicious actor then requires payment of a ransom before access is restored. (Federal Bureau of Investigation, n.d.)

Cyber Incidents

Honda: A ransomware incident involving auto maker Honda that occurred in 2020 utilized phishing emails to obtain Active Directory credentials of employees. The attack disrupted automation systems within its North American facilities, forcing them to shut down operations in affected plants to be able to restore system functionality from backups. The ransom demanded by the attackers was not paid. A similar incident occurred with the IT and automation systems of German auto parts manufacturer Gedia. Gedia is believed to have negotiated with the attackers to pay the ransom. (Benmalek, 2024)

These incidents showcase the impact phishing has on the overall system and network security. The complexity and ease of execution of a phishing attack is low, making it a risk to all systems within a network whether the attack is targeted or not.

Figure 2 below shows the ransomware process:

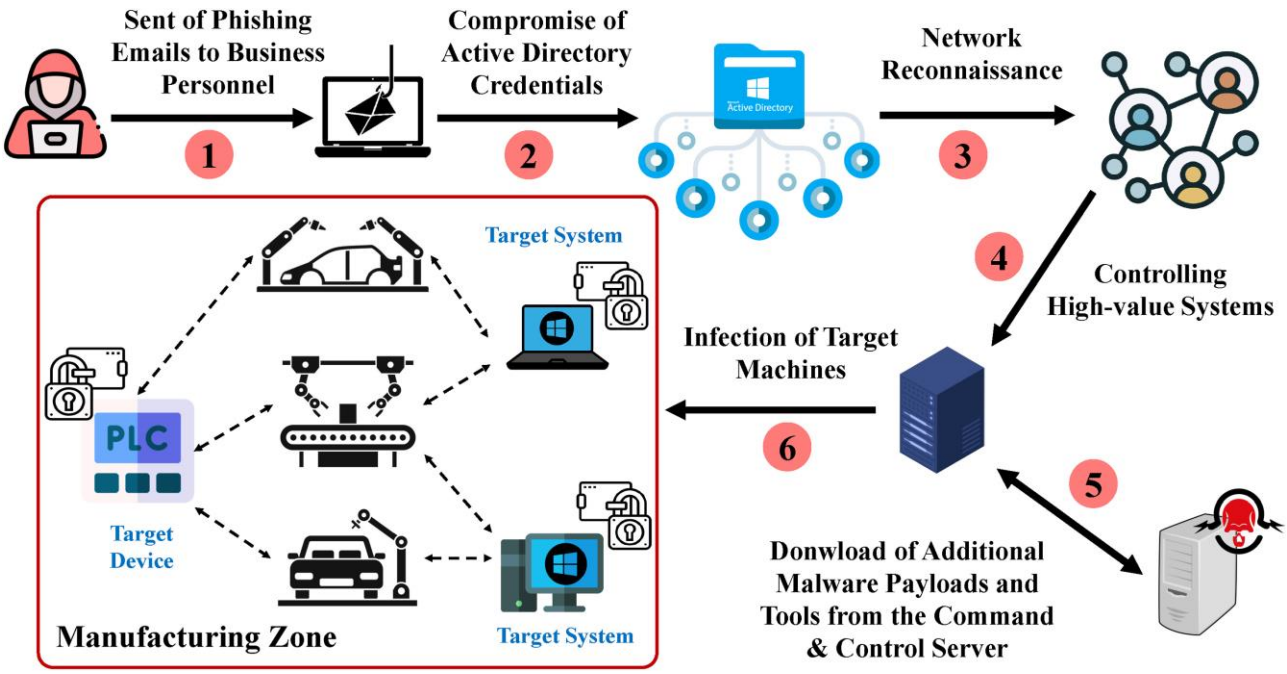

Figure 2. Ransomware process (Benmalek, 2024)

IDS/IPS

Intrusion detection/prevention systems are security tools used to monitor and respond to attempted attacks within a network. Intrusion detection systems identify evidence of threats and alert system and network administrators to act while intrusion prevention systems proactively identify threats and act punitively to thwart them. These systems may be host-based, monitoring files and resource usage on network hosts or network-based, monitoring network traffic. These systems perform their functions using three methods namely, Signature information-based method: Anomaly-based method and Hybrid-based method.
Figure 3 below shows a comparison of both systems within a corporate network:

