Manufacturing's Simple Phishing Expedition

Cybersecurity Series

By Michael Weller, Chief Technology Officer Manufacturing, Verizon Business

Manufacturing is more connected than ever, thanks to the maturation of 5G and the rise of IoT devices. Improved connectivity and greater bandwidth can enable manufacturers to harness data on the factory floor and across the supply chain in near real time. This capability delivers tremendous benefits, including superior machine maintenance and supply chain management, but it also creates new potential points of entry for threat actors to exploit. The cybersecurity stakes are high in manufacturing. A threat actor who has gained access to the manufacturer's network can hold machines and entire production lines hostage. To mitigate the threat, manufacturers must understand the threat. The following are some of the biggest cyber threats in manufacturing and what can be done to help counteract them.

A simple phishing expedition

There's a prevailing misconception about a lot of threat actors: They're criminal masterminds who use the most cutting-edge technologies to break into digital Fort Knoxes. The truth, however, is that a large number of them gravitate toward the quickest, easiest routes to a payday. One of the most straightforward social engineering tactics, phishing, is on the rise in manufacturing. Social engineering in general has remained a steady breach tactic, but according to the 2024 Data Breach Investigations Report (DBIR), phishing now makes up more than half (55%) of social engineering attacks.

Phishing may be a simple tactic, but it can metastasize into wider data breaches. Threat actors often use phishing to steal a network user's credentials, which occurs in a quarter of manufacturing data breaches. Stolen credentials pave the way for system intrusion, the most common attack type in manufacturing. At this point, a threat actor could be positioned to steal valuable IP. Imagine, for instance, if a hacker manages to obtain blueprints of a next-generation electric motor. Such a data breach may cause both financial and reputational damage as well as compromise an automaker's position within the industry.

A threat actor who has gained access to a manufacturer's network may also deploy ransomware or other malware. Ransomware, which is deployed in almost 40% of data breaches, can be especially threatening in a manufacturing setting, since manufacturers cannot afford protracted downtime in the event machines or production lines are down.

verizon business

As such, manufacturers feeling the mounting pressure to meet production deadlines may give in to a ransom, perceiving the concession as the lesser of two evils. Threat actors know that time-sensitive business operations can be used to create urgency and increase the likelihood of having their demands met. That's why malicious actors target retailers during the holiday season. All of which may have started with a simple phishing expedition.

A not-so-special delivery

The majority of data breaches in manufacturing are caused by external actors, but that hardly means there are no internal threats. More than a quarter (27%) of data breaches are caused by internal actors, the majority of which are made up of miscellaneous errors. Misdelivery, which is also prevalent in other industries such as healthcare, accounts for almost half (48%) of error-related breaches. Even an innocent mistake, like sending correspondence to an unintended recipient, can lead to data breaches with serious consequences.

Vigilance – the first line of defense

In an increasingly connected industry, manufacturers should invest in robust cybersecurity solutions, but even the most advanced security systems can't prevent human error. This year's DBIR has revealed that manufacturers too often fall prey to simple threats, regardless of whether they're malicious or not, internal or external. Organizations can't eliminate the risk of cyberattacks, but manufacturers can certainly do a better job of preventing the preventable.

It is possible to reduce the incidence of phishing as an industry. The retail industry saw a marked drop in phishing last year, for instance. It's a matter of educating employees about cybersecurity best practices, including common phishing scenarios, and running simulations to test their knowledge. Phishing, just like social engineering as a whole, relies on human error. Training one's workforces can help reduce those errors, effectively preventing the success of phishing attacks.

In a sense, misdelivery is the internal version of phishing because it depends on a lapse in vigilance or judgment. It's harder to train for misdelivery, but it is possible to limit the impact of misdelivery by implementing strict access controls. People will always make mistakes, but if their network access is customized to their role and function, what data they can access and how they can share data is limited. Even if they make a mistake, the consequence can be blunted.

People will always make mistakes, but if they're knowledgeable and systematic guardrails are in place, they should make fewer mistakes.