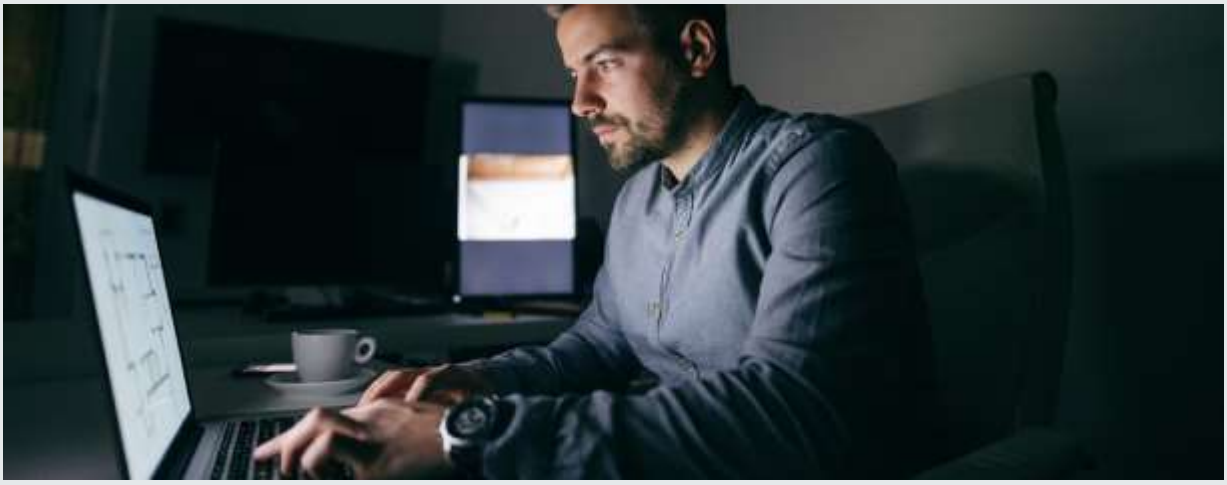
PARABLU

Ransomware shifts to Working from Home!



A global pandemic is hard enough to deal with. And, the last thing enterprises need right now is for a ransomware to wreak havoc on their network. But, the world over, enterprises continue to come under attack. In the second such attack of its kind, an electricity provider in the UK recently had to grapple with having its entire mail system crippled. Closer home, two employees of a private firm were sent ransomware laced links over a Zoom call while they worked from home which resulted in their data being encrypted for a ransom of 1000 Bitcoin!

If you thought even for a fleeting moment that these were problems of small to mid-sized firms, you should think again! Cognizant, a Fortune 500 firm was recently attacked by the Maze ransomware variant and is most likely going to see an impact on revenue and operations in the coming year, if their recent SEC filing is anything to go by. Their CEO Brian Humphries has said that the ransomware affected Cognizant's select systems supporting employees' work from home setups and the provisioning of laptops. Cognizant needed these systems to support their work from home capabilities for employees during the COVID-19 pandemic.

The world may have taken a bit of a break due to the COVID-19 crisis, but you may rest assured that ransomware is not. A report that VM Ware released Mid-April stated that in March 2020, ransomware attacks increased 148% over baseline levels from February 2020 – highlighting the abominable nature of opportunistic threat actors. In about 19 Million attacks that happened just in Asia, Microsoft Corporate Vice-President (Cybersecurity Solutions Group) Ann Johnson said they saw at least 9,100 files with malware links in them!

PARABLU

Covid-19 or not, ransomware attacks have always been prevalent. The work from home situation has just provided a conducive environment for popular attack vectors to be exploited more easily – thus exacerbating the threat. Organizations and employees are more vulnerable at this time being that they are distracted with business continuity processes and figuring out how to work from home. Working from home also tends to blur the line between a work device and a home device. You may go ahead and click on an email that looks like it's about that Amazon order you placed yesterday – except you're probably on your work device! And all it takes for a ransomware payload to drop is a single click in a moment of weakness.

Ransomware has already proved that it can get around the best laid security defenses – and is able to do some even more facilely during the crisis. Experts agree that a reliable backup strategy is still the best way to defend and recover against a ransomware attack. Having a secure and reliable backup means that you can get all your data back and not be held to ransom by a faceless attacker.

So, while you build 'digital empathy' and find the middle ground between relaxing restrictions for work-from-home and being obsessive about corporate security, take the time to put a data backup solution in place. But not just any data backup, one that's secure and automated. When your files are taken for ransom by threat actors, paying the ransom may become the only way to gain access back to your files and scarily, there have been instances where victims were unable to get their files back even after paying the ransom! In such scenarios, a secure backup is your best bet to gain back control of your data that's rightfully yours.

PARABLU

A secure backup helps in more ways than just protecting you against ransomware. Losses of data due to ransomware qualify as 'data breaches' in regulatory compliance parlance and enterprises could pay hefty compliance fines for data lost due to ransomware attacks. GDPR, for one, requires that organizations need to notify them, within 72 hours of being aware of the breach and notify all affected parties about it without delay. But, even if we looked at a scenario where you could afford to pay the fine, the loss of credibility caused due to bad press could cause irreversible damage to your business and your brand. Having a strategy for backups, where your backups are offsite and segmented away from production systems is critical.

For insights into why it is important to protect your employee data when they're working from home, check out our blog on "Why protecting end user data is even more important when they WFH" and for considerations to keep in mind when looking for a backup solution in these times, you may find our blog post on "Protect your data assets even as you let your employees WFH" useful.

Ransomware threats always existed, but the pandemic has just laid bare the nefarious lengths to which threat actors are willing to go during this difficult time. At this critical time, don't relax your backup strategy – strengthen it! You will need those backups more than ever.