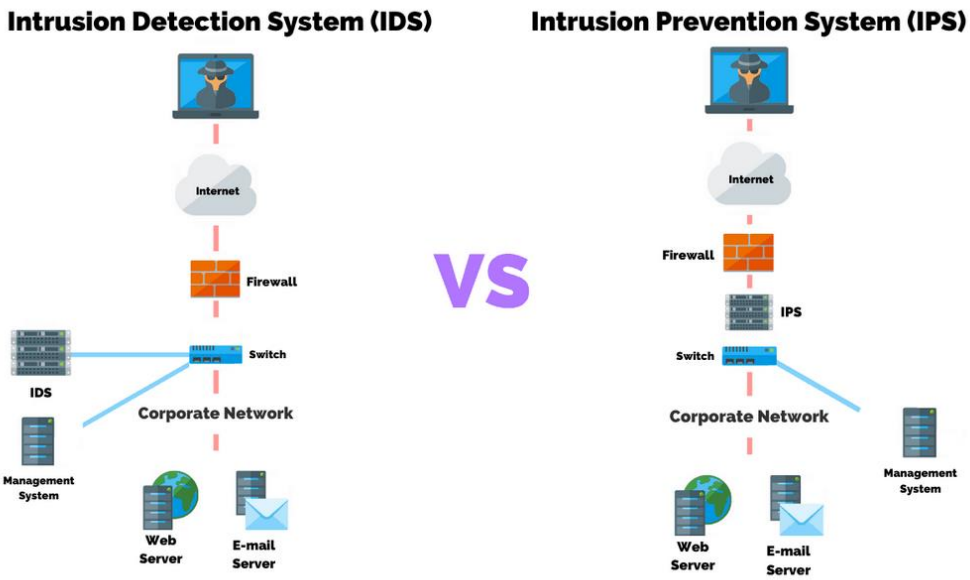

Fig. 3. Intrusion detection system and intrusion prevention system within a corporate network (Swanagan, 2019)

Signature Information-based monitoring method

An intrusion detection/prevention system operating with the signature information-based monitoring relies on identified patterns of malicious activity to detect and prevent attacks.

Strengths

- **Accuracy**: This method is fairly accurate because it uses identified signatures of known threats.
- **Efficiency**: This method is efficient because it uses known signatures to identify malicious activity. It has a low False Alarm Rate and detects most known attacks with low computational overhead. (Abdulganiyu et al., 2023)

Weaknesses

- **Evasion**: This method may be easy to evade because it uses identified signatures of known threats. Attackers may modify known techniques to avoid detection by the monitoring methods.
- **Maintenance Overhead**: This method may require significant overhead of information databases on known attack signatures, requiring computational power.
- **Zero-day and unknown threats:** This method may be susceptible to zero-day attacks and lesser or unknown threats not within its signature database.

Anomaly-based monitoring method

An intrusion detection/prevention system operating with the anomaly-based monitoring relies on deviations from normal network or host activity to detect and prevent attacks. A baseline is established to monitor activity against and activities that are significantly deviant from the established baseline. (Abdulganiyu et al., 2023)

Strengths

- **Detection of Unknown Threats**: This method is effective against lesser or unknown threats.
- **Adaptability**: This method is more adaptable to any changes in approach of known attack to evade detection.

Weaknesses

- **False Positives**: This method is susceptible to generating false positives for non-malicious changes in activity. This puts significant strain on human and computational resources in responding to threats. (Abdulganiyu et al., 2023)
- **Context of edge cases**: This method requires contextualization of its detection rules to ensure it covers edge cases of deviation from the activity baseline which may be hard to build into the logic of the detection rules. (Abdulganiyu et al., 2023)

Hybrid-based monitoring method

An intrusion detection/prevention system operating with the hybrid-based monitoring relies on identified patterns of malicious activity as well as known attack signatures to detect and prevent attacks.

Strengths

- **Comprehensive Detection**: This method leverages the strengths of anomaly-based and signature information-based methods.

Weaknesses

- **Complexity:** This method may be complex to implement and maintain due to the expertise required to utilize both detection methods.
- **Resource Intensive:** This method may be more resource intensive due to the corroboration it has to perform in identifying threats.

Cybersecurity Frameworks

A cybersecurity framework serves as a common organizing structure for approaching cybersecurity by assembling standards, guidelines and best practices to improve cyber security and resilience regardless of size or sophistication. (National Institute of

Standards and Technology, 2018) It is a flexible way to address cybersecurity concerns for organizations that rely on connected information technology to operate and provides a widely acceptable way to identify their exposure to cyber risks and implement mitigation strategies for identified risks. Frameworks also help organizations find solutions fit for their risk appetites and tailored to their unique cyber risks. (National Institute of

Standards and Technology, 2018) Different cybersecurity frameworks exist to address the needs of different organizations within the context of their functions with one such as the Payment Cards Industry Data Security Standard for organizations that deal with customer credit or debit card information and the Healthcare Insurance Portability and Accountability Act for organizations that deal with electronic health data. (Cisternelli, 2024)

Cybersecurity frameworks are important to organizations to ensure business continuity avoiding loss of reputation and revenue as well as avoiding breaches of the law in the event of a cyber incident occurring. The benefits of a framework can be illustrated by comparing two companies, ACME Corporation, a midsize marketing startup with an annual turnover of one hundred million euros, fifty full time employees as well as a five-man information technology team and Dexacorp Financial Services Limited, a Fortune 500 global financial services provider with an annual turnover of two billion euros, a four hundred rack space data centre, five thousand full time employees as well as a forty-man information security team. Both companies are victims of the WannaCry ransomware attack that occurred in 2017. (Kaspersky, n.d.-a) Their respective information security teams had implemented the necessary controls and ensured their employees, customers and partners followed best practices when accessing these information systems which minimized the impact of the attack. This is because both companies regardless of their size and annual turnover, were able to implement the same basic standards of protection which minimized the impact of a devastating ransomware attack that may have cost

them millions in recurring revenue and their reputations amongst their clients and business partners, impacting future revenue as well.

