The recent Cisco announcement of a breach may have many people rolling their eyes and wondering, “why can’t these companies figure out security?” After all, isn’t Cisco a major provider of security tools, software, and services? While they are a leading software and consultancy service provider in the security space, the reality is that there is very little room for failure in security controls. After all, malicious actors do not need a welcome sign to gain access. They just need one control, process, or vulnerability to not be patched, and then it is game on.

This article is not meant to rehash the technical details of how the breach happened and what took place. Rather, the focus is on what we can learn from the events leading up to and post breach from the Cisco report. With that in mind, let’s dig into some of the lessons we can learn from the information that has been disclosed about this breach.

People are Human

One of the first lessons that can be pulled from this attack is that people are, well, human. Most employees or contractors do not enter the day thinking that they are going to be the cause of a breach or that they may even be a target. They are often focused on doing their job and doing it as well as they can. In that effort, they may look for ways to make their life easier. This was evident by the passwords being stored in a personal Google account. The individual was targeted with the hopes of attaining credentials or other information that could be utilized to conduct the attack. This is a prime example of how security should be looking at not only what controls need to be applied but also how controls can help employees or staff life. Providing a strong password vault that had a layer of MFA attached to it may have saved the credentials from being harvested.

Odd Behavior is Odd

By all reports, Cisco had the recommended controls in place to help protect them. They had MFA implemented on their VPN to ensure that credentials alone would not be enough to compromise their network. Unfortunately, MFA systems can be bypassed by a motivated individual, either through a man in the middle style attack or, in this case, by acting like a toddler at dinner. The attackers essentially annoyed the employee into accepting a login, which allowed them to gain a foothold in the network. The odd behavior that should have been alerted on is the repeated login attempts without a successful MFA authentication. This behavior would be odd by a legitimate employee, and a simple phone call could have identified that the employee had a person account taken over.

Additionally, what we can learn from this is that MFA alone is not enough to prevent an attack. In this case, utilizing a third layer of MFA that validated the system was authorized to connect may have assisted in preventing the attack. However, if the attacker was coming from the device itself, this control would not have helped. If the latter was the case, then a network monitoring device on the endpoint could have indicated that the device had an active SSH or RDP session in place or reverse shell to an external IP address, which would have been strange behavior.

Layers for the Win

Another lesson we can learn from this is that a layered approach to security is required to protect an organization. Cisco was able to confirm that the attackers attempted to deploy ransomware, which was thwarted by security controls on their systems. When this was not successful, the attackers had to resort to other tactics, which allowed them to be detected. By having robust logging and monitoring, Cisco was able to detect and stop the movement of the attackers in their network. As the attackers elevated permissions and attempted to move laterally, these actions were detected due to unusual behavior. Additional monitoring of privileged accounts actions within the environment also assisted in detecting unusual behavior. By focusing on controls that allowed for detections of actions taken inside the network, Cisco was able to determine that they had a compromise, which allowed them to stop it before it was fully mature, conduct a robust investigation, and remediate the issue.

While these are not all the lessons that we could learn from this event, they are some key lessons learned. It is not always clear how a breach happened, and it must be noted that Cisco was incredibly open about their breach, which allows us in the security industry to analyze and attain some lessons learned without having to go through the event ourselves. This further proves that security is a moving target that requires constant assessment and adjustment to thwart, detect, or minimize attacks. It further shows that the largest companies with massive security budgets are not impenetrable and that we should not be so quick to pass judgment.