Melissa Wiak - Thornton network

From:	ATSi
To:	Trustees;
Date:	6/19/2024 1:57 PM
Subject:	Thornton network
Cc:	Department Heads;

Dear Trustees:

On January 19, 2024, threat actors utilizing bitlocker software attacked the Village of Thornton among many other organizations. The damage to the Thornton network was extreme. All virtual machines were destroyed, and data from various iron box servers were encrypted. Staff immediately reached out to the threat assessment team with the insurance company, who employed several forensic and legal teams to help diagnose the situation. We also reached out to a local company to assist in this catastrophic event.

Very basic services such as logging in to desktops and browsing the internet were restored in the matter of a couple days. With the recommendations from several of the forensic teams, we began doing a complete clean build of a couple Windows servers and all the desktop machines. We deployed new Microsoft baseline security policies and created strong password and authentication policies. We have implemented a new server configuration, which isolates the user access servers away from the host servers. This way, if an infiltration hits a file & print server, it will theoretically prevent access to one of the host servers. We also setup a traditional NAS backup solution with offsite and offline backups.

New security practices have been implemented including an upgraded firewall to protect the entire network with geo-policy, and the elimination of SSL/VPN access. User remote access into the network has been eliminated, which we hope to re integrate using IPsec in the near future.

Since the VM servers were destroyed, Doug set up the hosted Civic Systems Solution so the Village Hall could start entering data as quickly as possible.

We were very limited on what we could do to build the improved network since the insurance company would not pay for upgrades, only for restoration. We were able to rebuild the PCs relatively quickly with basic configurations. Some specialized applications took more time to get replacement installers and key codes since a lot was lost with the infiltration. A forensics team started working on restoration of some recovered files for the GroupWise system. They felt reasonably confident they would be able to restore the mail system so we would suffer little loss. While they were working on recovering the GroupWise system, Doug was speaking with Trust-tech about the possibility of moving to a hosted version of Office 365, which would include e-mail and MS office products. I was told the cost to move to the new system was too costly. After weeks of delay, I decided it was best to move forward with a clean installation of the GroupWise system. Users have been added per the lists provided by department heads.

In the middle of the cyber-attack situation, the website was migrated from the old provider to the new Civic Plus provider. Civic Plus also took control over our DNS information. We had to work with them to get our pointer records rebuilt. Doug oversaw the entire migration of the website and advised the department heads to determine whether or not they wanted to migrate their page directly over, or if they wanted to start over with a new page. I had very little involvement on the website migration.

As of a few weeks ago, all services have been restored, including user data for Village Hall and Fire Department. We encountered roughly 70% data loss, most of which was old and unused. Most of the critical data has been re-created. I am told there are concerns that the Planning Commission users are not in the mail system. In fact, they were added weeks ago. I gave Doug a list of trustees and planning commission members' emails and login information. Doug had that list in his office. Melissa now has that information.

Currently, the network is probably in the best condition it has ever been. However, there is still a lot that needs to be done. I have a relatively long list of technology that requires upgrade or replacement, which I will detail out in another e-mail.

It is my understanding there are some concerns with some of the things that may or may not have been done with the network. I invite everyone, including trustees, committee members, or village employees to reach out to me with any issues so I can either address them via email, or set up an in-person meeting. I do not want any of the problems to sit un-addressed.

As you know, I am very limited on working hours each week. The current contract allows me to work 16 hours a week throughout various departments in the Village. Given the limited time I have, I am trying to address everything as fast as I can.

Thank you.

David Watson
Village of Thornton IT
708-877-4456
ATSi@thorntonil.us

This message contains confidential information and is intended only for addressee(s) named above. If you are not addressee(s) you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If verification is required please request a hard-copy version.

Save a tree! Only print if necessary.

Melissa Wiak - Issues

From:	ATSi
To:	Trustees;
Date:	6/27/2024 10:17 AM
Subject:	Issues
Cc:	Department Heads;

Hello all.

I just wanted to reach out to everyone who responded to my previous email and say thank you. I do appreciate everyone's input and suggestions.

Many of the issues were actually small questions about email which is more stable and secure than ever.

As I have told a few, we now have 3 virtual machines performing different services for email and remote access into email. There are a few very small routing issues which are handled through Barracuda Networks which we subscribe to. I expect those issues to be resolved very quickly.

Several people reached out regarding the backup solution which I believe I've responded to everyone but just so everyone is up to speed, Thornton currently has a multi-tiered backup approach. We are doing the traditional backup to on-site NAS servers which fail over between both the village hall and the police department. We also have offline backups which reside in the police department as well as an off-site solution in case of disaster.

I know several people are concerned over remote access but we are working to build a remote access server as quickly as possible. Again, old machine and need to obtain a license to get the machine online.

We have been in contact with the vendor about a new PA system for the board room. I hope to have a plan soon.

As you all know, we are very limited on time with the maintenance agreement. We must prioritize each issue on importance and vulnerability. A fair portion of the issues I'm hearing about is users adjusting new use methods and security protocol. We realize some of the new security demands can be a bit hard to swallow but these are now required industry wide to protect us all.

As always, if you have any concerns or questions, feel free to reach out to me at this address.

Thanks

Dave

Village of Thornton IT

708-877-4456
ATSi@thorntonil.us

This message contains confidential information and is intended only for addressee(s) named above. If you are not addressee(s) you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If verification is required please request a hard-copy version.

Save a tree! Only print if necessary.