Alvaka Networks

Rapid Response for Secure IT Infrastructure

Ransomware is the most profound threat facing companies and government entities of all sizes in the 2020s. As new victims emerge daily in all business segments, no company is safe. Cyber criminals use ransomware attacks as a way to hold entire organizations hostage and extort the maximum amount of money from them. Today, we are seeing ransoms typically falling in the $1M to $20M range. Ransomware victimization poses both technical and business challenges, as it cripples operations of the companies that are hit. In these situations, businesses require a rapid response team to respond to the threat immediately, no matter the time of day or year. And very few IT service and security firms can respond 24 hours a day.

Alvaka Networks is a US-based firm that operates nationwide servicing clients who are in desperate need of immediate help, and providing services 24x7, 365 days a year. Even if it's 2 AM on December 25th, they will be available to respond. Almost no one else has that capability.

Oli Thordarson,
President and CEO

In an interview with CIO Applications, Oli Thordarson, President and CEO of Alvaka Networks, sheds light on their rapid response service to IT and security problems.

Please give us an overview of Alvaka Networks.

We help companies manage and secure their IT infrastructure, focusing on businesses that run 24/7, the non-stop businesses of the new economy. We are first responders to cyber breach incidents. Our experience also brings unique insight into preventing hacks in the first place. Since the threat actors' pricing methodologies vary, improper handling of the case by the victim—or an unqualified team they hire—can sometimes double or triple the ransom. In the most tragic situations, there is no recovery at all. Alvaka mitigates the damages the clients incur and gets them back up-and-running fast. We have performed ransomware recoveries for some of the largest global brands and bring a higher level of competence to the rapid recovery of paralyzing ransomware attacks. Our Ransomware R.E.S.U.E. Kit is a first of its kind device we utilize to speed recoveries.

How has the trend to work-from-home impacted organizations from a security standpoint?

The 2020 global pandemic has created turmoil by forcing companies to work from home, creating security issues they did not anticipate. Failure to implement proper security practices has led to cyber breaches; and failure to have good backups and test disaster recovery compounds the pain when disaster does happen. This causes debilitating revenue loss, additional expenses, and loss of valuation associated brand damage.

What process do you follow to deliver your services?

Most companies have a reactive approach to breaches rather than taking preventive measures to deal with threats. Therefore, we continually warn our clients about vulnerabilities and urge them to follow our recommended

Our Ransomware Rapid Response Team restores a victim's business operations in the fastest and most secure process available

security precautions. In case of an attack that has already happened, we follow a proven counter-attack plan to detect the hackers and eject them from the system. The initial steps of the recovery are to create a containment list that stops the attack and hardens the system, so that the company can get back online and back to business. If the recovery effort is done haphazardly, the risk of reinfection during the recovery process is quite likely. Our comprehensive process outlines each step in the recovery effort, executes the recovery to restore business operations, and then implements a new System Security Plan to protect from further attacks.

Explain the method that you follow while helping your clients get their business back up and running?

We start by communicating with all the decision-making stakeholders. This includes the company's top IT management, CEO, CFO, cyber breach lawyers, the Alvaka Recovery Team, and possibly a cyber breach experienced public relations firm. Our Recovery Team then figures out how the breach took place and what data is encrypted. We also examine whether any data was exfiltrated from the network in an attempt by the hackers to further extort the victim. We request that clients engage experienced cyber breach lawyers to provide legal guidance. Engaging lawyers provides attorney/client privilege to keep the findings confidential. The initial scope of work to discover what happened usually costs about $50,000. Once that is complete, a rough recovery budget can be determined. There is often not a viable backup because the hackers deleted that as part of their attack. In such situations, we negotiate the ransom amount down as much as possible, usually between 15 percent to 50 percent less.

Before paying the ransom, we make sure that the ransomer is not on the US government's list of forbidden companies. That list is managed by the Office of Foreign Assets Control (OFAC), a division of the U.S. Department of the Treasury that administers and enforces money laundering laws and payments to terrorists.

What does the future look like for Alvaka Networks?

Ransomware attacks continue to grow at an alarming pace, and the cost of ransoms and recoveries are rising dramatically each quarter. All sectors of business and government are getting hit hard. No company has safe harbor from these criminals. Therefore, Alvaka is continually spreading awareness and sharing resources around ransomware, in addition to educating our clients on how to protect themselves. It is a constantly shifting landscape. The protection measures need to be constantly updated, as well as our Ransomware R.E.S.U.E. Kit toolset. We live in a very dangerous online world of commerce, and our goal is to be a source of guidance to companies seeking a more secure IT environment.