AccumeView: Cybersecurity Pulse

accume partners

Relevant News

The recent string of ransomware attacks against supply chain entities has highlighted how susceptible organizations are to these types of attacks.

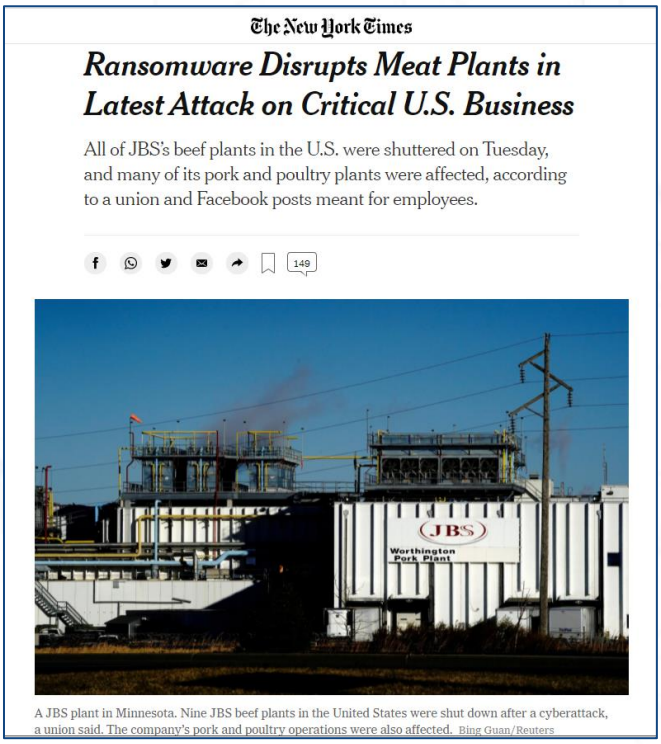
Although the Solarwinds attack in late 2020 and the Microsoft Exchange breach in early 2021 were not ransomware-related, the over-arching effects of those compromises has shown that despite the best efforts of information security programs, there are some serious gaps in how we have been preparing security incidents.

The ransomware attacks on Colonial Pipeline, and more recently, JBS, has, in our view, emboldened ransomware gangs to continue to target the supply chain.

Lack of preparation by these two organizations resulted in approximately $15 million dollars paid out, which doesn't include the financial losses and reputational losses experienced by the organizations from being shut down.

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.



The New York Times

Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business

All of JBS's beef plants in the U.S. were shuttered on Tuesday, and many of its pork and poultry plants were affected, according to a union and Facebook posts meant for employees.

A JBS plant in Minnesota. Nine JBS beef plants in the United States were shut down after a cyberattack, a union said. The company's pork and poultry operations were also affected. Bing Guan/Reuters

Accume's Perspective

As a cybersecurity professional, the first question I hear is "what could my organization do to prevent this from happening to us?" Unfortunately, there is no silver bullet that can protect you from these types of attacks. There must be a layering of different processes and methodologies working together to build and maintain a moving, living security architecture.

Picture if you will, the human body…it takes all our organs working together to ensure life. Should any of those organs fail, the body as a whole cannot continue. Unfortunately, it appears as though many of the supply chain vendors we rely on to provide services have fallen into a state of complacency, and that complacency is what is allowing these ransomware gangs to find success.

What can we do? First, organizations need to have a stronger due diligence processes in place for third-party vendors, particularly in the supply chain. Cyber due diligence is designed to identify risks that cyber criminals may be able to exploit and in turn, provide remediation efforts to address those issues. Such due diligence is not merely document collection and review, it is deep, probing and based on direct evidence.

By engaging in these third-party due diligence efforts, organizations can force their vendors to take the required actions necessary to safeguard their networks and their data. It becomes more than simply checking off a box that says "yes we do that" and provides an in depth look into processes and procedures leveraged by your third-party vendors to ensure they are doing the right thing to protect your data and our networks. For those who use managed services providers, dig deep; they are critical supply side providers whose controls should be examined closely.

Although still in draft format, NIST recently released SP 800-161, Cyber Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations. Even though the guidance is still open for public comment, the approach of applying risk management activities such as evaluating implementation strategy, risk assessments and mitigation as a means to supplement due diligence practices should allow organizations to better prepare for cyber attacks against third-party vendors and supply chain dependency.

Recommended Actions to Take

In keeping pace with the types of actions organizations can take, let's look closely at event and log monitoring. The reality is that despite our best efforts, chances are that we will encounter a breach at some point! As dire as that may seem, there are actions that we can take to ensure the response time to a breach minimizes the effects. Active log and event monitoring provides that ability.

In the case where ransomware infiltrates a network, active event monitoring would provide the notification needed to provide an actionable response. A properly configured Security Information and Event Management tool (SIEM) can provide alerts to notify security personnel of excessive encryption of files on the network, any escalation of account privileges, or excessive deletion of files.

These types of events are designed to alert management/security of anomalous activity and should evoke a dedicated response. Whether that response is to lockdown any suspicious account activity or isolate an affected network segment to prevent the spread of ransomware, the ability to actively respond to these events could be the difference between a minor breach or headline news.

Technology solutions such as Managed Detection and Response (MDR) and/or Extended Detection and Response (XDR) are becoming more commonplace, and their ability to integrate into SIEM solutions offers the ability to allow earlier detection of cyber-related threats across the network.

Recommended Actions to Take (continued)

Review, Update, Test

One of the most important actions an organization can take is to ensure their disaster recovery and business continuity programs are reviewed, updated, and tested annually.

As simple as this may sound, there are many facets to establishing an effective disaster recovery plan. Performing tabletop exercises for simulated events ensures that personnel are aware of their roles and the actions required without having to experience an actual breach or compromise.

Tabletop activities are also great in identifying areas within a disaster recovery plan that don't work for all scenarios. It allows for fine-tuning of specific actions to solidify the response and recovery steps. In performing annual testing, an organization can also validate data backup procedures and restoration. The last thing an organization wants to experience is an event where data is lost, only to find out data restoration procedures from backup do not work!

A Final Tip: Recovery and Business Continuity

Make sure that all members of the recovery team keep a printed copy of the plan. There have been several reported incidents of organizations being hit with ransomware that discovered during the event that all copies of their recovery plans were in digital format and encrypted along with all the organization's data. Being hit with ransomware is bad enough. Don't make it worse by being unprepared!

About the Author

Gabe Morales is Accume Partners' Senior Manager in the Technology Risk, IT Audit & Cybersecurity Group. Gabe has over 20 years of experience in the information technology (IT) industry, including system certification and accreditation, information systems auditing and security awareness.

His extensive experience includes vulnerability analysis, penetration testing, social engineering, risk assessment and management, host and network-based security IT auditing, workstation and server hardening and auditing, project management, information assurance and development of technical policies and documentation.

Have any further questions or concerns? We are here to help!

Call

888-696-1515

Email

info@accumepartners.com