Ransomware Discussion

International Federation of Health Plans – October 2020

Incident Response
FORENSIC & CYBER

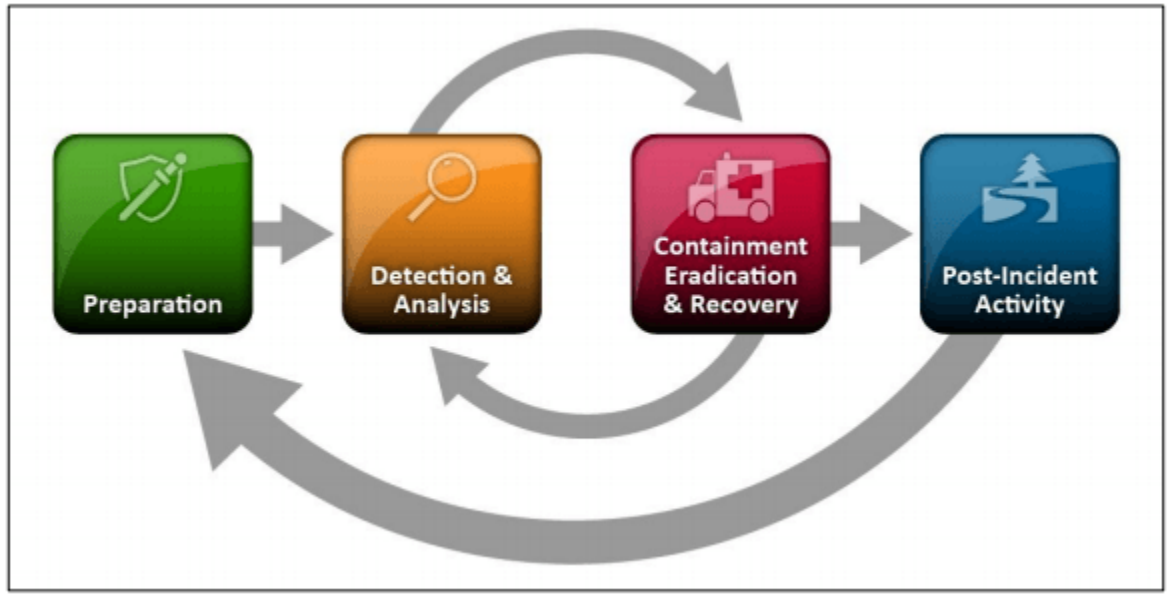
NIST


RECOVER
IDENTIFY
RESPOND
CYBERSECURITY
FRAMEWORK
VERSION 1.1
PROTECT
DETECT

Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks.

The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

Your Incident Response processes should analyse security events to learn how to prevent future attacks and attempt to recover stolen data.



Preparation

Manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident.

Create, maintain, and exercise a basic cyber incident response plan (and playbooks) and associated communications plan that includes response and notification procedures for a ransomware incident.

Run regular cyber simulations to evaluate the effectiveness of the incident response plan, and drill the training into the CSIRT team.

Clearly define and allocate roles and responsibilities in advance, and have a backup option for each.

Roles and Responsibilities

An incident response plan clearly sets out the roles and responsibilities of those involved in the incident response.

Privacy officer

Information security and ICT

Legal

Communications

Risk and assurance

Service delivery/operations

Senior leadership team

Ransomware **Prevention** Checklist

Key Best Practices		Additional Best Practices
• User Education • Allowlisting • Account Control • Backups • Workstation Management • Host-Based Intrusion Detection / Endpoint Detection and Response • Server Management • Server Configuration and Logging • Change Control	• Network Security • Network Infrastructure Recommendations • Host Recommendations • User Management • Segregate Networks and Functions • Physical Separation of Sensitive Information • Virtual Separation of Sensitive Information	• Vulnerability assessments • Encryption of sensitive data • Create an insider threat program • Review logging and alerting data • Complete independent security (not compliance) audits • Create an information sharing program • Maintain adequate documentation - QRH

Ransomware **Response** Checklist

Detection and Analysis	Containment and Eradication	Recovery and Post-Incident Activity
• Determine which systems were impacted, and immediately isolate them. • If possible, power down devices to avoid further spread of the ransomware infection. • Triage impacted systems for restoration and recovery. • Develop and document an initial understanding of what has occurred based on initial analysis. • Engage stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.	• Collect system images, memory captures and relevant logs. • Research the ransomware variant and follow recommended steps. • Identify the systems and accounts involved in the initial breach. • Contain systems that may be used for further unauthorized access. • Examine IDS systems. • Rebuild systems based on a prioritization of critical services. • Issue password resets for affected systems and address vulnerabilities. • The designated authority declares the ransomware incident over.	• Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services. • Document lessons learned from the incident to inform updates to incident response plans, and procedures and guide future exercises of the same. • Consider sharing lessons learned and relevant indicators of compromise with your sector for further sharing and to benefit others within the community.

Common Mistakes to Avoid

After determining that a system or multiple systems may be compromised, administrators are often tempted to take immediate actions. Although well intentioned to limit the damage of the compromise, some of those actions have adverse effect.:

- Mitigating the affected systems before responders can protect and recover data
- Touching or preemptively blocking adversary infrastructure
- Preemptive credential resets
- Failure to preserve or collect log data
- Communicating over the same network as the incident response is being conducted
- Only fixing the symptoms, not the root cause

Ransomware Advisory
1 Oct 2020

THE U.S. DEPARTMENT OF THE TREASURY'S OFFICE OF FOREIGN ASSETS CONTROL (OFAC) IS ISSUING AN ADVISORY TO ALERT COMPANIES THAT ENGAGE WITH VICTIMS OF RANSOMWARE ATTACKS OF THE POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS.

HTTPS://HOME.TREASURY.GOV/POLICY-ISSUES/FINANCIAL-SANCTIONS/RECENT-ACTIONS/20201001

Thank you

Campbell McKenzie

0800 WITNESS

021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents

Incident Response
FORENSIC & CYBER