WHITEPAPER

2024

CYBER RESILIENCE: FORTIFYING DEFENSES IN THE FACE OF PERSISTENT THREATS

SEPT
2024

rewterz

Organizational tech teams use diverse tools, techniques and services to attain the cyber security posture of their choice. However, there is a tech trend that most will agree on: in today's landscape of increased connectivity and reliance on IT, the question that tech teams focus on should not be "whether" security breach will happen to their IT infrastructure but "when" such an attack will occur.

Alarming cyber security stats within the last year indicate that cyber resilience should be a core strategy of every IT team. After reading this article, you will be able to differentiate between cyber resilience and traditional cybersecurity, recognize different types of persistent threats and identify effective strategies for cyber resilience for your organization.

Understanding Cyber Resilience

In order to fortify your organization's resistance to cyber attacks, a combined strategy of cyber security and cyber resilience is key to adopt.

Cyber security refers to the use of standard tools such as anti-virus software, multifactor authentication and regular device updates, to create tangible and crucial layer of protection for your organization's networks.

Cyber resilience however, goes one step further, evaluating people and processes in order to determine vulnerabilities within an organization's defenses, and ensure a company's ability to absorb and recover quickly from cyber assaults.

Some of the key components of cyber resilience can include:

- Ensuring the availability of offline backup capabilities.
- Implementing Multifactor Authentication
- Enhancing staff cyber security training and awareness to prevent human error.
- Preparing recovery strategies for public relations crises resulting from cyber attacks.
- Regularly conducting attack simulation exercises to boost business preparedness for cyber attacks.
- Developing a business continuity plan.

Cyber resilience, working synergistically with cyber security strategies, ensure that businesses develop a robust and well-rounded protection plan that can enhance business functions and reputation.

Identifying And Combating Persistent

Cyber threats intended to immobilize IT systems to extract ransom from businesses (ransomware) have gained notoriety. Other popular attacks known as Advanced Persistent Threats (APT) are steadily gaining ground.

An APT is an intentional, prolonged cyber attack intended to stealthily enter networks and linger there undetected, stealing sensitive information for the intruder to exploit later. APTs are generally carried out by well-funded and sophisticated groups, and can sometimes be a state-sponsored attack, with an element of espionage, in order to steal national security information. At other times, the goal can be grand theft of highly valuable and sensitive user data such as national identity markers and financial codes. This is the more popular motivation for APTs as IBM identified that 32% of cyberincidents involved data theft and leak, indicating that attackers favor stealing and selling data, rather than encrypting it for extortion.

Strategies for identifying persistent threats include Threat Intelligence and Monitoring, Anomaly Detection and Incident Response Planning.

TOOLS AND TECHNOLOGIES FOR ENHANCING CYBER RESILIENCE

Firewalls can be the first line of defense in a company's network security, controlling incoming and outgoing network traffic based on predetermined security rules. By creating a barrier between the internal network and external sources, they prevent unauthorized access and potential threats.

Intrusion Detection/Prevention Systems (IDPS) complement firewalls by continuously monitoring network traffic for suspicious activities and potential intrusions. They can detect and respond to threats in real-time, blocking malicious activities before they cause damage. Together, these tools significantly enhance a company's ability to prevent and detect cyber attacks, bolstering overall cyber resilience.

Endpoint Detection and Response (EDR) solutions monitor, detect, and respond to persistent threats on endpoints, such as laptops, desktops, and mobile devices. These tools provide visibility into endpoint activities, identify suspicious behaviors, and enable rapid response to threats. By continuously analyzing data from endpoints, EDR solutions can detect advanced threats that traditional antivirus software might miss. This proactive approach helps in containing and mitigating attacks, reducing the impact on the organization, and enhancing its ability to recover quickly.

Security Information and Event Management (SIEM) systems collect and analyze security data from various sources across the network, providing a comprehensive view of an organization's security posture. They correlate data from logs, network traffic, and other sources to identify patterns and anomalies indicative of potential threats. SIEM systems enable real-time threat detection, incident response, and compliance reporting. By centralizing and automating security monitoring and analysis, SIEM systems help organizations quickly identify and respond to security incidents, improving their overall cyber resilience.

