NETWITNESS

From Detection to Defense: Mastering Incident Response for Network Resilience

Table of Contents

INTRODUCTION

In today's ever-evolving cyber landscape, incident response and network protection are paramount for organizations of all sizes.

This eBook explores the strategies and tactics that are essential for enterprises to safeguard their networks from vulnerabilities and efficiently mitigate threats like ransomware. From identifying potential weaknesses to implementing robust incident response plans, you will gain insights into practices proven effective, and practical approaches to fortify your organization's defenses.

“In 2023, over 8.2 billion records were breached across all industries, with an average cost of $4.45 million."

Deloitte Cybersecurity Threat Trends Report 2024

Best Practices for Ransomware Preparedness

Organizations that develop fast and resilient response capabilities often achieve better outcomes when attacked. Visibility and detection capabilities help identify the precursors to ransomware attacks, as preventing the attacker from achieving their ultimate objective is key to reducing damage. Investing in and supporting a well-practiced and effective Incident Response (IR) capability gives organizations a fighting chance. Bringing in external expertise can also speed the development of these capabilities and augment them when necessary.

Priorities:

- **Enhance visibility and detection capabilities.**
- **Develop and practice effective Incident Response plans.**
- **Consider external expertise to strengthen internal capabilities.**

Key Areas for Improvement

Organizations often focus too much on perimeter controls, which are important but insufficient alone. Visibility into network, host, and log data is crucial. Many organizations have these capabilities but fail to configure or use them effectively, allowing attackers to exploit gaps.

Recommended Improvements:

- **Improve visibility into all network activities.**
- **Regularly test and train with a combination of traditional tabletop exercises and red team exercises to validate controls and identify weaknesses.**
- **Focus on effective configuration and utilization of existing tools.**

Common Mistakes in Ransomware Response

The most dangerous mistake is remediating the attack too quickly. Rushing to reimage compromised hosts and recover from backup without understanding the attack's true nature can leave the attacker's capabilities intact. Actions must be well-conceived and focused on fully expelling the attacker before remediation.

Damaging Mistakes:

- **Rushing to remediation without a full understanding of the attack.**
- **Failing to communicate effectively during an attack.**
- **Not preparing for long-term recovery efforts.**

Recommendations:

- **Respond quickly but ensure actions are deliberate and well-planned.**
- **Use external trusted advisors to provide dispassionate assessments and recommendations.**
- **Prepare for extended recovery periods and set appropriate expectations with business executives.**

Role of External Help in Ransomware Incidents

“Our team is large and very experienced. We can handle this.”

While a large and experienced team is beneficial, many organizations lack a dedicated Incident Response team. An internal team might have biases and might not always maintain the necessary readiness. External experts bring valuable experience and can provide objective assessments and recommendations.

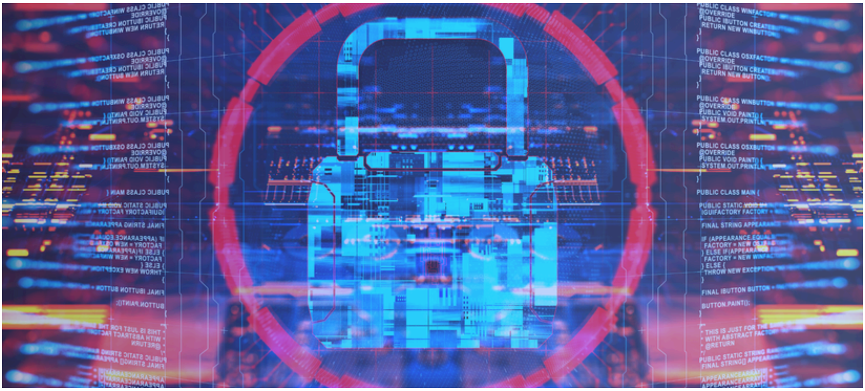
When to Consider External Help:

- **Legal requirements may necessitate hiring a firm working under privilege.**
- **For sophisticated attacks, external expertise can be more effective and justified compared to potential impacts.**

Positive Developments in Ransomware Defense

Organizations have improved in several areas, including:

- Enhanced backup and reimaging capabilities.
- Increased use of virtualization and containerization.
- Adoption of ephemeral hosts that can be quickly redeployed.
- Evolution towards cloud services that stabilize IT processes.
- Improved deployment of security tools like SIEM, NDR, and EDR.
- Use of industry frameworks like NIST and ISO to guide improvements.



Business Issues in Ransomware Defense

Effective communication of technical and complicated issues in a stressful environment is crucial. Security professionals need to relay situational awareness and recommended actions dispassionately. Legal considerations also play a significant role and should be communicated effectively.

Key Business Issues:

- **Communication under stress.**
- **Balancing security with business operations.**
- **Understanding and respecting legal implications.**

Negotiating with Attackers

Be very cautious about negotiating with attackers. Consider external help and restrict communication with the attacker to avoid furthering their objectives. Legal implications, such as violating regulations by paying ransom to certain entities, must also be considered.

Key Considerations:

- **Potential legal violations.**
- **Involvement of law enforcement.**
- **Risk of errors in communication with attackers.**

Guidance and Frameworks for Ransomware Defense

Several frameworks and best practices provide valuable guidance:

- **NIST Cybersecurity Framework:** A flexible, risk-based approach to managing cybersecurity risks.
- **CIS Controls:** Prioritized cybersecurity best practices to mitigate common threats.
- **Industry Best Practices:** Guidance from organizations, cybersecurity firms, and government agencies.

Components of NIST CSF:

- Identify: Understand and prioritize assets and vulnerabilities.
- Protect: Implement safeguards.
- Detect: Deploy mechanisms to detect incidents promptly.
- Respond: Develop and practice an incident response plan.
- Recover: Establish processes for recovery and post-incident analysis.

Components of CIS Controls:

- Inventory and control of hardware and software assets.
- Continuous vulnerability management.
- Email and web browser protections.
- Secure configuration for network devices.
- Incident response and management.

Conclusion

Ransomware preparedness requires a comprehensive approach that encompasses visibility, detection, response, and recovery. By focusing on best practices, addressing common mistakes, leveraging external expertise, and utilizing established frameworks, CISOs and SOC analysts can significantly enhance their organization's resilience against ransomware attacks. Effective communication and understanding of business and legal implications are also crucial for a successful defense strategy.

If you'd like to go deeper into this topic, we invite you to watch our on-demand webinar, "**Building Your Ransomware Preparedness Plan**".

About NetWitness

NetWitness is a pioneering cybersecurity software developer whose products are used by the world's most security-conscious and sophisticated organizations. NetWitness Platform delivers industrial-strength SIEM, NDR, and EDR capabilities that operate across on-premises, cloud, or hybrid infrastructures, providing a unified set of detection, investigation, and response tools. Threat analysts around the world rely on NetWitness for its robust threat intelligence, deep analytics, guided case management, and built-in response actions.

Learn more at www.netwitness.com