

Report on Patient Privacy Volume 21, Number 8. August 12, 2021 Conti Defense Security Checklist

By Jane Anderson

To defend against ransomware threats such as Conti, the HHS publication *Health Industry Cybersecurity Practices* recommends the following best practices:

- Provide social engineering and phishing training to employees.
- Develop and maintain policy on suspicious emails for end users, and ensure that suspicious emails are reported.
- Ensure emails originating from outside the organization are automatically marked before they are received.
- Apply patches and updates immediately after release/testing, and develop and maintain a patching program, if necessary.
- Implement an intrusion detection system, and keep signatures and rules updated.
- Implement spam filters at the email gateways, and keep signatures and rules updated.
- Block suspicious IP addresses at the firewall, and keep firewall rules updated.
- Implement whitelisting technology to ensure that only authorized software is allowed to execute.
- Implement access control based on the principle of least privilege.
- Implement and maintain anti-malware solutions.
- Conduct system hardening to ensure proper configurations.
- Disable the use of server message block protocol SMBv1 (and all other vulnerable services and protocols), require at least SMBv2, and restrict/minimize/eliminate remote desktop protocol usage.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)