mailmeteor

Mailmeteor’s Incident Response Plan

Incident response is a key aspect of Mailmeteor’s overall security and privacy program. We have a rigorous process for managing incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

Mailmeteor’s incident response program is managed by expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident.

Detection and Analysis

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of this procedure.

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, Mailmeteor will perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced.

These analyses can be performed either manually or utilizing automated tools depending upon the situation, timeliness, and availability of resources.

An incident will be categorized as one of four severity levels. These severity levels are based on the impact. The below table provides a listing of the severity levels and a definition of each severity level.

0 (Low)	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. Users' data or Mailmeteor's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting
3 (Extreme)	Incident where the impact is catastrophic. Examples may be a shutdown of all [municipality or county name]'s network services. Users' data or Mailmeteor's proprietary or confidential information has been compromised and published in/on a public venue or site.

Remediation

Mailmeteor's security team is responsible for eradication and will document all eradication activities during an incident. Remediation efforts for a security incident involve the removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may

have been exploited, and identification of other hosts that may have been affected within the organization.

Post-Incident Activity

Following the successful remediation and resolution of a data incident, our security team evaluates the lessons learned from the incident and shares its results with the rest of the company.

When the incident raises critical issues, Mailmeteor's CIO may initiate a post-mortem analysis. During this process, our security team reviews the cause(s) of the incident and identifies key areas for improvement. In some cases, this may require discussions with different product, engineering, and operations teams and product enhancement work.

If follow-up work is required, our security team develops an action plan to complete that work and assigns project managers to spearhead the long-term effort. The incident is closed after the remediation efforts conclude.

Disclaimer

The content contained herein is correct as of April 2022, and represents the status quo as of the time it was written. Mailmeteor's security policies and systems may change going forward, as we continually improve protection for our customers.

Make sure to regularly check our Privacy Policy and Security Center to stay up to date.