RANSOMWARE SCENARIO

1. INITIAL COMPROMISE OF YOUR ENVIRONMENT

Remote Access Security

Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.

RDP/RDG attacks are an attractive and common way for hackers to access systems and steal valuable information from devices and networks.

Phishing

A criminal group targets your organization with a phishing compaign.

Malware is successfully delivered to one of your un-suspecting users via a malicious attachment or web link in an email.

2. MALWARE IS INSTALLED

The user opens the attachment and malware is unknowingly installed on the user's PC.

Unbeknowst to the user, and your security and IT teams, the attackers now have a foothold in your environment.

Using this foothold, the hackers explore your network (still undetected) looking for vulnerable systems and sensitive data. This include other user PCs but also servers supporting critical applications and file stores.

3. RANSOMWARE IS DEPLOYED

The criminal group has achieved the access they need and are ready to spring their trap.

They deploy a strain of ransomeware which spreads across your network encrypting indiscriminately.

The attackers have now encrypted a material portion of your estate and parts of your business are completely disrupted while other parts are partially disrupted.

4. EXTORTION

The attackers demand $x million for the decryption key.

The attack also becomes public knowledge which causes repotational damage.

The regulator also wants to understand if there has been a mishandling of customer sensitive data - there is a risk of significant fine.

US PRO INSURANCE SERVICES

Kevin Sneed
630.717.4226
ksneed@usproins.com
www.usproins.com