PUBLIC NOTICE

February 5, 2020

The purpose of this communication is to post notice that Mississippi Center for Legal Services and North Mississippi Rural Legal Services, [MCLSC/NMRLS] has been the victim of a ransomware computer system attack that has resulted in a breach of security. This breach of security resulted in the temporary shutdown of the organization's computer system. This breach of security may have resulted in the compromise of data that may contain personal or confidential information relating to the current and/or former clients, contractors, vendors, attorneys or affiliated business partners of this organization. We have been working diligently to assess the situation.

With any unauthorized breach of computer system security, personal or confidential information of individuals maintained on the compromised system may be affected. As such, the personal or confidential information of current and/or former clients, contractors, vendors, attorneys or affiliated business partners of this organization may have been affected by this unauthorized breach of security. We have conducted and are in the process of further conducting an investigation to determine the scope and nature of the incident, to identify the affected individuals, and to restore the reasonable integrity of the data subject to the breach and the reasonable integrity of the computer system in general. Incorporated into this notice is the analysis from Complete Computers, our server vendor, which recaps the ransomware occurrence, what actions have been taken to restore services, and what measures are being undertaken to prevent this occurrence in the future.

This communication is meant to provide the notice contemplated by MS Code 75-24-29 and other applicable notice requirements. In addition, this notice is provided in conformity with the American Bar Association Standing Committee on Ethics and Professionalism, Formal Opinion 483.

Sam Buchanan, Jr. Executive Director MCLSC
Ben Cole, II Executive Director NMRLS

INCIDENT REPORT FROM COMPLETE COMPUTERS

Initial Incident

On December 24th 2019, MSLS IT staff was contacted in regards to inaccessible email and server access. Upon inspection, it was determined that two servers were attacked by ransomware which encrypted most of files on both servers (NMRLS and MCLSC). The exact variance of ransomware is named: Ryuk. The attack encrypted most aspects of these two servers, both including but not limited to: work product files (word, excel, word perfect, etc.), email server database files (Outlook emails), the running virtual servers (applications), as well as the local backups that were performed every night. However, there are some aspects of the network that remained unaffected since they were on separate servers and used a different configuration. One of the major servers which remained unaffected by this attack was the Clients Prime Database server which holds all the client information for both programs.

Incident Response

During inspection, the attacked servers were removed from the network as a precautionary measure and all connections from the office(s) of NMRLS and MCLS were shut down until the individual computers could be visually inspected by MSLS IT staff. During this process the unaffected servers were also taken off the network to safeguard them from possible attack until a reasonable expectation of safety could be established.

Attack Validation

After gaining an overview of the attack and an estimated level of data encryption, a 3rd party cybersecurity firm was contacted in an attempt to help provide additional insight as to the feasibility of possible recovery. After initial triage procedures were performed they advised that based upon the variance of the encryption and the level of encryption, there are no exploits, no vulnerability, and they had no direct means of possible recovery ofthe encrypted files.

Incident Reaction

With the information acquired from the investigation, the nature of the ransomware, the extent of the damage caused, and also the need for staff to regain as much functionality as possible, the server's operating systems were rebuilt using alternate hardware. Additional attempts to locate older data from earlier backups along with information from prior decommissioned servers were also performed. Some hardware has also been sent to a disaster recovery company to see if the drives contain any possible data that could be restored. In order to provide business communications, the determination and under the authorization ofMSLS IT staff, the email services were moved to Microsoft Office 365, and Outlook on the newly created application server was configured to check email. The original server that stored the database for Clients Prime was unaffected by the attack. With the assistance of Kemps Case Works, the frontend to Clients was recompiled and setup on the alternate application server, and Clients Prime access was restored.

Incident Response

Internet threats are ever evolving and increasing, they are more intelligent than prior versions and the frequency of attacks are increasing all around the world. As such the need to increase the overall security and protection of the network is needed to help safeguard the network from future attacks. As such the following solutions are currently being discussed and or implemented. All users need to use high complexity passwords, as well as password rotation. Simple dictionary

password make for easy targets for attacks. This process was also one of the requests provided to MSLS IT staff by LSC. The email for all staff has already been moved to a hosted Exchange platform at Microsoft Office 365. This hosted platform will help provide a constantly updated email service for all users. There is also a need for a centralized antivirus platform, which is currently being outlined. A centralized antivirus platform will aid in the potential detections of certain threats for MSLS IT staff and help protect the end user workstations. This solution was also a requests provided to MSLS IT staff by LSC. Additional server hardware is also being provisioned which will aid in the protection of user data. The additional hardware will provide more space for program applications, and will be configured so that the local backups are on a separate network, outside the environment of normal server operations. A replacement backup solution will be implemented, which can help provide additional features for backup. This backup solution can also be configured for a potential off-site replication of the backed up data to another location. The current firewall hardware platform will undergoing an upgrade, the current firewall(s) will be replaced and all VPN connections between offices will be increased to the highest level of encryption.

Conclusion

The exact nature of this incident is still ongoing, many aspects and facts regarding the attack are still being determined. There are additional discussions with the 3rd party cybersecurity company that will be held in the hope to gain a better idea of the attack's overall scope and hopefully provide additional information. MSLS IT Staff is still working to locate work product information (regardless of date) that can potentially be restored into the production environment. This process will be ongoing, however whatever inforrtlation can be obtained from older backups will be return to the user's working directories if they are deemed safe for production.

At this point and time, Outlook (new email) and Clients (all data) for both programs are online and should be safe. They have either been rebuilt from source, restored from clean files, or were untouched by the attack. If anyone experiences any unusual computer related issues such as but not limited to: desktop background changes, file icon changes, severe and uncommon computer performance issues please contact MSLS IT Staff as soon as possible and if necessary shut off the computer until it can be diagnosed.