Town Clerk | Swaffham Town Council

From: ICO Sales Team <sales@icosystems.co.uk>
Sent: 11 June 2020 15:16
To: Town Clerk | Swaffham Town Council
Subject: Ref : Ransomware Attack
Attachments: Brochure_Total_Security.pdf

Richard,

Sorry about the delay in sending this through. I wanted to get you some ball park prices so that you can consider your options.

Response from Technical

On 22/04/20 it was found that the servers had been encrypted by a Ransomware called Dewar. This is typically delivered via an unassuming email, fake ads or compromised websites, which when opened have a link that will install a malicious piece of software onto the machine. Unfortunately, we were unable to ascertain the exact method of infection, although the RDS looks to have been the most likely entry point of entry due to the time stamp of the encryption.
It is unlikely that a brute for attack was used to crack the password due to its complexity. From what we could see an administrator account password was likely to have been harvested from within one of the machines by the software, which allowed an attacker to logon to the servers, the domain administrator accounts were then locked out, except for the one with the harvested credentials and the encryption was run. This account was left accessible so that the demand for ransom could be seen. The VHost, Domain controller and RDS along with Hannah's PC had all been encrypted.
Due to the onsite backup being stored on a USB drive that is directly connected to the server, any local recovery points were encrypted. All of the servers were rebuilt and restored the latest available recovery point, that are stored offsite in our Data suite. This extended the recovery time required as these needed to be exported to USB to take to Swaffham Town Council offices. Hannah's PC was rebuilt from a new windows 10 installation disk.
At this point we have changed all user passwords and secured the remote access to the RDS by using the Draytek SSL VPN software (previously this was just using a different port and NAT to 3389 internally).

Further Recommended Improvements

We would recommend the following to bolster your security.

Microsoft Office

In addition to the Office 365 licences and other products we would recommend all accounts have Advanced Threat Protection (Apr £1.50 per user per month) applied alongside them. This provides a real security boost to your environment including;
•**Safe attachments** – Provides real time scanning of attachments for malicious content. If the attachment is verified as clean, it is then forwarded to the recipient inbox, Teams message, SharePoint or OneDrive.
•**Safe Links** – Provides 'time-of-click' verification of URLs or web addresses in emails and teams. Each link is scanned and if verified as safe they remain active and any identified as malicious are dynamically blocked
•**Anti-Phishing Protection** – Detects attempts to impersonate your users and domains. Incoming messages are scanned for indicators that the message may be phishing. An example of this would be an email with a link asking you to login to your Office 365 account or OneDrive, however the link won't log you in, and it will just harvest your details.

Network Devices

We would suggest that all computers have Bitlocker enabled on them. This would reduce the risk of a similar attack by encrypting the drive data.(This is an engineer only cost)

We would also suggest that the current Anti-Virus is bolstered with Bitdefender GravityZone(£3.50 per user per month). This will scan all files opened on the computer and test them before allowing you to open them.

Our preferred option to installing GravityZone would be to suggest upgrading the Firewall on-site to a WatchGuard Firewall(£700 inc 1 year licence but subscription based models are available). This has an advanced Treat Detection and Response that will look at the files, links and unauthorised access attempts. WatchGuard would be the preferred solution and I have included a brochure for the Total Security Suite with the mail.

Data Storage

We would suggest moving your data storage into a SharePoint cloud. As well as making the data always accessible on and off site, it can be remotely backed up and secured with access via the Windows Multi Factor Authenticator and user accounts.

For any data on-site we would suggest a NAS drive(£1300) for onsite backup storage with limited access to the backup data. If this had been in place then we may have been able to perform a restore from the onsite recovery points, which would have reduced the overall time taken to perform the restore. The data Backups can then be stored off-site in the ICO Data Suite for added security.

Wi-Fi

Using a secure WIFI with periodic changes of the SSID and separate guest network would also be another recommendation. By separating your guest Wi-fi you remove the vulnerability of Guests being able to browse, find open network shares and install malicious software. By using secure Wi-Fi you can stop “Man in the middle” style attacks which are often used to harvest users details for later use. (APR £450 per Access Point)

Please not that all pricing is only estimates and does not take into account any engineering time for configuration or installation and exact model specifications have yet to be determined.

I look forward to your reply and will be happy to arrange a quote for any of the above options.

Best Regards
ICO Sales Team

ICO Sales Account Team
D: 01473 211 330 Option 1
E: sales@icosystems.co.uk

T: 01473 211 330
F: 0872 11 33 55 7

ICO Systems
Harman House, Dunlop Road, Ipswich.
IP2 0UG
www.icosystems.co.uk