The Potential Hit From Ransomware

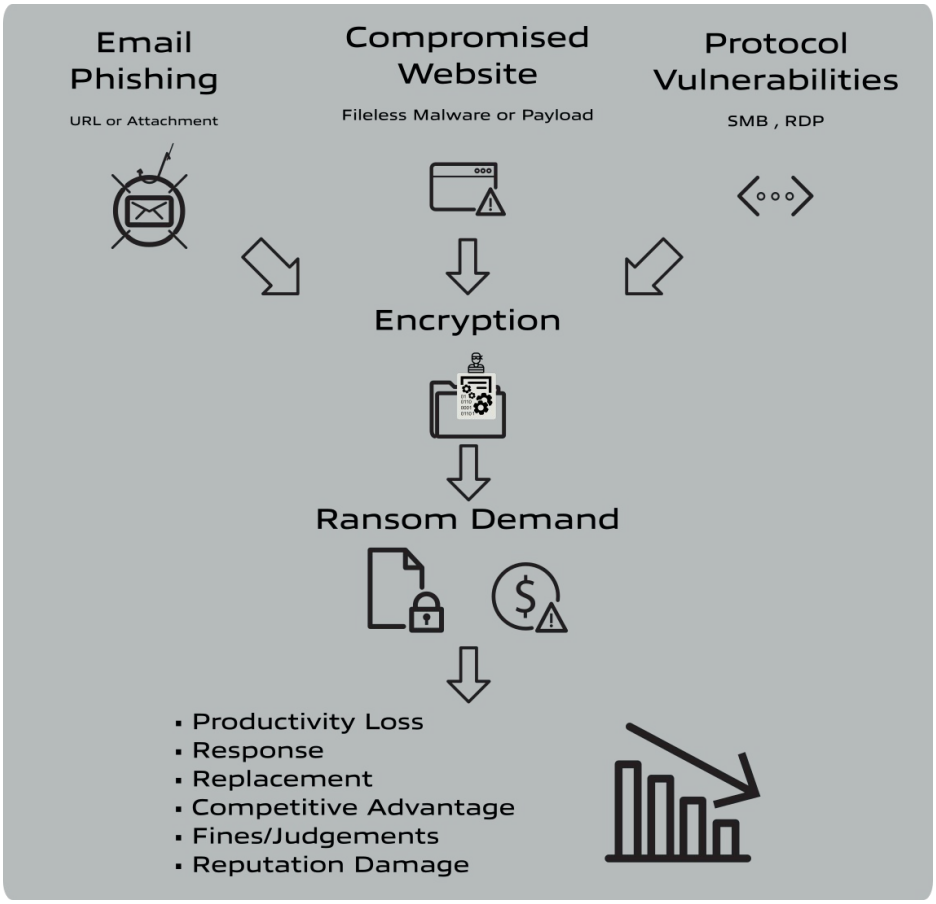
Availability of your digital processes, systems and data is critical to achieving your business goals

One study reported that nearly US $12 billion was paid out in ransoms due to ransomware during 2019. And nearly half of those that paid the demands did not recover their data. (ENISA Threat Landscape Report 2020)

There are multiple ways that ransomware infects your business:

- Phishing email with a link
- Attachment to email
- Compromised website visited
- Compromised Drive (i.e. USB, CD, Hard Drive etc.)
- Insecurely configured network file sharing protocols (i.e. SMB and RDP)

Once the ransomware has installed the malicious code on your computer, all of your files are encrypted and made inaccessible and require obtaining a private key from the attackers.



There are many ransomware threat vectors (ways of being attacked), but the result is always the same. Your access to your data is severely compromised. Whether it be access to your email system, access to your financial / accounting / payment systems, or even your critical business functions that deliver the service to your clients.

Recent examples of companies crippled by ransomware highlight the devastation to the bottom line. When Merck was hit by NotPetya (purportedly created by Russia to target Ukraine) some 30,000 computers were locked for weeks. The total cost of the attack is close to US $1.3billion, and this doesn't include the millions spent on lawyers fighting the insurance companies who refuse to payout.

However large corporations are not the only businesses targeted.

WannaCry ransomware attack used a known fault in Microsoft Windows operating system and locked up thousands of computers worldwide (a patch to fix this vulnerability had already been released by Microsoft weeks before). This attack hit 230,000 computers around the globe and caused up to US $4billion in damage. (https://www.kaspersky.com.au/resource-center/threats/ransomware-wannacry)

Unfortunately, paying the ransom does not guarantee a return to normal. Most attackers will be emboldened by such a payout that they may be tempted to come back for more.

It's imperative to protect and back-up your data in the event that a ransomware attack is successful. In the US it is illegal to make payments to terrorist organisations. Companies with subsidiaries in the US may fall foul of this law if you are found to have paid a ransom.

Tannhauser provides training for your staff that highlights basic steps and exercises to reinforce your company's strongest defence against ransomware - your people. Most ransomware programs rely on victims to execute the malware directly (visit a compromised website, click on email and open a file or run a macro). We also help raise the awareness of suspicious emails and attachments.

For your IT teams, we can perform strategy reviews that consider your threat landscape. Here are some simple steps that you can take to increase your cyber resilience and reduce the impact of a ransomware attack.

- Strong passwords and multi-factor authentication (MFA)
- Reduce access control for data to only users that absolutely require it
- Back-up data and systems offsite and regularly test recovery
- Whitelisting the programs that can execute on your network
- Segmentation of your network
- Install latest security patches and firmware updates

At Tannhauser, we can also improve how you assess threat intelligence, as we are continually updating our methodologies based on the latest threats in your industry.

For an in-depth assessment of your security service coverage, cyber security maturity, or validation of your cyber resilience if confronted with a ransomware attack please contact us at Tannhauser.

Further useful guidance for ransomware located here: https://www.cyber.gov.au/ransomware

Talk to us today to ensure you're appropriately prepared against the threat of ransomware.