CYBERATTACKS SURGE; RUSSIA-UKRAINE CONFLICT!

threatSHIELD security

threatSHIELD security

HOW TO PROTECT YOUR BUSINESS NOW

Both CISA and FBI have issued a new warning urging organizations of all sizes and sectors to increase security measures as malicious online activity continues to rise. State sponsored Russian cyber-attacks so far have targeted Ukrainian government systems and banks, but cybersecurity experts and government officials warn that the attacks could soon spread to American businesses and companies. Experts have spotted known Russian cyber gangs conducting reconnaissance against U.S.-based industrial infrastructure, including key electrical and natural gas sites.
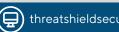
In their advisory, CISA and the FBI urge organizations to take general steps, such as strengthening defenses against malware, updating operating systems, protecting passwords, and implementing multi-factor authentication. Former White House adviser Richard Clarke says the only effective response is to "shield up".

DID HE MEAN, THREATSHIELD UP?

WHAT CAN YOU DO TO KEEP YOUR BUSINESS BE SAFE?

threatSHIELD security

OUR SECURITY IS ABOUT PREVENTION NOT JUST DETECTION!

ACT.

Work with a trustworthy and experienced cybersecurity provider now to assess the security of your network and be extra vigilant during a potential surge in cybersecurity risk— after all, a proactive approach to cybersecurity is always better than a reactionary one.

WHAT DO WE RECOMMEND?

- ☑ Infrastructure Assessment
- ☑ Ransomware Simulation Attack
- ☑ Risk Assessment
- ☑ Pen Test
- ☑ Vulnerability Assessment
- ☑ Maturity Assessment
- ☑ Cybersecurity Training

ENHANCED PERIMETER SECURITY.

Russian cybercriminals may or may not target your business directly, but other hackers will capitalize on the strength of a new strain and try to deploy their own version of a malware. The best way to prevent malware infection is to avoid it in the first place by using a multi-layer approach to cybersecurity and to implement a 24/7 all year long highly intelligent security device between the firewall and the existing core switch.

WHAT DO WE RECOMMEND?

t-INTELLIGENCE This is an innovative tool that detects and blocks all the invisible threats that bypass traditional security controls. Agnostic by nature, this is currently the most powerful tool on the market to **STOP IN REAL TIME** all types of malicious attacks including Ransomware, before the traffic is distributed across the network, without the need for human interaction.

ENHANCED LATERAL SECURITY (END POINT, DEVICES, ACCOUNTS).

Numerous cyberattacks target a particular endpoint like an email account, a portable phone, or a defenseless computer. The significance of a device that provides automated danger discovery, solid phishing sifting, ransomware recovery, email security, encryption administration and sandbox scanning for each device and each e-mail account, is exceptionally important.

WHAT DO WE RECOMMEND?

t-**EDR** End Point Detection and Response with threat intelligence and data analytics to track potential threats and give the IT Department visibility on all threats detected, to have them act on it. We recommend that clients upgrade their existing EDR or Anti-Virus to *t*-**EDR**, our special detection and response mechanism, which combines active monitoring with threat intelligence and data analytics to track potential threats. The difference… *t*-**EDR** receives intelligence feeds every 30 seconds.

threatSHIELD security

SAFETY FOR YOUR DIGITAL ASSETS.

Cyberattacks frequently begin with DDoS (distributed denial of service), which work by assaulting the servers that have websites. These assaults can take down hundreds or thousands of websites all at once. Essentially, brute-force attacks are troublesome endeavors that shut down whole segments of the Web at once—not necessarily targeting a particular company. Phishing campaigns will often try to capitalize on breaking news or global conflicts to trick you into "clicking". Automatic security patches and software updates help against these sorts of attacks.

WHAT DO WE RECOMMEND?

t-**PROTEC** combines the exclusive technology of *t*-**INTELLIGENCE**, our proactive/real time detection cybersecurity tool deployed as part of comprehensive cybersecurity protection to your network, combined with *t*-**EDR** a powerful and enhanced End Point Detection and Response for optimal visibility. These two keep a 24/7 eye out for all kinds of attacks by monitoring Internet traffic and identifying vulnerabilities before they're exploited. Automated security patches and software updates also protect against these kinds of blanket attacks, offering a level of IT support that no small business owner can achieve on their own.

INCIDENT RESPONSE.

If a cyberattack does impact your company, the quickest way to prevent negative effects is by restoring a backup for business data that has been captured regularly, remotely, and redundantly. Creating multiple copies of critical information stored in different cloud-based and physical locations offers businesses multiple levels of protection. The next step is an incident response plan that outlines the immediate steps to take to restore normal operations.

WHAT DO WE RECOMMEND?

vCISO services highly trained cybersecurity experts handle all aspects of IT security and compliance programs.

WHAT DO WE OFFER?

- On-demand Incident Response
- Years of cybersecurity experience gained from working with multiple organizations and across all areas of the economy
- Customer and partner support
- Qualitative information security risk assessments
- SOC2 or similar audit support
- Compliance with regulations and standards such as NIST-CSF, CMMC, PCI, or HITRUST
- IT security assessment
- Chairing a quarterly governance committee
- Third-party critical vendor reviews

vCIO services to oversee the entire IT infrastructure, ensuring everything in your business network is firing smoothly; the bridge between your business and the technology teams assisting you.

WHAT DO WE OFFER?

- A dedicated technology liaison for your company
- Technical reporting and interpretation, compliance, IT projects and expenses
- Partnership alignment
- Planning a technology roadmap for your company
- Expert IT consultation and guidance (Intellectual property protection, disaster recovery, employee onboarding)
- Cost effective
- C-Suite hiring support

threatSHIELD security

Be proactive, contact threatSHIELD security, we are here to help!