edgescan™

Resilience to Ransomware

Just some thoughts on what to do to be more resilient to ransomware. There is no silver bullet but the below may reduce the risk and impact if you're unfortunate enough to be faced with a breach.

Awareness & Resilience (and budget)

Folks who write the cheques need to understand the value and importance of cyber security. Its not a "Tax" or an "Insurance" its a process to which we try to help ensure we are somewhat resilient to breach. Breach is 9 times out of 10 more expensive than multiple years of cyber spend.

Embrace cyber security! "Hackers don't give a shit" and if you are weak you will be hit. Cyber-Resilience and awareness may not prevent breach but it may limit the extent of the breach and enable us to act in a timely manner before the genie is out of the bottle.

Investment in cyber security is paramount due to the potential losses due to fraud and breach recovery. Compliance is not security, focus needs to be on practical technical controls and a technical framework.

Asset Management and Attack surface Management – Identify and prioritize – Risk

Maintain a list of what assets you have (Data and systems), What's the bill of materials for your network or system?

We can't secure what we can't measure. Tracking of system resilience is of key importance. Deploy continuous monitoring and management of your external Internet facing estate. This will help detect weaknesses and exposures as they arise. Real-time attack surface management is a simple but very effective solution to understand what can be hacked at any point in time.

Establish an asset register and an IT BOM (Bill of materials). Identify critical assets (Systems and Data). Layer stronger controls around such systems. Perform threat modelling exercises surrounding critical systems to identify cyber chokepoints and audit points to detect malice.

Threat Awareness – Intelligence

Deploy a solution to monitor lateral movement, brute forcing and typical indicators of compromise (IoC) traffic and artefacts. Threat awareness is important to both help detect post breach activities and also internal threats and weakness. Early detection is important in terms of limiting breach.

Processing of logs. Maintaining of logs. Tracking what's important.

Ensure we are auditing transactions, traffic and events on core systems. Such audit logs need to be consolidated and monitored for anomalies. Log scraping looking for errors and nonstandard events would be a great start. Logging non-idempotent transactions, authentication between users and systems and between systems themselves.

Vulnerability Management

Detect weaknesses as they occur. Patching, web application and API weaknesses. Exposed remote access services, administration consoles, weak cryptography all need to be tracked continuously. Key to this solution to be effective is accuracy. Solutions with guaranteed accuracy are preferred resulting in a reduction of "white-noise" so we can focus on real issues. The majority of ransomware leverages CVE's to exploit target systems. Full stack Vulnerability management makes systems more resilient to such attacks.

Focus on a risk based approach to patching and addressing weakness. "All vulnerabilities are not created equal." focus on what matters; critical systems and data first, moving down the list.

Penetration testing

Hackers manually probe systems and they are expert operators. Using software alone to assess security is never going to work. To level the playing field we need to fight fire with fire. Today's cybercrime consists of working professionals and industrialized capability. We need to be the same. Penetration testing consists of manual "deep dive" assessments using human intelligence simulating a determined attacker. Generally more effective in uncovering weakness but it is expensive and not as scalable.

Metrics & Measure improvement

Record improvement. What's difficult what's taking a long time. What cyber security activities are taking a long time and are challenging. Which systems cause the most cyber security effort. Which systems are historically more problematic and require the most attention.

Which layer (network or application) has the highest risk density and where to we focus our efforts. Examine vulnerability types; be they patching, developer or architecture related. figure out the root cause to focus on training, nd awareness in order to prevent such bugs and errors which manifest as weaknesses.

Patch

Every year 1000's of CVE (Common Vulnerabilities and Exposures) are discovered. Systems previously thought secure today suffer from a critical risk tomorrow. Constant tracking is required, constant vulnerability management to detect, risk based parching is required. Establish a patching programme. Use automation if possible.

Email and Internet Browsing Security

Locking down email systems, deploying an email security service to help minimize exposure. Locking down users browsing access to a whitelist of legitimate sites.

Data Encryption and secure Storage

Data which is critical to the business, sensitive in nature of contains PII needs to be encrypted with a suitable key management solution in place. Passwords should be stored in an un-recoverable way (Salted-hashed).

Backup Frequently

Backing up of data and systems is undervalued and paramount to restoring after a breach. The frequency of backup has a bearing on loss. More frequent backups = Less window of exposure. Try to deploy a Realtime backup solution if possible. The backups should be stored in a secure part of the network which requires authentication etc. to limit the chance of malware affecting backup repositories.

Authentication and Limitation & Zero Trust

Enable multifactor authentication (MFA) for critical systems. Be it certificate based combined with password or other means. Ensure system-to-system authentication is also enabled, adopt a "Zero trust model". IP limit traffic between systems from a architectural standpoint in order to make a network more hierarchical and less "flat". This can limit the spread of infection.

The extent of this problem is only growing based on the statistics we produce every year alongside other organizations.

More statistics can be found on the Edgescan Website including the Verizon DBIR and Edgescan Vulnerability Stats Report 2021.....

Writer of whitepaper

Eoin Keary

CEO of Edgescan

edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

@edgescan
in @edgescan