A Proactive Approach: DCH's Strategies to Combat Cyber Threats and Ensure Data Security

Every day, cyber threats become increasingly sophisticated, and managing threats is an evolving process. Ensuring a threat-free environment at DCH includes regularly testing security infrastructure, utilizing the right tools and methodologies for threat management, and fostering a culture of cybersecurity awareness among all team members.

As per recent trends, cyberattacks have increased every month by 37% since the COVID-19 outbreak. Let's walk through a few cybersecurity-related vulnerabilities that impact DCH the most.

1) Phishing: Phishing is the most widespread cybersecurity vulnerability that impacts more than 85% of organizations worldwide. In phishing attacks, users are tricked into downloading malicious links sent to them through email. The most common type of phishing attack is email phishing. Over time, attackers have formulated other methods, including smishing, vishing, and search engine phishing. In smishing, malicious links are sent through SMS over a phone, whereas in vishing, phone calls are made to trick users.

2) Ransomware: Ransomware is among the most common threats impacting hundreds of organizations daily. In ransomware attacks, organizations' data is encrypted by attackers so that no one inside an organization can access it. To unlock the data, attackers demand heavy ransoms, thus resulting in massive loss of money and disruption of their services. Organizations usually tend to pay these ransoms to cyber attackers as they don't have the resources to recover from a ransomware attack. In some cases, even after paying the ransom, organizations cannot retrieve their data.

3) Malware Attacks: Malware attacks are malicious programs designed to cause harm or damage to an organization's infrastructure, system, or network. The origin of malware is usually public Wi-Fi, spam emails, downloading malicious content, and clicking on pop-up ads. Once malware is released into the system, it can compromise all the critical and personal information on the organization's servers and systems. Malware is classified into one of the following categories: virus, trojan, worm, adware, spyware, and malvertising. Malware is sometimes challenging to detect in the system and can change the system settings and permissions, spy on user activity, and block critical programs on users' computers.

As more employees work from home or hybrid, DCH needs robust cybersecurity and digital strategies for changing working practices and exposure to new threats. To meet these challenges, our IT Department has embarked on three cybersecurity strategies to enhance the Agency's security posture further.

1) Narrowing Local Admin Access: To understand the importance of Local Admin Access, we want you to visualize our computer systems as digital fortresses and user accounts as the access keys. User accounts determine who and/or what gets inside and outside the castle. Cyber threats act as sly intruders attempting to breach our defenses and steal valuable data. To combat this, our IT Department has taken the initiative to ensure that only a few authorized personnel possess the keys to access the castle. By restricting Local Admin Access, we can minimize the risk of unauthorized entry to mitigate the risk of unauthorized entry, thereby preserving the security of our digital fortresses.

2) Increased Application/System Patching: Because cyber threats are consistently emerging, our systems are constantly updating to defend against these cyber threats. To further uphold the security of DCH and the people of Georgia, our IT Department has embraced Application Patching—a proactive approach involving regular updates to software and systems. This method strengthens our digital defenses, making it harder for cybercriminals to exploit out-of-date software.

3) Continuous Monitoring: At DCH, our systems employ alerts to help the IT Department recognize vulnerabilities, detect unauthorized access attempts, and neutralize emerging risks. This is made possible through the use of Continuous Monioring. Our advanced tools enable us to enhance security measures, minimizing the risk of unauthorized entrys and ensuring the protection of your data and that of the people of Georgia.

Cybersecurity is a team sport, and we need your help to protect data and secure DCH systems from harmful attacks, vulnerabilities, and threats. Our IT Department would like you to:

1) Stay Alert: Watch for suspicious emails and/or messages. Cybercriminals try to deceive, but we can outsmart their maneuvers and stay multiple steps ahead.

2) If You See Something, Say Something: If Something feels off involving our computers and/or online activities, do not hesitate to notify the DCH Help Desk (helpdesk@dch.ga.gov or 404-657-7171) or Cybersecurity Team (DCHOIS@dch.ga.gov).

3) Avoid Password Theft: Weak or shared passwords are another major threat. With most users having multiple application services these days, reusing easily guessed passwords can lead to compromising data. Also, passwords can be compromised when users enter their credentials unknowingly into a fake website.

Together, we stand firm against cyber threats, securing our data to ensure smooth digital operations and fortify the safety of our digital world. We appreciate your help with protecting the people of Georgia.