UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM & COORDINATION CENTER [CERT.UG/CC]

8/06/2021

ADVISORY ON AVOIDING RANSOMWARE

The Threat

Ransomware launched on a system encrypts all user files and locks out the user with a demand note for anonymous online payment to restore access. Cybercriminals are mainly targeting Windows platform users. CERT.UG/CC is raising this advisory to alert CIOs/ Heads of IT to implement baseline protection controls that reduce the risk of ransomware infections. It is important to note that the chances of recovery of encrypted data are very slim especially with the latest strains of ransomware. We also discourage payment of ransomware demands.

The Advice

Here are twelve tips that we strongly recommend you implement:

- Increase user awareness so that a user can detect a phishing e-mail. This helps transform your staff into your first line of defense/ human firewall. Given the recent work from home measures to curb the COVID-19 spread, staff will increasingly be targeted through e-mail phishing.
- Protect your corporate e-mail service by enabling strong spam filters
- Configure your firewall with the right firewall policies and licensing
- Review your network to make sure you have segmented your corporate network
- Implement the Principle of Least Privilege to ensure all staff have the most minimum level of rights possible to do their work
- Lockdown your users' devices by ensuring all software installation is authorized
- Patch, patch, patch so you are using only the updated versions for all your corporate software.
- Only use supported Windows Operating System versions. No versions below Windows 10 receive updates from Microsoft. Using unsupported software only increases your risk of compromise.
- Keep up-to-date backup copies (protected and tested) of all your data. This will help you recover your data since making a payment is not advised.
- Check that you are using trusted anti-malware protection for all your devices
- Be prepared – have an incident response plan that will help quickly react and recover from any incident
- Report incidents to the CERT.UG/CC. This helps coordinate response.

//END