IS YOUR SECURITY INCIDENT RESPONSE PLAN YOUR WEAKEST LINK?

When it comes to security incident response, the saying “failure to plan is planning to fail” resonates deeply. We often get consumed with the latest tactics to prevent attacks but overlook the importance of a robust approach to security incident handling. Without a well-defined and comprehensive incident response plan in place, organizations are ill-prepared to handle security breaches, leaving them vulnerable to extensive damage and prolonged disruptions.

According to the *Cyber security skills in the UK labour market 2023* report, a quarter of businesses don’t regard incident response skills as essential. Almost half said they weren’t confident they could put together an incident response plan (IRP), which led to 41 percent saying they were not very or not at all confident that they would be able to deal with a cybersecurity breach or attack.

When an incident occurs, time is of the essence

Ensuring that organizations have a strong process for security incident handling is important for several reasons. First and foremost, it helps an organization minimize the impact of security incidents, which can include data breaches, network intrusions, malware infections, and other cyberattacks. By having a well-defined incident response plan in place, an organization can detect and respond in a timely manner, potentially reducing the amount of damage caused and the associated costs.

While not all cases of a data breach will lead to fraud or identity theft, compromised data is still an

expensive business for companies. The repercussions stretch further to impact consumer trust and brand reputation, not to mention the mental health of customers and the financial health of the business.

Building a culture of trust

As hackers are now using artificial intelligence (AI)-powered tools for increasingly sophisticated attacks, IT and security teams are striving more than ever to keep ahead of cybercriminals. The need for adequate staff training, as well as creating an atmosphere of trust to report any issues has never been greater. Rigorous training of staff to help recognize phishing emails and malicious activity—and understand how to report them—is a must. Employees who feel trusted they will be more likely to report an incident without fear of reprisals instead of ignoring it.

The quicker an organization can respond to a security incident, the better. That means effectively containing the damage to prevent further compromise and minimize the risk of an incident escalating and causing widespread disruption, financial loss, or reputational damage.

Preserve evidence and comply with industry regulations

A well-executed incident response plan can help restore affected systems and services to normal operation as quickly as possible, minimizing disruption to business operations and maintaining customer trust. Incident response plans also help organizations demonstrate their commitment to safeguarding sensitive information and complying with relevant laws and regulations by preserving evidence related to the security incident, which may be crucial for investigating and prosecuting cybercriminals. Properly collecting and preserving evidence can also support an organization's efforts to understand an incident and improve its security posture to reduce the likelihood of it happening again.

Identifying the right solutions for security incident handing

Security teams must often rely on an IT service management (ITSM) tool that has a "security" category under "IT incident." But this is not fit for purpose because it provides little flexibility and does not enable teams to create standard processes for handling different types of security incidents. It is also difficult to collaborate across teams as needed.

Leverage BMC Helix for security incident handling

BMC Helix has worked hand in hand with key customers to design a pre-built security incident handing solution based on industry best practices and customer feedback. The solution aligns tightly with industry and government standards such as NIST 800-61 and ISO 27001, so that each phase of the incident management lifecycle—identification, investigation, response, and remediation—is methodically addressed. Preconfigured runbooks are provided to address common security scenarios, help standardize the activities in each phase, and provide collaboration and integrations to ensure all essential areas and teams are part of the activities.

The solution is the missing piece in many organizations' security operations (SecOps) posture and solutions, bringing together prevent-and-respond processes and associated teams while also providing regulatory audit and evidence constructs and key lessons learned, which then become

part of the prevention activities.

Extending Service Management Across the Enterprise

BMC's security incident handling solutions is part of a suite of preconfigured out-of-the box workflow solutions which enable organizations to extend the value of BMC Helix for Service Management beyond IT and across their enterprise.

Learn more: BMC Helix Enterprise Service Management - BMC Software

Watch Video: BMC Helix Enterprise Service Management - Security Incident Handling - YouTube