sayers

SAYERS CONSULTING SERVICES:

Ransomware Readiness Assessments

sayers.com 800.323.5357

The Real Risk of Ransomware

Ransomware can be devastating to an organization:

- Real, permanent loss of critical business records, employee data and intellectual property
- Massive loss of public trust due to public disclosure (which in many cases, is legally mandated)
- “Double Extortion” – attackers are both demanding money for decryption keys, and for not selling/releasing sensitive exfiltrated data

Paying a ransomware demand does not guarantee a successful recovery, does not prevent the attackers from attacking the victim organization again, and only exacerbates the problem by encouraging more attacks!

26

of businesses were forced into total closure for a significant period of time due to a ransomware attack*

**Cybereason, “Ransomware: The True Cost to Business”, June 2021*

$350k - $1.4m

35% of businesses that experienced a successful ransomware attack and paid for decryption paid an amount in this range

Sayers' Approach to Ransomware Readiness

Sayers' ransomware readiness assessments are based on trusted, consensus-driven approaches to mitigation

- NIST IR 8374
- Center for Internet Security (CIS)

Address critical aspects of your environment

- Network segmentation, port/protocol ingress
- Firewall/IDS/IPS/NAC configurations
- Backup and restore strategy and technologies
- Incident response capability
- Security awareness and training
- MITRE ATT&CK and DEFEND TTP mapping
- "Real-World" payload breach attempts

Our Methodology

Sayers' approach to ransomware readiness assessments is based on industry standard best practices combined with our deep knowledge of current ransomware trends and risks

Readiness Assessment

- **Evaluate** key aspects of the environment including network access/lateral movement capabilities, assets exposed through poor access control, backup strategy, incident response and user security awareness and training
- **Determine further testing footprint** for authenticated and unauthenticated payload breach attempts

Payload Breach Attempt (Unauthenticated)

Conduct a simulated ransomware breach without authentication using harmless payloads, by answering the questions, "Can ransomware easily get onto our systems and detonate?" and "How much damage can ransomware do to our internal network without authentication?"

Payload Breach Attempt (Authenticated)

Conduct a simulated ransomware breach as a minimally-privileged authenticated user to answer the question, "How much damage can ransomware do to our internal network if it is unknowingly detonated by a rank-and-file employee or contractor?"

Engagement Review

- **Document the business risks of ransomware** to the organization through an understanding of downtime, lost productivity, and potential permanent loss of data assets
- **Comprehensive Q&A** with the security engineers who actually conducted to engagement

The Value of a Ransomware Mitigation

- **Understand the reach of ransomware** – for both unauthenticated attackers and authenticated users – before it gets detonated inside your network
- Determine the **mitigating controls that you can implement** to reduce the likelihood and impact of ransomware
- Provide C-level executives and Boards of Directors with **specific, quantifiable metrics** related to your organization's ransomware readiness posture