Building Ransomware Resilience

It's going to happen, so get 'digitally vaccinated'

Ransomware attacks are not going away anytime soon, hence every organization needs to enhance its digital immunity

Perpetrators have every incentive to increase their activities and continue to innovate their forms of attack. Ransomware attacks can occur remotely as a result of downloading malware, or can occur when an attacker gains access inside an organizations network.

Despite the innovations in form, the basic ransom tactics remain simple and crude – get inside the targets' defenses, grab a hold of something sensitive and apply pressure until target pays.

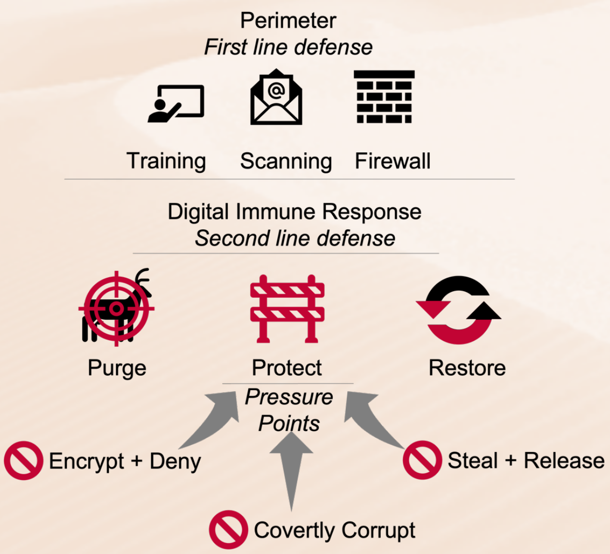

Figure 1 Two layers of Ransomware Resilience

Pressure can be applied in one of three ways:

1) **Encrypt + Deny** – encrypt the targets data, or temporarily disable some or all systems. Pay to have them released.

2) **Covertly Corrupt** - change data in ways that are potentially damaging to the business in a manner that is hard to detect. Pay to have the changes highlighted or reverted

3) **Steal + Release** – steal sensitive data and threaten release. Pay or find yourself on the front-page of tomorrows news

Ransomware attacks might not be going away but astute organizations can take steps to transform this risk from a potentially devastating crises to an on-going but low-level annoyance.

Achieving strong ransomware resilience means building capabilities to:

a) minimizing risk of initial attack and

b) mitigate the impact of attack

Perimeter defences include staff training in digital hygiene, email scanning products, firewalls and penetration testing.

Because no line of defense is ever perfect it is also essential to create a strong second line of defense which by analogy forms the organizations' digital immune response which can be broadly categorized as three supporting capabilities:

- **Purge** – detect and eliminate malware and persistent hackers
- **Protect** – limit the damage any attacker can inflict within tolerable range
- **Restore** - reliably return systems and data to a known state

Randtronics is a specialist in enterprise encryption our particular contribution to enhancing your Ransomware resilience is protect your data and minimize the opportunity for an attacker to exert coercive pressure during a ransomware attack. ***Read on to learn more….***

Building Ransomware Resilience

Air-gap sensitive data to isolate from ransomware attack

How can Randtronics help enhance your ransomware resilience?

Randtronics Data Privacy Manager (DPM) is a data security platform for managing encryption protections for structured and unstructured.

The obvious use-cases for encryption in alleviating ransomware pressure points include:

a) Ensuring data is not stored in clear format - so if it is stolen it can be exploited
b) Masking log files – disguising data systems making it harder for a persistent internal hacker to identify which systems are holding sensitive data
c) Preventing covert corruption of sensitive data – deny attackers the opportunity access the data or make changes

In the past sophisticated attackers have found ways to compromise privileged user accounts (such as System/DBA & Application Administrators), knowing that such users have the capacity to turn off or side-step locally deployed encryption solutions.

As illustrated in Figure 2 Randtronics DPM, easyCipher isolates encryption management outside the control of privileged users. With agents available for Windows and Linux environments, files in each protected environment are exclusively control by the DPM easyCipher Agent creating an airgap preventing any other user or program deleting, changing or encrypting files under easyCipher control.

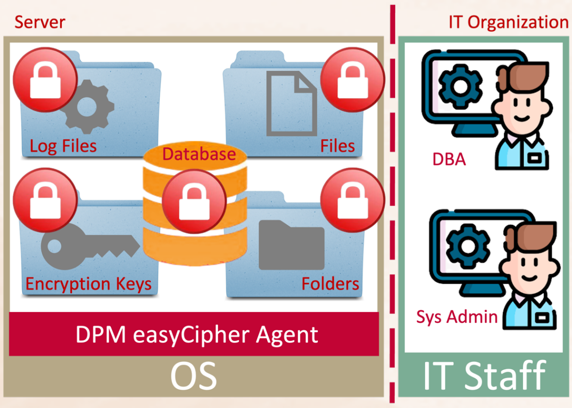

Figure 2 DPM easyCipher - Airgap protection

A foiled attacker may still seek threaten to permanently lock or destroy an entire system – however without the ability to steal sensitive data there is little leverage since such damage can is easily observed and quickly rectified via backup/restore.

Protecting your data with Randtronics DPM,
buys your cyber security team time to find and eliminate malware and persistent attackers
minimizes the attack surface for a

Contact us to today to discuss your data protection requirements at www.randtronics.com