Backup and recovery solutions are essential for ensuring data availability and integrity in the event of a cyber attack, such as ransomware, or other disasters. Regularly backing up critical data ensures that it can be restored to its original state if it is compromised or lost. Effective backup and recovery strategies include automated, frequent backups, secure storage of backup data, and regular testing of recovery procedures. By ensuring that data can be quickly and reliably restored, these solutions minimize downtime and data loss, contributing significantly to an organization's ability to recover from cyber incidents and maintain business continuity.

Cloud security tools are designed to protect data, applications, and services hosted in the cloud. These tools include cloud access security brokers (CASBs), encryption solutions, identity and access management (IAM), and more. They provide visibility into cloud usage, enforce security policies, and protect against data breaches and other threats specific to cloud environments. As organizations increasingly adopt cloud services, ensuring robust cloud security is critical. Cloud security tools help safeguard sensitive data, maintain regulatory compliance, and protect against cloud-specific vulnerabilities, enhancing an organization's overall cyber resilience by securing its cloud-based assets and operations.

TESTING AND MEASURING YOUR ORGANIZATION'S CYBER RESILIENCE

Regular testing and assessments are critical for maintaining and improving an organization's cyber resilience. They help identify vulnerabilities, ensure compliance with security policies, and validate the effectiveness of security controls. By routinely evaluating the security posture, organizations can proactively address weaknesses, adapt to new threats, and ensure that their defenses are robust and up-to-date. This proactive approach reduces the risk of successful cyber attacks and enhances the ability to respond swiftly and effectively when incidents occur.

METHODS FOR TESTING CYBER RESILIENCE

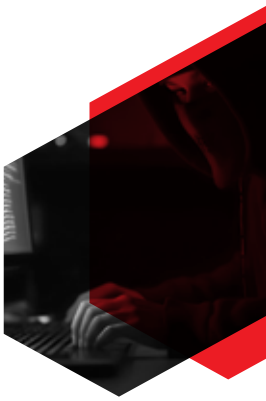
Penetration testing involves simulating cyber attacks on an organization's systems to identify vulnerabilities that could be exploited by attackers. By uncovering weaknesses in security measures, penetration tests provide valuable insights into potential points of failure, allowing organizations to strengthen their defenses before an actual attack occurs.

Red teaming exercises involve a group of security professionals (the red team) simulating advanced persistent threats against the organization, while another group (the blue team) defends against these attacks. This realistic simulation tests the organization's detection, response, and recovery capabilities, highlighting areas for improvement in incident response strategies and enhancing overall cyber resilience.

Tabletop exercises and simulations are discussion-based sessions where team members walk through hypothetical cyber incident scenarios. These exercises help organizations evaluate their incident response plans, improve coordination among different teams, and identify gaps in their procedures. By practicing response strategies in a controlled environment, organizations can better prepare for real-world incidents, enhancing their ability to manage and recover from persistent threats.

KEY METRICS FOR MEASURING CYBER RESILIENCE

Mean Time to Detect (MTTD) measures the average time it takes for an organization to identify a security incident after it has occurred. A shorter MTTD indicates that the organization is effective at quickly identifying threats, which is crucial for minimizing the impact of cyber attacks and preventing further damage.



Mean Time to Respond (MTTR) measures the average time it takes for an organization to respond to and mitigate a detected security incident. A lower MTTR reflects the organization's ability to efficiently contain and remediate threats, reducing the duration and impact of cyber incidents.

RECOVERY TIME OBJECTIVES (RTO) AND RECOVERY POINT OBJECTIVES (RPO)

Recovery Time Objectives (RTO) define the maximum acceptable downtime for critical systems before business operations are significantly affected.

Recovery Point Objectives (RPO) specify the maximum acceptable amount of data loss measured in time. Together, RTO and RPO help organizations set goals for restoring systems and data after an incident, ensuring that recovery processes are efficient and effective. By achieving these objectives, organizations can minimize disruption and maintain business continuity, enhancing their overall cyber resilience.

Cyber resilience must be recognized as a priority for organizations, distinct from their cyber security measures. Investing in cyber resilience measures can enhance detection and recovery time, creating an invaluable reputation for security and reliability for the organization.

Remaining knowledgeable about cyber resilience tools is valuable for in-house tech professionals. Partnering with a trusted cyber security provider is a key step that ensures an organization's preparedness for constantly evolving persistent threats.

Rewterz is an international cyber security service provider that protects organizations with best-in-class data security tools. To learn more about how your organization can enhance its cyber resilience posture and stay one step ahead of persistent threats, contact a Rewterz expert today.