protiviti®
Face the Future with Confidence

Are You in the Ransomware Sweet Spot?

Over the July 4, 2021 weekend, the Russia-based REvil hacker group perpetrated a ransomware attack on Kaseya software. The software is used by managed service providers (MSPs) to operate their clients' networks. This attack reportedly shut down 800-1,500 small-to-mid-size clients of around 50 Kaseya MSP customers.

The attack illustrates the evolution of ransomware. Historically, hackers penetrated systems and exfiltrated intellectual property and/or personal identifiable information, but now, attacks shut down operations altogether. In previous events, distribution might be affected, but paychecks still got cut. Or accounting was disrupted, but orders got filled. Today's ransomware attacks yield more devastating effects, quickly and effectively halting business in its tracks.

Imagine a grocery chain experiencing a ransomware attack. Produce buyers can't place orders online; instead, they're calling vendors to keep stores stocked. Clerks report for work but their inoperative badges lock them out. Cash registers won't open. The payables team resorts to manual payment operations. The ransomware perpetrator demands bitcoin: Has the organisation pre-arranged an account to access bitcoins? Can the transfer be protected with an escrow account?

The Ransomware Sweet Spot

Criminals find ransomware a good business to be in. They're refining their approach. Rather than go after the biggest dollars, they now focus on prosperous mid-sized businesses whose networks are less secure than those of large multinationals with advanced cyber protection.

This "sweet spot" encompasses organisations with the wherewithal to pay ransom, but who haven't achieved full cyber resilience. These businesses may not have segregated networks, and process internal information systems technology on the same networks as their operational technology (OT), and older OT systems which are less secure and easier to penetrate. Recent ransomware victims have included oil pipeline operators Colonial Pipeline (which recovered a portion of the $5M ransom reportedly paid in May), and meat processor JBS (which reportedly paid $11M in June).

If an organisation lacks appropriate defenses, bad actors will find a way to attack. Experience breeds innovation; tomorrow's threats bypass today's defenses. Businesses in the ransomware sweet spot can stay ahead of the curve, however. The approach has roots in business continuity and disaster recovery fundamentals and those fundamentals are extended to encompass anticipating ransomware attacks and responding to and recovering from them if they do occur.

In the past, a business would experience and respond to an attack by creating a team to fend it off. After the crisis, the business would take steps to recover. The approach was reactive in nature and ad hoc in execution. But as cybercriminals evolve ransomware methods, organisations need defenses that are always operating and available. Including secure data backups, held in off-site storage.

An Active Defense Blocks Prospective Perpetrators

Businesses must anticipate threats and counter them with an active defense that blocks prospective perpetrators. Active defense calls for understanding the overall evolving threat landscape, identifying potential threats, software weaknesses and insufficient controls within the organisation. Anticipation means tracking evolving threats actors constantly. Continuous monitoring reported attacks worldwide, industry-wide, and by business size enables leaders detect a potential attack as a component of a strong, timely defense. When businesses anticipate threats, they can execute predefined incident response plans and confidently respond and recover with fewer long-term impacts.

Crisis management plans provide an organisation the ability to respond effectively – with direct countermeasures and well-considered contingency processes. Enterprise-wide crises like ransomware attacks call for a response that draws upon multiple disciplines. When under attack, new requirements arise suddenly from every business function. A crisis management plan addresses all questions that will arise during a ransomware attack. Specialists will contribute expertise in systems, law, human resources, supply chain,

regulations, and other disciplines that the response will demand. New skills will be needed to evaluate threat severity – and the estimated losses. Plans must consider every aspect of managing the crisis while continuing operations.

With a good plan and an expert multidisciplinary response team, businesses can prevail over a ransomware attack. Recovery, however, requires additional activities to return verified working systems, without perpetrator presence. At this time, businesses will have unlocked their systems. They will have applied backups or retrieved data from the bad actors. Now, leaders will want to investigate – and address the aftermath.

Plan Now For Tomorrow's Threats

Paying ransom will not spare the enterprise other negative impacts. New expenses arise, disputes result, and regulations are inadvertently violated when ransomware disrupts operations. A thorough forensic evaluation will ensure every trace of malware is no longer present. and that data is returned to its original state and validated for integrity. Leaders will want to verify that financial reports are accurate.

Recovery is also an opportunity to reflect on what the business has experienced, to debrief with trading partners and other stakeholders. This is the time to capture every lesson – to make the business less susceptible to the next threat. Business leaders in the ransomware sweet spot can act now to fend off attacks like the ones suffered by Kaseya clients, Colonial Pipeline, and JBS. They can look within and outside their own organisations to assemble the specialists they need to anticipate, respond to, and recover from evolving ransomware threats.

As of July 30, the Kaseya website remains dark. On July 23, Kaseya announced they'd acquired a decryption tool so victims could restore the data encrypted by this attack. They've denied they paid ransom to acquire the tool. While several customers made some form of recovery, either with the tool or with hundreds of hours of their own work, others are still struggling. US officials aren't commenting, and Russian officials are denying any knowledge of the situation. Clearly, there is more ransomware news to come.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®