Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

Tech Talk with Data Net – Rob Slaughter

Data Net has received several warnings from CISA to be on “HIGH ALERT” due to the current world events. The Federal Government believes there will be a significant increase in email and ransom ware attacks over the next several weeks.

CISA is the official US Federal Government Cybersecurity & Infrastructure Security Agency. Data Net regularly receives warnings and bulletins from CISA called CISA Insights.

While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia’s unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region. Every organization—large and small—must be prepared to respond to disruptive cyber activity. As the nation’s cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyber-attacks. When cyber incidents are reported quickly, CISA can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack. - See the latest updates and developments from CISA here: https://www.cisa.gov/shields-up

SHIELDS UP Guidance for All Organizations

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

Recommended actions include:

Reduce the likelihood of a damaging cyber intrusion

- Validate that all remote access to the organization’s network and privileged or administrative access requires multi-factor authentication.

- Ensure that software is up to date, prioritizing updates that address **known exploited vulnerabilities identified by CISA**.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented **strong controls outlined in CISA's guidance**.
- Sign up for **CISA's free cyber hygiene services**, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review **Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure**. CISA also recommends organizations visit **StopRansomware.gov**, a centralized, whole-of-government webpage providing ransomware resources and alerts.

Steps You Can Take To Protect Yourself & Your Family

Every individual can take simple steps to improve their cyber hygiene and protect themselves online. **In fact there are 4 things you can do to keep yourself cyber safe**. CISA urges everyone to practice the following:

- **Implement multi-factor authentication on your accounts**. A password isn't enough to keep you safe online. By implementing a second layer of identification, like a confirmation text message or email, a code from an authentication app, a fingerprint or Face ID, you're giving your bank, email provider, or any other site you're logging into the confidence that it really is you. Multi-factor authentication can make you 99% less likely to get hacked. So enable multi-factor authentication on your email, social media, online shopping, and financial services accounts. And don't forget your gaming and streaming entertainment services!
- **Update your software. In fact, turn on automatic updates**. Bad actors will exploit flaws in the system. Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems.
- **Think before you click**. More than 90% of successful cyber-attacks start with a phishing email. A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites. And they may try to get you to run malicious software, also known as malware. If it's a link you don't recognize, trust your instincts, and think before you click.
- **Use strong passwords**, and ideally a password manager to generate and store unique passwords. Our world is increasingly digital and increasingly interconnected. So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on.

If you have questions or concerns about your current cybersecurity posture or simply need assistance with implementing any of the steps outlined in this article, contact Data Net today at (760) 466-1200 or online at www.4datanet.com.