MCX
CMAA Construction Management Association of America
Member Communication Experience

The Time is Now to Protect Your Firm From Ransomware Attacks

Written by: Stel Valavanis, Founder and CEO, onShore Security

Ransomware attacks are one of the biggest cybersecurity threats to U.S. businesses, and the construction industry is not immune. In fact, it was the most commonly attacked industry in 2022, according to research by NordLocker. Government agencies and insurance carriers are no longer waiting for improvements and instead mandating them as table stakes to do business.

Construction firms need to be vigilant and defense-minded as hackers look for any opportunity to break into their systems, which have become more vulnerable during the pandemic as support for remote and hybrid work has grown.

Construction companies may not think of themselves as likely victims, but from the perspective of cybercriminals, they are the weak point in the wall of defenses surrounding these high-value targets — which puts them squarely in the hacker's crosshairs.

This evolution coincides with a change in tactics once the hackers succeed in breaking in, according to CSO. Rather than simply locking the network down with malware and demanding payment to release it, cybercriminals are increasingly downloading sensitive information — such as passwords and financial data — from the victim's computer or network and threatening to leak it if the ransom is not paid. They may ratchet up the pressure to pay by contacting the victim's customers and other stakeholders via email or even phone to alert them that the victim has been hacked and their data is compromised.

The approach puts even more leverage on the victim to comply, and could potentially inflict more damage than the ransom itself in the form of lost business and reputation. In some documented cases, ransomware gangs are skipping the file encryption altogether and focusing solely on this data extortion scheme.

Government Pressure

The pressure on companies is not only from the cybercriminals. Cyber insurance policies have been drastically increasing insurance premiums and insisting on ever more stringent and costly security measures. Insurers now require clients to employ endpoint detection software and firewalls, conduct regular system updates and audits, implement recovery

tools and procedures, and maintain stricter controls such as multi-factor authentication and even full system logging and analysis.

Meanwhile, the Biden administration is weighing a ban on ransom payments in order to limit the profitability of attacks for ransomware gangs. A similar proposal is being considered in Australia. Other measures include increasing legal liability for companies and their boards and even requiring board members to receive training and sign off on cybersecurity posture.

Companies with federal contracts are required under the Department of Defense's Cybersecurity Maturity Model Certification 2.0 to implement cybersecurity standards in order to protect federal contract information and other controlled data. This requirement applies to vendor management as well.

A construction company may be several steps removed from the actual ransomware attack, but if government contract-related files have been shared with a victimized vendor, the company may still be held liable. And contractors will be passing this liability to their trade partners.

Take Defensive Action

In the face of this growing threat, it's important that companies do what they can to protect their systems from ransomware attacks. Here are three steps to take.

1. Get serious about IT support. It is tempting to keep the IT budget lean and rely on employees to maintain their own machines. But doing so often means security patches and other key updates go un-downloaded and uninstalled, progressively leaving more doors open for hackers to try. Hire knowledgeable and reliable IT staff (or a trustworthy contractor) who will be proactive about network maintenance and security.

2. Utilize a cybersecurity framework. A cybersecurity framework helps companies outline policy and procedure to find, identify, respond to, and recover from cyberattacks. Frameworks help establish best practices and provide step-by-step guidance on what security controls should be implemented to prevent infiltration, as well as clear rules and expectations for every department and actor within the network.

A number of cybersecurity frameworks are available, including CMMC, the National Institute of Standards and Technology, the ISO/EIC-27000 family of standards, and the Center for Internet Security Critical Security Controls. The CMMC framework was recently revised to more closely align with NIST, with phased implementation beginning this year, and federal contractors will be expected to comply with the CMMC 2.0 framework in order to continue to be eligible for bids.

3. Deploy Network Detection Systems. The reality is that prevention strategies are not enough to protect against these threats. The highest level of security maturity revolves around detection — proactively monitoring the network to spot exploits and preempt attacks. As compliance frameworks continue to grow in importance, the need for effective detection strategies is becoming more and more essential.

Security providers offer managed detection and response (MDR) systems that detect and log abnormalities anywhere on the network, correlate and analyze the data, and deliver real-time alerts and reports on potential attacks. Human beings watching and making sense of the firehose of data is what distinguishes MDR from a protection system — analyzing, identifying, and neutralizing threats instead of simply blocking them without providing any intelligence.

Ransomware is here to stay, and the construction industry is increasingly in cybercriminals' sights. Organizations must use every available resource to reduce downtime and limit financial exposure by taking action to proactively detect and preempt attacks.

About the Author

Stel Valavanis is the founder and CEO of onShore Security, a Chicago-based cybersecurity firm. Photo courtesy of onShore Security.

About the Article

Republished from Construction Dive online. Construction Dive is a leading industry publication operated by Industry Dive. Their business journalists spark ideas and shape agendas for 10+ million decision makers in the most competitive industries. The daily email newsletter and website cover topics such as commercial building, residential building, green building, design, deals, regulations, and more.