SecurityRisk
ADVISORS

Ransomware Strategy Assessment

Ransomware is an increasingly common threat with serious business implications. We will conduct a review of your existing controls and processes for preventing and detecting ransomware, develop or improve on your existing incident response playbook, and test the IR process with a Table Top Exercise.

Architecture and Process "Preparedness" Review

We review the current ransomware incident response plan / SIRT documentation and conduct interviews with key stakeholders to deepen our understanding of your ransomware Incident Response capabilities. We then perform a technical review of the tools in your environment to ensure that they are configured effectively to prevent and detect ransomware in your environment. We review the following preventative detection controls:

- SIEM Alert Management
- Malware Behavioral Analysis Protection
- Intrusion Protection
- Anti-Virus Software
- Process Whitelisting
- File Share Protection
- User Awareness Training
- Privileged Account Management
- Flow Data Analysis

Ransomware Playbook Development

We will create a practical guide for handling ransomware related security incidents. We will build on the Process Review activity to help you further define and develop your ransomware Incident Response capability in the event of a specific Ransomware threat. We will update the Incident Response Workflow (IRW), its documentation and templates. Deliverables include:

- Ransomware IRW Workflow Diagram
- Ransomware Incident Response Policy, Plan & Reporting Templates

Ransomware IR Table Top Exercise

When the Ransomware IRW and Playbook have been updated, we will conduct a table-top exercise to simulate use of the updated Ransomware IRW process and templates. We will incorporate lessons-learned and update templates based on the table top exercise and present the final Ransomware Incident Response Program documents.

Contact Us

Phone: 215.867.9051
Email: info@securityriskadvisors.com
Website: www.securityriskadvisors.com

Related Services

Vendor Management

You've hardened your business environment internally to address the threat of ransomware, but have your vendors? If you leverage third-parties to manage systems or devices, you need to be sure that those systems are protected. Most organizations don't have these systems and devices inventoried with roles and responsibilities documented appropriately. When ransomware hits, it's a scramble to find them all and get the vendors to fix it. In these cases, time is money! We will review and document your third-party managed systems to strengthen your response and remediation capability.

Purple Team Exercise

We work side-by-side with your security analysts to validate the effectiveness of current detection capabilities as well as identify, improve and tune detection gaps in existing defensive toolsets. We will lead "Purple Team" scripted attack simulations to test rules, identify gaps, and transfer knowledge to your team members.

We work with your security team to understand the indicators of attack and steps taken that allowed successful exploitation, escalation, and lateral movement on the internal network. We will execute various testing scenarios across the cybersecurity "kill chain."

About Our Company

SecurityRisk
ADVISORS

Security Risk Advisors provides expert consulting services with specializations in advanced threats controls implementation and 24x7 operation, red and blue teams, control frameworks, and GRC process improvement. Our approach emphasizes ongoing knowledge transfer and access to our analysts.