#RansomAware

Share your story

TALION

Top 8 Ransomware Mitigation Tactics

2021

01 Prioritise Remote Working Security

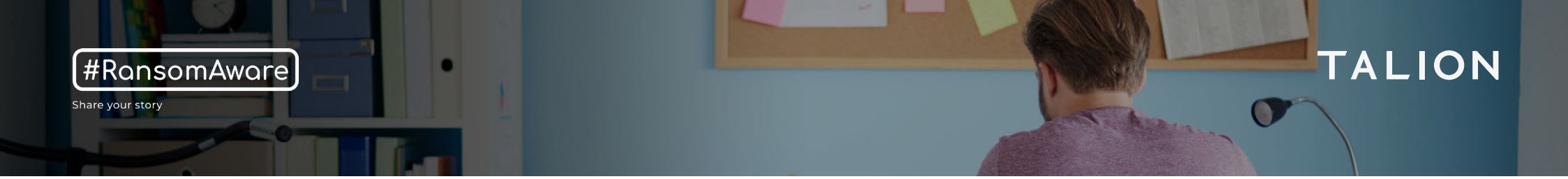
In the great global shift towards home working, prioritising good remote working security has never been more crucial, especially when considering the colossal number of attacks, we have seen in the last 12 months across the landscape leveraging remote access to virtual desktops during infiltration. Organisations can begin with some very simple steps, such as utilising strong passwords and two-factor authentication across your network. Also ensure that your organisation is using the latest versions of operating system and software by ensuring patching is implemented promptly.

02 Educate Users

Implement training teaching employees on how to recognise social engineering techniques, the key here is to keep this training regular. The threat landscape is constantly evolving, meaning it is pivotal that your users are kept up to date with the latest techniques, tactics and procedures. Additionally, exposing your users to planned phishing email tests will support this training.

03 Prioritise Patching

As mentioned, patching will improve remote working security and the potential for attackers utilising known exploits to infiltrate your system. Last year it was reported that 22% of all cyber-attacks leveraged one or more vulnerabilities during an infiltration, with 17% of ransomware attacks found to be leveraging an exploit, making patching management more paramount than ever.



04 \ Update Passwords Regularly

To avoid attackers performing an employee account take over to access your network, ensure you enforce users to regularly update their password on your system, highlighting the importance of your employees not reusing or duplicating personal passwords on your system.

The lengthier and more complex a password, the better. Passwords varying from 12-16 characters are an ideal, recommended length, differing on each platform. The use of a mixture of special characters and lower/higher case letters, also heightens password security.

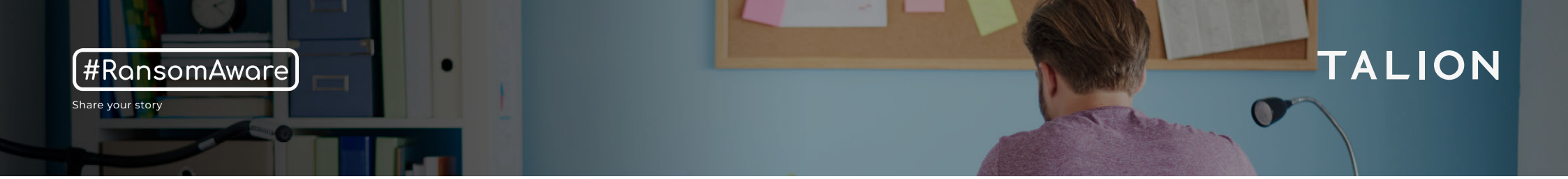
05 \ Keep a Close Eye on the Bad Guys

Keep up to date with the latest techniques, tactics and procedures (TTPs) being utilised by attackers. At Talion, we monitor and alert our clients to the ever-changing threat landscape as new TTPs emerge, advocating effective, timely procedures to defend their estate.

06 \ Make regular back ups

It was recently found that 92% of organisations who were compromised by a ransomware attack last year, who paid the ransom demand, did not receive all of their files back from the attacker post payment.

Making regular backups is an extremely important measure to take to improve your organisations recovery, in the event that your organisation is compromised by one of these strains.



07 \ Prepare to isolate

To reduce the impact a ransomware attack could have on your organisation, reducing the number of devices a strain could reach on your network shall prevent the malware from being able to move laterally across your network. You can do this by utilising Multi-factor authentication (MFA) to access platforms, ensure obsolete platforms (Operating Systems (OS) and apps) are segregated from the rest of the network. Also ensure unnecessary user permissions are regularly removed, that you are implementing good asset management across your software on devices, and as mentioned previously continually performing timely patching.

08 \ Be ready

Unfortunately, ransomware attacks are now so sophisticated and widespread that the likelihood that your organisation shall be compromised is extremely high. To have the smoothest possible recovery in the event of a potentially devastating attack, an organisations best chance is to be ready for an attack.

To prepare for an incident, establish your organisations critical assets and gauge the impact to these devices if they were to be infected. Create an internal and external communication strategy, ensuring the correct people are contactable at any time. Plan exactly how your organisation shall respond to a ransom demand and the threat of your organisations data being published, considering your organisations legal obligations regarding reporting an incident to regulators. Finally, exercise your incident management plan, clarifying everyone's role during an attack, this should consider both your staff and any third parties. By practicing a trial run, your organisation should be able to learn lessons and perfect your plan ready for the smoothest possible recovery if infiltrated.