THE ALS GROUP

Ransomware Demands Spike Due to Covid-19 Pandemic

Posted by The ALS Group on Oct 12, 2020 2:10:07 PM

As companies had to quickly pivot and implement a remote work plan (a lot of them did not have such a plan in place) due to the ongoing COVID-19 pandemic, they became more at risk for a cyber attack and/or breach due to the vulnerabilities they did not even know they had. As a result of this there has been an uptick in the success rate of cyber attacks in the United States.

Coalition Inc., a cyber insurance provider, recently released their H1 2020 Cyber Insurance Claims report that noted a decrease in the frequency of ransomware claims however, its policyholders have experienced a 100% increase in average demands from 2019 to the first quarter of 2020, then an increase of 47% from the first quarter to the second.[1]

According to the report, most of the attacks come by way of email/phishing scam, remote access, or social engineering techniques. It is what you would expect when employees are out of their element or separated from their company's IT security infrastructure due to COVID related remote work arrangements.

Out of all of the cyber attack threats, ransomware continues to be the top one. Newer versions of the file encrypting threats such as DoppelPaymer and Maze fetch an extremely high (into the hundreds of thousands of dollars) extortion demands to unlock encrypted files. Needless to say, demands of that nature can cripple or destroy a business very quickly.

Funds transfer fraud resulting from business email compromise, invoice manipulation, and domain spoofing is also a high threat level risk. Coalition's report noted that they observed a 35% increase in funds transfer fraud and social engineering claims since the onset of COVID-19.

The best way to combat ransomware is to identify your business' vulnerabilities, and prepare for the possibility of exposure. Below are a few actions a business owner must implement in order to protect their company from a ransomware attack:

- Keep your software patched and hardware up to date on firmware releases to reduce vulnerabilities. Outdated hardware and software is more susceptible to a cyber-attack.
- Back up your data and store the backup, both, off-site and off-line. Schedule backup recovery tests, so that it doesn't become a "set it and forget it" process.
- Train your staff to recognize suspicious emails and challenge them regularly. Educate them on social engineering and funds transfer fraud. Your staff should be able to recognize and know how to report any suspicious activity in their own inbox.
- Use two-factor authentication apps and strong passwords to ensure every login is a secure one.
- Mitigate cyber risk by buying appropriate coverage.

We've written numerous blogs on cyber risk to provide clients and friends of the firm with ways to identify and mitigate such risks, and below are links to these blogs and articles.   As cyber criminals are finding a more innovative ways to breach systems please use them as resources to help identify and thwart their attempts

4 Cyber Security Tips for Businesses with Remote Workers

Cyber Security During a Pandemic

3 Types of Employees that Expose Organizations to Cyber Risk

If you have any questions relating to cyber risk or need help mitigating cyber risk issues, please contact Jon Edwards, Partner, Cyber Risk Advisor, at 732-395-4281 or jedwards@thealsgroup.com.

[1] https://www.businessinsurance.com/article/20200911/NEWS06/912336571/Ransomware-demands-rise-sharply-in-H1-San-Francisco-Coalition-Inc-COVID-19-coron

Topics: Cyber Risk, Cyber Security, Ransomware, cyber attacks, COVID-19