algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

5 Tips to Prevent and Mitigate a Ransomware Attack

1 Clean up and tighten firewall rules

Unused, duplicate, or conflicting firewall rules make it harder to manage your network. Overly permissive and unused rules provide an open door for attackers to slip in.

2 Analyze the risks and vulnerabilities on your network

Identify the risks in your network security policies. Map vulnerabilities to their related firewall rules.

3 Keep the bad guys from running wild with network segmentation

Using network segmentation, you can build a defense-in-depth strategy to reduce your attack surface. If the bad guys get in, they won't be able to get very far.

4 Identify where your hybrid network is exposed to public networks

It's hard to secure what you can't see. A full topology map and traffic query simulation of your entire hybrid network will provide those insights and keep you from flying blind, so you can identify where your network is exposed.

5 Respond to incidents coming from SIEM/SOAR solutions with rapid isolation

Tie security incidents to network traffic. This way, you can understand if a compromised server is open to the web. Have measures in place to immediately isolate the infected server.

On average, ransomware attacks last

16.2 Days

Source: Coveware

By 2021, the cost of global ransomware damage is predicted to reach

$20 Billion

Source: Cybersecurity Ventures

Find out more www.algosec.com/ransomware