SOC2 Framework

The Service Organization Control 2 is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy against the defined standards in the Trust Services Criteria (TSC) defined by the American Institute of Certified Public Accountants (AICPA). A SOC2 report provides assurances to users on the reliability of the systems and privacy of the information processed by the systems of organizations that provide services to users. (American Institute of Certified Public Accountants, n.d., 2023)

To illustrate the use of the framework to improve the cybersecurity posture for an organization, a data centre company, ACME Data Centres Limited will be considered. ACME is headquartered in Dublin in Ireland but operate in fifty countries worldwide. They offer bespoke colocation and cloud services to their enterprise customers within their data centres. They have clientele from a diverse range of industries with many of their customers operating within the financial services, logistics and healthcare sectors. Due the sensitivity of information that is collected, stored, and processed by their client's information systems, ACME has decided to implement the controls within the SOC2 framework to provide assurances to their customers of the safety of their services.

Components

The main components of the SOC2 are the Trust Services Criteria namely:

- Security: This criterion assesses the information systems for levels of protection against unauthorized access, disclosure of information and damage to systems that could compromise their availability, integrity, and privacy of information. (American Institute of Certified Public Accountants, 2023) ACME Data Centres may implement physical controls such as perimeter security patrols and logical access controls such as internal network firewall appliances.
- **Availability:** This criterion assesses the accessibility of the information systems for operation, monitoring, and maintenance. It does not set minimum acceptable performance levels, functionality or usability of specific systems. (American Institute of Certified Public Accountants, 2023) ACME Data Centres may implement network redundancies to ensure customers are able to always access their collocated equipment remotely.
- **Processing Integrity:** This criterion assesses the information systems for their ability to consistently deliver results consistent with their functions. (American Institute of Certified Public Accountants, 2023) ACME Data Centres may implement controls to ensure changes within data stores are recorded appropriately.
- **Confidentiality:** This criterion assesses the information systems for their ability to protect information designated by their customers as limited for use or access to defined parties. ACME Data Centres may implement controls that ensure traffic over their internal data centre network is encrypted and their customer database is properly secured against breaches.
- **Privacy:** This criterion assesses the information systems for their ability to protect personal information that is collected, processed, and stored by the organization. Examples include databases of personal information of ACME Data Centre employees.

References

Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, *22*(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

American Institute of Certified Public Accountants. (n.d.). *SOC 2®—SOC for Service Organizations: Trust Services Criteria | AICPA & CIMA*. Retrieved May 10, 2024, from https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

American Institute of Certified Public Accountants. (2023, September 30). *Https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022*. 2017 Trust Services Criteria (With Revised Points of Focus – 2022). https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, *4*, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Cisternelli, E. (2024, February 27). *7 Cybersecurity Frameworks That Help Reduce Cyber Risk (List & Resources)*. 7 Cybersecurity Frameworks That Help Reduce Cyber Risk (List & Resources). https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk#HIPAA

Cybersecurity and Infrastructure Security Agency. (2023). *Phishing Guidance: Stopping the Attack Cycle at Phase One*.

Dzuba, & Cash, J. (2023, August 16). *Introducing Cloudflare's 2023 phishing threats report*. https://blog.cloudflare.com/2023-phishing-report

Federal Bureau of Investigation. (n.d.). *Ransomware—FBI*. Retrieved May 11, 2024, from https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware

Federal Bureau of Investigation. (2023, June). *Business Email Compromise: The $50 Billion Scam*. https://www.ic3.gov/Media/Y2023/PSA230609

Fortinet. (n.d.). *What is the CIA Triad and Why is it important? | Fortinet*. Retrieved May 11, 2024, from https://www.fortinet.com/resources/cyberglossary/cia-triad

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kaspersky. (n.d.-a). *Ransomware WannaCry: All you need to know*. Ransomware WannaCry: All You Need to Know. Retrieved May 9, 2024, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kaspersky. (n.d.-b). *What is a Botnet?* Retrieved May 12, 2024, from https://www.kaspersky.com/resource-center/threats/botnet-attacks

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Swanagan, M. (2019, October 3). *Intrusion Detection VS Prevention Systems: What's The Difference?* https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/