Protecting manufacturing systems against ransomware attacks

The importance of migrating critical business systems to the cloud

Ransomware on the rise

As manufacturing organizations continue to become more digitized, cyberattacks have increased in prevalence over the past decade. Recent attacks on U.S. companies such as Colonial Pipeline have revealed the severity of these threats, the frequency at which they're occurring, and exposed the potential impacts to our economy.

The risk is real – all it takes is one employee clicking a malicious link and an entire organization could be infiltrated and systems locked down. To minimize risk, companies have placed a heightened focus on cybersecurity, ensuring employees are trained to recognize suspicious activity and critical business systems are protected from potential attacks.

Implications to manufacturing

The costs associated with ransomware attacks are substantial. According to Purple Sec, an organization specializing in cybersecurity, the estimated cost of ransomware attacks in 2020 was $20 billion, including direct costs, and associated system downtime.[1]

With manufacturing organizations operating 24/7, the costs are amplified. Every minute of system downtime can cause significant financial damages due to lost production. Not to mention the potential downstream issues to the supply chain. Manufacturers cannot afford to fall victim to cyberattacks, yet according to a report released by Morphisec, one in five manufacturing companies in the U.S. and UK have been victims of a cyberattack in the last 12 months.[2]

Potential responses

Once a system is infiltrated, organizations typically only have two options to restore access. Option one, they can choose to pay the ransom demand in hopes that the hacker will restore access, which can come with a hefty price tag. In the instance of the Colonial Pipeline, that price tag was $4.4 million.[3] Even this is not a surefire approach, as in many cases hackers don't even possess the ability to restore access due to the special encryption used. Not to mention, it will make that organization a prime target for future ransomware campaigns. Most experts advise the second option, which is to consult with an IT firm to restore and potentially rebuild their systems. Depending on the severity, this can also be an extremely expensive option.

1 in 5

manufacturing companies in the U.S. and UK have been victims of a cyberattack in the last 12 months.

Protect operational systems in the cloud

The most effective way to protect the organization from cyberattacks is to ensure all critical business systems are maintained to the highest degree. This includes incorporating strict security standards, maintaining version currency, and regularly backing systems up. The easiest way to accomplish this is to migrate business systems into the cloud.

Hosting systems in an on-premise environment requires extensive and expensive in-house IT resources. By moving to the cloud, the required security measures are handled by the technology vendor delivering the solution. This frees organizational IT resources up to work on more strategic initiatives rather than software and server maintenance of third-party systems.

Maintain system currency

Running out-of-date software leaves an organization extremely vulnerable to cyberattacks. In 2017, the famous WannaCry ransomware attacks affected around 250,000 machines and was estimated to cause roughly $4 billion in damages.[4] The machines that were targeted were those running out-of-date software that Microsoft had issued a patch to several months prior.

Cloud-based solutions allow for automatic updates to the newest version once it is released by the developer. Usually, smaller updates that contain bug fixes and security patches will occur every few weeks. Major updates have larger intervals such as quarterly or annually. While there is usually a period after the release when the update is optional, it will eventually become required. When operating in the cloud, organizations can rest assured their systems are always operating on the current version containing all security patches.

Network security and privacy protection

By leveraging a cloud-based technology solution, manufacturers can ensure that their data is being protected by the latest and greatest security features. While an organization could implement the same security standards themselves, it's expensive and can be cost prohibitive for individual companies.

Cloud vendors are responsible for protecting the data of their customers, so security and privacy are top priorities – their reputation depends on it.

$20 billion

was the total estimated cost of ransomware attacks in 2020, including direct costs and associated system downtime.

As a result, cloud technology vendors spend millions of dollars on the best cybersecurity protection available and their customers reap the benefits. And because they can distribute these costs across their entire customer base, it's much more cost effective for individual clients.

To ensure maximum protection of their customers, leading cloud providers will also conduct regular vulnerability testing of their solutions. If there are any areas of weakness in the system, they are quickly identified and addressed.

Protect workforce data

Modern manufacturing organizations leverage a host of different systems to achieve operational objectives. Any one of these systems is potentially susceptible to a data breach and must be properly maintained to ensure its security.

Among the most important are workforce management and human capital management systems. These solutions contain personally identifiable information (PII) about their employees including names, Social Security numbers, addresses, and bank account information for direct deposit, just to name a few. If this information gets into the hands of cyber criminals, the organization could become liable to class action lawsuits and substantial fines. Such breaches could also lead to feelings of distrust among employees as well as customers who may be concerned about their own data falling into the wrong hands.

Act now – move to the cloud

As ransomware attacks continue to increase and the associated costs keep rising, it's paramount that manufacturers begin the process of migrating their critical business systems into the cloud. Start by protecting your employees' data today.

1. https://purplesec.us/resources/cyber-security-statistics/ransomware/.
2. https://engage.morphisec.com/2021-manufacturing-cybersecurity-threat-index.
3. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.
4. https://www.securitymagazine.com/articles/92235-how-to-protect-your-organization-from-ransomware.

Learn more about migrating your critical workforce solutions to the cloud today!

VISIT UKG.COM